GİRİŞ

Bu kitap , bilg i güvenliğ i v e toplu m mühendisliğiyl e ilgil i yoğu n bilgile r içermektedir. Yolunuz u bulmanız ı kolaylaştırma k için , işt e siz e kitabı n . içeriğine hızl ı bi r bakış :

Perde Arkas ı başlığınd a güvenliği n e n zayı f halkasın ı açıklayacak , sizin v e şirketinizi n nede n toplu m mühendisliğ i saldırıların a maru z kala - bileceğinizi göstereceğim .

Saldırı Sanat ı başlığında , toplu m mühendislerini n istediklerin i eld e etmek içi n güveninizle, yardımc ı olm a isteğinizle , sevecenliğinizle v e insanî saflıklarınızl a nası l oynadıkları m göreceksiniz . Sı k görüle n saldırılarla ilgil i hayal î öyküle r toplu m mühendislerini n pe k ço k kimliğ e ve yüz e bürünebildiklerin i siz e gösterecek . Eğe r dah a önc e bi r toplu m mühendisiyle karşılaşmadığınız ı düşünüyorsanız , büyü k olasılıkl a yanılıyorsunuzdur. Bakalım , b u öykülerd e dah a önc e sizi n d e yaşadığınız bi r senaryo görece k v e toplu m mühendisliğini n siz e dokunup dokunmadığın ı mera k edece k misiniz ? B u olmayaca k bi r şe y değil. Anca k ikinc i bölümde n dokuzunc u bölüm e kada r okudukta n sonra, siz i araya n il k toplu m mühendisini n nası l hakkında n geleceğiniz i öğrenmiş olacaksınız .

Davetsiz Misafirler e Dikka t adl ı başlıkt a İse , toplu m mühendis - lerinin, şirke t alanınız a girerek , şirketiniz i batıraca k y a d a çıkaraca k sır- ' lan çalıp , sizi n yükse k teknoloj i güvenli k önlemleriniz i atlatara k risk i nasıl artırdığını , uydurm a öykülerl e göreceksiniz . B u başlı k altınd a anlatılan senaryolar , bi r çalışanı n intika m almasında n tutu n da , sana l terörizme kada r oluşabilece k çeşitl i tehditleri n farkın a varmanız ı sağlay - acaktır. Eğe r işletmeniz i ayakt a tuta n bilgiler e v e verilerinizi n güven - liğine değe r veriyorsanız , onunc u v e o n dördünc ü bölümler i başta n sona okuma k isteyeceksiniz .

Aksi belirtilmediğ i takdirde , b u kitapt a kullanıla n tü m öyküleri n uydurma öyküle r olduklarını vurgulamakta yara r var .

Çıtayı Yükseltme k başlığınd a şirke t yaklaşımın ı el e alı p kuru - munuza yapıla n toplu m mühendisliğ i saldırılarını n başarıy a ulaş - malarının nası l engellenebileceğinde n sö z edeceğiz . O n beşinc i bölü m başarılı bi r güvenli k eğitim i program ı içi n bi r tasla k sunmaktadır . V e o n altıncı bölü m ta m hayatınız ı kurtaraca k şe y olabilir ; kurumunuz a uyarlayabileceğiniz, şirketiniz i v e bilgileriniz i emniyett e tutma k içi n hemen uygulamay a geçirebileceğiniz , he r yönüyl e ta m bi r güvenli k kuralları metni .

En sona , işbaşınd a karşılaştıklar ı bi r toplu m mühendisliğ i saldırısın ı önleyebilmeleri içi n çalışanlarınız a yo l göstermekt e kullanabileceğini z kilit bilgiler i özetleye n kontro l listeleri , tablola r v e şemala r içere n

Bir Bakışt a Güvenli k adınd a bi r bölü m ekledim . B u araçla r ayn ı zamanda, kend i güvenli k eğitim i programlarınız ı oluşturmakt a kullan - abileceğiniz değerl i bilgile r d e içermektedir .

Kitapta pe k ço k faydal ı unsurl a karşılaşacaksınız : Teri m kutuları , toplum mühendisliğ i v e bilgisaya r korsanlığ ı terimlerini n açıklamaların ı İçerirler; Mitnic k Mesajlar ı güvenli k stratejiniz i güçlendirmeniz e yardım - cı olaca k kıs a bilgile r sunmaktadır ; notlard a is e e k bilgile r v e ilgin ç ayrıntılar bulunmaktadır .

1

Perde Arkası

GÜVENLİĞİN E N ZAYI F HALKAS I

Bîr şirke t paranı n alabileceğ i e n iy i güvenli k teknolojilerin i satı n almış; çalışanlarını , akşa m ev e giderke n he r şeylerin i kili t altın a alaca k şekilde so n derec e iy i eğitmi ş v e bin a güvenli k görevlilerin i sektörü n e n iyi güvenli k şirketinde n kiralamı ş olabilir .

Bu şirke t yin e d e tamame n savunmasızdır .

Bireyler, uzmanları n önerdiğ i e n iy i güvenli k uygulamaların ı çalıştırıyor, önerile n he r güvenli k ürünün ü bilgisayarın a yüklüyo r olabilir - ler v e uygu n siste m yapılandırmasın ı v e güvenli k yamaların ! kullanma k konularında so n derec e dikkatl i davranabilirler .

Bu bireyle r yin e d e tamame n savunmasızdırlar . \ .-• - • : ., •

İnsan Unsur u

Yakın bi r geçmişt e Kongre'y e ifad e verirken , başk a biris i gib i davra - narak v e yalnızc a b u bilgiy i isteyerek , şifreler i v e diğe r hassa s bilgiler i çoğu zama n şirketlerde n alabildiğim i anlattım .

Tam anlamıyl a güvend e olduğun u bilmey i isteme k doğa l bi r duygudur am a bu , pe k ço k İnsanı n saht e bi r güvenli k hissiyl e yetinme - sine d e nede n olur . Karısını , çocukların ı v e evin i koruma k içi n ö n kapısı - na, maymuncukl a açılama z olara k bilinen , Medic o mark a bi r silindirl i kili t taktırmış, sorumlulu k sahib i v e sevece n bi r e v sahibin i düşünün . Davetsiz misafirler e karş ı ailesin i güvencey e aldığ ı içi n iç i rahat . Am a pencereyi kıra n y a d a gara j kapısını n şifresin i boza n hırsızlar a n e ola - cak? Güçl ü bi r aiar m sistem i yerleştirme k dah a iy i olurd u anca k yin e d e bir garantis i yok . Pahal ı kilitle r olsu n y a d a olmasın , e v sahibini n saldırıya açı k olm a hal i deva m ediyor .

Neden? Çünk ü İnsa n unsur u aslınd a güvenliği n e n zayı f halkasıdır .

Güvenlik çoğ u zama n bi r yanılgıda n ibarettir , jşi n için e dikkatsizlik , saflık v e cahilli k d e girinc e dah a d a köt ü olur . Yirminc i yüzyılı n e n saygı n bilimadamı ola n Alber t Einstei n şöyl e demiştir : "Yalnızc a ik i şe y sonsuz - dur, evre n v e insanoğlunu n aptallığı ; aslınd a evreni n sonsuzluğunda n o kadar d a emi n değilim. " Sonu ç olarak , insanla r aptailars a y a d a dah a sık görüle n şekliyle , doğr u güvenli k uygulamalar ı konusund a bilgisiz - lerse, toplu m mühendisliğ i saldırılar ı başarıl ı olmaktadır . Pe k ço k bi - lişim teknolojiler i (BT) sektör ü çalışanı , güvenli k bilincin e sahi p ail e

A Aldatm a Sanat ı

reisimizle ayn ı yaklaşım ı kullanarak , güvenli k duvarları , müdahaleler i ortaya çıkarm a sistemler i y a d a dah a güçl ü tanım a sistemler i ola n zaman tabanl ı kartla r v e biyometri k akıll ı kartla r gib i herkesç e kabu l gör - müş güvenli k ürünler i kullandıklar ı içi n şirketlerin i saldırılar a karş ı büyü k ölçüde güvend e tuttuklar ı doğrultusund a yanlı ş bi r kanıy a sahiptirler . Güvenlik ürünlerini n te k başların a ta m bi r güvenli k sağlayacağın a inanan biri , güvenli k konusund a kendin i kandırıyo r demektir . B u anca k hayal alemind e görülebilece k bi r durumdur . B u insanla r e r y a d a geç , kaçınılmaz olara k bi r güvenli k sorun u yaşayacaklardır .

Tanınmış bi r güvenli k danışman ı ola n Bruc e Schneier'ı n d a dediği gibi, "Güvenli k bi r ürü n değil , bi r süreçtir. " Dahası , güvenli k bi r teknoloj i sorunu değildir ; bi r insa n v e yöneti m sorunudur .

Araştırmacılar sürekl i olara k dah a iy i güvenli k teknolojiler i geliştiri p teknik açıklar ı sömürmey i gidere k zoriaştırınca , saldırganla r insa n unsurunu sömürm e yolun a dah a ço k gideceklerdir , insanları n güvenli k duvarını kırma k genellikl e dah a kolaydı r v e bi r telefo n görüşmesinde n başka yatırı m istemediğ i gib i risk i d e ço k düşüktür .

Klasik Bi r Aldatm a Olay ı

İşletmenizin ma l varlığını n güvenliğin e karş ı e n büyü k tehdi t nedir ? Yanıtlaması kolay : toplu m mühendisi ; si z sa ğ elin e bakarke n so l eliyl e sırlarınızı çala n acıması z bi r sihirbaz . B u kiş i çoğ u zama n o kada r arkadaş canlısı , samim i v e yardımseverdi r k i onuni a karşılaştığınız a şükredebilirsiniz bile .

Bîr toplu m mühendisliğ i örneğin e bakalım : Bugü n pe k ço k insa n Stanley Mar k Rifki n adındak i gen ç adam ı v e artı k va r olmaya n Lo s Angeles'taki Pasifi k Hisseler i Ulusa l Bankası'yl a ola n macerasın ı hatır - lamaz. Gerçekt e n e olduğuyl a ilgil i çeşitl i rivayetle r vardı r v e Rifki n de , benim gibi , hikâyesin i kend i ağzında n hiçbi r zama n anlatmamıştır . B u yüzden aşağıdakile r yayımlanmı ş makalelerde n derlenmiştir .

Şifre Kırma k

1978 yılınd a bi r gü n Rifkin , Pasifi k Hisseteri'ni n yalnızc a yetkil i per - sonelinin girebildiğ i v e odadakileri n he r gü n milyarlarc a dola r tutarınd a havale gönderi p aldıklar ı haval e odasın a doğr u yollandı .

Ana bilgisayarı n çökmes i olasılığın a karşı , haval e odasını n veriler i içi n yedekieme sistem i geliştirece k bi r şirkett e sözleşmel i olara k çalışıyordu . Bu görevi , bank a yetkililerini n havaleler i nası l gönderdikler i d e dahi l olma k üzere, tü m haval e süreçlerin i öğrenmesin i sağlamıştı . He r saba h haval e yapmaya yetkil i bank a çalışanlarına , haval e odasın ı aradıklarınd a kullan - maları için , özenl e koruna n günlü k bi r şifreni n verildiğin i öğrenmişti .

Güvenliğin E n Zayı f Halkas ı

Havale odasındak i memurla r he r gü n değişe n şifrey i ezberleme k içi n kendilerini yormuyorlardı : Şifrey i küçü k bi r kâğıd a yazı p kolayc a görebile - cekleri bi r yer e asıyorlardı . Kası m ayını n ta m o gününd e Rİfkin'i n oday ı ziyaret etmesini n öze l bi r neden i vardı . O kâğıd a bakma k istiyordu .

Havale odasın a gelerek , çalışm a süreçleriyl e ilgil i notla r aldı ; güy a yedekieme sistemini n olağa n sistemlerl e ta m olara k Örtüştüğünde n emin olma k istiyordu . B u sırad a asıl ı kâğıttak i güvenli k şifresin i gizlic e okudu v e ezberledi . Birka ç dakik a sonr a dışar ı çıktı . Dah a sonr a söylediğine göre , o a n kendin i piyangod a büyü k ikramiyey i kazanmı ş gibi hissetmişti .

Bir D e İsviçre'dek i Ş u Bank a Hesabına.. .

Öğleden sonr a saa t ü ç sularınd a odada n çıkmış , doğruc a binanı n mermer kaplamal ı girişindek i telefo n kulübelerin e gitmiş , telefon a jeto n atarak haval e odasını n numarasın ı çevirmişti . Sonra , telefond a başk a bir kılığ a bürünmüş , kendini , bank a danışman ı Stanle y Rifkin'den , bankanın Uluslararas ı İşlemle r Birimi'ni n bi r çalışan ı ola n Mik e Hansen'a dönüştürmüştü .

Bir kaynağ a göre , yapıla n görüşm e aşağıdak i gib i gelişmişti :

"Merhaba, be n Uluslararas ı İşlemler'de n Mik e Hansen, " ded i Rifkin , telefonun diğe r ucundak i gen ç kadına .

Kadın ofi s numarasın ı istedi . B u olağa n bi r soruyd u v e Rifki n hazır - lıklıydı: "286, " dedi .

Kadın sonr a "Peki , şifr e nedir? " diy e sordu .

Rİfkin'in adrenalini n etkisiyl e zate n hızl ı ata n kalb i o and a iyic e hız - landı. Duraksamada n yanıtladı , "4789. " Sonr a haval e talimatların ı ver - meye başladı : Ne w Yor k Irvin g Yatırı m Ortaklığı'nda n Züri h VVozcho d Handels Bankası'ndak i hesab a yatırılma k üzer e "ta m olara k o n milyo n iki yü z bi n dolar. " B ü hesab ı öncede n kendis i açtırmıştı .

Kadın söylenenler i no t edip , "Tamam , bilgiler i aidim . Şimd i d e birim - ler aras ı taka s numarasın a ihtiyacı m var. " ded i

Rİfkin'in başında n aşağ ı kayna r sula r döküldü ; b u beklemediğ i bi r soru, araştırmasınd a unuttuğ u bi r ayrıntıydı . Am a soğukkanlılığın ı koruyup he r şe y yolundaymı ş gib i davrand ı v e hi ç beklemede n ceva p verdi, "Bi r kontro l edeyim ; siz i heme n ararım. " B u ke z bankanı n başk a bir birimin i arama k içi n tekra r telefond a kılı k değiştirere k haval e odasın - daki bi r çalışa n gib i davrandı . Taka s numarasın ı öğrend i v e gen ç kadın ı yeniden aradı .

Genç kadı n numaray ı ald ı ve , "Teşekkürler " dedi . (B u koşulla r altında , teşekkür etmes i gerekeni n aslınd a Rifki n olmas ı gerektiğ i söylenebilir.)

6 Aldatm a Sanat ı

Amaca Ulaşılmas ı

Birkaç gü n sonr a Rifki n İsviçre'y e uçtu , parasın ı ald ı v e 8 milyo n dolarını bi r yığı n elma s karşılığınd a bi r Ru s acentasın a verdi . Tekra r uçağa bind i v e taşlar ı bi r par a kuşağın a saklayara k A.B.D . gümrüğün - den geçti . Tarihtek i e n büyü k bank a soygunun u yapmışt ı v e bun u bi r silah, hatt â bi r bilgisaya r bil e kullanmada n gerçekleştirmişti . Tuha f olan , işlediği suçu n bi r sür e sonr a "e n büyü k bilgisaya r dolandırıcılıkları " başlığı altınd a Güinnes s Rekorla r Kitabı'nı n sayfalarınd a ye r almasıydı .

Stanley Rifkin'i n insanlar ı aldatm a sanatınd a kullandığ ı b u becer i v e teknikler bütünün e artı k toplum mühendisliği diyoruz. Aslınd a b u i ş içi n gerekenler özenl i bi r planlam a v e iy i la f yapm a yeteneğinde n ibaret .

Ve b u kitabı n konus u işt e b u -bendenizi n ustas ı olduğu - toplu m mühendisliği teknikler i v e şirketini z üzerind e kullanılmalar ı durumund a nasıl karş ı savunm a yapacağınız .

Tehlikenin Boyut u

Rifkin'in öyküsü , güvend e olduğumu z hissini n n e kadar.yanlı ş bi r düşünce olduğun u mükemme l bi r şekild e açıklıyor . B u tar z olayla r -belk i 10 milyo n dolarlı k vurgunla r değ i l ama - he r gü n oluyor . Ş u and a pa - ralarınız gidiyo r olabili r y a d a biriler i yen i ürünlerinizi n tasartmlartn ı çalıyor olabili r v e si z bunu n farkınd a bil e değilsiniz . Eğe r şirketinizi n başına henü z böyl e bi r ola y gelmediyse , sormanı z gereke n şe y bunu n olup olmayacağ ı değil , n e zama n olacağı .

Artan Endiş e

Bilgisayar Güvenliğ i Enstitüsü'nün , 200 1 yılınd a bilgisaya r suçlarıy - la ilgil i yaptığ ı araştırmay a göre , geçe n o n ik i a y içerisind e araştırmay a katılan kuruluşları n yüzd e 85'ini n bilgisayarların a yetkisi z giri ş yapılmış . Bu şaşırtıc ı bî r rakam : Araştırmay a katıla n he r yü z kuruluşta n yalnızc a on beş i yı l boyunc a güvenli k ihlâf i yaşamadığın ı söyleyebilmiş . Bi r o kadar şaşırtıc ı ola n başk a bi r ver i d e bilgisayarların a izinsi z girişle r sonucunda mal i zarar a uğraya n kuruluşları n oranı : yüzd e 64 . Te k bi r yı l içerisinde kuruluşları n yansında n fazlas ı mal i zarar a uğramış .

Kendi deneyimleri m b u tar z araştırmalardak i rakamları n bira z abartılı olduğun u söylüyor . Araştırmay ı yapa n kişileri n niyetlerinde n kuşkuluyum. Am a bu , zararı n a z olduğ u anlamın a gelmez. Zara r büyük . Güvenlik ihlâllerin e karş ı hazırlıkl ı olmayanlar , aslınd a kaybetmey e hazırlanıyorlar.

Pek ço k şirkett e kullanıla n ticar i güvenli k ürünleri , çoğunlukla , yazılımcı veletler olara k biline n amatö r bilgisaya r korsanların a karş ı

Güvenliğin E n Zayı f Halkas ı

koruma sağlamay ı amaçlamaktadırlar . İnternette n indirilmi ş programla r kullanan b u yeniyetm e korsanla r çoğ u zama n bira z rahatsızlı k vermek - ten ötey e gidemiyorlar . Büyü k kayıpla r v e

gerçe k tehlike , madd i bi r kazanç sağlamay a güdülenmiş , hedefler i iy i tanımlanmış , planl ı saldır - ganlardan geliyor . B u İnsanlar , amatörle r gib i birço k sistem e birde n girmeye çalışmaktansa , he r seferind e te k bi r hede f üzerind e yoğun - laşıyorlar. Amatö r korsanla r sayıy ı ço k tutmay ı amaçlarken , profes - yoneller kalitel i v e değerl i bilgiy i hedefliyorlar .

Kimlik tespit i içi n kullanıla n tanım a araçları , siste m özkaynaklann a ve dosyalar a erişimi n yönetilmes i içi n erişi m kontrol ü sistemler i v e hırsı z alarmlarının elektroni k karşılığ ı ola n izinsi z girişler i tespi t sistemler i gib i teknolojiler, bi r şirke t güvenli k program ı içi n önemlidirler . Yin e d e şir - ketler, güvenli k önlemlerin e yatırı m yapmaktansa , kahvey e par a harca - mayı yeğliyorlar .

Suçluların akl ı nası l su ç işlemey e yöneli k çalışıyorsa , bilgisaya r kor - sanının d a akl ı güçl ü güvenli k teknolojilerini n açıkların ı bulmay a yöneli k çalışır. Çoğ u zama n d a bun u teknolojiy i kullana n kişiler i hedefleyere k yaparlar.

Yanıltıcı Uygulamala r

En emniyetl i bilgisayarı n kapal ı bi r bilgisaya r olduğun a dai r yaygı n bi r söz vardır . Akıllıc a am a yanlış : Ar t niyetl i bi r kiş i ofis e gidi p bilgisayar ı açması içi n birin i ikn a edere k iş i bitirir . Elinizdek i bilgiy e sahi p olma k isteyen bi r rakibiniz , çoğ u zama n va r ola n pe k ço k farkl ı yolda n birin i kul- lanarak on u eld e edebilir . B u i ş yalnızc a zamana , sabırl ı olmaya , kişiliğ e ve ısrarcılığ a bakar . İşt e b u noktad a aldatm a sanat ı devrey e girer .

Bir saldırganın , davetsi z misafiri n y a d a toplu m mühendisini n güven - lik önlemlerin i atlatma k amacıyla, bilgisin i paylaşaca k güvenili r bi r kul- lanıcıyı kandırmas ı y a d a hiçbi r şeyde n kuşkulanmaya n bi r hedef i on a giriş hakk ı tanımas ı içi n aldatmas ı gerekir . Güvenili r çalışanlar , hassa s bilgileri paylaşmalar ı içi n y a d a saldırganı n içer i sızmasın ı sağlayaca k bir güvenli k açığ ı yaratmalar ı içi n kandırılabildiklerinde , ikn a edilebildik - lerinde y a d a yönlendırilebildiklerind e dünyadak i hiçbi r teknoloji bi r şir - keti koruyamaz . Tıpk ı şifr e çözümleyicilerini n şifr e teknolojisin i bertara f edecek bi r açı k bularak , şifrelenmi ş bi r mesajı n içeriğin i öğrenebildikler i gibi, toplu m mühendisler i d e güvenli k teknolojilerin i bertara f etme k içi n çalışanlarınızı aldatm a yöntem i kullanıla n

Güvenin Kötüy e Kullanılmas ı

Çoğu durumda , başarıl ı toplu m mühendislerini n güçl ü İnsa n ilişkiler i vardır. Hızl ı dos t olu p güve n sağlayabilme k içi n gerekl i kişili k özellikle - rine sahip ; yan i etkileyici , nazi k v e seviml i kişilerdir . Deneyiml i bi r toplu m

mühendisi, sanatını n stratejilerin i v e taktiklerin i kullanara k neredeys e hedeflediği he r bilgiy e ulaşabilir .

Yetenekli teknoloj i uzmanlar ı alı n ter i dökere k bilgisaya r kullanımın a bağlı riskler i e n az a indirgeme k içi n bilg i güvenliğ i çözümler i üretmişler , ancak e n zayı f halk a ola n insa n unsurun a dokunmamışlardır . Tü m zekâmıza karşın , bi z insanla r -siz , be n v e diğe r herkes - birbirimizi n güvenliğine yöneli k e n büyü k tehdid i oluşturuyoruz .

Ulusal Karakterimi z

Özellikle Bat ı dünyasında , b u tar z tehditleri n üzerind e durmuyoruz . Bize birbirimizde n şüphelenmemi z öğretilmiyor . B u e n ço k d a Amerika'da böyle . Biz e "komşumuz u sevmemiz" , birbirimiz e güven - memiz v e inanmamı z öğretilir . Yere l güvenli k örgütlerinin , insanlar ı evlerini v e arabaların ı kilitlemey e ikn a etmelerini n n e kada r zo r olduğunu bi r düşünün . B u tar z açıkları n verilebileceğ i gü n gib i ortadadı r ve haya ! dünyasınd a yaşamay ı terci h ede n pe k çoklar ı tarafında n gö z ardı edilmektedir ; t a k i ağızlar ı yanan a kadar .

Her insanı n iy i niyetl i v e dürüs t olmadığın ı biliyoruz , anca k çoğ u zaman sank i öyl e değillermi ş gib i davranıyoruz . B u muhteşe m saflık , Amerikalıların yaşamlarını n teme l taşıdı r v e bunda n vazgeçme k ac ı verici olacaktır . Bi r ulu s olarak , özgürlü k anlayışımızı n içine , yaşanaca k en İy i yeri n anahtarları n v e kilitleri n e n a z gerekl i olduğ u ye r anlayışın ı da koymuşuz.

Çoğu insan , kandırılm a olasılığını n ço k düşü k olduğ u İnancın a dayanarak, başkalar ı tarafında n kandıramayacağ ı varsayımıyl a hareke t eder; b u orta k inancı n bilincind e oia n saldırgan , isteğin i o kada r akıllıc a sunar k i hi ç kuşk u uyandırma z v e kurbanı n güvenin i sömürür .

Kurumsal Saflı k

Ulusal karakterimizi n bi r parças ı ola n b u saflık , bilgisayarla r il k olarak uzakta n birbirlerin e bağlandıklarınd a d a görülüyordu . Hatırlayın , İntemet'ın il k şekl i ola n ARPANe t {Savunm a Bakanlığ ı iler i Araştırm a Projeleri Birim i Ağı } devlet , araştırm a v e eğiti m kurumla n arasınd a bilg i paylaşmanın bi r yol u olara k tasarlanmıştı . Amaç , teknoloji k ilerlemeni n yanısıra bilg i özgürlüğüydü . Böylec e pe k ço k eğiti m kurumu , il k bilgisa - yar sistemlerin i y a hi ç y a d a ço k a z güvenli k sağlayara k kurdular . Tanınmış bi r yazılı m Özgürlükçüs ü ola n Richar d Stallman , kend i hesabını bi r şifreyl e korumay ı bil e reddetmişti .

Ancak internet'i n elektroni k ticare t içi n kullanılmay a başlanması , zayıf güvenli k Önlemlerinin , he r şeyi n biribirin e kablolarl a bağl ı olduğ u dünyamızda yaratacağ ı tehlikeler i cidd i şekild e açığ a çıkardı .

Güvenliğin E n Zayı f Halkas ı

Bugünün havaalanların a bi r bakın . Güvenli k e n üs t düzey e ulaşmı ş durumda anca k güvenliğ i

aşıp , kontro l noktalarında n tehlikel i olabilece k silahlar geçire n yolcularl a ilgil i basınd a duyduğumu z haberlerl e dehşet e düşüyoruz. Hav a alanlarımı z böyl e bi r alar m durumundayke n b u nası l mümkün olabiliyor ? Meta l dedektörler i m i doğr u çalışmıyor ? Hayır . Sorun makinelerd e değil . Soru n insa n unsurunda : Makineler i çalıştıra n insanlarda. Hav a alan ı yetkililer i Ulusa ! Muhafizlar 1! kapıy a koyup , meta l dedektörleri v e yü z tanım a sistemler i yerleştirebilirle r am a akti f güvenli k görevlilerini, yolcular ı nası l kontro l edecekler i konusund a eğitme k dah a yararlı olu r gib i görünüyor .

Aynı sorun , düny a çapında , tü m devle t kurumları , eğiti m kuruluşlar ı v e ticari işletmele r içi n d e geçerli . Güvenli k uzmanlarını n çabaların a karşı n bilgiler savunması z kalıyo r v e güvenli k zincirini n e n zayı f halkas ı ola n İnsan halkas ı güçlendirümediğ i sürece , toplu m mühendisliğ i beceriler i olan saldırganlarc a işta h açıc ı bi r hede f olara k görülmey e deva m ediyor .

Her zamankinde n ço k ş u anda , pemb e gözlüklerimiz i çıkarıp , bil - gisayar sistemlerimizi n v e ağlarımızı n gizliliğine , bütünlüğün e v e varliğı - na saldırmay a yeltenece k olanları n kullandığ ı yöntemler e karş ı dah a gözü açı k olmalıyız . Trafikt e diğe r arabaları n herşey i yapabileceğ i olasılığına karş ı geliştirile n korunmac ı sürücülüğü n gerekliliğin e zaman - la inandık ; artı k korunmac ı programcılı k uygulamaların ı d a öğreni p onlara d a inanm a zamanımı z geldi .

Özel yaşantınızı , aklınız ı y a d a şirketinizi n bilg i sistemlerin i ihia l eden bi r saldır ı tehlikesi , başınız a gelen e kada r gerçekleşecekmi ş gib i görünmeyebilir. Maliyetler i yükse k ola n böyles i bi r gerçekl e yüzleşmek - ten kaçınma k için , bilg i varlıklarımızı , kend i kişise l bilgilerimiz i v e ulusumuzun hassa s al t yapıların ı koruma k konusund a hepimizi n bilinçli , eğitimli v e uyanı k olmamı z gerekmektedir . V e b u önlemler i bugünde n almamız şarttır .

Teröristler v e Aldatmacala r

Aldatma sanatı , doğa l olarak , yalnızc a toplu m mühendisin e özg ü bi r araç değildir . FizikseMeröriz m büyü k yankıla r uyandırıyo r v e dünyanı n tehlikeli bi r ye r olduğunu n dah a önc e hi ç varmadığımı z kada r farkın a var - mamıza yo l açıyor . Sonuçta , medeniye t yalnızc a inc e bi r kaplam a gibi .

Eylül 2001'de , Ne w Yor k v e VVashington' a yapıla n saldırıla r he r bi - rimizin -yalnızc a Amerikalıları n değil , tü m ulusları n iy i niyetl i insanlarını n da- yüreğin e hüzü n v e kork u saldı . Dünyanı n he r tarafında , iy i eğitilmi ş ve yen i saldırıla r yapmanı n firsatın ı kollayan , takıntıl ı teröristleri n olduğ u gerçeğine karş ı uyarıldık .

Devletlerin so n zamanlard a arta n çabalan , güvenli k bilinc i düze - yimizi artırdı . He r tü r terörizm e karş ı uyanı k v e tetikt e olmalıyız .

Teröristlerin nası l büyü k bi r hainlikl e saht e kimlikle r yarattıklarını , öğren - ci v e komş u rollerin e büründüklerin i v e kalabalığ a karıştıkların ı iyic e anlamamız gerekir . Entrikala r çevirirlerken , b u sayfalard a okuyacak - larınıza benze r aldatm a numaralar ı çekere k ası l niyetlerin i gizliyorlar .

Bildiğim kadarıyla , teröristle r şirketlere , içm e suy u tesislerine , elekt - rik üretm e tesislerin e y a d a ulusa l altyapımızı n başk a yaşamsa l Önem i olan parçaların a sızma k içi n henü z toplu m mühendisliğ i teknikler i kul- lanmadılarsa da , ası l soru n orad a yatıyor . Bun u yapma k so n derec e kolay. B u kita p sayesinde , şirke t üs t yönetimlerini n güvenli k bilincin i yer - leştirip yen i güvenli k politikaların ı uygulamay a koyacağın ı umuyorum .

Bu Kita p Hakkınd a

Şirket güvenliğ i bi r deng e konusudur . Yetersi z güvenlik , şirketiniz i çok savunması z bırakırken , güvenliği n üzerind e fazl a durma k is e işl e ilgilenilmesini engelleyip , şirketi n büyümesin i v e kazancın ı kısıtlar . Ası l zor i ş güvenli k v e üretkenli k arasındak i dengey i kurmaktır .

Şirket güvenliğiyl e İlgil i başk a kitapla r yazılı m v e donanı m teknoloji - leri üzerin e odaklanırla r v e e n cidd i tehlikey e yeterinc e ye r vermezler : insanların aldatılması . B u kitabı n amacı , diğerlerinde n farkl ı olarak , sizin, berabe r çalıştığını z insanları n v e şirketinizi n diğe r çalışanlarını n nasıl yönlendirilebileceğin i anlamanız a yardımc ı olma k v e kandırıla n kişi konumunda n çıkma k içi n n e gib i önlemle r alabileceğiniz i göster - mektir. Elinizdek i kitap , çoğunlukla , saldırganları n bilg i çalmak , güvenili r olduğu düşünüle n am a aslınd a öyl e olmaya n bi r bilgiy i doğrulama k y a da bi r şirke t ürünün ü tahri p etme k içi n kullandıkları, tekni k olmaya n yön - temler üzerind e duruyor .

Benim görevim , va r ola n basi t bi r gerçe k nedeniyl e dah a d a zor - laşıyor: He r okuyucu , toplu m mühendisliğini n e n büyü k ustalar ı ola n anne-babalar tarafında n zate n yönlendirilmi ş durumda . Ann e v e babanız "sizi n iyiliğini z için, " diyere k e n doğr u olduğun u düşündükler i şeyleri siz e yaptırmanı n yoifann ı buldular . Toplu m mühendisleri , hedef - lerine ulaşma k içi n hikâyelerin , nedenleri n v e gerekçeleri n üzerind e nasıl özenl e v e maharetl e oynuyorîarsa , anne-babala r d a ayn ı yöntem - leri kullana n başarıl ı bire r hikây e anlatıcısıdırlar . Evet , hepimiz , iy i niyetl i (ve baze n o kada r d a iy i niyetl i olmayan) toplu m mühendisler i ola n anne-babalarımtz tarafında n yoğrulduk .

Bu eğitiml e şartlanmı ş olara k yönlendirilmey e açı k hal e geldik . Eğe r her zama n tetikt e olu p başkaların a güvenmeseydik , bizde n yararlan - mak isteye n birini n kuklas ı olacağımı z endişesiyl e dol u olsaydık , zo r bi r yaşam sürüyo r olurduk . Kusursu z bi r dünyad a kuşk u bil e duymadan başkalarına güvenir , karşılaştığımı z insanları n dürüs t v e güvenili r olduk - larından emi n olurduk . Am a kusursu z bi r dünyad a yaşamıyoru z v e b u

yüzden rakiplerimizi n yanıltıc ı çabaların ı engelleme k içi n bi r derecey e kadar ihtiyatl ı olmalıyız .

Kitabın an a parçaların ı oluştura n ikinc i v e üçünc ü an a başlıklar , toplum mühendislerin i i ş başınd a göstere n hayal î öykülerde n oluşuyor . Bu bölümlerd e şunlar ı göreceksiniz :

. Telefo n beleşçilerini n yılla r önc e buldukları , telefo n şirketinde n

rehberde geçmeye n bi r numaray ı almanı n sağla m bi r yolunu .

• Saldırganları n kullandıkları, uyanı k v e kuşkuc u çalışanlar ı bil e

bilgisayar kullanıc ı adlann ı v e şifrelerin i vermey e ikn a edece k

çeşitli yöntemleri ,

• Bi r İşle m Merkez i yöneticisini n şirketini n e n gizl i ürü n bilgisin i

çalabilmesi içi n bi r saldırgan a nası l yardı m ettiğini ,

• Bi r hanımı , he r tuş a basışı m kaydede n sonr a d a ayrıntılar ı

saldırgana e-postalaya n bi r yazılı m indirmes i içi n kandıra n bi r

toplum mühendisini n kullandığ ı yöntemleri ,

• Öze l dedektifleri n şirketinizl e v e sizinl e ilgil i nası l bilg i topladıkların ı

okuyacaksınız. B u sonuncunu n içiniz i ürperteceğinde n eminim .

İkinci v e üçünc ü an a başlıklard a geçe n baz ı hikâyeler i okurken , bun - ların mümkü n olmadığın ı b u sayfalard a yazıl ı yalanların , aşağılı k numaraların v e dalavereleri n hi ç kimseni n yanına kalmayacağın ı düşünebilirsiniz. Gerçe k ş u ki , he r olayd a anlatıla n hikâyele r olmu ş v e olabilecek olaylar ı yansıtmaktadırlar : Pe k çoğ u dünyanı n bi r köşesind e her gü n olmaktadır; hatt â si z b u kitab ı okurke n sizi n kurumunuzu n bil e başına geliyo r olabilir .

Kitabın içeriği , işiniz i koruma k sö z konus u olduğund a gerçekte n ibret veric i olacaktır ; kişise l yönde n bakıldığınd a is e öze l yaşamınızd a bilginizin bütünlüğün ü koruma k içi n toplu m mühendislerini n hamlelerin i bertaraf etmeniz e d e fayd a sağlayacaktır .

Kitabın dördünc ü an a başlığınd a konuy u farkl ı bi r açıda n el e alı - yoruz. Buradak i amacım , çalışanlarınızı n toplu m mühendisler i tarafın - dan kandırılmalar ı ^olasılığın ı e n az a indirgeme k içi n gerekl i işletm e kurallarını v e bilinçlendirm e eğitimlerin i oluşturmanız a yardı m etmek . Toplum mühendislerini n stratejilerini , yöntemlerin i v e taktiklerin i anla - mak, şirketinizi n üretkenliğin i düşürmede n B T varlıklarınız ı koruma k içi n uygun kontrolle r yerleştirmeniz e yardımc ı olacaktır .

Kısacası, b u kitabı , toplu m mühendisliğini n oluşturduğ u ağı r tehlike - ye karş ı sizler i bilinçlendirme k v e şirketinizi n v e çalışanlarınızı n b u yoll a sömürülmesi olasılığın ı e n az a indirgemeniz e yardı m etme k içi n yazdım .

Ya d a belk i şöyl e söylemeliyim , b u olasılı k bi r dah a hi ç sömürüle - meyecekleh kada r azalacaktır .

2

Sanatı

ZARARSIZ GİB İ GÖRÜNE N BİLGİLER

Çoğu insan a gör e toplu m mühendislerinde n kaynaklanaca k e n büyük tehdi t nedir ? Kendiniz i koruma k içi n n e yapabilirsiniz ?

Eğer ama ç ço k değerl i bi r ödü l el e geçirmeks e -diyeli m ki , bi r şirketi n fikrî sermayesini n öneml i bi r parçasıysa - o zama n belk i d e gerekl i ola n şoy, mecaz î olarak , yalnızc a dah a güçl ü bi r kas a v e dah a iy i silahlanmı ş bekçilerdir. Öyl e deği l mi ?

Ama aslınd a bi r şirketi n güvenliğini n aşılması , genellikl e köt ü adamın şirkettek i pe k ço k insanı n korunmas ı v e sınırlandırılmas ı içi n bi r neden görmediği , so n derec e masum , günlü k v e önemsi z görünen bi r bilgiyi y a d a bi r belgey i eld e etmesiyl e başlar .

Bilginin Gizl i Değer i

Çoğu toplu m mühendisleri , bi r şirketi n elind e ola n v e zararsı z gib i görünen bilgiler i e l üstünd e tutarla r çünk ü b u bilgiler , kendilerin i dah a inandırıcı kNabilmelerind e ca n alıc ı bi r ro l oynayabilir .

Bu sayfalarda , toplu m mühendislerini n saldırıların a sizi n d e "tanık " olmanızı sağlayara k işlerin i nası l yaptıkların ı göstereceğim ; baze n olay ı kurban rolündek i kişileri n bakı ş açısında n sunacağım , böylec e kendiniz i onların yerin e koyabilece k v e si z (belk i d e çalışanlarınızda n y a d a i ş arkadaşlarınızdan biri) olsaydını z nası l bi r yanı t verebileceğiniz i tarta - bileceksiniz. Çoğ u durumd a ayn ı olaylar ı toplu m mühendisini n bakı ş açısından d a göreceksiniz .

İlk öyk ü finan s endüstrisindek i bi r açı k noktay a değinmektedir .

Creditchex

İngilizler, tutuc u bi r bankacılı k sistemin e uzu n bi r sür e katlanma k zorunda kaldılar . Sırada n v e dürüs t bi r vatanda ş olara k bi r bankada n içeri giri p bi r hesa p açtıramazdınız . Hatırl ı müşterilerde n bir i sizi n içi n bi r tavsiye mektub u yazmadığ ı sürec e bank a siz i müşter i olara k kabu l etmeyi düşünmezd i biie .

ingilizlerin b u sistem i günümüzü n görünüşt e eşitlikç i bankacılığın - dan doğa l olara k oldukç a farklı . İ ş yapmaktak i çağda ş rahatlığımız , neredeyse herkesi n bi r bankay a giri p kolaylıkl a vadesi z çe k hesab ı

açtırabildiği, arkada ş canlıs ı v e demokrati k Amerika'da n başk a hiçbi r yerde b u kada r göz e çarpmıyor , öyl e mi ? Ta m olara k değil . Gerçe k ş u ki, bankaların anlaşılabili r nedenlerde n ötürü , geçmişt e karşılıksı z çe k yazmış olabilece k bir i adın a -k i bu , kişini n adl i sicilind e bank a soygun u ya d a zimmet e geçirm e suçlarını n olmas ı kada r köt ü bi r durumdur - hesap açma k konusund a doğa l bi r çekingenlikler i vardır . B u yüzden , müstakbel bi r müşteriyl e ilgil i hızl ı bilgile r edinme k pe k ço k bank a içi n olağan bi r uygulamadır .

Bu tar z bilgiler i edinme k içi n bankaları n i ş yaptıklar ı başlıc a şirketler - den bir i d e bizi m CreditChe x adın ı vereceğimi z bi r kuruluş . Müşterilerin e çok öneml i bi r hizme t sunmakl a birlikte , birço k şirkett e olduğ u gibi , İşin i bilen toplu m mühendislerin e d e farkınd a olmada n kullanışl ı bilgile r sağlayabiliyorlar.

İlk Görüşme : Ki m Andrevv s

- Ulusal Banka, ben Kim. Size nasıl yardımcı olabilirim?

- Merhaba Kim. Sana bir sorum olacaktı. Sizler CreditChex kullanı- yor musunuz?

- Evet.

- CreditChex'i aradığınız zaman, onlara verdiğiniz numaraya ne ad veriyorsunuz? Üye İşyeri Numarası mı?

Kız bi r a n duraksadı ; soruy u tartıp , bunu n neyl e ilgil i olduğun u v e yanıt veri p vermemes i gerektiğin i düşündü .

Bu arada, telefondaki ara vermeden konuşmayı sürdürdü:

• Sormamın nedeni şu: özel dedektiflik konusunda bir kitap yazıyorum.

- Evet, ded i kız , soruy u gönü l rahatlığıyl a yanıtlayarak . Bi r yazar a yardımcı olabildiğ i İçi n memnun'olmuştu .

- Üye İşyeri Numarası deniyor, öyle mi?

- Ht ki.

- Tamam, harika. Terimleri doğru kullanabilmek için sormuştum. Yani kitap için. Yardımların için teşekkürler. Hoşçakal, Kim.

İkinci Görüşme : Chrİ s T a I ber t

- Ulusal Banka, Yeni Hesaplar, ben Chris.

- Merhaba, Chris. Ben Alex, ded i arayan . CreditChex'in müşteri tem-

silcisiyim. Hizmetlerimizi geliştirebilmek için bir araştırma yapıyoruz. 1 •••••• • Bana birkaç dakikanı ayırabilir misin?

Chris memnuniyetl e ayırabileceğin i söyled i v e araya n konuşmay a devam etti :

Zararsız Gib i Görüne n Bilgile r 1 7

- Pekâlâ. Şubenizin çalışma saatleri nedir? Kadı n yanıtlad ı v e ardar - da gele n somlar ı yanıtlamay a deva m etti .

- Şubenizin kaç çalışanı bizim hizmetlerimizden yara} lanı\ or 9

- Bilgi talebi için bizi ne sıklıkta arıyorsunuz?

- Sizin İçin ayırdığımız 800'lü numaralardan hangisini kullanıyorsunuz?

- Müşteri temsilcilerimiz her zaman size karşı nazikle/ mı *

- Talebinize yanıt verme süremiz ne kadar?

- Ne kadar süredir bankada çalışıyorsunuz?

- Şu anda kullandığınız Üye İşyeri Numarası nedir?

- Size sağladığımız bilgilerde hiç tutarsızlığa rastladınız mı"

- Hizmetlerimizi geliştirmemiz doğrultusunda önsrileı iniz olsavdı bunlar neler olurdu?

Ve:

- Şubenize düzenli olarak göndereceğimiz anketleri doldurmak ister

misiniz?

Kadın yapabileceğin i söyledi , bira z konuştular , araya n telefon u kapatt ı

ve Chri s işini n basm a döndü .

Üçüncü Görüşme : Henr y McKinse y

- CreditChex, ben Henry McKinsey, size nasıl yardımcı olabilirim? Arayan, Ulusa l Banka'da n aradığın ı söyledi . Doğr u Üy e İşyer i Numarasını, sonr a d a bilg i istediğ i kişini n adın ı v e sosya l güvenli k numarasını verdi . Henr y kişini n doğu m günün ü sord u v e araya n on u d a verdi.

Biraz sonr a Henr y bilgisaya r ekranında n kayıtlar ı okudu .

- Wells Fargo 1998'de, bir kerelik, 2.066 dolar tutarında YB rapor etmiş.

YB (Yetersi z Bakiye) , yazıla n çek e karşılı k hesapt a yeterinc e par a olmadığı durumla r içi n kullanıla n bankacılı k terimidir .

- O zamandan beri başka hareket olmuş mu?

- Hayır, olmamış.

- Başka sorgulama olmuş mu?

- Bir bakalım. Evet, iki tane olmuş, ikisi de geçen ay. Chicago, Üçüncü Birleşik Kredi Birliği.

Bir sonrak i adı , Schenectad y Yatırı m Ortaklığı'nı , okurke n bocalad ı v e harf har f kodlama k zorund a kaldı .

- New York Eyaleti'nde, diy e d e ekledi .

Özel Dedekti f İ ş Başınd a

Bu görüşmeleri n üç ü d e ayn ı kiş i tarafından , adın a Osca r Grac e diyeceğimiz bi r öze l dedekti f tarafında n yapılmıştı . Grace'i n yen i bi r müşterisi vard ı v e b u onu n il k müşterilerinde n biriydi . Birka ç a y öncesin e kadar poli s ola n Grace , yen i işleri n bazıların ı rahatlıkl a çözebildiğin) far k etmişti, anca k diğerler i kaynakların ı v e yaratıcılığın ı sonun a kada r kul- lanmasını gerektirece k kada r zorluydu . B u seferk i i ş kesinlikl e zorlula r sınıfına giriyordu .

Polisiye romanları n tanıdı k öze l dedektifler i -Sa m Spade s v e Phili p Marlovves- eşin i aldata n birin i yakalayabilme k içi n saatlerc e arabaların - da oturu p gec e yarıların a kada r beklerlerdi . Gerçe k hayattak i öze l dedektifler d e aynısın ı yapıyorlar . Öze l dedektifle r polisiy e romanlar a daha a z kon u olmu ş am a didişe n eşleri n işlerin e buru n sokmanı n bi r o kadar öneml i başk a bi r çeşidini , yan i gec e nöbetleriyl e cebelleşmekte n çok, büyü k ölçüd e toplu m mühendisliğ i becerilerin e dayana n bi r yönte m de kullanıyorlar .

Grace'in yen i müşterisi , giysile r v e mücevherle r içi n oldukç a geni ş bir bütç e ayırabiliyo r gib i görünen bi r hanımdı . Bi r gü n ofisin e gelmi ş v e üstünde kağı t yığıl ı olmaya n te k der i koltuğ a oturmuştu . Gucc i mark a büyük e l çantasını , markas ı on a dönü k kalaca k şekild e masay a koymu ş ve boşanma k istediğin i kocasın a söylemey i tasarladığın ı açıklamıştı , ancak "küçü k bi r sorun " olduğun u d a itira f etmişti .

Görünüşe gör e kocas ı bi r adı m öndeydi . Tasarru f hesaplarındak i parayı v e yatırı m hesaplarınd a dura n dah a d a büyü k bi r tutar ı çokta n çekmişti. Kadı n paraları n nerey e kaçırıldığın ı bilme k istiyord u v e boşan - ma avukat ı hi ç yardımc ı olmuyordu . Grace , avukatın , paranı n nerey e gittiği gib i pi s işler e elin i bulaştırmayacak , hızl ı yükselen , yükse k gelirl i danışmanlardan bir i olduğun u tahmi n etti .

Acaba Grac e on a yardımc ı olabili r miydi ?

Bu işi n çocu k oyuncağ ı olduğun a kadın ı ikn a etti , bi r fiya t verdi , mas - rafların, gerçekleştikç e faturalandırılacağın ı söyled i v e il k ödem e içi n bi r çek aldı .

Sonra d a çözmes i gereke n sorunl a yüzleşji . Dah a Önc e hi ç böyl e bi r iş yapmadıysanı z v e par a İz i sürme k konusund a pe k bi r şe y bilmiyor - sanız n e yaparsınız ? Ufa k adımla r atara k iş e başlarsınız . İşte , biz e aktarıldığı kadarıyl a Grace'i n öyküsü :

CreditChex'in n e olduğun u v e b u şirketi n bankaları n hang i konud a işine yaradığın ı -esk i karı m bi r bankad a çalışırdı - biliyordum . Am a kul - lanılan terimler i v e süreçler i bilmiyordu m v e esk i karım a sorma k zama n kaybı olacaktı .

Birinci adım : Bankacılı k terimlerin i öğre n v e İstene n şeyi n konuy a

hakim bir i tarafında n istendiğ i izlenimin i

yaratmanın bi r yolun u bul . Aradığı m Terimler bankada, ad ı Ki m ola n gen ç hanı m

CreditChex'İ aradıklar ı zama n kendileri -

HEDEF: Bir dalaverenin ni nası l tanıttıkların ı sorduğumd a kuşku -

kurbanı. landı. Duraksad ı v e ban a söyleyi p söyle - KA YNA ĞI KUR UTMA K: memekten emi n olamadı . B u ben i cay - Bir saldırgan, gerçek- dırdı mı ? Elbett e hayır . Üsteli k b u durak - leştirdiği saldırıyı kur- sama ban a öneml i bi r ipucu , onu n içi n banının anlamasına izin inandırıcı olaca k bi r nede n bulma m verirse, o zaman buna kay- gerektiğine dai r bi r işare t verdi . On a bi r nağı kurulmak denir. kitap içi n araştırm a yaptığı m oyunun u Kurban bir kez durumu oynadığımda, bu , kuşkuların ı giderdi . Bi r anlar ve diğer çalışanlara kitap y a d a senary o yazar ı olduğunuz u ve yönetime bu girişimden söyleyin, herkesi n dil i çözülüverır .

söz ederse, gelecek

Elimde Kim'i n üzerind e iş e yaraya -

saldırılarda aynı kaynağı bilecek başk a bilgile r d e vardı ; hakkınd a

sömürmek çok güçleşecektir. bilgi istediğini z kişiyl e ilgil i CreditChex'İ n

ne tü r bilgile r istediğini , sizi n o kişiyl e

ilgili nele r isteyebileceğiniz i v e e n önemlis i Kim'i n çalıştığ ı bankanı n Üy e İşyeri Numarası'n ı biliyordum . B u sorular ı sormay a hazırdı m am a duraksaması bi r tehlik e işaretiydi . Kita p araştırmas ı hikâyesin i yutmuş - tu, anca k işi n başınd a bira z kuşkuianmıştı . Eğe r başında n yardımc ı olmaya hevesl i olsaydı , süreçlerl e ilgil i dah a fazl a şe y anlatmasın ı ondan isteyebilirdim .

İçinizden gele n ses e kula k vermeli , hedefi n söylediklerin i v e nası l söylediğini dikkatl e dinlemelisiniz . B u hanım , ço k fazl a olağandış ı sor u soracak olsaydım , kafasınd a alar m ziller i çalaca k kada r zek i görünüyor - du. He r n e kada r ki m olduğum u v e hang i numarada n aradığım ı bilmes e de, eğe r b u işi n içindeyseniz , telefo n edere k şirketl e ilgil i bilg i almay a çalışan birin e karşı , birilerini n ortalığ ı ayağ a kaldırmasın ı istemezsiniz . Bunun neden i kaynağ ı kurutma k istememenizdir ; ayn ı işyerin i başk a bi r zaman bi r ke z dah a arama k isteyebilirsiniz .

Bir insanı n ban a "Buyru n emriniz e amadeyim, " diyere k yardımc ı m ı olacağını yoks a "B u adamı n niyet i bozuk , polis i arayayım, " diy e ortalığ ı uyağa m ı kaldıracağın ı anlama k amacıyl a ban a ipuc u verece k küçü k işaretleri yakalayabilme k içi n gözümü-kulağım ı he p açı k tutarım .

Kim'i bira z dike n üstünd e bir i olara k derecelendirdim , b u yüzde n l;ırklı bi r şubedek i başk a birin i aradım . Chris'l e yaptığı m ikinc i ıjürüşmede, araştırm a numaras ı ço k iy i i ş gördü . Buradak i yöntem , inandırıcılığı artıraca k ilgisi z soruları n arasın a öneml i sorula n sıkıştır - mnkta yatıyor . CredİtChex'dek i Üy e İşyer i Numarası'n ı sormada n önce , İKinkada n e kada r süredi r çalıştığıyl a ilgil i on a kişise l bi r sor u yöneltere k hır so n dakik a kontrol ü yaptım .

Kişisel bi r sor u mayı n gibidir ; bazılar ı üzerinde n geçe r v e hiçbi r zaman farketmezler ; bazılarınd a is e patla r v e güvenl i bi r ye r bulma k içi n telaş içind e kaçmaların a nede n olur . B u yüzden , eğe r kişise l bi r sor u sorarsam, karş ı tara f soruy u yanıtlars a v e se s tonund a bi r değişikli k olmazsa, büyü k olasılıkl a talebi n içeriğinde n şüphelenmemi ş demektir . Yanıtlanmasını istediği m soruy u ona , kuşk u uyandırmada n rahatlıkl a sorabilirim v e büyü k olasılıkl a ban a istediği m cevab ı verir .

İyi bi r öze l dedektifi n bildiğ i bi r şe y dah a vardır : Hiçbi r zaman , kili t bilgiyi eld e ettikte n sonr a görüşmey i heme n bitirme . Bir-ik i soru , bira z sohbetten sonr a ved a etme k yerind e olabilir . Eğe r kurba n sorduklarınız - la ilgil i bi r şeyler i dah a sonr a hatırlarsa , bunla r büyü k olasılıkl a so n birkaç sor u olacaktır . Kalan ı genellikl e unutulur .

Böylece Chri s ban a Üy e İşyer i Numarası'n ı v e taleplerin i bildirme k için kullandıklar ı telefo n numarasın ı verdi . CreditChex'te n n e kada r bilg i edinilebildiğini öğrenebileceği m sorula r d a sorabilseydi m dah a mutl u olurdum. Anca k şansım ı zorlama k istemedim .

Bu, CreditChex !ten tuta r hanes i bo ş bi r çe k alma k gib i bi r şeydi . Artı k istediğim zama n arayı p bilg i eld e edebilirdim . Aldığı m hizme t içi n par a ödememe bil e gere k yoktu . Görünüş e gör e CreditChe x temsilcis i İste - diğim bilgiler i beniml e paylaşmay a hazırdı . Müşterimi n kocasını n hesa p açtırmak içi n so n zamanlard a başvurduğ u ik i ye r vardı . O zaman , yakın - da esk i eş i konumun a gelece k ola n kadını n aradığ ı parala r neredeydi ? CreditChex'teki adamı n saydığ ı bankalarda n başk a nered e olabilird i ki ?

Aldatmacanın İncelenmes i

Tüm b u düze n toplu m mühendisliğini n teme l taktiklerinde n birini n üzerine kurulmuştur : Öyl e olmadığ ı halde , bi r şirke t çalışanının , zararsı z olduğunu düşündüğ ü bi r bilgiy e ulaşmak .

ilk bank a memur u CreditChex' İ ararke n kullanıla n tanımlayıc ı sayıy ı anlatan Üy e İşyer i Numaras ı terimin i doğruladı . İkincisi , CreditChex'i n telefon numarasın ı v e e n ca n alıc ı bilg i ola n bankanı n Üy e İşyer i Numarası'nı sağladı . Tü m b u bilgile r memur a zararsı z görünüyordu . B u sayıyı başkasın a söylemeni n n e zarar ı olabilird i ki ?

Tüm bunla r üçünc ü görüşm e içi n gereke n zemin i hazırladı . Grace'i n

Mitnick Mesajı : x

Üye İşyeri Numarası, bu durumda, bir şifre kadar önem. taşır. Eğer banka çalışanları onu bir ATM şifresi olarak görürlerse, bilginin hassaslığını kavrayabilirler. Şirketinizde insanların yeterli özeni göstermedikleri kurum içi bir şifre ya da numara var mı?

Zararsız Gib i Görüne n Bilgile r

i'lındı; CreditChex' i arayıp , kendin i müşter i bankalarda n bir i ola n Ulusa l HiinkH'nın bi r çalışan ı gib i tanıttıkta n sonr a istediğ i bilgiy i alabilmes i içi n ılıliyncı ola n he r şe y vardı .

Bilgi çalarken , iy i bi r dolandırıcını n paranız ı çalmad a gösterdiğ i htıcorikliliğe benze r bi r beceriklili k göstere n Grace'in , insanlar ı okuma k d,:in geliştirilmi ş yetenekler i vardı . Sıkç a uygulanan , masu m soruları n at.ısına anahta r sorular ı katm a yöntemin i o d a biliyordu . Üy e İşyer i Numarası'nı he r şe y yolundaymı ş gib i sormada n önc e kişise l bi r soru - nun ikinc i memuru n işbirliğ i yapm a eğilimin i ölçeceğin i d e biliyordu .

İlk memurun , CredİtChe x üy e numaras ı içi n kullanıla n terim i onayla - y.ırak yaptığ ı hatay a karş ı korunmay a neredeys e olana k yoktu . B u bil - ginin bankacılı k sektöründ e o kada r geni ş bi r kullanım ı va r k i önemsi z (jthi görünüyor ; zararsı z görünüml ü bilgiler e e n iy i örnek . Anca k ikinc i memur Chris , arayanı n gerçekt e söylediğ i kiş i olu p olmadığın ı doğrula - madan sorular ı yanıtlamay a b u kada r hevesl i olmamalıydı . E n azında n ,itlini v e telefo n numarasın ı alı p on u ger i aramalıydı ; böylec e dah a sonr a Viıphe uyanırsa , karş ı tarafı n hang i telefo n numarasın ı kullandığını n bi r knydını tutmu ş olabilirdi . B u durumda , böyl e bi r aram a yapmak , saldır - ganın CreditChe x görevlis i gib i davranmasın ı dah a d a güçleştirirdi .

Daha d a iyisi , CreditChex'i , arayanı n verdiğ i numarada n değil , hnnkanın kayıtlarınd a buluna n bi r numarada n arayıp , kişini n gerçekte n Df;ıda çalışı p çalışmadığın ı v e şirketi n gerçekte n müşter i araştırmas ı yapı p yapmadığını doğrulama k olurdu . Gerçe k düny a uygulamaların ı v e bugü n çoğu insanı n içind e bulunduğ u zama n baskısın ı gö z önün e aldığınızda , çalışanın bi r çeşi t saldır ı gerçekleştirildiğinde n kuşkulandığ ı durumla r dışında, b u tar z bi r kontro l aramas ı yapmas ı beklentileri n ço k ötesindedir .

Mühendislik Tuzağ ı

İnsan avcıs ı firmaları n şirke t iç i yetenekler i bulma k içi n toplu m mühendisliği taktiklerin i kullandıklar ı yaygı n olara k bilinir , İşt e bunu n nasıl olabileceğin e dai r bi r Örnek .

1990'ların sonlarında , pe k d e ahlağ a uygu n çalışmaya n bi r i ş bulm a ^contası, telefo n endüstrisind e deneyiml i elektri k mühendisler i araya n bir şirket i yen i müşteris i olara k aldı . B u görevi n sorumlusu , buğul u bi r ses tonun a v e çekic i tavırlar a sahi p bi r hanımdı . B u yeteneklerin i tele - fon üzerinden , güve n vere n v e dostç a bi r izleni m uyandırma k amacıyl a kullanmayı d a öğrenmişti .

Kadın, raki p bi r şirkett e çalışma k içi n ayartılabilece k mühendisle r bulup bulamayacağın a bakma k amacıyl a bi r ce p telefon u hizme t îüiglayıcısını yoklamay a kara r verdi . Santral ı arayıp , "Be ş yıllı k mühendislik deneyim i ola n herhang i biriyl e görüşme k istiyorum " diye - mezdi. Bunu n yerine , bira z sonr a göreceğini z nedenlerle , yetene k avın a

hiçbir hassasiyet i yokmu ş gib i görüne n v e şirke t çalışanlarını n neredeyse isteye n herkes e verdiğ i bi r bilgiy i arayara k başladı .

İlk Görüşme : Danışm a Görevlis i

Saldırgan, Did i Sand s adın ı kullanarak , ce p telefon u hizme t sağlayıcısının şirke t binasın a telefo n etti . Konuşma , kısme n şöyl e geçti:

Danışma Görevlisi: İyi günler. Ben Marie, size nasıl yardıma olabilirim?

Didi: Beni Nakliyat Bölümü'ne bağlar mısınız?

.< DG: Öyle bir bölümümüz olduğundan emin değilim, rehberime

bakayım. Kim arıyordu?

D: Didi

DG: Binada mısınız, yolma ...?

D: Hayır, dısardayım.

DG: Dİdi, soyadınız?

D: Didi Sands. Nakliye'nin dahilisini biliyordum ama unutmuşum. DG: Bir .saniye.

Kuşku uyandırmama k için , b u noktad a Didi , sohbet i sürdürme k amacıyla, "içerden " olduğun u v e şirke t binalarını n yerlerin i bildiğin i göstermek üzer e tasarlanmı ş sırada n gib i görüne n bi r sor u sordu . D: Hangi binadasınız? Lakeview'da mı yoksa ana binada mı?

DG: Ana binada (duraksama) . Numara 805 555 6469,

Nakliye Bölümü'n ü aramanı n iş e yaramayabileceği m de dikkat e alara k kendini sağlam a alma k amacıyl a Didi , Gayrimenku l Bölümü'yl e d e görüşmek istediğin i söyledi . Danışm a görevlis i o numaray ı d a verd i v e onu Nakliy e Bölümü'n e bağlamay ı dened i am a hatla r meşguldü . Bu aşamad a Did İ üçünc ü bi r telefo n numarasını , Austin-Texas'tak i şir - ket binasınd a buluna n Tahsila t Ofisi'ni n numarasın ı d a istedi . Danışm a görevlisi onda n bira z beklemesin i ric a ett i v e hatta n çıktı . Şüphel i bi r telefon geldiğin i v e bi r şeyleri n ter s gittiğin i düşündüğün ü güvenliğ e anlatıyor olabili r miydi ? Kesinlikl e olamaz , Didi'ni n içind e e n küçü k bir endiş e bil e yoktu . Yalnızc a bira z kızı n başın a bel a olmuşt u am a danışma görevlis i içi n b u sırada n bi r i ş gününü n bi r parçasıydı . Bi r dakika sonra , danışm a görevlis i yenide n hatt ı aldı , Tahsila t Ofisi'ni n numarasına bakı p oray ı arad ı v e Didi'y i bağladı .

İkinci Görüşme : Pegg y

Sonraki konuşm a şöyl e geçti ;

Peggy: Tahsilat Ofisi, Pegg)>.

Didi: Merhaba Peggy. Ben Didi, Thousand Oaks'dan.

Zararsız Gib i Görüne n Bilgile r 2 3

/-'. Merhaba Didi.

D: Nasıl gidiyor 7 ' . " . • " " • " .

P: İyi.

Sonra Didi , i ş dünyasınd a iy i bilme n v e belirl i bi r kuruluşu n y a d a

çalışma grubunu n bütçesin e harcamalar ı ma l etme k içi n kullanıla n

işlem kodun u ifad e ede n terim i kullandı .

D: Mükemmel. Sana bir sorum olacak. Belli bir bölümün maliyet 1 merkezi kodunu nasıl öğrenebilirim?

P: O bölümün bütçe sorumlusuna ulaşman gerek.

D: Thousand Oaks'un bütçe sorumlusunun kim olduğunu biliyor

musun? Bir form doldurmaya çalışıyorum ve doğru maliyet merkezi

kodunu bilmiyorum.

P: Tek bildiğim, maliyet merkezi kodunu öğrenmen gerektiği zaman,

bütçe sorumlusunu araman gerektiği.

D: Texas'daki bölümünüz için bir maliyet merkezi kodu var mı?

P: Burada bir maliyet merkezi var ama bize hepsinin listesini vermiyorlar.

D: Maliyet merkezi kodu kaç basamaklı? Örneğin, sizin maliyet

merkezi kodunuz ne?

P: Şey, şöyle, sen 9WC'yle misin yo/csa SAT'la mısın?

Bunlann hang i bölümler e y a d a gruplar a karşılı k geldiğ i konusund a Didi'nin e n küçü k bi r fikr i yokt u am a b u öneml i değildi . Soruy u yanıtladı : D: 9WC

P: O zaman genellikle dört basamaklıdırlar. Nereden olduğunu söylemiştin?

D: Thousand Oaks, Genel Müdürlük.

P: Evet, Thousand Oaks için bir tane söyleyebilirim. ÎA5N, Nancy'nin N'si. Yardım etmey e istekl i biriyî e yeterinc e uzu n sür e sohbe t ederek , Did i ihtiyacı ola n maliye t merkez i kodun u aldı ; dışarda n birini n işin e yara - yacakmış gib i görünmediğ i içi n kimseni n korumay ı düşünmediğ i bilg i parçacıklarından bir i daha .

Üçüncü Görüşme : İs e Yaraya n Yanlı ş Numar a

Didi'nin bi r sonrak i adımı , elindek i maliye t merkez i kodun u bi r poke r markası gib i kullanara k dah a değerl i bi r şey e dönüştürme k olacaktı . Gayrimenkul bölümün ü arayıp , yanlı ş numar a çevirmi ş gib i yaptı . "Sizi rahatsız ettiğim için özür dilerim, ama ..." il e söz e başlayara k şirke t rehberini kaybetmi ş bi r çalışa n olduğun u söyled i v e yen i bi r rehbe r ala - bilmek İçi n kiminl e konuşmas ı gerektiğin i sordu . Ada m rehbe r kitapçığının esk i tarihl i olduğun u am a şirketi n intrane t sitesind e telefo n numaralanmn bulunduğun u söyledi .

Didi basılmı ş bi r rehbe r kullanmay ı terci h ettiğin i anlatınca , ada m on a matbaayı aramasın ı söyled i v e sonra , hiçbi r tale p olmada n -belk i d e yalnızca çekic i sesl i kadın ı telefond a bira z dah a uzu n sür e tutabilme k için- numaray ı buld u v e kadın a verdi .

Dördüncü Görüşme : Mcttbaa'da n Bar t

Matbaa bölümünd e Bar t adınd a biriyl e konuştu . Didi , Thousan d Oaks'dan aradığın ı v e çalıştıklar ı yen i danışmanı n şirke t rehberin e ihtiyacı olduğun u söyledi . Esk i tarihl i ols a d a basıl ı bi r rehberi n danış - manın dah a ço k işin e yarayacağın ı d a vurguladı . Bart , bi r tale p form u doldurması v e kendisin e göndermes i gerektiğin i söyledi .

Didi elind e for m kalmadığını , bira z aceles i olduğun u söyled i v e acab a Bart bi r inceli k yapı p form u onu n yerin e doldurabili r miydi ? Ada m biraz fazlay a kaça n bi r hevesl e kabu l ett i v e Did i on a ayrıntılar ı anlat - tı. Hayal i danışmanı n adres i olara k da , toplu m mühendislerini n post a deliği dedikleri , Didi'nı n şirketini n b u tar z durumla r için , Mai l Boxe s Ete. tülünde n ticar i şirketlerde n kiraladığ ı post a kutusun u verdi . Edindiği il k bilg i şimd i işin e yarayacaktı : Rehberi n maliyet i v e karg o için bi r ücre t alınacaktı . Didi , Thousan d Oak s içi n maliye t merkez i kodunu verdi .

- 1A5N, Nancy'nin N'si. :

Şirket rehber i birka ç gü n sonr a geldiğinde , Did i beklediğinde n dah a d a başarılı olduğun u gördü : Rehberd e yalnızc a adla r v e telefo n numaralar ı listelenmekle kalmamış , kimi n kimi n içi n çalıştığ ı d a gösterilmişti . Tüm şirketi n kurulu ş şemas ı elindeydi .

Boğuk sesl i kadı n insa n avlaya n telefo n görüşmelerin i yapmay a hazırdı. He r yetenekl i toplu m mühendisini n sonun a kada r geliştirdiğ i laf yapm a becerisin i kullanarak , akınların ı başlatma k içi n gerekl i ola n bilgileri dalaver e yoluyl a eld e etmişti . Şimd i d e semeresin i toplamay a

• • hazırdı . .•••.•• . • .••••••.•••• . '•: : . . • : : : • • ; • •

ASdatmaeansn İncelenmes i ' . ' •".•• •

Bu toplu m mühendisliğ i saldırısınd a Didi , hede f şirketi n ü ç ayr ı Dölümünün telefo n numaraların ı eld e edere k iş e koyuldu , istediğ i numaralar sı r olmadığ ı içi n b u kolaydı , özellikl e d e çalışanla r için . Bi r toplum mühendis i içerde n biriymi ş gib i konuşmay ı öğreni r v e Did i b u oyunda becerikliydi . Telefo n numaralarında n bir i on u bi r maliye t merkez i koduna yönlendirmiş , o kod u d a şirketi n telefon rehberinde n bi r kopy a almak içi n kullanmıştı .

ihtiyacı ola n teme l araçlar ; arkadaşç a davranmak , bira z şirke t iç i te - rimleri kullanma k v e so n kurband a uyguladığı , işi n için e küçük , söze l göz kırpmala r karıştırmaktı . ••-. • '•• •

Zararsız Gib i Görüne n Bilgile r 2 5

Ve kola y eld e edilemeye n öneml i bi r

dlflor ara ç da , toplu m mühendisini n Terimler yofluı çalışmalarl a v e geçmi ş nesilleri n

İyi dolandırıcılarını n kâğıd a dökülmemi ş

POSTA DELİĞİ: Toplum ılnriüyimlerinden der s alara k geliştirdiğ i

mühendislerinin kiralık Inlfuanlık becerileridir .

posta kutusu için kullandık-

ları terim. Yaygın olarak

Başka Değersi z

sahte isimle kiralanır ve

kurbanın göndermeye ikna

Bilgiler

edildiği evrakları ya da

paketleri almak için

kullanılır.

Maliyet merkez i kod u v e dahil i telefon

numaralarının dışında , iş e yarama z gib i

i|orünen başk a hang i bilgile r rakibini z içi n so n derec e değerl i olabilir ?

Peter Abel'i n Telefo n Görüşmes i

- Merhaba, de r hattı n öbü r ucundak i ses .

- Ben Parkhurst Seyahat Acentası'ndan Tom. San Francisco bilet- leriniz hazır. Onları size gönderelim mi yoksa kendiniz mi gelip almak istersiniz?

- San Francisco mu? de r Peter .

- Ben San Francisco'ya gitmiyorum ki.

- Siz Peter Abel mısınız?

- Evet, ama yapmayı düşündüğüm bir yolculuk yok. - Hım, de r arayan , dostç a gülerek .

- Yani San Francisco'ya gitmek istememekte kararlısınız, öyle mi 7

- Eğer patronumu kandırabilirseniz ... de r Peter , oluşa n tatl ı sohbet e uyum sağlayarak . .

- Bir karışıklık var gibi görünüyor, de r arayan .

- Sistemlerimizde yolculuk ayrıntılarını özlük numarasına göre

sıralıyoruz. Belki birileri yanlış numarayı kullanmıştır. Sizin Sosyal Güvenlik Numaranız nedir?

Peter nazi k bi r şekild e numaray ı verir . Nede n olmasın ? Doldurduğu , neredeyse he r çalışa n fc-munu n üzerin e b u numaray ı yaza r v e şirkette -

Mitnick Mesajı : —

'Tıpkı bir bulmacanın parçaları gibi her bilgi kendi başına ilgisiz durabilir. Ancak parçalar bir araya getirildiğinde, açık bir resim oluşur. Bu olayda toplum mühendisinin gördüğü resim şirketin iç yapısının tamamı olmuştur.

Mitnick Mesajı :

Öykünü ana fikri: İstekte bulunan kişinin sesini tanımıyorsanız ve istemek için bir nedeni yoksa, hiç kimseye kişisel ya da şirket içi bilgileri ve tanım- layıcıları vermeyin.

ki pe k ço k insanı n bun u öğrenm e şans ı vardır ; insa n kaynaklarının , maaş servisini n v e doğa l olara k dışarıdak i bi r seyaha t acentasını n da . Kimse Sosya l Güvenli k Numarası' m sı r gib i saklamaz . N e far k ede r ki ?

Yanıtı bulma k zo r değil . Etkil i bi r canlandırm a (toplu m mühendisini n kendini başk a birini n kılığın a sokması) içi n iki-ü ç parç a bilg i fazlasıy - la yeterlidir . Yar ı yeterlilikt e bi r toplu m mühendisi , bi r çalışanı n adını , telefon numarasını , Sosya l Güvenli k Numarası'n ı -v e iş i sağlam a almak içi n yöneticisini n adın ı v e telefo n numarasını - eld e ettikte n sonra, sıradak i hedefin e yönelirke n kendin i inandırıc ı gösterme k içi n ihtiyacı olabilece k he r şeyl e donanmı ş olacaktır .

Eğer şirketinizi n başk a bi r bölümünde n olduğun u söyleye n bir i dü n aramış, maku l bi r nede n vermi ş v e özlü k numaranız ı sormu ş olsaydı , bu bilgiy i on a vermekt e tereddü t ede r miydiniz ?

- Bıı arada, Sosyal Güvenlik Numaranız neydi?

Aldatmacanın Engellenmes i

Şirketinizin, herkes e açı k olmaya n bilgileri n kötüy e kullanılmasında n doğabilecek cidd i sorunlar a karş ı çalışanların ı bilgilendirm e sorumluluğ u vardır. Üzerind e düşünülmü ş bi r bilg i güvenliğ i politikası , düzgü n bi r bil - gilendirme v e eğitiml e birleşinc e şirke t bilgilerini n doğr u kullanımıyl a ilgil i çalışan bilinc i görünü r şekild e artacaktır . Bi r ver i sınıflandırm a politikası , bilgi vermey e yöneli k uygu n denetimle r getirilmesin e yardımc ı olacaktır . Veri sınıflandırm a politikas ı olmadan , tü m şirke t iç i bilgileri n -aks i belir - tilmediği sürece - gizl i olara k değerlendirilmes i gerekecektir .

Şirketinizi zararsı z gib i görüne n bilgileri n dışar ı sızmasından koru - mak içi n şunlar ı yapın :

• Bilg i Güvenliğ i Birimi'nin , toplu m mühendislerinin kullandığ ı yön -

temleri anlata n bilgilendirm e eğitimler i düzenlemes i gerekir .

Yukarıda anlatıldığ ı üzere , yöntemlerde n biri , hassasmı ş gib i

durmayan bi r bilgiy i eld e etme k v e bun u kıs a vaded e güve n

yaratmak içi n bi r poke r markas ı gib i kullanmaktır . Telefonl a

arayan birinin , şirke t süreçleri , terimle r v e şirke t iç i tanımlayıcıla r

konusunda bilgil i olmasını n n e şeki l v e tarzd a olurs a olsu n iste k

sahibini gerçe k kılmadığında n y a d a bi r şey i bilmes i gerektiğ i

Zararsız Gib i Görüne n Bilgile r 2 7

konusunda on u yetkil i konum a getirmediğinde n te k te k he r çalışanın haberda r olmas ı gerekir . Araya n kiş i esk i bi r çalışa n y a <l;ı gerekl i şirke t iç i bilgiler e sahi p bi r sözleşmel i olabilir . Bun a ilörc, he r kuruluş , tanımadığ ı insanlarl a telefond a y a d a yüzyüz e iletişim kurarke n çalışanlarını n kullanmas ı gereke n uygu n kimli k tospit yöntemin i belirlem e sorumluluğun a sahiptir .

Mir ver i sınıflandırm a politikas ı tasarlamakla yüküml ü kiş i y a d a kimiler, zararsı z gib i görüne n am a hassa s bilgiler e erişim i ola n çalışanlara ulaşılmasın ı sağlayabilece k ayrıntılar ı gözde n geçirmelidirler. AT M kartınızı n şifresin i hiçbi r zama n dışar ı ver - memenize karşın , şirke t yazılı m ürünlerin i geliştirme k içi n kul- landığınız sunucunu n hangis i olduğun u birin e söyle r misiniz ? B u bilgi, şirke t ağın a erişi m hakk ı varmı ş gib i davrana n bir i tarafın - dan kullanılabili r mi ?

na/en şirke t iç i terimler i bilme k bil e toplu m mühendisini n dah a otoriter v e bilgil i görünmesin i sağlayabilir . Saldırgan , kurbanların ı ikna etme k içi n he r a n olabilece k b u yanlı ş anlamay a sı k sı k başvurur. Örneğin , Üy e İşyer i Numarası , bi r bankanı n Yen i Hesaplar birimind e insanları n he r gün , üzerind e pe k fazl a düşün - moden kullandıklar ı bi r tanımlayıcıdır . Anca k böyl e bi r tanım - layıcının bi r parolada n fark ı yoktur . Eğe r he r bi r çalışa n b u tanım - layıcının anlamın ı kavramışs a -yan i iste k sahibini n gerçe k olu p olmadığını kanıtlama k içi n kullanılıyorsa - o zama n b u veriy e daha saygıyl a bakabilirler .

Hiçbir şirke t -e n azında n birka ç tanesi - gene l müdürlerini n y a d a yönetim kurul u başkanlarını n doğruda n telefo n numaraların ı dışarı vermezler . Bun a karşın , çoğ u şirkette , çoğ u biri m v e çalış - ma grubunu n telefo n numaraların ı dışar ı -özellikl e d e diğe r bi r çalışana y a d a çalışa n gib i görünen birine - vermekl e ilgil i bi r çe - kince yoktur . Alınabilece k bi r önlem : Çalışanların , sözleş - melilerin, danışmanları n v e geçic i görevlileri n dahil i telefonlarını n başkalarına verilmesin i yasaklayan bi r yönetmeliğ i yürürlüğ e koyun. Dah a d a önemlisi , telefon numaras ı sora n kişini n gerçek - ten bi r çalışa n olu p olmadığın ı ta m olara k belirleme k içi n adı m adım bi r süre ç geliştirin .

Çalışma gruplarını n v e birimleri n muhaseb e hesa p numaralar ı da, (iste r basılı , iste r ver i dosyas ı y a d a intrane t üzerind e elekt - ronik telefo n defter i olsun) telefo n rehberler i kada r sık , toplu m mühendislerinin hedef i olmaktadırlar . He r şirketi n b u tar z bilgi - lerin dışar ı verilmesiyl e ilgil i iy i anlatılmış , yazıl ı bi r kuralla r Inilününe ihtiyac ı vardır . Alınaca k önlemle r arasında , hassa s bil - gilerin şirke t dışında n insanlar a verildiğ i durumları n no t edildiğ i bir kayı t defterini n tutulmas ı d a olmalıdır .

Mitnick Mesajı :

Eski bir deyişte de ifade edildiği gibi: Gerçek paranoyakların bile biivük olasılıkla düşmanları vardır. Her işletmenin de düşmanları olduğunu, şirket sırlarını tehlikeye sokmak amacıyla ağ altyapısına saldırabilecek saldırgan- lar bulunduğunu varsaymalıyız. Sonunuz bir bilgisayar suçları istatistiği olmasın, iyi düşünülmüş güvenlik kuralları ve süreçleri aracılığıyla uygun denetimleri yerleştirerek gerekli savunmaları kurmanın zamanı geldi de geçiyor bile.

• Sosya l Güvenli k Numaras ı gib i bilgiler , te k başların a bi r tanımla -

ma arac ı olara k kullanılmamalıdırlar . He r çalışa n yalnızc a iste k

sahibinin kimliğin i doğrulamakl a kalmamalı , ayn ı zamand a

isteğin nedenin i d e sorgulamalıdır . Güvenli k eğitimlerini z sırasın -

da çalışanlarınız a ş u yaklaşım ı öğretmey i deneyin : N e zama n

tanımadığınız bir i siz e bi r sor u sora r y a d a sizde n yardı m isterse ,

herşeyden önc e iste k onaylanan a kada r nazikç e ger i çevirmey i

öğrenin. Sonr a -ba y y a d a baya n Yardımseve r olm a yönündek i

doğal dürtünüz e yeni k düşmede n önce - onaylam a v e şirke t iç i

verilerin dışarıy a verilmesiyl e ilgil i yönetmelikler i v e süreçler i

uygulayın. B u yaklaşım , başkaların a yardı m etmey e yöneli k

doğal eğilimimiz e ter s düşebilir , anca k sağlıklı , azıcı k bi r şüphe -

cilik, toplu m mühendisini n bi r sonrak i kurban ı olmakta n kurtul -

manızı sağlayabilir .

Bu bölümdek i öyküleri n d e gösterdiğ i gib i zararsı z zannettiğini z bil - giler şirketinizi n e n öneml i sırlarını n anahtar ı olabilirler .

DOĞRUDAN SALDIRI : YALNIZCA İSTEYİVERME K

I'ek ço k toplu m mühendisliğ i saldırıs ı karmaşıktır . Bi r tekni k bilg i v e dtılavore karışımını n kullanıldığ ı bi r diz i aşam a v e ayrıntıl ı planlam a lı.tııı.

Ama becerikl i bi r toplu m mühendisini n zama n zama n amacın a lüi'.ilço, kolayc a v e laf ı dolandırmada n ulaşmasın ı d a he r zama n çarpıc ı lıılmuijumdur. Göreceğini z gibi , bilgiy i

doğruda n isteyiverme k bil e te k |ı« ı:,.ıı ı.) yeterl i olabilir .

Bir MHB M Marifet i

Birinin rehberd e geçmeye n telefo n numarasın ı m ı öğrenme k istiyor - MIMII/? Bi r toplu m mühendis i size , bi r kısmın ı b u kitabı n sayfalarınd a d a bulabileceğiniz, çeşitl i yöntemle r sıralayabilir , anca k büyü k olasılıkl a e n h.ısil yönte m te k bi r telefon konuşmas ı yapmaktır . Tıpk ı aşağıd a .ıı ıl,ılıklığı gibi .

Numara Lütfe n

Saldırgan öze l bi r telefon şirketini n MHB M (Mekani k Ha t Belirlem e Mm kezi) numarasın ı çeviri r v e telefon u aça n kadın a şöyl e der :

"Merhaba, be n Pau l Anthony . Kabl o tamircisiyim . Bi r sorunu m var , burudaki bi r termina l kutus u bi r yangınd a yanmış . Polisler , manyağı n birinin sigortada n par a alabilme k içi n evin i yaktığın ı düşünüyorlar . Bütü n bu ik i yü z hatlı k terminali n tümün ü yenide n bağlama m içi n ben i burad a lok başım a bıraktılar . Ş u and a gerçekte n ço k yardım a ihtiyacı m var . (i/23 Sout h Main'd e hang i hatları n çalışı r durumd a olmas ı gerektiğin i bana söylebili r misin? "

Telefon şirketini n diğe r birimlerinde , arana n kişi , rehberd e değmeyen numaralarl a ilgil i ter s sorgulam a bilgilerin i yalnızc a şirketi n yi «ikil i personelin e vermeler i gerektiğin i bilirler . Anca k MHBM'ni n d e yal - nızca şirke t çalışanlar ı tarafında n biliniyo r olmas ı gerekir . Dışarıy a hiç - bir zama n bilg i vermiyo r olsala r da , ağı r bi r işi n altında n kalkmay a çalışan başk a bi r şirke t çalışanın a bira z yardı m edilmesin e ki m itira z odelıilir ki ? Kadın , adamı n durumun a üzülür . Kendisini n d e işbaşınd a /,«ı günle r geçirdiğ i olmuştu r v e zo r durumd a ola n başk a bi r çalışan a yardım edebilme k içi n kurallar ı birazcı k esnetir . On a kabl o çiftlerin i söyler v e o adres e bağl ı tü m açı k numaralar ı verir .

AAitnick Mesajı :

Yanımızdaki adama güvenmek insan doğasının bir parçasıdır, özellikle de talep sağduyulu olup olmadığımızı ölçüyorsa. Toplum mühendisleri bu bilgiyi, kurbanlarını sömürmek ve amaçlarına ulaşmak için kullanırlar.

Aldatmaca'nın İncelenmes i • • • • •

Bu öykülerd e sı k sı k göreceğini z gibi , b' r şirkett e kullanıla n termi - nolojiyi y e şirke t yapısın ı - çeşitl i büroların ı v e birimlerini , he r birini n n e yaptığını v e hang i bilgiler i tuttuklarını - bilme k başarıl ı bi r toplu m mühen - disinin kullandığ ı araçları n öneml i bi r kısmın ı oluşturur .

Genç Bi r Kanu n Kaçağ ı

Kendisine Fran k Parson s diyeceğimi z bi r ada m yıllardı r poliste n kaç - maktaydı v e Federa l Hüküme t tarafından , hâlâ , 1960'lard a sava ş karşıt ı bir yeralt ı örgütünü n üyes i olduğ u gerekçesiyl e aranıyordu . Lokantalard a kapıya dönü k otururd u v e diğe r insanları n sıkınt ı veric i bulduğu , arad a bi r omuzunun üzerinde n geriy e bakm a huy u vardı . Birka ç yıld a bi r taşınırdı .

Arada bi r yerde , Fran k kendin i dah a önc e bulunmadığ ı bi r şehird e buldu v e i ş aramay a koyuldu . Gelişmi ş bilgisaya r becerilerin e sahi p ola n (aynı zamand a gelişmi ş toplu m mühendisliğ i becerilerin e d e sahipti , anca k bunları i ş başvurularınd a hi ç belirtmiyordu) Fran k gib i bir i içi n iy i bi r i ş bul - mak genellikl e soru n olmuyordu . Ekonomini n sıkışı k olduğ u zamanla r dışında iy i bilgisaya r bilgis i ola n kişileri n yeteneklerin e ola n tale p genellik - le yükse k oluyord u v e böyleler i çoğ u zama n dör t aya k üstün e düşüyorlardı . Frank, yaşadığ ı yeri n yakınlarındak i geli r düzey i yükse k insanlar a hizme t veren büyü k bi r bakı m yurdund a yükse k gelirl i bi r iş e girm e firsat ı buldu .

Bu işi n kendis i içi n biçilmi ş kafta n olduğun u düşündü . Anca k başvu - ru evrakıyl a boğuşmay a başlayınc a bi r noktad a durma k zorund a kaldı , işveren onda n Adl i Sici l Belges i istiyord u v e bun u eyale t polisinde n şah - sen almas ı gerekiyordu . İ ş başvur u evraklarını n arasınd a b u belgeni n istenmesi içi n kullanıla n matb u dilekç e d e vard ı v e dilekçeni n üzerind e parmak iz i basma k içi n küçü k bi r kutucu k bulunuyordu . He r n e kada r yalnızca sa ğ işare t parmağını n izin i istiyo r olsala r da , eğe r parma k izin i FBI veritabanındak i parma k iziyl e karşılaştırırlars a kıs a sür e içerisind e parasını devleti n ödediğ i bi r tati l köyünd e yeme k servis i yapıyo r olurdu .

Öte yanda n Frank , küçü k bi r olasılıkl a d a olsa , bunda n sıyrılabileceği - ni düşünüyordu . Belk i d e eyale t polis i parma k iz i örneklerin i FBI'y a hiçgön - dermiyordu. B u durumd a gönderi p göndermediklerin i nası l öğrenebilirdi ?

Nasıl mı ? O bi r toplu m mühendisiydi ; nası l öğrend i sanıyorsunuz ?

Doğrudan Saldırı : Yalnızc a isteyiverme k 3 1

Mifnick Mesajı :

Akıllı bilgi dolandırıcıları, emniyet teşkilatının asayişi sağlama süreçleriyle ilgili bilgi almak için devlet, eyalet ya da yerel yetkilileri aramaktan çekin- mezler. Elinde böyle bir bilgiler varken toplum mühendisi şirketinizin sıradan güvenlik uygulamalarını atlatabilir.

Eyalet polisin e telefon etti : "Merhaba . Adale t Bakanlığ ı içi n bi r çalışm a yapıyoruz. Yen i bi r parma k iz i tespi t sistem i yerleştirme k içi n gerekl i ö n koşulları araştırıyoruz . Yapıla n iş i iy i bile n v e biz e yardı m edebilece k biriyle görüşebili r miyim? "

Yerel uzma n telefon a geldikte n sonr a Frank , kullandıklar ı sistemler - le v e parma k iz i verilerin i saklam a v e taram a kapasiteleriyl e ilgil i bi r diz i soru sordu . Kullandıklar ı donanı m hi ç onlar a soru n çıkarmı ş mıydı ? Ulusal Su ç Bilgiler i Merkezi'ni n (USBM) Parma k iz i Taram a Ağı'n a m ı bağlıydılar yoks a yalnızc a eyaletinkin e mi ? Donanı m herkesi n öğrenebileceği kada r kola y bi r kullanım a sahi p miydi ?

Anahtar soruy u diğerlerini n arasın a kurnazc a sıkıştırmıştı .

Aldığı yanı t kulağın a müzi k gib i geldi . Hayır , USBM'y e bağl ı değiller - di, ellerindekin i yalnızc a eyaleti n Su ç Bilgiler i Dizini'yl e karşılaştırıyor - lardı. Frank'i n d e tü m bilme k istediğ i buydu . Bulunduğ u eyalett e su ç kaydı yoktu , böylec e başvurusun u yaptı , iş e alınmışt ı v e hi ç kims e bi r gün masasını n başın a dikili p d e ona , "B u beyle r FBI'da n geliyorlar , seninle konuşma k istiyorlarmış, " demedi .

Ve kend i söylediğin e bakılırs a işyerindek i herkes e örne k bi r çalışanın nası l olmas ı gerektiğin i göstermişti .

Kapının ön ü

Kâğıt kullanılmaya n ofi s inancın a karşı n şiketle r he r gü n yüzlerc e sayfa kâğı t tüketiyorlar . Şirketinizdek i basıl ı bilgiler , güvenli k önlemler i alıp üzerin e "gizlidir " damgas ı vursanı z da , açı k bi r nokt a oluşturabilirler .

işte size , toplu m mühendislerini n e n gizl i belgeleriniz i nası l el e geçirdiklerini anlata n bi r hikâye .

Hat Çevirm e Dalaveres i

Telefon şirket i he r yı l Deneme Numaralan Rehberi adınd a bi r kitapçık çıkarı r (y a d a e n azında n eskide n çıkarırlardı , şartl ı tahliy e sürem henü z dolmadığ ı içi n çıkarmay a deva m edi p etmediklerin i sor - mayacağım). B u kitapçık , telefon beleşçilerini n e l üstünd e tuttuklar ı bi r belgedir, çünk ü şirke t görevlilerinin , teknisyenlerini n v e diğerlerini n

Miînick Mesajı :

Bilgi varlıklarını korumaya ilişkin şirket kurallarıyla ilgili güvenlik eğitim- leri, yalnızca şirketin BT varlıklarına elektronik ya da maddi erişimi oları çalışanlara değil, şirketteki herkese yönelik olmalıdır.

sürekli meşgu l çala n numarala n y a d a şehirleraras ı hatlar ı kontro l etmek içi n kullandıkları , özenl e koruna n telefon numaralarıyl a doludur .

Bu numaralardan , telefo n beleşçiler i argosund a hat çeviren olara k bilinen bi r tanes i özellikl e ço k kullanışlıydı . Telefo n beleşçileri , kendiler i tek kuru ş par a ödemeden , konuşaca k başk a telefo n beleşçiler i bulma k için bun u kullanırlardı . B u numar a ayn ı zamanda , örneği n bi r bankay a vermek üzere , ger i aram a numaras ı yaratma k içi n d e kullanılırdı . Bi r toplum mühendis i bankadak i birin e on a ofisinde n ulaşılabileceğin i söyleyerek b u numaray ı verirdi . Banka , numaray ı kontro l etme k üzer e telefon ettiğind e (ha t çevirme) , telefon beleşçis i telefon a ceva p verebilir , izi sürülemeyece k bi r telefo n numaras ı kullanmanı n sağladığ ı koru - madan d a yararlanmı ş olurdu .

Bir Deneme Numaralan Rehberi, bilgiy e a ç v e testosteron u tavan a vur - muş herhang i bi r telefo n beleşçis i tarafında n kullanılabilece k bi r sür ü hari - ka bilg i içerir . B u yüzde n he r yı l yen i rehberle r çıktığında , hobiler i telefo n ağını keşfetme k ola n bi r yığı n gen ç derha l b u rehberleri n peşin e düşer .

Stevie'nin Oyun u , " ' . " . • : ' ' '

Telefon şirketler i doğa l olara k b u kitapçıklar ı kola y ulaşılabili r yerler e koymaz, b u yüzde n telefo n beleşçilerini n bi r tan e eld e edebilmeler i içi n yaratıcı olmalar ı gerekir . Bun u nası l yaparlar ? Kafasın ı rehber i el e geçirmeye takmış hevesl i bi r gen ç aşağıdak i gib i bi r oyu n oynayabilir .

Bir gün , güne y Californi a sonbaharını n seri n akşamlarında n birinde , kendisine Stevi e diyeceğimi z biri , küçü k bi r telefo n şirketini n gene l müdürlüğünü arar . Hizme t bölges i içerisindek i tü m evler e v e i ş yerlerin e telefon hatlar ı d a b u binada n dağılmaktadır . ,

Görev başındak i teknisye n telefon u açtığında , Stevi e telefon şirke - tinin basıl ı malzemelerin i bası p dağıta n bölümünd e çalıştığın ı açıklar . "Yeni Denem e Numaralar ı Rehberini z hazır, " der . "Anca k güvenli k gerekçeleriyle eskisin i ger i almada n yenisin i veremiyoruz . Dağıtımcımızın iş i d e oldukç a uzadı . Eğe r sizdek i rehber i kapınızı n önüne bırakabilirseniz , geçerke n eskisin i alı p yenisin i bırakabilir , sonr a da kend i işin e bakar. "

Hiçbir şeyde n kuşkulanmaya n teknisye n bunu n uygu n olduğun u düşünmüş olmalıdı r ki , istenen i ta m olara k yapar . Kapağınd a büyü k kır -

Doğrudan Saldırı : Yalnızc a isteyiverme k 3 3

- z ı harflerle , "GİZLİDİ R V E ŞİRKE T İÇ İ KULLANI M İÇİNDİR-İHTİYA Ç KALMADIĞI TAKDİRDE , B U BELG E KAĞI T ÖĞÜTM E MAKİNASIND A CGÜTÜLMELİDİR," uyarıs ı buluna n rehber i binanı n önün e koyar .

Stevie arabasıyl a geli r v e par k edilmi ş arabaları n içind e bekleye n y a ;s ağaçları n arkasın a saklanmı ş poli s y a d a şirke t güvenli k elemanları - na karş ı etraf ı dikkatl e kolaça n eder . Görünürd e kims e yoktur . Raha t tavırlarla ihtiyac ı ola n rehber i alır , arabasın a bine r v e gider .

işte size , bi r toplu m mühendisini n "yalnızc a isteyivermek " gib i basi t Dir yöntem i kullanara k istediklerin i n e kada r kola y eld e edebildiğin i gösteren bi r hikây e daha .

Gaz Saldırıs ı

Bir toplu m mühendisliğ i senaryosund a tehliked e ola n yalnızc a şirke t varlıkları değildir . Baze n kurbanla r şirke t müşterileridir . Müşter i hizme t temsilcisi olara k çalışmanı n getirdiğ i sıkıntılar , neşel i anla r v e masu m hatalar vardır . Anca k b u hataları n bazılar ı şirke t müşteriler i içi n köt ü sonuçlar doğurabilir .

Janie Acton'u n Öyküs ü

Janie Acton , ü ç yılda n bira z fazl a bi r süredir , Washington'daki Hometown Elektri k Şirketi'nd e müşter i hizme t temsilcis i olara k bi r ofi s bölmesini işga l etmektedir . Akl ı v e çalışkanlığıyla , e n iy i müşter i hizmet temsilcilerinde n bir i olara k görülmektedir .

Söz konus u telefo n geldiğind e Şükra n Haftası'dır . Araya n şöyl e der , "Ben Eduardo, Faturalama Bölümü'nden. Telefonda bir hanım var, genel müdür yardımcılarından birinin özel kaleminde sekreter. Bir bilgiye ihtiyacı var ve ben bilgisayarımı kullanamıyorum. İnsan Kaynaklarındaki şu kızdan 'SENİSEVİYORUM' diyen bir e-posta aldım ve ekini açtığımda, bir daha bilgisayarımı kullanamaz oldum. Vırüsmüş. Basit bir virüs tarafından avlandım. Herneyse, benim için bazı müşteri bilgilerine bakabilir misin?

"Elbette," diy e yanıtlad ı Janie . "Bilgisavarını m ı çökertti? Korkunç bir şey bu."

"Evet."

"Nasılyardımcı olabilirim?" diy e sord u Janie .

Bu noktad a saldırga n kendi m inanılı r kılma k içi n dah a önc e yaptığ ı araştırmalara başvurdu . İstediğ i bilgini n Müşter i Fatur a Bilgiler i Sistemi dene n bi r yerd e tutulduğun u v e çalışanları n b u sistem e n e a d verdiklerim öğrenmişti . "MFBS'den bir hesap numarasına bakabilir misin?" diy e sord u telefondak i adam .

"Evet, hesap numarası nedir?"

: "Numarayı bilmiyorum. İsimden sorgulaman gerekecek. " •'.

"Tamam, isim nedir?"

"Heather Marning. " İsmi n harflerin i kodlad ı v e Jani e d e ism i bilgisa -

yara girdi .

"Tamam. Geldi." ' '

"Harika. Hesap geçerli mi?" , , .

"Hı hı, geçerli."

.••'., "Hesap numarası nedir?" diy e sord u adam . , :

"Kalemin var mı?"

"Hazırım." ' • . . "Hesap numarası, BAZ6573NR27Q."

Adam numaray ı tekrarladı , sonr a da , "Hizmet adresi nedir?" diy e sordu.

, Kadı n on a adres i verdi . ,

"Telefon numarası nedir?" • ; •'..; . Janie nazi k bi r şekild e o bilgiy i d e okudu .

Arayan teşekkü r etti , hoşçaka l ded i v e telefon u kapadı . Jani e bek - lemedeki aramay a yanı t verd i v e konunu n üstünd e d e hi ç durmadı .

Art Sealy'ni n Araştırm a Projes i

Art Sealy , yazarla r v e işletmele r içi n araştırm a yapara k dah a ço k para kazanabileceğin i öğrenince , küçü k yayınevleriri e serbes t editö r olarak çalışmay ı bırakmıştı , işi n onu , yasallı k v e yasadışılı k arasındak i ince çizgiy e yaklaştırdığ ı orand a ücretini n d e artabileceğin i kıs a süred e fark etti . Art , hi ç farkınd a olmada n v e kesinlikl e yaptığın a bi r isi m verme - den bi r toplu m mühendis i olmuştu . He r bilg i simsarını n bildiğ i bütü n teknikleri kullanıyordu . Yaptığ ı iş e yöneli k doğa l bi r yeteneğini n olduğ u ortaya çıktı . Pe k ço k toplu m mühendisini n başkalarında n öğrendiğ i teknikleri kend i başın a keşfediyordu . Bi r sür e sonr a e n ufa k bi r suçlulu k duymadan o inc e çizgiy i aştı :

Nixon dönem i kabinesiyl e ilgil i kita p yaza n bi r ada m ben i aradı . Nixon'un Hazin e Müsteşar ı ola n VVİllia m E . Simon'l a igil i öze l bilgiler e ulaşabilecek bi r araştırmac ı arıyordu . Ba y Simo n artı k yaşamıyord u ama yazarı n elind e onunl a birlikt e çalışmı ş bi r kadını n ad ı vardı . Kadının başkentt e oturmay a deva m ettiğinde n d e oldukç a emindi , ancak adresin i bulamamıştı . Kadını n adına , e n azında n rehberd e olan - lar arasında , kayıtl ı bi r telefo n yoktu , işt e o zama n ben i aramıştı . On a kesinlikle-yapabilebileceğimi, soru n olmayacağın ı söyledim .

Eğer n e yaptığınız ı biliyorsanız , çoğunlukl a bir-ik i telefo n görüşme - siyle bulabileceğini z bi r bilgiyd i bu . He r yere l hizme t şirketini n b u bilgiy i

itnick Mesajı :

Bütün toplum mühendisliği saldırılarının, tamamlanmadan farkedilecek kadar karmaşık düzenler içerdiklerini sakın düşünmeyin. Bazıları gir-çık ya da vıır- kaç şeklinde çok basit saldırılardır v e .. . kısacası, yalnızca istemek üzerine kuruludurlar.

çoğu zama n paylaşacağında n emi n olabilirsiniz. Doğa l olara k bira z zır - valamanız gerekir . Arad a bi r küçü k beya z yalanla r söylemeni n kim e n e zararı dokunabili r ki ?

işleri ilgin ç kılma k içi n he r seferind e farkl ı bi r yönte m kullanma k hoşuma gider .

"Ben yöneti m katında n bilme m kim, " numaras ı bend e hi ç şaş - mamıştır. "Gene l müdü r yardımcıs ı bilme m kimi n ofisinde n bir i ş u and a diğer hatt â bekliyor, " numaras ı d a iyidi r v e b u olayd a d a iş e yaramıştır .

Telefonun diğe r ucundak i kişini n işbirliğ i yapmay a n e kada r eğilimli olduğunu hissedece k kada r toplu m mühendisliğ i içgüdünüz ü geliştirmi ş olmanız gerekir . B u ke z arkada ş canlıs ı yardımseve r bi r hanım a ras t geldim. Te k bi r görüşmede adres i v e telefon numarasın ı almıştım . Görev tamamlanmıştı .

Aldatmacanın İncelenmes i

Janie müşter i bilgilerini n n e kada r hassa s olduğun u kesinlikl e bili - yordu. Bi r müşterini n bilgilerin i başk a bi r müşteriyl e hiçbi r zama n pay - laşmaz y a d a öze l bilgiler i dışar ı vermezdi .

Ancak doğa l olara k şirke t içinde n araya n bir i içi n farkl ı kuralla r geçerliydi. Bi r mesa i arkadaş ı içi n b u birtakı m oyun u meselesiyd i v e iş i bitirmek karşılıkl ı yardımlaşmay a dayanıyordu . Faturalamadak i ada m eğer bilgisayar ı bi r virü s yüzünden çökmemi ş olsayd ı ilgil i bilgiler i kend i de bulabilirdi ; b u yüzde n Jani e bi r i ş arkadaşın a yardı m edebilmi ş olmaktan memnundu .

Art, peşind e olduğ u kili t bilgiler e ulaşırke n yava ş yo l ald ı v e hesa p numarası gib i aslınd a ihtiyac ı olmaya n şeylerl e ilgil i sorula r d a sordu . Ancak, ayn ı zamand a hesa p numaras ı bilgis i emniye t sübab ı görev i d e görüyordu. Eğe r görevl i kuşkulanaca k olsaydı , ikinc i bi r görevliy i araya - caktı v e böylec e başar ı şans ı dah a yükselecekti , çünk ü hesa p numarasını bilme k ulaşacağ ı bi r sonrak i görevliy e kendin i dah a d a inandırıcı göstermesin e yardımc ı olacaktı .

Birilerinin b u bilgile r içi n yala n söyleyebileceği , yan i arayanı n gerçekte faturalam a bölümünde n bir i olmayabileceği , Janie'ni n hi ç aklı -

na gelmemişti . Su ç elbettek i Janie'ni n değildi . Bi r müşter i dosyasındak i bilgileri paylaşmada n önc e kiminl e konuştuğunda n emi n olmas ı konusunda kims e on u bilgilendirmemişti . Kims e on a Art'ı n yaptığ ı gib i bir telefo n görüşmesini n oluşturabileceğ i tehlikelerde n sö z etmemişti . Şirket kurallar ı arasınd a d a yoktu , eğitimin i d e almamışt ı v e yöneticis i de bunda n hi ç bahsetmemişti . ,

Aldatmacanın Engellenmes i

Güvenlik eğitimlerind e aktarılmas ı gereke n bi r nokta : Telefonl a arayan birini n y a d a bi r ziyaretçinin , şirkettek i baz ı kişileri n adların ı y a dş şirke t iç i terimler i y a d a süreçler i biliyo r olması , onu n iddi a ettiğ i kiş i olduğunu göstermez . V e b u on u kesinlikl e ticar i bilgileri n v e bilgisaya r sistemine y a d a ağın a erişi m hakkını n verilebileceği , yetkil i bir i durumu - na d a getirmez .

Güvenlik eğitimini n şun u vurgulamas ı gerekir : Bi r kuşku n varsa , kontrol et , kontro l et , kontro l et .

ilk zamanlard a şirke t içind e bi r bilgiy e ulaşma k bi r konu m gösterge - siydi v e bi r ayrıcalıktı . İşçile r kazanlar ı doldururlar , makineler i çalıştırır - lar, mektuplar ı yazarla r v e evraklar ı dosyalarlardı . Ustabaş ı y a d a patron onlar a neyin , n e zama n v e nası l yapılacağın ı söylerdi . Bi r vardiyada he r işçini n ka ç ale t yapacağını ; b u haftayı , gelece k haftay ı v e ayın sonun u çıkarma k içi n fabrikanı n hang i boyu t v e renklerd e v e ka ç tane ale t üretmes i gerektiğin i ustabaş ı y a d a patro n bilirdi .

İşçiler makineleri , ara ç v e gereçleri ; patronla r is e bilgiy i kullanırlardı , işçilerin yalnızca , yaptıklar ı iş e özg ü bilgiler e ihtiyaçlar ı vardı .

Günümüz tablos u bira z farklı , öyl e değ i l mi ? Pe k ço k fabrik a işçis i bi r çeşit bilgisaya r y a d a bilgisayarl a çalışa n makin e kullanmaktadır . Sorumluluklarını yerin e getirere k işler i yürütebilmeler i için , hassa s bil - giler i ş başındak i kullanıcıları n bilgisayarların a kada r iner . B u duru m i ş gücünün büyü k çoğunluğ u içi n aynıdır . Bugünü n ortamınd a çalışanları n yaptığı neredeys e he r şe y bilg i kullanımın ı içermektedir . • . .

Bu yüzde n şirke t güvenli k kurallarını n konumda n bağımsı z olara k tüm kuru m için e dağıtılmas ı gerekmektedir . Bi r saldırganı n peşind e olduğu bilgiler e yalnızc a amirleri n v e üs t yöneticileri n sahi p olmadığın ı herkesin anlamas ı şarttır . Bugü n he r düzeydek i çalışanlar , hatt â bilgisa - yar kullanmayanla r bile , hede f olmay a açıktırlar . Müşter i hizmetler i bölümünde iş e yen i başlamı ş bi r müşter i temsilcisi , bi r toplu m mühen - disinin amacın a ulaşma k içi n kırma k isteyeceğ i zayı f halk a olabilir .

Güvenlik eğitim i v e şirke t güvenliğ i kurallar ı b u halkay ı güçlendirmelidir .

GÜVEN UYANDIRMA K

Bu öykülerde n bazıları , i ş dünyasındak i herkesi n süzm e sala k olduğuna v e mesleğiyl e ilgil i he r sırr ı dışar ı vermey e hazır , hatt â istekl i olduğuna inandığım ı düşünmeniz e nede n olabilir . Toplu m mühendis i Dunun doğr u olmadığın ı bilir . Nede n toplu m mühendisliğ i saldırılar ı b u kadar başarıl ı oluyor ? İnsanla r sala k y a d a sağduyusu z olduğ u içi n değil. Anca k bizle r aldatılmay a fazlasıyl a açığız , çünk ü insanla r bell i şekillerde yönlendirilirlers e yanlı ş şeyler e güve n duyabiliyorlar .

Toplum mühendisi , karş ı tarafta n kuşk u v e direniş bekle r v e he r zaman güvensizliğ i güven e dönüştürmey e hazırdır , iy i bi r toplu m mühendisi, saldırısın ı bi r satran ç oyun u gib i planla r v e doğr u yanıtlar ı verebilmek içi n hedefini n sorabileceğ i sorular ı öncede n tahmi n eder .

En ço k kullanıla n yöntemlerde n biri , kurband a güve n duygus u uyandırmaktır. Bi r dolandırıc ı on a inanı p güvenmeniz i nası l sağlayabili r ki? inanı n bana , bun u yapabilir .

Güven: Aldatmanı n Anahtar ı

Bir toplu m mühendisi , kurduğ u iletişim i n e kada r olağa n bi r işmi ş gib i gösterebilirse, oluşa n şüpheler i d e o kada r kola y bastırabilir . İnsanları n kuşkulanmak içi n bi r nedenler i olmazsa , toplu m mühendisinin , onları n güvenini kazanmas ı dah a kola y olur .

Bir ke z güvenlerin i kazandıkta n sonra , köpr ü ine r v e kaleni n kapılar ı ardı - na kada r açılır . Böylec e toplu m mühendis i içer i giri p istediğ i bilgiy i alabilir .

I Öykülerin çoğunda, toplum mühendislerine, telefon beleşçile- rine ve dolandırıcılara bir erkekmiş gibi gönderme yaptığım dikkatinizi çekmiş olabilir. Bu şovenizm değildir; yalnızca, bu alanlarda çalışanların çoğunun erkek olduğu gerçeğini vurgular. Her ne kadar çok fazla kadın toplum mühendisi olmasa da, sayılan giderek artmaktadır. Dışarıda, sadece telefonda bir kadın sesi duyduğunuz için yelkenleri suya indirme- menizi sağlamaya yetecek kadar çok dişi toplum mühendisi vardır. Doğrusunu isterseniz, kadın toplum mühendisleri, işbirliği sağlamak için cinselliklerini kullanabildiklerinden, belirgin bir üstünlükleri de yok değildir. Bu sayfalarda bu kadınların birkaçından söz edildiğini de göre- ceksiniz.

İlk Görüşme : Andre a Lope z

Andrea Lopez , çalıştığ ı vide o kiralam a mağazasınd a çala n telefon a baktı v e kıs a bi r sür e sonr a gülümsemey e başladı . Bi r müşterini n işin i gücünü bırakı p hizmette n n e kada r memnu n kaldığın ı söyleme k içi n , aradığın ı duyma k gibis i yoktu . B u arayan , mağazayl a i ş yapmakta n ço k memnun kaldığın ı v e yöneticiy e bi r mektu p gönderme k istediğin i söylemişti.

Yöneticinin adın ı v e adresin i sormuş , Andre a d a on a yöneticini n adını n Tommy Alliso n olduğun u söylemi ş v e adres i vermişti . Araya n ta m tele - fonu kapayacakke n aklın a başk a bi r şe y gelmi ş ve ,

- Şirket genel müdürlüğüne de birkaç satır yazabilirim. Mağaza kodunuz nedir, diy e sormuştu . Kadı n on a mağaz a kodun u d a verdik - ten sonr a ada m teşekkü r etmişti . Kendisin e ço k yardımc ı olduğ u içi n görevliye güze l bi r şeyle r dah a söyledikte n sonr a iy i günle r dileyere k telefonu kapatmıştı .

"Böyle bi r telefon , he r zama n mesaini n dah a hızl ı geçmesin i sağlıyor . İnsanlar bun u dah a sı k yapsala r n e kada r güze l olur. " diy e düşünmüşt ü Andrea.

İkinci Görüşme : Ginny

- Stıdio Video'yu aradığınız için teşekkürler. Ben Ginny, nasıl , yardımcı olabilirim?

- Merhaba, Ginny, ded i arayan , heyecanla . Ses i Ginny'l e dah a önc e her haft a konuşmu ş gib i geliyordu .

- Ben Tommy Allison, Forest Park, 863 kodlu mağazanın müdürü. Burada Roclcy V'i kiralamak isteyen bir müşterimiz var ve bizdeki tüm kopyalar dışarıda. Sende olup olmadığına bakabilir misin? Ginny bira z sonr a yenide n telefon u elin e ald ı ve ,

- Evet, bizde ü ç kopya var, dedi .

- Tamam. Müşteriye oraya gidip gidemeyeceğini soracağım. Teşekkür ederim. Eğer bizim mağazadan bir şeye ihtyiacm olursa, arayıp Tommy'i istemen yeterli. Senin için elimden geleni yapmaktan mem- nun olacağım.

Sonraki birka ç haft a boyunc a Tommy , bi r takı m konulard a yardım etmesi içi n Ginny' i üç-dör t ker e dah a aradı . İstekler i mantıkl ı şeylerd i ve kendisin e asıldığ ı duygusun u uyandırmada n he r zama n Ginny' e arkadaşça davranıyordu . Arad a bira z gevezeli k d e ediyordu . "Oak Park'taki büyük yangını duydun mu? Bir sürü yolu kapatmışlar" gib i şeylerden sö z ediyordu . B u aramala r günü n durağanlığında n bira z uzak - laşma firsat ı tanıyord u v e Ginn y onu n aramasında n he r zama n memnu n kalıyordu.

Bir gü n Tommy'ni n ses i gergindi .

. Güve n Uyandırma k 3 9

- Sizin bilgisayarda bir sorun var mı? diy e sordu .

- Hayır, diy e yanıtlad ı Ginny .

- Neden?

- Adamın biri arabasını bir telefon direğine çarpmış. Telefon şir- ketinden gelen tamircinin söylediğine göre şehrin bit bölgesi onarım tamamlanana kadar telefonlarım ve internet bağlantılarım kullana- mayacakmış.

- Oh, çok kötü. Adam yaralanmış mı?

- Cankurtaranla götürdüler. Her neyse biraz yardımını isteyebilirim. Burada Godfather H'yi kiralamak isteyen bir müşteriniz var ve kredi kartı yanında değil. Bilgileri benim için kontrol edebilir misin? - Elbette.

Tommy müşterini n adın ı v e adresin i verir . Ginn y d e adam ı bilgisa - yardan bulup , müşter i numarasın ı Tommy' e söyler .

- Geç getirmeleri y a d a mağazaya borcu var mı?" diy e sora r Tommy . - Görünen bir şey yok.

- Tamam, harika. Ona burada kağıt üzerinde bir müşteri numarası vereceğim. Daha sonra bilgisayarlarımız yeniden çalışmaya başladığında veritabanımıza da eklerim. Ödemesini sizin mağazada kullandığı kredi kartıyla yapmak istiyor ama kartı yanında değilmiş. Kart numarası ve son kullanma tarihi nedir?

Ginny so n kullanm a tarihiyl e birlikt e kar t numarasın ı d a on a verir . - Yardımın için teşekkürler. Yakında görüşürüz, de r Tomm y v e tele - fonu kapatır .

Doyle Lonnegan's n Öyküs ü

Lonnegan, kapınız ı açtığınızd a karşınızd a görme k isteyeceğini z tür - den bi r ada m değil . Bi r zamanla r ödenmeye n kuma r borçların ı toplam a işini yapa n Doyl e Lonnegan , kend i başın ı belay a sokmadığ ı sürece , arada bi r birilerin e yardı m etmey i d e sürdürmekteydi . B u olayda , bi r video mağazasın ı birka ç ke z telefonl a aramas ı içi n on a hatır ı sayılı r bi r miktar par a önerilmişti . Kulağ a oldukç a kola y geliyordu . Soru n "müşte - rilerinden" hiçbirinini n böyl e bi r dolabı n nası l çevrileceğin i bilmemesin - den kaynaklanıyordu . Lonnegan'ı n yeteneğin e v e bilgisin e sahi p birin e ihtiyaçları vardı .

İnsanlar poke r masasınd a şanssı z olduklarınd a y a d a saçmaladık - larında bahislerin i karşılama k içi n çe k yazmazlar . Bun u herke s bilir . Benim arkadaşlarım , elindek i paray ı masay a koymaya n bi r üçkağıtçıyl a neden sürekl i kuma r oynarla r ki ? Sormayın . Belk i d e kafalarınd a birka ç tahta eksiktir . Am a onla r beni m arkadaşlarım ; elde n n e gelir ?

• Adamı n paras ı yokmuş ; b u yüzde n d e çe k almışlar . Ş u iş e bakın !

Onu alı p bi r ATM'y e götürmeliydiler . Yapmalar ı gereke n şe y buydu . Am a hayır; çe k aldılar . He m d e ta m 3.23 0 dolarlık !

Doğal olarak , çe k karşılıksı z çıktı . N e bekliyordunu z ki ? O zama n beni aradılar ; yardı m edebili r miymişim ? Üzerlerin e kap ı kapayara k insanların ellerin i ezm e işin i artı k bıraktım . Dahas ı artı k ço k dah a iy i yöntemler var . Yüzd e 3 0 komisyo n alarak , onlar a elimde n gelen i yapacağımı söyledim . Böylec e ban a adamı n adın ı v e adresin i verdile r ve be n d e bilgisayarda n on a e n yakı n vide o kiralam a mağazasını n nere - si olduğun a baktım .

Çok acele m yoktu . Mağaz a müdürün ü ho ş tutma k içi n dör t telefo n görüşmesi yapmı ş v e sonra , hop , üçkağıtçını n kred i kart ı numarasın ı alıvermiştim.

Başka bi r arkadaşı m yar ı çıpla k kızları n dan s ettiğ i bi r ba r işletiyor - du. Ell i dola r karşılığınd a adamı n poke r parasın ı bardak i PO S maki - nasından çekti . Bakalı m üçkâğıtç ı bun u karısın a nası l açıklayacak ? Bankaya b u harcamanı n kendisin e ai t olmadığın ı söyleyeceğin i m i düşünüyorsunuz? Bi r dah a düşünün . Bizi m on u ço k iy i tanıdığımız ı bili - yor. V e eğe r kred i kart ı numarasın a ulaşabiliyorsak , bunu n yanısır a daha pe k ço k şey e d e ulaşabileceğimiz i anlayacaktır . İşi n o tarafind a endişelenecek hiçbi r şe y yok .

Aldatmacanın İncelenmes i

Tommy'nin Ginny'l e yaptığ ı il k konuşmala r tamame n güve n uyandır - maya yönelikti . Ası l saldır ı zaman ı geldiğinde , kadı n savunmay a geçmemiş v e Tommy' i iddi a ettiğ i kişi , yan i zincirdek i başk a bi r mağazanın müdür ü olara k kabul etmişti .

Hem nede n kabu l etmesi n ki ; on u zate n tanıyordu . Doğa l olara k onunla yalnızc a telefond a görüşmüşt ü am a güve n duymasın ı sağlaya - cak kada r bi r i ş arkadaşlığ ı yapıs ı kurulmuştu . Kadı n on u bi r ke z bi r müdür, ayn ı şirkett e çalışa n bi r yönetic i olara k gördükte n sonr a istene n güven sağlanmı ş v e geris i tereyağında n kı l çeke r gib i olu p bitmişti .

Mitnîck Mesajı :

Belalılar (The Sting) filmindeki güven uyandırma tekniği toplum mühendis- lerinin en etkili taktiklerinden biridir. Konuştuğunuz kişiyi gerçekten tanıyıp tanımadığınızı düşünmeniz gerekir. Az da olsa bazı durumlarda karşı taraftaki söylediği kişi olmayabilir. Bu nedenle hepimizin düşünmesi, incelemesi ve yet- kili olduğunu söyleyenleri sorgulamayı öğrenmesi gerekmektedir.

Güven Uyandırma k 4 1

Konuya Farkl ı Bi r Bakış : Kred i Kart ı Ele Geçirm e

Güven duygus u uyandırmak , bi r öncek i hikâyed e anlatıldığ ı gibi , he r zaman bi r diz i telefo n görüşmes i yapmay ı gerektirmez . Bunu n top u top u beş dakik a tuttuğ u bi r ola y hatırlıyorum .

Sürpriz! • ' • " • . .

Bir keresind e bi r lokantad a Henr y v e babasıyl a birlikt e oturuyordum . Sohbet sırasınd a Henry , kred i kart ı numarasın ı telefo n numaras ı gib i sağa sol a verdiğ i içi n babasın a kızdı . "Bir şey alırken tabi k i kart numaranı vereceksin" dedi . "Ama kart numaranı, onu kayıtlarında tutan bir mağazaya vermek; bu çok aptalca."

"Bunu yaptığım tek yer Studio Video" ded i Ba y Conklin , ayn ı vide o kiralama mağazalar ı zincirini n adı m vererek . "Ama fazla para çekişi var mı diye her ay kredi kartı ekstremi kontrol ediyorum."

"Elbette anlardın" ded i Henry , "ama kart numaranı onlara bir kere verdin mi, numarayı birinin çalması işten bile değil."

"Kötü niyetli bir çalışan gibi mi?"

"Hayır, herhangi biri; sadece çalışanlar değil."

"Saçmalıyorsun" ded i Ba y Conklin .

"Şimdi onları arayıp, bana senin Visa numaranı vermelerini sağlaya- bilirim" diy e heme n atıld ı Henry .

"Hayır, bunu yapamazsın" ded i babası .

"Beş dakika içinde yapabilirim, hem de tam burada, karşında. Masayı hiç terk etmeden."

Bay Conkli n gözlerin i kısmı ş on a bakıyordu . Kendinde n emi n olu p d a bunu gösterme k istemeye n birini n havas ı vardı . "Sen n e söylediğinin farkında değilsin" diyere k güld ü v e cüzdanın ı çıkarı p içinde n çıkardığ ı bir ell i dolarlı k banknot u masay a çarptı . "Eğer söylediğini yapa- bilirsen, şu senin."

"Paranı istemiyorum baba" ded i Henry .

Cep telefonun u çıkardı , babasın a hang i mağazay ı kullandığın ı sord u v e oranın telefo n numarasını n yanısır a Sherma n Oak s yakınlarındak i mağazanın telefonun u d a öğrenme k amacıyl a Bilinmeye n Numaralar' ı aradı.

Sonra Sherma n Oaks'dak i mağazay ı aradı . Öncek i öyküd e anlatıla n yaklaşıma oldukç a yakı n bi r yönte m kullanarak , heme n müdürü n adın ı ve mağazanı n kodun u öğrendi .

Sonra d a babasının müşteris i olduğ u mağazay ı aradı , müdürü n adın ı

kendi adıymı ş gib i kullanıp , a z önc e eld e ettiğ i mağaz a kodun u d a ve - rerek, herkesi n bildiğ i yönetici ayağına yatma numarasın ı çekti . V e aynı oyun u yaptı . "Bilgisayarlarınız düzgün çalışıyor mu? Bizimkiler gidip geliyor." Karş ı tarafi n yanıtın ı dinled i v e sonra , "Sizin müşteriler- den biri buradan bir video kiralamak istiyor ama bizim bilgisayarlar şu anda çökmüş durumdalar. Müşteri numarasına bakıp mağazanızın müşterisi olup olmadığını kontrol etmenizi rica edebilir miyim?" diy e sordu.

Henry karş ı taraf a babasını n adın ı verdi . Ardında n yöntemd e küçü k bi r değişiklik yaparak , adresi , telefo n numarasın ı v e müşter i numarasını n verildiği tarih i d e okumasın ı istedi . Sonr a da , "Burada bekleyen bir yığın müşterim var. Kredi kartı numarası ve son kullanma tarihi nedir?" diy e sordu .

Henry bi r eliyl e ce p telefonun u kulağınd a tutarke n diğe r eliyl e peçetenin üzerin e numaray ı yazdı . Konuşmay ı bitirirke n peçetey i babasının önün e doğr u itti . Babas ı is e ağz ı açı k bakakaltnıştı . Zavall ı adam tamame n şo k olmuştu ; sank i tü m emniye t hiss i bi r darbed e yıkılıp gitmişti . , •

Aldatmacanın İncelenmes i : . ' . •

Tanımadığınız bir i sizde n bi r şe y istediğ i zama n kend i vereceğini z tepkiyi düşünün . Pejmürd e görünüml ü bi r yabanc ı kapınız a geldiğind e onu içer i alm a olasılığını z düşüktür ; eğe r iy i giyimli , ayakkabılar ı boyalı , saçları taralı , nazi k tavırl ı ve gülümseye n bi r yabanc ı kapınız a gelirse , herhalde o kada r şüphec i olmazsınız . Belk i d e gele n aslınd a Onüçünc ü Cuma filmlerinde n çıkmı ş Jason'dır , am a olağa n görünüml ü v e elind e keskin bi r bıça k taşımaya n bir i vars a karşınızd a iş e on a güvenere k başlarsınız.

Bu kada r belirgi n olmamakl a birlikt e telefond a konuştuğumu z insan - lar hakkınd a d a benze r bi r şekild e hükü m veririz . B u kiş i ban a bi r şeyle r mi satmay a çalışıyor ? Arkadaşç a v e açı k m ı davranıyo r yoks a bi r bask ı ve saldırganlı k seziyo r muyum ? Eğitiml i bir i gib i m i konuşuyor ? Tü m bunları v e farkınd a olmada n bi r düzin e başk a şey i daha , gö z açı p kapayıncaya kadar , konuşmanı n il k anlarınd a tartıveririz .

işteyken insanla r sürekl i bizde n bi r şeyle r isterler . B u adamı n e-posta adres i send e va r mı ? Müşter i listesini n e n so n şekl i nerede ? Projenin b u kısmını n taşeron u kim ? Ban a e n so n proj e güncellemesin i gönderir misi n lütfen . Kayna k kodu n yen i sürümün e ihtiyacı m var .

Ve tahmi n edi n n e olur : B u istekler i aldığınızı n insanla r baze n şah - sen tanımadığını z kişiler , şirketi n başk a bi r bölümünd e çalışa n y a d a orada çalıştıkların ı söyleye n şahısla r olurlar . Am a eğe r verdikler i bilg i doğruysa v e kon u üzerind e bilgil i gib i görünüyorlars a ("Mariann e ded i k i . . ." ; "Dosy a K-1 6 sunucusundaymı ş . . ." ; "Yen i ürü n planlarını n 2 6

Güven Uyandırma k 4 3

Mitnîck Mesajı :

Aksi yönde düşünmemizi gerektirecek bir şey yol<sa, kurduğumuz herhangi bir iletişimde kandırılma olasılığımızın düşük olduğunu düşünmek insan doğasının bir gereğidir. Riskleri tartarız sonra da çoğu zaman insanlara güvenmeyi tercih ederiz. Medeni insanların davranış biçimi budur...en azından daha önce hiç dolandırma, yönlendirme ve kandırma yoluyla büyük paralar kaptırmamış olan medeni insanlar için.

Çocukken anne-babamız bize yabancılara güvenmememizi öğretmişlerdi. Belki de bu eski nasihati bugünün iş ortamlarında hepimiz hatırlamalıyız.

numaralı tashih i . . .") , güve n çemberimizi , onlar ı d a için e alaca k şekild e genişletiriz v e hi ç endiş e duymada n istediklerin i onlar a veririz .

Arada bi r duralayıp , kend i kendimize , "Dalla s fabrikasında n bir i neden yen i ürü n planların ı görmey e ihtiya ç duysu n ki? " y a d a "Hang i sunucuda olduğun u söyleme k herhang i bi r şey e zara r veri r m i ki? " diy e sorabiliriz. Böyl e bir-ik i sor u dah a sorarız . Eğe r yanıtla r mantıkl ı görünü r ve karş ı tarafı n tavr ı d a güve n veric i olurs a kuşkulanmay ı bırakır , karşımızdaki adam a y a d a kadın a güvenm e yolundak i doğa l eğilimimiz e geri döneriz . Maku l sınırla r içerisinde , bizde n istene n neys e on u yaparız.

Bir a n içi n bil e saldırganı n yalnızc a şirke t bilgisaya r sistemlerind e çalışan kişiler i hedefleyeceğin i düşünmeyin . Y a haberleşm e bürosunda - ki ada m n e olacak ? "Ban a bi r iyili k yapa r mısın ? Bun u şirke t iç i kury e torbasına atabili r misin? " Haberleşm e odasınd a çalışa n memu r torbay a attığı şeyin , için e gene l müdürü n sekreter i içi n öze l olara k hazırlanmı ş küçük bi r progra m kaydedilmi ş bi r diske t olduğun u biliyo r mudu r acaba ? Artık saldırgan , gene l müdürü n e-postalarını n bi r kopyasın ı d a kendin e alabilecektir, inanılmaz ! B u gerçekte n sizi n şirketinizd e d e olabili r mi ? Neden olmasın ?

Bir Sentli k Ce p Telefon u

Pek ço k insa n bi r ma l alacaklar ı zama n dah a ucuzun u bulan a kada r araştırırlar; toplu m mühendisleri is e dah a ucuzun u aramazlar , bi r ürünün fiyatın ı dah a aşağ ı çekmeni n yolların ı ararlar . Örneği n baze n bi r şirket öyl e bi r pazarlam a kampanyas ı düzenle r k i gö z ard ı edemezsiniz . Buna karşı n toplu m mühendis i teklif i incele r v e b u alışverişte n nası l daha kazançl ı çıkabileceğin e bakar .

Bir sür e önce , ülk e çapınd a i ş yapa n bi r GS M operatör ü büyü k bi r pro - mosyon yapmıştı . Şirketi n tarifelerinde n bi r tanesin e abon e olduğunuzd a bir sen t ödeyere k yen i bi r ce p telefonun a sahi p oluyordunuz .

Birçok insanı n oldukç a ge ç farkettiğ i üzere , bi r ce p telefon u tarife - sine abon e olmada n önc e dikkatl i bi r müşterini n sormas ı gereke n bi r yığın sor u vardır . Hizmeti n analog , dijita l y a d a he r ikis i birde n olu p olmadığı; sabi t ücretleri n n e kada r olduğ u gib i sorular , işi n başından , abonelik taahhüd ü süresini n n e kada r olduğunu n bilinmes i özellikl e önemlidir. Yani , ka ç a y y a d a yı l abon e kalmanı z gerekecek ?

Philadelphia'da otura n bi r toplu m mühendisin i hayal edin . Bi r ce p telefonu şirketini n abon e olunduğund a vereceğin i söylediğ i ucu z ce p telefonunu ço k beğenmiş , anca k telefonl a birlikt e sattıklar ı tarifede n hi ç hoşlanmamış. Soru n değil . İşt e b u iş i kotarmanın yollarında n biri .

İlk Görüşme : Te d

Toplum mühendis i il k i ş olarak , bi r elektroni k eşy a mağazala r zincirinin Wes t Girard'dak i mağazasın a telefo n eder .

- Electron City. Ben Ted.

- Merhaba, Ted. Ben George. Birkaç gün önce bir cep telefonuyla ilgili olarak bir satış görevlisiyle konuşmuştum. Hangi tarifeyi iste- diğime karar verdiğimde onu arayacağımı söylemiştim ama adını unuttum. O bölümde akşam mesaisinde çalışan adamın adı nedir? - Birden fazla kişi var. JVilliam olabilir mi?

- Emin değilim. Belki.de fVilliam'dır. Görünüşü nasıl?

- Uzun boylu. Zayıfça. '"•'". - Sanırım o . Soyadı n e demiştin? •;,". . '

- Hadley. H-A-D-L-E-Y. •'•••.' . ^ ,;:': '

- Tamam, oydu. N e zaman orada olacak? ! : ı ;

- Bu haftaki mesai çizelgesini bilemiyorum ama akşamcılar beş gibi gelirler.

- Çok iyi. Onu bu gece bulmaya çalışırım o zaman. Teşekkürler, Ted.

İkinci Arama : Kati e

Bir sonrak i görüşme , ayn ı mağazala r zincirini n Nort h Broa d Caddesi'ndeki mağazasıyl a yapılır .

- Merhaba, Electron City. Ben Katie, size nasıl yardımcı olabilirim? - Katie, merhaba. Ben fVilliam Hadley, West Girard mağazasından. İşler nasıl bugün?

- Biraz yavaş. Ne oldu? . • . - Şu bir sentlik cep telefonu promosyonu için gelmiş bir müşterim

var. Hangisini kastettiğimi biliyorsun değil mi?

- Biliyorum . Geçe n hafta onlarda n birka ç tan e sattım . .'.,•••,"

- O promosyon kapsamındaki telefonlardan elinde daha var mı? - Bir yığın.

- Harika, çünkü az önce bir müşteriye ondan bir tane sattım. Adam kredi kartıyla ödedi; kontratı da imzaladık. Sonra depoya baktım ki elimizde hiç telefon kalmamış. Çok mahcup oldum. Bana bir iyilik yapabilir misin? Telefonu almak için müşteriyi sizin mağazaya gön- dereceğim. Ona bir sent karşılığında telefonu satıp, fatura düzenler misin? Bir de, nasıl programlayacağını anlatabilmem için, telefonu aldıktan sonra beni araması gerekiyor.

- Elbette. Gönder onu buraya.

- Tamam. Adı Ted. Ted Yancy.

Adının Te d Yanc y olduğun u söyleye n bi r ada m Nort h Broa d Caddes i mağazasına geldiğinde , Kati e bi r fatur a düzenle r v e adam a bi r sen t karşılığında ce p telefonun u satar . He r şe y "mesa i arkadaşının " onda n rica ettiğ i şekild e gelişir . Kadı n zokay ı yutmuştur .

Ödeme zaman ı geldiğind e müşterini n cebind e hi ç bozu k par a yoktur . Bu yüzde n kasad a bi r sentleri n durduğ u küçü k bölmey e uzanır , bi r tan e alır v e ödem e yaparke n bun u kadın a verir . Telefon u bi r sent i bil e ödemeden almıştır .

Artık ayn ı mark a telefon u kullana n başk a bi r GS M operatörün e git - mekte v e istediğ i tarifey i seçmekt e özgürdür . Tercihe n hiçbi r taahhü t gerektirmeyen ayda n ay a bi r tarif e seçecektir .

Aldatmacanın İncelenmes i •

Çalışan olduğun u ön e süre n v e şirke t iç i süreçler i v e terimler i bile n kişilere karş ı insanları n dah a yükse k bi r güve n duymas ı doğaldır . B u hikâyedefcf toplu m murterratsr , çc<3<Tt<3$Y<? <?}art3)>g)üayx)Jû)\as\ öjjrenerek , kendini bi r şirke t çalışan ı olara k tanıtmı ş ve başk a bi r şubede n bi r

kolaylık yapmasın ı ric a edere k bunda n yararlanmıştır . Böyl e şeyle r pe -

rakende zincirlerini n farkl ı mağazalar ı arasınd a v e bi r şirketi n farkl ı bi -

rimleri arasınd a olur . İnsanla r farkl ı ortamlardadırla r v e hi ç karşılaş -

madıkları mesa i arkadaşlarıyl a sürekl i berabe r çalışırlar .

Federal Ajanlard ı

insanlar, kurumlarını n interne t üzerind e neler i tuttuğun u şöyl e bi r durup düşünmezler . Lo s Angeles , KF I Tal k Radyosu'ndak i haftalı k prog - ramım içi n yapımcı , interne t üzerind e bi r taram a yapmı ş v e Ulusa l Su ç Bilgileri Merkezi'ni n ver i tabanın a erişme k içi n kullanıla n USB M kılavuzunun bi r kopyasını eld e etmişti . B u kılavuzu n içind e FBl'ı n ulusa l suç veritabanında n bilg i almay a yöneli k tü m açıklamala r bulunuyordu . Yapımcı dah a sonr a interne t üzerind e ver i

tabanını n kendisin i d e bul - muştu. ."••".-'••• •

Bu kılavuz , ulusa l ver i tabanında n su ç v e suçlular a yöneli k bilg i çekebilmek içi n kullanılaca k biçemler i v e komutlar ı içeren , emniye t teş - kilatı içi n hazırlanmı ş bi r e l kitabıdır . Ülk e çapındak i tü m emniye t birim - leri, kend i yetk i bölgeler i içerisind e suçlular ı yakalamaların a yardımc ı olması içi n ayn ı ver i tabanında n sorgulam a yapabilirler . Kılavuz , dövmelerden tutu n da , gem i omurgaların a v e çalınt ı par a v e senetleri n nominal değerlerine kadar , ver i taban ı içerisind e herhang i bi r şe y içi n kullanılan kodlar ı d a kapsıyordu .

Kılavuza erişebile n bir i ulusa l ver i tabanında n bilg i çekebilme k içi n gerekli biçemler e v e komutlar a bakabilir . Sonr a d a süreçle r kılavuzun - daki açıklamalar ı izleyerek , bira z d a cesaret i varsa , ver i tabanında n bilg i çekebilir. Kılavuzd a ayrıc a sistem i kullanırke n danışabileceğini z telefo n numaraları d a vardır . Sizi n şirketinizd e d e ürü n kodların ı y a d a hassa s bilgilere erişi m kodların ı içere n benze r e l kitaplar ı olabilir .

FBI hassa s kılavuzlarını n v e süre ç bilgilerini n internet e bağlanabile n herkese açı k olduğun u kesinlikl e hi ç far k etmedi . Eğe r durum u bilseler - di bunda n memnu n kalacakların ı d a pe k sanmıyorum . Bi r kopyas ı Oregon'daki bi r devle t daires i tarafından , bi r diğer i d e Texas'dak i bi r emniyet büros u tarafında n internet e konmuştu . Neden ? Herhald e biri - leri, b u bilgini n öneml i olmadığın ı v e on u internet e koymanı n bi r zararının olmayacağın ı düşünmüştü . Belk i d e biri , kend i çalışanlarına kolaylık olmas ı içi n on u intranet e koymuştu . Bun u yapan , ver i tabanını , internet üzerinde , Googl e gib i iy i bi r aram a motorun a erişim i olan , aralarında meraklıların , poli s olm a heveslilerinin , bilgisaya r korsan - larının v e organiz e su ç patronlarını n d a bulunduğ u bi r sür ü insan a açtığını hiçbi r zama n far k etmemiştir .

Sisteme Açılma k • • " .. . . V "

Böyle bi r bilgiy i kamud a y a d a öze l sektörd e çalışa n bi r kişiy i kandır - mada kullanmanı n kural ı aynıdır . Belirl i ver i tabanların a v e uygula - malara nası l erişileceğini , bi r şirketi n bilgisaya r sunucularını n adların ı y a da bunu n gib i şeyler i bildiğ i içi n toplu m mühendisi , inandırıcılığın ı artırır , inandırıcılık is e güve n doğurur .

Toplum mühendisini n elind e böyl e kodla r oldukta n sonr a istediğ i bil - giyi eld e etmes i kola y bi r süreçtir . Örne k verme k gerekirse , bi r yere l emniyet müdürlüğünü n telek s bürosundak i bi r memur u arayı p kılavuz - daki komutlarda n biriyl e ilgil i bi r sor u sorara k iş e başlayabilir . Örneği n işlenen suçla r koduyl a ilgil i birşe y sorabilir . "USBM'd e bi r OF F sorgula - ması yaptığımda , 'Siste m Arızalı ' mesaj ı veriyor . Si z d e OF F sorgula - ması yaptığınızd a ayn ı mesaj ı alıyo r musunuz ? Beni m içi n deneyebili r misiniz?" Bunda n başk a belk i bi r AK D -arana n kiş i dosyas ı içi n polisle r arasında kullanıla n kısaltma - aradığın ı d a söyleyebilirdi .

Telefonun diğe r ucundak i telek s memuru , arayanı n USB M verita -

banın çalışm a süreçlerin e v e aram a komutların a aşin a olduğ u mesajın ı alacaktır. USB M kullanm a konusund a eğitilmi ş bir i dışınd a başk a ki m b u süreçleri bilebili r ki ?

Memur, sistemi n düzgü n çalıştığın ı doğruladıkta n sonra , konuşm a şöyle deva m edebilir .

"Biraz yardım a ihtiyacı m var. "

"Ne arıyordun? "

"Martin Reardo n adın a bi r OF F komut u çalıştırman ı isteyeceğim . Doğum tarih i 18/10/66. "

"SOS nedir? " (AB D Emniye t teşkilat ı çalışanlar ı Sosya l Güvenli k Numarası'na baze n kısac a SO S derler.)

"700-14-7435."

Listeye baktıkta n sonra , memu r şöyl e bi r sonu ç eld e edebilir , "2602'si varmış. "

Sayının anlamın ı öğrenme k içi n saldırganı n çevri m iç i USBM'y e bakması yeterl i olacaktır : Adamı n sicilind e bi r dolandırıcılı k suç u vardır .

Aldatmacanın İncelenmes i

Başarılı bi r toplu m mühendisi , USB M ver i tabanın a girmeni n yol - larını bulmakt a hi ç zorlanmaz . İstediğ i bilgiy i alma k içi n te k yapmas ı gereken, yere l emniye t müdürlüğün e bi r telefon açıp , içerde n biriymi ş gibi ikn a edic i bi r şekild e konuşmakken , nede n tereddü t etsi n ki ? He r seferinde başk a bi r poli s bürosun u arayı p ayn ı bahaney i ön e sürebilir .

Emniyet müdürlüklerini , karakollar ı y a d a trafi k şubelerin i aramanı n riskli olu p olmadığın ı mera k edebilirsiniz . Saldırga n kendin i büyü k bi r risk altın a sokmuyo r mu ?

Cevap: hayır . V e bunu n d a bi r neden i var . Tıpk ı ord u mensupların a olduğu gibi , emniye t teşkilat ı çalışanların a da , rütbey e sayg ı kavram ı akademideki il k günlerinde n ber i yoğu n bi r şekild e benimsetilmiştir . Toplum mühendisi , bi r komiser , komise r yardımcıs ı y a d a konuştuğ u kişiden dah a yükse k rütbel i bir i gib i davranırsa ; kurban , üstlerini n söz -

lerini sorgulamamas ı gerektiğin i söyle -

yen, iy i işlenmi ş bi r dersi n etkisiyl e

Terimler

hareket edebilecektir . Diğe r bi r deyişle ,

rütbenin, özellikl e d e al t rütbelile r tara -

findan sorgulanmama k gib i yararlar ı

SOS: Sosyal güvenlik

vardır.

numarası için ABD emniyet

teşkilatında kullanılan

Ancak emniye t teşkilatını n v e

gaynresmi kısaltma.

ordunun, bi r toplu m mühendisini n rüt -

beye ola n saygıy ı sömürülebileceğ i te k ye r olduğun u düşünmeyin . B u sayfalarda geçe n birka ç öyküd e d e göreceğini z gibi , toplu m mühendis - leri, şirketler e yaptıklar ı saldırılard a d a kuru m iç i unva n v e yetk i makam - larını sı k sı k kullanırlar .

Aldatmacanın Engellenmes i ;:.; : . •• •

Toplum mühendislerinin , çalışanlarınızı n insanlar a güvenmey e

yönelik doğa l eğilimlerinde n yararlanm a olasılığın ı düşürme k için , kuru - luşunuz n e gib i önlemle r alabilir ? işt e siz e birka ç öneri .

Müşterilerizi Koruyu n •••••••••••••••• ; ••••'•• • •••••••••• •

İçinde bulunduğumu z bilg i çağınd a müşteriy e doğruda n satı ş yapa n

pek ço k şirket , kred i kart ı numaraların ı bi r dosyad a tutmaktadır . Bunu n çeşitli nedenler i vardır: Alışveri ş yapma k içi n mağazay ı y a d a interne t sitesini he r ziyare t edişinde , müşteriy i kred i kart ı bilgilerin i yenide n verme sıkıntısında n kurtarır . Anca k b u uygulamada n vazgeçilmelidir .

Eğer kred i kart ı numaralarını bi r dosyad a tutmanı z gerekiyorsa , şifreleme v e erişi m sınırlamalarını n ötesin e çıka n güvenli k koşullarını n bu işlem e eşli k etmes i şarttır . Çalışanların , kitabı n b u bölümd e anlatıla n türden toplu m mühendisliğ i oyunların ı tespi t edebilece k şekild e eği - tilmeleri d e gerekmektedir . Telefond a iy i ahbaplı k kurduğunu z am a şah - sen karşılaşmadığını z mesa i arkadaşınız , aslınd a söylediğ i kiş i olmaya - bilir. Hassa s müşter i bilgilerin e nası l erişileceğin i o kada r d a bilmes i gerekmiyor olabilir , çünk ü aslınd a şirke t içi n çalışmıyordu n

. Kim e Güveneceğiniz i Bili n ; • . ••••••••' • •

Müdahalelere karş ı uyanı k olmas ı gerekenler , yalnızc a yazılı m mühendisleri, Ar-G e çalışanlar ı v e bunu n gib i hassa s bilgiler e erişim i ola n kişiler değildir . Kuruluşunuzdak i neredeys e herkes , kurum u sanay i casus - larına v e bilg i hırsızların a karş ı korumay a yöneli k olara k eğitilmelidir .

Böyle bi r çalışmanı n başlangıcında , kuru m çapınd a bilg i varlıklar ı incelenmeli; he r bilgi , hassaslığı , ciddiyet i v e değer i açısında n değer - lendirilmeli v e bi r saldırganı n b u varlıklar ı tehdi t etme k içi n hang i toplu m mühendisliği yöntemlerin i kullanacağ ı sorgulanmalıdır . B u soruları n

fVUtnick Mesajı :

Toplum mühendisinin temel çalışma yönteminden herkes haberdar olmalıdır: Hedefle ilgili mümkün olduğu kadar çok bilgi topla ve bu bilgiyi içerden birinin güvenini kazanmak için kullan. Sonra da onun gırtlağına yapış!

anıtları gö z önün e alınarak , b u tar z bilgiler e erişi m hakk ı verilmi ş î er e yöneli k eğitimleri n tasarlanmas ı gerekmektedir .

Şahsen tanımadığını z bir i bi r bilg i y a d a belg e istediğind e y a d a bii - : sayard a bi r işle m gerçekleştirilmesin i ric a ettiğinde , çalışanları n baz ı soruları kendilerin e sormaların ı sağlayın . Eğe r b u bilgiy i e n büyü k düş - manıma verirsem , bu , ban a y a d a çalıştığı m şirket e zara r verme k içi n • .^anılabili r mi ? Bilgisayarım a girme m istene n komutları n olas ı etki - sinin tamame n bilincind e miyim ?

Karşılaştığımız he r yen i insanda n kuşkulanara k yaşantımız ı sürdü - remeyiz. Yin e de , n e kada r güve n duymay a meyill i olursak , karşımız a çıkacak bi r toplu m mühendisini n biz i şirketimiz e ai t bilgiler i vermey e kandırabilme olasılığ ı d a o kada r yükse k olur .

Intranet'© Nele r Koyulabilir ?

intranetin baz ı bölümler i dışarıy a açık , baz ı bölümler i d e çalışanlar a kapalı olabilir . Şirketiniz , hassa s bilgileri n yanlı ş kişileri n d e erişebileceğ i oir yer e konmas ı olasılığın a karş ı n e kada r dikkatli ? Herhang i bi r has - sas bilgini n dikkatsizli k nedeniyl e interne t sitenizi n herkes e açı k böl - gelerinde d e sunulu p sunulmadığı , kuruluşunuzda n bir i tarafinda n e n son n e zama n kontro l edildi ?

Eğer şirketini z elektroni k güvenli k tehditlerinde n korunma k içi n ar a güvenlik olara k prox y sunucula r kurmuşsa , b u sunucular , doğr u ayarlandık - larından emi n olma k amacıyl a yakı n zamand a kontro l edildile r mi ?

Aslına bakarsanız , şimdiy e de k intrane t güvenliğiniz i hi ç kontro l eden old u mu ?

SİZE YARDIMC I OLABİLİRİ M

Sorunla boğuştuğumu z bi r sırad a biz e yardı m etme k içi n bilgili , oecerikli v e istekl i bir i çıkageldiğind e ço k memnu n oluruz . Toplu m mühendisi bunu n farkındadı r v e bunda n nası l yararlanacağın ı d a bilir .

Size nası l soru n çıkaracağın ı d a bilir.. . sonr a sorun u çözdüğünd e ona minnetta r kalmanız ı sağlar.. . v e sonund a sizden , b u karşılaşmada n şirketinizi (belk i d e sizi) zararl ı çıkaraca k bi r bilg i y a d a küçü k bi r i ş koparmak içi n b u minnettarlığınız ı kullanır . Am a si z değerli birşe y kay - oettiğinizin hiçbi r zama n farkın a varmazsınız .

işte size , toplu m mühendislerini n "yardı m etmek " içi n ön e çıktıklar ı tipik yollarda n bazıları .

Bilgisayar Ağ ı Zayiat ı

Gün/Zaman: 1 2 Şubat , Pazartesi , öğlede n sonr a 3:2 5

Yer: Starboar d Tersan e İşletmeler i

İlk Görüşme : To m D e La v

- Tom DeLay, muhasebe.

- Selam Tom. Ben Yardım Masası 'ndan Eddie. Bir bilgisayar ağı sorununu çözmeye çalışıyoruz. Ekibinde kimsenin çevrimiçi kalmakla ilgili bir sorunu var mı?

- Bildiğim kadarıyla hayır.

~ Sen de hiçbir sorunla karşılaşmadın, öyle mi?

- Hayır, her şey yolunda görünüyor.

- Tamam, iyi o zaman. Dinle, etkilenmiş olabilecek insanları bulmaya çalışıyoruz. Eğer ağ bağlantın kesilirse bize hemen haber vermen çok önemli.

- Bu, kulağa hiç hoş gelmiyor. Sence böyle birşey olabilir mi? - Umarım olmaz; ama olursa ararsın, değil mi?

- Bundan emin olabilirsin.

- Ağ bağlantısının kopması senin için gerçek bir sorun olacakmış gibi görünüyor.

- Kesinlikle.

- .. . o zaman, hazır biz bunun üstünde çalışırken, sana cep telef omu vereyim. Böylece ihtiyacın olursa bana doğrudan ulaşabilirsin. - Bu çok iyi olur. Numaranı alayım.

- 55 5 52 1 087 1 '•••' '•••' >, . v • • • • • ' • • ••'•••"• ••"• •'•'• '•••••• ••••• • ' '

- 555 521 0871. Tamam, Teşekkürler. Adın neydi?

- Eddie. Bir şey daha; ağa hangi noktadan bağlandığını kontrol etmem gerekiyor. Bilgisayarının bir yerlerinde, üzerinde 'Bağlantı Noktası Numarası'gibi birşey yazan bir etiket olup olmadığına baka- bilir misin?

- Dur bakayım. Hayır, öyle birşey görmüyorum. , , ,

- Peki, bilgisayarın arkasındaki ağ kablosunu biliyor musun? - Evet.

- Onu bağlı olduğu yere kadar takip et. Bak bakalım fişin takılı olduğu girişte bir etiket var mı.

- Bir saniye. Evet. Bir dakika, okuyabilmek için yere çömelmem gerekecek. Tamam, şöyle yazıyor: Bağlantı Noktası 6 tire 47. - İyi. Elimdeki kayıtlarda da öyle geçiyorsun, emin olmak istemiştim.

İkinci Görüşme : Siste m Sorumlus u : ' :':: ;

İki gü n sonr a ayn ı şirketi n A ğ Hizmetler i Merkezi'n e bi r telefo n gelir . - Merhaba, ben Bob. Muhasebeden Tom DeLay'in ofisimdeyim. Bir

kablo sorununu çözmeye çalışıyoruz. 6-47 numaralı bağlantıyı devre dışı bırakmanızı isteyecektim.

Sistem sorumlus u birka ç dakik a içind e yapabileceği m söyled i v e işler i bittiğinde bağlantını n tekra r açılmas ı içi n on a habe r vermeler i gerek - tiğini hatırlattı .

Üçüncü Görüşme : Düşmanda n Yardı m Alm a

Bir saa t kada r sonr a adını n Eddi e Marti n olduğun u söyleye n adamı n dışarda gezinirke n telefon u çaldı . Eddi e aramanı n tersanecili k işletmesinden geldiğin i görünc e telefonun u açmada n önc e hızl a sessi z bir ye r buldu .

- Yardım Masası , Eddie . • : ... . . : , .,:• . •,, . . - Selam Eddie. Senin tarafında bir yankı var, neredesin?

- Bir kablo dolabının içindeyim. Kim.arıyordu?

- Ben Tom DeLay. Seni bulabildiğime çok sevindim. Hatırlarsan geçen gün beni aramıştın. Söylediğin gibi ağ bağlantım az önce kesil- di. Ne yapacağım şimdi?

- Evet, ekip olarak şu anda bunun üstünde çalışıyoruz. Akşama kadar bitirmiş oluruz. B u uygun mu? . , , ,

. Siz e Yardımc ı Olabiliri m 5 3

- HAYIR! Olmaz! Bu kadar uzun süre bağlantısız kalırsam isimde

geri kahrım. En erken ne zaman halledebilirsin bu işi?

t- - Çok m u sıkışık durumdasın?

- Şu anda başka birkaç şeyle de ilgilenebilirim. Yarım saat içinde

bunu halletmeniz mümkün olur mu?

- YARIM SAAT Mİ? Çok da birşey istemiyorsun. Peki, elimdeki işi

bırakıp, senin sorununu çözmeye çalışacağım.

- Çok müteşekkir kalırım, Eddie.

Dördüncü Arama : Yakaladı m Seni !

Kırk be ş dakik a sonr a .. .

- Tom? Ben Eddie. Ağ bağlantım bir deneyebilir misin?

Biraz sonra :

- Oh, çok iyi; çalışıyor. Harika.

- İyi, sorununu çözebildiğime sevindim.

- Evet, çok teşekkürler. .

- Dinle, bağlantının yeniden kopmasını istemiyorsan çalıştırman gereken bir program var. Yalnızca birkaç dakika sürer.

- Şu an çok iyi bir zaman değil.

- Anlıyorum ama bu ağ sorunu yine ortaya çıkarsa ikimizi de büyük dertlerden kurtarır.

- Peki... birkaç dakika sürecekse.

- Yapman gereken şu...

Eddie, Tom' u bi r we b sitesinde n küçü k bi r progra m indirmes i içi n adı m adım yönlendirdi . Progra m indirildikte n sonra , Tom' a programı n üzerinde çif t tıklamasın ı söyledi . To m dened i ama :

- Çalışmıyor. Hiçbir şey yapmıyor, diy e karşılı k verdi .

- Of, çok kötü. Programla ilgili bir sorun olmalı. Silelim onu, başka bir zaman tekrar deneriz. Sonr a Tom' a program ı he m indirdiğ i yerde n hem d e çö p kutusunda n sildirdi .

Toplam geçe n zaman : o n ik i dakika . - -

Saldırganın öyküs ü

Bobby VVallace , bunu n gib i iy i bi r i ş aldıkta n sonra , bilgini n nede n istendiğiyle ilgil i açı k bi r soruy a müşterini n kaçama k yanıtla r vermesini n her zama n gülün ç olduğun u düşünmüştü . B u işt e d e aklın a yalnızc a ik i neden geliyordu . Müşteri , hede f şirke t olan , Starboar d Tersan e İşlet - melerini satı n almay ı düşüne n başk a bi r şirket i temsi l ediyo r v e şirketi n mali durumunu n gerçe k yüzün ü öğrenme k istiyo r olabilirdi . Özellikl e de , hedef şirketi n olas ı bi r alıcıda n saklama k isteyebileceğ i bilgileri . Y a d a

Terimler

belki par a yönetimind e karanlı k işleri n

döndüğünü düşüne n v e baz ı üs t düze y

yöneticilerin yolsuzlu k yapı p yapmadık - TRUVA ATI: Kurbanın bil-

larını öğrenme k isteye n şirke t ortakla n

gisayarından ve içinde

da olabilirlerdi .

bulunduğu ağdan bilgi

toplamak ya da kurbanın Belki d e müşteris i on a gerçe k neden i

T^Bff bilgisayarına ve dosyaları- söylemek istememişti , çünk ü bilgini n n e

na zarar verebilmek için kadar değerli olduğun u bilirs e Bobb y iş i tasarlanmış, kötü huylu ya
yapmak içi n dah a ço k par a isteyebilirdi . da zararlı kod içeren prog-

ramdır. Bazı Truva Atlan

Bir şirketi n e n gizl i dosyaların ı el e bilgisayarın işletim sistemi-

geçirmenin pe k ço k yol u vardır . Bobb y

nin içinde saklanıp her

birkaç gü n seçenekleri n üzerind e

işlemin ya da her tuşa

düşünmüştü v e bi r pla n üstünd e kara r

basışın kaydını tutacak

kılmadan önc e küçü k d e bi r araştırm a veya belirli işlevleri gerçek-

yapmıştı. Sonund a özellikl e sevdiğ i bi r

leştirebilmek için ağ

yöntemi, kurbanı n saldırganda n yardı m bağlantısı üzerinden talimat

istemek üzer e tuzağ a düşürüldüğ ü alabilecek şekilde tasarlan-

oyunu oynamay ı seçmişti .

mışlardır ve bunların hepsi-

Başlangıç olara k bi r mağazada n 3 9

ni, kendi varlıklarını kur-

dolar 9 5 sent e bi r ce p telefon u almıştı . bana sezdirmeden yaparlar.

Hedef olara k belirlediğ i adam ı aramı ş v e

kendini şirke t yardı m masasında n bir i

gibi tanıtarak , ağd a bi r soru n çıktığ ı anda Bobby' i ce p telefonunda n aramas ı doğrultusund a adam ı ayarlamıştı.

Kendini açı k etmeme k içi n aray a ik i gü n koymuşt u v e sonr a d a şir - ketin A ğ Hizmetler i Merkezi'n e (AHM) telefon etmişti . Tom'un , yan i hedefinin, bi r sorunun u çözmey e çalıştığın ı söyleyere k Tom'u n a ğ bağlantısının devr e dış ı bırakılmasın ı istemişti . Bobb y çektiğ i numaranın b u aşamasını n e n aşılmas ı zo r bölü m olduğun u biliyordu ; pek ço k şirkett e yardı m masas ı çalışanlar ı AHM'yl e yakı n tema s içind e çalışırlar; hattâ , yardı m masas ı çoğ u zama n bilg i işle m birimini n bi r parçasıdır. Anca k konuştuğ u vurdu m duyma z AH M görevlisi , olay ı sıradan bi r işle m yerin e koyu p bilgisaya r ağ ı sorunun u çözmekl e uğraşan v e yardı m masasınd a çalıştığın ı söyleye n kişiy e adın ı sor - madan hedefi n bağlant ı noktasın ı devr e dış ı bırakmay ı kabu l etmişti . İ ş tamamlandığında To m şirketi n intranetinde n bütünüyl e yalıtılmıştı . Sunucudaki dosyalar a erişmes i olanaksı z hal e gelmişti . Mesa i arkadaşlarıyla dosy a alı p verememekte , e-postaların ı okuyamamakta , hattâ yazıcıy a bi r çıkt ı bil e gönderememekteydi . B u durum , günümü z dünyasında mağarad a yaşama k gib i bi r şeydi .

Bobby'nin d e tahmi n ettiğ i üzer e ce p telefonunu n çalmas ı uzu n sürmemişti. Doğa l olara k sıkıntıl ı bi r durumd a ola n b u zavall ı "mesa i

i nadasına " yardımc ı olma k konusund a hevesl i görünü p sonr a AHM'y i F »ayara k adamı n a ğ bağlantısın ı yenide n açtırmıştı . Kurban ı tekra r ara - yarak on u bi r ke z dah a kandırmıştı . B u kez , Bobb y on a yardı m ettikte n r sonr a "hayır " dediğ i içi n Tom'u n kendin i suçl u hissetmesin i sağlamıştı . Bunun üzerin e Tom , bilgisayarın a bi r yazılı m indirm e önerisin i kabu l etmişti.

Doğal olarak , yapmay ı kabu l ettiğ i şe y ta m olara k göründüğ ü şe y değildi. Tom'u n a ğ bağlantısın ı çökmekte n koruyacağ ı söylene n yazılı m aslında bi r Truv a Atı'ydı . Bobby , Yunanları n Truvalılar a yaptığın ı Tom'u n bilgisayarına yapmıştı ; yan i düşman ı kaleni n için e sokmuştu . To m yazılı m simgesine çif t tıkladığınd a hiçbi r şe y olmadığın ı söylemişti . Zate n küçü k program, tasarım ı gereği , bilgisayar a erişim e izi n verece k gizl i bi r yazılı m yüklerken bil e herhang i birşe y olduğun u göstermezdi .

Program, Bobby'ni n uzakta n erişiml e Tom'u n bilgisayar ı üzerind e :am bi r hakimiye t kurmasın ı sağlamıştı . Bobb y Tom'u n bilgisayarın a girdiğinde on u ilgilendirebilece k muhasab e kayıtların ı arayabili r v e onları kendin e kopyalayabilirdi . Sonr a can ı istediğ i zama n müşterilerini n aradığı bilgiy i bulabilme k içi n dosyalar a bakabilirdi .

Her şe y bununl a d a bitmiyordu. He r zama n ger i dönüp , ilgin ç bilgile r sunabilecek anahta r sözcükler i kullanara k bi r meti n aramas ı yapıp , şir - ket yöneticilerini n elektroni k mesajların ı v e öze l notların ı tarayabilirdi .

Hedefini Truv a At ı yazılımın ı yüklemes i içi n kandırdığ ı günü n akşam ı Bobby ce p telefonun u bi r çö p bidonun a attı . Elbette , atmada n önc e hafızasını temizled i v e bataryasın ı çıkardı , isteyebileceğ i e n so n şe y birinin ce p telefonun u yanlışlıkl a aramas ı v e telefonu n çalmay a başla - masıydı!

Aldatmacanın incelenmes i . ••••- •

Saldırgan, hedefini , aslınd a va r olmaya n bi r sorun u olduğun a inandırarak kend i ağın a düşürür . Sorun , b u olayd a olduğ u gibi , henü z gerçekleşmemiş am a saldırganı n gerçekleşeceğin i bildiğ i çünk ü ken - disinin nede n olacağ ı bi r soru n d a olabilir . Sonr a d a kendisin i sorun u çözebilecek kiş i olara k tanıtır .

Bu tar z saldırıd a kullanıla n düzen , saldırganı n özellikl e işin e gelir , çünkü öncede n ekile n tohu m sayesind e hedef , bi r sorun u olduğun u

Mitnick Mesajı : x —

Eğer tanımadığınız biri size bir iyilik yapıyorsa ve sonra da karşılığında siz- den bir iyilik bekliyorsa, istenen şeyin ne olduğu üzerinde dikkatle düşünmeden karşılık vermeyin.

Terîmîer

UZAKTAN ERİŞİMLİ KOMUT KABUĞU: Belirli işlevleri gerçekleştirmek ya da programları çalıştırmak için metin tabanlı komutlar kabul eden grafik içerikli olmayan bir arayüzdür. Teknik açıkları sömürebilen ya da kurbanının bilgisa-

yarına bir Truva Atı yükleyebilen bir saldırgan bir komut kabuğuna uzak- tan erişim sağlayabilir.

anladığında yardı m isteme k içi n kend i ayağıyla gelir . Saldırga n yalnızc a oturu p telefonun çalmasın ı bekler . B u yönteme , meslekte büyü k bi r sevecenlikl e ters toplum mühendisliği denmiştir . Hedefi n kendisini aramasın ı sağlaya n saldırgan , anında inanılırlı k kazanır . Yan i eğe r be n yardım masasınd a çalıştığın ı düşün - düğüm birin i ararsa m onda n kimliğin i kanıtlamasını istemem . İşt e o zama n saldırgan başarmı ş demektir .

TERS TOPLUM

MÜHENDİSLİĞİ:

Kurbanın bir sorunla karşılaştığı ve yardım için saldırganı aradığı şeklinde gelişen toplum mühendisliği

saldırısı.

Ters toplum mühendis- liğinin başka bir türü de

saldırganın aleyhinde olanıdır. Hedef, bir saldırı yapıldığını anlar ve işlet- menin varlıklarım güvenc- eye alabilmek için psikolo- jik etkileme unsurları kulla-

narak saldırgandan mümkün olduğu kadar çok

bilgi almaya çalışır.

Böyle bi r dola p çevirirke n toplu m mühendisi bilgisayarlarl a ilgil i sınırl ı bil - giye sahi p ola n bi r hede f seçmey e çalışır. Hede f n e kada r ço k bilirs e şüphelenme olasılığ ı o kada r çoktur ; y a da onunl a oyu n oynandığın ı heme n anlayabilir. Zaman zama n bilgisayarl a savaşan çalışanla r olara k sö z ettiğim , teknoloji v e süreçleriyl e ilgil i konulard a az bilgil i ola n kişile r he r söylenen e inan - maya dah a eğilimlidirler . Bi r yazılımı n verebileceği zararl a ilgil i olara k hiçbi r fikirleri olmadığ ı içi n "ş u küçü k program ı yükleyiver," gib i bi r hiley i yutm a olasılık - ları d a yüksektir . Dahası , bilgisaya r ağ ı üzerinden tehlikey e soktuklar ı bilgini n değeri konusund a fiki r sahib i olm a olasılıkları d a azdır .

'İ-Z-Î-Â Başlaya n Kız a Küçük Bi r Yardı m

Yeni iş e başlayanlar , saldırganla r içi n e n iy i hedeflerdir . Henü z ço k insan tanımazlar , şirketi n süreçlerini , yapılmas ı v e yapılmamas ı gereken şeyler i bilmezler . V e iy i bi r izleni m bırakma k adın a n e kada r yardımsever v e hızl ı oldukların ı gösterme k içi n d e heveslidirler .

Yardımscwer Andre o " " - • i-•.,. ' •;•,,..: ••.•/•\.-:. > :

- İnsan Kaynakları, Andre a Calhoun .

- Andrea, merhaba, be n Alex ; Şirket Güvenliği'nde n . " ••••':' :

•• - Evet ? ' , :.•"•'••:'•:' • ' •'"• ' ' :

• • ' '

Size Yardımc ı Olabiliri m 5 7

- Bugün işler nasıl?

- İyi. Sizin için ne yapabilirim?

- Yeni başlayanlar için bir güvenlik semineri düzenliyoruz ve deneme için birkaç kişiyi biraraya getirmemiz gerekiyor. Geçen ay işe başlayan herkesin adlarına ve telefon numaralarına ihtiyacım var. Bana bu konuda yardımcı olabilir misin?

- Ancak öğleden sonra çıkarmam mümkün olabilir. Bu uygun mu? Dahili numaran nedir?

- Elbette olur, dahilim 52... aah, günün çoğunda toplantıda olacağım. Ofise döndükten sonra seni ararım, bu herhalde dörtten sonra olur. Alex 16:30'd a aradığınd a Andre a listey i hazırlamışt ı v e adlar ı v e dahil i numaralan ors a okudu .

Rosemary'e Bî r Mesa j

Rosemary Morga n yen i işinde n ço k memnundu . Dah a önc e hiçbi r derg i

için çalışmamışt ı v e insanlar ı beklediğinde n dah a arkada ş canlıs ı bul -

muştu. He r a y sonund a bitmes i gereke n bi r başk a sayıy ı çıkarabilme k

için çalışanları n çoğunu n bitme k bilmeye n bi r bask ı altınd a olduklar ı

düşünülünce b u şaşırtıc ı bi r durumdu . Bi r Perşemb e sabah ı aldığ ı tele -

fon b u dostç a izlenim i pekiştird i

- Rosemary Morgan'la mı görüşüyorum?

- Evet.

- Merhaba Rosemary. Ben Bili Jorday; Bilgi Güvenliği Grubu 'ndan.

- Evet?

- Bizim birimden kimse sizinle güvenlik uygulamaları hakkında

görüştü mü? .

- Sanmıyorum.

- Peki. Bakalım. Öncelikle kimsenin şirket dışından getirdiği prog- ! ramları yüklemesine izin vermiyoruz. Bunun nedeni lisanslı olmayan

yazılım kullanımından sorumlu olmak istememiz ve solucan ya da

virüs içeren yazılımların çıkarabileceği sorunlardan uzak durmak.

- Tamam.

- E-posta uygulamamızdan haberdar mısınız?

- Hayır. ,

- Şu anda kullandığınız e-posta adresi nedir? ....'••

- Rosemary@ttrzine.net. •

- Kullanıcı adı olarak Rosemary'i mi kullanıyorsunuz?

- Hayır, R altçizgi Morgan'ı kullanıyorum.

- Tamam. Tüm yeni çalışanlarımızı beklemedikleri e-posta eklerini açmalarının oluşturacağı tehlikelere karşı uyarmak istiyoruz. Pek çok solucan ve virüsler ortalıkta geziniyor ve tanıdığınız insanlardan

geliyor gibi görünen e-posta eklerinde geliyorlar. Bu yüzden bek- lemediğiniz bir ekli e-posta alırsanız, gönderici olarak görünen kişinin mesajı size gerçekten gönderip göndermediğini her zaman kontrol edip emin olmalısınız. Anlıyor musunuz?

- Evet. Bunu duymuştum.

- İyi. Uygulama her doksan günde bir parolanızı değiştirmeniz şek- linde. Parolanızı en son ne zaman değiştirdiniz?

- Yalnızca üç haftadır burada çalışıyorum, ve daha ilk aldığım şifreyi kullanıyorum.

- Tamam, bu iyi. Do/csan gün dolana kadar bekleyebilirsin. Ama insanların, tahmin edilmesi kolay olmayan şifreler kullandığından da emin olmak istiyoruz. Hem sayı hem de harf içeren bir şifre mi kul- lanıyorsunuz?

- Hayır. ...••• '

- Bunu düzeltmeliyiz. Şu anda kullandığınız şifre nedir?

- Kızımın adı, Annette.

- Bu çok güvenli bir şifre değil. Hiçbir zaman aile bilgilerinize

dayanan şifreler seçmemelisiniz. Peki... benim yaptığımın aynısını

yapabilirsiniz. Şifrenizin bir parçası olarak şu anda kullandığınızı

kullanmanın bir sakıncası yok ama her değiştirdiğinizde içinde bulun-

duğunuz ayın sayısını ekleyin.

- Bunu şimdi yaparsam, yani Mart için, üç mü kullanmalıyım, sıfir-üç

mü?

- Nasıl isterseniz. Hangisi sizin için daha rahat olur?

- Sanırım Annette-üç.

- İyi. Değişikliğin nasıl yapılacağı konusunda size yardımcı olmamı

ister misiniz?

- Hayır, nasıl yapılacağını biliyorum.

- Güzel. Söylemem gereken birşey daha var. Bilgisayarınızda bir

virüs koruma yazılımı var ve onu güncel tutmanız önemli. Arada bir

bilgisayarınız yavaşladığında bile otomatik güncellemeyi devre dışı

bırakmamalısınız. Tamam mı?

- Elbette.

- Çok iyi. Bilgisayarla ilgili bir sorununuz olduğunda aramanız için

buranın telefon numarası sizde var mı?

Yoktu. Adam ona numarayı verdi, kadın özenle notaldıvebirkezdahaona nekadariyi baktıklarını düşünerekişine geri döndü.

Aldatmacanın İncelenmesi

Bu öykü, elinizdeki kitabın temelinde yatan anafikri güçlendiriyor. Asıl amacında n bağımsız olarak bir toplum mühendisinin bir çalışanda n isteyeceği en temel bilgiler, hedefin tanımlama verileridir. Şirketin doğru

Mitnick Mesajı :

: - ; işe başlayanların, şirket bilgisayar sistemlerine girişlerine izin verilmeden _.;.e, özellikle şifrelerini başkalarına kesinlikle söylememekle ilgili olan güvenlik uygulamaları konusunda eğitilmeleri gerekir.

roümünden te k bi r çalışan a ai t kullanıc ı ad ı v e şifr e vars a saldırganı n çeri girebilme k içi n v e peşind e olduğ u herhang i bi r bilgiy e ulaşma k içi n htiyacı ola n he r şey i vardır . B u bilgiy i edinmek , krallığı n anahtarın ı bul - -ıak gibidir . Onla r elindeyke n şirke t bünyesind e özgürc e dolaşabili r v e 3 radığı hazineyi bulabilir .

sunduğunuz

"Hassas bilgilerin i korumak içi n çab a göstermeye n bi r şirke t düpedü z ihmalcidir." Pe k ço k insa n b u görüş e katılacaktır . Gerçe k ş u k i gizl i bil - gilerini korumay a yöneli k çab a göstere n şirketle r bil e cidd i bi r tehlike altında olabilirler .

İşte siz e şirketlerin , deneyiml i v e başarıl ı profesyonelle r tarafında n tasarlanmış güvenli k uygulamalarının aşılamayacağın ı düşünere k he r gün kend i kendilerin i nası l kandırdıklarını göstere n bi r öyk ü daha . Steve Cramer'i n öyküs ü

Steve'in pahal ı tohumlarl a çimlendirilmi ş v e herkesi n gıptayl a baktığ ı bir bahçes i yoktu . Çimler i biçme k içi n büyü k bi r makin e d a gerekmi - yordu. Zate n böyl e bi r makin e ols a bil e kullanmazdı . Çünk ü b u küçü k çim biçm e makinesiyl e işini n dah a uzu n sürmes i sayesind e Anna'nı n çalıştığı bankadak i insanlarl a ilgil i hikâyele r anlatmasında n y a d a on a yaptıkları işler i açıklamasında n kurtulu p kend i düşüncelerin e odakla - nabiliyordu. Haft a sonlarını n ayrılma z bi r parças ı halin e gele n 'sevgilim şun u d a yapa r mısın? ' listelerinde n nefre t ediyordu . Bazıları Steve'i n GeminiMe d Tıbb î Cihazla r Şirket i içi n yen i cihazla r tasarlama işini n sıkıc ı olduğun u düşünebilirdi . Anca k Stev e haya t kur - tardığını biliyordu . İşini n yaratıc ı olduğun u düşünüyordu . Sanatçılar , besteciler, mühendisle r d e Steve'i n yaptığın a benze r işle r yapıyorla r v e daha önc e kimseni n yapmadığ ı bi r şeyle r yaratıyorlardı . So n yaptığ ı v e oldukça zekic e tasarlanmı ş yen i bi r çeşi t kal p stent i ş u an a de k e n guru r duyduğu eseriydi .

O cumartesi , saa t neredeys e 11:3 0 olmuştu . Stev e çi m biçm e işin i dah a bitiremediği v e kal p stentini n tamamlanmasınd a so n enge l ola n gü ç gereksiniminin düşürülmes i sorunun a cidd i bi r çözü m bulamadığ ı içi n huzursuzdu. Çi m biçerke n üzerind e düşünme k içi n harik a bi r konuyd u ama hiçbi r çözü m üretememişti . . . . .

Anna kapıd a belirdi ; saçm ı he r zama n to z alırke n takdığ ı kırmız ı desen - li kovbo y eşarbıyl a Örtmüştü . "Telefon" diy e bağırdı , "işten arıyorlar. " "Kim?" diy e ger i bağırd ı Steve .

"Ralph diye biri sanırım."

"Ralph mı?" Stev e GeminiMed'd e çalışa n v e on u haft a son u arayabile - cek Ralp h isiml i birin i tanımıyordu . Ann a ad ı yanlı ş anlamı ş olmalıy - dı. Stev e bunlar ı düşünere k telefon a gitt i

"Steve, ben Teknik Destek'ten Ramon Perez." Steve , Anna'nı n Ramo n gibi bi r İspanyo l adın ı Ralph' a nası l çevirdiğin i mera k etti .

"Bu nezaket icabı yapılan bir arama" diyord u Ramon . "Sunuculardan üçü çöktü. Bir solucandan şüpheleniyoruz ve diskleri temizleyip yedek- leri yükleyeceğiz. Çarşamba ya da Perşembe'ye kadar dosyalarınızı yükleyip çalıştırılabilir duruma getiririz. Yani her şey yolunda giderse." "Bu kesinlikle mümkün değil" ded i Stev e ser t bi r şekild e v e sıkıntısın ı belli etmey e çalışarak . B u insanla r nası l b u kada r apta l olabiliyorlardı ? Tüm haftason u v e gelece k haftanı n çoğund a dosyaların a erişemede n i ş yapamayacağı akılların a gelmiyo r muydu ? "Olmaz. İki saate kadar evdeki bilgisayarımın başına oturacağım ve dosyalanma erişmem gerekecek. Bilmem anlatabiliyor muyum?"

"Evet, tabi, şimdiye kadar aradığım herkes listenin başında olmak istiyor. Buraya gelip bunun üstünde çalışmak için hafta sonumu harcı- yorum ve konuştuğum herkesin bana püskürmesi hiç hoş olmuyor. " "Teslim tarihim yaklaşıyor ve şirket çıkacak ürüne çok güveniyor. Benim bu işi bu öğleden sonra bitirmem lâzım. Bunu kafana sok. " "Başlamadan önce aramam gereken daha bir sürü insan var." ded i Ramon. "Dosyalarınızı salıya kadar hazır etsek nasıl olur?" "Salı değil, çarşamba değil. ŞİMDİ!" ded i Steve . B u kalı n kafal ı ada m durumun önemin i anlayamazs a mutlak a başk a birin i aramas ı gerekecekti.

"Tamam, tamam" ded i Ramo n v e Stev e onu n asab i bi r şekild e i ç geçirdiğini duydu . "Senin işini görebilmek için neler yapmam gerek- tiğine bir bakayım. RM22 sunucusunu kullanıyorsun, değil ini?" "RM22 ve GM16. Her ikisini de."

"Peki. Tamam, bazı işleri kısa yoldan yapıp zaman kazanabilirim. Kullanıcı adına ve parolana ihtiyacım olacak." -:'.'••.., Eyvah, diy e düşünd ü Steve . N e deme k oluyo r bu ? Beni m parolam a leden ihtiya ç duysu n ki ? Herke s bi r taraf a siste m sorumlular ı nede n sorsun k i bunu ? , ; : ; , , "Soyadın ne demiştin? Ve müdürün kim?"

"Ramon Perez. Bak sana ne diyeceğim, ilk işe başladığında kullanıcı idi alırken doldurduğun bir form vardı ve oraya parolanı da yazmıştın.

O parolayı bulup dosyaların burada olduğunu sana gösterebilirim. Olur mu?"

Steve bunu n üzerind e birka ç saniy e düşünd ü sonr a d a kabu l etti . Ramon dosy a dolabında n formlar ı almay a giderken , o arta n bi r sabırsız - lıkla telefonu n öbü r ucund a bekledi . Stev e Ramon'u n bi r kağı t yığının ı karıştırdığını duyuyordu .

"İşte burada" ded i Ramo n sonunda . "Janice diye bir şifre koymuşsun." "Janice", diy e düşünd ü Steve . Annesini n adıyd ı v e gerçekte n d e on u bazen şifr e olara k kullanırdı . İş e girm e belgelerin i doldururke n b u şifreyi pekal a koymu ş olabilirdi .

"Evet, b u doğru" diyere k onayladı .

"Tamam, zaman kaybediyoruz. Gerçek olduğumu biliyorsun. Kısa yolu kullanıp en çabuk şekilde dosyalarını kurtarmamı istiyorsan bana yardım etmen gerekecek."

"Kullanıcı adım s, d, altçizgi, cramer C-R-A-M-E-R. Şifre: pelikanl." "Hemen işe koyulacağım" ded i Ramon ; sonund a ses i yardımc ı olabile - cekmiş gib i geliyordu . "Bana birkaç saat ver."

Steve çi m biçm e işin i bitirdi , öğl e yemeğin i yed i v e bilgisayarını n başı - na geçtiğind e dosyalarını n ger i yüklenmi ş oldukların ı gördü . O huysu z sistem sorumlusun u bağırara k yol a getirdiğ i içi n kendiyl e guru r duyd u ve Anna'nır i d a n e kada r ser t konuştuğun u duymu ş olmasın ı diledi . Adama y a d a patronun a teşekkü r etme k iy i olurd u am a böyl e şeyler i yapacak bir i olmadığını n d a farkındaydı .

Craig Cogburne'ü n Öyküs ü ' " :

Craig Cogburn e yükse k teknoloj i ürünler i ürete n bi r şirkett e pazarla - macı olara k çalışıyord u v e işind e d e oldukç a iyiydi . Bi r sür e sonr a müş - teriyi okuma k konusund a bi r beceris i olduğun u far k etti . Kişini n hang i konularda dirençl i olduğunu , satış ı kapatmay ı kolaylaştıraca k baz ı zayıflıklarını v e açıkların ı görebiliyordu . Yeteneğin i kullanmanı n başk a yollarını bulmay a çalışt ı v e izlediğ i yo l on u sonu ç olara k dah a kazançl ı bir alan a götürdü : sanay i casusluğu . Kend i ağzında n dinleyelim : Bu seferk i ço k sık ı bi r işti . Ço k fazl a zamanımı almad ı v e Hawaii'y e hattâ belk i Tahiti'y e bi r gez i yapaca k kada r d a ço k kazan ç sağladım . Beni tuta n adam , doğa l olara k ban a müşterini n ki m olduğun u söyleme - di; am a atılaca k hızlı , büyü k v e kola y bi r adıml a rekabet i yakalama k isteyen bi r şirke t olduğun u anladım . Tü m yapma m gereke n kal p stent i denen yen i bi r zamazingoy a ai t ürü n özelliklerin i v e tasarımların ı el e geçirmekti. Bunu n n e olduğ u konusund a hiçbi r fikri m yoktu . Şirketi n adı GeminiMed'di . B u ad ı hi ç duymamıştı m am a yarı m düzin e yerd e ofisleri ola n Fortun e 50 0 şirketlerinde n biriydi ; b u d a iş i küçü k bi r şir - kete gör e dah a kolay , kılıyord u çünk ü küçü k şirkett e konuştuğu n

kişinin olduğun u iddi a ettiği n v e aslınd a olmadığı n adam ı tanım a şans ı oldukça yükse k oluyordu .

Müşterim ban a bi r fak s yolladı . Gönderile n bi r dokto r dergisinde n alın - mıştı v e GeminiMed'i n farkl ı v e yen i bi r tasarım ı ola n bi r sten t üzerinde çalıştığını , adm m d a STH-10 0 olduğun u yazıyordu . Doğruy u söylemek gerekirs e bi r gazetec i beni m içi n büyü k bi r aya k işin i hallet - mişti. İş e koyulmada n önc e ihtiyacı m ola n te k bi r şe y vard ı v e o d a yen i ürünün adıydı .

Birinci sorun : Şirkett e STH-10 0 üzerind e çalışa n kişileri n y a d a tasarımlan görm e yetkisin e sahi p insanları n adların ı öğren . Santral ı aradım ve , "Mühendislik ekibinizden biriyle bağlantı kuracağıma söz vermiştim ve soyadını hatırlamıyorum, ama adı S'yle başlıyordu," dedim. V e santraldak i kı z ded i ki , "Scott Archer v e Sam Davidson adın- da birileri var." Hangis i STH-10 0 ekibind e çaitşıyo r bilmiyordu ; b u yüzden rastgele _ Scot t Archer' i seçtim , kı z benLon a bağladı .

Adam telefon u açtığında , "Merhaba, ben Mike, posta odasından. Elimizde STH-100 Kalp Stenti proje ekibine gelmiş bir kargo paketi var. Bunun kime gideceği konusunda bir fikriniz var mı? " diy e sordum . Bana eki p liderini n adın ı verdi , Jerr y Mendel . Beni m içi n Mendel'i n numarasını bulmasın ı bil e sağladım .

Aradım. Mende l yerind e yokt u am a telesekreterindek i mesa j ayı n o n üçüne kada r tatild e olacağın ı söylüyordu . Bu , kayağ a mı , he r ney e git - tiyse bi r haft a dah a yerind e olmayacağ ı anlamın a geliyord u v e b u sür e zarfindan birilerini n birşey e ihtiyac ı olurs a 9137'de n Michelle' i ara - maları gerektiğin i söylüyordu . B u insanla r ço k yardımseve r oluyor - lardı. He m d e çok .

Telefonu kapattı m v e Michelle' i aradım . Telefon u açtığınd a on a dedi m ki, "Ben Bili Thomas. Jerry bana şartnameyi bitirdiğimde ekibindeki- lerin inceleyebilmesi için sizi aramam gerektiğini söylemişti. Kalp stenti üzerinde çalışıyorsunuz, öyle değil mi?" Kadı n öyl e olduğun u söyledi.

Şimdi oyunu n e n zorl u kısmın a gelmiştik . Eğe r kadı n kuşkulanı r gib i olursa, Jerry'ni n bende n yapmam ı ric a ettiğ i bi r iyiliğ i yerin e getirmey e çalıştığımla ilgil i kozum u oynamay a hazırdım . "Hangi sisteme bağlısınız?" diy e sordum .

"Sistem?"

"Ekibiniz hangi bilgisayar sunucularını kullanıyor?"

"Oh," ded i kadın , "RM22. Ekibin bazıları d a GMlö'yı kullanıyorlar." Buna ihtiyacı m vard ı v e b u on u kuşkulandırmada n alabileceği m bi r bil - giydi. Elimde n geldiğ i ölçüd e olağa n bi r tavı r takınmı ş v e bi r sonrak i adım içi n on u bira z yumuşamıştım . "Jerry bana geliştirme ekibinde çalışanların e-posta adreslerini verebileceğinizi söylemişti" dedi m v e nefesimi tuttum .

"Elbette. Evrak dağıtım listesi, okumak için çok uzun; size onu e-posta'yla gönderebilir miyim?"

Eyvah. Son u GeminiMed.com'l a bitmeye n herhang i bi r e-post a adres i işleri yokuş a sürerdi . "Bana listeyi falcslasanız nasıl olur? " dedim . Bunu yapabileceğin i söyledi .

"Faks makinemizin ışığı yanıp sönüyor. Başka bir tanesinin numarasını almam gerekecek. Sizi biraz sonra ararım." dedi m v e telefon u kapattım . Bu noktad a tatsı z bi r durumd a kaldığım ı düşünebilirsini z am a b u d a işin bi r parçası . Danışmad a otura n kadın a sesi m tanıdı k gelmesi n diy e bir sür e bekledi m sonr a d a on u arayıp , "Merhaba, ben Bili Thomas, buradaki faks makinemiz çalışmıyor, sizin makinenize benim için bir faks gönderebilirler mi?" dedim . Mümkü n olduğun u söyled i v e ban a numarayı verdi .

Sonra d a oray a gidi p faks ı alacaktım , öyl e mi ? Tab i k i hayır ! Birinc i kural: Ço k gerekmedikç e mekân a asl a girme . Yalnızc a telefondak i bi r ses olara k kalırsa n seni n kimliğin i belirlemeler i ço k dah a gü ç olur . V e eğer seni n kimliğin i belirleyemezlerse , sen i tutuklayamazlar . Bi r ses e kelepçe takma k kola y değildir . B u yüzde n bi r sür e sonr a danışmay ı yeniden aradı m v e kız a faksımı n geli p gelmediğin i sordum . "Evet," diye yanıtladı .

"Peki" dedi m ona , "Onu birlikte çalıştığımız bir danışmana vermem gerekiyor. Benim için gönderebilir misin?" Soru n olmayacağın ı söyle - di. He m nede n soru n olsund u ki ; danışmad a çalışa n birini n neyi n has - sas bilg i olduğun u bilmes i beklenemezdi . Danışm a görevlis i "danış - mana" faks ı gönderirken , be n d e vitrinind e "Fak s Gönderilir/A l mır " yazan yakınlardak i bi r kırtasiyey e doğr u yürüyere k günlü k sporum u yaptım. Faksı n bende n önc e oray a gelmi ş olmas ı gerekiyord u v e bek - lediğim gib i içer i girdiğimd e ben i bekliyordu . Alt ı sayfay a 1.7 5 dola r verdim. Bi r dolarlı k bi r bankno t v e bira z bozuklu k karşılığınd a tü m ekibin adların a v e e-post a adreslerin e sahi p olmuştum .

İçeri Girme k

Peki, birka ç saa t içind e ü ç y a d a dör t kişiyl e konuştu m v e şirke t bilgisa - yarlarına girebilme k içi n de v bi r adı m attım . Am a olay ı kalbinde n vur - mak içi n birka ç parç a bilgiy e dah a ihtiyacı m vardı .

Birincisi, mühendisli k sunucusun a dışarda n bağlanma k içi n gerekl i telefon numarasıydı . GeminiMed' i tekra r aradı m v e santra l memurun - dan Bilg i İşle m Birimi'n i bağlamasın ı istedim . Telefon a çıka n adam a bilgisayarlar konusund a yardımc ı olabilece k biriyl e görüşme k istediği - mi söyledim . Ben i aktard ı v e tekni k konularl a ilgil i olara k kafa m karışmış, bira z d a aptalmı ş gib i davrandım . "Evdeyim, yeni bir diziistü bilgisayar aldım ve dışardan bağlanabilecek şekilde onu ayarlamak istiyorum."

Süreç ço k açıkt ı am a bağlant ı içi n gerekl i telefo n numarasın a gelen e kadar he r şey i ban a te k te k anlatmasın a izi n verdim . Numaray ı ban a herhangi bi r önemsi z bilgiymi ş gib i verdi . Sonr a numaray ı denerke n onu beklettim . He r şe y yolundaydı .

Ağa bağlanm a engelin i aşmıştım . Numaray ı çevirdi m v e arayanı n dahili a ğ üzerindek i bilgisayarlar a bağlanmasın a izi n vere n bi r uçbiri m sunucusuyla donanmı ş olduğun u gördüm . Birka ç denemede n sonr a parolasız konu k hesab ı ola n bi r bilgisayar a den k geldim . Baz ı işleti m sistemleri il k kurulduklarınd a kullanıcıy ı bi r kullanıc ı ad ı v e parol a belirlemesi içi n yönlendirirler , anca k ayn ı zamand a bi r d e konu k hesab ı açarlar. Kullanıcını n konu k hesab ı içi n y a bi r parol a belirlemes i y a d a hesabı bütünüyl e kapatmas ı gereki r am a çoğ u insa n bun u bilme z y a d a umursamaz. B u siste m büyü k olasılıkl a yen i kurulmuşt u v e sahib i konuk hesabın ı kapatmakl a uğraşmamıştı .

Çok şükü r bi r konu k hesab ı varmı ş ki , ş u and a UNI X işleti m sistemi -

nin esk i bi r sürümün ü çalıştıra n bi r bilgisayar a erişimi m var . UNI X

altındaki işleti m sistemi , o bilgisayar a giri ş hakk ı ola n herkesi n şifre -

lenmiş parolaları m bi r parol a dosyasınd a saklar . Parol a dosyas ı he r kul -

lanıcının te k yönl ü karıştırılmı ş (b u ger i döndürüleme z bi r çeşi t

şifreleme yöntemidir) parolaların ı içerir . Te k yönl ü bi r karıştırm a sonu -

cunda "haydiyap " gib i bi r parol a şifrelenmi ş bi r karmaşayl a temsi l

edilir. B u durumd a parol a UNI X tarafında n o n ü ç alfanümefi k simge -

den oluşa n bi r karışım a dönüştürülecektir .

Bir kiş i bi r bilgisayar a dosy a aktarma k isterse , bi r kullanıc ı ad ı v e paro -

la girere k kendin i tanıtmas ı istenir . Tanıtı m bilgilerin i kontro l ede n sis -

tem yazılım ı girile n parolay ı şifrele r sonr a d a sonucu , parol a dosyasın -

daki şifrelenmi ş parolayl a (yan i karışımla) karşılaştırır . Eğe r ikis i

aynıysa, kullanıcıy a erişi m hakk ı verilir .

Dosyada yazıl ı parolala r şifrel i olduklar ı içi n dosya , şifreler i çözmeni n

bilinen bi r yol u olmadığ ı gerekçesin e dayanara k tü m kullanıcılar a açık -

tır. Çok saçma ! Dosyayı indirdim ve üze -

Terimler

rinde bir sözlük saldırısı yaptım (Bu yön -

temle ilgili bilgi için 12 . bölüme bakınız) ve PAROLA KARMAŞASI: Bir

geliştirme ekibindeki mühendislerden biri ,

parolayı tek yönlü bir

Steven Grame r adında bir adamın bilgisayar -

şifreleme sürecinden

da parolası "Janice " olan bir hesabı oldu - geçirdikten sonra ortaya

ğunu öğrendim . Şansım deneyip bu paro - çıkan anlamsız harf dizili-

layı kullanarak adamın geliştirme sunucu - mi. Bu sürecin güya geri

larından birindeki hesabına girmeye çalış - döndürülemez bir süreç

tım. İşe yarasaydı , bana bir zamanlar kazan - olduğu, yani karışımdan

dırır ve başka bir risk daha almamaya gerek

tekrar parolayı elde

kalmazdı. Ama olmadı .

etmenin mümkün olmadığı

Bu, adamı bana kullanıcı adını ve parolasını

düşünülür.

vermesi için kandırmam gerektiğini anlamına

geliyordu. Bunu n içi n haftasonun u

bekleyecektim. Terimler Kalam zate n biliyorsunuz. Cumar -

tesi gün ü Cramer' i aradı m v e şüphe -

ÖLÜ NOKTA: Bilginin lerini yenme k içi n bi r solucanl a v e

bırakılabileceği ve başkaları sunucuların yedekte n ger i yüklen -

tarafından bulunma mesi gerektiğiyl e ilgil i bi r hikây e

olasılığının düşük olduğu uydurdum.

yer. Geleneksel casusların

olduğu bir dünyada bu, Ya on a anlattığı m iş e giri ş formların -

duvarda yerinde oynamış bir da parolasını n yazdığıyl a ilgil i öyk ü

taşın arkası olurdu; bilgisa- tutmasaydı? İş e girerke n doldurduğ u

yar korsanlarının dünyasın- formlarla ilgil i bi r şe y hatırlamaya -

da bu çoğunlukla uzak bir cağından emindim . Yen i iş e gire n

ülkedeki bir internet biri o kada r ço k for m dolduru r k i yıl -

sitesidir. lar sonr a b u formları n nele r oldu -

ğunu ki m hatırlayabilir ? N e olurs a

olsun, eğe r ond a çuvallasaydım , elimd e

kullanabileceğim uzu n bi r isi m listesi vardı .

Cramer'in kullanıc ı adın ı v e parolasın ı kullanarak sunucuy a girdim , biraz ortalığ a bakındı m v e sonund a STH-100'ü n tasarı m dosyaların ı buldum. Hangilerini n anahta r dosyala r oldukların ı bilmiyordum , bu yüzden tü m dosyala n bi r öl ü noktaya , kimsey i kuşkulandırmada n dura - bilecekleri Çin'dek i ücretsi z bi r FT P sitesin e aktardım . Ivı r zıvır m için - den ney e ihtiyac ı vars a müşter i kend i arayı p bulsun .

• • Aldatmacanı n İncelenmes i - - : . .

Hırsızlık gib i ola n am a he r zama n yasadış ı olmaya n toplu m mühendisliği sanatında , kendisin e Crai g Cogburn e dediğimi z ada m y a da e n a z onu n kada r becerikl i bi r kiş i içi n burad a

anlatıla n zorlukla r neredeyse sırada n şeylerdir . B u adamı n amacı , güvenli k duvarlarıyl a v e ofağan güvenlik teknolojileriyle korunan bir şirke t bilgisayarınd a dura n gizli dosyala n bulu p indirmekti .

• İşi n çoğ u çocu k oyuncağıydı . İş e post a odasında n bir i gib i davra - narak başlad ı v e tesli m edilmey i bekleye n bi r karg o paket i olduğun u söyleyerek konuy a bira z aciliye t kattı . B u kandırmaca , kal p stent i geliştirme ekibini n tatild e ola n liderini n adın ı öğrenmesin i sağlad ı am a ekip lider i düşüncel i davranmı ş v e bilg i çalmay a çalışa n toplu m mühendislerinin işin i kolaylaştırma k içi n yardımcısını n adın ı v e telefo n numarasını bırakmıştı . Crai g eki p liderini n yardımcıs ı ola n kadın ı aramış v e eki p liderini n isteğ i üzerin e aradığın ı söyleyere k bütü n şüpheleri ortada n kaldırmıştı . Eki p lider i şehi r dışındayke n Michelle'i n söylenenleri doğrulamasın a d a olana k yoktu . Bun u gerçe k olara k kabul etti v e eki p üyelerini n bi r listesin i verme k konusund a tereddü t etmedi . Craig içi n b u oldukç a öneml i v e değerli bi r bilgiydi .

Craig listeyi , genellikl e he r ik i tara f içi n d e dah a kullanışl ı ola n e-posta yerin e faksl a göndermesin i istediğind e bil e kuşkulanmadı . Kadın nede n b u kada r kola y kanmıştı ? Pe k ço k çalışa n gibi , patronunu n işe dönü p d e yapılmasın ı istediğ i bi r iş i yapmay a çalışa n birini n engellerle karşılaştığın ı duymasın ı istememişti . Dahası , arayanı n söylediğine gör e patron u yalnızc a adamı n isteklerin i onaylamakl a kalmamış, ayn ı zamand a onda n yardı m d a istemişti . Bi r ke z daha , çoğ u insanı kandırılmay a açı k hal e getiren , takı m oyuncus u olm a isteğiyl e dolup taşa n biriyl e karş ı karşıyayız .

Craig, danışmadak i kızı n yardımc ı olacağın ı bilere k faksı n danış - maya gönderilmesin i sağlamı ş v e böylec e binay a girm e gereğinde n d e kurtulmuştu. N e d e ols a danışm a görevliler i etkileyic i kişilikler i v e iy i bi r izlenim yaratmadak i beceriler i nedeniyl e seçilirler . Fak s alı p gönderme k gibi küçü k iyilikler i yapma k danışmad a çalışa n birini n göre v alanın a girer v e Crai g d e bunda n nası l yararlanacağın ı biliyordu . Kızı n dışar ı gönderdiği şey , o bilgini n n e kada r değerl i olduğun u bile n bir i içi n alar m zillerinin çalmasın a nede n olabilirdi ; am a danışmad a çalışa n birini n hangi bilgini n hassas , hang i bilgini n sırada n olduğun u bilmes i nası l bek - lenebilir ki ?

Farklı bi r yönlendirm e kullana n Craig , şirketi n uçbiri m sunucusuna , yani dahil i a ğ üzerind e diğe r bilgisaya r sistemlerin e erişi m sağlaya n donanıma bağlanma k içi n kullanıla n telefon numarasın ı vermes i içi n bilgi işlemdek i adam ı ikn a etme k amacıyl a sa f v e şaşkı n davranmıştı .

Craig, hi ç değiştirilmemi ş v e güvenli k duvarıyl a koruna n pe k ço k dahili ağd a va r olu p doğruda n gö z önündek i açıklarda n birini , yan i varsayılan parolalarda n birin i deneyere k kolaylıkl a bağlanmay ı başardı . Aslında pe k ço k işleti m sisteminin , yönlendiricini n v e başk a benze r ürünün, hatt â öze l santralları n varsayıla n parolalar ı çevrimiç i olara k bulunabilir. Herhang i bi r toplu m mühendisi , bilgisaya r korsan ı y a d a sanayi casusunu n yanısır a yalnızc a konuy a merakl ı olanla r bil e listey i http://www.phenoelit.de/dpl/dpl.html adresinde n bulabilirler . (Nerey e bakması gerektiğin i bilenle r içi n interneti n yaşam ı b u kada r kolaylaştır - ması inanılmaz . Artı k si z d e nerey e bakmanı z gerektiğin i biliyorsunuz.)

Daha sonr a Cogburne , kal p stent i geliştirm e ekibini n kullandığ ı sunucuya girebilme k için , dikkatl i v e şüphec i bi r adam ı bil e ("Soyadı n n e demiştin? V e müdürü n kim?") kullanıc ı adın ı v e parolasın ı vermey e ikn a

JVUtnick Mesajı :

Çalışan herkesin birinci önceliği eldeki işi bitirmektir. Böyle bir baskı altında, güvenlik uygulamaları sık sık ikinci sıraya düşer veva gözden kaçar. Toplum mühendisleri, işlerini yaparken buna güvenirler.

etti. Bu , Craig'i n şirketi n e n iy i koruna n sırların ı karıştırmas ı v e yen i ürü n :asanmlarını indirmes i içi n kapıy ı açı k bırakma k gib i bi r şeydi .

Ya Stev e Crame r şüphelenmey i sürdürseydi ? Pazartes i sabah ı iş e gidene kada r kuşkuların ı dil e getirme k adın a birşe y yapm a olasılığ ı düşüktü, o zama n d a zate n saldırıy ı engelleyebilme k içi n ço k ge ç kalmı ş olacaktı.

Oynanan so n oyunu n kili t kısm ı şuydu : Crai g il k başt a Steve'i n endişelerine karş ı gayretsi z v e ilgisi z bi r ro l takınmış , sonr a d a se s tonunu değiştiri p Steve'i n işin i bitirebilmes i içi n on a yardı m etmey e çalışıyormuş gib i bi r hav a yaratmıştı . Çoğ u zama n kurban , on a yardı m ettiğinize y a d a bi r iyili k yapmay a çalıştığınız a inanırsa , başk a zaman - larda özenl e koruyacağ ı gizl i bilgiler i sizinl e paylaşacaktır .

Aldatmacanın Engellenmes i

Toplum mühendisini n kullandığı e n güçl ü numaralarda n bir i olayları n gidişini değiştirmektir . B u bölü m kapsamınd a gördüğünü z şe y budur . Toplum mühendis i sorun u yaratır , sonr a d a mucizev i bi r şekild e sorun u •çözerek kurban ı şirketi n e n gizl i bilgilerin e erişi m sağlamakt a kendisin e yardımcı olmas ı içi n kandırır . Sizi n çalışanlarını z d a böyl e bi r oyun a gelirler miydi ? Bun u önleme k içi n belirl i güvenli k kuralların ı bi r kâğıd a döküp dağıtmay ı hi ç denedini z mi ?

Eğitim, Eğitim , Eğitim.. .

New York' u görmey e gelmi ş bi r adaml a ilgil i esk i bi r fıkr a vardır . Adam yolda n birin i çeviri r v e sorar , "Camegi e Hall' a nası l ulaşabilirim? " Öteki ceva p verir , "Çalışarak , çalışarak , çalışarak. " Toplu m mühendisliğ i saldırılarına herke s o kada r açıktı r ki , bi r şirketi n te k etkil i savunmas ı çalışanlarını eğitmek , bilgilendirme k v e bi r toplu m mühendisin i tanıma k için gerekl i altyapıy ı onlar a vermektir . Sonr a d a insanlar a sürekl i olara k eğitim sırasınd a öğrendikler i hatırlatılmalıdı r am a bunları n heps i unutlur .

Kuruluştaki herkes , şahse n tanımadığ ı biriyl e görüştüğ ü zamanlard a -özellikle d e b u kiş i bi r bilgisayar a y a d a ağ a nası l erişileceğin i soruyor - sa- maku l düzeyd e şüphec i v e dikkatl i olma k konusund a eğitilmelidir . Başkalarına inanmay ı isteme k insa n yaratılışınd a vardı r am a Japonları n dediği gibi , i ş dünyas ı bi r sava ş alanıdır . İşini z savunmadak i bi r boşluk - tan büyü k zara r görebilir . Şirke t güvenli k kurallar ı uygu n ola n v e olmayan davranışlar ı açıkç a tanımlamalıdır .

Güvenliğin herkes e uygu n te k bi r kalıb ı yoktur . Çalışanları n çoğun - lukla farkl ı görevler i v e sorumlulukları , he r şirke t iç i konumu n d a kendin e özgü açı k noktalar ı vardır . Şirkettek i herkesi n tamamlamakl a yükümlü olduğu bi r teme l eğiti m olmalıdır . Dah a sonr a insanla r sorunu n bi r

parçası olm a olasılıkların ı düşürece k belirl i süreçler e bağl ı kalabilmeler i için i ş profillerin e gör e d e eğiti m görmelidirler . Hassa s bilgiler i kullana n ya d a sorumlu k gerektire n konumlardak i kişiler e ayrıc a öze l eğiti m ve - rilmelidir. .

Hassas Bilgiler i Emniyet e Alma k

Bu bölümdek i öykülerd e d e gördüğünü z gibi , bir i yanların a geli p yardım etmey i tekli f ettiğind e insanların , i ş gereklerine , büyüklüğ e v e şirket kültürün e uygu n olara k tasarlanmı ş şirke t güvenli k kuralların a başvurmaları gerekir .

Sizden bi r bilgiy i taramanızı , bilgisayarınız a bilmediğini z komutla r girmenizi, yazılı m ayarlarınız ı değiştirmeniz i v e -hepsini n arasınd a e n tehlikeli olanı - bi r e-post a ekin i açmanız ı y a d a kaynağ ı belirsi z bi r yazılımı indirmeniz i isteye n bi r yabancıyl a hiçbi r zama n işbirliğ i yap - mayın. Hiçbi r şe y yapmıyormu ş gib i görüns e bil e herhang i bi r yazılı m programı göründüğ ü kada r masu m olmayabilir .

Eğitiminiz n e kada r iy i olurs a olsu n zama n içind e uygulamakt a dikkat - siz davrandığımı z belirl i süreçle r vardır . Sıkışı k bi r zamanda , ta m d a on a ihtiyacımız olduğ u and a eğitim i unutuveririz . Kullanıc ı adın ı v e parolay ı vermemenin, neredeys e herkesi n bildiğ i (y a d a bilmes i gerektiği) v e hatır - latılmasına pe k d e gere k olmaya n bi r şe y olduğun u düşünebilirsiniz . Mantıklı ola n budur . Am a aslınd a he r çalışan a ofi s bilgisayarlarında , e v bilgisayarlarında, hatt â post a odasındak i sayılandırm a makinasınd a kul - landıkları kullanıc ı adın ı v e parolay ı dışarıy a vermelerinin , AT M kartlarını n şifresini vermekl e e ş değe r olduğ u sı k sı k hatırlatılmalıdır .

Bazen -am a ço k ende r olarak - gizl i bilgiler i bi r başkasın a vermeni n zorunlu hatt â öneml i olduğ u durumla r sö z konus u olabilir . B u nedenl e "hiçbir zaman " konusund a kat ı kuralla r oluşturmak , yerind e olmayacak - tır. Yin e d e güvenli k kurallarını z v e süreçlerinizde , bi r çalışanı n paro - lasını başkasın a verebileceğ i durumları n v e -dah a d a önemlisi - b u bil - giyi kimi n sormay a yetkil i olduğunu n açıkç a belirtilmes i gerekmektedir .

Pek ço k kuruluşta , kural , şirket e y a d a başk a bi r çalışan a zara r vere - bilecek bilgileri n yalnızc a yü z yüz e biline n kişiler e y a d a kuşkuy a ye r bırakmadan sesini n tanınabildiğ i kişiler e verilebileceğ i şeklind e olmalıdır .

Üst düze y güvenli k gerektire n durumlarda , sadec e kişise l olara k getirilen y a d a güvenili r bi r yetkilendirmeyl e -örneği n öncede n karar - laştırılmış gizl i bi r şifreyl e v e zama n ayarl ı kartla r gib i ik i farkl ı unsu r kul- lanılarak- gele n taleple r değerlendirilmelidir .

., Ver i korumas ı süreçleri , şirketi n hassa s işlevler i ola n bi r bölümün -

İN Ot * Şahsen hiç bir işletmede parola değiştokuşuna izin verilmesi gerektiğine inanmıyorum. Çalışanların kişisel parolalarını değiştokuş etmesini ya da paylaşmasını yasaklayan katı bir kural yerleştirmek çok daha kolaydır. Üstelik de çok daha güvenlidir. Ancak her işletmenin bu kararı verirken, kendi kültürünü ve güvenlik yaklaşımlarını göz önünde bulundurması gerekmektedir.

aen kişise l olara k tanınmaya n y a d a herhang i bi r şekild e kefi l olun - -namış birin e bilg i aktarılmaması m ifad e etmelidir .

Bu durumd a başk a bi r şirke t çalışanında n kulağ a gerçe k gib i gele n oir talebi , örneği n ekibinizdekileri n adlarını n v e e-post a adreslerini n üs - tesinin istendiğ i bi r durum u nası l el e alırsınız ? Y a d a baz ı evrakları n sadece şirke t içind e dolaşabileceğin i çalışanları n kafasın a nası l sokarsınız? Çözümü n öneml i bi r parçası , dışar ı gönderilece k bilgiler i değerlendirmek üzer e he r birimde n birin i görevlendirme k olabilir . B u durumda, görevlendirile n çalışanlar a izlemeler i gereke n öze l kontro l süreçlerinin anlatılacağ ı bi r iler i güvenli k eğitim i verilmelidir .

Kimseyi Unutmayı n

Hepimiz çalıştığımı z şirkettek i yükse k güvenli k gerektire n birimler i ezbere sayabiliriz . Am a çoğunlukl a gö z önünd e olmayan , bun a karşı n saldırılara oldukç a açı k ola n yerler e dikka t etmeyiz . B u olaylarda n birinde, şirke t içindek i bi r numaray a fak s çekilmes i yeterinc e masu m v e güvenli görünebilir ; anca k saldırgan , b u güvenli k açığında n yararla - nabilir. Buradak i ders : Sekreterle r v e idar i memurlardan , şirke t yönetici - leri v e üs t düze y idareciler e kada r herkesi n b u tar z oyunlar a karş ı uyanı k olmaları içi n öze l güvenli k eğitimler i almas ı gerektiğidir . Ö n kapıy ı kolla - mayı d a unutmayın : Danışm a görevliler i d e toplu m mühendislerini n öncelikli hedefler i arasındadı r v e baz ı ziyaretçile r v e arayanla r tarafında n kullanılabilecek aldatm a yöntemlerin e karş ı uyarılmalar ı gerekir .

Şirket güvenliğ i tarafından , bi r toplu m mühendisliğ i oyunun a hede f olduğunu düşüne n çalışanla r içi n bi r çeşi t bilg i biriki m merkez i niteliğind e tek bi r iletişi m noktas ı oluşturulmas ı gerekmektedir . Güvenli k olaylarını n bildirileceği te k bi r noktanı n olması , planl ı bi r saldır ı sırasınd a saldırını n ortaya çıkmas ı içi n etkil i bi r ö n uyar ı sistem i oluşmasın ı sağlayacak , böylece zama n kaybedilmede n duru m kontro l altın a alı-nabilecektir .

^_ s

!N| O t i Şaşılacak bir şekilde, arayanın adını v e telefon numarasını şir- ket çalışanları veri tabanından kontrol etmek ve geri aramak bile kesin bir çözüm değil. Toplum mühendisleri şirket veritabanına ad eklemenin ya da telefon aramalarını yönlendirmenin yollarını bilirler.

BANA YARDIMC I OLABİLİR MİSİNİZ ?

Yardım tekli f edere k toplu m mühendislerini n insanlar ı nası l kandırdıklarını gördünüz . Başk a bi r sevile n yöntemd e is e rolle r değişi r ve toplu m mühendis i karş ı tarafi n yardımın a ihtiyac ı olduğun u söyle - yerek yönlendirm e yapar . Zo r durumd a ola n insanlar a he p acımışızdır ; bu yüzde n b u yaklaşı m toplu m mühendisini n amacın a ulaşmasınd a et - {dîi olduğun u tekra r tekra r kanıtlamıştır .

Ziyaretçi

Üçüncü bölümd e anlatıla n öykülerde n biri , bi r saldırganı n Sosya l 3./enlik Numarası'n ı eld e edebilme k içi n kurbanın ı nası l kandırdığın - dan sö z ediyordu . B u seferk i toplu m mühendisimi z ayn ı sonuc u eld e stmek içi n farkl ı bi r yo l izliyo r v e sonr a d a b u bilgiy i kullanıyor .

Jones'Iann Çetelesin i Tutma k

Silikon Vadisi'nde , adı m vermeyeceğimi z bi r uluslararası şirke t var . Dünyanın he r tarafın a dağılmı ş satı ş bürolarını n ve diğe r tesislerini n hepsi d e bi r geni ş ala n ağ ı (WAN-Wid e Are a Netvvork) aracılığıyl a şir - ketin gene l müdürlüğün e bağlı . Bria n Atterb y adında , zeki , kıpı r kıpı r bir saldırgan , b u ti p bi r ağa , güvenliğin , gene l müdürlüğ e gör e dah a gevşek olduğ u e n u ç noktalarında n birinde n girmeni n dah a kola y olduğunu biliyordu .

Saldırgan, Chicag o bürosun u arad ı v e Ba y Jones'l a görüşme k istediği - ni söyledi . Danışmadaki kı z on a Ba y Jones'u n il k adın ı bili p bilmediği - ni sordu ; o da , "Bir yere yazmıştım, bulmaya çalışıyorum. Orada Jones adlı kaç kişi çalışıyor?" diy e sordu . Kız , "Üç," diy e yanıtladı . "Hangi bölümde çalışıyor?"

"Adlan okursanız belki hatırlayabilirim", ded i ada m v e kı z adlar ı okudu, "Barry, Joseph v e Gordon."

"Joseph. Evet adının b u olduğuna eminim" ded i adam . "Ve şeydeydi... hangi bölümdeydi?"

"İş geliştirme."

"Hah işte o. Beni ona bağlayabilir misiniz?"

Kız telefon u aktardı . Jone s telefon u açtığınd a saldırgan , "Bay Jones? Merhaba ben bordro servisinden Tony. Maaş çekinizin doğrudan vakıf hesabınıza yatırılmasıyla ilgili talebinizi a z önce yerine getirdik" dedi .

Tersmler

için dışar ı neo n tabelala r asmıyorlardı .

Doğru yerd e bulunma k çoğunlukl a içer i

girebilmek içi n yeterliydi . Benze r bi r

"BENİ ŞU GÖNDERDİ"

güvenlik yöntemi , şirke t dünyasınd a d a

TARZI GÜVENLİK: n e yaz| k k j s|kç a k u||am|lyor v e 'beni-şu -

Bilginin nerede olduğunu

bilmeye ve o bilgiye ya da

gönderdi' tarz ı güvenli k adın ı vereceğim ,

bilgisayar sistemine

işe yarama z bi r korum a sağlıyor .

erişmek için bir kelime ya

da ad kullanmaya dayanan

Filmlerde Gördü m

güvenlik şeklidir.

İşte siz e pe k ço k insanı n hatırlaya -

cağı güze l bi r filmde n bi r örnek .

Akbabanın'ın Ü ç Günü'nd e (Thre e Day s of th e Condor) Rober t Redford'u n oynadığ ı ba ş karakte r Turner , CI A adına i ş yapa n küçü k bi r araştırm a şirketind e çalışmaktadır . Bi r gü n öğl e yemeğinden döndüğünd e tü m arkadaşların ı vurulara k öldürülmü ş bulur . Kim oldukların ı bilmediğ i köt ü adamları n kendisin i aradıkların ı bilere k b u olayı kimi n v e nede n yaptığın ı bulmay a çalışır .

Hikâyenin ilerisind e Turne r köt ü adamlarda n birini n telefo n numarasını öğrenmey i başarır . Anca k b u ada m kimdi r v e Turne r onu n nerede olduğun u nası l bulabilir ? Tumer'ı n şans ı yave r gider , çünk ü senaryo yazar ı Davi d Rayfiel , Turner'ı n geçmişin e muhaber e bölüğünd e telefon hatt ı teknisyen i olara k eğiti m almı ş olm a özelliğin i koymuş , böylece on u telefon şirketini n yöntemler i v e uygulamalar ı hakkınd a bil - gili kılmıştı . Turner , köt ü adamı n telefo n numarasıyl a n e

yapmas ı gerek - tiğini gaye t iy i biliyordu . Senary o metnind e sahn e şöyl e anlatılır :

TURNER YENİDE N BAĞLANI R v e BAŞK A Bİ R NUMAR A ÇEVİRİR .

ZIRR! ZIRR ! Sonra :

KADIN SES İ (FİLTRELENMİŞ)

MAA, Baya n Colema n konuşuyor .

TURNER (ahizey e konuşur)

Ben Harol d Thomas , Baya n Coleman . Müşter i Hizmetleri . 202-555-7389 içi n MA A lütfen .

KADIN SES İ (FİLTRELENMİŞ)

Bir dakik a lütfen .

(hemen sonra)

Leonard Atwood , 76 5 MacKensi e Yolu , Chev y Chase , Marylan d

Senaryo yazarını n bi r Marylan d adres i içi n yanlışlıkl a bi r Washingto n alan kod u kullanıyo r olmas ı dışınd a burad a n e olduğun u anlayabildini z mi ?

Bana Yardımc ı Olabili r Misiniz ? 7 5

Mifnick Mesajı :

Gizlilik- üzerinden güvenlik sistemleri toplum mühendisliği saldırılarını engellemekte etkisizdirler. Dünyadaki herhangi bir bilgisayar sistemini kul- lanan en az bir insan yardır. Bu yüzden, eğer saldırgan, sistemleri kullanan insanları etkileyebilirse, sistemin gizliliği anlamsız olacaktır.

Aldığı telefo n hatt ı teknisyenliğ i eğitim i nedeniyl e Turner , bi r telefo n şirketinin MA A (Müşter i A d v e Adresi) bürosun a ulaşma k içi n hang i numarayı çevirmes i gerektiğin i biliyordu . MAA , tesisatçıla r v e diğe r yetkili telefo n şirket i çalışanların a kolaylı k sağlamas ı içi n kurulmuştu . Bi r tesisatçı MAA'y ı ara r v e telefo n numarasın ı verirdi . MA A memur u is e ".elefon numarasını n ai t olduğ u kişini n adın ı v e adresin i bulu p tesisatçıy a verirdi. . '

Telefon Şirketin i Kandırma k

Gerçek dünyad a MAA'nı n telefon numaras ı ço k iy i saklana n bi r sırdır . Her n e kada r telefon şirketler i şimdilerd e iş i sıkıy a almı ş v e bilg i verme k konusunda pe k cömer t davranmıyo r olsala r da , o zamanla r güvenli k uzmanlarının gizlili k üzerinde n güvenli k adın ı verdikler i bi r çeşi t 'ben i ş u gönderdi' tarz ı güvenli k uygulamas ı kullanıyorlardı . MAA'y ı araya n v e terminolojiyi bile n herhang i birini n ("Müşter i Hizmetleri . 555-1234'l e ilgil i MAA lütfen " gibi) bilg i alma k içi n yetkil i olduğun u varsayıyorlardı .

Ne kendiniz i tanıtmaya , n e kimliğiniz i kanıtlamaya , n e Sosya l Güvenlik Numaranız ı vermeye , n e d e hergü n değişe n bi r parol a gir - meye gere k yoktu . Eğe r aramanı z gereke n numaray ı biliyorsanı z v e sesiniz inandırıc ı geliyorsa , o zama n b u

bilgiyi almay a hakkını z va r demekti .

Bu, telefo n şirket i açısında n ço k

Terimler yerinde bi r varsayı m değildi . Güvenliğ i

GİZLİLİK ÜZERİNDEN sağlamak yolundak i te k çabalar ı yıld a bi r

GÜVENLİK: Sistemin (pro- kereden a z olmama k üzer e döne m döne m

tokollerin, algoritmaların telefon numarasın ı değiştirmekti . Bun a

ve dahili sistemlerin) çalış- rağmen b u numarala r hang i dönemd e

ma bilgileriyle ilgili ayrın- olursa olsu n b u kullanışl ı bilg i kaynağın -

tıları gizli tutmaya dayanan dan yararlanmakta n v e başk a beleşç i

etkisiz bir bilgisayar güven- arkadaşlarıyla yaptıkların ı paylaşmakta n

lik yöntemidir. Gizlilik hoşlanan telefo n beleşçiler i arasınd a
üzerinden güvenlik, güve- yaygın olara k biline n numaralardı . MA A
nilir bir grup insan dışında bürosu dalaveresi , gençliğimd e hob i
kimsenin sisteme giremeye- olarak telefo n beleşçiliğ i yaptığı m zaman -
ceği gibi bir yanlış inanışa larda il k öğrendiği m şeylerde n biriydi .
dayanır.

iş dünyasınd a v e devle t dairelerind e 'ben i ş u gönderdi ' tarz ı güven - lik sistemler i kullanılmay a deva m edilmektedir . Şirketinizi n birimleri , çalışanları v e terminolojisiyl e ilgil i yeterl i bilgiy i toplamı ş o kada r d a becerikli olmaya n herhang i bi r saldırganı n kendin i yetkil i bir i olara k tanıtması olasıdır . Baze n dah a az ı bil e yeterl i olur . Tü m gereke n şe y dahili bi r telefo n numarasıdır .

Her n e kada r şirketlerd e çalışa n pe k ço k kiş i güvenli k açıklarına karşı ihmalkâr , ilgisi z v e dikkatsi z ols a da , Fortun e 50 0 şirketler i arasın - da buluna n bi r bilgisaya r merkezind e yönetic i unvanıyl a buluna n birini n en iy i güvenli k uygulamalar ı konusund a bilgil i olmasın ı beklersiniz , öyl e değil mi ?

Şirketinin Bilişi m Teknolojiler i birimin e bağl ı olara k çalışa n bi r bil - gisayar merkez i yöneticisini n basi t v e bari z bi r toplu m mühendisliğ i dalaveresine kurba n gideceğ i aklınızı n ucunda n bil e geçmez . Özellikl e de toplu m mühendis i ergenli k çağında n yen i çıkmış , hâl â çocu k sayıla - bilecek biriyse . Anca k baze n beklentilerimizd e yanılabiliriz .

Yıllar önc e radyolar ı yere l poli s y a d a itfaiy e telsi z konuşmalarını dinleyecek şekild e ayarlama k v e he r zama n rastlanmaya n türde n oldukça heyecanlı bi r bank a soygununu , bi r işyer i yangının ı y a d a süratl i bir kovalamacay ı dah a olayla r olurke n dinlemek , vaki t geçirmeni n eğlenceli yollarında n biriydi . Poli s teşkilatını n v e itfaiyeni n kullandığ ı radyo frekanslar ı köşedek i kitapçıda n alabileceğini z kitapçıklard a bil e bulunuyordu; bugü n is e interne t üzerind e listele r Yıallnâ e âuruyofia i \ e bir kitapçıda n alabileceğini z kitaplardan , yere l teşkilatların , ilçe , eyale t ve hatt â baz ı durumlard a federa i büroları n bil e rady o frekansların ı bula - bilirsiniz.

Bunları dinleyenle r doğa l olara k yalnızc a meraklıla r değildi . Geceni n bir yarısınd a marke t soya n hırsızla r o taraf a doğr u bi r poli s arabasını n gelip gelmediğin i öğrenme k içi n poli s kanalın ı dinlerlerdi . Uyuşturuc u kaçakçıları Uyuşturuc u Masas ı polislerini n yere l hareketlerin i buralar - dan öğrenirlerdi . Bi r kundakçı , önc e bi r kibri t çakı p sonr a d a itfaiyecile r söndürmeye çabalarke n tü m rady o konuşmaların ı dinleyere k hast a zevkini tatmi n edebilirdi .

Günümüzde bilgisaya r teknolojisindek i gelişmele r se s mesajların ı şifreleme olanağ ı sağladı . Mühendisle r te k bi r mikroyongay a dah a fazl a işlem güc ü tıkmanı n yolların ı bulurlarken , bi r yanda n d a köt ü adamla r v e meraklıların dinlememes i içi n poli s kuvvetlerin e yöneli k küçük , şifrel i tel - sizler üretmey e başladılar .

Kulak Misafir i Dantı y " " ' . /

Adına Dann y diyeceğimi z ante n meraklıs ı v e yetenekl i bi r bilgisaya r korsanı, b u tü r telsi z sistemler i ürete n büyü k firmaları n birinden , gizl i şifreleme yazılımını n kayna k kodun u el e geçirmeni n bi r yolun u bulu p bulamayacağını denemey e kara r verirdi . Kod u incelemenin , poli s teşki - latını dinleyebilmesin e olana k sağlayacağın ı v e belk i de , e n gelişmi ş teknolojiye sahi p devle t kurumlarını n bil e arkadaşlarıyl a yaptığ ı konuş - maları dinlemesin i güçleştirece k şekild e teknolojiy i kullanabileceğin i umuyordu.

Bilgisayar korsanlarını n karanlı k dünyanı n Danny'ler i yalnızc a me - raklı -v e tamamıyla - zararsı z türde n adamlarl a tehlikel i adamla r arasın - da öze l bi r sınıflandırmay a tabidirler . Danny'ler , sunduğ u heyeca n içi n sistemlere v e ağlar a gire n v e teknolojinin nası l çalıştığını görmeni n keyfini çıkara n muzi p bi r korsanı n merakını n yan ı sır a bi r uzmanı n bilgi - sine d e sahiptirler . Anca k onları n elektroni k ortamlar ı kırm a v e o alan a girme maceralar ı gerçekte n d e yalnızc a bi r maceradır . B u adamlar , b u zararsız korsanlar , zev k içi n siteler e yasadış ı giri ş yaparlar . Yaptıklarından par a kazanmazlar ; dosyalar a zara r vermezler , a ğ rağlantılarını bozmazla r y a d a bilgisaya r sistemlerin i çökertmezler . Dnların yalnızc a orad a olup , güvenli k v e siste m yöneticilerini n sırt ı ;onükken dosyalar ı kopyalamas ı v e parolalar ı öğrenme k içi n e-posta - arı taraması , kendiler i gib i davetsi z misafirler i dışard a tutmakl a sorum - j adamları n kulakların ı bükmektedir , işi n en keyifl i yan ı karş ı taraf a üstünlük sağlamaktır .

Bu tanımlar a uygu n olara k bizi m Danny'miz , yalnızc a kend i Dastırılamaz merakın ı tatmi n etme k v e üreticini n bulduğ u akıllıc a yeni - kleri takdi r etme k için , hede f şirketi n e n iy i koruna n ürününü n ayrın - : arın ı inceleme k istiyordu .

Bilindiği üzere , ürü n tasarımlar ı şirketi n elindek i herhang i bi r şe y •adar değerli , korunmas ı gereke n v e özenl e saklana n ticar i sırlardır , lanny bun u biliyord u am a zerr e kada r

.•nurunda değildi . N e d e olsa , hedefteki ,

sadece büyü k v e isimsi z bi r şirketti .

Terimler

Ancak yazılı m kayna k kodun u nası l

i d e edecekti ? işleri n gidişin e bakılırsa ,

İKİ BASAMAKLI î 'keti n Güvenl i iletişi m Grubu'n a ai t

TANIMLAMA: Kimliği <raliyet mücevherlerini " el e geçirme k

belirlemek için iki farklı : dukç a kola y olmuştu . Üsteli k şirket ,

tanımlama şekli kullanıl- asanların kendilerin i tanıtmalar ı içi n bi r

masıdır. Örneğin, bir .erine ik i ayr ı anahta r gerektire n ik i

kişinin kendini tanıtabilmek zasamakl! bi r kimli k belirlem e sistem i

için belirli, tanımlanabilir • ..Hanıyordu .

bir noktadan ve parolayı

bilerek araması gerekebilir.

işte size , büyü k olasılıkl a artı k aşin a olduğunu z bi r örnek . Yen i kred i kartınız geldiğinde , kartı n doğr u kişini n elind e olduğunda n v e birilerini n zarfi post a kutusunda n çalmadığında n emi n olma k içi n kart ı vere n şir - ket onlar ı aramanız ı ister . Ş u sırala r kartl a birlikt e gele n talimatla r genel - likle evde n aramanız ı öneriyor . Aradığınızda , kred i kart ı şirketindek i yazılım, şirketi n ödediğ i ücretsi z aramaları n yapıldığ ı santralı n sağladığ ı ONT'yi (Otomati k Numar a Tanımlayıcısfnı) çözümlüyor .

Kredi kart ı şirketindek i bi r bilgisayar , araya n tarafı n numarasın ı şir - ketin kar t sahipler i ver i tabanınd a buluna n numarayl a karşılaştırır . Görevli, telefon u açan a kada r müşterini n ver i tabanında n çekile n bilgile r ekranda görünür . Böylec e görevli , bilgiler i gördüğ ü anda , aramanı n bi r müşterinin evinde n yapıldığın ı anlar . Bu , kimli k belirlemeni n bi r basamağıdır.

Sonra görevl i sizinl e ilgil i önün e çıka n bilgilerde n birin i seçe r -b u çoğunlukla Sosya l Güvenli k Numarası , doğu m tarih i y a d a anneni n kızlık soyad ı olur - v e b u bilgiy i doğrulama k içi n siz e sor u sorar . Eğe r doğru yanıt ı verirseniz , b u d a kimli k belirlemenin , sizi n bildiğini z bi r şey e dayanan ikinc i basamağın ı oluşturur .

Hikâyemizde geçe n güvenl i telsi z sistemlerin i ürete n şirketi n he r çalışanının bilgisayar a girme k içi n kullandığ ı kullanıc ı ad ı v e parolanı n yanı sır a bi r d e Güvenli Kimlik dedikler i küçü k bi r elektroni k cihaz ı vardır. Bun a zaman tabanlı anahtar denir . B u cihazla r ik i çeşittir : Bir i bi r kredi kartını n yarıs ı boyutundadı r am a bira z dah a kalındır ; diğer i is e insanların anahtarlıkların a takabilecekler i kada r küçüktür .

Şifreleme dünyasını n bi r eser i ola n b u aleti n üzerind e alt ı basamak - lı bi r say ı göstere n küçü k bi r ekra n vardır . He r altmı ş saniyed e bi r ekran - da farkl ı bi r alt ı basamakl ı say ı görünür . Yetkil i bi r kişinin , dışarıda n ağ a gireceği zaman , önc e gizl i bi r kişise l kimli k numaras ı sonr a d a anahta r cihazında görünen sayılar ı girere k kendin i yetkil i bir i olara k tanıtmas ı gerekir. Dahil i siste m tarafında n tanındıkta n sonr a kullanıc ı adın ı v e parolasını yazara k giriş i gerçekleştirir .

Genç korsa n Danny'ni n istediğ i kayna k kodun u alabilmes i içi n yal - nızca bi r çalışanı n kullanıc ı adın ı v e parolasın ı bulmas ı yetmiyo r (k i bu , deneyimli bi r toplu m mühendis i içi n ço k zo r bi r i ş değildir) , ayn ı zaman - da zama n tabanl ı anahta r kontrolün ü d e atlatmas ı gerekiyordu .

Gizli kişise l kimli k numarasıyl a birleşmi ş zama n tabanl ı anahta r kul- lanılan ik i basamakl ı bi r kimli k belirlem e sistemin i al t etme k kulağ a ta m Görevimiz Tehlike'de n fırlamı ş bi r i ş gib i geliyor . Am a toplu m mühendis i için böyl e bi r işt e karşılaşacağ ı zorluk , öze l bi r beceriy e sahi p bi r poke r oyuncusunun rakiplerini n yüzlerin i okumad a karşılaştığ ı zorlukl a ben - zerdir. Şans ı yave r giderse , oturduğ u masadan , diğe r insanlarda n aldığ ı tomarla parayl a birlikt e kalkabileceğin i bilir .

Kaleyi Fethetme k

Danny hazırlıkların ı yapmay a başladı . Ço k geçmede n gerçe k bi r çalışan rolün ü oynayaca k kada r bilg i toplamıştı . Elind e bi r çalışanı n adı , rolümü, telefo n numaras ı ve Sosya l Güvenli k Numarası'nı n yan ı sır a rneticisinin ad ı v e telefo n numaras ı d a vardı .

O and a kelimeni n ta m anlamıyl a fırtın a önces i sessizli k hakimdi . Yaptığı plan ı uygulayara k bi r sonrak i adım ı atmada n önc e Danny'ni n yapması gereke n birşe y dah a kalmıştı . Bu , kend i çabalarıyl a yapama - yacağı bi r şeydi . Bi r ka r fırtınasın a ihtiyac ı vardı . Danny'nin , çalışanları n --"islerine ulaşmasın ı engelleyece k kada r köt ü bi r hav a içi n Tabia t ^na'dan küçü k bi r yardı m almas ı gerekiyordu .

Söz konus u fabrikanı n bulunduğ u Güne y Dakota'd a kı ş mevsimind e <ötü hav a dileye n birini n ço k beklemes i gerekmez . Cum a geces i fırtın a koptu. Ka r şeklind e başlaya n yağış , soğu k bi r yağmur a dönüşt ü v e oöylece sabah a kada r tü m yolla r kayga n v e tehlikeJ i bi r bu z tabakasıy - a kaplandı . Dann y içi n b u harik a bi r fırsattı .

Fabrikayı arayıp , bilgisaya r odasın ı bağlattırd ı v e bilg i işlemi n işç i arılarından birine , kendin i Roge r Kovvalsk i olara k tanıta n bi r bilgisaya r işletmenine ulaştı .

Danny, el e geçirdiğ i v e gerçe k bi r çalışan a ai t ola n ad ı verere k Konuştu. "Be n Bo b Billings . Güvenl i İletişi m Grubu'nd a çalışıyorum . Ş u anda evdeyi m v e fırtın a yüzünde n iş e gelemiyorum . Bilgisayarım a v e sunucuya evde n ulaşma m gerekiyo r am a Güvenl i Kimli k Kartı'm ı masamda unutmuşum . On u beni m içi n alı r mısınız ? Y a d a başk a bir i d e alabilir. Sonr a ağ a girme m gerektiğind e ekranınd a yazan ı ban a okuya - bilirsiniz. Ekibimi n yetiştirmes i gereke n öneml i bi r teslima t va r v e b u durumda iş i bitirme m mümkü n değil . Ofis e gelemiyorum , b u taraflarda - ki yolla r ço k tehlikel i bi r hal e geldi. "

"Ben Bilgisaya r Merkezi'nde n ayrılamam " ded i bilgisaya r işletmeni .

Danny heme n atladı , "Sizi n bi r Güvenl i Kimli k Kartını z va r mı ?

"Bilgisayar Merkezi'nd e bi r tan e var, " ded i işletmen . "Aci l bi r durum - da işletmenleri n kullanmas ı için. "

"Tamam" ded i Danny . "Ban a büyü k bi r iyili k yapabili r misin ? Ağ a girmem gerektiğ i zama n Güvenl i Kimli k Kartı'n ı kullanabili r miyim ? Yalnızca yolla r düzelen e kadar. "

"Adınız n e demiştiniz? " diy e sord u Kovvalsk i

"Bob Billings. " • • • .

"Kimle çalışıyorsunuz? "

"Ed Trenton'la. " ••- • ' o / < : - . .,- • v

Zor bi r durumd a kalm a tehlikes i varsa , iy i bi r toplu m mühendisi , yapılması gerekende n dah a fazl a araştırm a yapar . "İkinc i kattayım " diy e devam ett i Danny . "Ro y Tucker'i n yanınd a oturuyorum. "

Adam b u ad ı d a biliyordu . Dann y on u işlemey e deva m etti . "Masam a gidip Güvenl i Kimli k Kartı'm ı alı p gelirseni z ço k dah a kola y olabilir. "

Danny adamı n bun u yapmayacağında n oldukç a emindi . He r şeyde n önce mesaisini n ortasınd a iş i bırakı p koridorlarda n geçi p merdivenler - den çıkı p binanı n öbü r köşesin e gitme k istemeyecekti . Ayrıc a başk a birinin masasını n başın a geçi p öze l eşyaların ı karıştırı r gib i bi r durumd a kalmak d a istemezdi . Evet , bun u yapmayacağ ı üstün e oynama k yerind e olacaktı.

Kowalski yardım a ihtiyac ı ola n birin e hayı r deme k istemiyord u am a evet deyi p başın ı belay a sokma k d a istemiyordu . B u yüzde n kara r ver - mekten çekinere k yan a adı m attı . "Müdürüm e sorma m gerekecek . Bira z bekler misiniz? " Telefon u bırakt ı v e Dann y onu n başk a bi r telefon u alıp , bir numar a çevirdiğin i sonr a d a isteğin i birin e anlattığın ı duydu . O and a Kovvalski açıklamas ı gü ç birşe y yaptı . Bo b Billing s adın ı kullana n adama kefi l olmuştu . "On u tanıyorum " ded i yöneticisine . "E d Trento n için çalışıyor . Bilgisaya r Merkezindek i Güvenl i Kimli k Kartı'n ı kullan - masına izi n verebili r miyiz? " Dann y telefon elind e amacın a verile n b u olağanüstü v e beklenmedi k deste k karşısınd a şaşırı p kalmıştı . N e şan - sına n e d e kulakların a inanamıyordu . .-.; . •-•• • -- •

Birkaç dakik a sonr a Kovvalsk i telefon u yenide n elin e aldı . "Müdürü m sizinle şahse n konuşma k istiyor " ded i v e on a müdürünü n adın ı v e ce p telefonu numarasın ı verdi .

Danny müdür ü arad ı v e üzerind e çalıştığ ı projeni n ayrıntıların ı v e ekibinin öneml i bi r teslimat ı yetiştirmes i gerektiğin i d e ekleyere k tü m hikâyeyi bi r ke z dah a anlattı . "Bir i gidi p kartım ı alabilirs e dah a kola y olur" dedi . "Masamı n kilitl i olduğun u sanmıyorum , so l üs t çekmeced e olmalı."

"Peki" ded i müdür, " Yalnızc a haft a son u içi n olma k kaydıyl a sanırı m Bilgisayar Merkezi'ndekin i kullanmanız a izi n verebiliriz . Görevl i arkadaşlara aradığınızd a erişi m şifresin i siz e okumaların ı söyleye- ceğim" ded i v e onunla birlikt e kullanılaca k kişise l tanıtı m numarasın ı d a verdi.

Tüm haft a son u boyunc a şirke t bilgisayarın a girme k istediğ i zama n Danny'nin yaptığ ı te k şe y Bilgisaya r Merkezi'n i arama k v e Güvenl i Kimli k Kartı'nda yaza n alt ı basamakl ı sayıy ı okumaların ı ric a etme k oldu .

Bana Yardımc ı Olabili r Misiniz ? 8 1

İşi İçerde n Bitirme k

Şirketin bilgisaya r sistemin e girdikte n sonr a n e olacaktı ? Dann y î'adığı yazılımı n bulunduğ u sunucuy a girmeni n yolun u nası l bulacaktı ?

Bunun içi n zate n hazırlıklıydı .

Bilgisayar kullanıcılarını n çoğ u tartışm a gurupların ı bilirler . Bunlar , insanların yanı t aradıklar ı soruların ı koyduklar ı y a d a müzik , bilgisaya r ve dah a yüzlerc e başk a konud a sanal arkadaşla r edinme k içi n kul- andıkları elektroni k bülte n panolarıdır .

Bir tartışm a gurub u sitesin e mesa j bıraktıklarında , mesajlarını n yıl - arca çevrimiç i v e erişilebili r kalacağın ı pe k a z kiş i bilir . Örneği n 3oogle'ın, bazılarını n tarih i yirm i yı l öncesin e dayana n yed i yü z milyo n mesajlık bi r arşiv i vardır ! Dann y iş e http://groups.google.co m adresin e girmekle başladı .

Arama metn i olara k "şifrel i telsi z iletişimi " v e şirketi n adın ı giri p bi r çalışana ai t yılla r öncesinde n kalmı ş bi r mesa j buldu . Şirketi n b u ürün ü geliştirmeye başladığ ı yıllarda , herhald e poli s teşkilatlarını n v e federa l Duraların telsi z sinyallerin i karıştırmay ı düşünmelerinde n ço k önc e Dirakılmış bi r mesajdı .

Mesajda göndereni n ad ı d a bulunuyordu . Yalnızc a ad ı değil , telefo n numarası v e hatt â çalıştığ ı grubu n adın ı vardı ; Güvenl i İletişi m Grubu .

Danny telefon u açı p numaray ı çevirdi . Yaptığ ı ço k uzu n bi r atı ş gib i görünüyordu. Adam , yılla r sonr a d a ayn ı kurulu ş içi n çalışmay a deva m ediyor muydu ? Böyl e fırtınal ı bi r haft a sonund a i ş yerind e olabili r miydi ? Telefon bi r kez , ik i kez , ü ç ke z çald ı v e sonund a açıldı . Açа n kişi , "Be n Scott" dedi .

Danny, şirketi n Bilg i İşle m Bölümü'nde n olduğun u söyleyere k geliştirme işler i içi n kullanıla n sunucuları n adın ı vermey e (öncek i bölüm - lerden artı k aşin a olduğunu z yollarda n birin i kullanarak) Scott' u ikn a etti . Bu sunucularda , şifrel i telsizlerd e kullanılan , şirket e özg ü algoritmaları n ve yazılımları n kayna k kodlarını n bulunduğun u düşünüyordu .

Danny gittikç e yaklaşıyo r v e heyecan ı d a gidere k artıyordu . Ço k a z insanın başarabileceğin i bildiğ i bi r şey i başardığınd a hissedeceğ i heye - canın v e büyü k coşkunu n beklentis i içindeydi .

Yine d e henü z hedefin e ulaşmamıştı . Yardımseve r bilgisaya r merkez i müdürü sayesind e tü m haft a son u boyunc a şirketi n ağın a istediğ i zama n girebiliyordu. Ayrıc a hang i sunucular a erişmes i gerektiğin i d e biliyordu . Ancak bağlanmay a çalıştığında , oturu m açtığ ı uçbiri m sunucus u Güvenl i iletişim Grub u geliştirm e sistemlerin e girmesin e izi n vermedi . O grubu n bilgisayar sistemlerin i koruya n bi r i ç güvenli k duvar ı y a d a yönlendiric i olmalıydı. Girme k içi n başk a bi r yo l bulmas ı gerekiyordu .

Bir sonrak i adı m gözün ü karartmasın ı gerektirmişti . Danny , Bilgisayar Merkezi'nd e çalışa n Kovvalski'y i arad ı ve , "Sunucu m bağlan - mama izi n vermiyor " diy e şikâye t etti . "Telne t kullanara k kend i sis - temime bağlanabilme m içi n sizi n bölümü n bilgisayarlarınd a beni m içi n bir hesa p açabili r misiniz? "

Müdür zate n zama n tabanl ı anahtarı n sağladığ ı erişi m şifresini n ve - rilmesini onaylamıştı , b u yüzde n böyl e bi r iste k tuha f karşılanmadı . Kovvalski, Bilgisaya r Merkez i bilgisayarlarında n birind e geçic i bi r hesa p açtı v e bi r d e parol a verdi . Danny' e de , "ihtiyacını z kalmadığ ı zama n haber verirseniz , hesab ı kaparım. " dedi .

Geçici hesab a girdikte n sonr a Danny , a ğ üzerinde n Güvenl i iletişi m Grubu'nun bilgisaya r sistemlerin e bağlanmay ı başardı . An a geliştirm e sunucusuna bağlanabilmek , amacıyl a tekni k bi r açı k bulabilme k içi n bi r saat boyunc a çevrimiç i aram a yapt ı v e sonund a turnay ı gözünde n vurdu. Görünüş e gör e siste m y a d a a ğ yöneticiler i işleti m sistemlerind e uzaktan erişim e izi n vere n güvenli k hatalarıyl a ilgil i gelişmelerde n ha - berdar değillerdi . Am a Dann y haberdardı .

Kısa sür e içerisinde , aradığ ı kayna k kodların ı buld u v e ücretsi z sak - lama alan ı vere n bi r e-ticare t sitesin e aktardı . Dosyala r buluns a bil e b u siteden kims e onu n izin i süremezdi .

Açtığı oturum u kapatmada n önc e atmas ı gereke n bi r adım dah a vardı: Bıraktığ ı izler i dikkatl e temizlemes i gerekiyordu . Cumartes i gece - si Ja y Leno'nu n program ı bittiğind e o d a kend i işin i bitirdi . Dann y bunu n çok veriml i bi r haft a son u olduğun a kara r verdi . Üsteli k d e kendin i hi ç riske atmas ı gerekmemişti . Ba ş döndürüc ü bi r heyecandı , hatt â kaya k sörfünden (snowboard) v e serbes t atlayışta n (sk y diving) bil e dah a heyecan vericiydi .

Danny o gec e sarho ş old u am a viski , cin , bir a y a d a sak e içere k değil. Aşırdığ ı dosyalara bakarken , parmaklarını n arasında n kaymay a çalışan so n derec e gizl i telsi z yazılımın a yaklaşmanı n verdiğ i gü ç v e başarı duygusuyl a sarho ş olmuştu . :

Aldatmacanın İncelenmes i . . .

Bir öncek i öyküd e olduğ u gibi , b u oyunu n d a iş e yaramasını n te k nedeni, bi r şirke t çalışanının , araya n kişini n söylediğ i kiş i olduğunu , sorgulamadan kabullenmesidir . Sorun u ola n bi r mesa i arkadaşın a yardım etme k sanay i tekerini n dönmesin i sağlaya n v e baz ı şirketleri n personeliyle çalışmay ı diğerlerin e gör e dah a keyifl i hal e getire n bi r unsurdur. Öt e yanda n b u yardımseverlik , bi r toplu m mühendisini n sömürebileceği öneml i bi r zaa f d a olabilir .

Danny'nin kullandığı başk a bi r yönte m is e nefisti . Birini n masasın -

dan Güvenl i Kimli k Kartı'n ı alı p gelmes i talebind e bulunurke n sürek; :

Bu öyküde anlatılanlar zaman tabanlı anahtarların ve benzer tanımlama yön- temlerinin kurnaz bir toplum mühendisine karşı koruma sağlamadıklarını bize gösteriyor. Tek savunma, güvenlik politikalarım bilen ve başkalarının kötü niyetle '. davranışlarını etkileyebileceğinin farkında olan sağduyulu bir çalışandır.

olarak emrede r gib i konuşuyordu . Kims e emi r almakta n hoşlanmaz . B u tavrıyla Dann y o isteğini n ger i çevrilmesin i sağlad ı v e başk a bi r çözü m önerisini kabu l etti . B u d a ta m istediğ i şeydi .

Bilgisayar Merkez i işletmen i Kovvalski , Danny'ni n adların ı verdiğ i Kişileri tanımas ı nedeniyl e tuzağ a düşmüştü . Am a nede n Kowalski'ni n müdürü, he m d e bi r bilg i işle m yöneticisi , tanımadığ ı birini n şirketi n dahili ağın a girmesin e izi n verdi ? Çünk ü toplu m mühendisini n araçlar ı arasında yardı m taleb i e n güçl ü silahlarda n biridir .

Böyle bi r şe y sizi n şirketinizd e d e olabili r mi ? Yoks a çokta n old u mu ?

Aldatmacanın Engellenmes i

Yardımcı ola n kişinin , arayanı n gerçe k bi r çalışa n olu p olmadığın ı kontrol etmede n ve gerekl i önlemler i almada n saldırgan a şirke t ağın a dışarıdan girebilm e hakkın ı tanımas ı b u öykülerde sı k sı k tekrarlana n bir kon u gib i görünüyor . Nede n b u konuy a b u kada r fazl a değiniyoru m dersiniz? Çünk ü bu , pe k ço k toplu m mühendisliğ i saldırısını n e n önem - li unsuru , bi r toplu m mühendisini n amacın a ulaşmasını n e n kola y yoludur. Nede n bi r saldırga n basi t bi r telefo n konuşmasıyl a b u iş i halledebilecekken saatlerc e güvenli k duvarların ı (firevvall) kırmay a uğraşsın?

Toplum mühendisini n b u tar z bi r saldırıy ı gerçekleştirme k içi n kul - landığı e n güçl ü yöntemlerde n biri , saldırganla r tarafında n sıkç a kul- lanılan, yardım a ihtiyac ı olduğ u oyunun u oynamaktır . Çalışanlarınızı n müşterilere v e mesa i arkadaşların a yardımc ı olmaların ı engelleme k istemeyeceğinize gör e onları , bilgisaya r erişim i y a d a gizl i bilgile r tale p eden kişiler e karş ı kullanmalar ı içi n öze l kontro l süreçleriyl e donatmanı z gerekmektedir.

Şirket güvenliğ i süreçleri , çeşitl i durumlard a n e tü r kontro l mekaniz - malarının kullanılacağın ı ayrıntıl ı olara k anlatmalıdır . O n yedinc i bölümde süreçleri n ayrıntıl ı bi r listesin i bulabilirsiniz , anca k işt e siz e gö z önünde bulundurulabilece k bi r takı m kurallar :

• İstekt e buluna n kişini n kimliğin i kontro l etme k içi n kullanılabile -

cek e n iy i yollarda n bir i o kişini n şirke t rehberindek i telefonun u

aramaktır. Eğe r kiş i bi r saldırgansa , o zama n kontro l telef e _ sahte çalışa n diğe r hatt â beklerke n gerçe k kişiyl e konuşma " ya d a çalışanı n bıraktığ ı sesl i mesaj a ulaşı p çalışanı n se s saldırganın sesiyl e karşılaştırmanız ı sağlar .

• Eğe r kimli k kontrol ü içi n şirketinizd e Sosya l Güvenli k

kullanılıyorsa, b u durumd a b u numaraları n hassa s bilg i sa >

ması v e özenl e korunu p yabancılar a verilmemes i gerekmekte c

Aynı şe y dahil i telefon numaraları , biri m fatur a bilgileri , har ;

e-posta adresler i gib i he r türl ü dahil i tanımlayıc ı içi n d e geçerli c

• Şirke t eğitimler i herkesi n dikkatini , yetkil i v e bilgil i göründükle "

için bilinmeye n kişileri n şirke t çalışan ı varsayılmalar ı uygula -

masına çekmelidir . Bi r kişini n şirke t uygulamaların ı bilmes i y a e s

şirket iç i terimler i kullanmas ı kimliğini n kontro l edilmemes i iç r

yeterli nede n değildir .

• Güvenli k görevliler i v e siste m yöneticiler i sadec e herkesi r

güvenlik kuralların a n e kada r uyduğun u görece k şekild e konuy a

odaklanmamalıdırlar. Ayn ı kurallara , süreçler e v e uygulamalar a

kendilerinin uyduğunda n d a emi n olmalıdırlar .

• Parol a v e benzer i şeyler , doğa l olarak , hiçbi r zama n başkasın a

verilmemelidir. Başkaların a verilmeyl e ilgil i kural , zama n taba n

anahtarlar v e diğe r tanımlam a yöntemler i sö z konus u olduğund a

daha d a öneml i olmaktadır . B u unsurlarda n herhang i birini n

başkalarına verilmesinin , şirketi n b u sistemler i kurm a amacın a

bütünüyle aykır ı olduğunu n herkesç e bilinmes i gerekmektedir .

Başkalarına verilmesi , izini n sürülemeyeceğ i anlamın a gelir .

Eğer bi r güvenli k sorun u yaşanırs a y a d a bi r şeyle r ter s giderse , kimin soruml u olduğun u bulamazsınız .

• B u kitapt a he p vurguladığı m gibi , çalışanları n kendilerin e gele n talepleri dikkatl e değerlendirebilmeler i içi n toplu m mühendisliğ i hilelerinin v e tekniklerini n bilincind e olmalar ı gerekmektedir .

Güvenlik eğitimini n bi r parças ı olara k ro l yapm a eğitimlerin i d e göz önün e alabilirsiniz , böylec e çalışanlarını z toplu m mühen - disinin nası l çalıştığın ı dah a iy i anlayabilirler .

DÜZMECE SİTELE R

TEHLİKELİ EKLE R

"Karşılıksız hiçbi r şe y olmaz " diy e esk i bi r sö z vardır . Bun a karşı n bedava bi r şeyle r sunm a tuzaklar ı he m yasa l ("Am a durun-dahas ı var ! Hemen arayı n v e yanınd a bi r bıça k set i bi r d e mısı r patlatm a makinas ı verelim!") he m d e o kada r d a yasa l olmaya n ("Florida'd a bi r dönü m bataklık arazis i alın , ikinc i dönü m bedavay a gelsin!") işle r içi n öneml i bi r ilgi çekm e yol u olmay ı sürdürüyor .

Pek çoğumu z bedav a birşeyle r eld e etmey e o kada r hevesliyi z k i yapılan öner i y a d a verile n sö z üzerind e mantıkl ı düşünemeyece k durumda olabiliyoruz . Şu yaygı n uyarıy ı hepimi z biliyoruz ; "müşterileri n dikkatine"; am a artı k başk a bi r uyarıy ı dah a dikkat e almanı n zaman ı geldi: Bedav a yazılımlar a v e "had i tıkla " diye n e-post a eklerin e dikkat . Bilinçli bi r saldırgan , bi r şirke t ağın a girebilme k içi n bedav a bi r hediyey e karşı duyduğumu z doğa l dürtüy e hita p etme k dahil , neredeys e he r yol u kullanacaktır. İşt e birka ç örnek .

Bedava Bi r (Boşluk) İsteme z Miydiniz ?

Tıpkı virüsleri n zamanı n başlangıcında n b u yan a insanoğlunu n v e tıp uzmanlarını n başın a bel a olmalar ı gibi , ço k isabetl i biçimd e adlandırılmış bilgisaya r virüsler i d e teknoloj i kullanıcılarını n başına ben - zer bi r bel a açmışlardır . E n ço k zara r vere n virüsler , -hi ç d e tesadü f olmayan bi r biçimde - e n ço k ilgiy i toplaya n v e gö z önünd e bulunanla r olmuştur. Bunla r bilgisaya r varidatlarının ürünleridir .

Kötü huyl u bilgisaya r vandalların a dönüşe n bilgisaya r hastaları , n e kadar zek i oldukların ı gösterebilme k içi n uğraşı p didinirler . Baze n yaptık - larıyla bi r kabu l törenindeymi ş gib i dah a yaşl ı v e deneyiml i bilgisaya r kor - sanlarını etkileme k amacındadırlar . B u insanlar , zara r verme k üzer e tasar - lanmış bi r virü s y a d a soluca n yaratmay a güdülenmişlerdir . Eğe r yaptıklar ı iş dosyalar ı yo k edip , sabi t sürücüler i göçertiyors a v e kendin i gizlic e bin - lerce insan a gönderebiliyorsa , Vandalla r başarılar ı karşısınd a gururl a kabarırlar. Eğe r virüs , gazeteleri n yazacağ ı kada r v e an a haberlerd e on a karşı uyarıla r yayınlanaca k kada r kargaş a yarattıys a dah a d a iy i olur .

Vandallar v e virüsleriyl e ilgil i pe k ço k şe y yazıldı ; kitaplar : yazılımlar ; ayrıca korum a sağlama k içi n şirketle r kuruld u am a bi z burad a onları n teknik saldırıların a karş ı savunmalarda n sözetmeyeceğiz . Bizi m ş u ank i ilgi noktamı z vandalı n yıkıc ı hareketlerinde n ço k onu n uzakta n akrabas ı olan toplu m mühendisini n maksatl ı çabalar ı üzerind e olacak .

E-posfayla Geld i

Her gü n rekla m mesajlar ı içere n y a d a n e istediğiniz , n e d e ihti - yacınız ola n birşeyler i bedav a olara k suna n istenmeye n e-postala r alı - yorsunuzdur. Nası l şeyle r oldukların ı biliyorsunuz . Yatırı m danışmanlığı , bilgisayarlar, televizyonlar , kameralar , vitaminle r y a d a seyahatle r içi n indirimler; ihtiyacını z olmaya n kred i kartlar ı içi n fırsatlar ; ücretl i televiz - yon kanalların ı bedav a seyretmeniz i sağlayaca k bi r cihaz ; sağlığınız ı y a dJ15QKs gücünüz ü artırmanı n yollar ı v e dah a nele r neler .

Ama arad a bir , elektroni k post a kutunuzd a sizi n d e ilginiz i çeke n bi r teklif gözünüz e ilişebilir . Belk i bedav a bi r oyundur , e n sevdiğini z yıldızı n 9 4 fotograflık albümüdür , bedav a bi r takvi m programıdı r y a d a bilgisayarınız ı virüslere karş ı koruyaca k ço k uygu n fiyatl ı bi r paylaşı m yazılımıdır . Sunulan herneyse , denemeni z içi n siz i ikn a etmey e çalıştığ ı dosyay ı indir - meniz içi n siz i yönlendirir .

Ya d a belk i kon u satırınd a "Dan , sen i özledim " y a d a "Anna , nede n bana yazmadın " y a d a "Sela m Tom , işt e san a sö z verdiği m seks i fotoğraf gib i şeyle r yaza n mesajla r alırsınız . Böylec e fotoğraf a bakma k ya d a mesaj ı okuma k içi n ek i açarsınız .

Tüm b u hareketle r -rekla m e-postalarında n öğrendiğini z yazılımlar ı indirmek, siz i dah a önc e duymadığını z bi r sitey e yönlendirece k bi r bağlantıya tıklamak , tanımadığını z birinde n gele n bi r ek i açmak - belay a davetiye çıkarmaktır . Ş u d a va r ki , çoğ u zama n n e bekliyorsanız ta m olarak on u görürsünü z y a d a dah a kötüs ü ümitlerini z boş a çıka r y a d a sevimsiz şeylerl e karşılaşırsını z am a bunla r zararsızdır . Am a bazen , karşınıza çıka n şe y bi r vandalı n eseridir .

Bilgisayarınıza köt ü huyl u bi r ko d gönderme k saldırını n yalnızc a küçük bi r parçasıdır . Saldırını n başarıl ı olabilmes i içi n saldırganı n siz i eki indirmey e ikn a etmes i gerekir .

En ço k zara r vere n köt ü huyl u solucanları n birkaçın ı belirtme k gerekirse, Lov e Letter , SirCa m v e Ann a Koumikov a gibi , heps i d e yayıla - bilmek içi n toplu m mühendisliğ i aldatm a tekniklerin e dayanmışla r v e birşeyleri karşılıksı z eld e etm e isteğimizde n yararlanmışlardı . Solucan , gizli bilgile r v e bedav a porn o gib i ilg i çekic i bi r şe y suna n y a d a ço k zekice bi r hileyle , sizi n güy a sipari ş etmi ş olduğunu z ço k pahal ı bi r eşyanın faturasını n ekt e olduğun u söyleye n bi r mesa j içere n bi r

IXI v j i * Bilgisayar dünyasında Uzaktan Erişindi TruvaAtı (Remote Access Trojan) olarak bilinen bir çeşit program, saldırganın bilgisayarınız üzerinde tam bir kontol kurmasını sağlar, tıpkı sizin klavyenizin başında oturuyormuş gibi!

Düzmece Sitele r v e Tehlikel i Ekle r 8 7

e-postanın ek i olara k gelir . B u so n tuza k i Z . ' 7 • " ~ i kredi kartınızda n sipari ş etmediğini z bi r ı T©riml© r | ürünün parasını n çekildiğ i endişesiyl e

sizi ek i açmay a yönlendirir .

MALWARE (Kötü huylu \

yazılımın argo karşılığı) bir j

Ne kada r ço k insanı n b u tuzaklar a

virüs, solucan ya da Truva I düştüğünü bilme k şaşırtıcıdır ; e-post a

Atı gibi zarar verici işlemler j eklerini açmanı n tehlikeler i konusund a \ yapan bilgisayar programı. tekrar tekra r uyarılmamız a rağme n

tehlikeye karş ı duyarlılığımı z zama n

içinde azalı r v e he r birimiz i savunması z bırakır .

Zararlı Yazılımları n Belirlenmes i • ' • ;• • • •

Başka türl ü bi r zararlı yazılım (malvvare-maliciou s softvvare) is e sizi n bilginiz y a d a onayını z dışınd a çalışa n v e si z farkınd a olmada n görevi - ni yerin e getire n bi r program ı bilgisayarınız a yükler . Zararl ı yazılımla r başta oldukç a masu m görünebili r hatt â bi r VVord ™ doküman ı y a d a Povverpoint™ sunum u y a d a makr o işlevler i ola n herhang i bi r progra m olabilir am a bunla r başk a bi r program ı gizlic e yükleyeceklerdir . Örneğin , zararlı yazılım , Bölü m 6'd a söz ü edile n Truv a Atı'nı n bi r çeşid i olabilir . Bu yazılı m makinanız a bi r ke z kuruld u mu , yazdığını z he r karakter i -tü m parolalarınız v e kred i kart ı numaralarını z dahil - saldırgan a bildirir .

Şok edic i bulabileceğini z başk a ik i tü r zararl ı yazılı m dah a var . Bi r tanesi saldırgan a bilgisaya r mikrofonunuzu n civarınd a konuştuğunu z her kelimey i bildiri r (mikrofonunuzu n kapal ı olduğun u düşündüğünü z zaman bile) . Dah a d a kötüsü , bilgisayarınız a bağl ı bi r kameranı z varsa , bir saldırgan , benze r bi r tekni k kullanara k terminalinizi n önünd e olu p biten he r şeyi , kameranı n kapal ı olduğun u düşündüğünü z zama n bile , gece y a d a gündüz , seyredebilir .

Kötü bi r şak a anlayış ı ola n bi r korsan , hınzırlıklarıyl a rahatsı z edic i olmak üzer e tasarlanmı ş küçü k bi r program ı bilgisayarınız a kurmay a çalışabilir. Örneği n C D sürücünüz ü ansızı n açabili r y a d a üzerind e çalıştığınız dosyay ı sürekl i simg e durumun a küçültebilir . Y a d a geceni n ortasında çığlı k yükl ü bi r se s dosyasını n e n yükse k sesl e çalmasın a neden olabilir . Uyumay a y a d a i ş yapmay a çalşırke n bunları n hiçbir i eğlenceli gelmeyecektir.. . am a e n azında n kalıc ı zara r vermezler .

Mitnick Mesajı :

Hediye veren saçmalıklara dikkat edin, yoksa şirketinizin başına Truva ken- tinin başına gelenler gelebilir. Ne yapmanız gerektiğini bilemiyorsanız, bir şey- lerin bulaşmasını engellemek için koruma kullanın.

Bir Arkadaşta n Mesa j

Aldığınız önlemler e karşı n senaryola r dah a d a vahimleşebilir . Düşünün : Şansınızı hi ç zorlamamay a kara r verdiniz . Artı k bildiğini z v e güvendiğiniz , SecurityFocus.com y a d a Amazon.co m gibi , güvenlikl i sitele r dışınd a hiçbi r yerden dosy a indirmemey e kara r verdiniz . Bilinmeye n kaynaklarda n gele n e-postalardaki bağlantılar a artı k tıklamıyorsunuz . Beklemediğini z hiçbi r e-postadak\ et a açmamay a kara r verdmiz. . V e e-ticare t işlemler i yapma k y a da kişise l bilgile r alı p verme k içi n girdiğini z sitelerd e güvenl i sit e simges i olduğundan emi n olma k içi n interne t tarayıcınız ı kontro l ediyorsunuz .

Ve bi r gü n bi r dostunuzda n y a d a i ş arkadaşınızdan , ek i ola n bi r e-posta alıyorsunuz . İy i tanıdığını z birinde n geliyors a zararl ı bi r şe y ola - maz, deği l mi ? Özellikl e d e bilgisaya r verilerini z zara r görürs e kim i

bildiğiniz, sürece .

Eki açıyorsunu z ve.. . GÜÜM ! A z önc e bi r soluca n y a d a Truv a At ı tarafından vuruldunuz . Tanıdığını z bir i nede n siz e bun u yapsın ? Çünk ü herşey göründüğ ü gib i değildir . Şun u okumuştunuz : Birini n bilgisayarın a giren v e sonr a d a kendin i o kişini n adre s listesindek i herkes e postalaya n solucan. Tü m b u insanla r d a bildikler i v e güvendikler i birinde n bi r e-post a almışlardı v e b u güvenili r e-postaları n he r birinde , durgu n bi r göl e atılmı ş bir taşı n yarattığ ı halkala r gib i kend i kendin i dağıta n solucanla r d a vardı .

Bu tekniği n b u kada r etkil i olmasını n neden i bi r taşl a ik i ku ş vurm a kuramına dayanır : Diğe r kuşkulanmaya n kurbanlar a yayılm a beceris i v e güvenilir birinde n geliyormu ş gib i görünmesi .

Teknolojinin bugünk ü seviyesinde , yakı n birinde n gele n bi r e-postanı n bile güvenl i olu p olmayacağın ı düşünüyo r olmanı z yaşamı n üzüc ü bi r gerçeğidir.

içinde bulunduğumu z bilg i çağında , görmey i beklemediğini z bi r internet sitesin e yönlendirilmey i d e içere n bi r dolandırıcılı k çeşid i dah a var. B u sı k sı k olu r v e değişi k şekillerd e karşımız a çıkar . Aşağıdak i örnek, intemet't e dolaşa n gerçe k bi r dümen e dayana n tipi k bi r örnektir .

İnsan, dünyayı ve kendi yaşam tarzım değiştiren pek çok harika şey keşfet- miştir. Ancak teknolojinin her iyi kullanımı için, ister bilgisayar, ister tele- fon ya da internet olsun, birileri her zaman bunu kendi çıkarları için kötüye kullanmanın yolunu bulurlar.

Düzmece Sitele r v e Tehlikel i Ekle r 8 9

Mutlu Noelle r . . .

Edgar adınd a emekl i bi r sigort a satıcıs ı bi r gü n PayPal'da n bi r e-posta alır . PayPal , hızl ı v e elverişl i koşullarl a çevri m iç i ödem e olanakları suna n bi r şirketti r v e b u tar z bi r hizmet , özellikl e ülkeni n (hatt â dünyanın) herhang i bi r yerind e otura n biri , tanımadığ ı birinde n bi r ma l satm alırke n kullanışlıdır . PayPal , alıcını n kred i kartında n tutar ı çeke r v e parayı doğruda n satıcını n hesabın a aktarır .

Bir antik a ca m kavano z koleksiyoncus u olara k Edga r çevri m iç i müzayede şirket i ola n eBa y aracılığıyl a birço k ke z i ş yapmıştır . PayPal' ı sık sı k kullanır , baze n haftad a birka ç ker e d e kullandığ ı olur . B u yüzde n 2001 tati l dönemind e aldığı , PayPal'da n geliyo r gib i görüne n v e PayPa l hesabını güncellemes i karşılığınd a bi r ödü l suna n bi r e-post a Edgar'ı n ilgisini çeker . Mesa j şöyledir :

Mutlu Yılla r Değerl i PayPa l Müşterisi ;

Yeni yı l yaklaşırke n v e hepimi z bi r yı l dah a ilerlerke n PayPa l siz e hesabınız a

5 dola r kred i ekleme k istiyor !

5 dolarlı k ödülünüz ü alabilmeni z içi n tü m yapmanı z gereken , 1 Oca k 200 2

tarihine kada r bilgileriniz i güvenl i Pa y Pa l sitemizde n güncellemektir .

Bizdeki bilgileriniz i güncelleyere k si z değerl i müşter i hizmetlerimiz e

mükemmel bi r hizme t verm e olanağ ı tanımı ş v e b u sırad a kayıtlarımız ı

doğru tutmamız ı sağlamı ş olacaksınız !

Bilgilerinizi şimd i güncelleme k v e PayPa l hesabınız a 5 dola r ekleme k içi n

bu bağlantıy ı tıklayınız : http://www.paypal-secure.com/cgi-bin .

PayPal.com sitesin i kullandığını z v e biz e türümüzü n e n büyüğ ü olmad a

yardımcı olduğunu z içi n teşekkü r ederiz !

En içte n dileklerimizl e ço k "Mutl u Noelle r v e Mutl u Yıllar, "

PayPal Ekib i

Edgar e-postayl a ilgil i birşeyleri n ter s olduğun u göstere n hatal ı ayrıntıları d a farketmemişt i (örneğin , selamlam a cümlesinde n sonrak i noktalı virgü l v e "değerl i müşter i hizmetlerimiz e mükemme l bi r hizmet " diyen bozu k cüml e gibi) . Link i tıkladı , istene n bilgiler i -ad , adres ,

telefo n numarası v e kred i kart ı bilgileri - gird i v e be ş dolarlı k kredisin i bi r sonra - ki kred i kart ı ekstresind e görme k içi n oturu p beklemey e başladı . Onu n yerine gördüğü , hiçbi r zama n almadığ ı eşyalar a ai t bi r ödem e listesiydi .

Ç 2\vi m iç i alışveri ş yapmay a yanaşmayan , Amazo n \«r- .. ; • 'T3 rKa olmu ş şirketlerde n y a d a Ol d Navy , Targe t y a 6-. . "S,

o,...:.. •..-• " ' " ' " ' 3i r

ta'aft^p b^ınc a kuşkuıartiYıiaMS » naKİıiai 1. c Mw ,i.^,:..- . .::..-'••.•::.:. z

buaünün sian.-ıard ı ola n 128-bi t şifrelem e kullanıyo r OÜV^H ; oı r

s»^,o .«ö-Hpajjğini z bilgile r bilgisayarınızda n şifrel i o.c.-s. . •....'..; • -

d'û7^w-- : - büyü k bi r çab a sarfedilere k deşifr e odı.ooıli.ife. - -Yı a

bnv^s-K-a maku l bi r sür e içerisind e kırılmazlar ; bun u belK i bi r

tek Ulusa l Güvenli k Ajans ı (NSA > başarabili r (v e bildiğimi z kad&ny -

la NSA'n. n n e Amerika n vatandaşlarını n kred i kar t numar a arın . cal -

r',1;-.,? - e d e kimleri n pornografi k vide o kasetle r y p - 3 fantez i i ç

çamaşırları aldıâın ı bulmay a yöneli k bi r ilgis i vardır) .

j

QI c.if r ^valar , aslın* . • m ~ J "*' '"'"\\

hernsV.J-i Jt f UY S finda n kırılabilir . Am a gerçeğ e • > * > v ŞPıal , u, r ,< , so . kcrt, mİmaras ! çalma k içi n tü m b u emeğ i saıfsd&r ; V'.cs c d ? ps: ? ÇO K

e"Lica, :ef «irfcs ^ müşterilerini n ftnansa l bilgilerin i şifrelenmemi ş verı -

fo^^nnda saklam a hatasm , yaparken ? Dah a d a kötüsü , beli , bi r

sVv 3,-.taban. kullana n baz ı e-ticare t şirketler i sorunu , fen a hald e

nendirler: Programı n imalatta n gele n siste m yönet.cs , şjfresınıhı ç

;•,= •:-•-.o^iciprrii r Yazılım ı kutusunda n çıkardıklannda , şrfres ı

«bo^İ'^u.-"^ ^ "boşluk " olara k kalmay a deva m eder . B u

Re^:.!. »opo^nırı m içeriğ i veritaban ı sunucusun a bağlanmay ı

denemeye ka.*, - vermi ş internet'tek i herkes e açiKc. r ^^ ^

zaman S3.!d !r! altındadı r « e aııoııe r oe\ çeKıe.: C o y ^. •••-•• ' -•• - •"• • •

senin ruh u GUVMÎC.:"L.". .

'3ğı korkuş""i' 5 üver -

yapmayan ayn ı insanlar , kred i kartların ı tuğl a v e

i bi r dükkânda n al.şveri ş ederke n kullanmakt a y a

beionoan yapıımı ş u« UUMOIMO

„.; w * -—ğ i akşa m yemeğ

ği

M ™«C"" S . -

vey

i ikili

a içkilerin ii ödeme

ödeme

kk içi

.çı

nn anneler

anneler

.

--

nî"bîle ^üin.eyeceMer i ark a soka k barlarınd a v e lokantalarınd a kul -

ı-nm-'V b'«- «adınc a görmezler . Kred i kart ı slipler ı b u \acz\-- "-~-r -

s1jre ;d! çai'ir... - -- s d = ark a sokaktak i çö p kutularında n arakıar.n . v e

"l rh,no: bi r «hiaks. z kasiye r y a d a garson , admız , v e kred , kan,_n,, -

âiio'.^ :- : •-••• - •- - ^r a no t edebili r y a d a içinde n geçirile n herhang i bi r

kr«rti"i^n-in & »= x bilgiler i sonrada n rahatç a kullanılma k üzer e sak -

isi.- v s T.^T.stt e kolayc a bulunabile n bi r kar t tokatlam a alet i kul -

r^,r^ iç i alışveri ş etmeni n tehliKeier i vatu » an-.a UÜ/Ü, ; GIŞS:|::' . la ûâ* v betonda n yapılmı ş
bi r dükkânda n alışveri ş yapma k kada r .nv^Hi^r w -o kred i kart ı şirketleri , kartınız ı çevri m iç i

kullanırke n de siz e ayn ı korumay ı sağlarla r -eğe r hesabınızda n siz e ai t olmaya n harcamalar yapılmışs a bunu n yalnızc a

Su vüzde n beni m görüşüm e gör e çsv.i m iç i SI^-MÜ ? v^n'iaı^a. . çeklpme!; başk a bi r kurunt u olmakta n ötey e gu.r.c:.: .

Düzmece Sitele r v e Tehlikel i Ekle r 9 1

Mitnick Mesajı :

Tam anlamıyla mükemmel bir gösterge olmasa da, her ne zaman bir site siz- den özel olduğunu düşündüğünüz bir bilgi istiyorsa, bağlantının belgeli ve şifreli olduğundan mutlaka emin olun. Ve daha da önemlisi, geçersiz, süresi dolmuş ya da iptal edilmiş dijital sertifikalar gibi, bir güvenlik sorunu gösteren herhangi bir iletişim kutusunda hemen Evet'i tıklamayın.

Aldatmacanın İncelenmes i

Edgar yaygı n kullanıla n bi r interne t dümenin e yakalanmıştı . Bu , çeşitl i sekilerde karşımız a çıka n bi r dolandırıcılı k türü . Dokuzunc u bölümd e anlatılan bi r tanes i tıpk ı asl ı gib i olup , saldırga n tarafında n ye m olara k yaratılmış bi r bağlanm a sayfasın ı içerir . Farkı , saht e sayfanın , kullanıcını n ulaşmak istediğ i bilgisaya r sistemin e erişi m sağlamamasıdır ; bunu n ye - rine kullanıcı , adın ı v e parolasın ı bilgisaya r korsanın a vermi ş olur .

Edgar, haydutları n "paypal-secure.com " adınd a -yasa l PayPa l site - sine ait , güvenl i bi r sayf a olmas ı gerekirmi ş gib i görüne n am a öyl e olmayan- bi r interne t adres i satı n aldığ ı bi r dümen e yakalanmıştır . Bilgileri o sitey e girdiğinde , saldırganlar a ta m istedikler i şey i vermiştir .

Çeşitleme Üzerin e Çeşitlemele r

Bilgisayar kullanıcıların ı gizl i bilgilerin i girebilecekler i düzmec e inter - net sitelerin e gitmeler i içi n kandırmanı n ka ç değişi k yol u olabilir ? Kimsenin geçerli , kesi n bi r yanıt ı olduğun u sanmıyoru m anca k "ço k am a çok" diy e bi r ceva p verebiliriz .

Kayıp Bağlant ı . ~ \ ' . • -

Bir hil e sürekl i karşımız a çıkar : Bi r sitey i ziyare t etme k içi n çekic i bi r neden suna n bi r e-post a gönderi p doğruda n oray a yönlendire n bi r bağlantı sağlamak . Farkl ı olarak , bağlant ı siz i gittiğiniz i düşündüğünü z siteye götürme z çünk ü bağlant ı aslınd a gerçe k sit e içi n ola n bağlantıy ı taklit eder . işt e internett e gerçekte n kullanılmı ş başk a bi r örnek , yin e çok suistima l edile n PayPal'ı n adın ı kullanmaktadır :

www.PayPai.com . •

Hemen bakıldığınd a burad a PayPa l yazıyormu ş gib i görünüyor . Kurban farkets e bil e yazıdak i küçü k bi r hatanı n " I " harfini " i " gib i gös - terdiğini düşünebilir . V e kim , baka r bakma z aşağıdak i linkt e küçü k har f L yerin e 1 sayısını n kullanıldığın ı farkedebilir ?

www.PayPal.com

Bu dalaverey i kred i kart ı haydutlar ı arasınd a sürekl i popüle r kılaca k kadar ço k yanlı ş yazımlar ı v e hatal ı yönlendirmeler i doğruymu ş gib i kabullenecek insa n var . İnsanla r düzmec e sitey e gittiklerinde , oras ı git- meyi umduklar ı ye r gib i görünü r v e kred i kart ı bilgilerin i huzu r içind e gi - rerler. B u dalaverelerde n birin i kurma k içi n saldırganı n te k yapmas ı gereken, düzmec e bi r sit e ad ı almak , e-postaların ı gönderme k v e ena - yilerin dolandırılma k içi n sitey e girmelerin i beklemektir .

2002'nin ortalarınd a bi r e-post a aldım ; görünüş e gör e "ebay@ebay.com"dan, bi r defad a pe k ço k adres e gönderilmişti . Mesa j Şekil 7.1'd e sunulmuştur .

Bağlantıyı tıklaya n kurbanla r eBa y sayfasın a ço k benzeye n bi r we b sayfasına gittiler . Aslınd a sayfa , özgü n eBa y amblem i v e "Ara" , "Sat " gibi, tıklandığınd a ziyaretçiy i gerçe k eBa y sayfasın a götüre n diğe r ge - zinme bağlantılarıyl a iy i tasarlanmıştı . Sa ğ al t köşed e bi r güvenli k sim - gesi d e bulunmaktaydı . Bilgisi z kurban ı kandırma k amacıyl a tasarımcı , kullanıcının sağladığ ı bilgileri n nerey e gönderildiğin i gizleme k içi n HTML şifrelemes i bil e kullanmıştı .

Kötü niyetli , bilgisaya r tabanl ı toplu m mühendisliğ i saldırısını n mükemmel bi r örneğiydi . Yin e d e kusursu z değildi .

E-posta mesaj ı ço k iy i yazılmamıştı ; özellikl e d e "B u duyuruy u eBay'den aldınız"l a başlaya n paragra f acemic e v e saçmayd ı (b u oyun - lardan soruml u kişile r yazdıkların ı kontro l etmes i içi n hiçbi r zama n deneyimli birin i tutmazla r v e b u heme n farkedilir) . Ayrıc a dikkatl i bir i eBay'in ziyaretçin e PayPa l bilgilerin i sormasında n kuşkulanırdı ; eBay'ı n müşterisine başk a bi r şirketl e ilgil i öze l bilgilerin i sormas ı içi n hiçbi r neden olamaz .

Ve interne t konusund a bilgil i herhang i bir i bağlantını n eBa y sayfası - na değil , ücretsi z bi r interne t hizme t sağlayıcıs ı ola n tripod.co m sayfası - na yönlendirildiğin i anlayacaktır . Bu , e-postanı n yasa l olmadığını n ta m bir göstergesidir . Yin e d e emini m pe k ço k insan , kred i kart ı numaralar ı dahil, istene n bilgiler i b u sayfay a girmişlerdir .

|N| \ J i î Neden insanların yanıltıcı veya uygunsuz alan adları almalarına izin veriliyor? Çünkü geçerli kanun ve çevrimiçi çalışma kuralları uyarınca, isteyen, kullanımda olmayan bir site adını alabilir. Şirketler taklit adreslerin kullanımıyla mücadele etmeye çalışıyorlar ama neye karşı olduklarını bir de siz düşünün. General Motors, f**kgeneral- motors.com adresini (yıldızlar olmadan) alıp URL'yi General Motors'un internet sitesine yönlendiren bir şirkete dava açtı. G.M. kaybetti.

Düzmece Sitele r v e Tehlikel i Ekle r 9 3

msj: Sevgil i eBa y Kullanıcısı ,

Başka şahısları n eBa y hesabınız ı uygunsu z oiara k kullandıklar ı oldukça far k edili r bi r ha l almıştı r v e Kullanıc ı Anlaşması'nı n ş u maddes i ihlal edilmiştir :

4. Fiya t Verm e v e Satı n Alm a •

Sabit fiyatl ı düzenlemelerimizde n bir i aracılığıyl a bi r ma l aldığını z vey a aşağıda açıklandığ ı üzer e e n yükse k fiyat ı verdiğini z takdird e satıcıyl a aranızdaki işlem i tamamlamanı z gerekmektedir . Eğe r bi r açı k artırm a sonunda e n yükse k fiyat ı vermişseni z (geçerli e n düşü k fiya t v e ihtiya t yükümlülüklerini karşılamak kaydıyla) v e verdiğini z fiya t satıc ı tarafında n kabul edilmişse , satıcıyl a İşleminiz i tamamlamanı z gerekmektedir . Aks ı halde, işle m kanune n vey a b u Anlaşm a gereğinc e yasaklanır .

Bu duyuruy u eBay'de n aldını z çünk ü ş u ank i hesabınızı n diğe r eBa y üyeleriyle uyuşmazlıkla r yaratmas ı dikkatimiz i çekt i v e eBay , hesabınızı n en kıs a süred e onaylanmasın ı gerekl i bulmaktadır . Lütfe n hesabınız ı onaylayınız aksi hald e hesa p ipta l edilebilecektir . Hesabınız ı Onaylama k için Buray ı Tıklayını z - http://error__ebay.tripod.co m , • .

Belirtilen ticar i markala r v e işaretle r sahiplerin e aittir . eBa y v e eBa y

amblemi eBa y Inc.' e ai t ticar i markalardır .

Şekil 7. 1 B u v e benzer i e-postalardak i bağlantıla r dikkatl e kullanılmalıdır .

İnternetin bireyse l kullanıcılar ı olara k hepimizi n uyanı k olmamız ; kişisel bilgilerin , şifrelerin , hesa p numaralarının , PIN'leri n v e bunu n gib i şeylerin n e zama n girileceğin e bilinçl i bi r şekild e kara r vermemi z gerekir.

Baktıkları bell i bi r interne t sayfasının , güvenl i bi r sayfanı n taşımas ı gereken şartlar a uyu p uymadığın ı söyleyebilece k ka ç kiş i tanıyor - sunuz? Şirketinizi n ka ç çalışan ı ney e bakmas ı gerektiğin i biliyor ?

İnternet kullana n herke s genellikl e siteleri n bi r yerlerind e belire n v e bir asm a kilid e benzeye n ufa k şekli n n e olduğun u bilmeli . Kili t kapal ı olduğunda siteni n güvenl i olara k sertifikalandığın ı anlamalıdır . Kili t açı k olduğu zama n y a d a kili t gözükmediğind e sit e özgü n bi r sit e olara k bel - gelenmemiştir v e gönderile n herhang i bi r bilg i açıktadır ; yani , şifrelen - memiştir.

Terimler

Her şey e karşı n bi r şirke t bilgisa -

yarının yönetimse l ayrıcalıkların ı eld e

etmeyi başarmı ş bi r saldırgan , kul -

ARKA KAPI: Kullanıcının

lanıcının gerçekt e n e olduğ u doğrul -

bilgisi dışında bilgisayara

tusundaki görüşün ü değiştirme k içi n

gizli bir yol sağlayan üstü

işletim sistem i kodun a yamala r yapabili r kapalı bir giriş noktası. Bir

ya d a üzerind e oynayabilir . Örneğin , bi r

yazılım programı

internet sitesini n dijita l sertifikasını n

geliştirirken programcılar

geçersiz olduğun u belirleye n İnterne t

tarafından da kullanılır,

tarayıcısı yazılımındak i progra m kod -

böylece sorunları çözmek

larını, kontrol ü aşabilme k içi n değişti -

için programa girebilirler.

rilebilir. Y a d a siste m kö k donanım ı ad ı

verilen birşeyl e değiştirebilir ; işleti m sis -

temi düzeyind e bi r y a d a dah a fazla , bulunması dah a gü ç arka kapı yükleyebilir .

Güvenli bi r bağlantı , sitey i özgü n olara k tanımla r v e iletile n bilgiy i şifreler, böylec e bi r saldırga n eld e ettiğ i veriler i kullanamaz . Bi r interne t sitesine, hatt â güvenl i bağlant ı kullana n birisin e güvenebili r misiniz ? Hayır, çünk ü sit e sahib i gerekl i tü m güvenli k yamaların ı uygulamakt a y a da kullanıcılar ı v e yöneticiler i doğr u şifr e uygulamalar ı konusund a zor - lamakta yetersi z kalabilir . B u yüzde n güvenl i görünen bi r siteni n saldırıya açı k olmadığın ı varsayamazsınız .

Güvenli HTT P (hypertex t transfe r protocol) vey a SS L (secur e socket s layer) dijita l sertifikalar ı yalnızc a uzaktak i sitey e gönderile n bilgiy i şifrelemekte kullanılmaz , ayn ı zamand a belgelem e yapma k içi n d e (doğru interne t sitesiyl e iletişi m kurduğunuz u doğrulama k amacıyla) otomatik bi r mekanizm a sağlar . Anca k b u korum a mekanizması , adre s çubuğunda görüne n site'adının , gerçekte n d e ulaşma k istediğ i sit e olu p olmadığına dikka t etmeye n kullanıcıla r sö z konus u olduğund a iş e yarayamaz.

Genellikle gö z ard ı edile n başk a bi r güvenli k konusu , karşımız a şunun gib i bi r uyar ı mesajıyl a çıka r "B u sit e güvenl i değ i l y a d a güven - lik sertifikasını n süres i dolmuş . Yin e d e deva m etme k istiyo r musunuz? " Pek ço k interne t kullanıcıs ı mesaj ı anlama z v e ortay a çıktığınd a heme n "Tamam" y a d a "Evef' e tıklayarak , bi r batağı n içind e olabileceğini n farkında olmada n işin e deva m eder . Dikka t edin ; güvenli k protokol ü kul- lanmayan bi r interne t sitesind e adresiniz , telefo n numaranız , kred i kart ı veya bank a hesa p numaranı z gib i kişise l bilgileriniz i y a d a öze l kalmasını istediğini z herhang i bi r şeyler i kesinlikl e girmemelisiniz .

Thomas Jefferso n özgürlüğümüz ü sürekl i tutmanı n "he r zama n tetikte" olmakta n geçtiğini söylemiştir . Bilgiy i değiştoku ş arac ı olara k kullanan bi r toplumd a öze l yaşam ı koruma k v e güvenliğ i sağlama k d a bir o kada r öze n gerektirir . .

Düzmece Sitele r v e Tehlikel i Ekle r 9 5

Virüslere Duyorİ i Olma k

Virüs yazılımlarıyl a ilgil i öze l bi r not : Virü s yazılımlar ı şirke t intranet i için önemlidi r am a ayn ı zamand a bilgisaya r kullana n he r çalışa n içi n d e önemlidir. Makinaların a virü s korum a yazılım ı yüklemi ş olma k bi r yana , kullanıcıların yazılım ı açı k tutmalar ı d a gereki r (b u pe k ço k insanı n sevmediği bi r şeydi r çünk ü bilgisayarı n baz ı işlevlerin i kaçınılma z olara k yavaşlatır).

Virüs korum a yazılımlarıyl a ilgil i akıld a tutulmas ı gereke n bi r başk a önemli nokt a dah a vardır : Virü s tanımların ı günce l tutmak . Şirketiniz , yazılımı y a d a güncellemelerin i a ğ üzerinde n dağıtma k üzer e yapı - landırmadığı sürece , he r bire y e n so n virü s tanımlar ı dosyasın ı kend i başına indirm e sorumluluğunu , taşımalıdır . Kend i kişise l öneri m herkesin virü s yazılım ı seçeneklerin i v e virü s tanımların ı he r gü n gün - cellenecek şekild e ayarlamalarıdır .

Basitçe söyleme k gerekirse , virü s tanımlarını z düzenl i olara k gün - cellenmiyorsa savunmasızsınızdır . Böyleyke n bile , virü s korum a yazılımı geliştire n şirketleri n henü z bilmediğ i y a d a bi r tanımlam a mo - deli çıkarmadıkları virü s v e solucanlar a karş ı ta m olara k korunuyo r sayılmazsınız.

Evdeki bilgisayarlar ı y a d a dizüst ü bilgisayarlar ı üzerinde n uzakta n erişim hakk ı tanınmı ş tü m çalışanları n b u makinala r üzerind e e n azın - dan güncellenmi ş virü s yazılım ı v e bi r kişise l güvenli k duvar ı bulundur - ması gerekir , işin i bile n bi r saldırga n e n zayı f noktay ı bulma k içi n büyü k resme bakı p orada n saldıracaktır . Uzakta n erişimler i ola n kişileri n kişisel güvenli k duvarlar ı v e güncellenmi ş antivirü s yazılımını n gerekler i konusunda düzenl i olara k uyarılmalar ı bi r şirke t sorumluluğudur ; çünk ü BT müdürlüğünde n uza k ola n bireyse l çalışanların , yöneticilerin , satı ş sorumlularının v e diğerlerini n bilgisayarların ı koruması z bırakmalarını n getireceği tehlikeler i hatırlamaların ı bekleyemezsiniz .

Bu adımları n dışında , dah a a z yaygı n am a dah a a z öneml i olmayan , Truva At ı saldırıların a karş ı korum a sağlaya n yazılı m paketlerinin , diğe r adıyla anti-Troja n yazılımlarını n kullanılmasın ı şiddetl e öneririm . B u

kitap yazıldığ ı sırad a iy i biline n program -

Terimler

lardan ik i tanes i şunlardır : Th e Cleane r

(www.moosoft.com) v e Troja n Defenc e

SSL (Güvenli Yuva

Sweep (www.diamondcs.com.au) . Katmanı): Hem istemcinin Sonuç olarak , a ğ geçitlerind e hem de sunucunun internet tehlikeli e-postalar a karş ı taram a yap - üzerinden güvenli iletişimle mayan tü m şirketle r içi n olabilece k e n

belgelenmesini sağlayan önemli güvenli k mesaj ı ş u olabilir :

Netscape tarafından Hepimiz unutm a eğiliml i olduğumuz a

geliştirilmiş bir protokol. veya işimiz i yaparke n kenard a kala n

şeyleri ihma l ettiğimiz e göre , güvenilebilece k bi r kiş i y a d a kuruluşta n gelmediği sürec e e-post a eklerin i açmamalar ı konusund a çalışanların , farklı şekillerde , tekra r tekra r uyarılmalar ı gerekir . Yönetim , faa l virü s koruma yazılımların ı v e içind e yıkıc ı bi r yü k taşıyabilen , görünüşt e güvenli e-postalar a karş ı değer i ölçülemez bi r korum a sağlaya n anti - Trojan yazılımların ı kullanmalar ı gerektiğin i çalışanlarına hatırlatmalıdır .

O ACINDIRMA , SUÇLULU K DUYURM A ° | V E SİNDİRM E TEKNİĞ İ KULLANMA K

On beşinc i bölümd e d e sö z edileceğ i gibi , bi r toplu m mühendis i steklerini yerin e getirmes i içi n hedefin i yönlendirme k amacıyl a etkilem e psikolojisini kullanır . Yetenekl i toplu m mühendisleri , korku , heyeca n y a ;a suçlulu k gib i duygular ı uyandıraca k bi r yönte m bulm a konusund a :ok ustadırlar . Bunu , eld e ola n bilgiler i derinlemesin e incelemeden nsanları isteklerin i yerin e getirmey e yönlendire n istemsi z mekanizmala r olan psikoloji k tetikleyiciler i kullanara k yaparlar .

Hem kendimi z he m d e başkalar ı adın a zo r durumlarda n kaçınm a eğilimindeyizdir. B u oluml u dürtüde n yol a çıkarak , saldırgan , kişini n acıma duygusuyl a oynayabilir ; onu n kendin i suçl u hissetmesin i sağlayabilir y a d a sila h olara k sindirmey i kullanabilir .

işte size , duygularl a oynam a konusund a e n sevile n manevralarl a ilgili birka ç üs t düze y ders . "-..-• •

Bazı insanları n bi r toplantının , öze l bi r eğlenceni n y a d a bi r kita p tanıtım kokteylini n yapıldığ ı bi r oteli n bal o salonunu n kapısınd a dura n görevliye gittiklerini , sonr a d a bile t y a d a davetiy e sorulmada n adamı n yanından geçtiklerin i hi ç gördünü z mü ?

Çok benze r bi r şekild e bi r toplu m mühendis i d e lafazanlıkla , girilme - si mümkü n değilmi ş gib i görünen yerler e girebilir . Tıpk ı aşağıdaki , fil m endüstrisiyle ilgil i öyküd e anlatıldığ ı gibi .

Telefon Görüşmes i

- Ron Hillyard'ın bürosu, ben Dorothy.

- Merhaba Dorothy. Benim adım Kyle Bellamy. Canlandırma

Tasarım'da Brian Glassman'ın ekibinde işe başladım. Sizler burada

işleri kesinlikle farklı yürütüyorsunuz.

- Sanırım. Daha önce başka bir film şirketinde çalışmadığım için pek

bilemiyorum. Sana nasıl yardımcı olabilirim?

- Doğruyu söylemek gerekirse kendimi biraz aptal gibi hissediyorum.

Öğleden sonra fikir alışverişi için bir yazar gelecek ve ben onu içeri

almak için kiminle konuşmam gerektiğini bilmiyorum. Burada,

Brian'ın ofisinde çalışanlar çok iyiler ama onları çok sıkboğaz edi-

yormuşum gibi geliyor, şunu nasıl yaparım, bunu nasıl yaparım...

Sanki yeni okula başlamışım da tuvaletin nerede olduğunu bilmiyor-

muşum gibi. Durumumu anlatabiliyor muyum?

Dorothy güldü . .'/ '

- Sen güvenlikle konuşmak istiyorsun. Önce 7'yi, sonra da 6138'i

çevir. Eğer telefonu Lauren açarsa, ona, sana iyi bakması gerektiğini

söylediğimi ilet.

- Teşekkürler, Dorothy. Ve eğer erkekler tuvaletini bulamazsam, seni

yine arayabilirim!

Bu fikr e birlikt e güldüle r v e telefon u kapattılar .

David Haroid'u n Hikâyes i '

Film seyretmey e bayılırı m v e Lo s Angeles' a taşındığımd a fil m endüstrisinde çalışa n bi r yığı n insanl a tanışacağım ı v e onları n ben i par - tilere götüreceğin i y a d a fil m stüdyolarınd a öğl e yemeğ i yiyeceğimiz i falan düşünmüştüm . Neyse , Lo s Angeles't a bi r yı l kaldım , yirm i alt ı yaşımı doldurma k üzereydi m v e fil m dünyasıyl a e n büyü k yakınlaşma m Pheonix v e Cleveland'da n gele n cic i insanlarl a birlikt e yaptığı m Universal Studio s tur u oldu . Sonunda , işleri , beklediği m gib i kend i elim e almam gerektiğin i anladım . Eğe r onla r ben i dave t etmezlerse , be n kendimi dave t edecektim . Yaptığı m d a b u oldu .

Bir Lo s Angele s Time s aldı m v e birka ç gü n boyunc a sinem a say - fasını okuyu p farkl ı stüdyolarda n baz ı yapımcıları n adların ı no t ettim . Önce büyü k stüdyolarda n birin i vurmay a kara r verdim .

Santralı aradı m v e gazeted e okuduğu m b u yapımcını n ofisin e bağlanmak istediğim i söyledim . Telefon u aça n sekrete r ana ç birin e ben - ziyordu. Şansl ı olduğum u düşündüm , çünk ü eğe r oradak i keşfedilme k için bekleye n gen ç bi r kı z olsayd ı büyü k olasılıkl a ban a saati n ka ç olduğunu bil e söylemezdi .

Ama Doroth y öyl e değildi , sokakt a kalmı ş bi r ked i yavrusun u evin e ala - cak birin e benziyordu . Yen i işind e kendin i bira z mahcu p hissede n yen i çocuğa acıyaca k biriydi . Be n d e kesinlikl e doğr u noktasın a dokunmuştum . Birilerini kandırmay a çalışırken , onları n siz e istediğinizde n dah a fazlasın ı vermeleri durum u he r gü n başınız a gelmez . Ban a acıyı p yalnızc a güven - likte çalışa n insanlarda n birini n adın ı vermekl e kalmadı , ayn ı zamand a o hanıma, ban a iy i bakmas ı gerektiğin i tembihlediğin i d e söylemem i istedi .

Dorothy'nin adın ı kullanmay ı zate n planlamıştım . Bu , iş i dah a d a kolaylaştırdı. Laure n heme n açıld ı v e verdiği m adı n çalışa n veritabanın - da olu p olmadığın a bakmay a bil e yeltenmedi .

Öğleden sonr a kapıy a gittiğimd e adım ı ziyaretç i listesin e eklemekl e kalmamışlar beni m içi n bi r par k yer i bil e ayırmışlardı . Fil m stüdyos u kan - tininde ge ç bi r öğl e yemeğ i yedi m v e akşam a kada r etraf ı gezdim . Hatt â birkaç se s stüdyosun a bil e girdi m v e fil m çekimlerin i seyrettim . Saa t 7'y e kadar orada n ayrılmadım . Geçirdiği m e n heyeca n veric i günlerde n biriydi .

Aldatmacanın İncelenmes i

Herkes bi r zamanla r yeniydi . Hepimizin , özellikl e gen ç v e deneyim - siz olduğumu z zamanlarda n kala n il k günlerl e ilgil i anılarımı z vardır . B u yüzden yen i bi r çalışa n yardı m istediğind e pe k ço k insanı n -özellikl e d e işe girel i ço k olmamı ş olanların - kend i yen i yetmeli k duyguların ı hatır - lamalarını v e yardımc ı olma k içi n he r iş i bi r kenar a bırakmaların ı bekleyebilirsiniz. Toplu m mühendis i bun u bili r v e kurbanlarını n acım a duygularıyla oynama k içi n bun u kullanabileceğini n farkındadır .

Tanımadığımız insanları n şirketimizi n binaların a v e büroların a dala - vere yapı p girmelerin i ço k kolaylaştırıyoruz . Girişt e güvenli k görevliler i olsa v e çalışa n olmaya n herhang i bir i içi n içer i alınm a işlemler i yapıls a bile, b u öyküd e anlatıla n oyunu n çeşitl i şekillerd e kullanılmas ı saldır - ganın bi r ziyaretç i kart ı almasın ı v e içer i girmesin i sağlayacaktır . Y a şir - ketiniz ziyaretçiler e eşli k edilmes i şartın ı koymuşsa ? B u iy i bi r kural ; ancak sadece , çalışanlarınız , ziyaretç i kart ı olsu n olmasın , te k başına gelen herkes i durduru p on a sorula r sorm a konusund a gerçekte n bi - linçliyse etkil i olur . Eğe r alına n yanıtla r tatmi n edic i olmazsa , çalışan - larınız güvenliğ e habe r verme k konusund a d a istekl i olmalıdırlar .

Dışardan gelenleri n lafazanlıkl a tesisleriniz e girmes i şirketinizi n hassa s bilgilerini tehlikey e sokar . Bugünü n ortamında , toplumumuzu n üzerind e gezi - nen terö r tehdidiyl e birlikte , bilgide n ço k dah a fazlas ı tehlik e altınd a olabilir .

Şimdi Yap '

Toplum mühendisliğ i teknikler i kullana n herke s gerçe k bi r toplu m mühendisi olma k zorund a değildir . Bell i bi r şirketi n i ç işlerin i bile n her - hangi bir i d e bi r tehdi t oluşturabilir . Dosyalarınd a v e veritabanlarınd a eleman bilgilerini n tümün ü tuta n şirketle r içi n tehlik e dah a d a büyüktür . Tahmin edeceğini z gibi , çoğ u şirke t d e böyl e yapar .

Çalışanlar toplu m mühendisliğ i saldırıların ı far k edece k şekild e eği - tilmediği v e yetiştirilmediğ i sürece , aşağıdak i öyküd e geçe n terkedilmi ş kadın gib i kararl ı insanlar , pe k ço k dürüs t insanı n olanaksı z olduğun u düşündüğü şeyler i yapabilirler . . . . . .

Doug'ın Hikâyes i ' .

Linda'yla işle r zate n iy i gitmiyord u v e Erinl e tanıştığı m and a onu n benim içi n yaratıldığın ı anladım . Linda , biraz , nası l desem , ta m olara k den - gesiz sayılmas a d a kafas ı bozulduğ u zama n ipi n ucun u kaçırabile n biri .

Mümkün olduğ u kada r nazi k bi r şekild e artı k taşınmas ı gerektiğin i ona söyledi m v e eşyaların ı toplanmasın a yardı m ettim . Hatt â aslınd a benim ola n birka ç Queensrych e CD'sin i almasın a bil e izi n verdim .

O gide r gitme z anahtarcıy a gidi p ö n kap ı içi n yen i bi r kili t aldı m v e hemen o gec e takdirdim . Ertes i saba h telefo n şirketin i aradı m v e numaramı değiştirti p kayıtlard a görünmemesin i istedim .

Artık Erin'i n peşinde n gitme k içi n özgürdüm .

Linda'nın Hikâyes i

Zaten ayrılmay a hazırdım , sadec e dah a kara r vermemiştim . Am a kimse ger i çevrilmekte n hoşlanmaz . B u durumd a iş , "n e kada r iğren ç biri olduğun u on a nası l gösterebilirirn" e geldi .

Bulmam ço k uzu n sürmedi . Başk a bi r kı z olmalıydı , yoks a ben i b u kadar alelacel e başında n atmazdı . Böylec e bi r sür e dah a bekleyecek , sonra d a gec e ge ç saatlerd e on u arayacaktım . Ta m d a e n a z aranma k istedikleri saatlerde .

Ertesi haft a sonun a kada r bekledi m v e Cumartes i geces i saa t 1 1 gib i aradım. Numarasın ı değiştirmişt i v e yen i numar a kayıtlard a yoktu . B u da onu n n e kada r ad i bir i olduğun u gösteriyordu .

Bu ço k d a büyü k bi r enge l değildi . Telefo n şirketindeki işimde n ayrıl - madan önc e ev e getirdiği m evraklar ı karıştırmay a başladım . V e işt e buradaydı; Doug'ı n telefo n hattınd a oluşa n bi r arızada n kala n tami r makbuzunu saklamıştı m v e makbuzu n üzerind e telefon a ai t kabl o v e çif t numaraları yazıyordu . Telefo n numaranız ı istediğini z kada r değiştirin , aynı bakı r te l çift i evinizde n çıkı p telefo n şirketini n merke z ofi s y a d a M O denen an a santralın a bağlanır . He r evde n v e dairede n çıka n bakı r telle r kablo v e çif t ad ı verile n sayılarl a tanımlanır . Eğe r telefo n şirketini n işler i nasıl yürüttüğün ü bilirseniz , k i be n biliyorum , hedefi n kabl o v e çif t sayılarını bilme k telefon numarasın ı bulma k içi n gerekl i ola n te k şeydir .

Kentteki tü m merke z ofisleri n adresler i v e telefo n numaralarını n bir - likte bi r listes i elimd e vardı , iğren ç Doug'l a yaşadığı m yeri n yakınların - daki bi r MO'nu n numarasın ı buldu m v e aradı m am a doğa l olara k kims e açmadı. Ta m d a ihtiyacını z olduğ u and a b u santra l görevlis i nerededir ? Yeni bi r pla n yapma k yaklaşı k yirm i saniyem i aldı . Diğe r merke z ofisler i aramaya başladı m v e sonund a birin i buldum . Am a kilometrelerc e ötedeydi v e görevl i büyü k olasılıkl a ayakların ı uzatmı ş oturuyordu . Yapmasını istediği m şey i yapma k istemeyecekti . Planı m hazırdı .

"Ben Linda , onarı m merkezinden, " dedim . "Aci l bi r duru m var . Hastan e acil servisini n telefon u arızalanmış . Bi r teknisye n onarmay a çalışıyo r am a sorunun nered e olduğun u bulamıyor . Heme n VVebste r Merke z Ofisi'n e gidip MO'da n ayrıla n hatt â çevi r ses i olu p olmadığın a bakılmas ı gerek. " '

Sonra ona , "Oray a vardığınd a sen i ararım " dedim . Çünk ü onarı m merkezini arayı p ben i sormasın ı istemiyordum .

Merkez ofisi n raha t ortamında n çıkı p arabasını n ö n camında n buz u ,

Mitnick Mesajı :

Hedef şirkette islerin nasıl yürüdüğünü öğrendikten sonra, toplum mühendisinin bu bilgiyi kullanarak gerçek çalışanlarla ahbaplık kurması kolaylaşır. Şirketlerin kendilerine diş bileyen eski ve yeni çalışanlarından gelebilecek toplum mühendisliği saldırılarına karşı hazırlıklı olmaları gerekir. Kişilerin geçmişini taramak, bu tarz davranışlara eğilimi olan şahısları belirlemeye yardımcı olabilir. Ancak çoğu durumda bu insanları tespit etmek oldukça zordur. Böyle durumlarda en uygun koruma, şirkette çalışıp çalışmadıkları şahsen bilinmeyen kişilere bilgi vermeden önce aralarında kişinin iş durumunun kontrolü de olmak üzere kimlik belirleme işlemlerini denetlemek ve sıklaştırmaktır.

kazıyıp geceni n bi r yarıs ı ısla k sokaklard a gezinme k istemeyeceğini n farkındaydım. Am a aci l bi r duru m vard ı ve bu yüzde n ne kada r meşgu l olduğuyla ilgil i bi r şe y söyleyemedi .

Kırk be ş dakik a sonr a on u VVebste r Merke z Ofisi'nde n aradığımda , ona 2 9 numaral ı kabloy u v e 248 1 numaral ı çift i kontro l etmesin i söyle - dim. Kutuy a gitti , kontro l ett i v e evet , çevi r ses i geliyordu . Be n bun u zaten biliyordum .

Sonra ona , "Tamam , şimd i bi r H K yapman ı istiyorum, " dedim . B u ha t kontrolü v e ayn ı zamand a telefo n numarasın ı tespi t etmes i anlamın a geliyordu. Bunu , aradığ ı numaray ı ger i bildire n öze l bi r numaray ı ara - yarak yapıyordu . Numaranı n kayıtsı z bi r numar a olduğun u y a d a dah a yeni değiştiğin i fala n bilmiyordu , b u yüzde n istediğim i yapt ı v e numaranın okunduğun u duydum . Harika . He r şe y tıkı r tıkı r yürümüştü .

Ona, sank i numarıy ı biliyormuşu m gib i "Soru n herhald e arad a bi r yerde" dedim . Adam a teşekkü r etti m v e bunu n üzerind e çalışmay a devam edeceğimiz i söyleyi p iy i gecele r diledim .

Doug'ın kayıtlard a gözükmeye n bi r telefo n numarasını n arkasın a saklanarak bende n kaçmay a çalışmas ı buray a kadardı . Eğlenc e başla - mak üzereydi .

Aldatmacanın İncelenmes i

Bu öyküdek i gen ç hanı m intika m alma k içi n istediğ i bilgiy i eld e etmeyi başarmıştı , çünk ü işleri n işleyişiyl e ilgil i bilgis i vardı , telefo n numaralarını, süreçler i v e telefo n şirketind e kullanıla n terimler i biliyordu . Bu bilgiler i kullanara k yalnızc a istediğ i numaray ı eld e etmekl e kalmamış, bun u soğu k bi r kı ş geces i bi r santra l görevlisin i şehri n diğe r ucundan işin i görmes i içi n getirtere k yapmıştı .

İmasını İstiyor "

Oldukça etkil i v e popüle r bi r sindirm e şekl i -popülerliğ i basi t olmasın - dan kaynaklanır- yetk i kullanara k insa n davranışların ı etkilemey e dayanır.

Genel müdü r asistanını n ad ı bil e ço k i ş görebilir . Öze l dedektifle r v e hatt â insan avcılar ı bun u he r zama n yaparlar . Santral ı ararla r v e gene l müdürl e görüşmek istediklerin i söylerler . Sekrete r y a d a asista n telefon u açtığınd a genel müdü r içi n bi r evra k vey a pake t geldiğin i söylerle r y a d a bi r elektroni k posta ek i gönderdiklerin i v e on u bası p basamayacağın ı sorarlar . Y a d a fak s numarasını öğrenme k isterler . B u arad a adını z neyd i diy e d e sorarlar .

Sonra bi r sonrak i adam ı ararla r ve : "Ba y Bigg'i n ofisinde n Jeanni e sizi aramam ı v e ban a bi r konud a yardımc ı olabileceğiniz i söyledi. "

Bu yöntem e a d düşürme deni r v e genellikl e saldırganı n üs t düze y biriyle bağlantıs ı olduğun a hedef i inandırara k hızl ı bi r ahbaplı k kurul - ması içi n kullanıla n bi r taktiktir . Kurban , orta k tanıdıklar ı ola n birin e dah a çok yardı m etm e eğilimindedir .

Eğer saldırga n oldukç a hassa s bilgiler e gö z koyduysa , kurbanda , müdürleriyle başını n derd e girmes i korkus u gib i iş e yara r duygula r uyandırmak içi n böyl e bi r yaklaşım a başvurabilir . İşt e bi r örnek .

Scoff'un Öyküs ü , ••..••• -

"Buyrun ben Scott Abrams."

"Scott, ben Christopher Dalbridge. Az önce Bay Biggley'le konuştum

ve sesi biraz kızgın geliyordu. Tüm pazar payı araştırma raporlarının

birer kopyasını incelenmemiz için bize göndermeniz doğrultusunda on

gün önce size bir talimat vermiş. Elimize hiçbir şey geçmedi."

"Pazar payı araştırmaları mı? Bana kimse bununla ilgili bir şey

söylemedi. Siz hangi birimdesiniz?"

"Biz danışmanlık flrmasıyız ve şimdiden takvimin oldukça gerisindeyiz."

• "Dinle, şu anda bir toplantıya girmek üzereyim. Bana telefon

numaranızı verin ve..."

O and a saldırga n iyic e can ı sıkılmı ş gib i konuşur . "Bay Biggley'e

böyle mi söylememi istiyorsunuz? Bakın, analizlerimizi yarın sabah

görmek istiyor ve bu gece onlar üstünde çalışmamız gerek. Şimdi,

raporları sizden alamadığımız için yapamadığımızı ona ben mi

söyleyeyim yoksa bunu kendiniz mi söylemek istersiniz?"

Öfkeli bi r gene l müdü r bütü n haftanız ı mahvedebilir . Hede f büyü k olasılıkla toplantıy a gitmede n önc e b u işi n halledilmes i gerektiğin e kara r verecektir. Toplu m mühendis i bi r ke z dah a istediğ i yanıt ı alma k içi n doğru düğmey e basmıştır .

Aldatmacanın İncelenmes i

Üst düze y yöneticileri n adın ı kullanara k sindirm e numaras ı özellikl e karşı taraf , şirkett e oldukç a al t seviyelerdeys e ço k iş e yarar . Öneml i birinin adını n geçmes i yalnızc a olağa n isteksizliği n y a d a şüpheciliği n üstesinden gelmekl e kalmaz , kişiy i yardımc ı olma k içi n dah a istekl i yapar: Yardı m ettiğini z kişini n öneml i y a d a etkil i bir i olduğun u düşünü - yorsanız, va r ola n yardımc ı olm a güdünü z doğa l olara k katlanacaktır .

Ancak toplu m mühendis i b u oyun u oynarken , kişini n kend i patro - nunun adın ı kullanma k yerin e dah a üs t düze y birini n adın ı kullanmanı n en iyis i olduğun u bilir . Ayrıc a b u yöntemi n küçü k bi r kuruluşt a uygulan- ması ço k güçtür . Saldırgan , kurbanını n kazar a pazarlam a gene l müdü r yardımcısıyla karşılaşı p ona , "Ben i aramasın ı söylediğiniz adam a ürü n pazarlama planların ı gönderdim " deyivermesin i istemez . Böyl e bi r cümle rahatlıkla, "N e pazarlam a planı ? Hang i adam? " gib i bi r tepk i doğurabilir. B u d a şirketi n bi r oyun a kurba n gittiğini n anlaşılmasın a neden olabilir .

Sosyal Güvenli k İdares i Sizinl e İlgil i

Ne Biliyo r

Ellerinde bizlerl e ilgil i dosyala r ola n devle t dairelerinin , görmey e yetkili olmaya n insanlarda n uza k tutma k içi n bilgilerimiz i kili t altınd a tut - tuklarını düşünme k isteriz . Gerçe k ş u ki , federa l hüküme t bil e saldırılar a karşı, haya l ettiğimi z kada r güvend e değildir .

May Linn'i n Telefon u

Yer: Sosya l Güvenli k îdaresi'ni n bölg e ofislerinde n biri . Zaman: Perşembe , saba h 10:18 .

Mitnick Mesajı :

Sindirme yöntemi, bir cezalandırılma korkusu yaratarak insanları iş birliği yap- maya zorlar. Sindirme aynı zamanda küçük düşme korkusunu ya da bir sonraki ikramiye için yetersiz görülme gibi korkulan da uyandırır.

İnsanlar, söz konusu güvenlik olduğunda yetkiyi sorgulamanın kabul edilebilir, hattâ beklenen bir hareket olduğu doğrultusunda yetiştirilmelidirler. Bilgi güven- liği eğitimleri, ilişkileri zedelemeden, müşteri memnuniyeti yöntemlerini kulla- narak yetkinin nasıl sorgulanman gerektiğini de vermelidir. Dahası bu beklenti yukarıdan aşağıya doğru da desteklenmelidir. Eğer konumlarına bakmadan insanları sorgulayan bir çalışanın arkasında durulmuyorsa, oluşacak tepki, sorgulanmanın durması, yani olmasını istediğiniz şeyin tam tersi olacaktır.

- Mod üç. Ben May Linn Wang."

Telefonun diğe r tarafindak i se s çekingen , neredeys e utanga ç geliyordu . - Bayan Wang, ben Arthur Arondale, Genel Müfettişlik makamından. Size 'May' diyebilir miyim?"

- May Linn lütfen, ded i kadın .

- Durum şu May Linn. Burada, henüz bilgisayarı olmayan yeni bir arkadaşımız var ve şu anda önemli bir projede çalıştığı için benim bilgisayarımı kullanıyor. Şu işe bakar mısın, bir Birleşik Devletler devlet dairesiyiz ve bu adamın kullanması için bir bilgisayar alacak kadar bütçede para olmadığını söylüyorlar. Şimdi de müdürüm işimde geri kaldığımı düşünüyor ve bahane duymak istemediğini söylüyor. Anlatabiliyor muyum?

- Demek istediğini çok iyi anlıyorum.

- MCS üzerinde bir küçük arama yapmada bana yardımcı olabilir misin, diy e sord u adam , verg i mükelleflerini n bilgilerini n tutulduğ u bilgisayar sistemini n adın ı kullanarak .

- Elbette. Ne gerekiyor?

- İlk önce Joseph Johnson, doğum tarihi 4/7/69 adıyla bir harf tara- ması yapmam istiyorum." (Har f taramas ı bilgisayar a verg i mükelle - flerinin adların a gör e hesa p aratmaktır . Aram a doğu m tarihiyl e genişletilir.)

May Lin n kıs a bi r duraksamada n sonr a sordu :

- Ne öğrenmek istiyorsun?"

- Hesap numarası nedir, ded i adam , Sosya l Güvenli k Numaras ı içi n kurum içind e kullanıla n terim i kullanarak . Kadı n numaray ı okudu . - Tamam. Bu hesapla ilgili bir de sayı taraması yapmanı isteyeceğim, dedi arayan .

Bu, teme l verg i mükellef i bilgilerin i okumasın ı istediğ i anlamın a geli - yordu v e Ma y Lin n verg i mükellefini n doğu m yerini , annesini n kızlı k soyadını v e bab a adın ı verdi . Kadı n kartı n verili ş a y v e yılın ı v e hang i bölge büros u tarafında n verildiğin i söylerke n araya n sabırl a dinledi . Sonra bi r AKA S yapmasın ı istedi , ("ayrıntıl ı kazan ç sorgusu"nu n kısaltılmışı.)

. AKA S taramas ı ş u soruy u getirdi :

- Hangi yıl?

Arayan ceva p verdi ,

- 2001 yılı.

- Miktar 190.286 dolar; yatıran Johnson MicroTech, ded i Ma y Linn . - Başka ücret var mı?

- Hcsvw ? , :

- Tefekkürler, çok yardımcı oldun, ded i adam .

Sonra bilgiy e ihtiyac ı olduğund a v e bilgisayarın ı kullanamadığınd a yeniden arayabilme k içi n onda n izi n aldı . Yin e toplu m mühendis - lerinin e n sevdiğ i numaralardan birini , he r seferind e yen i bi r hede f bulmakla uğraşmayı p sürekl i ayn ı kişiyl e görüşebilme k içi n bi r bağlantı kurmay a çalışm a yöntemin i kullanmıştı .

- Önümüzdeki hafta arayamazsın", ded i kadın ; çünk ü Kentucky'y e kızkardeşinin düğünün e gidiyordu . Başk a n e zama n isters e elinde n geleni yapacaktı .

Telefonu kapadığınd a Ma y Linn , kend i gib i değer i bilinmeye n başk a bir devle t memurun a bira z olsu n yardı m edebildiğ i içi n kendin i iy i hissediyordu. .

Keith Carter'i n Öyküs ü .

Filmlere v e ço k sata n polisiy e romanlar a bakılaca k olursa , öze l dedektifler, eti k konusund a eksikleri , insanlarda n istediklerin i alma k konusunda da fazlalar ı ola n kişiler , işlerin i tamame n yasadış ı yöntemle r kullanarak,yürütüyorlar v e yakalanmakta n kı l pay ı sıyrılıyorlar . Aslınd a özel dedektifleri n büyü k bi r kısm ı tamame n yasa l işle r yürütürler . Pe k çoğu i ş yaşamların a yeminl i poli s memurlar ı olara k başladıklar ı içi n neyin yasa l olu p neyi n olmadığın ı gaye t iy i bilirle r v e pe k çoğ u çizgiy i aşmaya hevesl i değillerdir .

Ancak istisnala r d a vardır . Baz ı öze l dedektifle r -he m d e sayılar ı azımsanmayacak kada r çok - polisiy e öykülerd e çizile n karakterler e tıpatıp uyarlar . Meslekt e b u adamlar a bilgi simsarları denir . Kurallar ı çiğnemeye istekl i insanla r içi n kullanıla n nazi k bi r deyimdir . Baz ı kısa - yollara başvurduklarınd a işlerin i dah a hızl ı v e dah a kola y yapabilecek - lerini bilirler . B u kısayolların , onlar ı birka ç yı l parmaklıkları n arkasın a tıkacak suçla r olması , e n ahlaksı z olanların ı caydırmamaktadır .

Yüksek gelirl i öze l dedektifle r -kenti n kiraları n yükse k olduğ u bi r semtinde haval ı bi r apartma n dairesind e çalışanlar - b u tar z işler i kendi - leri yapmazlar . B u işler i yapmas ı içi n bilg i simsarların ı tutmakl a yetinirler .

Kendisine Keit h Carte r diyeceğimi z kiş i etikl e kendin i yormaya n tür - den bi r öze l dedektifti .

Elindeki i ş ta m bi r "Koca m paray ı nered e saklıyor? " işiydi . Y a d a arada bi r olduğ u şekliyle , "Karı m paray ı nered e saklıyor?" . Baze n zen - gin bi r kadı n geli r v e kendisin e ai t parala n kocasını n nerey e sakladığın ı öğrenmek iste r (paral ı bi r kadını n nede n parası z bi r adaml a evlendiğ i bilmecesi Keit h Carter'i n zama n zama n aklın ı kurcalas a da , bun a hiçbi r zaman iy i bi r yanı t bulamamıştır) .

Bu olayd a ad ı Jo e Johnso n ola n koca , paranı n üstün e otura n taraftı . Karısının ailesinde n bor ç aldığ ı o n bi n dolarl a yükse k teknoloj i şirket i

kuran v e bun u yü z milyo n dolarlı k bi r şirket e dönüştüre n akıll ı bi r adamdı . Kadının boşanm a avukatın a gör e ada m malların ı saklama k konusund a muazzam bi r i ş yapmı ş v e avuka t ma l varlığ ı beyan ı tale p etmişti .

Keith başlangı ç noktasını n Sosya l Güvenli k İdares i olmasın a kara r ver - mişti. Böyl e bi r durumd a Johnson'l a ilgili , iş e yarayaca k bilgilerl e dol u ola - bilecek dosyalar ı hedefliyordu . B u bilgiyl e donanmı ş olara k Keit h kendin i hedef olara k tanıtabili r v e bankaların , komisyonc u firmaları n v e off-shor e bankacılığı yapa n kurumları n on a he r şey i anlatmasın ı sağlayabilirdi .

ilk olarak , yere l bi r ilç e bürosunu , herhang i birini n şehi r telefo n rehberinde bulabileceğ i 800'l ü numaray ı kullanara k aradı . Telefon a çıka n memura istihka k şubesinde n biriyl e görüşme k istediğin i söyledi . Bira z bekledi sonr a telefo n açıldı . O and a Keit h vite s değiştird i v e "Merhaba " diyerek söz e girişti . "Be n Gregor y Adams , 32 9 numaral ı Bölg e Bürosu'ndan. Son u 6363'l e bite n bi r hesapl a ilgilene n bi r tasfiy e memu - runa ulaşmay a çalışıyorum . Bendek i numaray ı çevirdiğimd e fak s çıkıyor. "

"O Mo d iki" , ded i adam . Telefo n numarasın a bakt ı v e Keith' e verdi .

Keith sonr a Mo d iki'y i aradı . Telefon u Ma y Lin n açtığınd a yin e tar z değiştirdi v e Gene l Müfettişli k makamında n aradığ ı v e başk a birini n kendi bilgisayarın ı kullandığıyl a ilgil i sırada n oyunun u oynadı . Kadı n ona istediğ i bilgiy i verd i v e gelecekt e yardım a ihtiyac ı olurs a elinde n geleni yapacağın ı söyledi .

Aldatmacanın İncelenmes i

Bu yaklaşım ı etkil i kıla n şey , başk a birini n bilgisayarın ı kullanmas ı ve "müdürü m bende n memnu n değil " hikâyesin i kullanara k çalışanı n duygularıyla oynamas ı oldu . İ ş yerind e insanla r duyguların ı pe k sı k açığa vurmazlar , vurduklarındays a birilerini n toplu m mühendisliğin e karşı koyduğ u savunmaları n üstünde n aşıverirler . "Ço k zo r durum - dayım, ban a yardı m ede r misin? " gib i duygusa l bi r hile , kazançl ı çıkma k için yapıla n te k şeydi .

Saldırgan, b u bilgiy i halkta n gele n telefonlar a baka n bi r memurda n alamazdı. Keith'i n kullandığ ı tarzd a bi r saldır ı yalnızc a karş ı taraft a tele - fonu halk a açı k olmaya n v e dolayısıyl a arayanı n içerde n bir i olduğ u beklentisi içind e ola n bir i vars a geçerlidir . B u d a "ben i ş u gönderdi " tarz ı güvenliğe başk a bi r örnektir .

Bu saldırını n iş e yaramasın a yardımc ı ola n unsurla r arasınd a şunla r vardı :

• Mod'u n telefon numarasını n bilinmesi .

• Kullanıla n terimleri n bilinmesi ; say ı tarama , har f taram a v e AKAS . • Gene l Müfettişli k makamında n olduğun u söylemek . He r federal

hükümet çalışan ı oranı n geni ş yetkiler e sahi p hüküme t çapınd a

bir kuru m olduğun u bili r v e bu , saldırgan a itibarl ı bi r hav a verir .

Sosyal Güvensizli k

İlginç bi r şekilde , Sosya l Güvenli k idaresi , kend i çalışanlar ı içi n yararlı bilgilerl e dol u anca k ayn ı zamand a toplu m mühendisleri içi n de oldukç a değerli ola n idar i işlemle r Talimatnamesi'ni n bi r kop - yasını internet e koydu . B u öyküd e geçtiğ i şekliyl e kısaltmalar , terim - ler v e istenile n şeyi n nası l dil e getirileceğ i orad a açıkç a anlatılıyor .

Sosyal Güvenli k İdaresi'yl e ilgil i dah a ço k şe y m i öğrenme k isti - yorsunuz? Googie'd a aratmanı z y a d a aşağıdak i adres i tarayıcınız a girmeniz yeterli : http://policy.ssa.gov/poms.nsf/ . Eğe r idar e b u öyküyü okumu ş v e si z bun u okuyan a kada r talimatnamey i kaldır - mamışsa, bi r SG İ memurunu n emniye t teşkilatın a verebileceğ i bilgi - lerin nele r olduğuyl a ilgil i ayrıntıl ı bilgilerd e dahi l olma k üzer e birço k çevrimiçi açıklam a bulacaksınız . Kullanı m açısında n bakılaca k otur - sa, teşkila t kavramı , bi r SG İ memurun u emniye t teşkilatında n olduğuna ikn a edebilece k toplu m mühendislerin i d e kapsıyor .

Başka bi r ilgin ç ayrınt ı is e -mantıksa l olara k bakıldığınd a tamame n farklı bi r bölümde n bambaşk a biriyl e görüşülseyd i ço k dah a uygu n ola - cak bi r durumd a bile - toplu m mühendislerini n kimseyi , "Nede n ben i arı - yor?" diy e düşündürmeyece k şekild e isteklerin i sunuyo r olmaları . Belk i de arayan a yardı m etme k günlü k döngünü n sıradanlığınd a bi r değişik - lik yarattığı içi n kurba n isteği n n e kada r olağandış ı olduğun a dikka t etmiyordur.

Sonuç olara k b u olaydak i saldırgan , eld e ola n iş e yetece k kada r bilg i toplamakla yetinmeyere k sürekl i başvurabileceğ i bi r bağlant ı kurma k d a istedi. Acındırm a saldırıs ı için , "klavyem e kahv e döktüm " gib i sırada n bi r hile d e kullanabilirdi . Anca k klavy e bi r günd e değiştirilebileceğ i için , burada iş e yaramazdı . B u nedenl e başk a birini n kend i bilgisayarın ı kul- landığıyla ilgil i öyküy ü yazdı . Bun u haftalarc a sürdürebilirdi : "Evet , bil - gisayarın dü n geleceğin i sanmıştım . Bi r tan e geld i am a başk a bir i bi r numara çeki p alet i kendin e almış . B u yüzde n b u soytar ı yin e beni m odamda bitiverdi. " V e b u i ş böyl e deva m edebilir .

"Zavallı ben , yardım a ihtiyacı m var. " Ço k iy i i ş görür .

Basit Bî r Telefo n

Bir saldırganı n başlıc a enstrümanlarında n biri , isteğin i maku l bi r şekilde sunmaktır . Kurbanı n günlü k işlerini n arasınd a gele n istekler e benzeyen, kurban ı fazlac a zorlamayaca k türde n bi r şe y olmalıdır . Yaşamda, pe k ço k başk a şeyd e olduğ u gibi , bi r gü n bi r isteğ i mantıkl ı bir şekild e sunma k zorken , başk a bi r gü n b u i ş çocu k oyuncağ ı olur .

Mary H'ni n Telefon u • ' ."""" . .-"-- .

Tarih/Saat: 2 3 Kasım , Pazartesi , saba h 7:49 .

Yer: Mauersb y & Storc h Müşavirlik , Ne w York .

Pek ço k insa n içi n muhaseb e iş i sayılarl a boğuşmakta n v e fasuly e saymaktan ibaretti r v e genellikl e kana l tedavis i kada r eğlencel i (!) olduğu düşünülür . Neys e k i herke s iş i böyl e görmez . Örneği n Mar y Harris; kıdeml i muhasebecili k görevin i ilg i çekic i bula n biridi r v e çalıştığ ı firmada konuy a e n haki m muhasebecilerinde n bir i olmasını n neden - lerinden bir i d e budur .

O pazartes i sabah ı Mar y uzu n bi r gü n olmasın ı beklediğ i içi n iş e bi r an önc e başlama k amacıyl a ofis e erke n geldi . O saatt e telefonunu n çaldığını duyunc a şaşırdı . Ahizey i kaldırdı :

"Merhaba, be n Pete r Sheppard . Arbuckl e Deste k Hizmetleri'nd e çalışıyorum, şirketiniz e tekni k deste k veriyoruz . Haft a sonund a bilgisa - yarlarında soru n ola n insanlarda n birka ç şikâye t aldık . B u saba h herke s işe gelmede n önc e kontro l etme k istedim . Bilgisayarınız ı kullanırke n y a da ağ a bağlanırke n soru n yaşıyo r musunuz? "

Mary hünü z böyl e bi r sorunl a karşılaşmadığın ı söyledi . Bilgisayarın ı açtı v e önyüklem e yapılırke n Pete r n e yapma k istediğin i on a anlatmay a başladı.

"Birkaç tes t yapma k istiyorum" , dedi . "Bastığını z tuşlar ı kend i ekranımda görebiliyoru m v e a ğ üzerinde n doğr u aktarıldığında n emi n olmak istiyorum . He r tuş a basışınızd a ban a onu n n e olduğun u söyle - menizi istiyorum , böylec e burad a d a ayn ı har f y a d a sayını n görünü p görünmediğine bakabilirim . Tama m mı? "

Bilgisayarının çalışmamasıyl a v e hiçbi r işi n bitmediğ i sıkıc ı bi r günl e ilgili kâbuslar ı ola n bir i olara k Mar y b u adamı n kendisin e yardımc ı olmasından fazlasıyl a memnu n kalmıştı . Bira z sonr a ona , "Giri ş ekranındayım v e kullanıc ı adım ı gireceğim . Şimd i giriyorum - M...A...R...Y...D."

"Şimdiye kada r gaye t iyi " ded i Peter . "On u burad a görebiliyorum . Şimdi parolan ı gi r am a n e olduğun u ban a söyleme . Hi ç kimsey e parolanı söylernemelisin , tekni k servis e bile . Parola n korumal ı olduğ u için burad a yıldızla r çıkacak , yan i parolan ı göremem. " Bunları n hiçbir i doğru değild i am a Mary'ni n aklın a yattı . Sonr a Peter , "Bilgisayarı n açıldığında haberi m olsun " dedi .

Mary açıldığın ı söylediğind e Pete r on a uygulamalarda n ik i tanesin i açmasını söyledi . Kadı n he r ikisini n d e gaye t iy i çalıştıkların ı habe r verdi .

Mary he r şeyi n doğr u bi r şekild e çalışmasında n memnu n olmuştu . "Bilgisayarının sağla m olu p olmadığın ı kontro l edebildiği m iy i oldu .

Birşey dah a var " ded i Pete r ve deva m etti , "Çalışanları n parolaların ı değiştirebilmesi içi n bi r güncellem e yaptık . Ban a birka ç dakikan ı ayırı p doğru çalışı p çalışmadığın ı görmem e yardımc ı olabili r misin? "

Mary, yardı m etmesinde n dolay ı adam a müteşekkird i v e heme n obul etti . Pete r ona , kullanıcıları n parolaların ı değiştirebilmesin i sağlayan uygulamay ı çalıştırma k içi n yapmas ı gerekenler i adı m adım anlattı. Parol a değiştirm e aslınd a VVindovv s 200 0 işleti m sistemini n sıradan unsurlarında n biridir . "Had i şimd i parolan ı gir" , ded i kadına . "Sesli bi r şekild e söylememe n gerektiğin i unutma. "

Kadın bun u d a yaptığında , Peter , "Hızl ı bi r denem e yapma k için , sana yen i parolanı sorduğunda , 'testi23 ' gir . Sonr a doğrulam a kutu - cuğuna bi r ke z dah a gi r v e ENTER' e bas" , dedi .

Sunucu bağlantısın ı çözm e işlemind e Mary' e yardımc ı oldu . Sonr a birkaç dakik a bekletip , yen i parolasın ı deneyere k yenide n bağlanmasın ı istedi. He r şe y saa t gib i işliyordu , Pete r ço k memnu n kalmışt ı v e -kadın ı bi r kez dah a parolasın ı açıkç a söylememes i içi n uyararak - Mary'ni n esk i paro - lasına dönmes i y a d a yen i bi r tan e seçmes i konusund a yardımc ı oldu .

"Çok iyi , Mary" , ded i Peter . "Hiçbi r soru n çıkmadı , b u ço k iyi . Dinle , eğer herhang i bi r soru n çıkars a Arbuckle'da n biz i ara . Be n çoğunlukl a özel projelerd e çalışıyoru m am a burad a telefon u aça n herke s san a yardımcı olabilir. " Mar y on a teşekkü r ett i v e vedalaştılar .

Peter'in Öyküs ü •

Peter'le ilgil i söylentile r alı p başın ı gitmişti . Mahallesind e onunla bir - likte okui a gide n birileri , başkalarını n bulamadığ ı şeyler i bulabile n zek i bir bilgisaya r manyağ ı olduğun u duymuşlardı . Alic e Conra d onda n bi r konuda yardı m istediğind e önc e hayı r dedi . Nede n yardı m edecekt i ki ? Bir keresind e o kızl a bi r yerlerd e karşılaştığınd a on a çıkm a tekli f etmiş , kız d a on u ger i çevirmişti .

Ancak yardı m etmey i reddetmes i kız ı şaşırtmı ş gib i görünmüyordu . Zaten Peter'i n yapabileceğ i birşe y olduğun u düşünmediğin i söyledi . B u bir meyda n okumaydı , çünk ü yapabileceğinde n emindi . Böylec e Pete r işi yapmay ı kabu l etti .

Alice'e bi r pazarlam a şirketin e danışmanlı k yapmas ı içi n sözleşm e teklif edilmişt i am a sözleşm e koşullar ı ço k iy i değildi . Dah a iy i koşulla r talep etmede n önc e diğe r danışmanları n sözleşmelerini n n e tü r koşullan içerdiğin i öğrenme k istiyordu .

Peter'in anlattığ ı şekliyl e hikây e şöyle :

Alice içi n bun u söyleyeme m am a yapabileceğim i düşünmedikler i birşeyi yapmam ı isteye n insanlarda n yak a silkmiştim . Üsteli k d e be n işi n kolay olduğun u bilirken . Peki , o kada r d a kola y değildi , e n azında n b u sefer. Bira z çab a gerektirecekt i am a soru n olmayacaktı . ; .: .

Ona akıllını n n e deme k olduğun u gösterecektim .

Pazartesi sabah ı 7:30' u bira z geç e pazarlam a şirketini n bürosun u aradım v e danışmayl a görüşü p onlar a muhasabede n biriyl e konuşma m gerektiğini söyledim . Muhasebede n kimseni n geli p gelmediğin i biliyo r muydu acaba ? Danışm a görevlis i bana , "Sanırı m birka ç dakik a önc e Mary'nin geldiğin i gördüm , siz i on a bağlamay a çalışayım " dedi .

Mary telefon u açtığınd a on a bilgisaya r sorunlarıyl a ilgil i küçü k hikâyemi anlattım . Hikây e tüyler i dike n dike n etme k üzer e tasarlanmıştı . Böylece ban a büyü k bi r memnuniyetl e yardımc ı olacaktı . Parolasın ı değiştirmesine yardımc ı olu r olma z kullanmasın ı istediği m geçic i parol a olan "testi23"l e heme n sistem e girdim .

Ustalık burad a işi n için e giriyordu ; şirketi n bilgisaya r sistemin e iste - diğim zama n kendim e ai t gizl i bi r parolayl a girmem i sağlayaca k küçü k bir progra m yükledim . Mary'l e konuşma m bittikte n sonra , il k işi m sis - teme girdiğim i kimseni n anlamamas ı içi n deneti m tarihçesin i silme k oldu. B u kola y bi r şeydi . Siste m yetkilerim i artırdıkta n sonr a güvenlikl e ilgili www.ntsecurity.n u adl ı bi r interne t sayfasınd a bulduğu m clearlogs adında bedav a bi r program ı indirdim .

Asıl iş e sır a gelmişti . Dosy a adınd a "sözleşme " kelimes i geçe n bel - geleri arattırdı m v e dosyala n indirdim . Sonr a bira z dah a aram a yaptı m ve an a damarı , danışma n ücre t bilgilerini n olduğ u klasör ü buldum . Böylece tü m sözleşm e dosyaların ı biraray a getirdi m v e bi r ödemele r lis - tesi yaptım .

Alice sözleşmeler e bakabili r v e diğe r danışmanlar a n e kada r verdik - lerini görebilirdi . Tü m b u dosyalar ı aram a hamallığın ı kendis i yapsın . Ben onu n bende n istediğ i şey i yapmıştım .

Verileri kaydettiği m disketlerden , kanıtlar ı Alice' e gösterebilme k içi n birkaç dosyanı n çıktısın ı aldım . On u beniml e buluşmay a v e akşa m yemeğe çıkmay a zorladım . Kâğıtlar ı karıştırırke n yüzünü n aldığ ı şekl i görmeliydiniz. "Olamaz " dedi . "Olamaz. "

Disketleri yanımd a getirmemiştim . Onla r yemdi . Disketler i alma k içi n bana gelmes i gerektiğin i söyledim ; on a yaptığı m iyilikte n dolay ı ban a duyduğu minnet i göstereceğin i umuyordum .

Aldatmacanın İncelenmes i

Peter'in pazarlam a şirketin i aramas ı e n teme l toplu m mühendisliğ i şekline bi r örnektir . Ço k a z hazırlı k gerektiren , il k denemed e işleye n v e birkaç dakikad a başarıl ı ola n basi t bi r girişimdir .

Daha d a iyisi , kurba n Mary'ni n bi r oyun a y a d a bi r hiley e kurba n git - tiğini düşünmesi , durum u bi r yerler e bildirmes i y a d a yaygar a koparmas ı için hiçbi r nede n yoktu .

AAitnick Mesajı :

İsteğini dile getirme şekline bağlı olarak bir toplum mühendisinin insanlara bir i şeyler yaptırmasının ne kadar kolay olduğunu görmek şaşırtıcı. Temel şart, • psikolojik kurallara dayalı istemsiz bir tepkiyi tetiklemek ve arayanı bir mütte- - fik olarak gördükleri zaman insanların zihinlerinde oluşan kısayollara güven- i mektir.

Plan, Peter'i n ü ç toplu m mühendisliğ i taktiğin i kullanmas ı üstün e kuruluydu. Önc e kork u uyandırı p -bilgisayarını n çalışmayabileceği m düşündürerek- Mary'ni n işbirliğ i yapmasın ı sağladı . Sonr a kadını n kul- landığı uygulamalarda n ikisin i çalıştırmasın ı bekledi , böylec e kadı n onların çalıştığında n emi n olacakt ı v e ikisini n arasındak i ilişkiy i güçlendirecek, bi r müttefikli k duygus u uyandıracaktı . E n sonunda , bil - gisayarının sağla m olduğunda n emi n olma k içi n gösterdiği yardımda n duyduğu minnettarlıkl a oynayara k işini n e n öneml i kısmın ı gerçek - leştirmek içi n bira z dah a yardı m etmesin i sağladı .

Ona parolasın ı kendisin e bil e açıklamamasın ı söyleyere k Pete r kusursuz bi r ustalıkl a şirke t dosyalarını n güvenliğiyl e ilgil i endişesi konusunda Mary' i ikn a etti . B u davranış ı da , şirket i v e kendisin i koruduğu içi n Peter'i n bi r sahtekâ r olmadığ ı yolundak i güvenin i artırdı .

Polis Baskın ı

Şöyle bi r sahn e haya l edin : Polis , interne t üzerinde n bedav a fil m dağı - tan Artur o Sanche z adınd a birin i kapan a kıstırma k ister . Hollyvvoo d stüd - yoları adamı n teli f hakların ı ihla l ettiğin i söylemektedir , ada m is e kaçınıl - maz olara k girecekler i bi r pazar ı görmeler i v e yen i filmler i indirilebili r şekl e sokmak içi n bi r şeyle r yapmay a başlamalar ı içi n onlar ı dürtmey e çalış - maktadır. Artur o bunu n stüdyola r için , tamame n gö z ard ı edilen , büyü k bi r gelir kaynağ ı olacağın a (hakl ı olarak) parma k basmay a uğraşmaktadır .

Amma İzn i Lütfe n

Bir gec e ge ç saatt e ev e döndüğünd e yolu n karşısında n evini n pencerelerine baka r v e tü m ışıkları n sönü k olduğun u far k eder . Halbuk i dışarı çıkarke n birin i he p açı k bırakmaktadır .

Kapısını çalara k komşusun u uyandırı r v e binay a bi r poli s baskın ı yapıldığını öğrenir . Anca k herkes i aşağıd a bekletmişlerdi r v e komşus u polislerin hang i ev i aradıklarında n emi n değildir . Te k bildiği , ellerind e bazı ağı r şeylerl e dışar ı çıktıklarıdır , anca k he r şe y sarıl ı olduğ u içi n n e olduklarını anlayamamıştı r v e kimsey i kelepçeleyi p götürmemişlerdir .

Arturo oturduğ u dairey i kontro l eder . Köt ü haber : polisleri n bıraktığ ı ve ü ç gü n içerisind e arayı p bi r randev u almas ı gerektiğin i söyleye n bi r kâğıt bulur . E n köt ü habe r ise : bilgisayarların ı götürmüşlerdir .

Arturo ortalıkta n kaybolu r v e bi r arkadaşını n yanınd a kalmay a başla r Ama belirsizli k için i kemirmektedir . Poli s n e bilmektedir ? Sonund a on u yakalamışlar am a kaçmas ı içi n d e bi r firsa t m ı tanımışlardır ? Yoks a bu , kent i terk etmesin e gere k kalmada n çözebileceği , tamame n farkl ı bi r kon u mudur ?

Devam etmede n önc e bi r a n duru p düşünün : Polisi n sizinl e ilgil i neler bildiğin i öğrenmeni n bi r yolun u haya l edebiliyo r musunuz ? Politikacı tanıdıklarınız , Emniye t Müdürlüğü'nd e arkadaşlarını z y a d a savıcılıkta dostlarını z olmadığın ı varsayarsak , sırada n bi r vatanda ş olarak sizi n b u bilgiy i eld e edebilmeni z içi n bi r yo l olabili r mi ? Y a d a toplum mühendisliğ i beceriler i ola n bir i böyl e bi r şey i başarabili r mi ?

Polisi oyun a Getirme k - - :

Arturo bilgilenm e isteğin i şöyl e tatmi n eder : Başlangı ç olara k yakın - lardaki bi r fotokop i dükkânını n telefo n numarasın ı bulur , onla n ara r v e faks numaraların ı ister .

Sonra bölg e savcılığın ı ara r v e evra k bölümün ü ister . Evra k büro - suna bağlandığınd a kendin i Lak e Bölgesi'nde n gele n bi r dedekti f olara k tanıtır v e halihazırd a geçerl i aram a emirlerin i taki p ede n memurl a görüşmek istediğin i söyler .

"Ben ilgileniyorum " de r kadın . "Ço k iyi" , diy e karşılı k veri r Arturo . "Dün gec e bi r suçluy a baskı n yaptık , baskını n yazıl ı beyanın a ulaşmay a çalışıyorum."

"Adreslere gör e tutuyoruz" , de r kadın .

Adresi verir . Kadını n ses i oldukç a heyecanl ı gelmiştir . "Ah , evet" , de r kadın coşkuyla . "Biliyoru m bunu . Teli f suçlusu. "

"Tamam, o" , de r Arturo . "Yazıl ı beyanı n v e aram a emrini n bi r kop - yasına ihtiyacı m var. "

"Burada, önümde. "

"Çok iyi" , de r adam . "Ş u and a dışarıdayı m v e b u konuyl a ilgil i o n be ş ' • dakika sonr a Gizl i Servis'l e bi r toplantıy a gireceğim . Bugünlerd e bira z dalgınım, dosyay ı evd e unutmuşu m v e gidi p almay a kalkarsa m yetişe - meyeceğim. Sizde n bi r kopyasın ı alabili r miyim? "

"Elbette, soru n olmaz . Fotokopilerin i çekerim , buray a geli p ala - bilirsiniz."

"Harika", de r Arturo . "Ço k iy i old u am a ş u and a şehri n diğe r uçun - dayım. Ban a fakslamanı z mümkü n mü? "

Bu bira z soru n yaratı r am a aşılama z birşe y değildir . "Evra k bürosun -

:a faksımı z yok" , de r kadın . "Am a aşağıd a sekrete r odasınd a bi r tan e .ar. Kullanmam a izi n verebilirler. "

"Ben sekrete r odasın ı arayıp , gerekl i ayarlamalar ı yaparım" , de r adam.

Sekreter odasındak i kadı n b u işl e memnuniyetl e ilgilenecekti r am a bun u kimin ödeyeceğin i bilme k istemektedir . Bi r fatur a numarasın a ihtiyac ı vardır .

"Ben numaray ı alıp , siz i yin e ararım" , de r kadına .

Sonra bölg e savcılığın ı arar , yin e kendin i bi r poii s memur u olara k tanıtır v e danışmadak i görevliy e soruveri n "Bölg e savcılığını n fatur a numarası nedir? " Görevl i duraksamada n numaray ı söyler .

Sekreter odasın ı ger i arayı p fatur a numarasın ı verir .

Fatura numarasın ı verme k içi n sekrete r odasın ı ger i aramas ı o hanımı bira z dah a işleme k içi n bahan e olur . Kadın ı yukar ı çıkı p fak - slanacak evraklar ı almay a ikn a eder .

Arturo'nun birka ç adım dah a atmas ı gereklidir . He r zama n birilerini n birşeylerden kuşkulanmas ı olasılığ ı vardı r v e fotokop i mağazasın a gidi p belli bi r faks ı alma k üzer e birini n gelmesin i bekleyen , sırada n giyiml i birkaç poli s memuruyl a karşılaşabilecektir . Bira z bekler , sonr a d a faksı n gönderilip gönderilmediğin i kontro l etme k içi n sekrete r odasın a telefo n eder. Şimdiy e de k he r şe y yolund a gitmiştir .

Aynı mağaz a zincirin e bağlı , şehri n diğe r tarafındak i başk a bi r fotokopi mağazasın ı ara r v e işlerini n görülmesinde n n e kada r memnu n kaldığını v e müdür e bi r teşekkü r mektub u yazma k istediğin i söyleyi p müdürün adın ı sorar . B u öneml i bilgiy i kullanara k il k fotokop i mağazası - na telefo n ede r v e müdürl e konuşma k istediğin i söyler . Karş ı tara f tele - fonu açtığınd a Arturo , "Merhaba , be n 62 8 Hartfiel d mağazasında n Edward. Müdürüm . Ann a siz i aramam ı söyledi . Bira z kızgı n bi r müşte - rimiz var ; bir i on a yanlı ş mağazanı n fak s numarasın ı vermiş . Burad a önemli bi r fak s bekliyo r v e on a verile n fak s sizi n mağazanı n numarası. " Müdür, mağaz a çalışanlarında n birin e faks ı bulduru p heme n Hartfiel d mağazasına gönderteceğin e sö z verir .

Faks ikinc i mağazay a geldiğind e Artur o orad a beklemektedir . Belgeleri aldıkta n sonr a sekrete r odasındak i hanım a teşekkü r etme k içi n arar v e "Elinizdek i kopyalar ı yukar ı çıkarmanız a gere k yok , onlar ı ata - bilirsiniz." der . Sonr a il k mağazanı n müdürün e d e telefo n ede r v e on a d a ellerindeki faks ı atabileceklerin i söyler . Böylec e birilerini n geli p sorula r sorması olasılığın a karşı , ola n bitenl e ilgil i ortalıkt a hiçbi r i z kalmayacak - tır. Toplu m mühendisler i tedbiri n elde n bırakılmamas ı gerektiğin i iy i bilirler .

Böyle bi r düzmeceyl e Artur o il k fotokop i mağazasın a gele n fak s içi n

ve ikinc i mağazay a fak s gönderme k içi n par a verme k zorund a kalmamıştır. Eğe r poli s il k mağazay a gelmi ş olsaydı , ikinc i noktay a adam gönderen e kada r o çokta n gitmi ş olurdu .

Öykünün sonu : Yazıl ı beya n v e aram a emrind e yazdığın a göre , polisi n elinde Arturo'nu n fil m kopyalam a faaliyetleriyl e ilgil i belgelenmi ş delille r vardır. Arturo'nu n bilme k istediğ i şe y budur . Geceyarıs ı olmada n eyale t sınırını geçer . Artur o yen i bi r yaşam a başlama k üzer e yol a çıkmıştı r v e başka bi r yerd e yen i bi r kimlikl e işin e yenide n başlamay a hazırdır .

Aldatmacanın İncelenmes i

Bölge savcılığınd a çalışa n insanla r sürekl i emniye t teşkilat ı mensup - larıyla tema s halindedirler ; sorula r sorarlar , düzenlemele r yaparla r mesajlar alırlar . Telefon u açı p d a kendin e poli s memuru , komise r yardımcısı y a d a başk a birşe y dem e cesaret i ola n herkesi n sözün e güvenilir. Kullanıla n terimler i bilmemesi , gergi n olması , söylediklerin i karıştırması y a d a sesind e bi r tersli k olmas ı gib i durumla r yoks a kimliği - ni doğrulamas ı içi n on a te k bi r sor u bil e sorulmaz . Burada , ik i farkl ı memurla yaşana n d a ta m olara k budur .

Eksik fatur a numaras ı te k bi r telefonl a halledilmişti . Sonr a Artur a "On be ş dakik a sonr a Gizl i Servisl e bi r toplantıy a gireceğim , bugün - lerde bira z dalgını m v e dosyay ı evd e unutmuşum" , gib i bi r öyküyl e acındırma kartın ı oynamıştı . Kadı n doğa l olara k on a acımı ş v e işin i gücünü bırakı p on a yardı m etmişti .

Daha sonr a Artur o bi r değ i l ik i fotokop i mağazas ı kullanara k fak s alma k konusunda kendin i sağlam a almıştı . Bunu n üzerind e bi r çeşitlem e yapma k faksın izlenmesin i dah a d a zorlaştırırdı : Saldırga n belgey i başk a bi r fotokop i mağazasına gönderme k yerine , fak s numaras ı gib i gözüke n am a aslınd a sizin adınız a fakslar ı ala n v e e-post a adresiniz e göndere n ücretsi z bi r inter - net hizmetin i kullanabilirdi . Böylec e belg e doğruda n saldırganı n bilgisayarı - na indirilir , saldırganı n yüzün ü göstermes i hi ç gerekmezdi , i ş tamamlanı r tamamlanmaz d a e-post a adres i v e elektroni k fak s numaras ı ter k edilirdi .

Rollerin Değişmes i

Kendisine Michae l Parke r diyeceğimi z gen ç bi r ada m yükse k gelirl i işlerin üniversit e mezunların a gittiğin i ge ç anlaya n insanlarda n biriydi .

İN \ J I ' . Nasıl oluyor d a bir toplum mühendisi emniyet müdürlükleri, savcılıklar, telefon şirketleri uygulamaları, saldırılarında işine yarayacak iletişim ve bilgisayar şirketlerinin yapıları gibi, bu kadar çok işleme yöne- lik ayrıntıyı bilebiliyor? Çünkü bu onun işi. Bu bilgiler toplum mühen- disinin sermayesidirler ve kandırma çabalarında ona yardımcı olurlar.

İşin gerçeği, kimsenin iyi bir toplum mühendisi tarafından kandırılmaya karşı bağışıklığı yoldur. Günlük yaşamın hızı nedeniyle, bizim için önemli olan konu- larda bile, her zaman üzerinde düşünülmüş kararlar veremeyiz. Karışık durum- lar, zaman kısıtlamaları, ruh hali ya da zihin yorgunluğu dikkatimizin dağıl- masına neden olabilir. Bu yüzden zihinsel kısayollar oluşturur, bilgiyi tam ve özenle incelemeden kararlarımızı veririz. Bu zihinsel sürece otomatik tepki verme denir. Tüm federal, eyalet ve yerel emniyet görevlileri için bile geçerlidir. Hepimiz insanız.

Yarım bur s art ı eğiti m kredileriyl e yere l bi r üniversitey e gitm e olanağ ı vardı am a bu , kirayı , yemeği , benzin i v e arab a sigortasın ı ödeme k içi n geceleri v e haft a sonla n çalışmas ı anlamın a geliyordu . He r zama n Kisayolları bulmay ı seve n Michael , dah a hızl ı ola n v e dah a a z çabayl a sonuç vere n başk a bi r yo l olabileceğin i düşündü . O n yaşınd a il k ke z bi r oilgisayarla oynadığında n ber i b u aletlerl e ilgil i pe k ço k şe y öğrenmi ş v e nasıl çalıştıklar ı konusun a kafay ı takmıştı . Hızlandırılmı ş bi r bilgisaya r Dilimleri lisan s diplomas ı yaratmay ı denemey e kara r verdi .

Üstün Başarısı z Mezuniye t

Eyalet üniversitesini n bilgisaya r sistemlerin e girip , temi z bi r B + y a d a A- ortalamayl a mezu n olmu ş birini n kayıtların ı bulabilir , kayıtlar ı kop - yalar, adın ı değiştiri r ve o yılı n mezuniye t sınıf ı listesin e ekleyebilirdi . Düşününce b u fikirde n rahatsı z oldu . Kampüst e buluna n bi r öğrenciy e ait başk a kayıtları n d a olmas ı gerektiğin e kara r verdi ; har ç ödem e kayıt - ları, yurtla r ofis i v e dah a ki m bili r başk a neler . Yalnızc a dersleri n v e not - arın kaydın ı çıkarma k ço k fazl a açı k oluşmasın a nede n olacaktı .

Düşünüp üzerind e kurdukç a aklın a uygu n bi r geçmişt e bilgisaya r bi - limlerinden mezu n kendiyl e ayn ı ad ı taşıya n bir i olu p olmadığın a bakma k geldi. Eğe r varsa , i ş başvur u formların a onu n Sosya l Güvenli k Numarası'nı girebilirdi , böylec e adın ı v e sosya l güvenli k numarasın ı üniversiteden kontro l etme k isteye n biri , "Evet , sö z konus u diplomay ı almıştır", yanıtı m alırdı . (Kendini n bildiğ i am a çoğ u insanı n farketmeye - ceği birşe y yapıp , iş e başvururke n diğe r Parker'i n Sosya l Güvenli k Numarası'nı giri p sonr a iş e alınırsa , başlam a formların a kend i gerçe k numarasını yazabilirdi . Çoğ u şirket , yen i iş e gire n birini n i ş başvurusun - da farkl ı bi r numar a kullanı p kullanmadığın ı kontro l etmey i akı l etmezdi.)

Belaya Bağlanma k

Üniversite kayıtlannd a Michae l Parker' i nası l bulacaktı ? Şöyl e bi r şey yaptı :

Üniversitenin an a kütüphanesin e gidere k bi r bilgisaya r uçbirimini n başına oturdu , üniversiteni n interne t sitesin e girdi . Sonr a Öğrenc i İşleri'n i aradı. Telefon a çıka n kişiy e artı k iyic e aşın a olduğunu z toplu m mühendis - liği taktiklerinde n birin i uyguladı . "Bilg i işle m Merkezi'nde n arıyorum . A ğ yapılandırmasında değişiklikle r yapıyoru z v e erişiminiz i engelle - mediğimizden emi n olma k istiyoruz . Hang i sunucuy a bağlısınız? "

"Sunucuyla n e deme k istiyorsunuz? " diy e sord u karş ı taraf .

"Öğrenci akademi k verilerin e ulaşma k istediğinizd e hang i bilgisa - yara bağlanıyorsunuz? "

Aldığı yanıt , admin.rnu.ed u oldu . Konuştuğ u kiş i öğrenc i kayıtlarını n tutulduğu bilgisayarı n adın ı on a vermişti . Bu , bulmacanı n il k parçasıydı . Artık hang i makiney i hede f alacağın ı biliyordu .

Adresi bilgisayar a gird i v e bi r yanı t alamadı . Bu , beklediğ i bi r durumdu , erişimi engelleye n bi r güvenli k duvar ı vardı . O bilgisaya r üzerind e çalışa n hizmetlerden herhang i birin e bağlanı p bağlanmadığın ı kontro l etme k içi n bir progra m çalıştırd ı v e bi r bilgisayarı n uzakta n başk a bi r bilgisayar a bağlanmasını v e on a bi r basi t uçbiri m olara k erişmesin i sağlaya n bi r Telne t servisinin çalıştığ ı açı k bi r bağlant ı noktas ı buldu . Oray a girme k içi n ihti - yacı ola n te k şe y standar t bi r kullanıc ı ad ı v e parolaydı .

Öğrenci İşleri'n i tekra r arad ı v e b u ke z farkl ı biriyl e konuştuğunda n emin olma k içi n önc e dikkatl e dinledi . Bi r kadı n çıkt ı v e on a yin e üniver - site Bilg i İşle m Merkezi'nde n olduğun u söyledi . İdar i kayıtla r içi n yen i bi r işletim sistem i yüklediklerin i anlattı . Bi r ayrıcalı k yapıp , denem e kipind e olan yen i sistem e onu n bağlanmasın ı v e öğrenc i akademi k kayıtların a erişip erişemediğin e bakmasın ı istedi . Bağlanacağ ı adresi n İ P numa - rasını verd i v e on a nele r yapmas ı gerektiğin i anlattı .

Aslında İ P adres i kadın ı Michael'ı n kütüphaned e önünd e oturduğ u bil - gisayara yönlendirmişti . Sekizinc i bölümd e açıklana n süreci n aynısın ı kul - lanarak, öğrenc i kayıtların a bakma k içi n girdiğ i sistemd e görmey e alışı k olduğunun tıpatı p aynıs ı bi r giri ş benzetimcisi , yan i saht e bi r giri ş ekran ı yaratmıştı. "Çalışmıyor " ded i kadın . "Sürekl i 'Giri ş Hatalı ' mesaj ı veriyor. "

Giriş benzetimcisi , kullanıc ı ad ı ve parol a girilirke n kullanıla n tuşlar ı çoktan Michael'i n uçbirimin e kaydetmişti bile . Kadına , "Baz ı hesapla r henüz b u makinay a aktarılmadı . Siz e bi r hesa p açayım , sonr a yin e ararım" dedi . He r yetenekl i toplu m mühendis i gib i açı k uçlar ı bağlama k konusuna dikka t ederek , kadın ı aramay ı unutmamay ı bi r kenar a no t etti . Telefon edi p tes t sistemini n henü z ta m olara k çalışmadığın ı v e eğe r onun içi n bi r soru n olmayacaks a sorunu n nerede n kaynaklandığın ı bul - duklarında arkadaşlarını n on u arayacakların ı söyleyecekti .

Artık Michae l hang i bilgisaya r sistemin e bağlanmas ı gerektiğin i bili -

BASİT UÇBİRİM: Kendi mikroişlemcisi olmayan uçbirim. Basit uçbirimler yalnızca basit komutlar kabul ederler ve sadece harf ve sayılan göstere-

bilirler.

yordu v e elind e bi r kullanıc ı ad ı v e paro - la vardı . Anca k doğr u a d v e mezuniye t tarihine sahi p bi r bilgisaya r bilimler i mezununu aratabilme k içi n hang i ko - mutlara gereksinim i olacaktı ? Öğrenc i veri taban ı bunu n içi n ço k uygundu . Üni- versitenin v e öğrenc i işlerini n ihtiyaçları - na gör e hazırlanmışt ı v e ver i tabanın a erişim içi n kendin e özg ü bi r kullanım ı vardı.

İlk adı m b u so n engel i kaldırmaktı : Öğrenci ver i tabanın ı taramanı n gizemler i konusund a on a kimi n yo l gösterebileceğini bulmalıydı . Öğrenc i işlerin i tekra r arad ı v e yin e başk a biriyle konuştu . Kadına , Mühendisli k Fakültes i Dekanlığı'nda n aradığın ı söyledi ve , "Öğrenc i akademi k dosyaların a ulaşmakt a soru n yaşadı - ğımız zama n kim i aramamı z gerekiyordu? " diy e sordu .

Bir sür e sonr a üniversiteni n ver i taban ı yöneticisiyl e telefond a görüşüyor, on a bi r acındırm a numaras ı çekiyordu : "Be n Mar k Sellers , öğrenci işlerinden . Yen i iş e başlaya n birin e yardı m ede r misin ? Sen i aradığım içi n özü r dileri m am a ş u and a herke s toplantıd a v e etraft a bana yardı m edebilece k kims e yok . 199 0 v e 200 0 yıllar ı arasındak i bil - gisayar bilimler i mezunlarını n listesin e ihtiyacı m var . B u akşam a kada r istiyorlar v e bun u onlar a veremezsem , b u işt e uzu n sür e kalamayabili - rim. Baş ı dertt e ola n birin e yardı m etme k iste r misin? " insanlar a yardı m etmek b u ver i taban ı yöneticisini n işini n bi r parças ı olduğ u içi n Michael' a yapması gerekenler i adı m adı m anlatırke n ik i ka t fazl a sabı r göstermişti .

Konuşmaları biten e kada r Michae l o yıllar a ai t tü m bilgisaya r bilim - leri mezunların ı içere n listey i indirmişti . Birka ç dakik a içind e bi r aram a yapmış v e ik i Michae l Parke r birde n bulmuştu . Bi r tanesin i seçt i v e adamın Sosya l Güvenli k Numarası'nı n yan ı sır a ver i tabanınd a buluna n başka iş e yara r bilgiler i d e aldı .

Az önce , "Michae l Parker , Bilgisaya r Bilimler i Lisan s Derecesi'n i 1998 yılınd a üstü n başar ı il e tamamlamıştır " unvanın ı almıştı . B u durumda 'Lisan s Derecesi ' sahib i olmas ı ço k yerind e bi r sonu ç olmuştu .

Aldatmacanın İncelenmes i

Bu saldırıd a dah a önc e sözün ü etmediği m bi r yönte m kullanıldı : Saldırganın, kuruluşu n ver i taban ı yöneticisin e nası l işleyeceğin i bilmediğ i bi r bilgisayar sürecini n adımların ı te k te k anlattırması . Rolleri n güçl ü v e etkil i bi r şekilde değiştirilmesi . Bu , raflarında n ma l arakladığını z dükkânı n sahibinde n kutuyu arabanız a kada r taşımanız a yardı m etmesin i isteme k gib i bi r şey .

Aldatmacanın Engellenmes i

Acındırma, suçlulu k duyurm a v e sindirme , toplu m mühendilerini n e n çok kullandığı ü ç psikoloji k yöntemdi r v e b u öyküle r b u taktikleri n kul - lanım şeklin i göstermiştir . Si z v e bilgisayarını z b u tar z saldırılarda n kaçınmak içi n nele r yapabilirsiniz , biliyo r musunuz ?

Verilerin Korunmas ı

Bu bölü m kapsamınd a anlatıla n baz ı öyküler , kiş i şirketinizd e çalışıyor (y a d a öyl e görünüyor) v e belge , şirke t iç i bi r elektroni k postaya y a d a fak s makinasın a gönderiliyo r ols a d a tanımadığını z birin e bir dosy a göndermeni n tehlikelerin i vurguluyor .

Şirket güvenli k kuralları , göndericini n şahse n tanımadığ ı birin e önemli bilgiler i tesli m etmesiyl e ilgil i so n derec e ne t olmalıdır . Hassa s bilgiler içere n dosyaları n aktarılmasın a yöneli k zorunl u süreçle r belirlen - melidir. Şahse n tanınmaya n birinde n gele n bi r tale p durumunda , kontro l etmek içi n tanımlanmı ş açı k adımla r olmalıdı r v e bunlar ı bilgini n has - saslığına gör e farkl ı düzeylerd e yetkile r gerektirmelidir .

işte gö z önün e alınaca k birka ç teknik :

• Bilgini n nede n istendiğin i öğreni n \\OTIYÎTI'I \ tesV ^ s>&WteU\d.er \ yetk i

alınmasını gerektirebilir) .

• B u işlemler e ai t kişise l y a d a biri m iç i günlü k tutun .

• Süreçle r konusund a eğitilmi ş v e hassa s bilgiler i dışar ı verme k

üzere yetkilendirilmi ş kişileri n bi r listesin i bulundurun . Çalışm a

grubunun dışın a gönderilece k bilgileri n yalnızc a b u kişile r

tarafından gönderilmesin i zorunl u kılın .

• Eğe r iste k yazıl ı olara k yapılmışs a (e-posta , fak s y a d a posta) ,

isteğin, gönderdiğin i düşündüğünü z kişide n geldiğinde n emi n

olmak içi n gerekl i önlemler i alın .

Parolalara İlişki n

Hassas bilgiy e erişim i ola n tü m çalışanları n -bugü n b u neredeys e

Mitnick Mesajı :

Bilgisayar kullanıcıları bu teknolojik dünyada var olan toplum mühendisliğine ilişkin tehditler ve zayıflıklardan bazen bütünüyle habersiz oluyorlar. Bilgiye erişimleri var, ancak yine de neyin bir güvenlik tehdidi olabileceğiyle ilgili ayrıntılı bilgileri yok. Toplum mühendisi, aradığı bilginin değerini tam olarak bilmeyen bir çalışanı hedefleyecektir; böylece hedef, tanımadığı birinin isteğini yerine getirmeye daha meyilli olacaktır.

bilgisayarla çalışa n herke s anlamın a geliyor - parol a değiştirme k gib i basit işler i birka ç saniyeliğin e bil e ols a yapmalarını n büyü k güvenli k açıklarına nede n olabileceğin i bilmeler i gerekiyor .

Güvenlik eğitimler i parol a konusun u d a içermelidi r v e konu , parolanın n e zama n v e nası l değiştirilebileceği , neleri n geçerl i parolala r olacağı v e b u sürec e başkaların ı d a katmanı n oluşturabileceğ i tehlikelere odaklanmalıdır. Eğitim , tü m çalışanlara , özellikl e paro - lalarının sorulduğ u istekler e karş ı şüpheyl e yaklaşmalar ı gerektiğin i vur - gulamalıdır.

Dışarıdan bakıldığınd a bunu n çalışanlar a aktarma k içi n ço k basi t bi r mesaj olduğ u düşünülebilir . Öyl e değildir . Böyl e bi r fikr i takdi r etmeler i için çalışanların , parolanı n değiştirilmes i gib i basi t bi r işi n nası l güvenli k açıklarına yo l açacağın ı anlamı ş olmalar ı gerekir . Bi r çocuğa , "Karşıda n karşıya geçerke n he r ik i yön e d e bak " diyebilirsini z am a çocu k bunu n neden öneml i olduğun u anlayan a kada r olay a a t gözlükleriyl e bakması - na gö z yummanı z gerekir . A t gözlükleriyl e bakıla n kuralla r y a gö z ard ı edilir y a d a unutulur .

Merkezî Bî r Bildiri m Noktas ı

Güvenlik politikanız , kuruluşunuz a girm e teşebbüsler i gib i görüne n şüpheli faaliyetleri n bildirileceğ i bi r kiş i y a d a gurupta n oluşa n merkez î bir nokt a d a oluşturmalıdır . Tü m çalışanla r elektroni k y a d a fizikse l bi r müdahaleden kuşkulandıklarınd a kim i aramalar ı gerektiğin i bilmelidirler . Bildirimin yapılmas ı gereke n noktanı n telefo n numaras ı he r zama n e l atında olmalıdır ; böylec e çalışanla r bi r saldır ı gerçekleştiğinde n şüphe - lenirlerse numaray ı bulmay a çalışma k zorund a kalmazlar .

Bilgisayar Âğın ı Koruyu n

Çalışanlar bi r bilgisaya r sunucus u y a d a a ğ adını n önemsi z bi r bilg i olmadığını bilmelidirler . Aksine , güve n uyandırabilmes i y a d a istediğ i bil - ginin yerin i öğrenmes i içi n saldırgan a öneml i bi r kayna k oluşturabilirler .

Özellikle ver i taban ı yöneticiler i gibi , yazılımlarl a çalışa n kişile r teknik uzmanlığ ı olanla r grubun a girerle r v e onların , kendilerinde n bilg i ve tavsiy e isteye n kişileri n kimliklerin i doğrulama k konusund a ço k kat ı ve öze l kuralla r çerçevesind e çalışmalar ı gereklidir .

Sürekli olara k bilgisaya r desteğ i vere n kişiler , n e tü r istekleri n kırmızı

Parolalar toplum mühendisliği saldırılarının o kadar önemli bir odak noktasıdır ki on altıncı bölümü tamamıyla buna ayırdık. Orada parolaların yönetilmesiyle ilgili önerilen kuralları bulabileceğiniz.

ışık yaktığını , diğe r bi r deyişle , arayanı n bi r toplu m mühendisliğ i saldırısı gerçekleştirdiğin i göstere n durumlar a karş ı ço k iy i bi r eğitimde n geçirilmelidirler.

Bu bölümü n e n so n öyküsünd e ver i taban ı yöneticisini n bakı ş açısından, arayanı n gerçe k birini n kıstasların a uyduğun u d a belirt - meden geçemeyeceğim . Kampüste n arıyord u v e içind e bulunduğ u sit e kesinlikle kullanıc ı ad ı v e parol a gerektire n bi r siteydi . Bilg i tale p ede n birinin kimliğin i doğrulama k içi n standar t süreçleri n olmasını n önemin i bu duru m bi r ke z dah a vurguluyor . Özellikl e de , arayanı n gizl i kayıtlar a ulaşmak konusund a yardı m istediğ i böyl e bi r olayda .

Tüm b u öneriler , üniversitele r v e yüksekokulla r içi n ikiy e katlanıyor . Bilgisayar korsanlığını n pe k ço k üniversit e öğrencisini n e n sevdiğ i uğra ş olduğu yen i bi r habe r sayılma z v e öğrenc i kayıtlarını n v e baze n d e fakülte kayıtlarını n çekic i hedefle r teşki l etmeler i d e şaşırtıc ı değildir . B u sömürü o kada r büyü k boyutlardadı r k i baz ı şirketle r kampüsler i tehlike - li bölgele r olara k değerlendirirle r v e son u .ed u il e bite n öğreti m kurum - larının erişimin i engelleme k içi n güvenli k duvarlar ı oluştururlar .

Uzun lafı n kısas ı he r türl ü öğrenc i v e persone l kayıtlar ı başlıc a hedef - ler olara k görülmel i v e hassa s bilg i kapsamınd a ço k iy i korunmalıdır .

• Eğiti m İpuçlar ı

Çoğu toplu m mühendisliğ i saldırılar ı -nerey e bakacağın ı bilenle r için- savunulmas ı komi k olaca k kada r kola y şeylerdir .

Şirket bakı ş açısında n baktığımızd a iy i bi r eğiti m verilmes i içi n önemli bi r gereksini m vardır . Anca k ayn ı zamanda , insanlar a öğrendik - lerini hatırlataca k çeşitl i yolla r d a olmalıdır .

Kullanıcının bilgisayar ı açılırke n he r gü n başk a bi r mesa j içere n bi r ekran çıkabilir . Mesa j öyl e tasarlanmı ş olmalıdı r ki , kendiliğinde n kay - bolmamalı v e kullanıcını n okuduğun a dai r bi r çeşi t ona y kutucuğun a tık - lamasını gerektirmelidir .

Önerebileceğim bi r başk a yaklaşı m is e bi r diz i güvenli k mesajıdır . Sık sı k görüle n hatırlatm a mesajlar ı önemlidi r çünk ü bi r bilinçlili k prog - ramı sürekl i v e sonsu z olmalıdır . İçerikler i sunarke n mesajla r he r seferinde ayn ı şekild e dil e getirilmemelidir . Araştırmalar a gör e farkl ı bi r •cümleyle sunulduğund a y a d a farkl ı örnekle r kullanıldığınd a b u mesajla r daha etkil i olmaktadır .

Bir diğe r kusursu z yaklaşı m is e şirke t bültenin e kıs a ilanla r vermek - tir. He r n e kada r bi r güvenli k köşes i ço k yerind e olacaks a d a b u ilanla r tam bi r köş e oluşturmamalıdır . Onu n yerine , okuduğunu z gazetedek i küçük ilanla r gibi , ik i y a d a ü ç sütu n genişliğind e bi r ila n kutus u tasar - lanabilir. Bülteni n he r baskısında , b u kıs a v e dikka t çekic i yönteml e yen i bir güvenli k unsur u hatırlatılabilir .

TERS DALAVER E

Bu kitabı n başk a bi r yerind e d e söz ü edile n Belalıla r (Th e Sting) film i -ki ban a gör e dolandırıcılıkl a ilgil i yapılmı ş herhald e e n iy i filmdir - zorl u bir kumpas ı büyüleyic i bi r ayrıntılıkt a anlatır . Fimdek i dalavere , "büyü k dalavereler" olara k biline n ü ç büyü k dolandırıcılı k çeşidinde n bir i ola n "telleme" işini n nası l yürütüldüğünü n açı k bi r örneğidir . Profesyone l bi r ekibin bi r oyu n çeviri p bi r geced e nası l büyü k parala r hortumladığı m öğrenmek istiyorsanı z bunda n iy i bi r der s kitab ı yoktur .

Ancak gelenekse l dolandırıcılıklar , n e tü r bi r aya k oyun u kullanır - larsa kullansınlar , bell i bi r yo l izlerler . Baze n oyu n ter s yönd e oynanır , buna d a ter s dalaver e denir . Saldırganın , kurbanı n yardı m içi n saldır - ganı arayacağ ı y a d a kurbanı n bi r mesa i arkadaşını n isteğin e saldır - ganın yanı t vereceğ i şekild e ortam ı düzenlediğ i karmaşı k bi r dolaptır .

Bu i ş nası l m ı yapılır ? Şimd i göreceksiniz .

Tatlı Diif e İkn a Sanat ı

Sıradan bir i bi r bilgisaya r korsanın ı gözünd e canlandırdığınd a çoğunlukla il k akl a gelen , e n iy i arkadaş ı bilgisaya r ola n v e anlı k mesajlar dışınd a konuşm a özürl ü olan , yalnız , için e kapanı k bi r gerzeğin sevimsi z görüntüsüdür . Genellikl e bilgisaya r korsanlığ ı bece - rileri d e ola n toplu m mühendisini n öbü r cebind e insan î beceriler i d e vardır, insanlar ı kullanı p yönlendirere k kesinlikl e aklınız a gelmeyece k yollarla bilg i toplamasın ı sağlayaca k iy i geliştirilmi ş yetenekler e sahiptir .

Angela'yı Araya n Kiş i

Yer: Federa l Sanay i Bankası , Valle y Şubesi .

Zaman: Saba h 11:27 .

Angela Wisnowski , kendisin e büyü k bi r mira s kalma k üzer e olduğun u

ve tasarru f hesaplan , mevdua t sertifikala n

Terimler

ve önerebileceğ i güvenl i am a iy i fai z vere n

başka yatırı m araçlar ı olu p olmadığ ı

TERS DALAVERE:

konusunda bilg i alma k istediğin i söyleye n Saldırıya uğrayan kişinin

bir adamda n bi r telefo n aldı . Angel a adam a saldırgandan yardım iste-

oldukça ço k seçene k olduğun u v e bankay a diği bir dolandırıcılık şekli.

kadar geli p karşılıkl ı görüşme k isteyi p iste -

meyeceğini sordu . Ada m par a elin e geçe r

Bu iy i diy e düşünd ü arayan . İnsanları n e n küçü k bi r dürtmeyl e düşüvermemeleri iy i oluyor . Eğe r bira z direnmezlers e i ş ço k kolay - laşıyor v e be n tembelleşmey e başlıyorum .

- Dışarıya birşey göndermeden önce onay almamız konusunda kafayı üşütmüş bir şube müdürüm var, hepsi bu. Ama bilgiyi fakslamamızı istemiyorsanız önemli değil. Onaya gerek yok.

- Angela yarım saat kadar sonra burada olur. Ona seni aramasını söyleyebilirim, ded i Louis .

- Şifreyi vererek bunun geçerli bir istek olduğunu gösteremediğiniz için ona bugün gönderemediğimi söylerim. Eğer yarın doktor bana rapor vermezse, onu yeniden ararım. ' :

- Tamam, olur.

- Mesaj, acil, diyordu. Neyse boş ver, onay olmadan elim kolum bağlı. Ona göndermeye çalıştığımı ama senin şifreyi veremediğini söylersin değil mi?

Louis sonund a baskıy a dayanamadı . Ahizede n sıkıntıl ı bi r i ç geçirm e duyuldu.

-Peki, dedi . Biraz bekle, bilgisayarıma kadar gitmem gerekiyor. Hangi şifreyi istiyorsun?

- B , ded i arayan .

Louis aramay ı beklemey e aldı , bira z sonr a yenide n açtı .

- 3184. .

- Bu doğru şifre değil. . •

- Bu doğru. B şifresi 3184..

- Ben B demedim, E dedim.

- Kahretsin. Bir dakika bekle.

Louis yenide n şifreler e bakarke n bira z dah a bekledi .

- E şifresi 9697.

- 9697, tamam. Faksı hemen gönderiyorum. Tamam mı?

- Tamam. Teşekkürler.

WaUer vı Araya n Kiş i

- Federal Sanayi Bankası, ben Walter.

- Merhaba, Walter, ben Studio City 38 nolu şubeden Bob Grabowski,

dedi arayan . Bir müşteri hesabına ait imza kartonuna ihtiyacım var,

bana onu fakslayabilir misin?

, İmz a karton u yalnızc a müşterini n imzasın ı içermez , sosya l güvenli k

numarası, doğu m tarihi , annesini n kızlı k soyad ı v e baze n d e ehliye t

numarasına gib i diğe r tanımlayıc ı bilgiler i d e içerir . Bi r toplu m

mühendisi içi n ço k kullanışlıdır .

- Elbette. C şifresi nedir?

- Ş u anda bilgisayarımı başka biri kullanıyor, ded i arayan . Ama a z önce B'yi ve E'yi kullanmıştım ve onları hatıhyorum. Onlardan birini sorabilirsin.

- Tamam, E şifresi nedir?

- E şifresi 9697.

Birkaç dakik a sonr a Waite r istene n imz a kartonun u fakslar .

Donncs Plaiee' i Araya n Kiş i

- Merhaba, ben Bay Anselmo.

- Size bugün nasıl yardımcı olabilirim?

- Hesabıma para yattığını öğrenebilmek için aramam gereken 800'lü numara hangisiydi?

- Bankanın bir müşterisi misiniz?

- Evet, ama numarayı uzun süredir kullanmadım ve şimdi de nereye yazdığımı hatırlamıyorum.

- Numara 800-555-8600. •

- Tamam, teşekkürler.

Vince Capelli'ni n öyküs ü

Spokane'li bi r poli s memurunu n oğl u ola n Vince , saatlerc e köl e gib i çalışıp, asgar î ücre t alabilme k içi n kelley i koltuğ a almayacağın ı erke n yaşlardan ber i biliyordu . Yaşamını n ik i teme l amac ı Spokane'de n ayrıl - mak v e kend i işin i kurma k oldu . Oku l yıllar ı boyunc a arkadaşlarını n onunla ala y etmes i on u dah a d a kızıştırmıştı . Kend i işin i kurmay a hevesli olmas ı am a bi r işi n nası l yürütüleceğiyl e ilgil i hiçbi r fikr i olma - ması onlar a gülün ç geliyordu .

İçten iç e Vinc e arkadaşlarını n hakl ı olduğun u d a biliyordu . İy i olduğ u tek şe y okulu n beyzbo l takımını n tutucus u olara k yaptığ ı işti . Am a bunda d a bur s kazanaca k y a d a profesyone l beyzbo l oynayaca k kada r iyi değildi . O zama n nası l bi r iş e girişecekti ?

Vince'in grubundak i arkadaşlar ı bi r şey i ta m olara k anlamamışlardı : Aralarında birini n ola n bi r şe y -yen i bi r sustal ı çakı , şı k bi r çif t sıca k tutan eldiven , çekic i bi r kı z arkadaş - eğe r Vince'i n hoşun a gitmişs e ço k geçmeden onu n oluyordu . N e çalıyo r n e d e birilerin i arkada n vuruyor - du, bun u yapmasın a gere k yoktu . Çocukla r ellerindekiler i isteyere k veriyorlardı v e sonr a d a bunu n nası l olduğun u düşünüyorlardı . Vince' e sormak d a bi r iş e yaramıyordu , çünk ü kend i d e bilmiyordu . Görünüş e göre he r n e isters e insanla r on a bunlar ı veriyordu .

Vince Capelli , b u ad ı hi ç duymamı ş ols a bile , erke n yaşlarda n ber i bi r toplum mühendisiydi .

Ters Dalaver e 12 5

Okul diplomaları m ellerin e aldıkta n sonr a arkadaşlar ı gülmey i kestiler . Diğerleri, şehird e dolaşı p "Yanınd a patate s kızartmas ı iste r misiniz? " diye sorma k zorund a kalmayacaklar ı bi r i ş bulmay a çalışırlarke n Vince'in babası , teşkilatta n ayrılı p kend i öze l dedektifli k işin i kura n eski bi r poli s arkadaşıyl a konuşmas ı içi n on u Sa n Francisco'y a gönder - mişti. Adam , Vince'i n b u iş e ço k uygu n ola n yeteneğin i görmü ş v e hemen on u iş e almıştı .

Bu alt ı yı l önceydi . İşin , oturu p beklemey i gerektire n ca n sıkıc ı saatler - le dol u sadakatsi z eşlerl e ilgil i bilg i toplam a kısmında n nefre t ediyor - du, anca k zavall ı bi r müteveffanı n dav a açılaca k kada r zengi n olu p olmadığım öğrenmey e çalışa n avukatları n verdiğ i ma l varlıkların ı öğrenme işlerin i he r zama n heyeca n veric i buluyordu . B u tar z işle r on a aklını kullanmas ı içi n pe k ço k firsa t sunuyordu .

Tıpkı Jo e Markowit z adınd a bi r adamı n bank a hesapların a bakmas ı gerektiği zama n olduğ u gibi . Joe'nu n esk i bi r arkadaşın ı dolandırmı ş gibi bi r durum u vard ı v e ş u and a arkadaşı , dav a açars a par a alabilece k kadar Markowitz'i n yükl ü olu p olmadığın ı öğrenme k istiyordu . Vince'in il k adım ı bankanı n güvenli k şifrelerinde n e n a z bir , am a tercihe n iki tanesin i el e geçirmekti . B u kulağ a neredeys e imkânsı z bi r işmi ş gib i geliyor. Nası l bi r numar a bi r bank a çalışanın ı şifreler i vermes i konusund a ikna edebilird i ki ? Kend i kendiniz e sorun ; eğe r si z b u iş i yapma k istiyo r olsaydınız, bun u nası r yapacağınızl a ilgil i bi r fikrini z olu r muydu ? Vince gib i insanla r içi n b u i ş ço k kolaydır .

İşlerinde v e şirketlerind e kullandıklar ı terimler i biliyorsanı z insanla r size güvenirler . Yakı n çevrelerini n bi r parçasıymı ş gib i görünürsünüz. Gizli bi r tokalaşma gibidir . Vince'de n dinleyelim :

Böyle bi r i ş içi n o kada r ço k şey e ihtiyacı m yoktu . B u i ş beyi n cerrahis i değil. İş e başlama k içi n te k gereke n şe y bi r şub e mımarasıydı . Buffal o Beacon Stree t şubesin i aradığımd a telefon a çıka n adamı n ses i bi r giş e görevlisi gib i geliyordu .

"Ben Tim Ackerman" dedim . Herhang i bi r a d olurdu , nası l ols a bi r yer - lere yazmayacaktı . " O şubenin numarası nedir?"

"Telefon numarası mı, şube numarası mı?" diy e bilme k isted i am a b u oldukça aptalcaydı , çünk ü zate n telefo n ediyordum , değ i l mi ? "Şube numarası."

"3182", ded i ada m hi ç duraksamadan . Ne , "Neden bilmek istiyor- sunuz?" diy e sordu , n e d e başk a bi r şey . Hassa s bilg i olmadığ ı için , kul - landıkları he r kâğı t parçasını n üstünd e yazılıydı .

İkinci adı m hedefimi n çalıştığ ı şubey i aramak , orad a çalışanlarda n birinin adın ı v e onu n n e zama n öğl e yemeğin e çıkacağın ı öğrenmekti . Angela 12:30'd a yemeğ e çıkıyordu . He r şe y oldukç a iy i gidiyordu . Üçüncü adımd a Angel a öğl e tatilindeyke n ayn ı şubey i tekra r arayacak , Boston'daki ş u v e ş u numaral ı şubede n aradığım ı söyleyecek , Angela'n m

bu bilgini n fakslanmasın ı istediğin i belirtere k günlü k şifrey i alacaktım . En zorl u kısı m buydu , tekerle r dönmey e burada n başlayacaktı . Eğe r toplum mühendisliğ i becerisin i sınayaca k bi r sına v yapıyo r olsaydım , kurbanın hakl ı olara k kuşkulandığ ı benze r bi r duru m koyardı m v e on u kırıp istediğini z bilgiy i alan a kada r orad a kalma k zorund a kalırdınız . Bunu bi r senaryodak i satırlar ı tekrarlayara k y a d a bell i kalıplar ı ezberle - yerek yapamazsınız ; kurbanınız ı okumanız , n e hissettiğin i anlamanız , oltayı suy a atı p çekere k bi r balığ ı yakahyormu ş gib i onunl a oynamanı z gerekir. T a k i zokay ı yutturup , on u kayığ a çeken e kadar .

Böylece on u ağım a düşürdü m v e günlü k şifrelerde n birin i aldım . Çoğ u bankada yalnızc a te k bi r tan e kullanırlar , öyl e olsayd ı işi m bitmi ş sayılırdı. Federa l Sanay i Bankası'nd a be ş tan e kullanıyorla r v e beşin - den birin i bilme k iş i ço k fazl a şans a bırakma k olurdu . Beşt e ik i olurs a bu küçü k oyunu n bi r sonrak i sahnesin i tamamlama k içi n dah a fazl a şansım olacaktı . " B demedim, E dedim," kısmın a bayılıyorum . İş e yaradığı zama n harik a oluyor . V e çoğ u zama n d a iş e yarıyor . Üçüncü bi r tan e alma k dah a d a iy i olurdu . Te k bi r aramad a ü ç tan e bir - den almay ı başarmışlığı m d a vardır . B , D v e E'ni n okunuşlar ı siz i yan - lış anladıkların ı iddi a edebileceğini z kada r birbirlerin e benzerler . Am a gerçek bi r şaşkınl a konuşuyo r olmanı z gerekir . B u kadı n öyl e değildi . İki taneyl e yetinecektim .

Günlük şifrele r imz a kartonun u alma k içi n beni m kozu m olacaklar . Arıyorum v e ada m bende n bi r şifr e istiyor . C'y i istiyo r v e be n d e yal - nızca B v e E var . Am a b u dünyanı n son u değil . Böyl e anlard a saki n olmalısınız, kendiniz e güvenmel i v e işiniz e deva m etmelisiniz . Hi ç istifimi bozmada n ona , "Biri benim bilgisayarımı kullanıyor, bana diğerlerinden birini sor" oyunun u oynadım .

"Hepimiz aynı şirketin çalışanlarıyız, hepimiz bu işin içindeyiz; adamı yokuşa sürme". Böyl e bi r and a kurbanınızı n b u şekild e düşündüğün ü ümit edersiniz . Ada m ta m kitabın a gör e oynadı . Sunduğu m seçenekler - den birin i sordu , on a doğr u yanıt ı verdi m v e imz a kartonun u faksladı . İş neredeys e bitmişti . Bi r görüşm e dah a yapı p elektroni k bi r sesi n iste - diğiniz bilgiy i okuduğ u v e müşterileri n otomati k hizme t içi n kullandık - ları 800'l ü numaray ı buldum . İmz a kartonund a hedefimi n tü m hesa p numaralan v e kişise l kimli k numaras ı vardı , çünk ü b u bank a Sosya l Güvenlik Numarası'nı n so n dör t y a d a be ş basamağın ı kullanıyordu . Elimde kale m 800'l ü numaray ı çevirdi m v e birka ç dakikam ı tuşlar a basarak geçirere k adamı n dör t hesabını n birde n so n durumların ı öğrendim. İş i sağlam a alma k içi n he r birin e e n so n yatırdığ ı v e çektiğ i paralan d a bi r kenar a no t ettim .

Müşterimin aradığ ı he r şe y fazlasıyl a tamamdı . He r olasılığ a karş ı he r zaman bira z fazl a bilg i verme k hoşum a gider . Müşter i velinime - timizdir. N e d e ols a sürekl i gele n işle r işletmeni n varlığın ı sürdürmesi - ni sağlaya n şeylerdir , öyl e değ i l mi ?

Ters Dalaver e 12 7

Aldatmacanın İncelenmes i

Tüm b u olayı n kili t noktas ı o ço k öneml i günlü k şifreler i almakt ı v e ounu yapma k içi n saldırgan , yan i Vince , pe k ço k farkl ı tekni k kullandı .

Biraz la f ebeliğ i yapara k iş e başlamışt ı k i Loui s on a şifrey i vermekt e isteksiz davrandı . Loui s şüphelenmekt e haklıydı , şifrele r diğe r yönd e kul - lanılmak üzer e tasarlanmışlardı . İşleri n olağa n sürecind e on u arayan , tanımadığı kişini n güvenli k kodun u vermes i gerekirdi . B u Vinc e içi n ço k kritik bi r andı , tü m çabalarını n başarıy a ulaşı p ulaşmamas ı bun a bağlıydı .

Louis'in şüphes i karşısınd a Vinc e adam ı etkilem e çabasın ı artırara k acındırma ("doktor a gitme") , bask ı ("yapaca k yığınl a işi m va r v e saa t neredeyse dör t oldu") v e etkilem e ("on a ban a şifrey i vermediğin i söyle") yöntemlerine başvurdu . Akıllılı k edi p Vinc e aslınd a hi ç tehdi t kullanmadı , yalnızca im a etti : Eğe r ban a güvenli k şifresin i vermezse n arkadaşını n ihtiyacı ola n müşter i bilgilerin i göndereme m v e on a aslınd a gönderebile - cek durumd a olduğum u faka t seni n işbirliğ i yapmadığın ı söylerim .

Yine d e kabahat i Louis' e atmakt a acel e etmeyelim . N e d e ols a tele - fondaki kişi , arkadaş ı Angela'nı n bi r fak s beklediğin i biliyordu ; e n azın - dan biliyormu ş gib i görünüyordu . Arayan , güvenli k şifrelerinde n d e hab - erdardı v e onlar a atanmı ş harflerl e tanımlandıkların ı biliyordu . Arayan , şube müdürünü n dah a fazl a güvenli k içi n bunu n yapılmasın ı istediğin i söylemişti, istediğ i doğrulamay ı on a vermeme k içi n ortalıkt a bi r nede n görünmüyordu.

Louis yalnı z değildi . Bank a çalışanlar ı neredeys e he r gü n güvenli k şifrelerini toplu m mühendislerin e verirler . İnanılma z am a gerçek .

Özel bi r dedektifi n kullandığ ı yöntemleri n yasa l olmakta n çıkı p yasadışı olmay a başladığ ı inc e bi r çizg i vardır . Şub e numarasın ı aldığında Vinc e henü z yasadış ı değildi . Louis' i günlü k güvenli k şifrelerinden ikisin i vermey e kandırdığınd a d a yasadış ı birşe y yap - mamıştı. Bi r bank a müşterisini n bilgilerin i kendisin e fakslanmasın ı iste - diği and a çizgiy i aştı .

Ama Vinc e v e patron u içi n b u düşü k riskl i bi r suçtu . Par a y a d a ma l çaldığınızda biriler i onu n kaybolduğun u anlarlar . Bilg i çaldığınızd a çoğ u zaman bun u kims e far k etmez , çünk ü bilg i hâl â ellerindedir .

AAitnick Mesajı :

Sözel güvenlik şifreleri, verilerin korunması için elverişli ve güvenilir bir yön- tem sunmada parolalara denktirler. Ancak çalışanların toplum, mühendislerinin kullandığı dalavereler konusunda bilgili olmaları ve krallığın anahtarlarını tes- lim etmemek üzere yetiştirilmeleri gerekir.

Dalavereye Âle t Ola n Polisle r

Hilebaz bi r öze l dedekti f y a d a toplu m mühendis i içi n birini n ehliye t numarasını bilmesini n gerektiğ i durumla r sı k sı k ortay a çıkar . Örneğin , birini n banka hesaplarıyl a ilgil i bilg i alma k içi n onu n kimliğin e bürünme k istiyorsanız .

Birinin cüzdanın ı yürütme k y a d a uygu n bi r and a omuzunu n üzerinden gö z ucuyl a bakma k dışınd a ehliye t numarasın ı öğrenme k olanaksıza yakı n olmalıdır . Anca k ço k fazl a toplu m mühendisliğ i bece - rilerine sahi p olmaya n bir i içi n bil e b u pe k zo r bi r i ş sayılmaz .

Düzenli olara k ehliye t numaralar ı v e ara ç plak a numarala n öğren - mesi gereke n -kendisin e Eri c Mantin i diyeceğim - bi r toplu m mühendis i var. Eric , Motorl u Taşıtla r Müdürlüğü'n ü aramanı n v e bilg i almas ı gerek - tiğinde he p ayn ı oyun u oynamanın , içind e bulunduğ u tehlikey i gereksi z ölçüde artırdığın a kara r verd i v e b u sürec i kolaylaştırmanı n bi r yolunu n bulunup bulunmadığın ı araştırdı .

Büyük olasılıkl a dah a önc e kims e düşünmemişt i am a istediğ i and a bu bilgiy i almanı n bi r yolun u buldu . B u iş i Bölg e Motorl u Taşıtla r Müdürlüğü'nün yürürlüğ e koyduğ u bi r hizmette n yararlanara k yaptı . Pe k çok bölg e müdürlüğü , ayrıcalıkl ı bilgile r olmadıklar ı sürece , vatandaşlar- la ilgil i bilgiler i sigort a kurumlarına , öze l dedektifler e v e eyale t yasalar ı uyarınca ticareti n v e gene l toplumu n lehin e olma k kaydıyl a paylaş - manın uygu n olduğ u bell i başk a kuruluşlar a açmışlardı .

Motorlu Taşıtla r Müdürlüğü'nün , doğa l olarak , hang i tü r verileri n ve - rileceğine ilişki n uygu n kısıtlamalar ı vardır . Sigort a sektör ü dosyalarda n belli tü r bilgile r alabili r am a diğerler i alamaz . Öze l dedektifle r içi n farkl ı sınırlamalar geçerlidi r v e b u böyl e gider .

Emniyet teşkilat ı mensuplar ı içi n d e farkl ı bi r kura l geçerlidir . Motorl u Taşıtlar Müdürlüğü , kendin i uygu n şekild e tanıta n yeminl i bi r poli s memuruna kayıtlar ı ndak i tü m bilgiler i açacaktır . Eric'i n yaşadığ ı eyalett e Motorlu Taşıtla r Müdürlüğü'nü n bi r emniye t görevlisinde n istediğ i tanım - lamalar Tale p Kod u v e memuru n ehliye t numarasıydı . MT M çalışanı , bilgi vermede n önc e he r zama n memuru n adın ı ehliye t numarasıyl a v e başka bi r bilgiyl e -genellikl e doğu m tarihiyle - karşılaştıracaktı .

Toplum mühendis i Eric'i n yapma k istediği , kendin i bi r emniye t teşki - latı mensubunu n kimliğin e büründürmekte n başk a birşe y değildi . Bun u nasıl başaracaktı ? Polisler e bi r ter s dalaver e uygulayarak !

Eric'in Dalaveres i

Önce bilinmeye n numarala n arad ı v e eyale t başkentindek i Motorl u Taşıtlar Gene l Müdürlüğü'nü n telefo n numarasın ı istedi . Aldığ ı numar a 503-555-5000'di v e doğa l olarak , vatandaşı n aramas ı içi n ayrılmı ş tele -

fondu. Sonr a yakınlardak i bi r karakol u arayara k haberleşm e bürosun u -diğer emniye t teşkilat ı birimleriyle , ulusa l su ç ver i tabanıyla , yere l yetkililerle v e benzer i yerlerl e iletişimi n kurulduğ u birimi - istedi . Haberleşme bürosund a telefon a çıka n memur a Eyale t Motorl u Taşıtla r Genel Müdürlüğü'nü n emniye t teşkilatın ı aramas ı içi n ayrılmı ş numarayı öğrenme k istediğin i söyledi .

"Sen kimsin?" diy e sord u haberleşmedek i polis .

"Ben Al. 503-555-5753'ü arıyordum" ded i Eric . B u yar ı yarıy a varsayım v e yar ı yarıy a uydurulmu ş bi r numaraydı . Emniye t teşkilatın - dan gelece k telefonla r içi n MTM'd e kurula n öze l bür o numarasını n halka açı k numarayl a ayn ı bölg e kodun a sahi p olmas ı gerekird i v e son - raki ü ç basamağı n d a ayn ı olacağ ı neredeys e kesindi . Tü m bilmes i gereken so n dör t basamaktı .

Karakol haberleşm e büroların a dışarda n telefo n gelmezd i v e araya n kişi numaranı n çoğun u biliyordu . Teşkilatta n bir i olduğ u açıktı . "Numara 503-555-6127" ded i memur .

Artık Eric'i n elind e emniye t teşkilat ı mensuplarını n kullanımın a öze l MTM numaras ı vardı . Am a yalnızc a telefo n numaras ı onu n işin i gör - müyordu; o büronu n birde n fazl a telefo n hatt ı olmalıyd ı v e Eric'i n ka ç hat olduğun u v e he r birini n numarasın ı öğrenmes i gerekiyordu .

Santral

Planını uygulamay a koyma k için , emniye t teşkilatında n arayanları n

aramalarım yönlendire n MT M santralın a erişmes i gerekiyordu .

Telekomünikasyon Müdürlüğü'n ü arad ı ve en ço k kullanıla n ticar i tele -

fon santrallerinde n bir i ola n DMS-100'ler i ürete n Nortel'de n aradığın ı

söyledi. "DMS-100 üzerinde çalışan santral teknisyenlerinden biriyle

görüşebilir miyim?"

Teknisyen telefon u açtığında , Teksa s Norte l Tekni k Deste k Merkezi'nde n

aradığını v e tü m santrallar ı e n so n yazılıml a güncelleyebilme k içi n

merkezî bi r ver i taban ı oluşturdukların ı anlattı . He r şe y uzakta n yapıla -

caktı v e santra l teknisyenlerini n müdahalesin e gere k olmayacaktı . Anca k

santralın bilgisaya r bağlant ı numarasın a ihtiyaçlar ı vardı , böylec e gün -

cellemeleri doğruda n Deste k Merkezi'nde n yapabileceklerdi .

Oldukça akl a yatkı n görünüyord u v e teknisyen , Eric' e telefo n

numarasını verdi . Artı k eyaleti n telefo n santrallarmda n birin e doğruda n

bağlanabilecekti.

Tıpkı he r şirke t bilgisaya r ağınd a olduğ u gib i saldırganlar a karşı korun -

mak içi n b u tar z ticar i santralle r d e parol a korumalıdır . Telefo n

beleşçiliği geçmiş i ola n he r iy i toplu m mühendisinin bildiğ i üzer e

Nortel santralleri n yazılı m güncellemeler i içi n kullandığ ı standar t bi r

kullanıcı ad ı vardı : NT D (Norte l Tekni k Destek'i n ba ş harfleri , yan i . ço k gizl i bi r şe y değil) . Pek i ya parola ? Eri c pe k ço k ke z bağlanmay a

çalışarak, he r seferind e bari z v e sı k kullanıla n olasılıklar ı denedi . Kullanıcı adıyl a ayn ı harfleri , NTD , girme k d e iş e yaramadı . "Yardımcı" kelimes i d e olmadı , "yama " da .

Sonra "güncelleme"y i denedi.. . v e girdi . Başk a n e beklenird i ki ! Bariz , kolayca tahmi n edilebile n bi r parol a kullanılması , hi ç parol a olma - masından yalnızc a bi r nebz e dah a iyidir .

Konunuzda bilgil i olma k iyidir . Eric'i n o santrali n nası l programlandığ ı ve sorunları n nası l çözüldüğ ü hakkınd a büyü k olasılıkl a o telaıisye n kadar bilgis i vardı . Yetkil i bi r kullanıc ı olara k santral e eriştikte n sonr a hedefi ola n telefo n hatlar ı üzerind e ta m kontro l sağlayabilecekti . Emniyet teşkilat ı mensuplarını n MTM'y i arama k içi n kullandıklar ı numarayı, 555-6127 , bilgisayarında n arattırdı . Ayn ı müdürlükt e o n dokuz tan e dah a ha t olduğun u gördü . Görünüş e gör e arayanlar ı çoktu . Her gele n aramad a santra l meşgu l olmaya n birin i bulan a kada r yirm i hattı taramay a programlanmıştı.

Sıradaki o n seki z numaral ı hatt ı seçt i v e b u hatta n aramalar ı başk a bi r telefona yönlendirece k şifrey i girdi . Yönlendirile n telefo n numaras ı olarak d a yen i v e ucuz , hazı r kartl ı ce p telefon u numarasın ı kullandı . Bunlar, i ş bittikte n sonr a atacak kada r ucu z olduklar ı içi n uyuşturuc u kaçakçılarının terci h ettiğ i türde n telefonlardı .

On sekizinc i hatt â aram a yönlendirm e çalışı r durumdayken , büronu n ardarda gele n o n yed i telefonl a uğraştığ ı bi r sırad a bi r sonrak i telefo n MTM bürosund a çalmayaca k onu n yerin e Eric'i n ce p telefonun a yön - lendirilecekti. Arkasın a yasland ı v e beklemey e başladı .

MTM'ye gele n aram a

O saba h saa t sekizde n bira z önc e telefo n çaldı . B u işi n e n iy i v e e n ke - yifli bölümüydü . Toplu m mühendis i Eri c oturmuş , on u geli p tutukla - maya yetkil i y a d a bi r aram a emr i çıkarı p aleyhin e deli l toplama k içi n baskın yapabilece k bi r polisl e konuşuyordu .

Ve yalnızc a te k bi r poli s aramayacaktı , bi r bir i ardın a bi r sür ü poli s arayacaktı. Bi r keresind e Eri c bi r lokantad a arkadaşlarıyl a öğl e yemeğ i yerken he r be ş dakikad a bi r telefo n gelmiş , ödün ç aldığ ı bi r kaleml e bilgileri bi r kağı t peçeteni n üstün e yazmıştı . Bun a hâl â duru p duru p güler.

Ancak poli s memurlarıyla konuşma k iy i bi r topta n m\ı\"\«\4\s.m t te ç sıkıntı vermez . Aslınd a emniye t teşkilat ı birimlerin i kandırmanı n heye - canı Eric'i n oynadığ ı oyun u büyü k olasılıkl a dah a eğlencel i kılmıştır . Eric'in anlattığ ı kadarıyl a görüşmele r şöyl e geçiyordu :

"MTM, yardımcı olabilir miyim?"

"Ben Dedektif Andrew Cole."

"Merhaba dedektif. Bugün sizin için ne yapabilirim?"

Emniyet teşkilatınd a fotoğra f isteme k içi n kullanıla n terim i kullanarak

"005602789 nolu ehliyet için soundex gerekiyor" diyebilirdi . Bu , iş e yarar bi r şeydi ; örneği n polisle r bi r şüpheliy i tutuklamay a giderlerke n adamın ney e benzediğin i görme k içi n kullanırlardı .

"Elbette, hemen kayıtlara bakayım" diyord u Eric . "Detektif Cole, bağlı olduğunuz yer neresi?"

"Jefferson Bölgesi." Sonr a Eri c ası l sorula n sormay a başlıyordu : "Dedektif, talep kodunuz nedir?", "Ehliyet numaranız?", "Doğum tari- hiniz?"

Arayan, kişise l tanımlam a bilgilerin i veriyordu . Eri c bilgiler i doğrula - makla uğraşıyormu ş gib i yapıp , sonr a d a arayan a bilgilerini n doğru - landığını söylüyordu . E n sonund a arayanı n MTM'de n istediğ i şeyleri n ayrıntılarını soruyordu . İstene n ad ı arıyormu ş gib i yapıp , arayanı n tuşların tıklamasın ı duymasın ı sağlıyo r sonr a d a şöyl e bi r şe y diyordu . "Kahretsin, bilgisayarım yine çöktü. Kusura bakma, dedektif, bilgisa- yarım bu hafta hep gidip geliyor. Tekrar arayıp başka bir görevlinin size yardımcı olmasını isteyebilir misiniz?'"

Böylece nede n isteğind e yardımc ı olamadığıyl a ilgil i memu r beyd e herhangi bi r şüph e uyandırmada n açı k uçlar ı bağlıyordu . B u arad a Eri c bir kimli k çalmıştı . Bunlar , ihtiyac ı olduğ u zama n gizl i MT M bilgileri - ni almakt a kullanabileceğ i ayrıntılardı .

Eric birka ç saa t telefonlar a yanı t veri p düzinelerc e tale p kod u eld e ettikten sonr a santral e bağland ı v e yönlendirm e işlemin i ipta l etti . Sonraki aylarda , bilgiy i nası l aldığın ı bilme k istemeye n yasa l öze l dedektiflik firmalarını n on a verdiğ i işler i yapmay ı sürdürdü . Gerektiğ i zaman yenide n santral a bağlanıyor , yönlendirmey i açıyo r v e bi r yığı n polis memur u bilgis i dah a topluyordu .

Aldatmacanın İncelenmes i

Eric'in b u dalaverey i yapma k içi n bi r diz i insa n üstünd e oynadığ ı oyunları bi r gözde n geçirelim . İl k başarıl ı adımd a haberleşm e bürosun - daki bi r memurun , karşısındakin i başk a bi r poli s memur u varsayıp , hiç - bir kimli k tespit i yapmada n tamamıyl a yabanc ı birin e gizl i MT M telefo n numarasını vermesin i sağladı .

Sonra Eyale t Telekomünikasyo n Müdürlüğü'ndek i kiş i d e ayn ı şey i yaptı. Eric'i n santra l üreticis i firmad a çalıştığ ı iddiasın ı olduğ u gib i kabul etti v e MTM'y e hizme t vere n telefon santralını n dışarıda n bağlanm a numarasını bi r yabancıy a verdi .

Eric'in santral a erişebilmesini n nedeni , büyü k ölçüde , santra l üreti - cisinin tü m santrallarınd a ayn ı kullanıc ı adın ı kullanmasında n kay - naklanan zayı f güvenli k uygulamasıydı . B u dikkatsizlik , toplu m mühen - disinin parolay ı tahmi n etmesin i kolaylaştırdı , çünk ü santra l teknisyen - lerinin herke s gib i hatırlamas ı kola y olaca k parolala r seçeceğin i biliyordu .

Santrala eriştikte n sonr a MTM'ni n emniye t teşkilat ı telefo n hatların - dan birin i kend i ce p telefonun a yönlendirdi .

Hepsinin üstün e e n cüretkâ r kısı m olarak , birbir i ardın a poli s memurlarını kandırı p yalnızc a tale p kodların ı almakl a kalmadı , ayn ı zamanda onları n kend i kişise l bilgilerin i vermelerin i d e sağladı . Böylec e Eric onları n kimliğin e bürünebilecekti .

Bu dolab ı çevirme k içi n he r n e kada r tekni k bilg i gereks e de , bi r sahtekârla konuştukların ı bilmeye n bi r gru p insanı n yardım ı olmasayd ı bu dola p iş e yaramazdı .

Bu öykü , insanların , "Nede n ben? " diy e sormadıklar ı bi r durumu n bi r başka örneği . Haberleşm e büros u memur u nede n tanımadığ ı bi r poli s memuruna -y a d a b u durumd a olduğ u gib i kendin i poli s memur u olara k tanıtan birine - b u bilgiy i versi n ki ? Bilgiy i kend i mesa i arkadaşlarında n ya d a amirinde n almasın ı d a söyleyebilirdi . Verebileceği m te k yanıt , insanların b u soruy u kendilerin e sı k sı k sormamalar ı şeklind e olur . Sormak akılların a gelmiyo r mu ? Meyda n okuya n y a d a yardı m etmey e isteksiz bir i gib i gözükme k m i istemiyorlar ? Belk i de . Diğe r açıklamala r tahminden ötey e gitmez . Am a toplu m mühendisleri nedenlerl e ilgilen - mezler; yalnızc a bu küçü k gerçeğin , aks i durumd a alınmas ı zo r olaca k bilgileri almaların ı kolaylaştırmasıyl a ilgilenirler .

Aldatmacanın Engellenmes i

Doğru kullanıldığ ı takdird e bi r şifr e ço k öneml i bi r güvenli k önlemidir . Yanlış kullanıla n bi r güvenli k şifresi , hi ç olmamas ı kada r köt ü olabilir ; çünkü aslınd a va r olmaya n saht e bi r güve n hiss i uyandırır . Eğe r çalışan - larınız onlar ı gizl i tutamıyorlars a şifreleri n ne anlam ı var ?

Sözel güvenli k şifreler i kullanmas ı gereke n herhang i bi r şirketin , çalışanlarına b u şifreler i n e zama n v e nası l kullanacakların ı açıkç a anlatması gerekmektedir . İy i bi r eğitimle , b u bölümü n il k öyküsünd e geçen karakter , yabanc ı birin e güvenli k şifres i vermes i istendiğinde , kolaylıkla aşılabile n içgüdülerin i dinleme k zorund a kalmazdı . B u koşullar altında b u bilgini n on a sorulmamas ı gerektiğin i hissett i am a açık bi r güvenli k politikasını n olmamas ı -v e güçl ü bi r sağduyu - yelken - leri suy a indirmesin e nede n oldu .

Mitnick Mesajı :

Şirketinizde bir telefon santralı olsaydı, sorumlu kişi satıcıdan gelen ve bağlan- tı numarasını isteyen bir telefon karşısında ne yapardı? Ve bu arada, bu kişi santralın standart parolasını hiç değiştirmiş miydi? O parola herhangi bir sözlükte bulunabilecek, kolay tahmin edilebilir bir parola mıydı?

Ters Dalaver e 13 3

Güvenlik süreçlerinde , bi r çalışanı n doğr u olmaya n bi r güvenli k şifre - si talebind e bulunduğ u durumlar ı d a içere n adımla r olmalıdır . Tü m çalışanlar, günlü k şifr e y a d a parol a gib i tanımlam a bilgileriyl e ilgil i gele n şüpheli talepler i heme n bildirece k şekild e eğitilmelidirler . Ayrıc a istekt e bulunan kişini n kimliğini n onaylanmadığ ı durumlar ı d a habe r vermelidirler .

En azından , çalışan , arayanı n adını , telefo n numarasını , ofi s y a d a birimini no t etmeli , sonr a telefon u kapatmalıdır . Ger i aramada n önc e şir - kette o isimd e çalışa n birini n olu p olmadığın ı v e arayacağ ı telefonu n çevrimiçi y a d a basıl ı rehberdek i numarayl a uyuşu p uyuşmadığın ı kont - rol etmelidir . Çoğ u zama n b u basi t yönte m bil e arayanı n söylediğ i kiş i olup olmadığın ı anlama k içi n yeterlidir .

Şirketin çevrimiç i bi r rehbe r yerin e basıl ı bi r telefo n rehber i vars a kimlik tespit i işlem i bira z güçleşir . İş e yen i başlayanla r olur ; işte n ayrılanlar; insanları n birimleri , konumlar ı v e telefo n numaralar ı değişe - bilir. Basıl ı rehberle r basıldıklar ı gün , hatt â dah a dağıtılmada n önc e güncelliklerini yitirirler . Çevrimiç i rehberle r bil e he r zama n güvenili r değillerdir, çünk ü toplu m mühendisleri onlarl a nası l oynayacakların ı bilirler. Eğe r bi r çalışan , bağımsı z bi r kaynakta n telefo n numarasın ı doğrulayamıyorsa, ona , ilgil i kişini n yöneticisin i arama k gib i farkl ı bi r yo l kullanması konusund a talimatla r d a verilmelidir .

r

i-

Davetsiz

Dihhati

iln

İÇERİYE GİRME K

Dışarıdan birini n bi r şirke t çalışanını n kimliğin e bürünmes i v e güven - lik konusund a e n duyarl ı olanlar ı bil e inandıraca k kada r başarıl ı bi r tak - lit yapmas ı nede n b u kada r kolaydır ? Peki , güvenli k süreçlerin i ço k iy i bilen, tanımadıklar ı insanlar a şüpheyl e baka n v e şirketlerini n çıkarların ı korumak konusund a titi z davrana n kişiler i kandırma k nede n b u kada r kolaydır?

Bu bölümd e anlatıla n öyküler i okurke n b u sorula n aklınızd a tutun .

Mahcup Olmu ş Güvenli k Görevlis i

Gün/Saat: 1 7 Ekim , Salı , saba h 02:16 .

Yer: Skywatche r Havacılı k Şirketi'ni n Tucson-Arizon a dışındak i fabrikası .

Güvenlik Görevlisini n Öyküs ü

Deri ayakkabılarını n topuklarının , içind e neredeys e hi ç kimseni n bulunmadığı fabrikanı n zeminind e tıklayışm ı duyma k Lero y Greene' e gece saatlerin i güvenli k odasınd a vide o monitörlerin i seyredere k geçirmekten dah a iy i gelmişti . Orad a ekranlar a bakmakta n başk a bi r şey yapmasına , hatt â bi r derg i y a d a ciltl i İncil'in i okumasın a dah i izi n verilmiyordu. Oturu p hiçbi r şeyi n hareke t etmediğ i sabi t görüntüler e bakması gerekiyordu .

Ama koridorlard a gezinirke n e n azında n bacakları m açıyo r v e işin için e kollarım v e omuzların ı d a kattığ ı zama n bira z egzersi z yapmı ş oluyor - du. Lis e Amerika n futbol u takımınd a şehi r şampiyonasınd a sa ğ kana t oynamış bir i içi n b u pe k d e bi r egzersi z sayılmazdı . Yin e d e i ş iştir , diy e düşündü.

Güneybatı köşesin i dönd ü v e bi r kilometr e uzunluğundak i üreti m alanına baka n köprüde n yürümey e başladı . Aşağıy a bakt ı v e ik i kişinin , yapımı tamamlanmamı ş helikopterleri n üreti m hattını n yanında n geçtiklerini gördü . Geceni n b u saat i içi n tuha f bi r görüntüydü . "Kontrol etsem iyi olacak" diy e düşündü .

Leroy, on u üreti m alanınd a ikilini n arkasın a çıkaraca k merdivenler e doğru yöneld i v e o ta m yanların a gelen e kada r adamla r onu n geldiğin i hissetmediler. "Günaydın. Güvenlik kartlarınızı görebilir miyim lütfen" dedi. Lero y böyl e anlard a he p sesin i yumuşa k tutmay a çalışırdı ; sadec e cüssesinin bil e ürkütüc ü gözükebileceği m biliyordu .

"Merhaba Leroy", ded i bi r tanesi , yak a kartında n adın ı okuyarak . "Ben Tom Stilton, Phoenbc'deki Genel Müdürlük pazarlama bölümünden. Toplantı için şehre geldim ve arkadaşıma dünyanın en iyi helikopter- lerinin yapıldığı yeri göstermek istedim."

"Evet. Kartınız lütfen" ded i Leroy . N e kada r gen ç olduklar ı gözünde n kaçmamıştı. Pazarlamad a olduğun u söyleyen , lisey i yen i bitirmi ş gib i duruyordu, diğerini n saçlar ı omuzların a kada r iniyo r v e o n be ş yaşlarında görünüyordu .

Kısa saçl ı olan , kartı m çıkarma k içi n elin i cebin e att ı sonr a tü m cepleri - ni yoklamay a başladı . Lero y birdenbir e b u işl e ilgil i köt ü bi r hiss e kapıldı. "Kahretsin" ded i adam . "Arabada bırakmış olmalıyım. Gidip alabilirim; park yerine gidip gelmem on dakika sürmez."

Leroy b u arad a no t defteri m çıkarmıştı . "Adınız n e demiştiniz?" diy e sordu v e aldığ ı cevab ı dikkatl e no t etti . Sonr a d a Güvenli k Ofisi'n e kadar onunl a gelmelerin i ric a etti . Tom , asansörd e alt ı aydı r şirkett e çalıştığını v e b u yüzde n başını n belay a girmesin i istemediğin i söyledi . Güvenlik odasınd a Lero y ikiliy i sorgularke n gec e devriyesinde n ik i kişi dah a onlar a katıldı . Stilto n kend i telefo n numarasın ı verd i v e müdürünün Jud y Undenvoo d olduğun u söyleyere k onu n telefo n numarasını d a verdi . Bilgile r bilgisayardak i verilerl e uyuyordu . Lero y diğer ik i güvenli k görevlisin i bi r kenar a çekt i v e aralarınd a n e yap - maları gerektiğin i konuştular . Kims e b u işt e yanlı ş birşe y yapma k istemiyordu. Üç ü de , kadın ı geceni n bi r yansınd a yatağında n kaldır - mak anlamın a gels e d e müdür ü aramanı n e n iyis i olduğun u düşünüyor - lardı.

Leroy Baya n Undervvood' u kendis i aradı , ki m olduğun u anlatt ı v e ken - disiyle birlikt e çalışa n To m Stilto n adl ı birini n olu p olmadığın ı sordu . Kadının ses i yar ı uykul u geliyordu . "Evet" dedi .

"Sabah 2:30'da onu üzerinde kimlik kartı olmadan üretim hatlarının bulunduğu alanda bulduk."

"Onunla konuşayım" ded i Baya n Undenvood .

Stilton telefon a çıkt ı v e "Judy, gecenin ortasında b u adamlar seni uyandırdığı için çok üzgünüm. Umarım bu benim aleyhime bir durum olmaz." dedi .

Adam dinled i v e sonr a deva m etti . "Yeni basın açıklamasıyla ilgili toplantı için zaten sabah erkenden burada olmam gerekiyordu. Her neyse, Thompson anlaşmasıyla ilgili e-postayı aldın mı? Bu işi kaybet- memek için Pazartesi sabahı Jim'le görüşmemiz gerekiyor. Ve sai: günkü öğle yemeği planımız hâlâ geçerli, değil mi?"

Biraz dah a dinledi , hoşçaka l ded i v e telefon u kapattı .

Bu Leroy' u şaşırttı ; kadm m he r şeyi n yolund a olduğun u kendisin e d e söylemesi içi n telefon u ger i alacağın ı düşünüyordu . Müdür ü tekra r arayıp on a bun u soru p sormamas ı gerektiğin i düşünd ü am a sonıv .

vazgeçti. Geceni n ortasınd a on u zate n bi r ker e rahatsı z etmişti , ikinc i bir ker e arayaca k olurs a sinirlenebili r v e kendisin i müdürün e şikaye t edebilirdi. "Ortalığı karıştırmaya n e gerek var?" diy e düşündü . Stilton, "Üretim hattının kalanını arkadaşıma göstermemde bir salan- ca var mı?" diy e sord u Leroy'a . "Bizimle gelip yanımızda durmak ister misiniz? "

"Gidebilirsiniz" ded i Leroy . "Gezin ama bir dahaki sefere kartınızı unutmayın. Ve mesai saatleri dışında fabrikada kalacaksanız güvenliği haberdar edin. Kural böyle."

"Bunu unutmam Leroy", ded i Stilto n v e gittiler .

Daha o n dakik a geçmemişt i k i Güvenli k Ofisi'ndek i telefo n çaldı . Arayan Baya n Undenvood'du . " O adam kimdi?", diy e sordu . Sürekl i soru sormay a çalıştığın ı am a adamı n konuşmasın ı kesmeyi p öğle n yemeğe çıkmakta n fala n sö z ettiğin i anlatt ı v e kad m onu n ki m olduğunu bilmiyordu .

Güvenlik görevliler i danışmay ı v e par k yer i girişind e görevl i bekçiy i aradılar. He r ikis i d e birka ç dakik a önc e ik i gen ç adamı n çıktığın ı söylediler.

Sonradan öyküy ü anlatırke n Lero y he r zama n şöyl e bitiriyordu ; "Tanrı biliyor patron beni baştan aşağı fırçaladı. Hâlâ bir işim olduğu için çok şanslıyım."

Joe Harper'ı n Öyküs ü

On yed i yaşındak i Jo e Harpe r yalnızc a nele r bulabileceğin i mera k ettiği içi n bi r yılda n uzu n süredir , baze n gec e baze n gündü z binalar a giriyordu. He r ikis i d e gec e çalışan , müzisye n bi r babanı n v e koktey l garsonu bi r anneni n oğl u olara k Joe'nu n kend i başın a geçirece k ço k zamanı vardı . Ayn ı olay a ai t kend i öyküs ü he r şeyi n nası l geliştiğin e eğitici bi r ışı k tutmaktadır :

Helikopter pilot u olma k isteye n Kenn y adınd a bi r arkadaşı m var . Helikopterleri yaptıklar ı üreti m alanı m görme k içi n on u Skywatche r fabrikasına soku p sokamayacağım ı sordu . Dah a önc e başk a yerler e girdiğimi biliyordu . Girmeme m gereke n yerler e girmey e çalışma k benim içi n ta m bi r heyeca n firtmasıdır .

Ancak bi r fabrikay a y a d a ofi s binasın a elin i kolun u sallayara k gire - mezsin. Üzerind e düşünmeli , planla r v e hedefl e ilgil i ta m bi r keşi f yap - malısın. Adlar , unvanlar , raporlam a yapıs ı v e telefo n numaralar ı içi n şirketin interne t sayfasın a bakar , gazet e kupürlerin i v e derg i yazıların ı okursun. Beni m güvenli k anlayışım ı titi z bi r araştırm a oluşturur ; b u yüzden ban a meyda n okuya n herkesle , bi r çalışa n kada r bilgil i bi r şe - kilde konuşabilirim .

Bu durumd a nerede n başlayacaktım? Önc e internette n şirketi n nerel -

erde bürolarını n olduğun a baktı m v e şirke t Gene l Müdürlüğü'nü n Phoenix'de olduğun u öğrendim . Mükemmel . Arayı p pazarlam a bölümünü istedim ; he r şirketi n bi r pazarlama bölüm ü vardır . Telefon u bir hanı m açt ı v e on a Blu e Penci l Graphics'de n aradığım ı söyleyerek , hizmetlerimizden yararlanma k isteyi p istemeyeceklerin i öğrenme k içi n kiminle konuşma m gerektiğin i sordum . İlgilini n To m Stilto n olduğun u söyledi. Telefo n numarasın ı istedi m am a kadı n ban a b u bilgiy i dışar ı vermediklerini anca k ben i on a bağlayabileceğin i söyledi . Stilton' m telefonunu telesekrete r açt ı v e sesl i mesa j şöyl e dedi , "Ben Grafik Bölümü'nden Tom Stilton, dahilî 3147, lütfen mesaj bırakınız." Dışar ı dahili numar a vermiyorlard ı am a b u ada m bıraktığ ı sesl i mesajd a ken - disinkini veriyordu . B u iyiydi . Artı k elimd e bi r a d v e bi r dahil î numar a vardı.

Aynı ofis i bi r ke z dah a aradım . "Merhaba, Tom Stilton'u arıyordum ama yerinde yok. Müdürüne birkaç küçük soru sormak istiyordum. ' y Müdürü d e dışardaydı , am a işi m bittiğind e müd'irünü n d e adın ı öğren - miştim. V e o d a nazi k bi r şekild e sesl i mesajın d a dahil î numarasın ı bırakmıştı.

Herhalde danışm a görevlisinde n zorlanmada n geçebilirdi m am a fab - rikanın orada n arabayl a geçmişti m v e par k yerini n çevresind e te l çi t olduğunu hatırlıyordum . Çi t demek , içer i girmey e çalıştığınızd a siz i kontrol etme k isteye n bi r bekç i demektir . Geceler i plakalar ı no t ediyo r olabilirlerdi; b u yüzde n bi t pazarında n esk i bi r plak a alma k zorund a kaldım.

Ama önc e bekç i kulübesini n telefo n numarasın ı bulma m gerekiyordu . Yeniden aradığımd a ayn ı santra l memur u çıkars a ben i tanımaması içi n biraz bekledim . Sonr a aradı m v e dedi m ki , "Ridge Caddesi bekçi kulübesindeki telefonun sürekli gidip geldiği yolunda bir şikâyet almıştık; sorun devam ediyor mu?" Santra l memur u kadı n bilmediğin i söyledi am a ben i oray a bağlayacaktı .

Telefonu bi r ada m açtı . "Ridge Caddesi kapısı, ben Ryan." "Merhaba Ryan, adım John." dedim . "Orada telefonlarla ilgili bir sorun yaşıyor musunuz? " Ada m yalnızc a düşü k ücretl i bi r güvenli k görevlisiyd i am a sanırım bira z eğiti m almıştı ; çünk ü hemen , "Adınız John muydu? Soyadınız neydi?" diy e sordu . Sank i on u duymamı ş gib i konuşmay ı sürdürdüm. "Daha önce biri arayıp bir sorun olduğunu söylemişti". Telefonu ağzında n uzakt a tutu p bağırdığı m duyabiliyordum . "Hey, Bruce, Roger. B u telefonda bir sorun olmuş muydu?" Tekra r ahizey i kulağına götürd ü v e "Hayır, bildiğimiz kadarıyla hiç sorun çıkmamış." dedi.

"Orada kaç hat var? "

Adımla ilgilenmey i tamame n bırakmıştı . "İki" dedi .

"Şu anda hangisini kullanıyorsun?"

İçeriye Girme k 14 1

"3140."

Yakaladım! "Her ikisi d e çalışıyor mu?"

"Öyle görünüyor."

"Tamam" dedim . "Tom, eğer herhangi bir sorunla karşılaşırsanız, teknik servisi aramanız yeterli. Seve seve yardımcı oluruz." Arkadaşım v e be n heme n ertes i gec e fabrikay ı ziyare t etmey e kara r verdik. Akşamüstün e doğr u pazarlamadak i adamı n adın ı kullanara k nöbetçi kulübesin i aradım . "Merhaba , be n Grafi k bölümünde n To m Stilton. Zorl u bi r tesli m tarih i yaklaşıyo r v e biz e yardı m etme k içi n şehre gelece k birka ç arkada ş var . Büyü k olasılıkl a saba h birde n ikide n önce orad a olmazlar . O saatt e vardiyanı z deva m ediyo r mu? " Hayır dediğ i içi n mutluydu ; gec e yarıs ı çıkıyordu .

"Bir sonraki adam için bir not bırak" dedim . "İki kişi gelip d e Tom Stilton'u görmek istediklerini söylerlerse, onları içeri alsın, olur mu?" Evet, ded i ada m soru n olmazdı . Adımı , bölümüm ü v e dahil i numaram ı aldı v e ilgileneceğin i söyledi .

İkiyi bira z geç e arabayl a kapıy a gittik , To m Stilton'ı n adın ı verdi m v e uykulu bi r bekç i içer i girmemi z gereke n kapıy ı işare t ett i v e nerey e park etmemi z gerektiğin i gösterdi .

Binaya girdiğimizde , danışmada , he r zamank i mesa i saatler i dış ı imzalarının atıldığ ı bi r güvenli k noktas ı dah a vardı . Görevliy e sabah a bitirmem gereke n bi r rapo r olduğun u v e b u arkadaşımı n fabrikay ı görmek istediğin i söyledim . "Helikopterlere bayılır" dedi m "Sanırım helikopter kullanmayı öğrenmek istiyor." Bende n kartım ı istedi . Elim i cebime attı m sonr a üstüm ü yokladı m v e arabad a bırakmı ş olabileceği - mi söyledim . "Gidip alayım" dedim . "On dakika sürer." Ada m ise , "Boş ver, sorun yok, imzalaman yeterli." dedi .

Üretim hatt ı boyunc a yürüme k ço k iyiydi . T a k i o ça m yarmas ı Lero y bizi durduran a kadar .

Güvenlik ofisinde , şirke t çalışan ı olmaya n birini n ço k sinirl i v e kork - muş davranacağın ı anladım . İşle r iyic e karıştığında gerçekte n kızmı ş gibi davrandım . Sank i gerçekte n söylediği m kişiymişi m d e ban a inan - mamalarına bozulmuşu m gibi.

Müdürüm olduğun u söylediği m kadın ı arayı p aramayacakların a kara r vermeye v e e v numarasın ı bilgisayardan bulmay a çalışırlarke n bi r a n için, "Tabana kuvvet kaçmanın tam zamanı" diy e düşündüm . Am a işi n içinde par k yer i kapıs ı vardı , binada n çıkmay ı basarsa k bile . kapıy ı kapatırlardı v e bi z hepte n içerd e kalırdık .

Leroy, Stilton'u n müdür ü ola n kadın ı arayı p sonrasınd a telefon u ban a verdiğinde kadı n ban a bağırmay a başladı . "Kimsiniz, kiminle konuşu- yorum ? " ded i am a be n d e sank i tatl ı bi r sohbe t ediyormışcasın a konuş - maya deva m ettim , sonr a d a telefon u kapattım .

Gecenin ortasınd a şirke t numarasın ı verebilece k birin i bulma k n e kada r zaman alır ? Kadı n güvenli k ofisin i arayı p adamlar ı uyarmada n önc e buradan çıkma k içi n o n be ş dakikada n a z zamanımı z olduğun a kara r verdim.

Çok acelemi z varmı ş gib i görünmede n orada n çıkabildiğimi z kada r hızlı çıktık . Kapıdak i bekç i biz e e l sallamakl a yetindiğind e kesinlikl e çok ferahlamıştık .

Aldatmacanın İncelenmes i

Bu hikâyeni n dayandığ ı gerçe k olayd a saldırganları n gerçekte n ergenlik çağınd a gençle r oldukların ı vurgulamakt a yara r var . içer i girm e girişimi b u işte n sıyrılı p sıyrılmayacakların ı görme k içi n yaptıklar ı bi r eğlenceydi. Am a bi r çif t gen ç içi n b u kada r kola y olduys a yetişki n hırsız - lar, sanay i casuslar ı y a d a teröristle r içi n ço k dah a kola y olurdu .

Üç deneyiml i güvenli k görevlis i bi r çif t davetsi z misafiri n ellerin i kol - larını sallayara k gitmelerin e nası l izi n verdiler ? Üsteli k bunla r herhang i iki kiş i değil , maku l birin i kuşkuy a düşürece k kada r gen ç bi r ikiliyken .

Leroy önceler i doğr u bi r hareke t yapı p şüphelenmişti . Onlar ı Güvenlik Ofisi'n e götürmekt e v e adını n Tö m Stilto n olduğun u söyleye n adamı sorgulayarak , verdiğ i adlar ı v e telefon numaraların ı kontro l etmekte haklıydı . Yöneticisin e telefon etme k konusundak i karar ı d a so n derece yerindeydi .

Ama sonund a gen ç adamı n kendin e güvenin e v e öfkesin e aldandı . Bir hırsı z y a d a içer i zorl a girmey e çalışa n birinde n beklenece k türde n bir davranı ş değildi ; yalnızc a bi r çalışa n böyl e davranabilirdi.. . Y a d a Leroy öyl e olacağın ı varsaymıştı . Lero y hislerin e değil , sağla m kimli k tespitine inanaca k şekild e eğitilmeliydi .

Genç ada m telefonu , kendisin e vermede n kapattığınd a nede n dah a fazla kuşkulanmamıştı ? Böylec e Leroy , kimliği n doğrulun u doğruda n Judy Underwood'da n öğrenebili r v e çocuğu n gec e ge ç saatt e fabrikad a bulunmasının bi r neden i olduğun a dai r onda n güvenc e alabilirdi .

Mitnick Mesajı :

Etkileyici insanların çoğu zaman çekici kişilikleri vardır. Genellikle hızlı harekete geçerler ve oldukça konuşkandırlar. Toplum mühendisleri de işbirliği yaptıracak şekilde insanların düşünce süreçlerini bozmakta ustadırlar. Herhangi birinin bu tarz bir etkilemeye açık olmadığını düşünmek toplum mühendisinin becerilerini ve avlanma güdüsünü hafife almak olur.

Öte yandan iyi bir toplum mühendisi hiç bir zaman hasmını hafife almaz.

içeriye Girme k 14 3

Leroy öyl e cüretkâ r bi r dalaverey e gelmişt i k i durum u şa k diy e görmesi gerekirdi . Am a bi r d e onu n bakı ş açısında n bakalım : Bi r lis e mezunu, i ş endişesi , geceni n ortasınd a bi r şirke t yöneticisin i ikinc i ke z rahatsız etmeni n kend i başın ı derd e soku p sokmayacağ ı düşüncesini n getirdiği kararsızlık . Eğe r si z onu n yerind e olsaydınız , ikinc i aramay ı yapar mıydınız? "

Ancak doğa l olara k ikinc i aram a te k olas ı hareke t değildi . Güvenli k görevlisi başk a n e yapabilirdi ?

Müdüre telefon etmede n önc e ikilide n resiml i kimli k belgeler i göster - melerini isteyebilirdi . Fabrikay a arabayl a gelmişlerdi , yan i e n azında n birinin sürüc ü ehliyet i vardı . İşi n başınd a saht e isi m verdikler i heme n ortaya çıkard ı (profesyone l bir i elind e saht e bi r kimlikl e gelebilird i am a bu gençle r öyl e bi r önle m almamışlardı) . He r koşuld a Lero y kimli k bel - gelerini inceleyi p bilgiy i no t etmeliydi . İkis i d e üzerlerind e kimli k olmadığını söyleyece k olsalardı , b u durumd a onlar ı arabay a kada r götürüp "To m Stilton"u n orad a bıraktığın ı söylediğ i şirke t kimli k kartın ı alacaklardı.

Telefon görüşmesini n ardından , güvenli k ekibinde n biri , binada n ayrılana kada r ikisiyl e birlikt e kalmalıydı . Sonr a arabaların a kada r onlar - la birlikt e gitmel i v e plakaların ı no t etmeliydi . Eğe r yeterinc e dikkatl i biriyse (saldırganı n bi t pazarında n aldığı) plakanı n geçerl i bi r kayı t pulu - na sahi p olmadığın ı görürdü . B u d a durum u dah a derinlemesin e incele - mek üzer e ikisin i alıkoyma k içi n yeterl i bi r nedendi .

Çöp Dalış ı

Çöp dalışı terimi , iş e yara r bilgile r bulma k içi n hedefi n çöpün ü karıştırma iş i içi n kullanılır . B u yöntem i kullanara k bi r hedefl e ilgil i eld e edebileceğiniz bilg i miktar ı şaşırtıcıdır .

Çoğu insa n neler i attığın a pe k dikka t etmez : telefon faturaları , kred i kartı ekstreleri , reçetel i ila ç kutuları , bank a faturaları , işl e ilgil i belgele r ve dah a nele r neler .

İş yerlerind e çalışanlar , birilerinin , işlerin e yarayaca k bilgiler i bulma k için çöpler i karıştırdıklar ı konusund a uyarılmalıdırlar .

Lise yıllarımd a yere l telefon şirket i binalarını n arkasındak i çöpler i karıştırmaya giderdim . Genellikl e yalnı z olurdu m am a arad a bi r telefon şirketlerine benze r bi r ilg i duya n başk a arkadaşlarl a d a gittiği m olurdu . Çöp dalışınd a bi r ker e ustalaştını z mı , birka ç numar a kapıyordunuz ; örneğin tuvaletlerde n gele n çö p torbalarında n uza k durma k içi n öze n göstermeyi v e eldive n giymeni n önemin i kavrama k gibi .

Çöp dalış ı eğlencel i değildir , am a getiriş i inanılmazdır-şirketi n dahl î

Terimler

telefon rehberleri , bilgisaya r kullanı m

kılavuzları, çalışa n listeleri , santra l cihaz -

ÇÖP DALIŞI: Ya kendi

larının nası l programlandığın ı göstere n

başına değerli olan ya da

atılmış çıktıla r v e dah a fazlası - heps i dahilî telefon numaraları ve

orada durmu ş alınmay ı beklerler .

unvanlar gibi toplum

Yeni rehberleri n çıktığ ı akşamlard a mühendisliği sırasında kul-

çöp ziyaretler i yapardım , çünk ü çö p

lanılabilecek araçlar olan

bidonlarında düşünmede n atılmı ş yığın -

atılmış bilgileri bir şirketin

la esk i rehbe r olurdu . Başk a tuha f çöpünden (genellikle dışarı-

zamanlarda d a baz ı ilgin ç bilg i cevher -

da ve korumasız olan bir

leri içerebilece k no t kâğıtları , mektuplar ,

çöplükten) toplama işi.

raporlar gib i şeyle r bulma k içi n giderdim .

Gittiğimde önc e mukavv a kutula r bulur, bunlar ı çeki p çıkarır , bi r kenar a koyardım . Bir i ban a n e yaptığım ı soracak olursa , k i b u arad a sırad a olurdu , bi r arkadaşımı n taşındığın ı v e ona yardımc ı olma k içi n kut u topladığım ı söylerdim . Bekçiler , götürme k için kutular a koyduğu m belgeler i hiçbi r zama n far k etmezdi . Baz ı durum - larda ban a çeki p gitmem i söylerlerdi , be n d e başk a bi r telefo n şirketini n merkez binasın a giderdim .

Bugün nası l bilmiyoru m am a o zamanla r hang i torbalard a ilgin ç bi r şeylerin olabileceğin i anlama k kolaydı . Yerde n süpürüle n tozla r v e kan - tin çöpler i doğruda n büyü k torbalar a koyulurken , ofi s çö p kutularınd a temizlikçilerin bi r bi r çıkarı p ağızların ı bağladıklar ı beyaz , te k kullanım - lık çö p torbalar ı kullanılırdı .

Bir keresinde , arkadaşlarl a birlikt e karıştırırke n ell e yırtılmı ş kağıtla r bulduk. Sadec e yırtılmakl a kalmamış , biriler i üşenmeyi p kağıtlar ı küçü k parçalara d a ayırmıştı . Heps i birden , kullanışl ı bi r şekild e te k bi r yirm i litrelik çö p torbasın a doldurulmuştu . Torbay ı civardak i çöre k dükkân - larından birin e götürdük , parçala n bi r masay a yaydı k v e hepsin i te k te k birleştirmeye başladık .

Hepimiz yapbo z yapa n kişilerdik , o yüzde n b u biz e de v bi r yapbozu n heyecan veric i meyda n okumasın ı yaşatıyordu.. . Am a sonucun a bakılır - sa, çocuks u bi r heyecanda n dah a fazlasın ı içeriyordu . Tamamlandığın - da, şirketi n kriti k bilgisaya r sistemlerinde n birin e ai t tü m kullanıc ı adlar ı ve parolalarını n bulunduğ u bi r list e ortay a çıkmıştı .

Çöp dalış ı maceralarımı z gösterdiğimi z çabay a v e aldığımı z risk e değer miydi ? Kesinlikl e değerdi . Düşündüğünüzde n dah a d a fazlasın a değerdi, çünk ü b u işi n tehlikes i sıfırdı . O zamanla r böyleydi , bugü n d e böyle. Arazilerin e izinsi z girmediğini z sürec e başkalarını n çöpün ü karıştırmak yüzd e yü z yasaldır .

Doğal olara k kafaların ı çöp e sokanla r bi r te k telefon beleşçiler i v e bilgisayar korsanlar ı değildir . Ülkedek i tü m poli s kuvvetleri , düzenl i

içeriye Girme k 14 5

aralıklarla çöplerde n bilg i toplarla r v e mafy a babalarında n tutu n d a basi t hırsızlara kada r bi r yığı n insa n çöplerde n toplana n kanıtlar a dayandırılarak hükü m giymiştir . Bizimk i d e dahil , istihbara t örgütler i b u yola yıllardı r başvurmaktadırlar .

James Bon d içi n aşağılı k bi r yönte m olabilir . Sinemaseverle r on u dizlerinin üstünd e çö p karıştırırke n değe r d e kurnazc a düşmanın ı al t edi p bir fıstığ ı yatağa atarke n görmey i terci h edeceklerdir . Değerl i bi r şe y muz kabuklarını n v e kahv e artıklarını n arasında n çıkarabildiğind e gerçek casusla r o kada r müşkülpesent değildirler . Özellikl e çöpte n bilg i toplamak tehlikey e atılmalarını önleyecekse .

Şirketler d e çö p dalış ı oyunun u oynarlar . Gazeteleri n Hazira n 2000'd e bayram ettikler i bi r gü n vardı , Oracl e şirketini n (Oracl e Gene l Müdür ü Larr y Ellison herhald e ülkeni n e n lafın ı esirgemeye n Microsof t karşıtıydı) bi r araştırma şirket i tuttuğun u v e araştırm a şirketini n suçüst ü yakalandığın ı yazıyorlardı. Görünüş e göre , araştırmacılar , Microsoft'u n desteklediğ i AC T adlı bi r halkl a ilişkile r şirketini n çöpün ü istiyorlard ı am a yakalanm a tehlikesini göz e alamadılar . Basınd a çıkanlar a gör e araştırm a şirket i bi r kadın göndermi ş v e kadı n AC T çöp ü karşılığınd a kapıcılar a 6 0 dola r tekli f etmişti. Kapıcıla r teklif i ger i çevirmişlerdi . Ertes i gec e kadı n yin e gelmi ş v e teklifini 50 0 dolar a çıkarmış , başlarındak i adam a d a 20 0 dola r tekli f etmişti .

Kapıcılar kadın a "hayır " demişler , sonr a d a polis e habe r vermişlerdi .

Önde gele n interne t gazetecilerinde n Decla n McCullah , edebiyatta n esinlenerek, konuyl a ilgil i VVire d New s yazısını n başlığın ı şöyl e atmıştı , "MS'yi Gözetleye n Oracl e Olmasın? " Tim e dergis i doğruda n Oracl e Genel Müdür ü Ellison' u mimleyip , yazısın ı başlığın ı basitçe , "Dikizc i Larry," şeklind e belirlemişti .

Aldatmacanın İncelenmes i '

Benim yaşadıklarım a v e Oracle'ı n yaptığın a bakara k nede n biri - lerinin başkalarını n çöpün ü çalma k isteyeceğin i mera k edebilirsiniz .

Yanıt, sanırım , tehlik e boyutunu n sıfı r am a kazancı n hatır ı sayılı r olması olurdu . Tamam , belk i kapıcılara rüşve t verme k sonuçları n istendiği gib i olm a olasılığın ı artırı r am a bira z kirlenmey i göz e ala n bir i için rüşve t gerekl i değildir .

Bir toplu m mühendis i içi n çö p dalışlarını n kend i faydalar ı d a vardır . Hedef şirket e yapacağ ı saldırıy ı yönlendirebilece k kada r isim , bölümler , unvanlar, telefo n numarala n v e proj e görevlendirmeler i gib i bilgiler i bulabileceği, aralarınd a no t defterleri , ajandalar , mektupla r ve benzer i şeyler ola n eşyala r toplayabilir . Çöplerden , şirke t kurulu ş şemaları , şir -

Mitnick Mesajı :

Sizin çöpünüz düşmanınızın hazinesi olabilir. Özel yaşamımızda attığımız eşya- ların çok üzerinde durmayız; o zaman neden iş yerindeki insanların farklı bir yaklaşımı olması gerektiğine inanıyoruz? Her şey işgücünü tehlikeler (değerli bilgiler arayan ahlaksızlar) ve verilen açıklara (öğütücüden geçirilmemiş ya da doğru dürüst silinmemiş hassas bilgiler) konusunda eğitmekte bitiyor.

ket yapısıyl a ilgil i notlar , yolculu k tarihler i v e bunu n gib i bilgile r çıkabilir . Tüm b u ayrıntıla r içeride n birin e önemsi z gib i görünebilir , anca k bi r saldırgan içi n fazlasıyl a değerli bilgile r olabilir .

Mark Josep h Edvvards , Internet Security with Windows N T adl ı kitabında kimilerin e sadec e çö p gib i görüne n materyallerde n "yazı m hataları yüzünden atılmı ş raporlar , kâğı t parçaların a yazılmı ş parolalar , üzerlerinde telefon numaras ı ola n 'sen i surda n aradılar ' gib i notlar , içinde hâl â evra k ola n klasörler , silinmemi ş y a d a imh a edilmemi ş disketler v e bantlar ; heps i d e olas ı bi r saldırgan a yardımc ı olaca k şeylerdir." diy e bahseder .

Yazar deva m ede r v e ş u soruy u sorar : ".. . temizlikç i olara k çalışa n kişiler kimlerdir ? Temizlikçileri n bilgisaya r odasın a girmemesin e kara r vermişsinizdir; am a unutmayı n k i çö p kutular ı girebilir . Eğe r federa l kurumlar çö p kutuların a v e kâğı t öğütücülerin e erişim i ola n insanlar a sicil soruşturmas ı yapmay ı gerekl i görüyorlarsa , belk i si z d e bun u yap - malısınız."

Küçük Düşe n AAüdü r

Harlan Forti s he r zamank i gib i Bölg e Otoyo l Dairesi'ndek i işin e geldiği zama n kims e bi r tuhaflı k olduğun u düşünmemişti . Evde n aceleyl e çıktığını v e kartın ı unuttuğun u söyledi . Güvenli k görevlisi , burad a çalıştığı ik i yıllı k sür e boyunc a Harlan'ı n haft a iç i he r gü n ofis e giri p çık - tığını görmüştü . Geçic i bi r çalışa n kart ı verere k bi r imz a attırd ı v e ada m işinin başın a gitti .

iki gü n sonr a işle r karışmay a başladı . Hikây e tü m bölüm e sama n alevi gib i yayıldı . Duya n insanları n yarıs ı olayı n doğr u olamayacağın ı düşünüyordu. Kalanla r is e kahkahalarl a gülsünle r m i yoks a zavall ı adama acısınla r m ı bilemiyorlardı .

Ne d e ols a Georg e Adamso n nazi k v e sevece n bir i v e başların a gelen e n iy i bölü m yöneticisiydi . Yaşadıkların ı ha k etmemişti . Yan i hikâyenin gerçe k olduğ u düşünülürse .

Sorun, George'u n bi r cum a gün ü ge ç saatt e Harlan' ı odasın a

içeriye Girme k 14 7

çağırıp, elinde n geldiğ i kada r nazi k bi r şekild e pazartes i gün ü yen i bi - rimine gitmesini n gerektiğin i söylemesiyl e başladı ; Sağlı k Hizmetler i Dairesi'ne. Harla n içi n b u işte n atılma k gib i değildi . Dah a d a kötüydü ; küçük düşürücüydü . Sesin i kısı p bun u siney e çekmeyecekti .

Aynı akşam , sundurmasınd a oturmuş , evlerin e döne n insanlar ı seyrediyordu. Sonund a ayn ı mahalled e otura n Davi d adındak i çocuğ u gördü. Okulda n mobiletiyl e ev e döne n o çocuğ a herke s "Sava ş Oyunlan'ndaki Çocuk " diyordu . David' i durdurdu ; b u ama ç içi n aldığ ı Mountain De w Cod e Re d içeceğin i verd i v e on a bi r i ş tekli f etti : Bilgisayarlarla ilgil i yardı m v e ağzın ı sık ı tutmas ı karşılığınd a e n yen i video oyu n konsol u v e alt ı yen i oyun .

Harlan -şüph e uyandırabilece k ayrıntılar a girmeden - projesin i anlattık - tan sonr a Davi d yardı m etmey i kabu l etti . Harlan' a n e yapmas ı gerektiğin i açıkladı. Bi r mode m satı n alacak , ofis e gidecek , fazlada n bi r telefo n giriş i olan birini n bilgisayarın a modem i bağlayacaktı . Cihaz ı kimseni n göre - meyeceği bi r şekild e masanı n altın a saklayacaktı . Sonr a tehlikel i kısı m geliyordu. Harlan'ın , bilgisayarı n başın a oturup , bi r uzakta n erişi m yazılı m paketini indiri p çalıştırmas ı gerekiyordu . He r a n masanı n sahib i ger i gelebilir y a d a başk a bir i geçerke n Harlan' ı adamı n ofisind e görebilirdi . O kadar huzursuzd u k i çocuğu n onu n içi n yazdığ ı listede n yapmas ı gereken - leri güçlükl e okuyabiliyordu . Am a iş i bitird i v e farkedilmede n binada n çıktı .

Bombayı Yerleştirme k . .

David o gec e yemekte n sonr a on a uğradı , ikis i birlikt e Harlan'ı n bil - gisayarının başın a oturdula r v e oğla n birka ç dakik a içind e modem e bağlanıp erişi m sağlayara k Georg e Adamson'ı n makinasın a ulaştı . Ço k zor olmamıştı , çünk ü Georg e parolasın ı değiştirme k gib i emniye t önlemlerini hiçbi r zama n almazd ı ve sürekl i birilerinde n bi r dosyay ı indirmesini y a d a elektroni k postayl a göndermesin i isterdi . Zama n içinde ofistek i herke s adamı n parolasın ı öğrenmişti .

David bira z gezindikte n sonr a bilgisayard a BütçeSlaytları2002.pp t dosyasını buld u v e on u Harlan'ı n bilgisayarın a indirdi . Harla n sonr a çocuğa ev e gitmesin i v e birka ç saa t sonr a ger i gelmesin i söyledi .

David ger i geldiğinde , Harla n onda n Otoyo l Dairesi'ni n bilgisaya r sistemine bağlanmasın ı v e ayn ı dosyayı , eskisin i silerek , bulduklar ı yere koymasın ı istedi . Harla n David' e vide o oyu n konsolun u gösterd i v e her şe y yolund a giders e aleti n yarı n onu n olacağın a sö z verdi .

George'u Şaşırtma k

Bütçe görüşmeler i gib i kulağ a sıkıc ı gele n bi r şeyi n pe k kimseni n ilgisini çekeceğin i düşünmezsini z am a Bölg e Konseyi'ni n toplant ı odası , gazeteciler, öze l ilg i guruplarını n temsilcileri , halkta n insanla r v e hatt â ik i televizyon habe r ekibiyl e tıkabas a dolmuştu .

George b u görüşmelerd e he r zama n ço k şeyi n ris k altınd a olduğun u düşünmüştü. Keseni n ağzın ı açaca k ola n İlç e Konseyi'yd i v e Georg e ikna edic i bi r sunu m yapmazs a Otoyo l Bütçes i kısalacaktı . Sonr a d a herkes yollardak i çukurlardan , çalışmaya n trafi k lambalarında n v e tehlikeli dörtyo l ağızlarında n şikâyetç i olmay a başlayaca k v e on u suçlayacaktı. Ertes i yı l yaşa m dah a d a sefi l bi r ha l alacaktı . Kürsüy e çıkacak kiş i olara k tanıtıldığınd a kendin e güveniyordu . B u sunu m üzerinde alt ı haft a çalışmışt ı v e PovverPoin t slaytların ı karısına , diğe r yöneticilere v e baz ı yakı n arkadaşların a göstermişti . Herke s bunu n şimdiye kada r yaptığ ı e n iy i sunu m olduğund a hemfikirdi .

ilk ü ç slay t ço k iy i gitti . He r zamankinda n farkl ı olara k bütü n Konse y üyeleri dikkatlerin i on a vermi ş gibiydiler . Vurgulama k istediğ i noktalar ı etkili bi r şekild e belirtiyordu .

Ve sonr a birde n he r şe y ter s gitmey e başladı . Dördünc ü slaytt a geçen yı l açıla n yen i otoyolu n günbatımınd a çekilmi ş bi r fotoğrafını n olması gerekiyordu . Onu n yerin e başk a bi r şe y vardı , fazlasıyl a küçü k düşürücü bi r şey : Penthous e y a d a Hustle r tür ü bi r dergide n alınm a bi r resim. Dinleyicileri n hayre t dol u seslerin i duyd u v e bi r sonrak i slayt a geçmek içi n heme n dizüst ü bilgisayarını n düğmesin e bastı .

Bu dah a d a kötüydü . Haya l gücün e hiçbi r şe y bırakılmamıştı .

Tıklayarak bi r sonrak i slayt a geçmey e çalışıyord u k i dinleyicilerden biri projektörün fişin i çekt i v e b u sırad a toplant ı başkan ı tokmağın ı sertçe vurara k gürültünü n içind e toplantını n ertelendiğin i duyurdu .

Aldatmacanın İncelenmes i

Bu tepes i atmı ş çalışan , gen ç bi r bilgisaya r korsanını n bilgilerin i kul- lanarak, dair e yöneticisini n bilgisayarın a girmey i başarmış , öneml i bi r PovverPoint sunumun u indirmi ş v e baz ı slaytlar ı kesinlikl e küçü k düşürücü başk a resimlerl e değiştirmişti . Sonr a d a sunum u adamı n bil - gisayarına ger i koymuştu .

Modem bi r fiş e takıl ı ve ofi s bilgisayarlarında n birin e bağlıyke n genç korsa n telefo n hattın ı kullanara k dışarıda n bağlanabilmişti . Çocuk, uzakta n erişi m yazılımın ı öncede n kurmuştu , böylec e bilgisa - yara bağlandıkta n sonr a sistemd e dura n he r dosyay a ta m erişi m sağlayabilecekti. Bilgisayar , kuruluşu n ağm a bağl ı olduğ u v e çocu k müdürün kullanıc ı adın ı v e parolasın ı bildiğ i içi n kolaylıkl a müdürü n dosyalarına erişebilirdi .

Dergi resimlerin i tarayıcıda n geçirme k d e dahil , tü m i ş yalnızc a birkaç saa t sürmüştü . Sonu ç olara k iy i bi r adamı n şerefin e sürüle n lek e ise akı l alma z bi r büyüklüktedir .

içeriye Girme k 14 9

Mitnick Mesajı :

işten atılan, başka bir birime aktarılan ya da küçülme nedeniyle işine son ve- rilen çalışanların büyük bölümü hiç sorun yaratmazlar. Ancak bir şirketin felaketi önlemek için ne gibi önlemler alabileceğini anlaması için bir tane sorun çıkması yeter.

Deneyimlerin ve istatistiklerin açıkça gösterdiğine göre şirkete en büyük tehlike içerden gelmektedir. Değerli bilgilerin nerede durduğuyla ilgili ayrıntılı bilgiyi ve şirketi nereden vurmanın en büyük zararı vereceğini ancak içerdekiler bilebilirler.

Terfi İsteye n Bir i

Güzel bi r sonbaha r gün ü öğlede n önc e Pete r Milton , Honorabl e Ot o Yedek Parçalan'nı n Denver'dak i bölg e ofis i binasını n lobisin e girdi . B u şirket, arab a piyasas ı içi n ulusa l boyutt a bi r yede k parç a toptancısıdır . Peter danışmad a beklediğ i sırad a danışm a görevlis i gen ç hanı m on u ziyaretçi olara k kaydetti , araya n birin e arabayl a geli ş yolun u anlatt ı v e kargo şirketinde n gele n bi r adaml a ilgilendi . Bunları n heps i aşağ ı yukar ı aynı zamand a oldu .

Kadın on a yardımc ı olma k içi n zama n bulunca , "B u kada r ço k şey i bir arad a yapmay ı nası l öğrendiniz?" , diy e sord u Peter . Kadı n gülümse - di; görünüş e gör e bun u farketmesinde n memnu n olmuştu . On a Dalla s Bürosu pazarlamadan olduğun u v e Atlant a bölg e satışlar ı sorumlus u Mike Talbott'u n kendisiyl e görüşeceğin i söyledi . "Bugü n ziyare t ede- ceğimiz bi r müşterimi z var " dedi . "Burada , lobid e bekleyeceğim. "

"Pazarlama", ded i gen ç kadı n neredeys e arz u dol u bi r şekild e v e Peter on a gülümsedi . Ardında n n e geleceğin i duyma k istiyordu . "Üniver - siteye gitseydim , b u konud a eğiti m alırdım. " dedi . "Pazarlamad a çalış - mayı ço k isterdim. "

Peter yenide n gülümsedi . "Kaila" , dedi , masanı n üstündek i levhada n kadının adın ı okuyarak . "Dalla s büromuzd a eskide n sekrete r ola n bi r hanım vardı . Kendin i ü ç yı l önc e pazarlamay a aldırdı . Şimd i pazarlam a müdür yardımcıs ı v e eskide n kazandığını n ik i katın ı kazanıyor. "

Kaila ışıltıl ı gözlerl e baktı . Ada m deva m etti , "Bilgisaya r kullanabili r misin?"

"Elbette", ded i kadın .

"Pazarlamada bi r sekreterli k iş i içi n yukardakiler e sen i önermem e ne dersin? "

Birden yüz ü aydınlandı . "Bunu n içi n Dallas' a bil e giderim. "

"Dallas'a bayılacaksın. " ded i adam . "Ş u and a bi r açı k olu p olmadığı - na dai r birşe y söyleyeme m am a elimde n gelen i yapacağım. " |

Kaila, takı m elbiseli , kravatlı , düzgü n kesiml i v e iy i taral ı saçlar ı ola n bu cic i adamı n i ş yaşamınd a büyü k bi r değişikli k yaratabileceğin i düşündü. 1

Peter lobid e oturdu , dizüst ü bilgisayarın ı açt ı v e i ş yapmay a başladı . On-on be ş dakik a sonr a yenide n masay a geldi . "Görünüş e gör e Mike'i n işi uzadı . Beklerke n e-postalarım a bakabileceği m bi r konferan s salon u var mı? " ı

• • - • - i

Kaila konferan s salonlarını n kullanı m saatlerin i ayarlaya n adam ı aradı v e Peter'i n ayırtılmamı ş bi r tanesin i kullanabilmes i içi n gerekl i ayarlamaları yaptı . Siliko n Vadis i şirketlerinde n gele n bi r geleneğ i sürdürerek (Appl e herhald e b u uygulamay ı il k başlatandır) , baz ı konfe - rans salonların a çizg i fil m kahramanlarının , lokant a zincirlerinin , fil m yıldızlarının y a d a çizg i roma n kahramanlarını n isimler i verilmişti . Far e Minnie salonun u bulmas ı söylendi . Kadı n giri ş işlemlerin i yapt ı v e Far e Minnie salonun a nası l gideceğin i anlattı .

Peter oday ı buldu , içer i yerleşt i v e bilgisayarın ı etheme t girişin i kul- lanarak ağ a bağladı .

Neler olu p bittiğin i anlayabildini z mi ?

Doğru; saldırga n şirketi n güvenli k duvarını n arkasın a geçere k şirke t ağına bağlanmıştı .

Anîhony'nin Öyküs ü '* "

Sanırım Anthon y Lake'i n tembe l bi r işadam ı olduğ u söylenebilirdi . Ya d a belk i "düzenbaz " deme k dah a yerind e olabilir . j

Başka insanla r içi n çalışma k yerin e kend i işin i kurma k istemişti ; ha - yali sabi t bi r yerd e duracağ ı v e tü m ülked e koşturu p durmasın ı gerek - tirmeyecek bi r dükkâ n açmaktı . Anca k par a getireceğinde n emi n olduğ u

bir i ş yapma k istiyordu . d

Ne tü r bi r dükkâ n olabilird i acaba ? Bulmas ı uzu n sürmedi . Arab a tamiratından anlıyordu , böylec e arab a yede k parçalar ı dükkânınd a karar kıldı . 1

Başarılı olmay ı nası l garantiy e alabilirdi ? Yanı t aklın a şimşe k gib i geldi: Honorabl e Ot o Yede k Parç a Toptancısı'n ı tü m malların ı kendisin e maliyetine satmay a ikn a etmek . - i

Doğal olara k böyl e bi r şey i isteyere k yapmazlardı . Anca k Anthon y insanları nası l kandıracağını , arkadaş ı Micke y is e başkalarını n bilgisa - yarlarına nası l gireceğin i biliyordu . İkis i birlikt e zekic e bi r pla n yaptılar .

içeriye Girme k 15 1

Mitnick Mesajı :

Çalışanlarınızı, bir kitabı yalnızca kapağına bakarak değerlendirmemeleri konusunda eğitin. Bir kişiye, yalnızca iyi giyimli olduğu ve saçı başı yapılı olduğu için inanılmamak.

O sonbaha r gün ü kendin i inandırıc ı bi r şekild e Pete r Milto n adınd a bir çalışa n olara k tanıtt ı v e çalışanlar ı dalaverey e getiri p Honorabl e Ot o Yedek Parç a binasın a girerek , dizüst ü bilgisayarın ı ağ a bağladı . Şimdiye kada r he r şe y yolund a gitmişti . Bunda n sonr a yapmas ı gerekenler kola y olmayacaktı , özellikl e d e Anthon y kendin e o n be ş dakikalık bi r limi t belirlemişken . Dah a uzu n sürers e farkedilm e tehlikesinin gidere k artacağın ı düşünüyordu .

Bilgisayar aldıklar ı şirket e bağl ı bi r deste k personel i gib i davranara k daha önc e yaptığ ı bi r telefo n görüşmesind e onlar a uzu n bi r teran e oku - muştu. "Şirketinizi n biziml e ik i yıllı k bi r deste k kontrat ı var , b u yüzde n sizi ver i tabanımız a ekliyoru z böylec e kullandığını z bi r yazılı m içi n bi r yama y a d a yen i bi r yükseltilmi ş sürü m çıktığınd a haberini z olacak . Hangi uygulamalar ı kullandığınız ı öğrenebili r miyim? " Gele n yanı t bi r program listes i şeklindeyd i v e muhasebec i bi r arkada ş MA S 9 0 adl ı programın aradıklar ı -perakend e dükkânları n listes i v e he r birin e verile n indirimler v e ödem e koşulların ı içeren - progra m olduğun u söyledi .

Bu kili t bilgide n yararlanarak , ağdak i tü m geçerl i terminaller i tanım - layan bi r yazılı m kulland ı v e muhaseb e bölümünü n kullandığ ı doğr u sunucuyu bulmas ı ço k zamanın ı almadı . Dizüst ü bilgisayarın a yükl ü korsanlık araçlar ı takımında n bi r progra m çalıştırd ı v e on u hede f sunucuda buluna n yetkil i kullanıcılar ı belirleme k içi n kullandı . Başk a bi r programla, "boşluk " v e "parola " gib i sı k kullanıla n parolalar ı denemey e başladı. "Parola " iş e yaradı . Şaşılaca k bi r duru m değildi . İ ş parol a seçmeye gelinc e insanla r tü m yaratıcılıkların ı kaybediyorlardı .

Yalnızca alt ı dakik a geçmişt i v e oyunu n yarıs ı bitmiş , içer i girmişti .

Bir ü ç dakikay ı d a yen i şirke t adını , adresini , telefo n numarasın ı v e bağlantı numarasın ı dikkatl e müşter i listesin e eklemekl e geçirdi . V e sır a en kritik , he r şeyi n teme l amac ı ola n değişikliğ e geldi . Bu , tü m Honorable Ot o Yede k Parçaları'nı n on a % 1 kazançl a satılacağın ı belirleyen değişiklikti .

Yaklaşık o n dakik a içind e iş i bitmişti . Kaila'y a teşekkü r edi p e-posta - larını okum a işin i bitirdiğin i söyleyece k kada r oyalandı . Ayrıc a Mik e Talbot'un kendisin e ulaştığını , pland a bi r değişikli k olduğun u v e müş - terinin ofisind e buluşacakların ı söyledi . Kaila'y a on u pazarlamadak i o i ş için önereceğin i söylemey i d e ihma l etmed i ekledi .

Kendini Pete r Milto n olara k adlandıra n saldırga n ik i psikoloji k tahri p tekniği kullanmıştı ; bir i planlıyd ı diğer i d e o and a uydurulmuştu .

İyi par a kazana n bi r yönetic i gib i giyinmişti . Kravat , ceket , düzgü n kesimli saçlar ; bunla r küçü k ayrıntıla r gib i görünebilirle r am a kesinlikl e bir etk i bırakırlardı . Bun u be n istemede n keşfetmiştim . GT E Kaliforniy a ofisinde -artı k va r olmaya n büyü k bi r telefo n şirketinde - çalıştığı m kıs a süre içerisind e kartı m olmada n raha t am a düzgü n giyiml i -örneğin , spo r bir gömlek , pilisi z pantolo n v e Docker s ayakkabılarla - bi r şekild e iş e gelirsem durdurulu p sorguy a çekilirdim . Kartı n nerede , kimsin , nered e çalışıyorsun? Başk a bi r gü n ise , yin e kartsı z am a takı m elbis e v e krava t takıp i ş adam ı gib i giderdim . Eskide n kalma , heme n arkasında n geçm e yönteminin bi r türün ü kullanıp , binanı n için e y a d a güvenlikl i bi r giriş e doğru yürüye n insa n kalabalığını n arasın a karışırdım . An a giriş e yak - laşırlarken baz ı insanlar a takılı p onlarda n biriymi ş gib i sohbe t ed e ed e yürürdüm. Kapıda n geçerdi m v e güvenli k görevliler i kartımı n olmadığın ı anlasalar bil e yönetic i gib i gözüktüğü m v e kartlar ı ola n insanlarl a birlik - te yürüdüğü m içi n ban a birşe y demezlerdi .

Bu deneyimi m sayesind e güvenli k görevlilerini n davranışlarını n n e kadar tahmi n edilebili r olduğun u öğrendim . Onla r d a hepimi z gib i görünüşe bakı p kara r veriyorlardı . B u d a toplu m mühendislerinin kullan - mayı öğrendikler i cidd i bi r zayıflıktı .

Saldırganın ikinc i psikoloji k silah ı danışmad a görevl i kızı n gösterdi ğ olağanüstü çabay ı görmesiyl e devrey e girdi . Pe k ço k iş i ayn ı and a yaparak, telaş a kapılmadan , herkes e tü m dikkatin i verdiğ i hissin i yaratı - yordu. Peter , kızın , kendin i kanıtlamay a çalışan , yükselme k isteye n bir i olduğu kanısın a vardı . Pazarlam a bölümünd e çalıştığın ı söyleyinc e kızı n tepkisine bakı p onunla bi r yakınlı k kuru p kuramayacağın a dai r ipuçla r aradı. Saldırga n içi n bu , dah a iy i bi r iş e kaydırılmas ı içi n yardı m etmey e çalışacağına sö z verere k etkileyebileceğ i insanla r listesin e birini n dah a eklenmesi anlamın a geliyordu . (Eğe r Muhaseb e bölümün e gitme k iste - diğini söylemi ş olsaydı , doğa l olara k Pete r d a orad a bi r i ş bulmasınd a yardımcı olabilece k bağlantılarını n olduğun u söyleyecekti.)

Saldırganlar b u öyküd e kullanıla n başk a bi r psikoloji k silah ı dah s kullanmayı ço k severler : İk i kademel i bi r saldırıyl a güve n yaratma k Önce pazarlamadak i işl e ilgil i bira z sohbe t ett i v e sonr a d a gerçe k birinin "ismin i bırakma " -başk a bi r çalışanı n adın ı verme - tekniğin i k u - landı. Sıras ı gelmişken , kend i kullandığı a d d a gerçe k bi r çalışan a aitt :

Açılış sohbetinde n sonr a konferan s salonun a geçmey i heme r isteyebilirdi. Am a onu n yerin e bira z oturu p çalışırmı ş gib i yaptı ; güy a bı - arkadaşını bekliyordu . Olas ı şüpheler i bastırmanı n başk a bi r yol u d a buydu, çünk ü saldırganla r ortalıkt a fazl a dolaşmazlardı . Yin e d e ortalık -

içeriye Girme k 15 3

Mitnick Mesajı :X

Yabancı birinin şirket ağma dizüstü bilgisayarını bağlayabileceği bir yere girmesine izin vermek güvenlik sorunları oluşma tehlikesini artırır. Br çalışanın, özellikle de şehir dışından gelmiş birinin, konferans salonundan e-postalanna bakması son derece makuldür. Ama ziyaretçi güvenilir bir çalışan değilse ya da ağ, yetkisiz bağlantıları engelleyecek şekilde yapılandırılmamışsa, bu durum şirket dosyalarının tehlikeye girmesine olanak tanıyan zayıf halka olabilir.

ta fazl a dolaşmadı ; toplu m mühendisleri su ç mahalind e gereğinde n uzun kalmanı n doğr u birşe y olmadığın ı bilirler . ;

Şunu d a ekleme k gereki r ki : B u yazını n hazırlandığ ı dönemdek i yasalara gör e Anthon y lobiy e girere k bi r su ç işlememiştir . Gerçe k bi r çalışanın adın ı kullandığı zama n d a su ç işlememiştir . Ayrıc a konferan s salonunu kendis i içi n açmaların ı sağlamasınd a d a bi r su ç unsur u bulun - mamaktadır. Şirke t ağın a bağlandığınd a v e hede f bilgisayar ı aradığınd a da henü z bi r su ç işlememiştir .

Bilgisayar sistemin i kıran a kada r herhang i bi r su ç işlememiştir .

Kevin'î Mera k Edenle r

Yıllar önc e küçü k bi r işt e çalışırken , bilg i işle m bölümün ü oluştura n diğer ü ç bilgisayarcıyl a birlikt e oturduğu m ofis e n e zama n girsem , adamlardan bir i (burad a on a Jo e diyeceğim) bilgisayarındak i görüntüy ü hızla değiştiriyordu . Bunu n şüphel i bi r duru m olduğun u heme n anladım . Aynı gü n içerisind e b u ola y ik i ker e dah a tekrarlanınca , bilme m gereke n bir şeyle r olduğunda n emi n olmuştum . B u ada m beni m görmem i istemediği nası l bi r i ş yapıyo r olabilirdi ?

Joe'nun bilgisayar ı şirketi n minibilgisayarların a erişim i ola n bi r uçbiri m gibi çalışıyordu , böylec e nele r yaptığın ı izleyebileceği m bi r taki p program ı yükledim. Progra m omuzunu n üstünde n baka n bi r televizyo n kameras ı gibi çalışıyor , bilgisayarınd a n e görüyors a aynısın ı ban a d a gösteriyordu .

Benim masa m Joe'nu n masasını n yanındaydı ; görmesin i zorlaştır - mak içi n kend i monitörüm ü mümkü n olduğunc a döndürdü m am a he r a n bakabilir v e onu n yaptıkların ı izlediğim i anlayabilirdi . Anca k b u soru n olmayacaktı, çünk ü yaptığ ı iş e kendin i fazlasıyl a kaptırmıştı .

Gördüğüm şe y karşısınd a ço k şaşırdım . Alça k herifi n beni m bordr o bilgilerimi karıştırdığın ı görünc e ağzı m açı k kaldı . Ada m beni m maaşı - ma bakıyordu !

O sırad a orad a ü ç aylıktı m v e Joe'nu n onda n dah a fazl a maa c aldığım fikrin e dayanamadığın ı düşündüm .

Birkaç dakik a sonra , programlam a bilgis i olmaya n deneyimsi z bil - gisayar korsanlarını n kullandığ ı türde n araçla r indirdiğin i gördüm . Demek Jo e dünyada n habersizd i v e Amerika'nı n e n deneyiml i bilgisaya r korsanlarından birini n yanınd a oturduğ u konusund a e n küçü k bi r fikr i yoktu. B u ço k gülün ç bi r durumdu .

Maaşımla ilgil i bilgiler i çokta n almıştı , b u yüzde n on u durdurma k içi n çok geçti . Ayrıc a verg i dairesind e y a d a Sosya l Güvenli k Dairesi'nd e çalışan v e bilgisaya r erişim i ola n herhang i bir i d e maaşınız a bakabilirdi . Ne işle r karıştırdığın ı bildiğim i söyleyere k elimdek i koz u kaybetme k istemiyordum. O zamanla r e n büyü k amacı m fazl a s u yüzün e çıkma - maktı, iy i bi r toplu m mühendisi , becerilerini n v e bilgisini n reklamın ı yap - maz. İnsanları n he r zama n siz i hafif e almaların ı istersiniz , tehlik e olara k görmelerini değil . :

Böylece olayı n üstünd e durmadı m v e Jo e beniml e ilgil i bi r sı r bildiği - ni sanırke n be n kend i kendim e güldüm , halbuk i he r şe y ta m tersiydi . Onun nele r karıştırdığın ı bilere k kozlar ı be n elimd e tutuyordum .

Zamanla, B i grubund a çalıştığımı z ü ç mesa i arkadaşımı n hepsini n de -ekiptek i te k kı z içi n d e geçerl i olma k üzere - gördükler i ş u y a d a b u şirin sekreteri n y a d a yakışıkl ı bi r oğlanı n ev e götürdükler i maaşların a bakıp eğlendiklerin i keşfettim . Mera k ettikler i herkesi n maaşın a v e prim - lerine bakıyorlardı . Bunları n arasınd a üs t düze y yöneticile r d e vardı .

Aldatmacanın İncelenmes i

Bu öyk ü ilgin ç bi r sorun u yansıtmaktadır . Bordr o dosyalar ı şirketi n bilgisayar sistemini n yönetiminde n soruml u kişile r tarafında n erişilebile - cek bi r konumdadırlar . İ ş yin e bi r persone l sorun u durumun a gelir : kimi n güvenilir olduğun a kara r vermek . Baz ı durumlard a B İ çalışanlar ı sağ a sola gö z atma k fikrin i çekic i bulurlar . Bun u yapaca k olanaklar ı d a vardı r çünkü b u dosyalara erişim i kısıtlaya n kontroller i aşma k içi n öze l haklar a sahiptirler.

Alınacak bi r önlem , bordr o dosyala n gib i özellikl e hassa s dosyalara erişimi denetleme k olabilir . Gerekl i haklar a sahi p herhang i bir i denetim i kaldırabilir y a d a taki p edilmelerin i sağlayaca k yerler i temizleyebilir , ancak atılaca k he r adı m ahlâksı z bi r çalışanı n izlerin i saklayabilmes i için dah a fazl a çab a harcamasın ı gerektirecektir .

Aldatmacanın Engellenmes i

Toplum mühendisleri , çöpler i karıştırmakta n tutu n d a bi r güvenli k görevlisini y a d a danışm a memurun u kandırmay a kada r çeşitl i yöntem - lerle şirke t alanınız a girebilirler . Am a bunlar a karş ı d a alabileceğini z önlemler olduğun u duyma k hoşunuz a gidecektir .

içeriye Girme k 15 5

Mesai Saatler i Dışınd a Güvenli k

işyerine kartlar ı olmada n gele n tü m çalışanların , lobid e y a d a güven - lik ofisinde , o gü n içi n geçic i bi r kar t verme k amacıyl a durdurulmalar ı gerekir. Persone l kart ı yanınd a olmaya n biriyl e karşılaştıklarınd a şirke t güvenlik görevlilerini n izleyecekler i belirl i adımla r olsaydı , b u bölümd e anlatılan il k ola y ço k dah a farkl ı bi r şekild e sonuçlanabilirdi .

Güvenliğin önceli k taşımadığ ı şirketlerd e y a d a şirke t iç i alanlard a herkesin kartın ı görünü r bi r yerd e taşımasınd a ısra r etme k öneml i olmayabilir. Am a hassa s bölgeler e sahi p alanlard a b u kural , kat ı bi r şe - kilde uygulanan , standar t bi r kura l olmalıdır . Çalışanla r kar t göster - meyen kişiler i durdurma k konusund a eğitilmel i v e teşvi k edilmelidirler . Üst düze y çalışanlar a d a kendisin i durdura n kişiy i küçü k düşürmede n bu tar z kontroller i kabullenmeler i öğretilmelidir .

Şirket kuralları , sürekl i kartın ı takmay ı unuta n kişiler e verilece k cezalar konusund a çalışanlar ı uyarmalıdır . Cezaları n arasınd a çalışanı n bir günlüğün e ücretsi z uzaklaştırılmas ı y a d a sicilin e geçece k bi r uyarının verilmes i olabilir . Baz ı şirketle r gidere k arta n ser t cezalar ı yürürlüğe koymuşlardır . B u cezalar , kişini n müdürün e durumu n iletilemesi, sonr a d a resm î bi r ihta r şeklind e olabilir .

Ek olarak , korunmas ı gereke n hassa s bilgileri n olduğ u yerlerde , mesai saatler i dışınd a iş e gelece k kişiler e izi n verilebilmes i içi n gerekl i süreçler oturtulmalıdır . Bi r çözüm , b u ziyaretleri n şirke t güvenliğ i y a d a bu iş e baka n biri m aracılığıyl a yapılmas ı olabilir . B u biri m mesa i dış ı çalışma talebiyl e araya n herhang i bi r çalışanı n kimliğin i kişini n müdürünü arayara k y a d a başk a maku l bi r güvenli k yöntem i izleyere k düzenli olara k kontro l edebilir .

Çöplere Saygıl ı Olma k

Çöp dalış ı öyküsü , şirke t atıklarınızı n olas ı kötüy e kullanı m yol - larının üstünd e durdu . İşt e çöple r konusund a akıll ı olmanı n seki z anahtarı:

• Tü m hassa s bilgiler i hassaslı k derecesin e gör e sınıflandırın .

• Hassa s bilgileri n atılmasın a yöneli k olara k şirke t çapınd a i ş

süreçleri oluşturun .

• Atılaca k tü m hassa s bilgileri n önc e kâğı t öğütücüde n geçirilmes i

konusunda ısrarl ı davranı n v e öğütücüde n geçmeyece k kada r

küçük olu p öneml i bilgile r içere n kağı t parçalarında n kurtulma k

üzere güvenl i bi r yönte m belirleyin . Kâğı t öğütücüler , kararl ı bi r

saldırganın bira z sabırl a bi r aray a getirebileceğ i kâğı t şeritle. ;

çıkaran ucu z makinelerde n olmamalıdırlar . Onla r yerin e çapra z öğütücü dene n türle r y a d a çıktıy ı iş e yarama z bi r küspey e dönüştüren makinele r kullanılmalıdır .

• Atılmada n önc e ver i kayı t ortamların ı -disketler , sıkıştırılmı ş diskler, dosy a saklama k içi n kullanıla n CD'le r v e DVD'ler , bant - lar, esk i sabi t sürücüle r v e diğerlerini - tamame n silece k y a d a kullanılmaz hal e getirece k bi r yönte m oluşturulmasın ı sağlayın .

Dosyaları silmeni n onlar ı gerçe k anlamd a ortada n kaldır - madığını, siline n dosyaları n yenide n kurtarılabildiklerin i unut - mayın. Enro n yöneticiler i v e pe k ço k başkalar ı bun u ac ı bi r şe - kilde öğrendiler . Kaydedilebili r ortamlar ı yalnızc a çöp e atma k mahallenizin arkada ş canlıs ı çö p dalıcısın a davetiy e çıkarmaktır .

(Kaydedilebilir ortamları n v e araçları n atılmasın a yöneli k belirl i kurallar içi n 16 . bölüm e bakınız.)

• Temizli k ekiplerinizi n seçimind e uygu n ölçüd e bi r kontro l sağlayın, gerekirs e sicillerin e bakırı .

• Çalışanlarınızı , çöp e attıklar ı şeyi n içeriğin e dikka t etmeler i konusunda düzenl i olara k uyarın .

• Büyü k çö p bidonların ı kilitleyin .

• Hassa s malzemele r içi n farkl ı atı k variller i kullanı n v e b u tar z işlerde uzmanlaşmı ş bi r şirketl e anlaşara k malzemeleri n imhasını sağlayın .

Çalışanlara Gül e Gül e Derke n

Hassas bilgilere , parolalara , dışarıda n erişi m numaraların a v e ben - zer şeyler e erişim i ola n bi r çalışa n işte n ayrılırke n uyulmas ı gereke n kat ı kurallar olmas ı gerektiğ i b u sayfalard a dah a önc e vurgulanmıştı . Güvenlik süreçlerini z kimleri n hang i sistemlerd e yetkil i olduğun u taki p edecek yolla r içermelidir . Kararl ı bi r toplu m mühendisini n güvenli k bari - yerlerinizden geçmesin i engelleme k zo r bi r işti r am a esk i çalışanlarını z için d e bunu n kola y olmamas ı gerekir .

Kolaylıkla gö z ard ı edilebile n başk a bi r ayrınt ı is e arşivde n yedeklem e bantlarını almay a yetkil i bi r çalışa n işte n ayrıldığınd a görülür . Kâğıd a dökülmüş bi r kuralla r bütünü , kişini n adını n yetk i listesinde n silinmes i içi n hemen arşivlem e şirketini n aranmas ı gerektiğin i vurgulamalıd'ır .

Kitabın o n altınc ı bölümünd e b u öneml i konuyl a ilgil i ayrıntıl ı bilg i ve - rilmektedir, anca k b u öyküd e d e görüldüğ ü üzere , yerleştirilmes i gereke n bazı kili t güvenli k önlemlerin i burad a belirtme k yerind e olacaktır :

• Bi r çalışa n ayrıldığınd a atılaca k adımları n ta m v e ayrıntıl ı bi r

kontrol listes i tutulmaiidı r v e hassa s bilgiler e erişim i ola n çalışan -

lar içi n öze l maddele r bulunmalıdır .

• Çalışanı n bilgisaya r erişimini n zama n kaybetmede n -hatt â kiş i

daha binay ı ter k etmede n önce - kapatılmasın a yöneli k bi r kura l

belirlenmelidir.

• Kişini n tanıtı m kartını n v e eğe r varsa , anahtarları n v e elektroni k erişim cihazlarını n ger i alınmasıyl a ilgil i bi r süre ç oluşturulmalıdır .

• Güvenli k görevlilerini n giri ş kart ı olmaya n çalışanlar ı içer i almadan önc e resiml i bi r kimli k kart ı görmeler i v e kişini n şirkett e çalışıp çalışmadığını n bi r listede n kontro l edilmes i kuralların ı getiren maddele r olmalıdır .

Bazı adımla r kim i şirketle r içi n aşır ı y a d a dah a pahal ı olabilirke n başkaları içi n uygu n olabilir . B u tar z kat ı güvenli k önlemler i arasınd a aşağıdakiler bulunabilir :

« Elektroni k kimli k kartlarıyl a çalışa n manyeti k giri ş kapılar ı bulun - malıdır. Kişini n şirke t personel i olduğunu n v e binay a girmey e yetkili olu p olmadığını n elektroni k olara k anınd a belirlenebilmes i için he r çalışan , kartın ı tarayıcıda n geçirir . (Ş u d a unutulma - malıdır ki , he r şey e karşı n güvenli k görevliler i heme n arkasında n geçmelere -yetkisi z birini n gerçe k bi r çalışanı n heme n arkasın - dan içeriy e sızmasına - karş ı uyanı k olaca k şekild e eğitilmelidir.)

e Ayrıla n kişiyl e (özellikl e b u kiş i işte n atılmışsa) ayn ı i ş ekibind e çalışan herkes e parolaların ı değiştirm e zorunluluğ u getirilmelidir .

(Bu ço k abartıl ı gib i m i görünüyor ? Genera l Telephon e şir - ketindeki kıs a sürel i hizmetimde n uzu n yılla r sonra , Pacifi c Bel l güvenlik sorumlularını n Genera l Telephone'u n ben i iş e aldığın ı öğrendiklerinde "gülmekte n kırıldıklarını " duydum . B u Genera l Telephone'un yararın a oldu , çünk ü ben i işte n çıkardıkta n sonr a ünlü bi r bilgisaya r korsanı n onlarl a çalışmı ş olduğun u öğrendik - lerinde, şirkettek i herkesi n parolaların ı değiştirmesin i zorunl u

kılmışlar!)

Binalarınızın hapishan e gib i olmasın ı istemezsini z am a ayn ı zaman - da dü n işte n atılı p bugü n zara r vermey e niyetl i olara k ger i gelen birin e karşı d a korunmanı z gerekir . ,

Kimseyi Unutmayı n ' • • • -

Güvenlik politikalar ı iş e yen i girmi ş çalışanlar ı v e hassa s bilgiyl e haşır neşi r olmayan , danışm a görevlis i gib i kişiler i gö z ard ı etm e eğili - mindedirler. Dah a önc e gördüğümü z gibi , danışm a görevliler i saldırgan - lar içi n elverişli hedeflerdi r v e arab a yedek parçala n şirketin e giriş i anla - tan öyk ü d e b u konud a örne k oluşturuyor . Şirketi n farkl ı bi r tesisind e çalıştığını söyleye n v e bi r profesyone l gib i giyinmi ş arkada ş canlıs ı bi r kişi göründüğ ü gib i olmayabilir . Danışm a görevliler i yer i geldiğind e şir - ket kimliğin i nazikç e soraca k şekild e eğitilmi ş olmalıdırla r ve bu eğiti m yalnızca an a girişt e dura n danışm a görevlisin e değil , öğl e saatlerind e ya d a kahv e molalarınd a onları n yerin e baka n kişiler e d e verilmelidir .

Şirket dışında n gele n ziyaretçile r içi n güvenli k kurallar ı resiml i bi r

kimlik gösterilmesin i v e bilgini n kaydedilmesin i zorunl u tutmalıdır . Saht e kimlik üretme k zo r değildir , anca k kimliği n gösterilmes i olas ı saldırgan - lar içi n bahan e üretm e işin i bi r derec e zorlaştırmaktadır .

Bazı şirketlerd e ziyaretçileri n lobide n alını p toplantıda n toplantıy a giderken kendilerin e eşli k edilmes i zorunluluğ u getire n bi r kura l uygula - mak mantıkl ı olabilir . Eşli k ede n görevlini n ziyaretçiy i il k toplantısın a götürdüğünde b u kişini n binay a çalışa n olara k m ı yoks a dışarda n bi r ziyaretçi olara k m ı girdiğin i açıkç a belirtm e koşul u olmalıdır . Nede n b u önemlidir? Çünkü , dah a öncek i hikâyelerd e d e gördüğümü z gibi , bi r saldırgan sı k sı k il k karşılaştığ ı kişiy e kendin i belirl i bi r kiş i olara k tanıtırken ikinc i karşılaştığın a tamame n farkl ı bir i olara k tanıtmaktadır . Bir saldırganı n lobid e kendin i göstermesi , danışm a görevlisin i bi r mühendisle randevus u olduğun a inandırması.. . sonr a mühendisi n odasına kada r götürülmes i ve orad a kendin i şirket e bi r ürü n satma k isteyen bi r satı ş temsilcis i olara k tanıtması.. . v e e n sonund a d a mühendisle görüşmes i bittiğind e binad a serbestç e gezinm e firsat ı bul - ması so n derec e kolaydır .

Başka bi r ofiste n gele n bi r çalışan ı içer i almada n önc e kişini n gerçekten bi r çalışa n olu p olmadığını n tespit i içi n uygu n süreçle r bulun - malıdır. Danışm a v e güvenli k görevlileri , saldırganları n şirke t binaların a girebilmek içi n kullandıkları , bi r çalışanı n kimliğin e bürünm e yöntem - lerinin bilincind e olmalıdırlar .

Binanın için e girmey i başara n v e dizüst ü bilgisayarın ı şirke t güven - lik duvarını n arkasında n ağ a bağlaya n bi r saldırgan a karş ı korunma k için n e yapılabilir ? Bugünü n teknolojiler i gö z önün e alındığınd a b u gü ç bir iştir . Konferan s salonları , eğiti m odalar ı v e benzer i yerlerd e kili t altı - na alınmamı ş a ğ girişler i bulunmamalıdır ; y a d a e n azından , b u girişle r güvenlik duvarlar ı y a d a routerlarl a korum a altın a alınmı ş olmalıdırlar . Ama e n iy i koruma , ağ a bağlana n herkesi n kendin i tanıtmas ı içi n güven - li bi r yo l oluşturmaktı r

Bilgiyi Sağlam a Âlın !

Küçük bi r uyarı : Şirketinizi n he r B İ çalışan ı n e kada r maa ş aldığınızı , genel müdürü n n e kada r par a aldığın ı v e kaya k tatilin e giderke n kimi n şirket jetin i kullandığın ı büyü k olasılıkl a biliyordu r y a d a ço k geçmede n öğrenecektir.

Bazı şirketlerd e B İ y a d a muhaseb e çalışanlarını n kend i maaşların ı yükseltmeleri, saht e bi r satıcıy a ödem e yapmaları , insa n kaynaklar ı kayıtlarından olumsu z siciller i silmeler i v e bunu n gib i şeyle r yapmalar ı bile mümkündür . Baze n yalnızc a yakalanm a korkus u onlar ı dürüs t olmaya iter.. . sonund a bi r gü n geli r v e adamı n açgözlülüğ ü y a d a ahlâk - sız ruh u tehlikey i bi r kenar a iterek , götürebildiğ i kada r par a götürmesin e neden olur .

içeriye Girme k 15 9

Elbette bun a karş ı d a çözümle r vardır . Hassa s dosyalara , uygu n erişim kontroller i yerleştirilere k yalnızc a yetkil i kişileri n onlar ı açmas ı sağlanabilir. Baz ı işleti m sistemler i bell i olayları , örneği n başarıl ı olsu n olmasın korumal ı bi r dosyay a ulaşmay a çalışa n herkesi , kaydedece k şekilde ayarlanabile n deneti m kontroller i içerir .

Eğer şirketini z konunu n bilincindeys e v e hassa s dosyalar ı koruya n uygun deneti m mekanizmalar ı v e erişi m sınırlamalar ı yerleştirmişse , doğru yönd e güçl ü adımla r atıyorsunu z demektir .

'1

TEKNOLOJİYİ V E TOPLU M

MÜHENDİSLİĞİNİ BİRLEŞTİRME K

Bir toplu m mühendisi , amacın a ulaşmasın a yardımc ı olmas ı içi n insanları birşeyle r yapmay a yönlendirebilirl e yeteneğiyl e yaşar ; anca k başarılı olabilme k için , çoğ u zama n hatır ı sayılı r bi r bilg i birikimin e sahi p olmasının yanısır a bilgisaya r v e telefo n sistemleriyl e haşı r neşi r olmas ı da gerekir .

İşte siz e teknolojini n öneml i bi r ro l oynadığ ı özgü n toplu m mühendis - liği dolaplarında n bi r örnek .

Parmaklıkların arasında n korsanlı k

Fiziksel, iletişimse l y a d a elektroni k olara k zorl a içer i girmeler e karş ı korunan e n güvenl i yerle r arasınd a sizc e nerele r vardır ? For t Knox * mu? Doğru . Beya z Sara y mı ? Kesinlikle . Bi r dağı n altın a gömül ü Kuze y Amerika Hav a Savunm a Üssü , NORA D mı ? Şüphesiz .

Ya hapishanele r v e tutukevlerin e n e dersiniz ? Ülkedek i herhang i bi r yerden dah a korunakl ı olmalılar , öyl e değ i l mi ? İnsanla r ende r olara k kaçarlar, kaçtıklarınd a d a genellikl e kıs a süred e yakalanırlar . Federa l bi r tesisin toplu m mühendisliğ i saldırıların a karş ı dayanıkl ı olacağın ı düşünürsünüz. Anca k yanılırsınız , hiçbi r yerd e kusursu z güvenli k diy e birşey yoktur .

Birkaç yı l önc e bi r çif t düzenba z (aslınd a profesyone l dolandırıcılar) bir sorunl a karşılaştılar . E n so n kaldırdıklar ı yükl ü paranı n bi r bölg e yargıcına ai t olduğ u ortay a çıktı . İkilini n geçe n yıllard a zama n zama n yasayla başlar ı derd e girmişt i am a b u ke z federal yetkilile r duruml a daha ço k ilgilendiler . Düzenbazlarda n birini , Charle s Gondorf f u enselediler v e on u Sa n Dieg o yakınlarındak i bi r tutukevin e attılar . Federal sul h hakimi , kaçm a olasılığ ı olduğ u v e toplum a zararl ı olduğ u gerekçesiyle Gondorf f u n gö z altın a alınmasın a kara r verdi .

Arkadaşı Johnn y Hooker , Charlie'ni n bi r savunm a avukatın a ihtiyac ı olacağını biliyordu . Am a paray ı nerede n bulacaktı ? Pe k ço k dolandırıc ı gibi o d a paralar ı güzel giysilere , haval ı kameralar a v e kadınlar a yatır - mış, böylec e para , geldiğ i kada r hızl a suyun u çekmişti . Johnny'nin , üzerinde, yaşamasın a yetece k kada r par a nadire n bulunurdu .

iyi bi r avuka t tutaca k kada r paray ı başk a bi r dola p çevirere k bulmas ı gerekiyordu. Johnn y bun u te k başına başaramazdı . Oynadıklar ı oyun - ların arkasındak i ada m he p Charli e Gondorf f olmuştu . Am a Johnny ,

Terimler

Federaller işi n içind e ik i kişini n olduğun u
bilirken v e diğerin i d e yakalama k içi n b u
kadar heveslilerke n n e yapacağın ı sor -

DOĞR UDAN BAĞLANTI

HİZMETİ: Ahize
mak içi n tutukevin e gitmey e cesare t
kaldırıldığında doğrudan
edemezdi. Yalnızc a ailesini n ziyare t
etmesine izi n veriliyordu , b u d a saht e
sabit bir numaraya
kimlik belges i gösteri p aileni n bi r ferd i
bağlanan telefonlar için
olduğunu ön e sürmes i gerekece k
telefon şirketlerinde
demekti. Federa l bi r hapishaned e saht e
kullanılan bir terim.

kimlik kullanmay a çalışma k pe k iy i bi r

REDDET-KES: Belirli bir fikir gib i gelmedi .

telefon numarasında gelen
aramaların engellenmesi

Hayır, Gondorffl a bağlant ı kurma k
şeklinde gerekli ayarla-

için başk a bi r yo l bulmas ı gerekecekti .

malar yapılarak sunulan

Kolay olmayacaktı . Herhang i bi r fed -

bir telefon şirketi hizmet

eral, eyale t y a d a yere l hapishaned e

seçeneği.

tutuklu buluna n birini n gele n telefonlar a

çıkmasına izi n verilmezdi . Federa l bi r

tutukevinde he r tutukl u telefonunu n yanında asıl ı dura n levhad a şöyl e bi r şe y yazılıdır : "B u levh a buraya , b u telefondan yapıla n tü m görüşmeleri n dinlendiğin i v e telefon u kullan - manın konuşmanı n dinleneceğini n kabu l edilmes i anlamın a geldiğini hatırlatmak içi n koyulmuştur. " Eğe r su ç işleme k gib i bi r planını z varsa , devlet görevlilerini n telefon u dinlemesini n te k bi r sonuc u vardır : Hapishanedeki tatilinizi n süresini n bira z dah a uzaması .

Ancak Johnn y bell i aramaları n dinlenmediğin i biliyordu . Örneği n müvekkil-avukat görüşmes i gibi . Aslınd a Gondorffu n tutulduğ u yerd e doğrudan Federa l Kam u Savunm a Bürosu'n a (KSB) bağl ı telefonla r vardı. O telefonlarda n birin i kaldırıyordu n v e KSB'dek i bağl ı olduğ u tele - fona doğruda n ulaşıyordun . Telefo n şirketler i bun a Doğruda n Bağlant ı Hizmeti adın ı verir . Hiçbi r şeyde n kuşkulanmaya n yetkilile r b u hizmeti n güvenli v e kurcalanmay a dayanıkl ı olduğun u varsayıyorlardı , çünk ü dışarıya yapıla n aramala r yalnızc a KSB'y e gidiyor , gele n aramala r is e engelleniyordu. Bir i telefo n numaraların ı bulmay ı basars a bil e numar - alar telefo n şirketindeki santrald a reddet-ke s şeklind e programlan - mışlardı.

Johnny b u sorun u çözmeni n bi r yol u olmas ı gerektiğin e kara r verdi . Gondorff zate n içerden , KS B telefonlarında n birin i kaldırı p şun u söyle - meyi d e denemişti : "Be n Tom , telefon şirket i onarı m bölümünden . Bi - ri a t üstünd e bi r tes t yapıyoruz , önc e doku z sonr a d a sıfı r sıfı r tuşla - manız gerekiyor. " Doku z dı ş hatt â erişim i sağlayacak , sıfı r sıfı r d a şehirlerarası santral e bağlayacaktı , iş e yaramadı . KSB'd e telefon u açа r kişi b u numaray ı zate n biliyordu .

Johnny'nin işler i dah a iy i gidiyordu . Tutukevind e o n hücr e biri r

oulunduğunu v e bunları n he r birini n Kam u Savunm a Bürosu'yl a doğru - dan bağlantıl ı olduğun u kolaylıkl a öğrenmişti . Baz ı engellerl e karşılaşıy - ordu am a iy i bi r toplu m mühendis i olara k ayağ a takılı p dura n b u ca n sıkıcı taşları n çevresinde n dolaşmanı n yolların ı d a buluyordu . Acab a Gondorff hang i birimdeydi ? O hücr e birimind e buluna n doğruda n bağlan - tı hattını n telefo n numaras ı neydi ? V e hapishan e yetkililer i tarafında n engellenmeden il k mesaj ı Gondorf f a nası l ulaştıracaktı ?

Federal kurumlard a buluna n gizl i telefonları n numaralarını eld e etmek, sırada n insanlar a olanaksı z gib i görüne n bi r şe y ike n anca k bi r dalavereci içi n çoğunlukl a birka ç telefo n görüşmesiyl e el e geçirebilece k bir bilgidir . Kafasınd a oluşturduğ u plan ı birka ç gec e yatağınd a dönere k gözden geçirdikte n sonr a Johnn y bi r saba h he r şe y kafasınd a be ş adım olarak planlanmı ş bi r şekild e uyandı .

Önce, KSB'y e doğruda n bağl ı o n telefonu n numaraların ı öğrenecekti .

On telefon u birde n gele n aramalar ı alaca k şekild e değiştirecekti .

Gondorffun hang i hücr e birimind e olduğun u bulacaktı .

Sonra hang i telefonu n b u birim e bağl ı olduğun u öğrenecekti .

En sonunda , yetkiler i kuşkulandırmada n Gondorffl a bi r telefo n görüşmesi ayarlayacaktı .

Çocuk oyuncağı , diy e düşündü .

Bell Ânct'y ı Arıyor.. . •

Johnny, federa l hüküme t adın a ma l v e hizme t satı n ala n Gene l Hizmet İdaresi'nde n arıyormu ş numaras ı yapara k telefo n şirket i müdür - lüğünü aramakl a iş e başladı . Bi r e k hizme t sözleşmes i üzerind e çalıştığını v e kullanıla n doğruda n bağlant ı hizmetlerini n fatur a bilgilerin e ihtiyacı olduğun u söyledi . B u listey e Sa n Dieg o tutukevini n telefo n numaralarının v e aylı k giderlerini n d e dahi l olmas ı gerektiğin i ekledi . Karşıdaki hanı m yardımc ı olmakta n memnu n olacaktı .

Numaraları eld e ettikte n sonr a emi n olma k içi n b u hatlarda n birin i çevirdi v e karşılığınd a duyduğ u şe y tipi k bi r kayd ı oldu . "B u hattı n bağlantısı kesilmişti r y a d a ha t hizme t dışıdır. " işi n aslını n b u kayıtt a söylenenle uzakta n yakında n bi r ilgis i olmadığın ı biliyordu , ta m bek - lediği gibi , hat , gele n aramalar ı engelleme k üzer e programlanmıştı .

Telefon şirketini n çalışm a şekiller i v e süreçleriyl e ilgil i geni ş bilgis i sayesinde RCMAC , Recen t Chang e Memor y Authorizatio n Cente r (Kısa Sürel i Hafız a Değişi m Yetk i Merkez i - b u adlar ı kimi n uydurduğun u hep mera k etmişimdir!) adınd a bi r bölüm e ulaşmas ı gerektiğin i biliyor - du. Telefo n şirketini n İşlemle r Ofisi'n i aramakl a iş e başlad ı v e onarım - dan aradığın ı söyleyip , verdiğ i ala n kod u v e öneki n ai t olduğ u bölgey e

bakan RCMAC'ni n telefon numarasın ı istedi . Tutukevindek i tü m telefo n hattı hizmetler i ayn ı merke z ofiste n veriliyordu . Bu , onanm a gitmi ş v e yardıma ihtiyac ı ola n teknisyenleri n he r zama n yaptığ ı türden , sırada n bir istekt i v e memu r on a numaray ı vermekt e tereddü t etmedi .

RCMAC'yi aradı , saht e bi r a d verd i v e yin e onarı m bölümünd e çalıştığını söyledi . Telefon u aça n kadından , dah a önc e işlemle r ofisin - den aldığ ı numaralarda n birin e ulaşmasın ı istedi . Kadı n numaray ı bul - duğunda Johnn y sordu : "Numar a reddet-ke s olara k m ı ayarlanmış?"

"Evet", ded i kadın .

"Eh, bu , müşteriy e nede n hi ç telefon gelmediğin i açıklıyor!" , ded i Johnny. "Ban a bi r iyili k yapabili r misin ? Ha t sını f numarasın ı değiştir - meni y a d a reddet-ke s özelliğin i kaldırman ı isteyeceğim , olu r mu? " Kadın, değişim i gerçekleştirebilme k içi n bi r hizme t emr i gereki p gerekmediğini kontro l etme k içi n başk a bi r bilgisaya r sistemin e bakarken kıs a bi r sessizli k oldu . "B u numaranı n yalnızc a aram a yap - maya açı k olmas ı gerekiyor . Değişikli k yapma k içi n hizme t emr i yok. "

"Doğru, bi r yanlışlı k oldu . Emr i dü n çıkarmamı z gerekiyord u am a b u müşteriyle he r zama n ilgilene n abon e temsilcis i hastalanı p ev e gitt i v e bu iş i yapmay ı başkasın a söylemey i d e unuttu . B u yüzde n müşter i ş u anda küpler e binmi ş durumda. "

Kadın bi r a n duralayıp , standar t çalışm a şeklin e aykır ı v e olağa n dış ı bu isteğ i değerlendirdi , sonr a da , "Tamam" , dedi . Kadını n değişikliğ i girmek içi n tuşlar a bastığın ı duyabiliyordu . Birka ç saniy e sonr a i ş bit - mişti.

Buzlar çözülmüş , aralarınd a bi r çeşi t yakınlaşm a oluşmuştu . Kadının tavırların ı v e yardı m etm e isteğin i tartarak , Johnn y hepsin i yap - tırmakta tereddü t etmedi . "Ban a yardı m edebileceğini z birka ç dakikanı z daha va r mı? " diy e sordu .

"Var", diy e yanıtlad ı kadın . "N e gerekiyordu? "

"Aynı müşteriy e ai t başk a numarala r d a va r v e hepsind e d e ayn ı sorun mevcut . Be n numaralar ı siz e okursam , si z d e reddet-ke s ayarların ı düzeltebilir misiniz? " Kadı n bunu n soru n olmayacağın ı söyledi .

Birkaç dakik a sonr a telefon hatlarını n heps i d e gele n aramalar ı ala - cak şekild e "düzeltilmişti. "

Gondorffun bulunmas ı

Bir sonrak i adı m Gondorffu n hang i hücr e birimind e olduğun u bul - maktı. Hapishan e v e tutukevlerin i yönetenle r b u bilgiy i dışarıda n biri - lerinin öğrenmesin i kesinlikl e istemezler . Johnny'ni n bi r ke z dah a toplu m mühendisliği becerilerin e güvenmes i gerekiyordu .

Başka bi r şehirdek i bi r federal hapishaney i aradı ; Johnn y Miami'y i aramıştı -am a başk a herhang i bi r ye r d e i ş görürdü - v e Ne w York'tak i tutukevinden aradığın ı söyledi . Müdürlüğü n tutukl u bilgisayarınd a çalışan biriyl e konuşma k istedi . Tutukl u bilgisayarı , ülkeni n herhang i bi r yerinde Hapishanele r Müdürlüğü'n e bağl ı tesislerd e tutula n mahkûmlar - la ilgil i bilgileri n saklandığ ı bilgisaya r sistemiydi .

İlgili kiş i telefon a çıktığınd a Johnny , Brookly n aksanıyl a konuşmay a başladı. "Merhaba, " dedi . Be n Ne w Yor k Federa l Tutukevi'nde n Thomas. Tutukl u bilgisayarıyl a bağlantımı z gidi p geliyor , bi r tutuklunu n yerini bulmam a yardımc ı olabili r misin , sanırı m sizi n orad a tutuluyor " v e GondonTun adın ı v e kayı t numarasın ı verdi .

"Hayır, burad a değil" , ded i ada m birka ç saniy e sonra . "Sa n Diego'daki tutukevinde. "

Johnny şaşırmı ş gib i yaptı . "Sa n Dieg o mu ? Geçe n haft a korumal ı bir uçakl a Miami'y e aktarılmas ı gerekiyordu ! Ayn ı adamda n m ı sö z ediy - oruz? Adamı n doğu m tarih i nedir? "

"3/12/60", ded i ada m ekranda n okuyarak .

"Evet, ayn ı adam . Hang i hücr e birimind e tutuluyor? "

"Hücre O n Kuzey" , ded i adam . He r n e kada r Ne w York'tak i bi r hapis - hane görevlisini n böyl e bi r şey i öğrenme k istemesini n anlaşılı r bi r nedeni olmas a d a soruy u neşeyl e yanıtlamıştı .

Johnny tü m telefonlar ı gele n aramala r içi n açtırmı ş v e Gondorffu n hangi hücr e birimind e olduğun u da öğrenmişti . Bi r sonrak i adı m hang i telefon numarasını n Hücre O n Kuzey olduğun u bulmaktı .

Bu bira z zo r olacaktı . Johnn y numaralarda n birin i aradı . Telefo n zil i kapalı olacağ ı içi n kimseni n telefonu n çaldığın ı anlamayacağın ı biliyor - du. Oturd u v e Fodor'u n Avrupa'nı n Büyü k Kentler i adl ı gez i rehberin e göz gezdirirke n bi r yanda n d a ahizede n çalm a sesin i dinliyordu . Sonunda bir i telefon u açtı . Diğe r uçtak i tutukl u doğa l olara k mahkemec e belirlenmiş avukatın a ulaşmay a çalışıyordu . Johnn y karş ı tarafi n bek - lentisine karşılı k verece k yanıt ı hazırlamıştı . "Kam u Savunm a Bürosu" , dedi.

Adam avukatıyl a görüşme k istediğin i söylediğinde , Johnny , "Burad a olup olmadığın ı bakayım , hang i hücr e biriminde n arıyorsun? " dedi . Adamın yanıtın ı no t etti , bekletm e düğmesin e bastı , otu z saniy e sonr a yeniden açt ı ve , "Mahkemedeymiş , dah a sonr a arama n gerekecek" , diyerek kapattı .

Sabahının çoğun u bun u yapara k geçird i am a dah a kötüs ü d e ola - bilirdi. Dördünc ü denemesind e Hücre O n Kuzey"\ buldu . Böylec e Johnny artı k Gondorffu n birimin e ai t KS B numarasın ı biliyordu .

Saatlerinizi ayarlayı n • ' '

Şimdi i ş Gondorff a tutuklular ı doğruda n Kam u Savunm a Bürosu'yl a görüştüren telefon u n e zama n açacağın ı söyleye n bi r mesa j gönderm - eye kalıyordu . B u göründüğünde n dah a kola y bi r işti .

Johnny tutukevin i arayarak , e n resm i sesiyl e kendin i bi r çalışa n olarak tanıtt ı v e Hücr e O n Kuzey'l e görüşme k istediğin i söyledi . Aram a hemen aktarıldı . İnfa z korum a memur u telefon u açtığınd a Johnny , yen i tutukluların giri ş v e çıkışların ı düzenleye n Dağıtı m v e Tahliy e Birimi'ni n i ç görüşmelerde kullanıla n kısaltmasın ı kullanara k memur u kandırdı . "Be n DT'den Tyson" , dedi . "Tutukl u Gondorffl a görüşme m gerek . Göndermemiz gereke n on a ai t eşyala r var , nerey e gönderilmesin i istiy - orsa oranı n adresin i vermes i gerekiyor . On u telefon a çağırabili r misiniz? "

Johnny memuru n oturm a salonun a bağırdığın ı duydu . Birka ç dakikalık sabırsı z bi r bekleyişten sonra , telefon a tanıdı k bi r se s çıktı .

Johnny ona , "Konuşma m biten e kada r sakı n sesin i çıkarma" , dedi . Eşyaların nerey e gönderilmesin i istediğin i konuşuyorlarmı ş gib i görün - mesi içi n Johnn y on a söylemes i gerekenler i anlattı , sonr a da , "Bugü n öğleden sonr a saa t bird e Kam u Savunm a Büros u telefonunu n başınd a olabileceksen, yanı t verme . Olamayacaksan , o zama n orad a olabileceği n bir saat i söyle" , dedi . Gondorf f yanı t vermedi . Johnn y deva m etti . "iyi . Saat bird e orad a ol . Sen i arayacağım . Ahizey i kaldır . Eğe r telefo n otomatik olara k Kam u Savunm a Bürosu'n u aramay a başlars a he r yirm i saniyede bi r telefonu n düğmesin e bas . Sesim i duyan a kada r bun u yap - mayı sürdür. "

Saat bird e Gondorf f telefon u açt ı v e Johnn y orad a on u bekliyordu . Sohbet ede r gibi , aceley e getirmeden , keyifl e konuştula r v e benze t görüşmeler Gondorffu n mahkem e masrafların ı karşılama k içi n çevire - cekleri dolabı n ayrıntıların ı konuşma k amacıyl a birka ç ker e dah a tekrar - landı. Heps i d e devle t gözetimini n dışınd a gerçekleşmişti .

Aldatmacanın incelenmes i

Bu olay , bi r toplu m mühendisinin , he r bir i te k başın a önemsi z gib i duran işler i yapmalar ı içi n farkl ı insanlar ı kandırarak , olanaksı z zannedilen bi r iş i nası l başardığın ı göstere n çarpıc ı bi r örnektir . Aslında , yapılan he r hareket , dalaver e tamamlanan a kada r bulmacanı n bi r parçasını oluşturur .

ilk telefo n şirket i çalışanı , federa l hükümet e bağl ı Gene l Hizmetle r İdaresi'nden birin e bilg i verdiğin i düşünüyordu.. .

Bir sonrak i telefo n şirket i çalışanı , telefon hizme t sınıfın ı bi r hizme t emri olmada n değiştirmemes i gerektiğin i biliyord u am a yin e d e sevimi , adama yardımc ı oldu . Böylec e tutukevindek i Kam u Savunm a Büros u

telefonlarının tüm ü dışarıda n aranabili r durum a geldi .

Miami tutukevindek i ada m içi n başk a bi r federa l merkezd e çalışa n v e bilgisayarla soru n yaşaya n birin e yardı m etme k gaye t mantıklıydı . He r n e kadar hücr e birimin i öğrenme k istemes i içi n bi r nede n yokmu ş gib i gözüks e de, soruy a yanı t vermemes i içi n d e bi r nede n yoktu , öyl e deği l mi ?

Ve arayanı n ayn ı tesi s içinde n bir i olduğun u sana n Hücre O n Kuzej/de görevl i memur , adamı n resm i bi r i ş içi n aradığın ı düşünüyor - du, istediğ i oldukç a mantıklıydı , b u yüzde n Gondorf f isiml i tutukluy u telefona çağırdı . Soru n olmadı .

Bir diz i iy i planlanmı ş adım ı bi r aray a getiri p dalaverey i tamam - lamışlardı.

Hızlı dosy a indirm e

Hukuk fakültesin i bitirmelerinde n o n yı l sonr a Ne d Racin e hâlâ , fat - urasını ödeyece k kada r paras ı olmaya n insanları n kıytırı k işleriyl e uğraşırken, sını f arkadaşları , bahçeler i ola n güzel evlerd e yaşıyor , şehi r klüplerine üy e oluyor , haftad a bir-ik i ke z gol f oynuyorlardı . Sonund a bi r gün Ned'i n canın a ta k etti .

Şimdiye kada r eld e ettiğ i te k iy i müşterisi , şirke t birleşmeler i v e devirler konusund a uzmanlaşmış , küçü k am a oldukç a başarıl ı bi r muhasebe şirketiydi . Uzu n süredi r Ned'l e i ş yapmıyorlardı . Ne d müşter - ilerinin, gazetelerd e çıkmas ı halind e birka ç halk a açı k şirketi n hiss e senedi fiyatların ı etkileyebilece k baz ı işler e karıştıkların ı anlamıştı . Önemsiz, doğruda n işle m görmeye n hisselerd i am a baz ı açılarda n b u daha iyiydi ; fiyatlardak i küçü k bi r firlam a yatırımlarda n eld e edile n büyü k yüzdeli bi r getir i anlamın a geliyordu . Adamları n dosyaların a ulaşı p neyl e uğraştıklarını bi r bulabilirs e i ş tama m olacaktı .

Alışılmadık yöntemle r konusund a akıll ı birin i tanıya n bi r arkadaş ı vardı . Adam plan ı dinledi , gaz a geld i v e yardı m etmey i kabu l etti . Ned'i n port - föyündeki hiss e senetler i yüzdesin e bakı p he r zama n aldığında n dah a küçük bi r ücre t karşılığınd a Ned' e n e yapmas ı geveteğOT . aulattı . Ayrıc a on a piyasaya çıkal ı ço k a z zama n olmu ş küçü k v e kullanışl ı bi r ale t d e verdi .

Birkaç gü n boyunc a Ned , muhaseb e şirketini n gösterişsiz , mağaz a

Mitnick Mesajı :

Sanayi casusları ve bilgisayarlara giren kişiler, hedef işletmelere bazen fiziksel olarak da girerler. İçeri girmek için bir demir sopa kullanmak yerine, toplum mühendisi kapının diğer tarafındaki insanı etkilemek için aldatma sanatını kullanır.

vitrinine benzeyen bürosunu n bulunduğ u küçü k i ş hanını n arab a par k yerini gözetledi . Çoğ u insa n be ş buçuk , alt ı gib i çıkıyordu . Yediy e doğr u park yer i tamame n boşalıyordu . Temizlikçile r yed i buçu k gib i geliyor - lardı. Mükemmel .

Ertesi gece , sekiz e birka ç dakik a kala , Ne d otoparkı n kaşısındak i yola arabasın ı par k etti . Beklediğ i gib i temizli k hizmetler i şirketini n kamyonu sayılmazs a par k yer i boştu . Ne d kapıy a kulağın ı koyd u v e elektrikli süpürgeni n gürültüsün ü duydu . Sertç e kapıy ı çald ı v e beklem - eye başladı . Takı m elbis e giymiş , krava t takmışt ı v e elind e yıpranmı ş çantasını taşıyordu . Yanı t gelmed i am a o sabırlıydı . Bi r dah a çaldı . Sonunda kapıd a temizlikçilerde n bir i belirdi . "Merhaba" , ded i Ned , ca m kapının arkasında n bağırara k v e dah a önc e şirke t ortaklarında n birinden aldığ ı kartvizit i göstererek . "Anahtarlarım ı arabam a kilitlemişim , masama gitme m gerekiyor. "

Adam kapıy ı açtı , sonr a Ned'i n arkasında n tekra r kilitled i v e korido - ra gidere k Ned'i n gittiğ i yer i görebilmes i içi n ışıklar ı açtı . Nede n olmasın ; ekmeğini kazanmasın ı sağlaya n insanlarda n birin e yardımc ı olmay a çalışıyordu. Böyl e düşünmes i içi n he r neden i vardı .

Ned ortaklardan birini n bilgisayarını n başın a oturd u v e makinay ı açtı. Bilgisaya r açılırke n on a verile n küçü k alet i bilgisayarı n US B girişin e taktı. Bi r anahtarlıkt a taşınabilece k kada r küçü k bi r aletti , anca k yin e d e 120 megabay t ver i taşıyabiliyordu . Ortağı n sekreterini n bi r Post-i t kâğı - da yazı p ekran a yapıştırdığ ı kullanıc ı adın ı v e parolasın ı kullanara k ağ a girdi. Be ş dakikada n az bi r süred e bilgisayard a ve ortakları n ağ klasöründe yükl ü tü m çizelg e v e belg e dosyaların ı indirmi ş evin e gidiy- ordu.

Kolay par a

Lisede il k def a bilgisayarlarl a tanıştığımda , Lo s Angeles'tak i tü m okulların paylaştığı merkez i bi r DE C PD P 1 1 minibilgisayarın a mode m aracılığıyla bağlanıyorduk . O bilgisayard a kurul u işleti m sistemini n ad ı RSTS/E'ydi v e il k kullanmay ı öğrendiği m işleti m sistemiydi .

O zamanlar , yan i 1981'd e DE C firmas ı ürü n kullanıcılar ı içi n yıllı k bi r kon - ferans düzenliyord u v e bi r yerd e konferanslarda n birini n Lo s Angeles't a düzenleneceğini okudum . B u işleti m sistemini n kullanıcılar ı içi n hazırlana n tanınmış bi r dergid e LOCK-1 1 adl ı yen i bi r güvenli k ürününü n duyurus u vardı . Ürün akıllıc a hazırlanmı ş bi r rekla m kampanyasıyl a sunuluyordu . "Saa t sabah 3:3 0 v e sokağı n ilersind e otura n Johnn y sizi n bağlant ı numaranız ı 336 . denemesinde bulmuş , 555-0336 . O içer i girmiş , siz i d e dışar ı sepetlemi ş Sizin d e bi r LOCK-11'ini z olsun. " Reklamı n anlattığın a gör e ürü n bilgisaya r korsanlarına karş ı ta m korum a sağlıyordu . V e konferanst a tanıtılıyo r olacakt ı

Ürünü görmey i be n d e ço k istiyordum . Yıllardı r birlikt e korsanlı k yap -

F

Teknolojiyi v e Toplu m Mühendisliğin i Birleştirme k 16 9

tığımız, lisede n sını f arkadaşı m v e dostu m am a sonrada n ban a karş ı çalışan bi r federa l ihbarc ı ola n Vinny , yen i DE C ürünün e yöneli k ilgim i paylaşıyordu v e konferans a onunl a birlikt e gitme m içi n ısra r etti .

Peşin par a '

Ürün tanıtımın a gittiğimizd e LOCK-11'i n çevresindek i kalabalıkt a bi r çalkalanma vardı . Görünüş e gör e tasarımcıla r kimseni n ürünlerin i kıra - mayacağına dai r anınd a ödem e yapacaklar ı bi r bahi s oluşturmuşlardı . Bu reddedemeyeceği m bi r meyda n okumaydı .

Doğrudan LOCK-11'i n tanıtı m masasın a gitti k v e başınd a ürünü n tasarımcıları ola n ü ç adamı n durduğun u gördük . Onlar ı tanımıştı m v e onlar d a ben i tanımışlardı ; yetkililerl e yaşadığı m il k gençli k sürtüşmeler - imle ilgil i Lo s Angele s Time s gazetesind e çıka n büyü k bi r yaz ı nedeniyle, gençliğimd e bil e bi r telefo n beleşçis i v e bilgisaya r korsan ı olarak bell i bi r ünü m vardı . Yazıd a anlatıldığın a göre , geceni n bi r yarısında Pasifi k Telefo n şirket i binasın a girebilme k içi n kapıdakiler i ikna etmi ş v e güvenli k görevlilerini n burunlarını n dibinde n elimd e bil - gisayar kullanı m kılavuziarıyl a çıkı p gitmiştim . (Görünüş e gör e Lo s Angeles Time s çarpıc ı bi r öyk ü çıkarma k istemişt i v e adım ı yayınlama k işlerine yaramıştı . Dah a ergenli k çağınd a olduğu m için , yaz ı su ç işleye n çocukların isimlerini n saklanmas ı yasasın ı çiğnemes e d e gelenekler e aykırı bi r durum u vardı.)

Vinny v e be n oray a gittiğimizde , b u he r ik i taraft a d a bi r ilg i uyandı . Karşı taraft a bi r ilg i uyandırmıştı , çünk ü beni m gazeted e okuduklar ı kor - san olduğum u anlamışlard ı v e ben i gördüklerin e bira z şaşırmışlardı . Bizim taraft a d a şaşkınlı k yaratmıştı , çünk ü tasarımcılarda n he r birini n yaka kartını n arkasın a bi r 10 0 dolarlı k bankno t sıkıştırılmıştı . Sistemlerin i kırabilecek kişiy e verecekler i ödü l 30 0 dolardı . Bu , bi r çif t oku l çocuğ u için ço k par a gib i görünüyordu . İş e koyulma k içi n sabırsızlanıyorduk .

LOCK-11 ik i katl ı güvenliğ e dayana n bilindi k bi r yönteml e yapılmıştı . Her zamank i gib i kullanıcını n geçerl i bi r kimliğ i v e parolas ı olmalıydı , ama bun a e k olara k kimli k v e parol a yal -

nızca yetkil i uçbirimlerde n girildiğind e .

işe yarıyordu . B u yaklaşım a uçhirim \ T©rİfTil© f i tabanlı güvenlik deniyordu . Sistem i kıra - | i bilmek içi n bi r korsanı n yalnızc a kimli k \ UÇBİRİM TABANLI \ ve parolay ı bilmes i yeterl i değildi , bilgiy i j GÜVENLİK: Kısmen belirli I doğru uçbirimde n giriyo r olmas ı d a j bir uçbirimin tanımlan- \ gerekiyordu. İy i kurulmu ş bi r sistemd i v e i masına bağlı olarak kul- i LOCK-11'in yaratıcılar ı köt ü adamlar ı j landan güvenlik; b u güven- I dışarıda tutacağında n emindiler . Onlar a | ti k yöntemi özellikle IBM i n j bir der s verece k v e üstün e üstlü k ü ç yü z I büyük bilgisayarlarında çok \ dolar kazanacaktık . i kullanılırdı. i

Mitnick Mesajı : ^

| İşte, akıllı insanların rakiplerini hafife almalarına bir örnek daha. Siz ne dersiniz: Siz de şirketinizin güvenlik önlemlerine, üzerlerine 300 dolar bahse girecek kadar güveniyor musunuz? Bazen teknolojik bir güvenlik önleminin çevresinden dolaş- I manın tek yolu sizin düşündüğünüz şekilde değildir.

RSTS/E üstad ı olara k biline n v e beni m d e tanıdığı m adamlarda n bir i bizden önc e tanıtı m masasın a gelmişti . Yılla r önc e kend i arkadaşlar ı beni ger i çevirdikte n sonr a DE C dahil î geliştirm e bilgisayarın a girme m konusunda ban a meyda n okuya n adamlarda n biriydi . O günde n b u yan a saygın bi r programc ı olmuştu . Bi z gelmede n önc e LOCK-11' i kırmay ı denediğini faka t başaramadığın ı öğrendik . Ola y tasarımcılara , ürün - lerinin gerçekte n güvenl i olduğ u konusund a büyü k güve n vermişti .

Yarışma ço k basitti : Kırıyordun , paray ı alıyordun . İy i bi r tanıtı m gös - terisiydi; bir i onlar ı küçü k düşürüp paray ı almadığ ı sürece . Ürünlerinde n o kada r eminlerd i k i tanıtı m masasın a sistemdek i baz ı hesaplar a ai t hesap numaraların ı v e parola n içere n bi r listey i asm a cüretin i bil e göstermişlerdi. Hiçbir i d e öyl e sırada n hesapla r değildi , heps i d e yetkil - erle donatılmı ş ayrıcalıkl ı hesaplardı .

Bu aslınd a kulağ a geldiğ i kada r çarpıc ı birşe y değildi . Böyl e bi r düzenekte, he r uçbirimi n doğruda n bilgisayarı n üstündek i girişlerde n birine bağlandığın ı biliyordum . Konferan s salonun a bi r ziyaretçini n yal - nızca ayrıcalıklar ı olmaya n bi r kullanıc ı olara k bağlanabilmesin e izi n veren be ş uçbiri m kurdukların ı anlama k içi n dâh i olmay a gere k yoktu . Diğer bi r deyişl e b u uçbirimierde n bağlanma k yalnızc a siste m yöneticis i olmayan hesaplarl a mümkündü , ik i yo l varmı ş gib i görünüyordu : Y a güvenlik yazılımın ı olduğ u gib i bertara f edecekti k -k i b u LOCK-11'i n tasarlanış amacıydı - y a d a bi r şekild e tasarımcıları n düşünmediğ i bi r şekilde yazılımı n çevresinde n dolaşacaktık .

Meydan okumay a karşılı k verme k

Vinny v e be n orada n uzaklaşı p bahs i konuşmay a başladı k v e beni m aklıma bi r pla n geldi . Masu m masu m ortalıkt a gezini p uzakta n tanıtı m masasını gözlüyorduk . Öğle n olduğund a v e kalabalı k azaldığınd a ü ç tasarımcı aralıkta n yararlanı p birlikt e yemeğ e gittile r v e gerid e araların - dan birini n karıs ı y a d a kı z arkadaş ı olabilece k bi r kadı n bıraktılar . Tekrar ger i gitti k v e onda n bunda n konuşara k be n kadın ı oyalamay a başladım. "N e kada r zamandı r şirkett e çalışıyorsunuz ? Şirketinizi n pazarda başk a hang i ürünler i var? " gib i şeyler .

Bu sırad a Vinn y kadını n görebileceğ i alanı n dışınd a iş e koyulmuş , her ikimizi n d e geliştirdiğ i bi r becerisin i kullanıyordu . Bilgisayarlar a

girme çılgınlığımı z v e sihirbazlığ a duyduğu m kend i ilgi m dışında , ikimi z de kili t açmakl a ço k ilgileniyorduk . Küçükke n Sa n Femand o Vadisi'nde , kilit açma , kelepçelerde n kurtulma , saht e kimli k yaratm a gib i konularda - bir çocuğu n bilmemes i gereke n he r şeyl e ilgil i aykır ı kitapları n bulun - duğu bi r kitapçını n rafların ı didi k didi k etmiştim .

Vinny de beni m gib i hırdavatçıda n alınmı ş herhang i bi r sırada n kili - di açma k konusund a oldukç a iy i olan a kada r çalışmıştı . Bi r ar a kilitlerl e ilgili şakala r yapmay a bayılırdım . Örneği n dah a güvenl i olsu n diy e ik i kilit birde n kullana n birin i görürse m ik i kilid i d e açar , yerlerin i değiştirirdim, b u d a he r birin i yanlı ş anahtarl a açmay a çalışa n kili t sahib - inin kafasın ı karıştırı p canın ı sıkardı .

Sergi salonund a be n gen ç kadın ı oyalarke n Vinn y masanı n gerisinde görülmeyece k şekild e yer e çökmüş , adamları n PDP-1 1 mini - bilgisayarlarının v e kabl o sonlarını n durduğ u dolabı n kilidin i açıyordu . Dolabın kilitl i olduğun u düşünmeler i şak a gibiydi . Çilingirleri n gofre t kili t dedikleri, bizi m gib i oldukç a acem i kili t açıcıla r tarafında n bil e anahtarsız açmas ı ço k kola y ola n kilitle r kullanıyorlardı .

Vinny'nin kilid i açmas ı bi r dakik a kada r sürdü . Dolabı n içind e ta m aradığı şey i bulmuştu . Kullanıc ı uçbirimlerin i bağlama k içi n bi r diz i bağlantı noktasını n yan ı sır a konso l uçbirim i içi n d e ayr ı bi r bağlant ı noktası vardı . B u uçbiri m bilgisaya r işletmenini n y a d a siste m yöneti - cisinin tü m bilgisayarlar ı yönetmes i içi n kullanılıyordu . Vinn y konso l bağlantısından çıka n bi r kabloy u tanıtı m masasındak i uçbirimlerde n birine taktı .

Bu, b u uçbirimi n artı k bi r konso l uçbirim i olara k tanınacağ ı anlamın a geliyordu. Yen i bi r kabl o takılmı ş makinanı n başın a oturdu m v e tasarım - cıların korkusuzc a verdikler i parolalarda n birin i kullanara k sistem e girdim. LOCK-1 1 yazılım ı artı k ben i yetkil i bi r uçbirimde n bağlanıyo r olarak gördüğ ü içi n ban a giri ş izn i vermişt i v e bi r siste m yöneticisini n yetkileriyle bağlanmıştım . Buradak i tü m uçbirimlerde n ayrıcalıkl ı kul - lanıcı olara k bağlanmam ı sağlayaca k şekild e değiştirere k işleti m sis - temini yamaladım .

Gizli yama m yüklendikte n sonr a Vinn y uçbiri m kablosun u çıkarı p il k takılı olduğ u yer e ger i takm a işin i yaptı . Sonr a kilid i yenide n kurcalayı p bu sefe r dolabı n kapısın ı kilitledi .

Bilgisayarda hang i dosyaları n olduğun u görme k içi n bi r dizi n dökümü aldım . LOCK-11'i n programın a v e ilgil i dosyalara bakarke n ço k şaşırtıcı bulduğu m bi r şeyle , b u bilgisayard a bulunmamas ı gereke n bi r dizinle karşılaştım . Tasarımcıla r kendilerinde n v e yazılımlarını n aşıla - maz olduğunda n o kada r eminlerd i ki , yen i ürünlerini n kayna k kodların ı kaldırmaya bil e yeltenmemişlerdi . Heme n yanındak i çıkt ı alm a uçbirim - ine geçerek , kayna k kodunu n parçalarını , o zamanla r kullanıla n yeşi l şeritli sürekl i formlar a bastırmay a başladım .

Vinny kilid i kapamay ı yen i bitirmi ş v e yanım a gelmişt i k i adamla r öğle yemeğinde n dönüyorlardı . Yazıc ı yazmasın ı sürdürürken , ben i bil - gisayarın klavyesin e birşeyle r girerke n buldular . "N e yapıyorsun , Kevin?" diy e sord u bi r tanesi .

"Sadece kayna k kodlarınızı n çıktısın ı aldırıyorum " dedim . Doğa l olarak şak a yaptığım ı düşündüler . T a k i yazıcıy a bakı p çıktıları n gerçek - ten titizlikl e koruduklar ı ürünlerini n kayna k kod u olduğun u görüncey e . kadar .

Ayrıcalıklı kullanıc ı olara k girdiğim e inanamadılar . "Bi r Kontrol- T gir" , dedi tasarımcılarda n biri . Girdim . Ekrand a çıka n görünt ü söylediklerim i doğruluyordu. Vinny , "Ü ç yü z dolar , lütfen" , derke n ada m alnın a vuruyordu .

Adamlar paray ı ödediler . Günü n kalanınd a Vinn y v e be n konferan s kartlarımıza taktığımı z yü z dolarlı k banknotlarl a dolaştık . Herke s par - aların n e anlam a geldiğin i biliyordu .

Vinny v e ben , doğa l olarak , yazılım ı yenmişti k v e eğe r tasarı m ekib i yarışma içi n dah a iy i kuralla r belirleselerd i y a d a dah a iy i bi r kili t kul - lansalardı y a d a teçhizatlarını n başınd a dursalardı , o gü n bi r çif t çocuğun elinde n çektiklerin i çekmeyeceklerdi .

Sonradan öğrendi m k i tasarı m ekib i par a çekme k içi n bankay a uğra - mak zorund a kalmış . Biz e verdikler i yü z dolarlı k banknotla r yanlarınd a getirdikleri tü m paraymış .

Bir saldır ı aracı olara k sözlü k

Eğer bir i parolanız ı el e geçirirs e sisteminiz i işga l edebilir . Çoğ u durumda neyi n ter s gittiğin i bil e anlamazsınız .

Adına İva n Peter s diyeceği m gen ç bi r saldırganı n yen i bi r oyunu n kaynak kodun u el e geçirme k gib i bi r hedef i vardı . Şirketi n geni ş ala n ağına (WAN) girmekt e zorlanmamıştı , çünk ü bilgisaya r korsan ı arkadaşlarından bir i şirketi n interne t sunucularında n birin i çokta n aşmıştı. Arkadaş ı interne t yazılımınd a güncellenmemi ş bi r açı k bulduk - tan sonr a sistemi n ik i yönl ü sunuc u olara k kurulduğun u anlayınc a neredeyse küçü k dilin i yutmuştu . Yan i dahil î ağ a girme k içi n d e bi r giri ş noktası bulunuyordu .

Ama iva n bağlandıkta n sonra , Louvr e müzesin e girme k v e Mon a Lisa'yı bulmay a çalışmakl a e ş değe r bi r zorlukl a karşılaşmıştı . Müz e haritası elinizd e yoks a orad a haftalarc a gezinebilirdiniz . Şirket , yüzlerc e ofisi v e binlerc e bilgisaya r sunucus u ola n düny a çapınd a bi r şirkett i v e tam olara k geliştirm e sistemlerin e ai t bi r dizi n sunmuyo r y a d a on u doğru yer e götürece k bi r tu r rehber i d e sağlamıyordu .

Hedeflediği sunucuy u bulma k içi n tekni k bi r yaklaşı m kullanma k yer -

ine iva n bi r toplu m mühendisliğ i yaklaşım ı kullandı . B u kitapt a açıklana n yöntemlere dayana n telefo n görüşmeler i yaptı . Önce , B l tekni k deste k servisini arayara k ekibiyl e tasarladıklar ı üründ e arayü z sorun u yaşaya n bir şirke t çalışan ı olduğun u söyled i v e oyu n geliştirm e ekibini n proj e lid - erinin telefo n numarasın ı istedi .

Sonra kendisin e verile n adı , Bi'de n bir i gib i davranara k aradı . "B u gece ge ç saatlerd e bi r router ı değiştireceği z v e ekibinizi n sunucuyl a bağlantısının kopmayacağında n emi n olma k istiyoruz . Bunu n içi n ekib - inizin hang i sunucuy u kullandığın ı bilmemi z gerekiyor. " A ğ sürekl i yenileniyordu v e sunucunu n adın ı vermeni n hiçbi r zarar ı olmazdı , öyl e değil mi ? Sunuc u parol a korumal ı olduğun a gör e yalnızc a adın ı bilme k içeri girmey e çalışa n birini n işin e yaramazdı . Böylec e ada m saldırgan a sunucunun adın ı verdi . Arayanı n anlattıklarını n doğr u olu p olmadığın ı kontrol etmey e y a d a adamı n adın ı soyad ı v e telefonun u almay a yelten - medi bile . Yalnızc a sunuc u adların ı verdi ; ATM 5 v e ATM6 .

Parola saldırıs ı ....._. ;.;. . . . .. . -

Bu noktad a iva n tanımlam a bilgilerin i alma k içi n tekni k bi r yaklaşı m kullandı. Uzakta n erişi m kabiliyet i suna n sistemler e yapıla n tekni k saldırıların çoğund a il k adı m sistem e il k giri ş noktasın ı oluşturaca k zayı f parolalı bi r hesa p bulmaktır .

Bir saldırga n parolalar ı uzakta n tanımlayaca k korsanlı k araçlar ı kul - lanmaya kalkarsa , b u çabas ı onu n şirketi n ağm a saatlerc e bağl ı kalmasını gerektirebilirdi . Açıkças ı bun u yapmas ı pe k akıllıc a olmazdı , çünkü n e kada r uzu n sür e bağl ı kalırs a farkedilm e v e yakalanm a risk i de o kada r artardı . -•-..... •

Hazırlık adım ı olara k iva n hede f sistemi n ayrıntıların ı göstere n bi r sayım yapacaktı . Bi r ke z dah a interne t b u ama ç içi n gerekl i yazılım ı kolayca sağlıyord u (http://ntsleuth.Ocatch.com ; "catch " kelimesini n başındaki sıfir) . İvan , internet'te sayı m sürecin i otomatikleştire n v e herkese açı k pe k ço k korsanlı k arac ı buldu . Kuruluşu n çoğunlukl a Windows tabanl ı sunucula r kullandığın ı bilerek , bi r NetBIO S (teme l giriş/çıkış sistemi) sayı m program ı ola n NBTE'ni n yazılımın ı indirdi .

ATM5 sunucusunu n İ P adresin i gird i v e

programı çalıştırmay a başladı . Sayı m

programı sunucud a tanıml ı pe k ço k

1 hesa p bulmuştu .

SAYIM: Hedef sistemde

sunulan hizmetleri, işletim

Var ola n hesapla r belirlendikte n sistemi tabanını ve sisteme

sonra, ayn ı sayı m aracını n bilgisaya r
erişimi olan kullanıcıların
sistemine sözlü k saldırıs ı yapm a özelliğ i
hesap adlarının listesini
kullanılabilirdi. Sözlü k saldırıs ı çoğ u bil -
veren bir süreç.
gisayar güvenliğ i çalışanını n v e saldır -
ganların oldukç a yakında n bildikler i bî r

şeydir am a pe k ço k kiş i bunu n mümkü n olduğunu , duyunc a herhald e şaşkına uğrayacaktır . B u tar z bi r saldırı , sistemdek i he r kullanıcını n parolasını sıkç a kullanıla n kelimeler i tarayara k ortay a çıkarmay a yöne - liktir.

Bazı şeyler i yapma k konusund a tembelli k edebiliyoru z am a paro - lalarını seçerlerke n insanları n yaratıcılıklarını n v e hayal güçlerini n kay - bolduğunu görme k ben i he p hayret e düşürmüştür . Çoğumu z biz e koru - ma sağlaya n bi r parol a isteri z am a ayn ı zamand a kola y hatırlanmasın ı da isteri z v e b u genellikl e kendimiz e yakı n şeyle r olmas ı anlamın a gelir . Adımızın ba ş harfleri , göbek adımız , lâkabımız , eşimizi n adı , e n sevdiğimiz şarkı , fil m y a d a yeme k olabilir . Oturduğumu z sokağı n ad ı y a da yaşadığımı z şehri n adı , kullandığımı z arabanı n markası , Havvai'd e kalmak istediğimi z sahildek i tati l köyünü n ad ı y a d a e n iy i alabalıklar ı avladığımız e n sevdiğimi z akarsuyu n adı . Burad a çıka n desen i gördünüz mü ? Bunla r çoğunlukl a kiş i adları , ye r adlar ı y a d a sözlükt e bulunabilecek sözcükler . Bi r sözlü k saldırısı , sı k kullanıla n kelimeler i hızlı bi r şekild e girere k he r birini n bi r y a d a dah a fazl a kullanıc ı hesabının parolas ı olu p olmadığın a bakar .

İvan sözlü k saldırısın ı ü ç basamakt a çalıştırdı . İlkind e yaklaşı k 80 0 kelimelik e n sı k kullanıla n parolalarda n oluşa n basi t bi r list e kullandı . B u listede gizli , i ş v e parol a kelimeler i d e vardı . Progra m ayrıc a sözlü k kelimelerinin yanına say ı ekleyere k y a d a içind e buluna n ayı n sayısın ı girerek sır a değişiklikler i d e yapıyordu . Progra m he r kelimey i belirlenmi ş tüm kullanıc ı hesaplarınd a deniyordu . İş e yaramadı .

Sonraki denemesind e ivan , Googl e aram a motorun a gitt i v e "sözcü k listeleri sözlükler " anahta r kelimeleriyl e aram a yaptı , ingilizc e v e pe k çok yabanc ı di l içi n kapsaml ı sözcü k listeler i v e sözlükle r buluna n bin - lerce sit e buldu . Bi r İngilizc e sözlüğü n tümün ü indirdi . Sonr a Google'd a bulduğu baz ı sözcü k listelerin i d e indirere k elindekiler i zenginleştirdi . İvan www.outpost9.com/filesAA/ordLists.htm l sitesin i seçmişti .

Bu sit e ona , aralarınd a soyadların , adların , kongr e üyelerini n adlarını n ve ilgil i kelimelerin , oyuncuları n adlarının , incil'de n kelimeleri n v e adları n olduğu, indirilebilece k (heps i d e ücretsiz) bi r diz i dosy a sunuyordu .

Sözcük listeler i suna n pe k ço k sitede n bir i d e aslınd a Oxfor d Üniver - sitesinin sitesiydi ; ftp://ftp.ox.ac.uk/pub/wordlists .

Diğer sitele r çizg i fil m karakterlerini , Shakespeare'i n kullandığ ı sözcükleri, Odyssea'd a geçe n kelimeleri , Tolkie n v e Uza y Yol u dizisini n yanı sır a bili m v e dinl e ilgil i olanlar ı d a içere n başk a listele r d e sunuyor - lardı. (Bi r şirke t 4, 4 milyo n sözcü k içere n bi r listey i yalnızc a 2 0 dolar a sat - maktadır.) Saldır ı program ı sözlüktek i kelimeleri n anagramların ı -pe k ço k bilgisayar kullanıcısını n güvenliklerin i artırdığın ı düşündüğü , sevile n W yöntemdir- deneyece k şekild e d e programlanabilir . « ,

Teknolojiyi v e Toplu m Mühendisliğin i Birleştirme k 17 5

Düşündüğünden dah a hızl ı

ivan hang i sözcü k listesin i kullanacağın a kara r verdikte n sonr a saldırıy a geçti. Yazılı m otomati k olara k çalışıyord u v e İva n dikkatin i başk a şeyler e .erebilirdi. İşi n inanılma z taraf ı is e şuydu : Böyl e bi r saldır ı sırasınd a bilgisa - .ar korsanını n Ri p va n Winkl e gib i uykuy a dalacağın ı v e uyandığınd a yazılımın dah a küçücü k bi r yo l katetmi ş olacağın ı düşünebilirsiniz . Aslında , saldırılan işleti m sistem i tabanına , sistemi n güvenli k ayarların a v e a ğ bağlan - tısına bakılara k ingilizc e sözlükt e buluna n bütü n sözcükle r -şaşılaca k şek - "ide- otu z dakikada n a z bi r sür e içerisind e denenebilir !

Bu saldır ı sürerke n iva n başk a bi r bilgisayarda n geliştirm e grubunu n kullandığı diğe r sunuc u ola n ATMö'y a benze r bi r saldır ı başlattı . Yirm i dakika sonr a saldır ı yazılım ı hiçbi r şeyi n farkınd a olmaya n kullanıcıları n çoğunun olanaksı z olduğun u düşündüğ ü bi r iş i başardı . Yazılı m kul - lanıcılardan birinin , Yüzükleri n Efendis i kitabındak i Hobbitlerden birini n adı ola n "Frodo " kelimesin i parol a olara k kullandığın ı bulmuştu .

ivan, elind e b u parolayl a b u kullanıcını n hesabında n ATM 6 sunucusuna bağlandı .

Saldırganımız içi n he m iy i he m d e köt ü haberle r vardı . İy i haber , kırdığı hesabın , bi r sonrak i adımd a öneml i olaca k yönetic i özellikler i olmasıydı. Köt ü habe r is e oyunu n kayna k kod u hiçbi r yerd e yoktu . O zaman diğe r makinada , sözlü k saldırısın a karş ı dirençl i olduğun u anladığı ATM5't e olmalıydı . Am a ivan'ı n vazgeçmey e niyet i yoktu , den - emediği birka ç numaras ı dah a vardı .

Bazı Window s v e Uni x işleti m sistemlerind e şifrelenmi ş oarolalar , yüklü olduklar ı bilgisayar a erişim i ola n herkes e açıktır . Bunu n neden i şifreli parolaları n kınlamamas ı v e b u yüzde n korumay a gere k olma - masıdır. B u kura m yanlıştır . Yin e internett e bulunabile n pwdump 3 adl ı başka bi r araçl a İvan , ATM 6 makinasındak i şifrelenmi ş parolalar ı bulu p indirdi.

Tipik bi r şifrelenmi ş parol a dosyas ı aşağıdak i gibidir :

Administrator:500:95E4321A38AD8D6AB75EOC8D76954A50:
2E48927AOBO4F3BFB341E26F6D6E9A97:::

akasper:1110:5A8D7E9E3C3954F642C5C736306CBFEF:393C
E7F90A8357F157873D72D0490821: : :

digger:llll:5D15COD58DD216C525AD3B83FA6627C7:17AD
564144308B42B8403DOIAE256558: : :

ellgan:1112:2017D4A5D8D1383EFF17365FAFIFFE89:O7AEC9
50C22CBB9C2C734EB89320DB13: : :

tabeck:1115:9F5890B3FECCAB7EAAD3B435B51404EE:lFOl
5A728447212FCO5EID2D820B35B: : :

vkantar:1116:81A6A5DO35596E7DAAD3B435B51404EE;B93
3D36DD12258946FCC7BD153F1CD6E : ; :

vwallwick:1119:25904EC665BA30F4449AF42E1054F192:15B
2B7953FB632907455D2706A432469 : : :

mmcdonald:1121:A4AEDO98D29A3217AAD3B435B51404EE:
E40670F936B79C2ED522F5ECA9398A27 : : :

kworkman:1141:C5C598AF45768635AAD3B435B51404EE:DE
C8E827A121273EFO84CDBF5FD1925C : : :

İvan bilgisayarın a indirdiğ i şifrelenmi ş parolalara , başk a bi r ara ç kul - lanarak kab a kuvve t (brüte force) olara k biline n farkl ı bi r parol a saldırıs ı yaptı. B u tar z saldırıla r alfanümeri k karakterleri n v e çoğ u öze l simgeni n kombinasyonlarını dener .

ivan, L0phtcrack 3 adl ı bi r yazılı m kullandı , ("loft-kra k şeklind e okunur v e www.atstake.co m sitesind e bulunabilir ; baz ı mükemme l paro - la el e geçirm e araçlar ı içi n başk a bi r kayna k d a www.elcomsoft.co m 'dur.) Siste m yöneticiler i L0phtcrack 3 yazılımın ı zayı f parolalar ı denetle - mek için , saldırganla r is e parolalar ı kırma k içi n kullanırlar . LC 3 harf , say ı ve aralarınd a !@#$% A& gib i simgeleri n d e bulunduğ u karakte r kombi - nasyonlarıyla parolalar ı yokla r (Ancak , dikka t edilmelidi r ki , yazıcıda n bastırılamayacak karakterle r kullanıldığınd a LC 3 parolay ı bulmay ı başaramaz).

Programın neredeys e inanılmaz a yakı n bi r hız ı vardır . İşlemcis i 1 GHz ola n bi r makinad a hız ı saniyed e 2, 8 milyo n denemey e kada r çıka - bilmektedir. B u hızd a bile , eğe r siste m yöneticis i Window s işleti m siste - minde doğr u ayarlamalar ı yaptıys a (LANMA N şifrel i parolalarını n kul - lanılmasını ipta l etme k gibi) , bi r parolanı n kırılmas ı yin e d e oldukç a uzun bi r zama n alabilir .

Bu nedenl e saldırga n sı k sı k parol a dosyaların ı indiri r v e hede f şir - ketin ağın a bağl ı kalı p farkedilm e riskin i artırmaktans a saldırıy ı kend i bilgisayarında y a d a başk a bi r bilgisayard a yapar .

Terimler

KABA KUVVET SALDIRISI: Harfsayısal karakterlerin v e özel simgelerin mümkün olan her kombinasyonunu deneyen bir parola belir-

leme stratejisi.

İvan için , bekleyi ş o kada r uzu n sürmedi. Birka ç saa t sonra , kullandığ ı yazılım, geliştirm e ekib i üyelerini n he r birine ai t parolalar ı verdi . Am a bunla r ATM6 makinasını n kullanıcılarını n paro - lalarıydı v e iva n peşind e olduğ u kayna k kodlarının b u sunucud a olmadığın ı zaten biliyordu .

Şimdi n e olacaktı ? Dah a ATM 5 maki - nesinde buluna n bi r hesabı n parolası n bulmayı başaramamıştı . Bilgisaya r kor -

sanlarına özg ü düşünm e şeklin i kullanara k v e sırada n kullanıcıları n zayıf güvenli k alışkanlıkların ı anlamı ş bir i olarak , eki p üyelerinde n birinin he r ik i makin a içi n d e ayn ı parolay ı kullanıyo r olabileceğin i düşündü.

Tam tahmi n ettiğ i gibiydi . Eki p üyelerinde n bir i "oyuncular " ola n parolasını he m ATM5'd e he m d e ATM6'd a kullanıyordu .

Aradığı programlar ı bulabilmes i içi n kap ı ardın a kada r açılmıştı . Kaynak kod u klasörün ü buldukta n v e on u zevkl e indirdikte n sonr a sis - tem kıranlar a özg ü bi r adım dah a attı . İlerid e yazılımı n güncellenmi ş sürümünü alma k isteyebileceğin i düşünere k yönetic i haklar ı ola n am a kullanılmayan bi r hesabı n parolasın ı değiştirdi .

Aldatmacanın incelenmes i

Hem tekni k he m d e insa n kaynakl ı açıklarda n faydalana n b u saldırı - da saldırgan , tescill i bilgiler i tuta n geliştirm e sunucularını n adların ı v e yerlerini öğrenme k içi n saht e bi r telefo n görüşmes i yapmıştı .

Sonra, geliştirm e sunucusund a hesab ı ola n herkesi n geçerl i hesa p adlarını belirleme k içi n bi r yazılı m kullandı . Sonr a d a birbir i ardın a ik i parola saldırıs ı gerçekleştirdi . Bunları n arasında , bi r İngilizc e sözlükt e bulunan tü m kelimeler i deneyere k sıkç a kullanıla n parolalar ı araya n sözlük saldırıs ı d a vardı . Baze n b u sözlük , adlar , yerle r v e öze l ilg i alan - ları içere n pe k ço k başk a sözcü k listesiyl e desteklenebilir .

Hem ticar i he m d e halk a açı k korsanlı k araçları , akl a gele n herhan - gi bi r ama ç içi n kullanabilme k üzer e herke s tarafında n eld e edilebildik - lerinden, yatırımlarını z ola n bilgisaya r sistemlerin i v e a ğ altyapınız ı korurken uyanı k davranmanı z oldukç a önemlidir .

Bu tehlikeni n boyut u abartılmı ş değildir . Compute r VVorl d dergisin e göre, Ne w Yor k merkezl i Oppenheime r Fonları'nı n incelenmesinde n şaşırtıcı bi r bulg u eld e edilmiştir . Şirketi n A ğ Güvenliğinde n Soruml u Genel Müdü r Yardımcısı , standar t yazılı m paketler i kullanara k şirke t çalışanlarına bi r parol a saldırıs ı yapmıştır . Dergidek i yazıy a gör e ü ç dakika içerisind e 80 0 çalışanı n parolas ı kırılmıştır .

Mitnick Mesajı :

Monopol oyununun terimleri gibi, parolanız için sözlükten aldığınız bir kelime kul- lanırsanız sonuç, Hemen Hapse Git; Başlanmıştan Geçme, 200 Dolar Alma şek- linde olur. Çalışanlarınızı, varlıklarınızı gerçekten koruyacak parolalar seçmeleri konusunda eğitmelisiniz.

Aldatmacanın engellenmes i

Toplum mühendisliğ i saldırılar ı teknoloji k bi r unsu r eklendiğind e daha tehlikel i bi r ha l alabilmektedir . B u tar z bi r saldırıy ı engellemek , genellikle he m insa n boyutund a he m d e tekni k boyutt a önle m almay ı gerektirir.

Hayır demey i öğreni n •

Buradaki il k öyküd e telefon şirketini n RCMA C memuru , değişim i onaylayan hizme t emirler i yokke n o n telefon hattını n reddet-ke s duru - munu kaldırmamalıydı . Çalışanları n güvenli k kuralların ı v e süreçlerin i bilmeleri yeterl i değildir ; b u kuralların, zararı n oluşmasın ı engelleme k için n e kada r öneml i olduğun u d a anlamı ş olmalar ı gerekir .

Güvenlik kurallar ı süreçlerini n uygulanmas ı bi r ödül-cez a sistem i içerisinde teşvi k edilmelidir . Doğa l olara k kuralla r esne k olmal ı anca k göz ard ı edilm e olasılıklar ı yüksek , sorumlulu k gerektire n adımlar ı atm a işini çalışanlar a bırakmamalıdır . Ayrıc a bi r güvenli k bilinc i programı , güvenlik süreçlerini n çevresinde n dolaşa n kısayolla r kullanmanı n -he r ne kada r alına n işler i zamanınd a tamamlama k öneml i ols a da - şirke t v e çalışanlar içi n yıkıc ı olabileceğ i konusund a ikn a edic i olmalıdır .

Aynı dikka t telefond a yabanc ı birin e bilg i verirke n d e gösterilmelidir . Arayan kendin i n e kada r ikn a edic i bi r tarzd a tanıtırs a tanıtsın , şirkette - ki deneyiminde n v e konumunda n bağımsı z olarak , kimliğ i onaylanan a kadar, on a herkes e açı k olara k belirlenmi ş bilgile r dışınd a bilg i ver - ilmemelidir. Eğe r b u kural a sık ı bi r şekild e uyulsaydı , b u öyküd e geçe n toplum mühendisliğ i oyun u başarısı z olu r v e federa l tutukl u Gondorf f bi r daha arkadaş ı Johnny'l e birlikt e kimsey e yen i bi r oyu n oynayamazdı .

Şu husu s o kada r öneml i k i b u kitapt a bun u sürekl i yineliyorum : Kontrol, kontrol , kontrol . Yüzyüz e yapılmamı ş herhang i bi r istek , iste k sahibinin kimliğin i kontro l etmede n yerin e getirilmemelidir ; nokta .

Temizlik

Yirmi dör t saa t çalışa n güvenli k görevliler i olmaya n şirketle r içi n

saldırganın mesa i saatlerinde n sonr a ofis e girmes i cidd i bi r sorundu r Temizlikçiler, şirkette n gib i görünen v e bi r tuhaflı k görmedikler i herkes e çoğunlukla saygıyl a davranırlar . N e d e ols a b u kiş i onları n başın ı belay a sokabilecek y a d a onlar ı işte n attırabilece k biridir . B u yüzde n iste r şirke t elemanı olsunla r iste r taşero n bi r temizli k şirketinde n geliyo r olsunla ^ temizlik ekipler i fizikse l güvenli k konularınd a eğitilmelidirler .

Temizlik işini n üniversit e diplomas ı gerektirdiğ i söylenemez , hatt â ingilizce konuşmay ı bil e gerektirme z v e verile n eğitimler , eğe r vars s farklı işle r içi n n e tü r temizli k malzemeler i kullanılacağ ı gib i güvenli k e

ilgisi olmaya n konulard a olurlar . Genellikl e b u insanlar , "Eğe r mesa i saatleri dışınd a kendisin i içer i almanız ı isteye n bir i olursa , şirke t kimli k kartını göstermes i şarttır . Sonr a sizi n temizli k şirketin i arayıp , durum u anlatmanız v e karş ı tarafı n siz e izi n vermesin i beklemeni z gerekir" , gib i talimatlar almazlar .

Bir kuruluşu n -başın a gelmede n önce - b u bölümd e anlatıla n durum - lara karş ı hazırlıkl ı olmas ı v e çalışanların ı on a gör e eğitmes i gerekir . Gördüğüm kadarıyla , heps i olmas a da , öze l sektö r işletmelerini n çoğ u fiziksel güvenliği n b u boyut u konusund a fazlasıyl a gevşe k davranıyor - lar. Sorun a diğe r yönde n yaklaşı p sorumluluğ u şirketi n kend i çalışan - larına d a yükleyebilirsiniz . Yirm i dör t saa t güvenli k hizmet i olmaya n bi r şirket, mesa i saatler i dışınd a i ş yerin e gele n çalışanların a kend i anahtarlarını v e manyeti k giri ş kartların ı getirmelerin i şar t koşabilir . Temizlik görevlilerin e hiçbi r zama n birin i içer i almamalar ı konusund a kesin talimatla r verebilir . Temizli k şirketin e d e içeriy e kimsey i alma - maları konusund a çalışanlarını n he r zama n eğitiml i olmalar ı gerektiğin i hatırlatabilirsiniz. Ş u basi t bi r kuraldır : Kapıy ı kimsey e açmayın . Eğe r b u uygunsa, temizli k şirket i sözleşmesini n maddelerinde n bir i olara k yazıya dökülebilir .

Temizlik ekipler i ayn ı zamand a birini n arkasında n geçm e teknikleriyle ilgil i d e eğitilmelidirler . Ayrıc a birinin , bi r şirke t çalışanın a benziyor diye , heme n peşlerinde n binay a girmey e çalışmasın a izi n ver - meyecek şekild e d e bilgilendirilmeliler .

Arada bi r -örneği n yıld a ü ç y a d a dör t kere - içer i girm e testler i v e açıklık değerlendirmeler i yapın . Temizli k ekib i çalışırke n kapıy a birin i gönderin v e o kiş i temizlikçiler i ikn a edere k içer i girmey e çalışsın . B u i ş için kend i çalışanlarınız ı kullanmaktans a b u tar z içer i girm e testlerind e uzmanlaşmış şirketlerl e çalışmay ı terci h edin .

Kulaktan kulağa : Parolalarınız ı gizl i tutu n

Giderek dah a ço k şirke t tekni k yöntemler e dayana n güvenli k kural - larını uygulamay a geçiriyor . Örneğin , parol a kuralların ı denetleyece k şekilde işleti m sistem i ayarlanabili r v e hesab ı kilitlemede n önc e başarısız parol a giri ş denemelerini n sayıs ı sınırlandırılabilir . Aslınd a Microsoft VVİndovvs'u n işletmeler e yöneli k sürü m paketlerin e b u özelli k genellikle mevcuttur . Anca k dah a fazt e çab a gerektire n özelliklerde n müşterilerin n e kada r çabu k sıkıldığ ı görülünce , ürünle r güvenli k ayarları kapal ı olara k sunulmay a başlandı . Yazılı m şirketlerini n -ta m tersi olmas ı gerekirken - ürünlerin i güvenli k ayarlar ı kapatılmı ş olara k teslim etmey i durdurmasını n ta m zamanıymı ş gib i görünüyor . (Sanırı m yakında bun u kendiler i d e anlayacaklar.)

Şirket güvenli k kurallarının , kola y yanılabile n insanlar a gereğinde n fazla be l bağlamama k amacıyla , mümkü n olduğunc a teknoloji k güven -

lik unsurların ı uygulamalar ı konusund a siste m yöneticilerin e dayatmad a bulunması so n derec e doğaldır . Örneği n belirl i bi r hesapt a birbir i ardın a yapılan başarısı z giri ş denemelerini n sayısın ı sınırlamanı n bi r saldır - ganın işin i oldukç a zorlaştıracağın ı görme k ço k fazl a kaf a yormay ı gerektirmez.

Her kuruluş , sağla m güvenli k v e çalışa n üretkenliğ i arasındak i has - sas dengey i koruma k zorundadır . Bu , baz ı çalışanları n güvenliğ i hiç e saymalarına, alma n önlemleri n hassa s şirke t bilgilerin i korumad a n e kadar öneml i olduğun u görememelerin e nede n olur .

Eğer şirke t kurallarını n değinmediğ i baz ı konula r varsa , çalışanlar en a z zorlu k çekecekler i yoldan , işlerin i kolaylaştıraca k e n uygu n hareketi yapara k görevlerin i yerin e getirebilirler . Baz ı çalışanla r değişime diren ç gösterebili r ve doğr u güvenli k alışkanlıkların ı açı k açı k hiçe sayabilir . Basi t olmaya n v e uzu n parol a kuralların a uya n am a sonr a da parolasın ı bi r no t kâğıdın a yazı p meyda n okurcasın a bilgisayarını n ekranına yapıştıra n çalışanlarl a karşılaşmışsınızdır .

Şirketinizi korumanı n e n etkil i yollarında n biri , tekni k altyapınızda , güçlü güvenli k ayarlarını n yan ı sır a keşfedilmes i zo r parolala r kullan - maktır.

Parola kurallarıyl a ilgil i ayrıntıl ı değerlendirmeler i 16 . bölümd e bula - bilirsiniz.

İŞE YEN İ GİRENLER E SALDIRILA R

Burada anlatıla n öyküleri n çoğunu n d a gösterdiği gib i becerikl i bi r toplum mühendis i çoğunlukl a kuru m iç i yetk i sıralamasınd a al t seviyed e olan çalışanlar ı hedefler . B u insanları , hassa s şirke t bilgilerin e saldır - ganı bi r adım dah a yaklaştıracak , zararsı z gib i görüne n bilgiler i ver - meleri doğrultusund a yönlendirme k kolaydır .

Bir saldırganı n iş e yen i başlamı ş çalışanlar a saldırmasını n nedeni , onların çoğ u zama n belirl i şirke t bilgilerini n y a d a baz ı hareketleri n olas ı sonuçlarının farkınd a olmamalarıdır . Ayrıc a e n biline n toplu m mühendis - liği tekniklerinde n bazılarıyl a kolayc a etk i altın a girm e eğilimindedirler ; yetkili kiş i izlenim i uyandıra n biri , arkada ş canlıs ı v e sevimli dura n biri , şirkette kurbanı n d a tanıdığ ı kişiler i tanıya n biri , saldırganı n isteklerini n çok aci l olduğuyl a ilgil i bi r tale p y a d a kurbanı n bi r yardı m göreceğin e y a da göz e gireceğin e yöneli k edindiğ i bi r kan ı gibi .

Şimdi d e i ş başındak i al t seviy e çalışanlar a yapıla n saldırılar a baz ı örnekler verelim .

Yardımsever Güvenli k Görevlis i

Dolandırıcılar açgözl ü birin i bulmay a çalışırla r çünk ü dolandırılm a olasılıkları yükse k olanla r onlardır . Toplu m mühendisler i temizli k ekibinden y a d a güvenli k görevlilerinde n birin i seçerke n iy i huylu , arkadaş canlıs ı v e güvenili r birin i bulmay ı umarlar . Çünk ü e n büyü k olasılıkla yardı m etmey i isteyebilecekle r onlardır . Aşağıda anlatıla n öyküde saldırganı n aklında n geçe n d e ta m böyl e bi r şeydir .

Elliot'un Bakı ş Açıs ı • . .. ,

Gün/Saat: Şuba t 1998 , Salı , saba h 03:26 .

Yer: Marchan d Mikrosistemle r tesisi , Nashua-Ne w Hampshir e

Elliot Stanle y saa t baş ı çıkmas ı gereke n devriyele r dışınd a yerinde n ayrılmaması gerektiğin i biliyordu . Am a geceni n bi r yans ı olmuşt u v e mesaisi başladığında n ber i te k bi r kiş i bil e görmemişti . Telefondak i zavallı adamı n ses i gerçekte n yardım a ihtiyac ı varmı ş gib i geliyordu . V e birilerine küçü k bi r iyili k yapma k insanı n he r zama n kendin i dah a iy i his - setmesini sağlıyordu .

'in Öyküs ü

Bili Goodrock'u n ço k basit , hi ç değişmede n o n ik i yaşında n ber i bağ - landığı te k bi r amac ı vardı : Yirm i dör t yaşın a gelmede n v e kend i birikim - lerinin te k kuruşun a dokunmada n emekl i olmak . Kend i başın a d a başarılı olabileceğini , he r şey e kadir , huysu z babasın a gösterecekti .

İki yı l kalmışt ı v e gelece k yirm i dör t ayd a başarıl ı bi r i ş adam ı v e zek i bir yatırımc ı olara k zengi n olamayacağ ı oldukç a açıktı . Bi r ar a silahl a banka soymay ı d a düşünmü ş am a bunu n hikâyelerd e kalmas ı gerek - tiğine v e tehlike-kazan ç dengesini n berba t olduğun a kara r vermişti . Onun yerine , Rifki n gibi , bi r bankay ı elektroni k olara k soymanı n hayal - lerini kuruyordu .

Bili e n so n ailesiyl e birlikt e Avrupa'y a gittiğind e Monaco'd a 10 0 franklık bi r bank a hesab ı açtırdı . Yü z fran k orad a duruyord u am a o paranın bi r and a yed i basamakl ı olmasın ı sağlayaca k bi r plan ı vardı . Eğer şans ı yave r giders e b u mikta r seki z basamakl ı bil e olabilirdi .

BiH'in kı z arkadaş ı Annemari e büyü k bi r Bosto n bankasınd a birleşm e ve devirle r bölümünd e çalışıyordu . Bi r gü n kı z arkadaşını n ofisinde , onu n geç saatler e kalmı ş bi r toplantıda n çıkmasın ı beklerken , merakın ı yene - medi v e kend i dizüst ü bilgisayarını , içind e beklediğ i konferan s salonun - daki etherne t girişin e bağladı , işte ! Dahil i ağa , bankanı n ağın a bağlan - mıştı... he m d e güvenli k duvarını n arkasından . Aklın a bi r fikir.geldi .

Başarılı bi r bilgisaya r mühendisliğ i doktoras ı yapmakt a ola n v e Marchand Microsystems'd a sta j yapa n Juli a adınd a gen ç bi r kadın ı tanıyan bi r sını f arkadaşıyl a yeteneklerin i bi r aray a getirdiler . Juli a içer - den öneml i bilgile r edinme k içi n iy i bi r kayna k gib i görünüyordu . Kadın a bir fil m senaryos u yazdıkların ı söyledile r v e Juli a onlar a inandı . Onlarl a bir öyk ü yazmanı n eğlencel i olduğun u düşünüyord u v e anlattıklar ı dümenin nası l çevrileceğiyl e ilgil i tü m ayrıntılar ı onlar a anlattı . Fikri n ço k iyi olduğun u düşünüyo r v e fil m yazılarınd a adını n geçmes i içi n sürekl i kafalarını ütülüyordu . On u senaryoları n nası l sı k sı k çalındığıyl a ilgil i uyardılar v e bunlar ı kimsey i anlatmamas ı içi n yemi n ettirdiler .

Julia tarafında n iy i yetiştirilmi ş olara k işi n tehlikel i kısmın ı Bil i kend i yaptı v e iş i kotarabileceğinde n hi ç kuşk u duymadı . Kend i ağzında n dinleyelim:

Öğleden sonr a telefo n etti m v e gec e güvenli k amirini n adını n isaia h Adams olduğun u öğrenmey i başardım . Gec e 21:30'd a binay ı aradı m v e giriş güvenli k masasınd a dura n bekçiyl e konuştum . Hikâye m tamame n aciliyete dayalıyd ı v e bira z telaş a kapılmı ş gib i konuştum . "Arabaml a ilgili bi r soru n çıkt ı v e tesis e gelemiyorum " dedim . "Aci l bi r duru m va r v e gerçekten yardım a ihtiyacı m var . Güvenli k amir i isaiah' ı aramay ı dene - dim am a evd e değil . Ban a bi r kereli k yardımc ı olabili r misiniz , ço k mak - bule geçecek. "

İşe Yen i Girenler e Saldırıla r 18 3

Geniş tesistek i odaları n he r bir i numaralıydı , böylec e adam a bilgisa - yar laboratuvarını n numarasın ı verdi m v e yerin i bili p bilmediğin i sor - dum. Bildiğin i söyled i v e beni m içi n oray a gitmey i kabu l etti . Oday a gitmesi birka ç dakikasın ı alacaktı . Te k bi r telefo n hattı m olduğun u v e onu d a sorun u çözme k içi n ağ a bağlanmakt a kullandığı m gib i bi r baha - neyi ön e sürere k on u laboratuvarda n arayacağım ı söyledim .

Aradığımda oray a varmı ş ben i bekliyordu . On a üzerind e "elmer " yazan bi r etike t ola n uçbirim i nered e bulacağın ı açıkladım . Bu , Julia'nı n anlattığına göre , şirketi n pazarladığ ı işleti m sistemlerini n piyas a sürüm - lerinin yapıldığ ı an a bilgisayardı . Bekç i bilgisayar ı bulduğun u söylediğinde Julia'nı n biz e doğr u bilg i verdiğin i anladı m v e içi m bi r ho ş oldu. Birka ç ker e Ente r tuşun a basmasın ı söyledim , o d a ban a ekran a pound (£) işaretlerini n çıktığın ı söyledi . B u bilgisayar a kö k hesaptan , yani tü m siste m yetkilerini n olduğ u süper-kullanıc ı hesabında n girildiği - ni gösteriyordu . Bekçi , klavyed e te k parma k yazıyord u v e be n ona , bira z zorlu ola n bi r sonrak i komut u söylerke n ka n te r içind e kaldı .

echo 'fix'.x:0:0::/:/bin/sh ' > > /etc/passw d

Sonunda doğr u girmey i başard ı v e böylec e hesaplarda n birini n adın ı değiştirdik. Sonr a on a ş u komut u girmesin i söyledim :

echo 'fix : : 10300;0:0 ' 5 5 /etc/shado w

Bu komut , ik i nokt a üs t üsteleri n arasındak i şifrel i parolay ı oluşturdu , iki nokt a üstüsteleri n arasın a hiçbi r şe y koymama k parolanı n olmaya - cağı anlamın a gelir . B u yüzden , hesaptak i düzeltmey i bo ş bi r parol a kul - lanarak parol a dosyasın a ekleme k içi n b u ik i komu t yetmişti . Dah a d a iyisi, b u hesa p d a süper-kullanıc ı yetkilerin e sahi p olacaktı .

Bunun ardında n onda n yapmasın ı istediği m şey , dosy a adlarını n uzun bi r listesin i çıkara n tekrarlana n bi r dizi n komut u oldu . Sonr a kâğıd ı ileri doğr u beslemesini , yırtmasın ı v e yanın a alı p bekç i kulübesin e dön - mesini söyledim , çünk ü dah a sonr a orada n ban a birşeyle r okumasın ı isteyebilirdim.

işin güze l yan ı bekçini n yen i bi r hesa p açtığında n haber i yoktu . On a dizinlere gör e dosy a adların ı bastırtmıştım , çünk ü dah a önc e yazdığ ı

NOT t Burada kullanılan arka kapı, işletim sistemi giriş programını değiştiren türden değil. Daha doğrusu giriş programının kullandığı dinamik kitaplıktaki belirli bir işlev, gizli bir giriş noktasını yaratacak şe- kilde değiştiriliyor. Sıradan saldırılarda saldırganlar çoğunlukla ya giriş programını değiştirirler ya da doğrudan ona yama yaparlar ama dikkatli sistem yöneticileri programı yükleme cd'sinde ya da başka dağıtım ortam- larında bulunan şekliyle karşılaştırarak değişikliği fark edebilirler.

komutların bilgisaya r odasında n onunla

birlikte çıkmasın ı istiyordum . Böylec e sis -

tem yöneticis i y a d a işletmen i ertes i

YAMA: Çalıştırılabilir bir

sabah bi r güvenli k ihlal i olduğun a dai r programa yerleştirildiğinde,

hiçbir şe y far k etmeyecekti .

var olan sorunu çözen bir

program parçacığı.

Artık bi r hesabım , parola m v e ta m

yetkim vardı . Geceyarısında n a z önc e

sisteme telefonl a bağlandı m v e Julia'nı n "film senaryos u için " özenl e yazdığ ı komutlar ı girmey e başladım . Gö z açıp kapayıncay a kada r şirketi n işleti m sistem i yazılımını n yen i sürümü - nün kayna k kodunu n an a kopyasını n durduğ u geliştirm e sistemin e erişmiştim.

Julia'nın yazdığ ı v e işleti m sistem i kitaplıklarında n birindek i bi r alt - programı değiştirdiğin i söylediğ i yamay ı yükledim . Aslınd a b u yama , sis - teme gizl i bi r parol a kullanara k uzakta n erişi m sağlayaca k bi r ark a kap ı oluşturuyordu.

Julia'nın beni m içi n yazdığ ı talimatlar ı özenl e uygulayarak , önc e yamayı yükledim ; sonr a da , yaptıklarımda n geriy e hiçbi r i z kalmayaca k şekilde düzeltm e hesabın ı kaldıra n v e tü m denetlem e günlüklerin i tertemiz ede n adımla r atı p etkil i bi r şekild e izlerim i yokettim .

Yakında şirke t yen i işleti m sistem i güncellemelerini , düny a çapınd a finansal kuruluşla r ola n müşterilerin e göndermey e başlayacaktı . V e gönderdikleri he r kopya , gönderilmede n önc e an a dağıtı m sürümün e yerleştirdiğim ark a kapıy ı içerecekti . Böylec e güncellemey i yükleye n he r bankanın v e menku l değerle r şirketini n bilgisaya r sistemin e erişmem i sağlayacaktı.

Henüz ta m olara k hedefim e varmamıştım , yapaca k dah a ço k işi m vardı. "Ziyaret " etme k istediği m he r finansa l kurumu n dahil i ağın a girmem gerekiyordu . Sonr a hang i bilgisayarların ı par a havaleler i içi n kullandıklarını bulma m v e yaptıklar ı işlemleri n ayrıntıların ı v e paray ı ta m olarak nası l haval e ettiklerin i öğrenebilme k içi n gözetlem e yazılımlar ı yüklemem gerekecekti .

Bunları tümün ü uzaktan , herhang i bi r yerdek i bi r bilgisayarda n yapa - bilirdim. Örneği n bi r deni z kıyısından . Bekl e ben i Tahiti , geliyorum .

Yeniden bekçiy i aradım , yardımlar ı içi n teşekkü r etti m v e on a dökümü çöp e atabileceğin i söyledim .

Güvenlik görevlisini n görevleriyl e ilgil i aldığ ı talimatla r vard ı am a n e kadar ayrıntıl ı v e iy i düşünülmü ş d e olsala r b u talimatla r he r olas ı durum u öngörmüyordu. Şirke t çalışan ı olduğun u düşündüğ ü bir i içi n bi r bilgisayar a

işe Yen i Girenler e Saldırıla r 18 5

Mitnick Mesajı :

Bir saldırgan bir bilgisayar sistemine ya da ağına İçendi ulaşamıyorsa, bunu yap- ması için başka birisini bulmaya çalışacaktır. Planın yürümesi için fiziksel giriş- lerin zorunlu olduğu durumlarda kurbanı aracı olarak kullanmak, işi kendisinin yapmasından daha iyi bile olabilir, çünkü saldırgan böylece farkedilme ve yakalan- ma tehlikesini oldukça azaltabilir.

oirkaç komu t girmesini n yaratabileceğ i zararda n kims e on a sö z etmemişti .

Her n e kada r güvenl i bi r laboratuvarı n kilitl i kapısını n arkasınd a d a olsa, bekçini n d e işbirliğiyle , dağıtı m kopyasınını n saklandığ ı kriti k sis - teme erişi m oldukç a kola y olmuştu . Bekçini n elinde , doğa l olarak , tü m kilitli kapıları n anahtarlar ı vardı .

Aslında dürüs t ola n bi r çalışa n bil e (hikâyemizd e doktor a öğrencis i ve şirke t stajyer i ola n Julia) bi r toplu m mühendisliğ i saldırıs ı içi n ca n alıcı önem e sahi p bilgiler i vermes i içi n kandırılabiliry a d a bun u yapmas ı için on a par a yedirilebilir . Örneği n hede f bilgisaya r sistemini n nered e olduğu v e -b u saldırını n başarıs ı içi n ço k öneml i olan - yazılımı n yen i sürümünün n e zama n dağıtım a çıkacağ ı gib i bilgiler i verebilirler , işleti m sisteminin temi z bi r kaynakta n yenide n yapılandırıldığ ı durumda , b u tar z bir değişikliği n ço k erke n yapılması , far k edilm e y a d a geçersi z olm a tehlikesini getirdiğ i içi n zaman ı bilme k önemlidir .

Bekçinin çıktıy ı giriştek i masasın a götürmesin i sağlamanın , sonr a d a onu orad a çöp e attırmanı n altındak i neden i görebildini z mi ? B u öneml i bi r adımdı. Bi r sonrak i i ş gününd e bilgisaya r işletmenler i iş e geldiklerinde , saldırgan, çıkt ı alm a uçbirimind e y a d a laboratuvarı n çöpünd e onları n b u kanıtı görmelerin i istemiyordu . Bekçiy e akl a yatkı n bi r açıklam a yapara k dökümü yanınd a götürmesin i sağlamas ı b u riskte n kurtulmasın a yetmişti .

Acil Yam a

Teknik deste k birimind e çalışa n birini n dışarda n birin e bilgisaya r ağına giri ş hakk ı tanımanı n doğuracağ ı sakıncaları n bilincind e olmasın ı beklersiniz. Anca k b u dışarda n biri , yardımseve r bi r yazılı m satıcıs ı gib i davranan akıll ı bi r toplu m mühendis i ise , sonuçla r pe k beklediğini z gib i çıkmayabilir.

Faydalı Bi r Telefo n Görüşmes i - ; ' ' • \ •

Arayan, orad a bilgisayarlarda n kimi n soruml u olduğun u bilme k isti - yordu v e santra l memur u on u tekni k deste k sorumlus u Pau l Ahearn' a bağladı.

Arayan, kendin i Edwar d olara k tanıtarak , veritaban ı satıcıs ı SeerVVare'dan aradığın ı söyledi . "Görünüş e gör e baz ı müşterilerimi z acil güncellemeyl e ilgil i e-postamız ı almamışlar , b u yüzde n yamanı n yüklenmesinde soru n çıkı p çıkmadığın ı kontro l etme k içi n bazıların ı arıyoruz. Yen i güncellemey i yükleyebildini z mi? "

Paul öyl e birşe y görmediğinde n oldukç a emi n olduğun u söyledi .

Edvvard, "Progra m zama n zama n büyü k ver i kayıpların a nede n olabilir , bu nedenl e e n kıs a süred e yüklemeniz i öneririz " dedi . "Evet " ded i Paul , b u kesinlikle yapma k isteyeceğ i bi r şe y olurdu . "Tamam " diy e karşılı k verd i arayan. "Siz e yamay ı bi r ban t y a d a CD'y e yüklenmi ş olara k gönderebiliri z ve şun u d a ekleme k isteri m k i b u gerçekte n öneml i çünk ü ik i şirket , şimdi - den pe k ço k gün e ai t verilerin i kaybettiler . B u yüzden , b u ola y sizi n d e başınıza gelmeden , eliniz e geçe r geçme z yamay ı yüklenmelisiniz. "

"internet sitenizde n indirme m mümkü n değ i l mi? " diy e sord u Paul .

* "Yakınd a hazı r olacağın ı sanıyorum ; tekni k eki p hasar ı düzeltmey e çalışmakla meşgul . İsterseni z müşter i deste k hizmetlerini n yamay ı uzaktan yüklemesin i sağlayabiliriz . Sisteminiz e bağlanma k içi n telefo n hattını kullanabili r y a da , destekliyorsanız , Telnef i deneyebiliriz. "

"Özellikle internette n Telnet' e izi n vermiyoruz ; güvenl i değil " diy e karşılık verd i Paul . "Eğe r SS H kullanabilirseniz , b u olabilir" .

"Evet, SSH'imi z var . İ P adresini z nedir? "

Paul on a İ P adresin i verd i v e Edvvar d hang i kullanıc ı adın ı v e paro - layı kullanabileceğin i sordu . Pau l on a b u bilgiler i d e verdi .

Aldatmacanın incelenmes i

Bu telefo n gerçekte n d e veritaban ı üreticisinde n gelmi ş olabilirdi . Ancak o zama n b u öyk ü b u kitapt a ye r almazdı .

Topjum mühendis i kriti k verileri n yo k olabileceğ i gib i bi r kork u uyandırarak kurbanın ı etkiled i v e sorun u halledece k hızl ı bi r çözü m önerdi .

Ayrıca bi r toplu m mühendisinin , bilgini n değerin i bile n birin i hedef - lediği zaman , uzakta n erişi m eld e edebilme k içi n ço k inandırıc ı v e ikn a edici nedenle r bulmas ı gerekir . Baze n işi n için e aciliye t katara k kur - banını hızl ı hareke t etmey e zorlayı p konuy u fazl a düşünmesin e izi n ver - meden isteğin i kabu l etmesin i sağlar .

Bir saldırgan , şirketinizi n dosyalarınd a dura n hang i tü r bilgiy e ulaş - mak isteyebilir ? Baze n hi ç korumay a ihtiyacını z olmadığın ı düşündü - günüz bi r şe y olabilir .

işe Yen i Girenler e Saldırıla r 18 7

Kara h 'y.q _ G e 1 e n T e I e l o n

- İnsan Kaynakları, ben Sarah.

- Merhaba Sarah. Ben George, şirket otoparkında görevliyim. Asansörlere binmek ve otoparka girmek için kullandığınız erişim kart- larını hatırlıyor musun? Bir sorun çıktı ve son on beş gün içinde yeni girenler için açtığımız bütün kartları yeniden programlamamı: gerekiyor.

- Adlarına mı ihtiyacınız var?

- Ve telefon numaralarına.

- Yeni işe alınanlar listesine bakıp seni geri arayabilirim. Tele]on numaran nedir?

- 73... Ah, az sonra kahve molasına çıkacağım, yarım saat sonr ı ben seni arasam nasıl olur?

- Tamam, olur.

Adam ger i aradığında , kız~ .

- Evet, yalnızca iki kişi var. Finans bölümünden Anna Myrtle, sekreter, v e yeni genel müdür yardımcısı Bay Undenvood, dedi . - Telefon numaraları?

- Evet, tamam. Bay Undenvood 6973. Anna Myrtle. 2127.

- Çok yardımcı oldun, teşekkürler.

Anna'ya Gele n Telefo n

- Finans bölümü, Anna'yla görüşüyorsunuz.

- Geç saatlere kadar çalışan birini bulabildiğim için çok memnunum. Ben Ron Vittaro. Ticaret bölümünün ağ sorumlusuyum. Sanırım henvz tanıştırılmadık. Şirkete hoşgeldin.

- Teşekkür ederim.

- Anna, Los Angeles'tayım ve bir krizi çözmeye çalışıyorum. Bana ayırabileceğin bir on dakikan var mı?

- Elbette. Ne yapmam gerekiyor?

- Ofisime çık. Nerede olduğunu biliyor musun?

- Hayır.

- Peki, on beşinci katta köşedeki oda; oda numarası 1502. Birkaç dakika içinde seni oradan ararım.

Ofise gittiğinde aramamın doğru- dan sesli mesaja bağlanmaması için ileri tuşuna basman gerekecek.
- Tamam, şimdi gidiyorum.

On dakik a sonr a Ron'u n odasın a varmış , aram a aktarm a işlevin i ipta l etmiş bekliyord u k i telefo n çaldı . Adam , kız a oturmasın ı v e interne t tarayıcısını çalıştırmasın ı söyledi . Açıldığınd a yazması içi n www.geoc - ities.com/ron-insen/eser.doc.exe adresin i verdi .

Bir iletişi m kutus u çıkt ı v e ada m "Aç " düğmesin i tıklamasın ı söyledi . Bilgisayar yazıy ı indiriyormu ş gib i gözükt ü am a sonr a ekra n karardı . Anna birşeyleri n ter s gidiyo r gib i göründüğün ü söylediğind e adam karşılık verdi :

- Ah, hayır. Sürekli o web sitesinden bir şeyler indirmekte güçlük çekiyorum ama düzeltildiğini sanmıştım. Peki, boş ver o zaman, dosyayı daha sonra başka bir şekilde indiririm.

Oluşan sorunda n sonr a bilgisayarını n düzgü n çalışı p çalışmadığında n emin olma k içi n Anna'da n bilgisayarın ı yenide n başlatmasın ı istedi . Yeniden başlatmas ı içi n gerekl i adımlar ı kız a anlattı .

Bilgisayar yenide n düzgü n bi r şekild e çalışmay a başladığında , on a içtenlikle teşekkü r ett i v e telefon u kapattı . Ann a üzerind e çalıştığ ı iş i bitirmek içi n fman s bölümün e ger i döndü .

Kurt Dillon'u n Öyküs ü

Millard-Fenton yayıncılık , i ş yapma k üzer e olduklar ı yen i yazarlar ı konusunda oldukç a heyecanlıydılar . B u yazar , bi r Fortun e 50 0 şirke - tinin, anlataca k ilgin ç öyküler i ola n emekl i gene l müdürüydü . Biri , görüşmeleri ayarlamas ı içi n adam ı bi r yaza r manajerin e yönlendirmişti . Menajer, yayınev i sözleşmelerini n nası l yapıldığıyl a ilgil i hiçbi r şe y

bilmediğini itira f etme k istemiyordu ; b u

nedenle, bilmes i gerekenler i öğrenme -

sine yardımc ı olmas ı içi n esk i bi r arka -

daşını tutmuştu . B u esk i arkadaş , n e

CASUS YAZILIM: Hedefin

yazık ki , pe k iy i bi r seçi m değildi . Kur t

bilgisayar faaliyetlerini

Dillon araştırmalarınd a olağandış ı ola -

gizlice izlemesi için özel

rak adlandırabileceğimiz , pe k d e eti k

olarak yapılmış program.

olmayan yöntemle r kullanırdı .

Bunun bir çeşidi de,

çevrimiçi reklamların inter-

Kurt, Ro n Vittar o adıyl a Geocities'de n

nette gezinme alışkanlık-

ücretsiz bi r sit e ald ı v e yen i sitey e bi r larına göre tasarlanabilme-

casus yazılı m yükledi . Yazılımı n adın ı si için internetten alışveriş

eser.doc.exe olara k değiştirdi , böylec e

dosya bi r Wor d belges i olara k gözükece k

edenlerin ziyaret ettikleri

ve kuşk u uyandırmayacaktı . Aslınd a işle r siteleri takip etmek için kul-

Kurt'un beklediğinde n dah a iy i yürümüştü , lanılır. Yazılım, kullanıcının,

çünkü gerçe k Vittaro , Windo w s işleti m sis - aralarında girilen parolalar

temindeki "Biline n dosy a türler i içi n dosy a

ve klavyeden yazdığı

uzantılarını gizle " seçeneğini n varsayıla r

yazılar, e-postalar, soh-

ayarını hi ç değiştirmemişti . B u aya r yü -

betler, anında mesajlar,

zünden dosyanı n ad ı zate n eser.doc ziyaret edilen tüm ağ say-

olarak çıkmıştı .

faları ve ekran resimleri

olan tüm faaliyetlerini Sonra hanı m arkadaşlarında n birini n

yakalar. Vittaro'nun sekreterin i aramasın ı sağ -

işe Yen i Girenler e Saldırıla r 18 9

ladı. Dillon'u n yönlendirmeleriyl e kadı n Vittaro'nun sekreteriyl e konuştu . "Ultimat e Kitabevleri, Toronto'nu n başkan ı Pau l Spadone'un yönetic i asistanıyım . Ba y Vittaro patronuml a bi r sür e önc e bi r kita p fuarında tanışmı ş v e orta k yürütülebile - cek bi r projeyl e ilgil i konuşma k içi n ara - masını istemiş . Ba y Spadon e sürekl i seyahatlerde, b u yüzde n bende n Ba y Vittaro'nun n e zama n ofisind e olacağın ı öğrenmemi istedi. "

SESSİZ YÜKLEME: Bilgisayar kullanıcısının ya

da işletmeninin fark

etmeyeceği şekilde bir yazdım uygulaması yükleme

yöntemi.

İkisi ajandalar ı karşılaştırmay ı bitirdiklerinde , Kurt'u n baya n arkadaş ı Bay Vittaro'nu n ofisind e olacağ ı tarihlerl e ilgil i saldırgan a yeterinc e bilg i sağlamıştı. B u ayn ı zamand a Vittaro'nu n yerind e olmayacağ ı tarihler i d e bildirdiği anlamın a geliyordu . Vittaro'nu n sekreterini n d e onu n yokluğun - dan faydalanı p bira z kaya k yapmay a gideceğin i öğrenme k içi n d e uzu n uzun sohbe t etmes i gerekmemişti . Kıs a bi r sür e içi n ikis i d e ofist e olma - yacaklardı. Mükemmel .

ikisinin birde n olmadıklar ı il k gün , emi n olma k içi n uyduruk , aci l bi r mesajla telefo n ettiğind e danışm a görevlis i ona , "Ba y Vittar o ofisind e değil, sekreter i d e bugü n yok . ikis i d e bugün , yarı n v e sonrak i gü n bura - da olmayacaklar " dedi .

Yeni bi r çalışan ı oyunun a ale t etm e konusund a il k denemesind e başarılı olmuşt u v e aslınd a herkesç e bilinen, ticar i olara k bulunabile n v e saldırganın sessi z yüklem e içi n üzerind e oynadığ ı bi r casu s yazılı m olan bi r "eseri " indirmesin i istediğind e kı z gözün ü kırpmada n indirmişti . Sessiz yüklem e yöntemiyl e kurulum hiçbi r virü s korum a yazılım ı tarafın - dan farkedilmez . Tuha f bi r nedende n ötür ü virü s korum a programlar ı yapan üreticile r halihazırd a varola n casu s yazılımlar ı bulaca k bi r ürün ü pazara sürmüyorlar .

Genç kadının , yazılım ı Vittaro'nu n bilgisayarın a yüklemesini n heme n ardından, Kurt , Geocitie s sitesin e ger i gitt i v e doc.ex e dosyasın ı inter - nette bulduğ u bi r kitapl a değiştirdi . Biriler i oyun u farkede r v e n e olduğun u anlamak içi n sitey e geli p bakaca k olurlars a tü m bulabilecekler i zararsız , acemice yazılmış , basılama z bi r kita p metninde n ibare t olacaktı.

Program, yüklendikte n v e bilgisaya r yenide n başlatıldıkta n sonr a hemen hareket e geçme k üzer e ayarlanmıştı . Ro n Vittar o birka ç gü n içinde dönecek , iş e başlayaca k v e casu s yazılı m klavyede n bilgisayarı - na girdiğ i he r şeyi , gönderdiğ i e-postalar ı v e o and a ekranında n gördük - lerinin bi r resmin i on a iletecekti . Heps i düzenl i aralıklarl a Ukrayna'dak i ücretsiz elektroni k post a hizmet i vere n bi r sitey e gönderilecekti .

I

Vittaro'nun dönüşünde n birka ç gü n sonr a Kurt , Ukrayna'dak i post a kutusuna birikmi ş günlü k

dosyaların ı karıştırıyord u v e ço k geçmede n

Millard-Fenton Yayıncılığı n o yazarl a anlaşma k içi n ta m olara k nerey e kadar gitme k istediğin i anlata n gizl i e-postala r buldu . B u bilgiyl e dona - narak yazarı n menajerini n anlaşmay ı bütünüyl e kaybetme risk i oluş - madan, il k tekli f edilende n ço k dah a iy i koşulla r içi n pazarlı k etmes i kolay olacaktı . B u d a doğa l olara k menaje r içi n dah a dolgu n bi r komis - yon anlamın a geliyordu .

Aldatmacanın İncelenmes i

Bu oyund a saldırgan , arac ı olara k yen i bi r çalışa n seçerek , onu n işbirliği yapm a v e iy i birtakı m oyuncus u olm a isteğin e güvend i v e başar ı şansını artırdı . Yen i elemanı n şirket , çalışanlar v e dalaver e teşeb - büsünü aksataca k güvenli k uygulamalar ı konusund a dah a a z bilgil i olma olasılığ ı vardı .

Kurt, finan s bölümünd e bi r memu r ola n Anna'yl a görüşmesind e genel müdü r yardımcıs ı gib i davrandığ ı için , kızın , kendisini n yetkisin i sorgulama olasılığını n ço k düşü k olduğun u biliyordu . Aksine , bi r gene l müdür yardımcısın a hizme t edere k göz e girebileceğin i d e düşünebilirdi .

Anna'ya adım adı m anlattığı , casu s yazılı m kurmay a yöneli k süre ç dışarıdan bakıldığınd a zararsı z görünüyordu . Anna'nın , zararsı z gib i görü - nen davranışlarını n bi r saldırgan a şirketi n çıkarlarıyl a ter s yönd e kullanıla - bilecek değerl i bilgile r sağladığ ı konusund a e n küçü k bi r fikr i yoktu .

Ve nede n gene l müdü r yardımcısını n mesajların ı Ukrayna'dak i bi r e-posta adresin e göndermey i seçmişti ? Pe k ço k nedende n ötür ü uza k yerler bi r saldırganı n izini n sürülmes i y a d a on a karş ı hareket e geçilme - si şansın ı azaltır . Bunu n gib i ülkelerd e b u tar z suçla r genellikl e düşü k önceliklidirler v e interne t üzerinde n işlene n bi r su ç kaydadeğe r bi r su ç değildir. B u yüzde n Amerika n emniye t birimiyl e işbirliği yapm a olasılığ ı düşük ola n ülkelerde n e-post a adresler i alma k çekic i bi r stratejidir .

Aldatmacanın Engellenmes i

Bir toplu m mühendisi , he r zama n isteklerind e yanlı ş bi r şeyle r olduğunu anlam a şans ı düşü k çalışanlar ı hedeflemey i terci h eder . Bu , işini kolaylaştırmakl a kalmaz , b u bölümd e anlatıla n öykülerd e olduğ u gibi tehlikey i d e azaltır .

Gafili Kandırma k

Daha önc e bi r yabancını n talimatların ı yerin e getirmey e ikn a olma - maları içi n çalışanları n yoğu n bi r şekild e eğitilmeler i gerektiğin i vurgu - lamıştım. Tü m çalışanlar ayrıc a bi r isteği , başk a birini n bilgisayarınd a yerine getirmeni n tehlikesin i d e anlama k zorundadırlar . Şirke t kuralları , yöneticiler tarafında n özellikl e onaylanmadığ ı sürec e bun u yasakla -

işe Yen i Girenler e Saldırıla r 19 1

Mitnick Mesajı :

Mesai arkadaşınızdan ya da bir astınızdan yardım istemek olağan bir durumdur. Toplum mühendisleri insanların yardım etmeye v e iyi bir talam oyuncusu olmaya yönelik isteklerim sömürmeyi bilirler. Saldırgan, amacına yaklaşabilmek için hiç bir şeyin farkında olmayan çalışanları kandırıp çeşitli işleri yapmalarını sağlayarak bu olumlu ve insanî niteliği kullanır. Birilerinin sizi kandırmaya çalışıp çalışmadığım anlayabilmeniz için bu basit nohayı anlamış olmanız gereklidir.

malıdırlar. Mümkü n olabileceğ i durumla r arasınd a şunla r olabilir :

• İste k iy i tanıdığını z birinde n gelıiVyse , yto . vüx. e tu r görüşmed e

dile getirildiys e y a d a arayanı n sesin i tanıdığınızda n emi n

olduğunuz bi r telefo n görüşmes i sırasınd a alındıysa .

« Denenmi ş yöntemle r kullanara k iste k sahibini n kimli k tespit i

olumlu bi r şekild e yapılmışsa .

• Yapılaca k işlem , iste k sahibin i şahse n tanıya n bi r yönetic i y a d a

benzeri bi r yetkil i tarafında n onaylandıysa .

Bir şeyle r isteye n kiş i üs t düze y bi r yönetic i olduğun u iddi a ets e bil e çalışanlar şahse n tanımadıklar ı kişiler e yardı m etmemeler i konusund a eğitilmelidirler. Kimli k tespitiyl e ilgil i güvenli k süreçler i yürürlüğ e konduk - tan sonr a yönetim , bi r kural ı bertara f etmesin i isteye n üs t düze y bi r yöneticiye meyda n okumas ı anlamın a gels e bil e çalışanları n b u kural - lara uymaların ı desteklemelidir .

Her şirketin , bilgisayarla r y a d a bilgisaya r donanımlarıyl a ilgil i talep - lere yanı t verme k konusund a çalışanlar a yo l gösterece k kura l v e süreç - leri olmalıdır . Yayıncılı k şirketiyl e ilgil i öyküd e toplu m mühendis i bilg i güvenliği kurallar ı v e süreçleriyl e i\giV \ b\ r eğ\t\ m almamı ş yen i bi r çalışan ı seçti. B u tar z bi r saldırını n önün e geçme k içi n yen i y a d a esk i he r çalışanın basi t bi r kural a uymas ı sağlanmalıdır : Tanımadığını z birini n isteğini yerin e getirme k içi n bilgisaya r sistemin i kullanmayınız . Nokta .

Bir bilgisayar a y a d a bilgisayarl a ilgil i bi r donanım a fizikse l y a d a elektronik erişim i ola n bi r çalışanı n bi r saldırga n adın a zararl ı hareketle r yapmak üzer e yönlendirilmey e açı k olduğun u unutmayınız .

Çalışanlar v e özellikl e B i elemanları , dışarıda n birini n bilgisaya r ağına erişmesin e izirfvermenin , bank a hesa p numarasın ı telefonl a satı ş yapan birin e vermekl e y a d a telefo n kart ı kodun u hapistek i bi r yabancıya vermekl e arasınd a bi r far k olmadığını n bilincind e olmalıdır - lar. Çalışanla r bi r isteğ i yerin e getirmenin , hassa s bilgileri n açığ a çık - masına ya da şirke t

bilgisaya r sistemini n paylaşım a açılmasın a nede n olup olmadığ ı konus u dikkatl e tartmalıdırlar .

Bi personel i d e satıc ı gib i araya n tanımadıklar ı kişiler e karş ı tetikt e olmalıdırlar. Gene l olara k bi r şirke t he r teknoloj i satıcısını n bağlant ı kuracağı bell i kişile r görevlendirme n v e diğe r çalışanları n telefo n y a d a bilgisayar donanımların a yöneli k satıcılarda n gele n bilg i y a d a değişikli k taleplerine yanı t vermemes i içi n bi r kura l koymalıdır . B u yoll a belirlene n kişiler, araya n y a d a ziyare t ede n satıcılar a aşin a olurla r v e sahtekâ r tarafından kandırılm a olasılıklar ı düşer . Şirketi n deste k sözleşmesini n olmadığı bi r satıc ı aradığınd a bil e bun a kuşkuyl a bakılmalıdır .

Kuruluştaki herkesin , bilg i güvenliğini n zayıflıklar ı v e gelebilece k tehditler konusund a uyarılmalar ı gerekmektedir . Güvenli k görevliler i v e benzer çalışanlar a yalnızc a güvenli k eğitimini n değ i l ayn ı zamand a bilg i güvenliği eğilimini n d e verilmes i gerektiğ i unutulmamalıdır . Güvenli k görevlileri, tü m tesis e fizikse l erişimler i olduğ u için , kendilerin e karş ı kul - lanılabilecek toplu m mühendisliğ i tekniklerin i tanıyabilmelidirler .

Casus Yazılımlar a Dikka t

Casus yazılımla r bi r zamanla r çoğunlukl a çocuklarını n internett e n e yaptığını mera k ede n ana-babala r tarafında n y a d a hang i çalışanları n internette gezere k işte n kaytardığın ı belirlemey e çalışa n işverenle r tarafından kullanılırdı . Dah a cidd i bi r kullanım ı bilg i varlıkların a karş ı olası hırsızlıklar ı y a d a sanay i casusluğun u belirlemey e yönelikti . Tasarımcılar casu s yazılımların ı çocuklar ı koruma k içi n bi r ara ç olduğunu söyleyere k pazarlarla r am a ası l paza r başkaların ı gözetleme k isteyen insanlardır . Bugünlerde , casu s yazılı m satışlar ı insanları n eşlerinin y a d a benze r öneml i kişileri n kendilerin i aldatı p aldatmadık - larını öğrenme k istemeleriyl e büyü k ölçüd e artmıştır .

Bu kitaptak i casu s yazılı m öyküsün ü yazmay a başlamada n kıs a bi r süre önce , beni m adım a e-postalarım a baka n kiş i (interne t kullanma m yasak olduğundan) bi r diz i casu s yazılımı n reklamın ı yapa n bi r spa m e-posta bulmuş . Reklam ı yapıla n programlarda n bir i şöyl e birşey :

EN ÇO K İSTEYECEĞİNİ Z ŞEY : B u güçl ü gözetlem e v e casus programı , ger i pland a kendisin i farkettirmede n çalışırke n : tüm klavy e girişlerin i v e tü m açı k pencereleri n zama n v e başlık - larını gizlic e kaydeder . Günlükle r şifreleni p sizi n belirlediğini z bir e-post a adresin e otomati k olara k gönderilebili r y a d a sabi t diske kaydedilebilirler . Program a erişi m parol a korumalıdı r v e CTRL+ALT+DEL menüsünd e gözükmes i engellenebilir .

Yazılan ınterne t adreslerin i görmek , sohbe t oturumlarını , e-postaları v e pe k ço k başk a şey i (hatt â parolalar ı ;-)) izleme k için kullanabilirsiniz .

Farkedilmeden HERHANG İ Bİ R PC'y e yükleyi n v e gün - lükleri kendiniz e göndertin'.'. î

işe Yen i Girenler e Saldırıla r 19 3

Virüs Korum a Boşluğ u : :

Virüs korum a yazılımlar ı ticar î casu s yazılımlar ı bulamazla r v e böylece amac ı başkaların ı gözetleme k bil e ols a yazılım a köt ü huyl u bir yazılı m değilmi ş gib i yaklaşmı ş olurlar . Böylec e telefo n dinle - menin bilgisaya r karşılığ ı farkedilme z v e hepimi z içi n sürekl i yasadışı bi r gözle m altınd a olm a riskin i yaratır . Virü s korum a prog - ramlan üreticileri , doğa l olarak , casu s yazılımları n yasa l amaçla r içi n de kullanıldığın ı v e b u nedenl e köt ü huyl u olara k nitelendirilmemes i gerektiğini ön e sürebilirler . Ancak , bi r zamanla r bilgisaya r korsanlar ı tarafından kullanılmı ş araçların , artı k serbestç e dağıtıla n y a d a güvenliğe yöneli k yazılı m olara k satıla n gelişmiş şekiller i yin e d e kötü huyl u yazılı m olara k muamel e görebiliyor . Burad a bi r çift e stan - dart va r v e be n bunu n nedenin i mera k ediyorum .

Aynı e-postad a tanıtıla n başk a bi r ürün , kullanıcını n bilgisayarından , tıpkı kullanıcını n omuzunu n üzerinde n baka n bi r vide o kamer a gib i ekran resimler i alabileceğin i söylüyordu . B u yazılımlarda n bazılar ı kur - banın bilgisayarın a fizikse l erişi m sağlamay ı bil e gerektirmez . Kur , prog - ramı uzakta n ayarl a v e anınd a bilgisayar ı dinleyebili r durum a geç ! FB I bu teknolojiy e bayılıyo r olmalı .

Casus yazılımla r b u kada r kola y bulunurken , şirketinizi n ik i korum a düzeyi oluşturmas ı gerekmektedir . Tü m bilgisayarlar a SpyCo p gib i (www.spycop.com adresinde n sağlanabilir) casu s yazılımlar ı tespi t eden bi r progra m yüklemel i v e çalışanlarınızı n düzenl i olara k taram a yaptırmalarını sağlamalısınız . Bun a e k olarak , çalışanlarınız ı bi r prog - ram indirmey e y a d a köt ü huyl u bi r yazılı m kurabilece k bi r e-post a ek i açmaya yöneltece k dalavereleri n oluşturduğ u tehlikeler e karş ı eğit - meniz d e gerekir .

Bir çalışanı n kahv e molası , öğl e yemeğ i y a d a bi r toplant ı içi n masasında bulunmadığ ı durumlard a casu s yazılımları n yüklenmesin i engellemek içi n alınaca k önlemler e e k olarak , tü m çalışanları n bilgisa - yar sistemlerin i şifrel i bi r ekra n koruyuc u y a d a benze r bi r yönteml e kilit - lemeleri d e yetkisi z birini n çalışanı n bilgisayarın a erişmes i tehlikesin i büyük ölçüd e azaltacaktır . Kişini n odasın a y a d a bölmesin e sıza n hi ç kimse dosyaların a erişip , e-postaların ı okuyu p casu s yazılımla r v e köt ü huylu programla r yükleyemeyecektir . Ekra n koruyuc u parolasın ı dev - reye sokma k içi n gerekl i kayna k yo k denece k kada r az , çalışanları n bil - gisayarlarını korumad a sağladığ ı kazançs a muazza m ölçüd e büyüktür . Bu koşullard a fayda-maliye t analizin i yapma k içi n ço k kaf a yormay a gerek yoktur .

ZEKİCE OYNANMI Ş OYUNLA R

Hassas bilgile r tale p ede n y a d a bi r saldırganı n işin e yarayabilece k bir şeyle r isteye n yabanc ı bir i aradığında , telefon u açа n kişinin , arayanın telefo n numarasın ı alaca k v e kişini n gerçekte n söylediğ i kiş i -şirket çalışan ı y a d a orta k çalışıla n bi r firm a personel i y a d a satıcılar - dan birinde n gele n bi r tekni k deste k görevlisi - olu p olmadığın ı kontro l etmek içi n on u ger i arayaca k şekild e eğitilmes i gerektiğin i artı k iyic e görmüş olmalısınız .

Arayanların kimliğini n tespit i içi n şirke t çalışanlarını n özenl e izleme - si gereke n oturmu ş bi r süre ç ols a bile , ço k yönl ü saldırganla r kurban - larını söyledikler i kişile r oldukların a inandırma k içi n yin e d e çeşitl i oyun - lar oynayabilirler . Aşağıd a anlatıldığ ı gibi , güvenli k bilinc i yerleşmi ş çalışanlar bil e b u tar z yöntemlerl e tuzağ a düşürülebilirler .

Yanıltıcı Araya n Kimliğ i

Cep telefonun a aram a gele n herkes , araya n kimliğ i olara k bilinen , arayanın numarasın ı görm e özelliğin i bilir , i ş dünyasında , aramanı n şir - ket içinde n m i yoks a dışında n m ı geldiğin i bi r bakışt a anlama k gib i d e bir faydas ı vardır .

Yıllar önce , telefo n şirketlerini n b u hizmet i halk a sunmaların a izi n verilmediği zamanlard a baz ı hırsl ı telefo n beleşçiler i araya n numaray ı görmenin sağladığ ı olanaklarl a tanışmışlardı . Dah a araya n kiş i bi r şe y söyleyemeden on u adıyl a selamlayı p insanlar ı hayret e düşürere k eğleniyorlardı.

Güvende olduğunuz u düşündüğünü z bi r anda , gördüğünüz e güvenerek -yan i telefonu n ekranında , arayanı n numarasın ı görerek - kimlik tespit i uygulaması , aslınd a saldırganı n ta m d a yapmanız ı istediğ i şey olabilir .

Lînda'mn Telefo n Görüşmes i

Gün/Saat: 2 3 Temmuz , Salı , saa t 15:1 2

Yer: Starbea t Havacılık , Finan s Daires i

Tam patronun a bi r no t yazarke n Lind a HİH'i n telefon u çaldı . Arayanı n numarasına baktığınd a aramanı n Ne w Yor k Gene l Müdürlü k binasından , Victor Marti n adl ı birinde n geldiğini gördü . B u tanıdığ ı bi r isi m değildi .

Yazdığı notl a ilgil i düşünc e akışın ı kaybetmeme k içi n aramay ı tele - sekretere bırakmay ı düşündü . Am a merakın a yenild i v e telefon u açtı . Arayan kendin i tanıtt ı v e Ürü n Araştırma'da n olduğunu , Gene l Müdür'ü n istediği bi r şeyle r üzerind e çalıştığın ı söyledi . "Baz ı bankacılarl a toplant ı için Boston' a gidiyor , içind e bulunduğumu z ü ç aylı k dönem e ai t başlıc a finansal veriler e ihtiyac ı var " dedi . "V e bi r şe y daha . Apach e projesiyl e ilgil i finansal tahminler e d e gereksinim i var " diy e ekled i Victor , şirketi n bahar - da piyasay a süreceğ i öneml i ürünlerde n birini n ko d adın ı kullanarak .

Kadın on a e-post a adresin i sord u am a ada m e-post a almakl a ilgil i bir sorun u olduğunu , tekni k servisi n bunu n üzerind e çalıştığını söyled i ve b u yüzde n veriler i fakslayı p fakslayamayacağın ı sordu . Kadı n bunu n sorun olmayacağın ı söyled i v e Victo r on a dahil i fak s numarasın ı verdi .

Birkaç dakik a sonr a Lind a on a faks ı yolladı .

Ama Victor , Ürü n Araştırma'd a çalışmıyordu . Aslınd a o şirkett e bil e çalışmıyordu.

" Jack'ı n Öyküs ü • .."-. .

Jack Davvkin s profesyone l yaşamın a erke n yaşlard a Yanke e Stadyumu'nda oynana n maçlarda , kalabalı k metr o istasyonlarınd a v e Times Meydanı'n a gec e gele n turis t kalabalığını n arasınd a yankesicili k yaparak başladı . O kada r çevi k v e becerikliyd i k i adam a far k ettirmede n kolundan saatin i bil e alabilirdi . Am a sarsa k ergenli k çağınd a han - tallaşmış v e yakalanmıştı . Islahevinde , yakalanm a tehlikes i ço k dah a düşük ola n yen i bi r mesle k edinmişti .

Şu ank i işi , bi r şirketi n ü ç aylı k kâr-zara r durumun u v e naki t akı m bil - gilerini, verile r AB D Sermay e Piyasas ı Kurulu'n a verilmede n v e halk a açılmadan önc e el e geçirmesin i gerektiriyordu . Müşterisi , b u bilgiler i neden istediğin i söylemeye n bi r di ş hekimiydi . Jack' e kalırs a adamı n gizliliği komikti . Böylelerin i dah a önc e d e görmüştü ; adamı n büyü k olasılıkla bi r kuma r sorun u vard ı y a d a dah a karısını n bilmediğ i masrafl ı bir kı z arkadaş a sahipti . Y a d a belk i hiss e senetleriyl e oynamad a n e kadar akıll ı olduğuyl a ilgil i karısın a hav a atarke n bi r toma r par a kaybet - miş v e çeyre k dönemli k sonuçların ı açıkladıklarınd a şirke t hiss e senet - lerinin n e yön e gideceğin i öğrenenerek , kesi n bi r şey e büyü k oynayı p çok kazanma k istiyordu .

İnsanlar, dikkatl i bi r toplu m mühendisini n dah a önc e karşılaşmadığ ı bir durum u çözme k içi n n e kada r a z zaman a ihtiyac ı olduğun u öğrendik - lerinde şaşırıyorlar . Jac k di ş hekimiyl e yaptığ ı toplantıda n ev e dönen e kadar çokta n bi r pla n yapmıştı . Arkadaş ı Charle s Bate s kend i telefon santralı diğe r bi r deyişl e PBX' İ ola n Pand a ithala t adl ı bi r şirkett e çalış ı yordu.

Telefon sistemler i konusund a bilgil i insanları n aşin a olduğ u terimler -

rr-

[Zekic e Oynanmı ş Oyunla r 19 7

i

I

le ifad e edersek , PBX , T l olara k biline n bi r dijita l telefo n hizmetin e bağlıydı v e PR I ISD N olara k ayarlıydı . Bu , Panda'da n yapıla n he r ara - mada kurulum v e diğe r görüşm e bilgiler i ver i kanalında n telefo n şirket i santralına gidiyo r anlamın a geliyordu . B u bilgile r arasınd a (eğe r engel - lenmemişse) alıc ı uçt a numar a görüntülem e arayüzün e aktarılan , arayanın telefo n numaras ı d a vardı .

Jack'in arkadaşı , arana n kişini n araya n numaray ı görebileceğ i ş e kilde santral ı nası l programlayacağın ı biliyordu . Üsteli k Pand a ofisinde n kullanılan gerçe k telefo n numarasın ı değil , santral a he r n e telefo n numarası programlandıys a karş ı tarafi n on u görmesin i sağlayabiliyordu . Bu dümeni n işlemesini n nedeni , yere l telefo n şirketlerini n müşterini n kullandığı telefo n numarasıyl a müşterini n parasın ı ödediğ i telefo n numarasını karşılaştırmay a yanaşmamasıydı .

Jack Davvkins'i n ihtiyac ı ola n te k şe y böyl e bi r telefo n hizmetin i kul - lanabilmekti. Neysek i arkadaş ı v e kıs a bi r sür e içi n su ç ortağ ı ola n Charles Bate s küçü k bi r ücre t karşılığınd a he r zama n yardı m etmey e hazırdı. B u durumd a Jac k v e Charle s şirke t telefo n santralın ı geçic i olarak programlamışlardı . Böylec e Pand a şirketini n içindek i bell i bi r telefondan arandığınd a Victo r Martin'i n telefo n numarasın ı gösterece k ve aram a Starbea t Havacılık'ta n geliyo r gib i görünecekti .

Görünen numaranı n istediğini z numarayl a değiştirilebileceğ i fikr i o kadar a z bilini r k i b u yüzde n ço k a z sorgulanır . B u olayd a Linda , Ürü n Araştırma'dan olduğun u düşündüğ ü kişiy e istediğ i faks ı memnuniyetl e gönderdi.

Jack telefon u kapattığınd a Charle s şirke t telefo n santralın ı yenide n programlayıp telefo n numarasın ı ası l ayarların a ger i döndürdü .

Aldatmacanın İncelenmes i

Bazı şirketle r müşterilerini n y a d a ma l aldıklar ı şirketleri n çalışan - larının telefo n numaralarını bilmelerin i istemez . Örneğin , For d firmas ı Müşteri Deste k Merkezi'nde n araya n he r müşter i temsilcisini n doğruda n telefon numarasın ı görme k yerine , Merkezde n gele n tü m aramaları n Merkezin 800'l ü numarasın ı v e "For d Destek " gib i bi r bilg i göstermesin i isteyebilir. Microsoft , çalışanlarını n aradığ ı herkesi n araya n numaray a bakıp dahil i numarala n öğrenmemes i için , çalışanlarına telefo n num a ralarını yalnızc a kend i seçtikler i muhatapların a verm e seçeneğin i tanıyabilir. B u yoll a şirke t dahil î numaralarını n gizliliğin i koruyabilir .

Ancak b u yenide n programlanm a özelliği , şakacılar , fatur a tahsildar - ları, telefonl a satı ş yapanla r v e tabii , toplu m mühendisler i içi n ço k kul - lanışlı bi r ara ç oluşturmaktadır .

Çeşitleme: Amerik a Birleşi k Devletleri Başkan ı Arıyo r

Los Angeles , KF I Tal k Radi o adındak i bi r radyod a "interneti n Karanlık Yüzü " adl ı bi r programı n ikinc i sunucus u olara k radyonu n prog - ram yönetmeniyl e birlikt e çalışıyordum . Tanıdığı m e n işin e bağl ı v e çalışkan insanlarda n bir i ola n David , ço k meşgu l olduğ u içi n telefonl a ulaşılması zo r biriydi . Araya n numar a göstergesin e bakı p konuşma k istediği bir i değils e telefon u açmaya n insanlardandı .

Cep telefonumd a aram a engel i olduğ u içi n be n aradığımd a kimi n aradığını göremiyo r v e telefon u açmıyordu . Telesekrete r devrey e giri - yordu v e b u beni m içi n ço k ca n sıkıc ı oluyordu .

Yüksek teknoloj i şirketleri n ofi s bula n bi r emla k şirketini n sahib i ola n eski bi r arkadaşıml a b u konud a n e yapılabileceğin i görüştüm . Birlikt e bi r plan yaptık . Şirketin e ai t bi r Meridia n telefo n santralın a erişim i vard ı v e bir öncek i öyküd e anlatıldığ ı gibi , araya n tarafı n numarasın ı yenide n programlayabiliyordu. N e zama n progra m yönetmeniyl e konuşma m gerekse v e on a ulaşamazsam , arkadaşımdan , seçtiği m bi r numaranı n arayan numar a olara k gözükmes i içi n gerekl i programlamay ı yapmasın ı rica ederdim . Baze n aramay ı David'i n yardımcısında n y a d a rady o istas - yonunun sahib i ola n holdingde n geliyormu ş gib i göstermesin i isterdim .

Ama e n sevdiğim , aramay ı David'i n kend i evinde n geliyormu ş gib i göstermekti. Böyl e olduğ u zama n telefon u he p açıyordu . Anca k adam a hakkını verme k lâzım . Telefon u açı p on u bi r ke z dah a kandırdığım ı görünce olay ı şak a yoll u karşılamay ı biliyordu . Bunu n e n iy i taraf ı is e istediğim şeyi n n e olduğun u anlayı p sorun u çözen e kada r telefond a kalmasıydı.

Bu küçü k numaray ı Ar t Bel l Shovv'd a gösterdiğimde , araya n kimliği - mi FB I Lo s Angele s gene l merkezini n ad ı v e numaras ı olara k değiştirdim. Ar t tü m b u olanLr a oldukç a şaşırd ı v e yasadış ı bi r şe y yap - tığım konusund a ben i uyardı . Sahtecili k yapmadığı m sürec e bunu n tamamıyla yasa l olduğun u on a anlattım . Programda n sonr a bun u nası i yaptığımı sora n yüzlerc e e-post a aldım . Artı k si z biliyorsunuz .

Toplum mühendisini n inanılırlığın ı artırmas ı içi n b u kusursu z bi r araçtır. Örneğin , toplu m mühendisliğ i saldır ı sürecini n araştırm a aşa - masında hedefi n araya n numaralar ı görebildiğ i anlaşılırsa , saldırga n kendi numarasın ı güvenili r bi r şirkette n y a d a çalışanda n geliyormu ş gibi gösterebilir . Bi r fatur a tahsildarı , yaptığ ı aramalar ı işyerinizde n geliyor gib i gösterebilir .

Ama duru p bunu n etkilerin i düşünme k gerek . Bi r bilgisaya r saldır - ganı, şirketinizi n B İ biriminde n olduğun u söyleyere k siz i evinizde n arayabilir. Telefondak i kişi , çöke n bi r sunucuda n dosyalarınız ı kurtarma k

Zekice Oynanmı ş Oyunla r 1 99

JVÜtnick Mesajı :

Bir daha size bir telefon geldiğinde ve telefonun göstergesine bakıp arayanın sevgili anneniz olduğunu gördüğünüzde, hiç belli olmaz, sevimli, yaşlı bir toplum mühen- disiyle karşılaşabilirsiniz.

için acile n parolanız a ihtiya ç duymaktadır . Y a d a araya n numar a olara k bankanızın vey a menku l kıyme t danışmanınızı n ad ı v e numaras ı gözükebilir v e o tatl ı sesl i kı z hesa p numaralarınız ı v e annenizi n kızlı k soyadını kontro l etmes i gerektiğin i söylemektedir . İş i sağlam a alma k için sistemd e oluşa n bi r soru n nedeniyl e AT M kar t numaranız ı d a elin - deki bilgiyl e karşılaştırmas ı gerekmektedir . Şüphel i hiss e senetlerini n alınıp satıldığ ı bi r yer , aramaların ı Merril l Lync h y a d a Citibank'ta n yapılıyormuş gib i gösterebilir . Kimli k bilgileriniz i çalmay a çalışa n bir i Visa'dan arıyormu ş gib i görünüp , siz i kred i kart ı numaranız ı vermey e kandırabilir. Siz e di ş bileye n biri , arayı p verg i dairesinde n y a d a FBI'da n olduğunu söyleyebilir .

Bir PRI'y a bağl ı bi r telefo n sistemin e erişimini z v e satıc ı şirketi n internet sayfasında n edinebileceğini z küçü k bi r programlam a bilgini z varsa, b u taktiğ i arkadaşlarınız a sık ı oyunla r oynama k içi n kulla - nabilirsiniz. Tanıdığını z abartıl ı politi k eğilimler i ola n bir i va r mı ? Gösterilecek numaray ı 20 2 456-141 4 programlayıp , araya n numaralar - da gösterile n araya n kimliğin i "BEYA Z SARAY " olara k değiştirebilirsiniz .

Başkanın on u aradığın ı düşünecektir !

Hikâyenin an a fikr i basittir : Dahil î aramalar ı gördüğünü z durumla r dışında araya n kimliğin e güvenilmez . He m işt e he m d e evde , herke s arayan numar a üçkâğıdını n farkınd a olmal ı v e telefond a gözüke n adı n ve numaranı n kimli k tespit i içi n güvenili r bi r ver i olmadığını n bilincind e olmalıdır.

Görünmez Çalışa n

Shirley Cutlas s hızl ı par a kazanmanı n yen i v e heyecanl ı bi r yolun u bulmuştu. Artı k par a kazanma k içi n yırtınm a devr i kapanmıştı . So n yıl - ların e n sı k işlene n suçun u işleye n yüzlerc e dalaverecide n bir i olmuştu . Shirley bi r kimli k hırsızıydı .

Bugün gözün ü bi r kred i kart ı şirketini n müşter i hizmetler i bölümün - den gizl i bilg i almay a dikmişti . He r zamank i ödevlerin i yerin e getirdikte n sonra, hede f şirket i arad ı v e telefon u aça n santra l memurun a Telekomü - nikasyon birimin e bağlanma k istediğin i söyledi . Telekomünikasyon a bağlandığında sesl i mesa j yöneticisiyl e konuşma k istedi .

Araştırmalarından edindiğ i bilgiler i kullanara k adını n Norm a Tod d olduğunu v e Clevelan d bürosunda n aradığın ı söyledi . Artı k siz e d e tanıdı k gelen bi r kılı f uydurara k bi r haftalığın a şirke t gene l müdürlüğün e geleceği - ni v e şehirleraras ı telefo n görüşmes i yapmada n sesl i mesajların ı kontro l etmek içi n orad a bi r sesl i mesa j kutusun a ihtiyac ı olduğun u anlattı . Ada m konuyla ilgileneceğin i v e gerekl i düzenlemeler i yaptıkta n sonr a ihtiyac ı olan bilgiler i verme k içi n on u arayacağın ı söyledi .

Şuh bi r se s tonuyl a kadın , "Ş u and a bi r toplantıy a gidiyorum , siz i bi r saat sonr a yenide n arayabili r miyim? " diy e sordu .

Tekrar aradığınd a ada m he r şeyi n ayarlandığın ı söyled i v e on a dahil i numara v e geçic i parolada n oluşa n bilgiy i verdi . Adam , sesl i mesa j parolasını nası l değiştireceğin i bili p bilmediğin i sord u v e kadı n yapıl - ması gerekenler i ada m kada r iy i bils e d e yin e d e anlatmasın a izi n verdi .

"Ha, birde" , ded i kadı n v e sordu , "mesajlarım ı otelde n kontro l etme k için hang i numaray ı çevirme m gerekiyor? " Ada m on a numaray ı verdi .

Shirley o numaray ı aradı , parolay ı değiştird i v e arayanla r içi n yen i bir selamlam a mesaj ı kaydetti .

, Shirle y Saldırı r

Şimdiye kada r yaptığı , altyapıy ı oluşturmakta n ibaretti . Artı k aldatm a sanatını kullanmay a hazırdı .

Şirketin müşter i hizmetler i bölümün ü aradı . "Clevelan d bürosu . Tahsilatta çalışıyorum " ded i v e artı k aşin a olduğunu z bahaneni n bi r başka çeşidin i anlatmay a girişti . "Tekni k deste k ekib i bilgisayarım ı tami r etmeye uğraşıyor , b u yüzde n bi r bilgiy i bulma k içi n yardımınız a ihti - yacım var. " V e kimliğin i çalmay a niyetl i olduğ u kişini n adın ı v e doğu m tarihini verdi . Sonr a istediğ i bilgiler i sıraladı : Adresi , annesini n kızlı k so - yadı, kar t numarası , kred i limiti , kullanabileceğ i kred i miktar ı v e geçmi ş ödemeleri. "Ben i b u numarada n arayabilirsiniz" , diyere k se s mesa j yöneticisinin onu n içi n ayırdığ ı dahil i numaray ı verdi . "Eğe r yerimd e yok - sam, bilgiy i sesl i mesa j olara k bırakabilirsiniz. "

Sabah başk a işlerl e uğraşmay ı sürdürd ü v e öğlede n sonr a se s mesajını kontro l etti . İstediğ i he r şe y oradaydı . Telefon u kapamada " önce kend i selamlam a mesajın ı sildi . Gerid e sesini n kaydın ı bırakma - dikkatsiz bi r hareke t olacaktı .

Amerika'nın e n hızl ı artan , yen i yüzyılı n e n popüle r suç u ola n kim i - hırsızlığına bi r kurba n dah a verilmişti . Shirle y a z önc e el e geçirdiğ i kre : kartını v e kimli k bilgilerin i kullanara k kurbanı n kartında n harcam a yak - maya başlamışt ı bile . . -., - .

r r.

Zekice Oynanmı ş Oyunla r 20 1

Mitnick Mesajı :

Arada bir itendi sesli mesaj kutunuzu aramayı deneyin; eğer size ait olmayan bir selam- lama mesajı duyarsanız, hayatınmn ilk toplum mühendisiyle karşılaştınız demeldir.

Aldatmacanın İncelenmes i .

Çevirileri b u dalavered e saldırga n önc e şirketi n sesl i mesa j yöneti - cisini, geçic i bi r sesl i mesa j kutus u açmas ı içi n bi r şirke t çalışan ı olduğ u yolunda kandırdı . Eğe r ada m kimli k tespit i yapaca k olsaydı , kadını n verdiği adı n v e telefo n numarasını n şirke t çalışanlar ı ver i tabanındak i listelerle uyuştuğun u görecekti .

Geriye kalan , yalnızc a bilgisaya r sorunuyla ilgil i geçerl i bi r mazere t vermek, ihtiyac ı ola n bilgiler i karş ı tarafta n isteme k v e bilgileri n sesl i mesaja bırakılmasın ı ric a etmekte n ibaretti . Nede n bi r çalışa n başk a bi r şirket mensubun a yardı m etmesi n ki ? Shirley'ni n verdiğ i numaranı n dahili bi r numar a olduğ u açı k bi r şekild e görülürke n kuşkulanma k içi n hiçbir nede n yoktu .

Sekreter

Robert Jorda y adındak i bilgisaya r korsan ı küresel bi r şirke t ola n Rudolfo Gemicili k Inc.'i n bilgisaya r sistemlerin e düzenl i olara k giriyordu . Şirket, sonund a birilerini n uçbiri m sunucuların a bağlandığın ı v e b u sunucular üzerinde n kullanıcını n şirkettek i herhang i bi r bilgisayar a gire - bildiğini anladı . Şirke t ağın ı koruma k için , he r uçbiri m sunucusun a tele - fon hatl ı mode m takılmasın a kara r verildi . .- . • •

Robert, A ğ Hizmetler i Merkezi'ni , Huku k işleri'nde n araya n bi r avukatmış gib i arad ı v e ağ a bağlanmakt a güçlü k çektiğin i söyledi . Konuştuğu ağ yöneticis i on a birka ç güvenli k sorun u yaşadıkların ı bu yüz - den tü m telefo n bağlantıl ı kullanıcıları n aylı k parolay ı yöneticilerinde n alması gerektiğin i belirtti . Rober t he r ayı n parolasını n yöneticiler e nası l aktarıldığını v e parolay ı nası l el e geçirebileceğin i düşündü . Öğrendiği kadarıyla aradığ ı yanıt , bi r sonrak i ayı n parolasını n ofi s postas ı aracılığıyla bi r no t olara k he r şirke t yöneticisin e iletilmesind e yatıyordu .

Bu, işler i kolaylaştırmıştı . Rober t küçü k bi r araştırm a yaptı , heme n ayın birinde n sonr a şirket i arad ı v e yöneticilerde n birinin , adını n Jane t olduğunu söylediğ i sekreteriyl e görüştü . "Merhaba , Janet . Be n Araştırm a ve Geliştirme'de n Rand y Goldstein . Şirke t dışında n uçbiri m sunucusun a bağlanmak içi n kullanıla n yen i parol a notun u aldığım a emi n gibiyi m am a hiçbir yerd e bulamıyorum . B u ayı n notun u si z aldını z mı? "

Evet, ded i kadın , almışlardı .

Mitnick Mesajı :

Becerikli toplum mühendisi, insanları etkileyerek kendisine iyilikyapmalarım sağla- mak konusunda çok akıllıdır. Bir faks alıp sonra onu başka bir yere göndermek o kadar zararsız görünür ki bir danışma görevlisini ya da başka birini bunuyapmaya Uma etmek çok kolaydır. Biri sizden bilgi talep ederek bir iyilik yapmanızı istiyorsa ve siz o kişiyi tanımıyor ya da lamliğini kontrol edemiyorsanız, "hayır" deyin.

Onu kendisin e fakslayı p fakslayamayacağın ı sord u v e kı z kabu l etti . Ona şirke t alanınd a başk a bi r binanı n danışm a fak s numarasın ı verdi . Burada faksları n kendis i adın a bekletimesi içi n gerekl i düzenlemeler i çoktan yapmıştı . Dah a sonr a d a parol a faksını n kendisin e yön - lendirilmesini sağlayacaktı . Anca k b u ke z Rober t farkl ı bi r fak s yön - lendirme yöntem i kullandı . Danışm a görevlisin e bi r çevrimiç i fak s hizmetinin numarasın ı vermişti . B u numaray a fak s gönderdiğinizd e otomatik siste m on u aboneni n e-post a adresin e gönderiyordu .

Yeni parol a Robert' m Çin'dek i bi r ücretsi z e-post a hizmetinde n aldığ ı e-posta öl ü noktasın a geldi . Faksı n nerey e gittiğ i izlenece k olursa , soruşturmayı yürüte n kiş i Çinl i yetkililerl e işbirliğ i sağlayabilme k içi n saçını başın ı yolacaktı . Böyl e konulard a Çinlileri n pe k yardımc ı olma - yacaklarını Rober t biliyordu . E n güzel i is e fak s makinasını n başınd a hi ç bulunmamış olmasıydı .

Trafik Mahkemes i

Aşırı hı z cezas ı kesile n herke s herhald e cezada n sıyrılmanı n bi r yolu - nu bulmay ı haya l etmiştir . Ehliye t kursun a giderek , cezay ı ödeyere k y a d a yargıcı poli s hızölçerini n y a d a rada r cihazını n e n so n n e zama n bakım - dan geçtiğin i değerlendirmey e ikn a etmey e çalışara k b u i ş olmaz . Hayır , en güze l senary o sistem i ai t edere k cez a makbuzunda n kurtulmaktır .

Dalavere

Her n e kada r bi r trafi k cezasında n kurtulma k içi n b u yöntem i öner - mesem d e (he r zama n söylendiğ i üzere , bun u kendini z yapmay ı dene - meyin), toplu m mühendislerini n aldatm a sanatın ı kullanmaların a iy i bi r örnek oluşturmaktadır .

Bu trafi k ihlalcisini n ad ı Pau l Dure a olsun .

İlk Adımla r

- Los Angeles Emniyet Müdürlüğü, Hollenbeck birimi.

- Merhaba, Celp Bürosu'ndan biriyle görüşmek istemiştim.

- Mahkeme celplerine ben bakıyorum.

- Çok iyi. Ben avukat John Leland; Meecham, Meecham ve Talbott Avukatlık Bürosu'ndan. Bir memuru bir davaya çağırmam gerekiyor. - Peki, hangi memuru?

- Büronuzda Memur Kendall adında biri var mı?

- Sicil numarası nedir?

- 21349

- Evet, var. Ne zaman ihtiyacınız var?

- Gelecek ay bir ara ama bu dava için başka tanıklar da davet etmem ve sonra da mahkemeye hangi günlerin bizim için daha uygun olduğunu söylemem gerekiyor. Gelecek ay Memur Kendall'm müsait olabileceği günler hangileri?

- Bakalım...Yirmisinden yirmi üçüne kadar tatilde ve sekiziyle on altısı arasında da eğitimde olacak.

- Teşekkürler. Öğrenmek istediğim buydu. Mahkeme tarihi belli olduğu zaman sizi yine ararım.

Bölge Mahkemesi , Kâti p Masas ı

Paul: Bu trafik cezası için bir mahkeme tarihi belirlemek istiyorum. Kâtip: Tamam. Size, gelecek ayın yirmi altısını verebilirim. - Bir tebligat ayarlamak istiyordum.

- Trafik cezası için tebligat mı istiyorsunuz? ' • • - Evet.

- Tamam. Tebligatı varın sabah ya da öğleden sonra yapabiliriz. Hangisini tercih edersiniz?

- Öğleden sonra.

- Tebligat yarın öğleden sonra 13:30'da 6 numaralı mahkeme salonunda. - Teşekkürler, orada olacağım.

Bölge Mahkemesi , Alt ı Numaral ı Mahkem e

Tarih: Perşembe , öğlede n sonr a 13:4 5

Katip: Bay Durea, lütfen kürsüye yaklaşın.

Yargıç: Bay Durea, bugün öğleden sonra size açıklanan seçenekleri anladınız mı?

Paul: Evet, sayın yargıç.

Yargıç: Trafik okuluna gitme seçeneğini kullanmak ister misiniz? Sekiz saatlik bir kursu başarıyla

tamamladıktan sonra davanız düşe- cektir. Kayıtlarınızı inceledim ve şu anda gerekli niteliklere sahip görünüyorsunuz.

Paul: Hayır, sayın yargıç. Davamın görülmesini talep ediyorum. Bir şey daha var sayın yargıç, ülke dışına çıkmam gerekiyor ama ayın sekizinde ve dokuzunda uygun olacağım. Davamın o günlerden birinde görülmesi mümkün olabilir mi? Yarın Avrupa'ya iş gezisine gidiyorum v e dört hafta sonra döneceğim.

Yargıç: Pekala. Dava 8 Haziran, sabah 08:30'de dört numaralı mahkeme salonunda görülecektir.

Paul: Teşekkürler, sayın yargıç.

Bölge Mahkemesi , Dör t Numaral ı Mahkem e

Paul ayı n sekizind e mahkemey e erke n geldi . Yargı ç geldiğind e kati p

ona poli s memurlarını n gelmediğ i davaları n bi r listesin i verdi . Yargıç ,

aralarında Paul'ti n d e olduğ u davalılar ı çağırd ı v e onlar a davalarını n

düştüğünü söyledi .

Aldatmacanın İncelenmes i

Polis cez a kestiğ i zama n cez a makbuzunu n üzerin e adın ı v e sici l numarasını d a yaza r (y a d a çalıştığ ı kurumd a b u kişiy e özg ü numaray a ne a d veriliyors a on u yazar) . Görevl i olduğ u karakol u bulma k ço k kola y olur. Bilinmeye n numarala n arayı p makbuzu n üstünd e yaza n emniye t müdürlüğü karakolunu n adın ı (otoyo l devriyesi , bölg e şerif i y a d a her - neyse) vermeni z ayağınız ı kapıda n içer i sokmanı z içi n yeterlidir . Karakolu aradıkta n sonra , trafi k cezasını n kesildiğ i bölgeyl e ilgil i mahkeme celplerin e baka n memur a siz i yönlendirebilirler .

Emniyet mensuplar ı düzenl i olara k mahkemeler e çağırılırlar ; bu , yaptıkları işi n bi r parçasıdır . Bi r bölg e savcıs ı y a d a savunm a avukat ı bi r polis memurunu n tanıklığın a ihtiya ç duyars a v e sistemi n nası l işlediğin i biliyorsa, önc e memuru n n e zama n uygu n olduğun u öğrenir . Bun u yap - mak kolaydır , karakoldak i cel p memurun u arama k yeterl i olur .

Çoğunlukla b u görüşmelerd e avuka t memuru n ş u v e ş u tarihlerd e uygun olu p olmadığın ı sorar . B u oyun u oynayabilme k içi n Paui'u n duru - ma gör e davranması , cel p görevlisini n poli s memurunu n dol u olduğ u zamanlan vermes i içi n ell e tutulu r bi r nede n bulmas ı gerekiyordu .

Mahkeme binasın a gittiğind e nede n Pau l kâtib e doğruda n istedi ö şeyi söylemedi ? Basit ; anladığı m kadarıyl a çoğ u yerd e trafi k mahkeme - si kâtipler i halkı n mahkem e tarih i seçmesin e izi n vermezler . Eğe r kâti - bin önerdiğ i bî r tari h kişiy e uymuyorsa , kâti p bi r ik i tari h önerisind e dah a bulunur am a dah a fazlasın ı yapmaz . Öt e yanda n tebligatt a kendi r gösterecek zaman ı ayırabilmi ş birini n şans ı dah a yüksektir .

Paul bi r tebliga t hakk ı olduğun u biliyordu . Yargıçları n gü n taleplerin e çoğunlukla oluml u baktığın ı d a biliyordu . Poli s memurunu n eğiti m günlerir e denk gele n günler i özellikl e seçti .

Polisi n durum u gö z önün e alındığına. -

Mitnick Mesajı* .

İnsan aklı muhteşem bir eser. Biçimsiz bir durumdan sıyrılmak ya da istediklerini elde etmek için dolambaçlı yolla üretmekte insanların ne kadar yaratıcı olduğunu görmek ilginç. Kamu v e özel sektörde bilgi v e bilgisayar sistemlerini korumak için sizin d e aynı yaratıcılığı v e hayal gücünü göstermeniz gerekir. B u yüzden dostlarım, şirke- tinizin güvenlik politikalarını oluştururken yaratıcı olun ve olaylara dışardan bakın.

eğitime gitme k bi r trafi k mahkemesind e bulunmakta n dah a öneml i olacaktı .

Trafik mahkemelerinde , poli s memur u mahkemey e gelmezs e dav a düşer. N e par a cezası , n e trafi k okulu , n e cez a puanı.. . hiçbi r şe y olmaz . Daha d a iyis i trafi k suç u kayd a d a geçmez !

Tahminime gör e baz ı poli s yetkilileri , mahkem e görevlileri , bölg e savcıları v e benzer i kişile r b u öyküy ü okuyacakla r v e b u numaranı n işlediğini bildikler i içi n başların ı sallayacaklar . Am a ba ş sallamakl a kala - caklar v e hiçbi r şe y değişmeyecek . B u konud a bahs e girebilirim . 1992'd e çıkan Sneakers adl ı filmdek i Cosm o karakterini n d e söylediğ i gibi , "He r şey y a birdi r y a sıfırdır" , yan i sonu ç olara k he r şe y bilgiy e dayanıyor .

Emniyet müdürlüğ ü birimler i bi r poli s memurunu n aylı k programını , arayan neredeys e herkes e vermey e istekl i olduklar ı sürec e trafi k cezalarından kurtulma k he r zama n mümkü n olacaktır . Şirketinizi n y a d a kurumunuzun yaptığ ı işlemlerd e de akıll ı bi r toplu m mühendisini n almalarını pe k d e istemeyeceğini z bilgiler i alma k içi n kullanabileceğ i benzer açıkla r va r mı ?

Samantba'nın İntikam ı - . , ...

Samantha Gregso n kızgındı .

Üniversiteden işletm e diplomas ı alabilme k içi n ço k çalışmı ş v e bun u başarmak içi n bi r yığı n öğrenc i kredis i almıştı . Büyü k parala r kaza - nabileceği bi r kariye r sahib i olma k içi n üniversit e diplomas ı gerektiğ i he r zaman beynin e kazınmıştı . Sonund a mezu n olmu ş am a hiçbi r yerd e el i yüzü düzgü n bi r i ş bulamamıştı .

Lambeck İmalattak i iş e girebildiğ i içi n ço k memnu n olmuştu . Sekreterlik iş i yapma k küçü k düşürüc ü olabilird i am a Ba y Cartrigh t on u işe almakta n n e kada r memnu n oldukların ı v e ş u and a iş e sekreterlikl e başlamasının, açılaca k il k idar i olmaya n konum a onu n gelmesin i sağlayacağını söylemişti .

İki a y sonr a Cartright'ı n e n alttak i ürü n yöneticilerinde n birini n ayrıla - cağını duydu . O gec e gözün ü kırpmad ı v e kendin i beşinc i katta , kapıs ı olan bi r odada , toplantılar a katılı p kararla r alırke n hayal etti .

Ertesi saba h il k i ş olara k Ba y Cartright'ı n odasın a gitti . Cartrigh t ona , profesyonel bi r konum a geçmede n önc e yaptıklar ı işi n piyasasın ı dah a iyi öğrenmes i gerektiğin i düşündüklerin i söyledi . Sonr a d a gidip , piyasayı onda n ço k dah a a z tanıya n şirke t dışında n bi r amatör ü iş e aldılar.

O zama n yava ş yava ş anlamay a başladı . Şirkett e çalışa n pe k ço k kadın vard ı am a neredeys e heps i d e sekrete r konumundaydılar . On a yöneticilik görev i vermeyeceklerdi . Hiçbi r zaman .

Ödeşme -

Onlara bun u nası l ödeteceğin i planlamas ı neredeys e bi r haftasın ı aldı. Bi r a y kada r önc e yen i bi r ürü n tanıtım ı içi n bi r ticare t dergisinde n gelen ada m on a asılmıştı . Birka ç haft a sonr a ada m Samantha'y ı işte n aramış v e Cobr a 27 3 ürünüyl e ilgil i bira z ö n bilg i verebilirs e on a çiçe k göndereceğini v e gerçekte n ço k sık ı bi r bilg i olurs a on u yemeğ e çıkar - mak içi n Şikago'da n kalkı p geleceğin i söylemişti .

Bu konuşmada n kıs a bi r sür e sonr a şirke t ağın a bağlanmay a çalışan gen ç Ba y Johannson'u n yanınd a durmuştu . Hi ç düşünmede n adamın parmakların ı seyrett i (bun a omu z gezintis i d e denir) . Parol a olarak "marty63 " girmişti .

Planı oluşmay a başlıyordu . Şirket e geldikte n sonr a yazdığ ı bi r not u hatırladı. Dosyaları n arasınd a bi r kopyasın ı buld u v e ilkini n tarzın ı kulla - narak yen i bi r tan e dah a yazdı . Şöyl e bi r şe y olmuştu :

KİME: C . Pelton , B İ Bölüm ü ' ;

KİMDEN: L . Cartright , Geliştirm e

Martin Johansson , bölümümdek i bi r öze l projele r ekibiyl e birlikt e

çalışacaktır.

Bu nedenl e kendisine , mühendisli k grubunu n tü m sunucuların a

erişmek üzer e yetk i vermi ş bulunuyorum . Ba y Johansson'u n güvenli k

profilinin bi r ürü n geliştiricisiyl e ayn ı haklar a sahi p olaca k şekild e

güncellenmesi gerekecektir .

Louis Cartrigh t

Herkes yemeğ e çıktıkta n sonr a Ba y Cartright'ı n imzasın ı il k notta r kesip yenisin e yapıştırd ı v e kenarların ı daksilledi . Eld e ettiğ i şeyi n b'~ fotokopisini çekt i v e sonr a fotokopini n fotokopisin i çekti . İmzanı " çevresindeki kâğı t kena r izler i güçlükl e seçilebiliyordu .

Bay Cartrigth'ı n odasını n yakınındak i makinada n fak s çekti .

Üç gü n sonr a mesaiy e kald ı v e herke s giden e kada r bekle ; Johannson'un odasın a gird i v e ağ a adamı n kullanıc ı adın ı v e parolası " marty63'ü, girere k bağlanmay ı denedi . İş e yaradı .

Zekice Oynanmı ş Oyunla r 20 7

Dakikalar içerisind e Cobr a 273'ü n ürün özelliklerin i içere n dosyay ı buld u v e onları sıkıştırara k bi r disketi n için e kay - detti.

Terimler

Serin gec e esintisind e par k yerin e doğru yürürke n diske t güvenl i bi r şekild e çantasında duruyordu . Disket i o gec e dergi muhabirin e yollayacaktı .

OMUZ GEZİNTİSİ: Klavyeye bilgi giren birini, parolasını ya da başka kul- lanıcı bilgilerini görüp çal- mak amacıyla seyretmek.

Aldatmacanın İncelenmes i - .- . - .

Canı sıkılmı ş bi r çalışan , dosyala n tarar , hızl ı bi r kes-yapıştı r v e dak - silleme işlemini n ardında n bira z yaratıc ı bi r fotokopicili k yapa r v e ardın - dan fak s gider . V e bingo ! Gizl i pazarlam a v e ürü n bilgilerin i dışar ı çıkar - mıştır.

Birkaç gü n sonr a bi r ekonom i dergis i muhabir i ço k yen i bi r ürünü n özellikleri v e pazarlam a planlarıyl a ilgil i büyü k bi r habe r patlatır . B u haberi içere n dergi , ürünü n piyasay a sürülmesinde n ayla r önc e piyasadaki derg i abonelerini n elind e olacaktır . Rekabetç i firmala r ayla r öncesinden benze r ürünle r geliştirmey e başlayacakla r v e Cobr a 273' ü köstekleyecek rekla m kampanyalar ı hazırlayacaklardır .

Doğal olara k derg i hiçbi r zama n habe r kaynağın ı açıklamayacaktır . Aldatmacanın Engellenmes i

Rekabetçi bi r şirketi n y a d a başkalarını n işlerin e yarayabilece k değerli, hassa s v e öneml i bilgile r istendiğinde , çalışanlar , araya n numaraya bakmanı n kabu l edilebili r bi r kimli k tespi t yöntem i olmadığının bilinc e olmalıdırlar . Talebi n geçerliliğini n v e arayanı n b u bil - giyi almay a yetkil i olu p olmadığının , kişini n yöneticisin e sorulara k doğrulanması gib i farkl ı kontro l yöntemler i d e kullanılmalıdır .

Kontrol sürec i he r şirketi n kendis i içi n tanımlamas ı gereke n bi r denge unsur u içerir : Güveniik-Üretkenli k dengesi . Bağlayıc ı güvenli k önlemlerine hang i öncelikle r tanınacaktır ? Çalışanla r güvenli k işlemleri - ni uygulamay a direnecekle r v e hatt â i ş yükümlülüklerin i yerin e getire - bilmek içi n güvenliğ i bi r kenar a m ı bırakacaklardır ? Çalışanla r güven - liğin kendiler i ve şirketler i içi n taşıdığ ı önemi n farkındala r mıdır ? Şirke t kültürüne v e ticar i gereksinimler e gör e geliştirilece k bi r güvenli k poli - tikasının b u sorular ı yanıtlamas ı gerekmektedir .

Çoğu insan , işlerin i yapmaların ı geciktire n şeyler e kaçınılma z olara k sıkıntı gözüyl e baka r v e zama n kayb ı gib i görüne n herhang i bi r güven - lik önlemin i ciddiy e almayabilir . B u işt e kili t unsur , güvenliği n günlü k sorumluluklarının bi r parças ı olduğ u konusund a çalışanlar ı eğitimlerl e teşvik etmektir .

Arayan kimliğ i hizmeti , şirke t dışında n gele n sesl i aramalar ı tanım - lamak içi n hiçbi r zama n kullanılmas a d a ON T (otomati k numar a tanım - layıcısı) yöntem i kullanılabilir . Gele n tü m aramaları n ücretini n şirke t tarafından ödendiğ i bi r ücretsi z aram a hizmetin e abon e olunurs a ON T hizmeti şirket e verili r v e bu , kimli k tespit i içi n güvenili r bi r ara ç oluşturur . Arayan kimliğini n aksin e telefo n şirket i santral ı araya n numaray ı verirken müşterini n gönderdiğ i bilgiy i kullanmaz . ON T tarafında n aktarılan numar a araya n taraf a ai t fatur a numarasıdır .

Pek ço k mode m üreticisini n ürünlerin e araya n kimliğ i görm e özelliğ i eklediklerine de dikka t ediniz , böylec e yalnızc a öncede n yetkilendirilmi ş bir telefo n numaras ı listesin e uzakta n erişi m hakk ı tanıyara k şirke t ağın ı korumaktadırlar. Araya n numaray ı tanıya n modemle r düşü k güvenlikl i bir ortamd a kabul edilebili r tanımlam a yöntemleridir , anca k ş u an a kada r da açıkç a görülebildiğ i üzere , görünen numaray ı değiştirme k bilgisaya r kırıcıları içi n nispete n kola y bi r teknikti r v e b u nedenl e yükse k güvenlik - li bi r ortamd a arayanı n kimliğin i v e aradığ ı yer i tanımlama k konusund a güvenilir değildir .

Şirket telefo n sistemind e bi r sesl i mesa j kutus u oluşturmas ı içi n sis - tem yöneticisini n kandırıldığ ı hikâyedek i şekliyl e kimli k hırsızlığ ı olayını çözmek içi n tü m telefon hizmetlerinin , tü m sesl i mesa j kutularını n v e gerek basıl ı gereks e çevrimiç i şirke t rehberind e geçe n tü m numaraları n bu ama ç içi n hazırlanmı ş bi r for m doldurulara k yazıl ı tale p edilmesin i zorunlu tutun . Çalışanı n yöneticis i taleb i imzaiamal ı v e sesl i mesa j yöneticisi imzay ı kontro l etmelidir .

Şirket güvenli k kuralları , yen i bilgisaya r hesaplarını n açılmasını n y a da yetkileri n artırılmasını n sadec e talept e buluna n kişini n oluml u onayının alınmasında n sonr a gerçekleştirilmesin i zorunl u kılmalıdır . Talep onayı , siste m yöneticisin i y a d a onu n yerin e baka n kişiy i basıl ı y a da çevrimiç i şirke t rehberind e geçe n numarasında n arama k şeklind e olabilir. Eğe r şirket , çalışanları n dijita l olara k mesajların ı imzalayabildik - leri güvenl i e-post a sistem i kullanıyorsa , b u tanımlam a yöntem i d e geçerli bi r yönte m olara k kullanılabilir .

Şirket bilgisaya r sistemlerin e erişim i olsu n olmasın , he r çalışanı n bi r toplum mühendis i tarafında n kandırılabileceğin i unutmayın . Güvenli k bilin e eğitimlerine herkesi n katılmasın ı sağlayın . İdar i yardımcılar , danışm a görevlileri, santra l memurlar ı v e güvenli k görevliler i kendilerin e yöneltilebîle ^ cek toplu m mühendisliğ i saldır ı tekniklerini n bilincind e olmalıdırlar . Böylec e bu saldırılar a karş ı kendilerin i savunmay a hazı r olabilirler .

SANAYI CASUSLUĞ U

Devlete, şirketler e v e üniversit e sistemlerin e karş ı oldukç a yoğu n bi r bilgi saldırıs ı tehdid i vardır . Bası n neredeys e he r gün , yen i bi r bilgisaya r virüsünden, "hizme t dışıdı r (denia l o f service) " saldırısında n y a d a inter - netteki bi r e-ticare t sitesinde n kred i kart ı bilgilerini n çalınmasında n sö z etmektedir. •••-•• - :

Borland'ın Symantec' i ticar i sırların ı çalmakl a suçlaması , Cadenc e Tasarım Sistemleri'ni n bi r rakibin i kayna k kodların ı çalmakl a suçlayara k dava açmas ı gib i sanay i casusluğ u olayların ı basınd a görüyoruz .

Bunlar he r gü n oluyor .

Bîr Dalaver e Üzerin e Çeşitlem e

Aşağıdaki öyküd e anlatıla n dalavere , he r n e kada r Köstebe k (Th e Insider) gib i bi r Hoilyvvoo d filminde n y a d a Joh n Grisham'ı n bi r romanın - dan firlamı ş gibiys e d e herhald e birço k kerele r başarıyl a uygulanmıştır .

Toplu Dav a

Önemli bi r eczacılı k şirket i ola n Pharmomedic' e karş ı açılmı ş büyü k bir topl u dav a haya l edin . Davanı n konusu , şirketi n ço k kullanıla n ilaçların - dan birinin , anca k bi r hastanı n ilac ı yıllarc a kullanmasıyl a ortay a çıkabile - cek, yıkıc ı bi r ya n etkis i olduğunu n şirke t tarafında n bilinmesidir , iddiay a göre b u tehlikeni n varlığın ı göstere n çeşitl i araştırm a sonuçlar ı şirketi n elinde vardı r am a b u kanıtla r saklanmı ş v e olmas ı gerektiğ i gib i FDA'y a (Food an d Dru g Administratio n - Gıd a v e ila ç idaresi) tesli m edilmemiştir .

Toplu davay ı aça n Ne w Yor k huku k firmasını n başındak i yetkil i avukat VVillia m ("Billy") Chaney'i n elind e iddiay ı destekleye n ik i Pharmomedic doktorun a ai t görevde n alınm a belgeler i vardır . Anca k he r iki dokto r d a emekl i olmu ş v e n e ellerind e dosy a y a d a belg e vardır , n e de güçl ü v e ikn a edic i bi r şekild e tanıklı k yapaca k konumdadırlar . Bill y durumunun sallantıd a olduğunu n farkındadır . Sonu ç raporlarında n birinin bi r kopyasın ı y a d a yöneticile r arasınd a gidi p gelmi ş bi r yazışm a ya d a bilg i notun u eld e edemezse , dav a düşecektir .

Böylece, dah a önc e d e kendilerin e i ş verdiği , Andreeso n v e Oğullar ı özel dedektifli k acentasın a yen i bi r işl e gider . Billy , Pet e v e adamlarını n o bilgiler i nası l eld e ettiklerin i bilmez , bilme k d e istemez . Te k bildiği , Pete Andreeson'u n iy i bi r dedekti f olduğudur .

Andreeson içi n b u tar z bi r görev , kendisini n karanlı k işle r dediğ i tür - den bi r iştir . Birinc i kural , on u tuta n şirketle r v e huku k firmalar ı hiçbi r zaman bilgiy i nası l eld e ettiğin i öğrenemeyeceklerdi r v e böylec e he r zaman ta m v e akl a yatkı n bi r inkâ r nedenler i olacaktır . Eğe r elin i taşı n altına sokaca k bir i vars a b u d a Pete'ti r v e büyü k işlerd e aldığ ı ücretler e bakılırsa b u tehlikey e girdiğin e değe r gib i görünmektedir . Ayrıc a insan - ları tongay a düşürmekte n d e kişise l bi r zev k almaktadır .

Eğer Chaney'i n bulmasın ı istediğ i dosyala r gerçekte n varlars a v e imha edilmemişterse , Pharmomedic'i n dosyala n arasınd a bi r yerlerd e olmalan gerekir . Am a onlar ı koc a şirketi n de v dosy a yığınını n arasınd a bulmak büyü k bi r i ş olacaktır . Öt e yanda n dosyaları n kopyaların ı kend i hukukçularına, Jenkin s v e Petry' e d e vermi ş olabilirler . Eğe r savunm a avukatları b u belgeleri n varlığında n haberdarlars a v e araştırm a safhasında onlar ı ger i çevirmedilerse , o zama n hukukçulu k mesleğini n etiğine aykır ı davranmışla r v e yasalar ı çiğnemişlerdir . Pete'i n kitabında , böyle bi r duru m he r saldırıy ı muba h kılmaktadır .

Pete'in Saldırıs ı

Pete adamlarında n bazıların ı b u konuy u araştırmalar ı içi n görevlendirir v e birka ç gü n içind e Jenkin s v e Petry'ni n kend i bünyelerinde tutmadıklar ı yedeklemelerin i hang i şirkett e sakladıkların ı öğrenir. Ayrıc a saklam a şirketini n elinde , huku k firmasını n bantlar ı alma k için yetkilendirdiğ i kişiler e ai t bi r list e olduğun u d a öğrenir . B u insanları n her birini n kendilerin e ai t parolalar ı olduğ u d a biline n şeyle r arasındadır . Pete, adamlarında n ikisin i karanlı k bi r i ş yapmalar ı içi n yollar .

Adamlar internett e www.southord.co m adresinde n sipari ş edilebilece k bir maymuncukl a kilid i açarlar . Birka ç dakik a içinde , sabah a karş ı ü ç sularında saklam a şirketini n büroların a sızarla r v e bi r bilgisayar ı açarlar . Windows 9 8 logosun u görme k hoşların a gider , çünk ü bu , işi n ço k kola y olacağı anlamın a gelmektedir . Window s 9 8 kendin i tanıtman ı gerektirmez . Kısa bi r aramada n sonr a saklam a şirket i müşterilerinde n he r birinin , bant - ları almas ı içi n yetkilendirdiğ i insanları n adlarını n bulunduğ u bi r Microsof t Access veritaban ı bulurlar . Jenkin s v e Petr y yetk i listesin e saht e bi r a d eklerler. B u ad , adamlarda n birini n bulduğ u saht e ehliyetlerde n birindek i adla aynıdır . (Kilitl i dep o bölgesin e zorl a giri p müşterini n istediğ i bantlar ı d a o and a bulabilirle r miydi ? Kesinlikle ; am a o'zaman , aralarınd a huku k fir - masının d a olduğ u tü m müşterile r şirket e girildiğin i öğrenirle r v e saldırgan - lar üstünlüklerin i kaybederlerdi . Profesyonelle r "gerekirse " diy e he r zama r gelecekte ulaşabilecekler i açı k bi r kap ı bırakırlar.)

Sanayi casuslarını n gelecekt e kullanma k üzer e ark a cept e tutm a uygulamasını uyarak , he r ihtimal e karşı , yetkilendirm e listesini n olduğ u dosyayı bi r disket e kopyalarlar . Hiçbirini n bunu n nered e iş e yarayabile - ceği konusund a bi r fikr i yoktu r am a b u d a arad a bi r iş e yarayan , "Haz r gelmişken şun u d a alsak" , türünde n bi r bilgidir .

Mitnick Mesaj; :

Değerli bilgiler ne şekilde olurlarsa olsunlar ya da nerede dururlarsa dursun- lar korunmalıdırlar. Bir kuruluşun müşteri listesi kâğıt üzerinde ya da elektro- nik dosya olarak ofisinizde veya bir kasada dursa da aynı değere sahiptir. Toplum mühendisleri, çevresinden en kolay dolaşacakları ve en az korunan saldırı noktasını her zaman tercih ederler. Bir şirketin şirket dışı yedekleme bantlarını sakladığı yer, farkedilme ya da yakalanma tehlikesinin düşük olduğu bir nokta olarak görülmüştü. Değerli, hassas ve önemli verilerini üçüncü şahıs- lara emanet eden her kuruluş gizliliğini korumak için verilerini şifremelidir.

Ertesi gü n adamlarda n bir i saklam a şirketin i arayarak , yetk i listesin e ekledikleri ad ı v e ad a ai t parolay ı verir . Geçe n ay a ai t tü m Jenkin s v e Petry bantların ı iste r v e paket i bi r kury e servisini n geli p alacağın ı söyler . İkindi vaktind e bantla r Andreeson'u n elindedir . Adamları , istedikler i zaman taram a yapaca k şekilde , tü m veriler i kend i bilgisaya r sistemlerin e aktarmışlardır. Pe k ço k başk a şirke t gibi , huku k firmasını n d a yedekien - miş verilerin i şifrelemeyl e uğraşmamas ı Andreeson' u memnu n eder .

Bantlar ertes i gü n saklam a şirketin e tesli m edili r v e kimseni n operasyondan haber i olmaz .

Aldatmacanın İncelenmes i

Gevşek fizikse l güvenli k nedeniyle , köt ü adamla r saklam a şirketini n kilidini kolaylıkl a açmışlar , bilgisayarın a ulaşmışla r v e saklam a depo - suna ulaşmay a yetkil i kişileri n listesini n bulunduğ u ver i tabanıyl a oynamışlardır. Listey e bi r a d ekleme k sahtekârların , şirketi n saklam a deposuna zorl a girmelerin e gere k bırakmada n istedikler i yedeklem e bantlarını eld e etmelerin i sağlamıştır . Çoğ u şirket , yedeklem e dosyalarını şifrelemediğinde n bilgi , almalar ı içi n orad a durmaktadır .

Bu olay , geçerl i güvenli k önlemler i almaya n bi r hizme t şirketinin , saldırganların müşterisini n bilg i varlıkların a ulaşmasın ı nası l kolay - laştırdığına bi r örne k dah a oluşturuyor .

Yeni İ ş Ortağ ı

Toplum mühendislerini n sırada n dolandırıcılar a v e üçkâğıtçılar a gör e bir üstünlüğ ü vardır , b u d a uzaklıktır . Bi r üçkâğıtçı , yalnızc a yanınızdayke n sizi kandırabili r v e eğe r oyun a geldiğiniz i yeterinc e erke n anlarsanız , on u iyice tari f edebili r hatt â polisler i zamanınd a çağırabilirsiniz .

Toplum mühendisler i çoğunlukl a b u tehlikede n hastalıkmı ş gib i uza k dururlar. Anca k baze n b u tehlikey e d e girme k gerekir .

Jessica'nın Öyküs ü -

Jessica Andove r gösterişl i bi r roboti k şirketind e çalıştığ ı içi n ço k mutluydu. Yalnızc a yen i nesi l bi r teknoloj i şirketiyd i v e pe k d e iy i par a vermiyor olabilird i am a küçükt ü v e insanla r arkada ş canlısıydı . Ayrıc a kendisine verile n şirke t hiss e senetlerini n he r a n on u zengi n edebile - ceğini bilmeni n heyecan ı d a vardı . Belk i şirke t kurucular ı gib i milyone r olmazdı am a yeterinc e zengi n olurdu .

Ağustos'ta bi r Sal ı sabah ı lobide n girdiğind e Ric k Daggot'u n ışı l ışı l gülümsemesine nede n ola n şe y d e ayne n buydu . Pahal ı görünüml ü takım elbises i (Armani) , ağı r altı n ko l saat i (Role x President) v e kusursuz sa ç kesimiyle , lis e yıllarınd a Jessic a gib i kızlar ı çılgın a çevire n türden, erkeksi , kend i güvene n bi r havay a sahipti .

"Merhaba", ded i adam . "Be n Ric k Daggot . Larry'yl e randevu m vardı. "

Jessica'nın gülümsemes i birde n kayboldu . "Larr y mi? " deyiverdi . "Larry b u haft a tatilde. "

Rick, elektroni k ajandasın ı çıkarı p açtıkta n sonr a on a göstererek , "Saat bird e onunla randevu m var . Onunl a buluşma k içi n Louisville'de n buraya uçtum" , dedi . Jessic a on a bakt ı v e başın ı olumsu z bi r şekild e ik i yana salladı . "Yirmisi " dedi . "B u gelece k hafta. " Ada m avu ç iç i bilgisa - yarını kendin e çeviri p baktı . "Ah , hayır! " diy e inledi . "Yaptığı m aptallığ a inanamıyorum."

"En azında n sizi n içi n dönü ş biletiniz i ayarlayabili r miyim? " diy e sordu kız , ada m içi n üzülerek .

Kız telefo n görüşmesin i yaparke n Rick , Larry'yl e birlikt e bi r strateji k pazarlama ortaklığ ı kurmay ı tasarladıkların ı itira f etti . Rick'i n şirket i üre - tim v e monta j band ı içi n ürünle r üretiyordu . B u parçala r yen i ürünle r C2Alpha'yı mükemme l bi r şekild e tamamlayacaktı . Rick'i n ürünler i v e C2Alpha birlikte , he r ik i şirke t içi n d e öneml i sanay i pazarlar ı açaca - güçlü bi r çözü m oluşturacaktı .

Jessica öğlede n sonr a ge ç bi r saat e uça k reservasyonun u yapma; , bitirdiğinde, Rick , "E n azından , eğe r buradays a Steve'l e görüşebiliri m dedi. Am a şirketi n gene l müdü r yardımcıs ı v e kurucularında n bir i ola " Steve d e ofi s dışındaydı .

Jessica'ya ço k iy i davrana n v e bira z d a asıla n Rick , burad a olduğ. - na v e öğlede n sonr a ge ç saatler e kada r ev e dönemeyeceğine gör e ba z kilit kişiler i öğl e yemeğin e götürme k istediğin i söyledi . Sonr a d a ekle : "Sen d e tabii ; öğl e saatind e yerin e bakabilece k bir i va r mı? "

Kendisinin d e araların a katılacağ ı düşüncesiyl e mahcu p c a Jessica sordu , "Kimleri n gelmesin i istiyorsun? " Adam , yenide n avu ç : bilgisayarına bakt ı v e birka ç kişini n -AR-GE'de n ik i mühendisin , ye "

satış v e pazarlam a sorumlusunu n v e projey e atana n finan s müdürünün - adını verdi . Rick , Jessica'y a şirketl e ola n ilişkisin i onlar a anlatmasın ı önerdi v e kendin i onlar a tanıtma k istediğin i söyledi . Jessica'nı n he r zaman gitme k istediği , çevredek i e n iy i lokantay a gideceklerin i v e saa t 12:30 içi n bi r mas a ayırtacağın ı d a ekledi . He r şeyi n yolund a olu p olmadığından emi n olma k içi n öğlede n önc e arayacaktı .

Lokantada buluştuklarınd a -dörd ü v e Jessica - mas a henü z hazı r değildi, böylec e bar a oturdula r v e Ric k içkiler i v e yemeğ i kendisini n ödeyeceğini bi r ke z dah a vurguladı . Rick , tarz ı v e kalites i ola n bi r adamdı. İl k tanıştığını z anda n itibare n onu n yanınd a kendiniz i yıllardı r tanıdığınız birini n yanınd a olduğunu z kada r raha t hissediyordunuz . He r zaman n e söylemes i gerektiğin i iy i biliyormu ş gib i görünüyor , sohbe t durulduğunda neşel i y a d a komi k bi r yoru m yapabiliyo r v e onu n yakın - larında olduğunu z içi n kendiniz i iy i hissetmeniz i sağlıyordu .

Kurmakta ço k hevesl i göründüğ ü orta k pazarlam a çözümün ü hep - sinin gözlerind e canlandırmasın a yetece k kadar , kend i şirketini n ürün - leriyle ilgil i d e yeterinc e ayrınt ı anlatmıştı . Şirketini n satı ş yapmakt a olduğu pe k ço k Fortun e 50 0 şirketini n adın ı d a vermiş , masadak i herkese, fabrikada n çıktığ ı anda n itibaren , ürünlerini n ço k iy i i ş yapacağı hayalin i kurdurmay ı başarmıştı .

Sonra Ric k mühendislerde n bir i ola n Brian'ı n yanın a geçti . Diğerler i kendi aralarınd a sohbe t ederlerken , Ric k baz ı fikirlerin i Brian'l a öze l olarak paylaşt ı v e onda n C2Alpha'nı n kendin e özg ü nitelikler i v e on u piyasadaki benzerlerinde n neyi n ayırdığ ı gib i bilgile r aldı . Brian'ı n guru r duyduğu v e ço k "sıkı " olduğun u düşündüğ ü bi r ik i özelliğ i şirketi n önem - sizmiş gib i göstermey e çalıştığını d a öğrendi .

Rick, tarzın ı sürdürü p he r biriyl e küçü k sohbetle r etti . Pazarlam a sorumlusu, piyasay a sürü m tarih i v e pazarlam a planlarında n bahsetm e olanağı bulduğ u içi n mutluydu . Cebinde n bi r zar f çıkardı . Malzem e v e imalat maliyetlerini n ayrıntılarını , fiya t noktas ı il e beklene n kâ r payını , adlarını sıraladığ ı satıcılarl a n e tü r anlaşmala r yaptığın ı bi r bi r anlattı .

Masaları hazı r olduğund a Ric k herkesl e görü ş alışverişind e bulun - muş v e herkes i kendin e hayra n bırakmıştı . Yemeği n sonund a heps i Rick'le tokalaşı p teşekkü r ettiler . Ric k he r biriyl e kartvizi t alı p verdikte n sonra, mühendi s ola n Brian' a Larr y döne r dönme z dah a uzu n bi r görüşme yapma k istediğin i d e söyledi .

Ertesi gü n Bria n telefon u açtığınd a arayanı n Ric k olduğun u gör - müştü. Ric k a z önc e Larry'l e konuştuğun u söylüyordu . "Baz ı özellikler i görüşmek içi n Pazartes i ger i geleceğim" , dedi . "Sizi n ürünl e ilgil i e n kıs a sürede bilg i sahib i olmam ı istiyor . E n so n tasarımlar ı v e özellikler i on a e-postalamanı istediğin i söyledi . Bilmem i istediğ i kısımlar ı çıkarıp , ban a yollayacak."

Mühendis bunu n uygu n olacağın ı söyledi . "İyi" , diy e karşılı k verd i Rick. Sonr a sürdürdü , "Larr y e-postasın a ulaşmakt a bi r soru n yaşıyor - muş. Oteli n i ş merkezinde n kendisin e bi r Yaho o adres i almaların ı ric a etmiş. Belgeler i onu n he r zama n kullandığı e-post a adresin e gönder - mek yerin e dosyalar ı larryrobotics@yahoo.co m adresin e gönderme n gerekiyormuş."

Ertesi Pazartes i sabah ı Larr y güneşte n yanmı ş v e rahatlamı ş olara k girdiğinde Jessic a il k haber i verme k v e Rick' i öv e öv e anlatma k içi n ço k heyecanlıydı. "N e müthi ş bi r adam . Bazılarımız ı yemeğ e götürdü , ben i bile." Larr y anlamamı ş gib i duruyordu . "Ric k mi ? Ric k d e ki m ya? "

"Neden sö z ediyorsun ? Yen i i ş ortağın. "

"Ne!!!???"

"Sorduğu sorularda n herke s ço k etkilendi. "

"Rick diy e birin i tanımıyoru m ... "

"Senin neyi n var ? Şak a m ı bu , Larry ? Beniml e dalg a geçiyorsu n değil mi?" .

"Yöneticileri konferan s salonun a topla . Heme n şimdi . N e işler i vars a bırakıp gelsinler . O gü n öğl e yemeğin e gelenler i d e çağır . Se n d e dahil. "

Kasvetli bi r havada , pe k konuşmada n masanı n çevresin e top - landılar. Larr y içer i giri p oturd u v e konuşmay a başladı . "Ric k adınd a kimseyi tanımıyorum . Sizde n sakladığı m bi r i ş ortağı m d a yok . Bunu n en azında n açı k olduğun u düşünüyordum . Eğe r aramızd a şak a yap - maktan hoşlana n bir i varsa , şimd i ortay a çıkmasın ı istiyorum. "

Hiç se s çıkmadı . He r a n od a dah a kararıyormu ş gibiydi .

Sonunda Bria n konuştu . "Ekind e ürü n özellikler i v e kayna k kod u olan e-postay ı san a gönderdiğimd e nede n birşe y söylemedin? "

"Ne e-postası?! "

Brian gerildi . "A h .. . hayır! "

Cliff, diğe r mühendis , aray a girdi . "Hepimiz e kartvizitin i verdi . Te k yapmamız gereke n on u arayı p nele r olu p bittiğin i öğrenmek. "

Brian avu ç iç i bilgisayarın ı çıkardı , bi r bilgiy e bakt ı v e alet i masanı " üstünden kaydırara k Larry' e doğr u itti . Ümitlerin i kesmede n heps i hipno - tize gib i Larry'nı n telefon u çevirişin i seyrediyorlardı . Bi r a n sonr a telefo - nun hoperlörün ü açа n düğmey e bast ı v e heps i meşgu l sesin i duydula ' Yirmi dakik a boyunc a numaray ı defalarc a çevirdikte n sonra , can ı iyic e sıkılmış Larr y aci l bi r kesint i yaratmasın ı ric a etme k içi n santral ı arad ı

Biraz sonr a santra l yenide n hatt â geldi . Meyda n oku r bi r tonc a "Beyefendi b u numaray ı nerede n buldunuz? " diy e sordu . Larr y ac i e -

görüşmesi gereke n bi r adamı n kartvizitinde n aldığın ı söyledi . Santral , "Üzgünüm", dedi . " O bi r telefo n şirket i tes t numarası . He r zama n meşgul çalar. "

•* Larry , Rick'l e paylaşıla n bilgileri n bi r listesin i çıkarmay a başladı . Görüntü hi ç iy i değildi .

iki poli s dedektif i geli p tutana k tuttular . Hikâyey i dinledikte n sonra , eyalet kanunların a gör e herhang i bi r su ç işlenmediğin i v e yapabilecek - leri bi r şe y olmadığın ı söylediler . Larry' e FBI'l a görüşmesin i önerdiler , çünkü eyaletle r aras ı ticaretl e ilgil i suçla r onları n yetk i alanın a giriyordu . Rick Daggo t kendin i farkl ı tanıtara k mühendiste n tes t sonuçların ı gön - dermesini istediğind e federa l bi r su ç işlemi ş olabilird i am a bun u öğren - mek içi n FBI'l a konuşmas ı gerekiyordu .

Üç a y sonr a Larr y mutfakt a oturmuş , kahvalt ı edi p gazetesin i okurken a z kalsı n kahvesin i döküyordu . "Rick " adın ı il k duyduğ u anda n beri olmasında n korktuğ u şey , e n büyü k kâbus u gerçekleşmişti . Ekonomi sayfasınd a büyü k puntolarl a verile n haberde , dah a önc e adın ı hiç duymadığ ı bi r şirketin , geçe n ik i yıldı r kend i şirketini n geliştirdiğ i C2Alpha'nm tıpatı p aynıs ı gib i görüne n yen i ürünün ü piyasay a sürdüğünü duyuruyordu .

Kandırmaca yoluyl a o insanla r pazard a ön e geçmişlerdi . Rüyalar ı yıkılmıştı. Araştırmay a v e geliştirmey e yatırıla n milyonlarc a dola r ziya n olmuştu. V e onlar a karş ı te k bi r •kanıt ı bil e yoktu .

Scirtirny Sanford'u n Öyküs ü

Düzgün bi r işte çalışıp büyü k parala r kazanaca k kada r akıll ı am a bi r dolandırıcı olara k hayatın ı kazanmay ı terci h edece k kada r d a sahtekâ r bir ada m ola n Samm y Sanfor d kendin i ço k iy i idar e ediyordu . Zamanında içk i sorun u olduğ u içi n erke n emekliliğ e zorlanmı ş bi r casusun dikkatin i çekmişti . Ada m kızgı n v e intika m doluyd u v e devleti n onu uzmanlaştırdığ ı yetenekler i satmanı n bi r yolun u bulmuştu . He r zaman kullanabileceğ i insanlar a karş ı göz ü açıkt ı v e il k karşılaştıkların - da Sammy'ni n yeteneğin i görmüştü . Samm y b u iş i kola y bulmu ş v e ilg i noktasını insanları n paraların ı çarpmakta n şirke t sırların ı çarpmay a doğru çevirmeni n oldukç a kazançl ı olduğun u d a görmüştü . Devamın ı kendisinden dinleyelim :

Çoğu insanı n beni m yaptığı m işler i yapaca k cesaret i yoktur , insan - ları telefonda n y a d a interne t üzerinde n kandırmay a çalışırsını z v e kimse siz i görmez . Am a esk i usul , yü z yüz e türünde n iy i bi r dolandırıc ı (ve onlardan , ortalıkt a düşündüğünüzde n dah a ço k var) gözünüzü n içine bakı p kuyrukl u bi r yala n söyle r v e si z on a inanırsınız . Bunu n su ç olduğunu düşüne n bi r ik i savc ı biliyorum . Be n bun a yetene k derdim .

Ama gözünüz ü kapatı p iş e dalamazsınız , önc e ortalığ ı yoklamanı z

gerekir. Sokakt a tavcılı k yaparke n dostç a bi r sohbetl e v e dikkatl e kurul - muş cümlelerl e adamı n nabzın ı yoklayabilirsiniz . Doğr u yanıtlar ı alırsınız v e şak!. , kuş u kafes e alırsınız .

Şirket işi , büyü k dalaver e dediğimi z türde n bi r iştir . Önde n hazırlı k yapmanız gerekir . Hassa s noktalarını n n e olduğunu , n e bilme k istedik - lerini, ney e ihtiyaçlar ı olduğun u bilmelisiniz . Bi r saldır ı planlayın , sabırl ı olun, ödeviniz i yapın . Oynayacağını z rol ü belirleyi n v e n e söyleye - ceğinizi iy i çalışın . Hazı r olan a kada r kapıların a gitmeyin .

Bu i ş içi n hı z kazanan a kada r ü ç haftada n fazl a zama n harcadım . Müşteri, "şirketimin " n e yaptığın ı v e bunu n nede n iy i bi r pazarlam a ortaklığı olacağın ı nası l anlatacağım ı ban a ik i günd e öğretti .

Sonra şansı m yave r gitti . Şirket i aradı m v e bi r girişi m sermayes i şir - ketinden aradığımı , bi r toplant ı ayarlama k istediğimiz i söyledim . Önümüzdeki bi r ik i a y içind e tü m ortaklarımızı n bulunabileceğ i bi r zaman ayarlamay a çalışıyorum . Uza k durma m gereken , Larry'ni n şehirde olmayacağ ı herhang i bi r zama n aralığ ı va r mıyd ı acaba ? V e kadın "evet " dedi . Şirket i kurduğunda n ber i ik i yıldı r hi ç tati l yapmamıştı ; ancak karıs ı Ağustos'u n il k haftasınd a on u bi r gol f tatilin e sürüklüyordu .

Yalnızca ik i haft a sonraydı . Bekleyebilirdim .

Bu sırad a bi r ekonom i dergisinden , şirketi n halkl a ilişkilerin i yürüte n firmanın adın ı buldum . Roboti k şirket i müşteriler i içi n topladıklar ı ilgini n hoşuma gittiğin i v e onları n işin i ki m görüyors a kend i şirketiml e ilgil i olarak onunl a konuşma k istediğim i belirttim . Yen i bi r müşter i kazanm a fikrinden hoşlana n cıvı l cıvı l gen ç bi r hanı m olduğ u ortay a çıktı . Pahal ı bir öğl e yemeğinde , niyetlendiğinde n bi r kade h fazl a içt i v e "müşteri - lerinin sorunların ı anlamakt a v e doğr u halkl a ilişkile r çözümler i bulmak - ta a h n e kada r iyi " oldukların a ben i ikn a etme k içi n elinde n gelen i yaptı , ikna edilmes i gü ç birin i oynuyordum . Baz ı ayrıntılar a ihtiyacı m vardı . Biraz dürtüklemeni n ardında n mas a temizlenen e kada r ban a yen i ürü n ve şirketi n karşılaştığ ı sorunla r hakkınd a beklediğimde n dah a ço k şe y anlatmıştı. • • .

Her şe y tıkı r tıkı r yürüdü . Buluşmanı n gelece k haft a olmasıyl a ilgil i çok mahcu p olduğu m am a gelmişke n ekipl e tanışabileceği m öyküsün ü danışma görevlis i olduğ u gib i yutmuştu . Hatt â arad a ban a acımışt ı bil e Öğle yemeği , bahşi ş dahil , ban a 15 0 dolar a ma l old u v e istediğim i aldım. Telefo n numaraları , unvanla r v e söylediği m kiş i olduğum a inana n kilit bi r mühendis .

Brian'ın ben i şaşırttığın ı itira f etmeliyim . N e istese m gönderece k tür - den bi r adam a benziyordu . Konuy u açtığımda , bi r şeyler i söylemiyor - muş gib i gelmişti . Beklenmeyen i bekleme k he r zama n iş e yarar . Larr y adına alınmı ş e-post a adresi , he r olasılığ a karş ı ark a cebimd e duruyor - du. Yaho o güvenli k sorumluları , izleyebilmeler i içi n adres i birini n kullan -

masını herhald e hâl â bekliyorlardır . Dah a ço k bekleyecekler . İ ş işte n geçmişti. Be n yen i bi r projey e atılmıştı m bile .

Aldatmacanın İncelenmes i

Yüz yüz e dalaver e çevire n kiş i kendin i hedef e kabul ettirebilece k bi r şekilde göstermelidir . Yarışlar a giderke n kendin i başk a bi r şekl e sokarken, mahalleni n barın a giderke n başka , haval ı bi r oteli n şı k barın a giderken dah a başk a görünecektir .

Sanayi casusluğund a d a ayn ı şekildedir . Eğe r casus , oturmu ş bi r fir - manın yöneticisi , bi r danışma n y a d a satı ş sorumlus u kılığın a gireceks e yapacağı saldır ı ceke t giyi p krava t takmay ı v e pahal ı bi r çant a taşımay ı gerektirebilir. Bi r yazılı m mühendisi , tekni k elema n y a d a post a odasın - dan bir i gib i davranacağ ı başk a bi r işt e giysiler , üniforma , he r şe y farkl ı görünmelidir.

Şirkete sızabilme k içi n kendin i Ric k Daggo t olara k tanıta n kişini n şir - ketin ürün ü v e piyasayl a ilgil i ayrıntıl ı bilgiyl e donanmış , bi r güve n v e başarı görüntüs ü oluşturmas ı gerekiyordu .

Önceden bilmes i gereke n bilgiy i edinmekt e ço k güçlü k çekmemişti . Genel müdürü n n e zama n yerind e olmayacağın ı öğrenme k içi n basi t bi r oyun oynamıştı . Ço k zo r olmas a da , bira z dikka t gerektire n konu , yap - tıklarıyla ilgil i "konuy a hakim " görünece k kada r projey e yöneli k bilg i toplamaktı. B u tar z bilgile r çoğ u zama n ma l aldıklar ı şirketlerin , yatırım - cıların, par a toplama k içi n konuştuklar ı girişi m sermayecilerinin , çalıştık - ları bankanı n v e huku k şirketini n bildikler i şeylerdi . Anca k saldırga n dikkatli olmalıydı . Şirke t iç i bilgiler i paylaşabilece k birin i bulma k zo r bi r işti v e bilg i alınabilece k birin i bulma k içi n ik i y a d a ü ç kaynağ ı yoklama k

itnick Mesajı :

Her ne kadar çoğu toplum mühendisliği saldırısı telefon ya da e-posta üzerinden gerçekleşse de gözükara bir saldırganın işyerinizde şahsen belirmeyeceğini düşünmemelisiniz. Çoğu zaman sahtekâr, Photoshop gibi kolayca bulunabilen bir yazılımı kullanarak bir personel kartının sahtesini hazırladıktan sonra şirket binasına girebilmek için bazı toplum mühendisliği tekniklerini kullanır. Ya tele- fon şirketinin test numarasının yazılı olduğu kartvizitlere ne demeli? Bir özel dedektiflik dizisi olan Rockford Dosyaları adlı televizyon programında akıllıca ve eğlenceli sayılabilecek bir teknik gösterilmişti. Aktör James Garner'ın oynadığı Rodçford karakterinin arabasında, gerektiği hallerde uygun kartı basmak için kullandığı, taşınabilir bir kartvizit basma makinası vardı. Bu günlerde toplum mühendisleri kartvizitlerini bir saat içinde bir fotokopicide bastırabilir ya da bir lazer yazıcıdan çıktı alabilirler.

'. Soğuktan Gelen Casus, Son Casus ve daha pek çok dikkate değer romanın yazarı olan John Le Carre, itinalı, yaşam boyu

dolandırıcılıkla uğraşmış bir babanın oğlu olarak büyüdü. Daha Le Carre bir çocukken, babasını başkalarını kandırmakta başarılı olmasına rağmen, ahmak durumuna düşüp başka bir dolandırıcının kurbanı olduğunu öğrendiğinde çok şaşırmıştı. Bu da herkesin, hattâ bir toplum mühen- disinin bile, başka bir toplum mühendisi tarafından avlanabileceğini bize gösteriyor.

insanların oynana n oyun u farketmelerin e nede n olabilirdi . O tara f tehlikeliydi. Dünyadak i Ric k Daggot'la r seçimlerin i dikkatl e yapmal ı v e her bilg i patikasında n bi r ke z geçmelidirler . :

Öğle yemeğ i d e başk a bi r zorl u girişimdi . Öncelikl e he r şey i öyl e ayarlamalıydı ki , diğerlerin e duyurmada n herkesl e birka ç dakik a yalnı z kalabilmel'ıydi. Jessica'y a 12:3 0 ded i am a masay ı saa t 13:0 0 içi n ayırt - tı. Yeme k yiyecekler i yer , hesab ı şirke t masrafların a ekleyebileceğini z türden, şı k bi r lokantaydı . Saa t oynamasını n bire r içk i içi n bar a otur - malarını gerektireceğin i umuyordu , ta m d a böyl e olmuştu . Te k te k herkesin yanların a gidi p sohbe t etme k içi n kusursu z bi r fırsattı .

Yine d e Rick'i n bi r sahtekâ r olduğun u ortay a çıkaracak , atabileceğ i bir sür ü yanlı ş adım vardı . Anca k kendin e fazlasıyl a güvene n v e kurna z bir sanay i casus u kendin i böyl e bi r tehlikey e maru z bırakırdı . Am a yıllar - ca sokaklard a tavc ı olara k çalışma k Rick'i n yeteneklerin i geliştirmi ş v e dili sürçs e d e tü m kuşkular ı yatıştıraca k kada r iy i bi r şekild e olay ı kapa - tabileceğine dai r kendin e güvenmesin i sağlamıştı . Buras ı tü m süreci n en zorl u v e e n tehlikel i kısmıyd ı v e böyl e bi r dalaverey i çevirirke n duy - duğu kıvan ç nede n hızl ı arabala r kullanmadığı , gö k dalış ı (skydiving 1 yapmadığı y a d a karısın ı aldatmadığın ı anlamasın ı sağlamıştı . İşin i yaparken yeterinc e heyecanlanıyordu . Ka ç kişi , diy e mera k etti , ka ç ki ş bu kada r şansl ı olabilird i ki ?

Aklı başınd a bi r avu ç kadı n v e erkeği n araların a bi r sahtekâ ' almalarının neden i n e olabilir ? Oluşa n bi r durum u he m aklımızl a he m d e içgüdülerimizle tartarız . Eğe r anlattığ ı hikây e tutarlıys a -bu , akıll a yapıla r kısımdır- v e dolandırıc ı inanılı r bi r görünt ü çizdiys e çoğ u zama n yelker - leri suy a indiririz . Başarıl ı bi r dolandırıcıy ı y a d a toplu m mühendisin i par - maklıkların arkasın a düşenlerde n ayıra n unsu r inanılı r görüntüdür .

Kendi kendiniz e sorun : Rick'i n anlattığ ı gib i bi r öyküy ü asl a yutrr-a - yacağımdan n e kada r eminim ? Eğe r yutmayacağınızda n eminseni z : zaman kendiniz e birini n siz e böyl e bi r numar a yapmay a kalkı p kak - madığını sorun . Eğe r ikinc i soruy a verdiğini z yanı t evetse , bü\ - olasılıkla birinc i sorunu n doğr u yanıt ı d a b u olacaktır .

Zekice Oynanmı ş Oyunla r 21 9

Birdirbir

Size bi r soru : Aşağıdak i öyküd e sanay i casusluğuyl a ilgil i bi r şe y yoktur. Okurken , bakı n bakalım , nede n b u öyküy ü b u bölümd e anlat - tığımı anlayabilecek misiniz !

Harry Tard y evin e dönmüşt ü v e can ı sıkkındı . Asker e yazılmak , acemi birliğinde n atılan a kadar , ço k iy i bi r fiki r gib i gelmişti . Şimd i nefre t ettiği b u yer e ger i dönmü ş yere l yüksekokuld a bilgisaya r dersler i alıyo r ve dünyay a bi r toka t patlatmanı n yolların ı arıyordu .

Sonunda bi r pla n yaptı . Sınıfindak i adamlarda n biriyl e bi r kade h bi r şey içerlerken , herkes i küçümseyen , ço k bilmi ş bi r heri f ola n hocaların - dan şikâye t ediyorlardı . Birlikt e adam ı yakaca k kurna z bi r pla n yaptılar . Çok kullanıla n bi r PDA'nı n (persona l digita l asistan t - kişise l dijita l yardımcı) kayna k kodun u el e geçirecekle r v e şirketin , köt ü adamı n bil - gisayar hocas ı olduğun u düşüneceğ i şekild e gerid e i z bırakarak , hocanın bilgisayarın a göndereceklerdi .

Yeni arkada ş Kar i Alexander , birka ç numar a bildiğin i söylemişt i v e bu işi n nası l kotarılacağın ı Harry'y e gösterecekti . Tabii , yakalanmadan .

Ödevlerini Yapıyorla r

Yaptığı il k araştırmad a Harry , ürünün , PD A üreticisini n deni z aşı n bi r yerdeki Gene l Müdürlüğü'n e bağl ı Geliştirm e Merkezi'nd e yapıldığın ı öğrenmişti. Am a Birleşi k Devletler'd e d e bi r Ar-G e merkez i vardı . Karl'ı n söylediğine gör e b u iy i bi r şeydi , çünk ü yaptıklar ı işi n yürümes i içi n Birleşik Devletler'd e d e kayna k kodun a ihtiya ç duya n bi r şirket e ai t bi r tesis olmas ı gerekiyordu .

Bu noktad a Harr y deni z aşı n Geliştirm e Merkezi'n i aramay a hazırdı . Burada devrey e kendin i acındırm a girecekti . "Ama n tanrım , başı m dertte, yardım a ihtiyacı m var , lütfen , lütfe n ban a yardı m edin. " Yapacak - ları acındırm a doğa l olara k bunda n dah a üst ü kapal ı olacaktı . Kar i bi r metin yazd ı am a Harr y on u okumay a çalışırke n saht e olduğ u çıkardığ ı her seste n bell i oluyordu . Sonu ç olara k söyleme k istediğin i sohbe t ede r gibi söyleyebilmes i içi n Karl'l a oturu p çalıştılar .

Sonunda, Kar i yanınd a otururken ,

Harry'nin söylediğ i şe y aşağıdak i gibiydi , r

i

"Minneapolis Ar-Ge'de n arıyorum . |

Sunucumuza tü m bölüm ü etkileye n bi r [GZIP- Bir Linux GNU solucan girdi , işleti m sistemin i yenide n | uygu ı aması kullanarak yükleyeceğimiyüklememiz

gerekt

z zama

i v

ne yedeklemeler

yedekler i ger

-i

j dosyaların tek bir

sıkıştırılmış dosyada den hiçbirini n sağla m olmadığın ı gördük .

toplanması.

Bilin bakalı m yedekleri n sağlamlığın ı
kimin kontro l etmes i gerekiyor ? Bende -
nizin. B u yüzde n patronumda n bi r arab a HERKESE A ÇIK FTP: FTP
dolusu firç a yedi m v e yöneticile r ver i
(file transfer protocol -
kaybettik diy e veryansı n ettiler . Mümkü n
dosya aktarım protokolü)
olduğu kada r hızlı , kayna k kod u kullanma hesabınız olmasa
klasörünün e n so n halin e ihtiyacı m var .
da bir bilgisayara uzaktan
Ne kada r hızl ı gönderebilirseni z o kada r
erişmenizi sağlayan bir
iyi. Kayna k kodun u zip'leyi p ban a gön -
programdır. Her ne kadar
dermenizi ric a ediyorum. "
herkese açık FTP'lere paro-
lanız erişim mümkünse de
Bu aşamad a Kar i bi r kâğıd a bi r no t genellikle belli kalsörlerin
yazıp verd i v e Harr y telefonu n diğe r
kullanıcı hakları sınır-
ucundaki adam a dosyay ı dahil î olara k
landırılmıştır.
Minneapolis Ar-Ge'y e yollamasın ı iste -

diğini söyledi . B u öneml i bi r ayrıntıydı .

Telefonun ucundak i adam , dosyanı n şir - ketin başk a bi r bölümün e gönderilmesinin istendiğinde n emi n olunca , rahatlamıştı; bund a n e tersli k olabilird i ki ?

Adam dosyalar ı zip'leyi p göndermey i kabu l etti . Kar i yanındayke n Harry, büyü k kayna k kodun u te k bi r dosyay a sığdırma k içi n yapmas ı gerekenleri adam a adı m adı m anlattı . Ayrıc a sıkıştırılmı ş dosyad a kul- lanması içi n bi r dosy a ism i verdi : "yeniveri" . Bunu n eski , bozu k dosyalarla karışmamas ı içi n gerekl i olduğun u d a anlattı .

Bir sonrak i adım ı Harry'ni n anlamas ı içi n Karl'ı n ik i ker e anlatmas ı gerekmişti am a Karl'ı n hayalin i kurduğ u küçü k birdirbi r oyun u içi n b u önemliydi. Harr y Minneapoli s Ar-Ge'y i arayaca k v e oradak i birin e şöyl e diyecekti: "Siz e bi r dosy a gönderme k istiyoru m v e sonr a b u dosyay ı beni m için başk a bi r yer e göndermeniz i ric a ediyorum. " B u tale p doğa l olara k kulağa akl a yatkı n gele n he r türl ü nedenl e süsleni p püslenmişti . Harry'ni n kafasını karıştıra n şe y şuydu : "Siz e bi r dosy a göndereceğim" , demes i gerekiyordu anca k dosyay ı gönderece k kiş i kendis i değildi . Ar-G e bölümünde konuştuğ u adamı n dosyanı n kendisinde n geldiğin i düşün - mesini istiyordu . Aslınd a merkez e gelece k dosy a Avrupa'da n gele n tescil - li kayna k kod u dosyasıydı . "Başk a bi r kıtada n gele n bi r şe y içi n nede n be n gönderdim diyorum? " Harr y bunu n nedenin i bilme k istiyordu .

"Ar-Ge Merkezi'ndek i ada m kili t kişi" , diy e açıklad ı Kar! . "Amerika'daki bi r başk a çalışan a bi r iyili k yaptığın ı düşünüyo r olmas i gerek, sende n bi r dosy a alaca k sonr a seni n içi n o dosyay ı başk a birin e iletecek."

Harry sonund a anlamıştı . Ar-G e Merkezin i aradı , Bilgisaya - Merkezi'yle görüşme k istediğin i söyledi , orad a d a bi r bilgisaya r işlei - meniyle konuşma k istedi . Ses i Harr y kada r gen ç gele n bir i çıkt ı telefon a Harry on a "merhaba " ded i v e şirketi n Chicag o üreti m bölümünde "

aradığını v e birlikt e bi r projed e çalıştıklar ı bi r dosyay ı ortaklarında n birine göndermey e çalıştığı m açıMadı . "Ancak" , ded i v e ekledi , "Yönlen - diricide bi r soru n va r v e onları n ağın a ulaşamıyor . Dosyay ı siz e gönder - mek istiyorum . Dosyay ı gönderdikte n sonr a siz i arayı p on u ortağı n bil - gisayarına aktarmanı z içi n gerekl i adımlar ı anlatırım. "

Şimdilik he r şe y yolundaydı . Sonr a Harr y adam a bilgisaya r merkezinin herkes e açı k bi r FT P hesabını n olu p olmadığın ı sordu . Bu , bir dizin e dosy a yükleme k y a d a bi r dizinde n dosy a alma k içi n kullanıla n parolasız bi r kurulumdu . Evet , herkes e açı k FT P vard ı v e ada m oray a ulaşmak içi n gerekl i ola n İ P adresin i Harry' e verdi .

Eldeki b u bilgilerl e Harr y denizaşır ı Geliştirm e Merkezi'n i yin e aradı . Sıkıştırılmış dosy a hazırd ı v e Harr y herkes e açı k FT P sitesin e dosyay ı aktarmak içi n gerekl i açıklamalar ı yaptı . Be ş dakikada n kıs a bi r sür e içinde sıkıştırılmı ş kayna k kod u dosyas ı Ar-G e Merkezi'ndek i çocuğ a gönderilmişti..

Kurbanı Tuzağ a Düşürme k

Hedeflerine gide n yol u yarılamışlardı . Şimdi , deva m etmede n önc e dosyanın geldiğinde n emi n olma k içi n Harr y v e Karl'ı n beklemeler i gerekiyordu. Beklerken , odanı n diğe r tarafınd a duran , hocanı n masası - na gittile r v e atılmas ı gereke n ik i öneml i adıml a ilgilendiler , il k adı m b u makinada d a bi r herkes e açı k FT P sunucus u oluşturmaktı , böylec e oyunlarının so n ayağınd a dosyanı n gelebileceğ i bi r ye r olacaktı .

ikinci adı m zorl u olabiliece k bi r sorun a çözü m bulmay a yönelikti . Ar-G e Merkezi'ndeki adamda n dosyay ı warren@rms.ca.ed u gib i bi r adres e göndermelerini açıkças ı isteyemezlerdi . Ala n adını n ".edu " olmas ı büyük bi r açı k verme k demekti . Yar ı uyanı k bi r bilgisayarc ı bil e bunu n bir okulu n adresin i olduğun u anlar , anınd a tü m harekât ı son a erdirirdi . Bundan kaçınma k içi n hocanı n bilgisayarındak i VVİndovvs' a girdile r v e dosyanın gönderileceğ i adre s olara k verecekler i makinanı n İ P numarasına baktılar .

O sırad a Ar-G e Merkezi'ndek i bilgisaya r işletmenin i aram a zaman ı gelmişti. Harr y telefonl a on a ulaşt ı ve , "Sö z ettiği m dosyay ı a z önc e gönderdim. Geli p gelmediğin e bi r bakabili r misin? " diy e sordu . Evet , gelmişti. Harr y dosyay ı başk a bi r yer e iletmesin i ric a ett i v e on a İ P adresini verdi . Gen ç ada m bağlantıy ı kuru p dosyay ı göndermey e başlayana kada r telefond a bekled i v e hocanı n bilgisayarındak i -dosyay ı almakla meşgul - sabi t sürücünü n ışığ ı yanı p sönmey e başlayınc a ikisinin d e suratınd a kocama n bire r gülümsem e belirdi .

Harry v e adam , bi r gü n bilgisayarları n v e ar a birimlerini n nası l dah a güvenilir olacağıyl a ilgil i bira z sohbe t ettile r v e sonr a Harr y teşekkü r ederek ved a etti .

İkisi, dosyay ı hocanı n bilgisayarında n bi r çif t disket e kopyaladılar . Daha sonr a bakma k içi n he r bir i bire r kopy a almıştı , doy a doy a baka - bileceğin bi r tabloy u müzede n çalı p kimsey e birşe y söyleyememe k gib i bir şeyd i bu . Anca k b u durumd a dah a ço k onla r gerçe k tablonu n bire r kopyasını almı ş gibiydile r v e gerçe k ola n hâl â müzed e duruyordu .

Sonra Kari , Harry' e hocanı n makinasında n FT P sunucusun u kaldır - manın adımların ı v e yaptıklarında n geriy e birşe y kalmamas ı içi n denetleme izlerin i nası l sileceğin i anlattı . Geriy e bi r tek , kolayc a bulu - nabilecek bi r yerd e dura n çalınt ı bi r dosy a kalmıştı .

Son bi r adı m olara k kayna k kodunu n bi r parçasın ı doğruda n hocanın bilgisayarında n Usenet' e koydular . Yalnızc a küçü k bi r parçay - dı, böylec e şirket e büyü k bi r zara r vermemi ş olacakla r am a hocay a kadar taki p edilebilece k açı k izle r bırakmı ş olacaklardı . Ada m baz ı şey - leri açıklamakt a ço k zorlanacaktı .

Aldatmacanın İncelenmes i

Bu dalavereni n yürümes i içi n birka ç unsu r bi r aray a getirilmi ş ols a da kendin i açındırı p yardı m isteye n -patronumda n firç a yedim , yönetici - ler veryansı n ettiler , gibi - iy i bi r ro l yapm a olmada n b u i ş başarılamazdı . Bu v e telefonu n diğe r ucundak i adam a sorun u nası l çözeceğin i anlata n ayrıntılı bi r açıklam a oldukç a inandırıc ı bi r dalaver e olara k kendin i gös - terdi. B u noktad a v e pe k ço k başk a zamand a d a iş e yaramıştı .

ikinci öneml i nokta , dosyanı n değerin i anlayaca k adamda n dosyay ı şirket iç i bi r adres e göndermesin i istemişlerdi .

Bulmacanın üçünc ü parças ı is e bilgisaya r işletmenini n dosyanı n şir - ket içinde n gönderildiğin i görmesiydi . B u d a yalnızca , dosyay ı on a gön - deren adamı n eğe r dı ş a ğ bağlantıs ı çalışıyo r olsayd ı bun u kendisini n de gönderebileceğ i anlamın a gelebilird i y a d a e n azında n öyl e gib i görünürdü. Dosyay ı onu n adın a göndermekt e n e gib i bi r sakınc a ola - bilirdi ki ?

Sıkıştırılmış dosyay a farkl ı bi r a d verilmesin e n e dersiniz ? Küçü k gibi görüns e d e öneml i bi r ayrıntı . Saldırgan , dosyanı n içind e bi r kayna k kod olduğun u göstere n y a d a ürünl e ilgil i bi r adl a görülmes i riskin i göz e alamazdı. Böyl e bi r ad a sahi p bi r dosyay ı şirke t dışın a gönderm e taleb i alarm zillerin i çaldırabilirdi . Dosyanı n zararsı z görünüml ü bi r adl a

Mitnick Mesajı :

Her çalışanın beynine kazınmış temel bir kural olmalıdır: Yönetimin onayı olmadığı sürece, göndereceğiniz yer şirketinizin dahilî ağındaymış gibi gözülcse de, şahsen tanımadığınız kişilere dosya göndermeyin.

yeniden adlandırılması önemliydi . Saldırganları n d a öngördüğ ü üzer e ikinci gen ç adamı n dosyay ı şirke t dışın a göndermekl e ilgil i hiçbi r çekin - cesi olmadı . Bilgini n gerçekt e n e olduğuyl a ilgil i hiçbi r ipuc u vermeye n "yeniveri" gib i bi r ad ı ola n bi r dosy a zate n on u pe k kuşkulandırmazdı .

Sonuç olara k b u öykünü n sanay i casusluğuyl a ilgil i bi r bölümd e n e aradığını çözebildiniz mi ? Çözemediyseniz , işt e yanıtı : B u ik i öğrencini n hainc e bi r şak a olara k yaptıklar ı şey , raki p bi r firmanı n y a d a yabanc ı bi r ülkenin tuttuğ u profesyone l bi r sanay i casus u tarafında n kolaylıkl a yapılabilirdi. He r koşuld a d a şirketi n zarar ı korkun ç olur , raki p firmanı n • ürünü piyasay a çıktığ ı zama n yen i ürünlerini n satışların a cidd i bi r darb e vurulmuş olurdu .

Benzer bi r saldır ı sizi n şirketiniz e karş ı kolayc a gerçekleştirilebili r mi ?

Aldatmacanın Engellenmes i

Uzun süredi r şirketler e soru n oluştura n sanay i casusluğu , Soğu k Savaş'ın d a son a ermesiyl e ücre t karşılığ ı şirke t sırların ı el e geçirmey e odaklanmış gelenekse l casusları n ekme k kapıs ı oldu . Yabanc ı hükümetler v e şirketle r serbes t çalışa n sanay i casusların ı bilg i çalmalar ı için tutuyorlar . Yere l şirketle r de , rekabetç i bilgile r eld e etm e çabaların - da çizgiy i aşa n bilg i simsarların a başvuruyorlar . Çoğ u zama n esk i askerî casuslar , kuruluşlar ı kolaylıkl a sömürme k içi n gerekl i ö n bilgiy e ve deneyim e sahi p endüstriye l bilg i simsarların a dönüşüyorlardı . Özel - likle bilgilerin i koruma k v e çalışanların ı eğitme k konusund a gerekl i önlemleri almay ı başaramamı ş kuruluşla r başlıc a hedeflerdi .

Güvenli Saklam a Şirket i . .

Bilgilerini farkl ı bi r yerd e tuta n bi r şirketi n yaşadığ ı sorunlar a n e çözü m getirebilirdi? Şirket , verilerin i şifrelemi ş olsayd ı buradak i tehlik e önlenebilirdi. Evet , şifrelem e dah a fazl a zama n v e harcam a gerektiri r am a harcanan çabalar a değer . Şifrel i dosyaları n şifreleme/deşifrelem e sistem - lerinin düzgü n çalışı p çalışmadığ ı düzenl i olara k kontro l edilmelidir .

Her zama n şifr e anahtarını n kaybolmas ı y a d a anahtar ı bile n te k kişiye otobü s çarpmas ı gib i tehlikele r vardır . Am a yaşanabilece k ca n sıkıntısı, b u şekild e asgar î düzey e indirili r v e hassa s bilgilerin i kend i bünyesi dışınd a ticar î bi r firmad a tuta n v e şifrelem e kullanmaya n her - hangi biri , açı k sözlülüğüm ü bağışlayı n ama , salaktır . Köt ü bi r mahallede cebinizde n yirm i dolarlı k banknotlar ı sarkıtara k yürümek , esasen soyulmay a davetiy e çıkarma k gib i bi r şeydir .

Yedekleme ortamların ı birilerini n alı p götürebileceğ i bi r yerd e bırak - mak sı k görüle n bi r güvenli k açığıdır . Yılla r önc e müşter i bilgilerin i koru - mak içi n dah a iy i önlemle r alabilece k bi r şirkett e çalışıyordum .

Yedekleme sorumlular ı şirketi n yedeklem e bantların ı he r gü n bi r kuryenin geli p almas ı içi n kilitl i bilgisaya r odasını n dışın a bırakıyorlardı . Herhangi biri , şirketi n şifrelenmemi ş metinle r içere n tü m belgelerini n bulunduğu b u bantlar ı alı p gidebilirdi . Eğe r yedeklem e veriler i şifrelen - miş olsalardı , malzem e kayb ı sadec e bira z ba ş ağrıtırdı . Eğe r şifrelen - memiş olsalardı ; şirke t üstündek i böyl e bi r etkiy i bende n dah a iy i gözünüzde canlandırabilirsiniz .

Büyük şirketle r için , veriler i bünyeler i dışınd a saklam a gereksinim i kaçınılmazdır. Anca k şirketinizi n güvenli k süreçlerini n arasında , sakla - ma şirketini n kend i güvenli k kurallar ı v e uygulamalar ı konusund a n e kadar sağduyul u davrandığın ı kontro l etm e zorunluluğ u d a olmalıdır . Eğer sizi n şirketini z kada r kararl ı değillerse , tü m güvenli k çabalarını z boşa gidebilir .

Küçük şirketleri n yedeklem e içi n iy i bi r seçenekler i dah a vardır . Yen i ve değiştirilmi ş dosyaların ı he r gec e çevrimiç i saklam a ortam ı suna n şir - ketlerden birin e gönderebilirler . Yin e verileri n şifrelenmes i önemlidir . Aksi durumd a bilgiler , yolda n çıkmı ş bi r saklam a şirket i çalışanını n yanısıra çevrimiç i saklam a şirketini n bilgisaya r sistemlerin e y a d a ağın a girebilecek he r bilgisaya r korsanın a d a açı k olur .

Tabii ki , yedeklem e dosyalarınızı n güvenliğin i koruma k içi n bi r şifreleme sistem i kurduğunu z gibi , şifr e anahtarların ı y a d a parolalar ı saklamak içi n d e üstü n bi r güvenli k sürec i oluşturmanı z gerekmektedir . Verileri şifreleme k içi n kullanıla n anahtarla r bi r kasad a y a d a kili t altınd a tutulmalıdır. Sırada n şirke t uygulamalar ı b u verilerl e ilgilene n çalışanı n aniden ayrılabileceği , ölebileceğ i y a d a başk a bi r iş e geçebileceğ i olasılıklarına karş ı alınaca k önlemler i d e kapsamalıdır . Saklam a yerin i ve şifreleme/deşifrelem e adımlarını n yanısır a anahtarları n nası l değiştirildiğiyle ilgil i kurallar ı d a bile n he r zama n e n a z ik i kiş i olmalıdır . Kurallar ayrıc a şifrelem e anahtarların a erişim i ola n çalışanı n ayrılmas ı durumunda şifreleri n heme n değiştirilmesin i d e zorunl u kılmalıdır .

O D a Kim ?

Bu bölümd e anlatılan , bilg i paylaşmalar ı içi n çalışanlar ı kandırma k amacıyla etkileyiciliğin i kullana n kurna z dolandırıc ı örneği , kimli k tespi - tinin önemin i bi r ke z dah a vurgular . Kayna k kodunu n bi r FT P sitesin e yönlendirilmesi taleb i d e tale p sahibin i tanımanı n önemin e işare t eder .

On altınc ı bölümde , bilg i y a d a bi r işlemi n yapılmas ı talebiyl e gele n herhangi bi r yabancını n kimli k tespitin i yapma k içi n belirl i kuralla r bula - caksınız. Kimli k tespitini n öneminde n kitabı n he r yerind e sö z ettik ; 1 6 bölümde bunu n nası l yapılmas ı gerektiğini n ayrıntıların ı göreceksiniz.

Çıtam VühsEltmeln

'5

BİLGİ GÜVENLİĞİNİ N ON !

BİLMEK V E EĞİTİ M

Birtoplum mühendisine , ik i a y içind e piyasay a çıkaracağını z ço k sık ı yeni ürününüzü n planların ı el e geçirm e görev i verilmiş . On u n e durdu - racak?

Güvenlik duvarını z mı ? Hayır .

Güçlü kimli k tespi t cihazlar ı mı ? Hayır .

Hırsız uyar ı sistemler i mi ? Hayır .

Şifreleme mi ? Hayır .

Telefon hatt ı kullana n aramal ı modemle r içi n sınırl ı numar a kullanım ı mı? Hayır .

Dışarıdan birini n hang i sunucunu n ürü n planların ı içerdiğin i bul - masını zorlaştırma k içi n sunucular a şifrel i adla r verme k mi ? Hayır .

Gerçek ş u ki , dünyad a bi r toplu m mühendisliğ i saldırısın ı engelleye - bilecek bi r teknoloj i yok .

Teknoloji, Eğiti m v @ Süreçle r Üzerine Güvenli k

Güvenlik delm e testler i yapa n şirketleri n raporların a gör e toplu m mühendisliği yöntemler i kullanılara k müşter i şirketi n bilgisaya r sistem - lerine girm e denemeler i neredeys e yüzd e 10 0 başarıl ı oluyor . Güvenli k teknolojileri insanlar ı kara r verm e sürecini n dışınd a tutara k b u tar z saldırıları dah a güçleştiriyor . Anca k toplu m mühendisliğ i tehdidin i azalt - manın aslınd a e n etkil i yolu , güvenli k teknolojileriyl e birlikte , çalışa n davranışlarına v e alınaca k eğitimler e baz ı teme l şartla r getire n güvenli k süreçlerinin orta k kullanımında n geçmektedir .

Ürün planların ı korumanı n yalnızc a te k bi r yol u vardı r v e b u d a eğitim - li, bilinçl i v e sağduyul u bi r i ş gücüdür . Bunlar , süreçle r v e kuralla r konusun - daki eğitimleri n yan ı sır a - belk i d e dah a öneml i olan - sürekl i bi r bilinçlili k programı d a içerir . Baz ı yetkilile r bi r şirketi n topla m güvenli k bütçesini n yüzde 40'ını n bilinçUi k eğitimlerin e ayırılmasın ı önermektedirler .

ilk adım , psikoloji k olara k onlar ı etkileme k isteyece k tekinsi z insan - ların bulunduğun a dair , kuruluştak i herkes i bilinçlendirmektir . Çalışanla r

hangi bilgileri n korunmas ı gerektiğ i v e bunları n nası l korunacağ ı konusunda eğitilmelidirler , insanları n nası l etk i altınd a kalabilecekleriyl e ilgili bilgiler i olursa , gelişmekt e ola n bi r saldırıy ı görebilme k içi n ço k daha iy i bi r konumd a olacaklardır .

Güvenlik bilinci , ayn ı zamand a şirkettek i herkes i şirke t güvenli k kuralları v e süreçleriyl e ilgil i olara k eğitme k anlamın a d a gelir . 17 . bölümde d e anlatıldığ ı gibi , politikalar , şirke t bilg i sistemlerin i v e hassa s bilgileri korum a doğrultusunda , çalışa n davranışların ı yönlendirmes i içi n hazırlanmış öneml i kurallardır .

Bu bölü m v e bi r sonraki , siz i maliyetl i olabilece k saldırılarda n koruyabilecek bi r güvenli k tasarım ı ortay a koymaktadır . Eğe r iy i düşünülmüş süreçler i taki p eden , eğitiml i v e dikkatl i çalışanlarını z yoks a bu i ş olasılı k olmakta n çıkı p değerl i bilgileriniz i n e zama n bi r toplu m mühendisine kaptıracağını z şeklin e bürünere k kesinli k kazanır . B u kuralları yerleştirmede n önc e bi r saldırını n gerçekleşmesin i beklemeyin , işinizin v e çalışanlarınızı n rahatlığ ı açısından b u ço k yıkıc ı olabilir .

Saldırganların İnsa n Yaradılışında n Nasıl Faydalandıklarını n Anlaşılmas ı

Başarılı bi r eğiti m program ı geliştirme k için , öncelikl e insanları n neden saldırılar a karş ı açı k olduğun u anlamanı z gerekir . Eğitimlerinizd e bu eğilimler i tanımlayara k -örneği n ro l yapm a görüşmelerind e dikkat i buna çekebilirsiniz - nede n hepimizi n toplu m mühendislerini n etkis i altın - da kalabileceğimiz i anlamalar ı içi n çalışanlarınız a yardımc ı olabilirsiniz .

Etkileme, toplu m bilimcileri n e n azında n ell i yıldı r üzerind e çalıştık - ları bi r konudur . Rober t B . Cialdini , Scientifi c American'd a (Şuba t 2001) araştırmasını özetleyerek , bi r isteğ e oluml u yanı t alm a girişimind e kul - lanılan "insa n yaradılışını n alt ı eğilimi"n i sundu .

Bu alt ı eğilim , toplu m mühendislerinin (baze n bilinçli , çoğ u zama n d a bilinçsiz olarak) etkilem e denemelerin i dayandırdıklar ı eğilimlerl e aynıdır.

Yetki •'•••• •

Yetkili bir i bi r talepte bulunduğ u zama n insanları n b u taleb i yerir ; getirme eğilim i vardır . Bu sayfalard a dah a önc e de sö z edildiğ i üzere , c " kişi, talept e buluna n kişini n yetkil i olduğun a y a d a böyl e bi r talep: ? bulunabilmek içi n yetkilendirilmi ş olduğun a inanırs a isteğ i yerin e get" - meye ikn a edilebilir .

Dr. Cialdin i "Etki " adl ı kitabınd a ABD'ni n ort a bat ı kesimindek i ü ç has - tanede yapıla n bi r araştırmay ı yazmaktadır . Yirm i ik i ayr ı hemşir e ke^; -

ni hastan e doktorlarında n bir i olara k tanıta n bir i tarafında n aranı r v e kendilerine koğuştak i bi r hastay a bi r ila ç vermeler i konusund a talimatla r verilir. B u talimatlar ı ala n hemşirele r arayan ı tanımıyorlardı r v e gerçe k bi r doktor olu p olmadığın ı (k i değildir) bilmiyorlardır . İlaçl a ilgil i talima t tele - fonla verilmektedi r v e b u d a hastan e kuralların a aykırıdır . Ayrıc a verilme - si istene n ilacı n koğuşlard a kullanılmasın a izi n verilmemektedi r v e uygu - lanması istene n do z günlü k dozu n ik i katıdır . B u yüzde n hastanı n yaşamını tehlikey e atm a olasılığ ı vardır . Anca k olayları n yüzd e 95'ind e Cialdini'nin anlattığın a gör e "hemşire , koğu ş ila ç dolabında n istene n dozu alı r v e ilac ı verme k üzer e hastanı n odasın a doğr u giderken" , bi r gözlemci tarafında n durdurulu r v e kendisin e deneyde n bahsedilir .

Saldın örnekleri : Bi r toplu m mühendisi , bügi-işle m birimin - den aradığı m y a d a yönetic i olduğun u vey a bi r şirke t yöneti - cisinin yanında n aradığın ı söyleyere k kendin i yetkil i biriymi ş gibi göstermey e çalışır .

Sevme

İstekte buluna n kiş i kendin i sevimli y a d a kurbanl a orta k ilg i alanları , inançları v e tavırlar ı ola n bir i olara k gösterebilirse , insanlard a isteğ i ye - rine getirm e eğilim i ortay a çıkar .

Saldırı örnekleri : Sohbe t aracılığıyl a saldırgan , kurbanı n bi r hobisini y a d a ilg i alanın ı öğrenmey i başarı r v e ayn ı hob i y a d a ilgi alanın a benze r bi r ilg i v e hayranlık duyduğun u söyler . Ayn ı eyaletten y a d a ayn ı okulda n oldukların ı vey a benze r hedefler i paylaştıklarını iddi a edebilir . Toplu m mühendisi , benzerli k görüntüsünü yaratabilme k içi n hedefini n davranışların ı takli t etme yoluna d a gidecektir .

Karşılık Beklem e

Bize değerl i bi r şe y verili r y a d a verileceğ i taahüdünd e bulunulurs a hiç düşünmede n isteğ i yerin e getiririz . Armağan , bi r madd i cisim , tavsiy e ya d a yardı m olabilir . Bir i sizi n içi n bi r şe y yaptığ ı zaman , karşılı k verm e eğilimi hissedersiniz . B u karşılı k vermey e yöneli k güçl ü eğili m armağan ı alacak ola n kişini n on u tale p etmediğ i durumlard a bil e kendin i gösterir , insanları biz e bi r "iyilik " yapmalar ı (isteğimiz i yerin e getirmeleri) konusunda etkilemeni n e n etkil i yollarında n bir i on a bi r hediy e verere k y a da yardı m edere k bi r zorunlulu k duymaların ı sağlamaktır .

Hare Krişn a din i tarikatını n üyeleri , önc e insanlar a hediy e olara k bi r kitap y a d a çiçe k verere k insanlar ı amaçlar ı içi n bağışt a bulunmalar ı konusunda etkilemekt e ço k başarılıdırlar . Eğe r kişi , hediyeyi ger i ver - meyi denerse , vere n kişi , " O bizi m siz e armağanımız" , diyere k ger i çevirir. Karşılı k vermey e yöneli k davranışsa l kura l Krişnala r tarafında n bağışları büyü k ölçüd e artırma k içi n kullanılmıştır .

Saldırı örnekleri : Bi r çalışan , B İ biriminde n aradığın ı söyleye n birinden bi r telefo n alır . Arayan , baz ı şirke t bilgisayarların a virüs korum a yazılımını n tanımadığı , bilgisayardak i tü m dosyalan yo k edebilece k bi r virü s bulaştığın ı v e oluşabilece k sorunları engelleme k içi n baz ı yöntemler i anlatma k istediğin i söyler. Bunu n ardında n araya n kişini n yen i güncellenmi ş v e kul - lanıcılarm parolaların ı değiştirebilmelerin i sağlaya n bi r yazılım ı denemesini ric a eder . Çalışa n ger i çevirmekt e isteksi z kalır , çünkü araya n a z önc e on u güy a bi r virüste n koruyara k yardı m etmiştir. Arayanı n isteğin i yerin e getirere k karşılı k verir .

Herkesin içind e bi r amac a deste k y a d a bi r sö z verdikte n sonr a insanların isteklerin i yerin e getirm e eğilimler i depreşir . Bi r ke z birşey i yapacağımıza dai r bi r sö z verdi k mi , güvenilmeye n y a d a istenmeye n biri olara k görünme k istemeyi z v e verdiğimi z sözl e y a d a yaptığımı z açıklamayla ter s düşmeme k içi n iş i tamamlam a eğilimin e gireriz .

Saldırı örneği : Saldırgan , işind e yen i sayılabilece k bi r çalışanl a , bağlantı kura r v e şirketi n bilg i sistemlerin i kullanmasın a izi n verilebilmesinin bi r şart ı olara k belirl i güvenli k kuralların a v e ° süreçlerine uymas ı gerektiğin i hatırlatır . Birka ç güvenli k uygula - . masından sö z ettikte n sonr a arayan , kullanıcıdan , tahmi n etmes i güç bi r parol a seçilmes i kural ı uyarınc a "uyumlulu k kontrolü " için parolasın ı söylemesin i ister . Kullanıc ı parolasın ı açıkladık - tan sonr a araya n gelecekt e parolalar ı öyl e bi r yönteml e oluştur - masını öneri r k i böylec e saldırga n parolay ı tahmi n edebilecektir . Kurban, şirke t kuralların a uyma k üzer e dah a önc e verdiğ i taah - hüt doğrultusund a v e arayanı n yalnızc a kurallar a uyulu p uyul - madığını kontro l ettiğ i varsayımıyl a isteğ i yerin e getirir .

Toplum İçind e Kabu l Görm e ' • ;

İnsanlar, davranışlarını n başkalarını n davranışlarıyl a ayn ı olduğun u bilirlerse istekler i yerin e getirm e eğilimler i dah a d a artar . Başkalarını n hareketleri, sö z konus u davranışı n doğr u v e yerind e bi r hareke t olduğu - nun onay ı olara k görülür .

Saldırı örneği : Arayan , bi r araştırm a yaptığı m anlatı r v e bi - rimde kendisin e yardımc ı olduğun u iddi a ettiğ i diğe r insanları n adlarını verir . Kurba n diğerlerini n katılımının , isteği n geçerli - liğini gösterdiğin i düşünere k yardımc ı olmay ı kabu l eder . Arayan, aralarınd a kurbanı n bilgisaya r kullanıc ı adın ı v e paro - lasını açıklamay a yönelte n soruları n d a bulunduğ u bi r diz i sor u

Aranan nesneni n miktar ı azs a v e on u eld e etme k içi n bi r rekabe t varsa y a d a yalnızc a kıs a bi r sür e içi n orad a olacaks a insanla r istekler i yerine getirm e eğilimin e girerler .

Saldırı örneği : Saldırgan , şirketi n yen i interne t sitesin e kayı t olan il k 50 0 kişini n e n yen i filmler e bedav a bile t kazanacağın ı söyleyen e-postala r yollar . Hiçbi r şeyi n farkınd a olmaya n bi r çalışan, sitey e kaydolurke n onda n şirke t e-post a adres i v e bi r parola seçmes i istenir . Pe k ço k insanın , kolaylı k olsu n diye , kul - landıkları he r bilgisaya r sistemind e ayn ı y a d a benze r parolalar ı kullanma eğilim i vardır . Saldırga n bunda n yararlanara k interne t sitesi kayı t işlemlerind e girile n kullanıc ı ad ı v e parolay ı kullanı p hedefin e v y a d a i ş bilgisaya r sistemlerin e girmey e çalışır .

Eğitim v e Bilinçlendirm e Programları Hazırlama k

Bir güvenli k kurallar ı kitapçığ ı çıkarma k y a d a çalışanlar ı güvenli k kurallarını ayrıntıl ı olara k anlata n bi r intrane t sayfasın a yönlendirme k riski te k başın a azaltmaz . He r işletm e yalnızc a kurallar ı yazıl ı olara k belirlemekle kalmamalı , ayn ı zamand a şirke t bilg i y a d a bilgisaya r sis - temleriyle çalışa n herkes i kurallar ı öğrenmey e v e uygulamay a yön - lendirmek içi n gerekl i çabay ı d a göstermelidir . Ayrıca , insanları n kolaylı k olsun diy e kuralı n etrafında n dolaşmamalar ı için , he r kuralı n altında yatan nedenleri n herke s tarafında n anlaşıldığında n emi n olmalısınız . Aksi hald e bilgisizli k he r zama n çalışanı n bahanes i olu r v e toplu m mühendisleri b u açığ ı he p sömürürler .

Herhangi bi r güvenli k bilinçlendirm e programını n teme l amacı , kuru - luşun bilg i varlıkların ı koruma k içi n he r çalışanı n katkıd a bulunmasın ı teşvik edip , insanları n davranı ş v e tavırların ı değiştirme k amacıyl a onlar ı etkilemektir. B u noktad a e n büyü k teşvi k edic i unsur , katkılarını n yalnız - ca şirket e deği l ayn ı zamand a te k te k he r çalışan a getireceğ i kazançta n söz etme k olacaktır . Şirke t he r çalışanl a ilgil i bell i öze l bilgiler e sahi p olduğuna göre , çalışanla r bilg i v e bilg i sistemlerin i koruma k içi n payları - na düşen i yaptıklarında , aslınd a kend i bilgilerin i d e koruyo r olacaklardır .

Bir güvenli k eğiti m program ı büyü k bi r desteğ e ihtiya ç duyar . Eğiti m girişiminin hassa s bilgiler e y a d a şirke t bilgisaya r sistemlerin e erişim i olan herkes e ulaşması , sürekl i olmas ı v e çalışanlar ı yen i tehditler e v e açıklara karş ı uyarabilme k içi n düzenl i olara k güncellenmes i gerekir . Çalışanlar, üs t yönetimi n program a tamame n bağl ı olduğun u görme - lidirler. B u bağlılı k gerçe k bi r bağlılı k olmalıdı r v e sadec e mühürl ü bi r "Tam deste k veriyoruz" , notunda n ibare t olmamalıdır . Program , on u

geliştirmeye, duyurmaya , denemey e v e başarısın ı ölçmey e yetece k kadar d a kaynağ a sahi p olmalıdır .

Hedefler .

Bir bilg i güvenliğ i eğitim i v e bilinçlendirm e programını n gelişti - rilmesinde akıld a tutulmas ı gereke n e n öneml i yo l gösterici , programı n şirketlerinin he r an bi r saldırıy a uğrayabileceğ i bilincin i tü m çalışanlard a uyandırmaya odaklanmas ı olmalıdır . Bilgisaya r sistemlerin e girmey e y a da hassa s bilgiler i çalmay a yöneli k girişimler e karş ı yapıla n he r savun - mada çalışanları n tümünü n bire r rol ü olduğun u öğrenmeler i şarttır .

Bilgi güvenliğini n pe k ço k şekl i teknoloj i içerdiğ i için , çalışanların , sorunun güvenli k duvarlar ı v e diğe r güvenli k teknolojileriyl e çözüldüğünü düşünmeler i ço k kolaydır . Eğitimi n başlıc a hedeflerinde n biri, he r çalışanın , kuruluşu n gene l güvenliğini n e n ö n saflarınd a dur - duğunun farkın a varmasın ı sağlama k olmalıdır .

Güvenlik eğitimlerini n kurallar ı aktarmakta n öt e dah a öneml i bi r amacı olmalıdır . Eğiti m program ı tasarımcısı , işlerin i bitirm e baskısıyl a güvenlik yükümlülüklerin i uygulamam a y a d a gö z ard ı etm e şeklind e görülen, çalışa n tarafindak i güçl ü tahrikler i görebilmelidir . Toplu m mühendisliği taktikleriyl e ilgil i bilg i v e saldırılar a karş ı nası l savunm a yapılacağı önemlidi r am a b u sadec e eğiti m ağırlıkl ı olara k çalışanlar ı bilgiyi kullanmay a teşvi k etme k üzer e tasarlanmışs a iş e yarar .

Eğer eğitim i tamamlaya n herkes , bilg i güvenliğini n işini n bi r parças ı olduğu gerçeğin e inanmı ş v e hareket e geçmişs e şirke t o zama n prog - ramının an a hedefin e ulaştığın ı varsayabilir .

Çalışanlar, toplu m mühendisliğ i saldırılar ı tehdidini n gerçe k olduğunu v e cidd i bi r hassa s bilg i kaybını n şirket i olduğ u kada r kend i kişisel bilgilerin i v e işlerin i d e tehlikey e sokabileceğin i kabu l edi p anla - malıdırlar, iştek i bilg i güvenliğ i konusund a dikkatsi z davranmakla , AT M ya d a kred i kart ı numaras ı konusund a dikkatsi z davranma k bi r bakım a aynıdır. Güvenli k uygulamalar ı konusund a iste k uyandırma k içi n b u ço k yerinde bi r benzetm e olabilir .

Eğitim v e Bilinçlendirm e

Programını Oluşturma k

Bilgi güvenliğ i programın ı tasarlamakl a yüküml ü kiş i bunu n te k beden bi r proj e olmadığın ı bilmelidir . Eğiti m dah a ço k şirke t içindek i farklı grupları n belirl i gereksinimlerin i karşılayaca k şekild e tasarlan - malıdır. 16 . bölümd e dı ş çerçeves i verile n güvenli k kurallarını n çoğ u tüm çalışanla r içi n uygu n ols a da , diğe r pe k çoklar ı d a özgündür . Er . azından çoğ u şirke t ş u belirgi n grupla r içi n eğiti m programların a ihtiya ç

I Özgün bir program geliştirmek için yeterli kaynağı olmayan işletmeler için güvenlik bilinçlendirme eğitimi hizmeti veren pek çok eğitim şirketi bulunmaktadır. Güvenli Dünya Fuarı (www.secureworldexpo.com) gibi fuarlar bu şirketlerin bir araya gelme yerleridir.

duyacaktır: Yöneticiler , bilgi-işle m personeli , bilgisaya r kullanıcıları , teknik olmaya n personel , idar î yardımcılar , danışm a görevliler i v e gü - venlik görevliler i (16 . bölümd e görevler e gör e kura l dağılımın a bakınız.) .

Bir şirketi n güvenli k görevlileri , bilgisaya r konusund a bilgilerini n olması beklenmediğ i içi n v e belk i ço k sınırl ı kullanımla r dışında , şirke t bilgisayarlarıyla haşı r neşi r olmadıklarından , b u tar z eğitimle r gelişti - rilirken gö z önün e alınmazlar . Anca k toplu m mühendisleri güvenli k görevlilerini y a d a başk a insanlar ı binay a y a d a ofis e girmelerin e izi n vermeleri içi n y a d a bilgisaya r güvenli k ihlallerin e nede n olaca k bi r davranışta bulunmalar ı doğrultusund a kandırabilirler . He r n e kada r güvenlik güçler i bilgisayarl a çalışa n personel e verile n eğitimi n tümün ü almak zorund a değils e d e güvenli k bilinçlendirm e programlarınd a d a göz ard ı edilmemelidir .

İş dünyasında , tü m çalışanları n eğitilmesini n gerektiğ i v e güvenli k kadar herhald e ayn ı and a he m öneml i he m d e sıkıc ı ço k a z kon u vardır , iyi tasarlanmı ş güvenli k eğitim i programları , öğrenenleri n he m ilgisin i çekmeli he m d e onlar ı heveslendirmelidir .

Amaç, bilg i güvenliğ i bilinçlendirm e eğitimlerin i çekic i v e karşılıkl ı etkileşimli yapma k olmalıdır . Kullanılabilece k yöntemle r arasında , toplum mühendisliğ i tekniklerin i ro l yapm a oyunlarıyl a göstermek ; dah a az şansl ı ola n diğe r işletmeler e yakı n zamand a yapıla n saldırılarl a ilgil i basın haberlerin i inceleme k v e şirketleri n kayıplar ı önlem e yolların ı tartışmak y a d a ayn ı and a he m eğlencel i he m d e eğitic i olmas ı açısın - dan güvenli k videoların ı gösterme k olabilir . Videola r v e ilgil i malzemeler i pazarlayan pe k ço k güvenli k bilinçlendirm e şirket i bulunmaktadır .

Bu kitaptak i öyküler , tehlikey e karş ı uyarma k v e insa n davranışlarının açıkların ı gösterme k amacıyl a toplu m mühendisliğ i teknik v e yöntemleriyl e ilgil i pe k ço k bilg i sunmaktadır . Oradak i senar - yoları, ro l yapm a faaliyetlerin e teme l olaca k şekild e kullanabilirsiniz . Öyküler ayn ı zamanda , saldırını n başarıl ı olmasın ı engelleme k içi n kur - banların nası l davranmas ı gerektiğiyl e ilgil i renkl i tartışmala r yapabilm e firsatı d a sunmaktadır .

Becerikli bi r progra m geliştiricis i v e becerikl i eğiticiler , sınıfı n havasını canl ı tutma k ve bu sırad a insanlar ı çözümü n parças ı olmay a teşvik etme k içi n çözülece k bi r sür ü sorunu n yan ı sır a pe k ço k başk a fir - sat d a bulacaklardır .

Eğitimin Yapıs ı

Temel bi r güvenli k bilinçlendirm e eğiti m program ı tü m çalışanları n katılacağı şekild e geliştirilmelidir . Yen i iş e girenleri n intiba k eğitimlerini n bir parças ı olara k b u eğitim i alm a zorunluluklar ı olmalıdır . Hiçbi r çalı - şana teme l bi r güvenli k bilinçlendirm e oturumun a katılmada n bilgisaya r erişimi verilmemesin i öneririm .

İlk bilinçlendirm e eğitim i içi n dikkatler i çekmey e odaklanmı ş v e önemli mesajları n hatırlanacağ ı kada r kıs a bi r oturu m uygu n olabilir . Üzerinde durduğumu z konuları n miktar ı kesinlikl e dah a uzu n bi r eğiti m gerektirse de , maku l sayıda , öneml i mesajlarl a birlikt e verilmi ş bi r bilin ç ve iste k oluşturmanı n önemi , beni m görüşüm e göre , insanlar ı ço k fazl a bilgiyle buluştura n yarı m günlü k y a d a ta m günlü k eğitimlerde n ço k daha fazladır .

Bu oturumları n üzerind e durulması , tü m çalışanları n sık ı sıkıy a uyduğu güvenli k alışkanlıklar ı olmadığ ı durumd a şirket e v e bireyse l olarak çalışanlar a gelebilece k zararları n değerlendirildiğin i göstermek - tedir. Belirl i güvenli k uygulamaların ı öğrenmekte n dah a d a önemlisi ; çalışanların, güvenli k adın a kişise l sorumlulu k almalar ı konusund a teşvik edilmeleridir .

Çalışanların rahatlıkl a sınıflard a toplanamadığ ı durumlard a şirket , videolar, bilgisaya r tabanl ı eğitimler , çevrimiç i dersle r ya da basıl ı malzemeler gib i farkl ı bilgilendirm e yöntemler i kullanara k bilinçlendirm e eğitimleri geliştirmey i d e gö z önünd e tutmalıdır .

ilk kıs a oturumda n sonra , belirl i açıkla r v e şirkettek i konumların a göre saldır ı teknikler i konusund a çalışanlar ı eğitece k dah a uzu n otu - rumlar geliştirilmelidir . Hatırlatm a eğitimler i yıld a e n a z bi r ke z zorunl u olmalıdır. Tehdidi n boyut u v e insanlar ı sömürme k içi n kullanıla n yön - temler sürekl i değişmektedir , b u yüzde n programı n içeriğ i d e sürekl i güncellenmelidir. Dahası , insanları n bilinçliliğ i v e uyanıklığ ı zama n içinde azalır ; b u nedenl e güvenli k ilkelerin i vurgulama k içi n eğitimi n düzenli aralıklarl a tekrarlanmas ı gerekir . B u noktad a dikkatle r yine , belirli tehditleri n v e toplu m mühendisliğ i yöntemlerini n üzerind e olduğ u kadar, çalışanlar ı güvenli k kurallarını n önemin e inandırma k v e kurallar a bağlı kalmay a teşvi k etme k üzerind e d e olmalıdır .

Yöneticiler altlarınd a çalışanlar a güvenli k kurallar ı v e süreçlerin e aşina olmalar ı v e güvenli k bilinçlendirm e programın a katılmalar ı içi n yeterince zama n tanımalıdırlar . Çalışanları n kend i istedikler i zama n güvenlik kuralların ı öğrenmeler i y a d a eğitimler e katılmalar ı beklene - mez. Yen i iş e girenler e is e i ş sorumlulukların ı almada n önc e güvenli k kurallarını v e basıl ı güvenli k uygulamaların ı gözde n geçirme k içi n yeter - li zama n verilmelidir .

Kurum içind e konumlar ı değişere k hassa s bilgiler e y a d a bilgisaya r

sistemlerine erişim i gerektire n bi r iş e geçe n çalışanların , doğa l olarak , yeni sorumlulukların a uygu n olara k tasarlanmı ş güvenli k eğitim i prog - ramını tamamlamalar ı gerekir . Örneğin , bi r bilgisaya r işletmen i siste m yöneticisi olurs a y a d a bi r danışm a görevlisi , idar î yardımc ı olurs a on a yeniden eğiti m verilmes i şarttır .

Eğitimin İçerig i

Temele indirgendiklerind e tü m toplu m mühendisliğ i saldırılar ı ayn ı unsuru kullanırlar : Aldatma . Saldırganı n bi r çalışa n y a d a hassa s bil - gilere ulaşmay a vey a bilgisayarla r v e bilgisaya r donanımlar ı kullanılara k yapılan işle r konusund a kurban a talima t vermey e yetkil i başk a bi r kiş i olduğuna kurba n inandırılır . B u saldırıları n heme n heps i hede f ola n çalışanın ik i şe y yapmasıyl a boş a çıkarılabilir :

• istekt e buluna n kişini n kimliğin i kontro l etmekle : B u kiş i gerçek -

ten olduğun u söylediğ i kiş i mi ?

• Kişini n yetkil i olu p olmadığın ı kontro l etmekle : Kişini n b u bilgiy i

öğrenmeye ihtiyac ı va r m ı y a d a böyl e bi r istekt e bulunma k içi n

yetkili mi ?

Eğer bilinçlendirm e eğitim i programlan , he r çalışanı n davranışların ı bu kriterler e aykır ı ola n tü m istekler i sorgulama k konusund a tutarl ı ola - cak şekild e değiştirebilirse , o zama n toplu m mühendisliğ i saldırılarıyl a ilişkilendirilebilecek ris k büyü k ölçüd e azaltmı ş olur .

İnsan davranışların a v e toplu m mühendisliğ i tekniklerin e odaklana n güvenlik bilinçlendirm e v e eğiti m programlarınd a bulunabilece k kul- lanışlı bilgile r arasınd a şunla r ye r alabilir :

« Saldırganları n insanlar ı aldatma k içi n toplu m mühendisliğ i

becerilerini nası l kullandıklarını n bi r açıklaması ,

• Toplu m mühendislerini n amaçların a ulaşma k içi n kullandıklar ı

yöntemler,

• Olas ı bi r toplu m mühendisliğ i saldırısını n nası l farkedileceği ,

• Şüphel i bi r isteğ i değerlendirm e süreçleri ,

• Toplu m mühendisliğ i girişimlerini n y a d a başarıl ı saldırıları n ne -

reye habe r verileceği ,

İNİ V j I I Güvenlik bilinci v e eğitimi hiç bir zaman kusursuz olmayacağı için derinlemesine bir savunma oluşturabilmek için mümkün olduğu kadar güvenlik teknolojisi kullanmaya çalışın. Bu, güvenlik önlemlerinin çalışan- lardan çok, teknoloji tarafından alınmasıdır. Örneğin, işletim sistemi, çalışanların internetten dosya indirmesini ya da kısa ve kolay parolalar seçmesini engelleyecek şekilde ayarlanabilir.

• Kişini n sahi p olduğun u iddi a ettiğ i konumun a v e önemin e bak -
maksızın şüphel i bi r istekt e buluna n herkes i sorgulamanı n
önemi,
• içlerindek i dürt ü karş ı taraf a yardımc ı olmalar ı gerektiğin i
söylese de , düzgü n bi r kimli k tespit i olmada n göz ü kapal ı kim -
seye güvenmemeler i gerektiğ i gerçeği ,
• Bi r bilg i y a d a işle m talebind e buluna n herhang i birini n kimliğin i
ve yetkisin i kontro l etmeni n önem i (Kimli k tespit i yöntemler i içi n
bakınız "Ona y v e Yetkilendirm e Süreçleri" , 16 . Bölüm) ,
• He r türl ü ver i sınıflandırm a sistemiyl e ilgil i bilgini n yanısır a has -
sas bilgiler i korum a süreçleri ,
• Şirketi n güvenli k kurallarını n v e süreçlerini n yer i il e bilg i v e şirke t
bilgi sistemlerin i korumadak i önemleri ,
• Kili t güvenli k kurallar ı v e anlamların a ilişki n bi r özet . Örneğin , he r
çalışanın tahmin i gü ç bi r parolay ı nası l oluşturacağın a ilişki n bil -
gilendirilmesi.

Tanım itibarıyl a toplu m mühendisliği , insanla r aras ı bi r çeşi t etkileşi m yöntemidir. Bi r saldırga n hedefin e ulaşma k içi n çeşitl i iletişi m yöntemler i v e teknolojilerini sı k sı k kullanacaktır . B u nedenl e iy i tasarlanmı ş bi r bi - linçlendirme programını n aşağıdakileri n tümün ü y a d a bi r kısmın ı içerme - si gerekmektedir :

• Bilgisaya r v e sesl i mesa j parolalarıyl a ilgil i güvenli k süreçleri ,
• Hassa s bilgileri n y a d a malzemeleri n verilmesin e yöneli k süreç ,
• Aralarınd a virüslerin , solucanları n v e Truv a Atlarını n d a olduğ u
kötü huyl u yazılımlar a karş ı alınaca k önlemler i d e içerece k şe -
kilde e-post a kullanım ı kuralları ,

• Yak a kart ı takma k gib i fizikse l güvenli k zorunlulukları ,

• Binad a kar t takmaya n kişiler i sorgulam a yükümlülüğü ,

• Sesl i mesa j kullanım ı içi n e n doğr u güvenli k uygulamaları ,

« Bilgileri n sınıflandırmasını n nası l yapılacağ ı v e hassa s bilgile '

korumak içi n alınaca k önlemler ,

• Hassa s belgeleri n v e gizl i dosyala r içere n y a d a bi r zamanla "

içermiş bilgisaya r taşınabili r ortamlarınını n doğr u bi r şekild e silir -

mesi,

Eğer şirket , toplu m mühendisliğ i saldırıların a karş ı savunmasını " etkinliğini ölçme k içi n delm e test i yapmay ı planlıyorsa , çalışanlar ı t _ uygulamadan haberda r ede n bi r uyar ı yapmalıdır . Böyl e bi r test " parçası olara k saldırganları n yöntemlerin i kullana n birini n telefo n y a e s

başka bi r ara ç kullanara k iletişim e geçebileceğin i çalışanlarınızı n bilmesini sağlayın . B u testleri n sonuçlarını , çalışanlar ı cezalandırma k için değil , baz ı alanlardak i e k eğiti m ihtiyacın ı belirleme k içi n kullanın .

Yukarıdaki türr.-maddelerl e ilgil i ayrıntılar ı 16 . bölümd e bulabilirsiniz .

Ölçüm

Şirketiniz, bilgisaya r sistemin e erişi m hakk ı tanımada n önc e çalışan - ların güvenli k bilinçlendirm e eğitimind e sunula n bilgiler e hakimiyetin i ölçmek isteyebilir . Eğe r çevrimiç i yapılaca k testle r tasarlarsanız , pe k çok sına v değerlendirm e yazılımı , güçlendirilmes i gereke n eğiti m alan - larını belirleme k içi n tes t sonuçların ı çabuca k değerlendirebilir .

Şirketiniz bi r ödü l v e çalışanını teşvi k amacıyl a güvenli k eğitimin i tamamladığını göstere n bi r sertifik a sunmay ı d a düşünebilir .

Programı tamamlamanı n kalıplaşmı ş bi r sonuc u olarak , programd a öğretilen güvenli k kuralların a v e ilkelerin e uyacağın a dai r he r çalışan - dan bi r taahhü t belgesin i imzalamasını n istenmesin i öneririm . Araştırmalara göre , böyl e bi r belg e imzalayara k bağlılığın ı göstere n kişi , süreçlere uyma k konusund a dah a ço k çab a gösterebiliyor .

Sürekli Bilin ç

Pek ço k insa n bili r ki , öneml i konulard a bile , öğrenilenler , düzenl i olarak tekrarlanmadıklar ı sürec e yo k olm a eğilimindedirler . Çalışanları n toplum mühendisliğ i saldırıların a karş ı korunma k konusund a hızların ı kaybetmemeleri içi n bi r sürekl i bilin ç program ı önemlidir .

Güvenliği, çalışa n düşünc e zincirini n e n önünd e tuta n yöntemlerde n biri d e bilg i güvenliğin i he r şirke t çalışan ı içi n bi r i ş sorumluluğ u olara k tanımlamaktır. Bu , çalışanları n şirketi n gene l güvenliğindek i ca n alıc ı rollerini anlamaların a yardımc ı olacaktır . Aks i takdird e "güvenli k beni m işim değil " türünde n güçl ü bi r eğili m oluşacaktır .

Bir bilg i güvenliğ i programını n gene l sorumluluğ u çoğunlukl a güvenli k birimindeki y a d a bilg i işle m birimindek i birin e verils e de , bi r bilg i güvenliğ i bilinçlendirme programını n geliştirilmes i işi , büyü k olasılıkl a eğiti m biri - minin orta k bi r projes i olara k e n iy i şekild e yapılandırılmı ş olacaktır .

Sürekli bilin ç programını n yaratıc ı olmas ı gereki r v e iy i güvenli k alışkanlıkları konusund a çalışanlar a sürekl i hatırlatıc ı güvenli k mesajlar ı iletmek içi n mümkü n ola n he r kanal ı kullanmalıdır . Yöntemler , program ı geliştirip uygulamay a koyaca k insanları n haya l edebildiğ i ölçüd e yen i kanalların yan ı sır a S"o r türl ü gelenekse l kanalda n d a yararlanmalıdırlar . Geleneksel reklamcılıkt a olduğ u gib i eğlencel i v e akıllıc a oim&la n iş e

yarar. Mesajlardak i sö z sıralarını n değiştirilmes i d e aşinalı k yaratı p gö z ardı edilmelerin i engeller .

Bir sürekl i bilin ç programını n içeriğind e bulunabilecekle r şunla r olabilir :

• B u kitabı n bire r kopyasını tü m çalışanlar a vermek .

• Şirke t bültenin e bilg i sağlayıc ı unsurla r koymak : Makaleler , kut u

içine yazılmı ş hatırlatmala r (tercihe n kısa , dikka t çekic i noktala r

şeklinde) y a d a karikatürle r olabilir .

• Ayı n Güvenli k Çalışanı'nı n bi r resmin i koymak .

• Çalışanları n gittikler i yerler e posterle r asmak .

« Bülte n panoların a duyurula r asmak .

• Maa ş bordr o zarfların a broşürle r koymak .

• Hatırlatm a amaçl ı e-postala r göndermek .

• Güvenlikl e ilişkil i ekra n koruyucula r kullanmak .

• Sesl i mesa j sistem i aracılığıyl a güvenliğ i hatırlata n duyurula r

yapmak.

« Üzerinde , "Siz i araya n gerçekte n olduğun u iddi a ettiğ i kiş i mi? "

gibi şeyle r yaza n yapışkanl ı etiketle r bastırmak .

• Bilgisayar a bağlanırken , "Eğe r e-postayl a gizl i bilgile r gönderi -

yorsanız, mutlak a şifr e koyun" , gib i hatırlatm a mesajlarını n çık -

ması içi n ayarlamala r yapmak .

• Güvenli k bilincin i çalışa n performan s raporlarını n v e yıllı k değer -

lendirmelerin ayrılma z bi r parças ı durumun a getirmek . • İntranete , çalışanları n ilgisin i çekece k karikatürler , fıkrala r y a d a

başka şeyle r biçimind e güvenli k bilinc i hatırlatıcılar ı koymak . • Kafeteryad a sı k sı k farkl ı bi r güvenli k unsurun u hatırlata n bi r

elektronik mesa j tahtas ı kullanmak .

• Dosyala r v e broşürle r dağıtmak .

• Dikka t çekic i ayrıntıla r düşünülebilir , örneği n kafeteryad a ücret -

siz fa l kurabiyeler i dağıtılabili r v e he r birind e fa l yerin e bi r güven -

lik hatırlatıcıs ı olabilir .

Tehlike he r zama n var ; hatırlatıcıları n d a he r zama n va r olmas ı gerekir.

Benim Bunda n Çıkarı m Ne ?

Güvenlik bilinçlendirm e v e eğiti m programların a e k olarak , işleye n ve iy i tanıtılmı ş bi r ödüllendirm e sistemin i d e cidd i şekild e öneririm . Bi r toplum mühendisliğ i saldırısın ı tespi t edi p önlemi ş y a d a bilg i güvenliğ i

programının başarısın a büyü k bi r katkıd a bulunmu ş çalışanlarınız a teşekkür etmelisiniz . Ödü l programını n varlığ ı güvenli k bilinçlendirm e oturumlarında tü m çalışanlar a anlatılmal ı v e güvenli k ihlaller i tü m kuru - luşa geni ş bi r şekild e duyurulmalıdır .

işin diğe r yüzünd e insanlar , iste r dikkatsizlikte n iste r direnmekte n olsun, bilg i güvenliğ i kuralların a uymamanı n sonuçlarını n d a farkınd a olmalıdırlar. He r n e kada r hepimi z hat a yapsa k d a güvenli k kurallarını n sürekli ihlal i d e ho ş karşılanmamalıdır .

ŞİRKET BİLG İ GÜVENLİĞ İ KURALLARI ÖNERİLER İ

FBl'in yaptığ ı v e Associate d Press'i n Nisa n 2002'd e yayınladığ ı bi r araştırmanın sonuçların a bakılırsa , büyü k şirketleri n v e devle t kurum - larının ond a dokuz u bilgisaya r kırıcılarını n saldırısın a uğramış . İlgin ç bi r şekilde araştırm a he r ü ç şirkette n yalnızc a birini n saldırılar ı bildirdiğin i ya d a kamuoyun a açıkladığın ı ortay a çıkarmış . Bi r saldırıy a kurba n git - tikleri konusund a susku n kalmalar ı mantıkl ı olabilir . Müşterilerini n güvenini yitirmeme k v e şirketi n açıklarını n olabileceğin i öğrene n saldır - ganların yen i saldırılarını engelleme k içi n çoğ u işletme , bilgisaya r güvenliğine yöneli k saldırılar ı kamuoyun a açıklamazla r oiayların ı açı k bir şekild e rapo r etmezler .

Görünüşe göre , toplu m mühendisliğ i saldırılarıyl a ilgil i hi ç istatisti k yok; olsayd ı d a sayıla r oldukç a güvenilme z olurdu . Çoğ u durumda , bi r şir - ket, bi r toplu m mühendisini n bilgiy i n e zama n çaldığın ı hiçbi r zama n bile - mez v e b u yüzde n pe k ço k saldır ı far k edilme z v e rapo r edilmede n kalır .

Toplum mühendisliğ i saldırılarını n çoğun a karş ı etkil i önlemle r alı - nabilir. Doğruy u söyleme k gerekirs e kuruluştak i herke s güvenliği n öne - mini anlamadığ ı v e şirke t güvenli k kuralların a uyu p bun u işini n bi r parçası olara k kabul etmediğ i sürece , toplu m mühendisliğ i saldırıla n he r zaman şirketle r içi n büyü k bi r tehlik e olmay a deva m edeceklerdir .

Aslında, güvenli k açıkların ı kapama k içi n teknoloji k silahları n gelişmesi, tescill i şirke t bilgilerin e ulaşma k y a d a şirke t ağın a girme k içi n insanları kullana n toplu m mühendisliğ i saldırıların ı kesinlikl e cidd i ölçüd e sıklaştıracak v e ortam , bilg i hırsızla n içi n dah a çekic i bi r ha l alacaktır . Bi r sanayi casus u doğa l olara k amacın a ulaşm a işin i e n kola y v e e n düşü k fark edilm e tehlikes i ola n yolda n yapacaktır , işi n doğrusu , bilgisaya r sis - temlerini v e ağın ı e n so n çıka n güvenli k teknolojilerin i kullanara k koruya n bir şirket , hedeflerin e ulaşma k içi n toplu m mühendisliğ i stratejilerini , yön - temlerini v e taktiklerin i kullana n saldırganlarda n gelece k saldırılar a dah a çok maru z kalm a tehlikesiyl e karş ı karşıy a kalacaktır .

Bu bölüm , toplu m mühendisliğ i saldır ı riskin i e n az a indirgeyece k şekilde tasarlanmı ş bell i kuralla r sunmaktadır . Kuralla r ta m olara k sadece tekni k açıkla n sömürmey e yöneli k saldırılar a hita p etmemekte - dirler. Güvenili r bi r çalışanı , saldırganı n hassa s şirke t bilgilerin e y a d a bilgisayar siste m v e ağların a erişebilmesin i sağlaya n bilgile r vermey e ya d a bi r i ş yapmay a kandırabilme k içi n oynana n oyunlar ı y a d a ön e sürülen bahaneler i d e kapsamaktadırlar .

Güvenlik Kural ı Nedir ?

Güvenlik kuralları , bilgiy i koruma k amacıyla , çalışa n davranışlar ı içi n yön göstericidi r v e olas ı güvenli k tehditlerin i bertara f etme k içi n etkil i kontroller geliştirilmesini n teme l taşıdır . B u kurallar , i ş toplu m mühendis - liği saldırılarını tespi t etmey e v e önlemeye gelinc e dah a d a öneml i olmaktadırlar.

Etkili güvenli k kontrolleri , iy i düzenlenmi ş kuralla r v e süreçlerl e çalışanları eğitere k yerleştirilir . Anca k şun u d a vurgulama k gereki r ki , tüm çalışanla r tarafında n sadakatl e uygulans a d a güvenli k kurallar ı he r toplum mühendisliğ i saldırısını n engelleneceğin i garant i etmezler . Amaç, dah a çok , risk i kabu l edilebili r düzey e indirebilmektir .

Burada sunula n kurallar , ta m anlamıyl a toplu m mühendisliğ i konu - larıyla ilgil i olmas a d a toplu m mühendisliğ i saldırılarınd a çoğunlukl a kul - lanılan teknikler i d e içermektedirler . Örneği n e-postalar ı açmakl a ilgil i kurallar bilgisaya r kırıcılarını n sı k sı k kullandığ ı bi r yönteml e ilgilidir . Saldırgan, kurbanı n bilgisayarınd a kontrol ü el e geçirmesin i sağlaya n kötü huyl u Truv a At ı yazılımların ı e-post a aracılığıyl a yükleyebilir .

Bir Progra m Oluşturmanı n Adımlar ı

Kapsamlı bi r bilg i güvenliğ i programı , iş e genellikl e ü ç şey i belirleyi p risk ölçüm ü yapara k başlar :

a Kurumu n bilg i varlıklarında n hangilerini n korunmas ı gerekir ?

• B u varlıklar a karş ı n e gib i tehditle r vardır ?

• B u olas ı tehditle r gerçekleştiğ i durumd a kurum a n e gib i zararla r

gelebilir?

Risk değerlendirmeni n öncelikl i amac ı hang i bilg i varlıklarını n acile n korunmaları gerektiğin i belirleme k v e maliyet-kâ r analiz i yapara k önle m almanın uygu n maliyetl i olu p olmadığın a bakmaktır . Dah a açı k ifad e etmek gerekirse , hang i varlıkla r e n önc e korum a altın a alınaca k v e b u varlıkları koruma k içi n n e kada r zama n harcanacaktır ?

Üst yönetimi n güvenli k kurallar ı v e bilg i güvenliğ i program ı geliştir - menin önemin i güçl ü bi r şekild e desteklemes i v e b u görüş ü paylaşmas ı önemlidir. Diğe r herhang i bi r şirke t programında olduğ u gibi , eğe r güvenlik program ı başarıl ı olacaksa , yöneti m yalnızc a bi r ona y imzas ı atmakla kalmamalı , şahse n örne k olara k bağlılığın ı göstermelidir . Çalışanlar, bilg i güvenliğini n şirke t faaliyetler i açısından ca n alıc ı olduğu, şirke t iç i bilgileri n korunmasını n şirke t varlığını n korunmas ı içi n önemli olduğ u v e çalışanları n işlerini n programı n başarısın a bağl ı ola - bileceği gerçeklerin e yönetimi n güçl ü bi r şekild e bağl ı olduğunu n bi - lincinde olmalıdırlar .

Bilgi güvenliğ i kuralların ı temiz e çekmekl e görevlendirilmi ş perso - nelin, kuralları n tekni k terimle r kullanılmada n yazılmas ı v e tekni k olmayan çalışanla r tarafında n rahatç a anlaşılabilmes i gerektiğin i anlamış olmas ı şarttır . Belgenin , he r kuralı n nede n öneml i olduğun u d a açıklaması gerekir ; aks i halde , çalışanlar , kurallar ı zama n kayb ı olara k görerek bi r kenar a itebilirler . Kuralla r büyü k olasılıkl a onlar ı yerleştir - meye yaraya n süreçlerde n dah a a z sıklıkt a değişeceğinde n kurallar ı kaleme ala n kişi , kurallar ı tanıta n bi r belg e oluşturmal ı v e süreçle r içi n de ayr ı bi r belg e açmalıdır .

Ek olarak , kurallar ı yaza n kişi , güvenli k teknolojilerinin iy i bilg i güvenliği uygulamaların ı oturtmakt a kullanılabileceğin i d e bilmelidir . Örneğin, çoğ u işleti m sistemi , kullanıc ı parolalarını n uzunlu k gib i baz ı özelliklere uyu p uymadıkların ı kontro l edece k şekild e ayarlanabilmekte - dir. Baz ı şirketlerd e kullanıcıları n progra m indirmes i işleti m sisteminde - ki yere l y a d a gene l ayarla r aracılığıyl a denetlenebilir . Kurallar , insan - kaynaklı kara r alm a mekanizmaların ı devr e dış ı bırakmay a kıyasl a dah a uygun maliyetl i olduğ u koşullarda , güvenli k teknolojileri kullanm a zorun - luluğunu d a getirmelidir .

Çalışanlar, güvenli k kuraların a v e süreçlerin e uymadıklar ı takdird e t oluşabilece k sonuçla r hakkınd a d a uyarılmalıdırlar . Kurallar a uyma -

manın karşılığ ı olara k bi r takı m uygu n cezala r yerleştirilmel i v e herkes e

duyurulmalıdır. Ayn ı zamanda , güvenli k uygulamalar ı konusund a

başarılı y a d a bi r güvenli k olayını farkedi p bildirmi ş çalışanla r içi n d e bi r

ödül sistem i oluşturulmalıdır . N e zama n bi r çalışa n bi r güvenli k ihlalin i

engellemekten ödü l alırsa , bu , tü m şirke t içind e -şirke t bültenind e çıka n

bir makal e şeklind e bil e olsa - duyurulmalıdır .

Güvenlik bilinçlendirm e programını n bi r amacı , güvenli k kurallarını n önemini v e b u kurallar a uymamakta n doğabilece k zarar ı anlatmaktır . İnsan yaradılış ı gereği , çalışanla r zama n zama n maku l gözükmeyen y a da zama n alıc ı gib i görüne n kurallar ı gö z ard ı edece k y a d a boşlukların - dan yararlanacaktır . Çalışanların , kurallar ı çevrelerinde n dolaşılaca k birer enge l gib i görme k yerine , kuralları n önemin i anlamalar ı v e uymay a istekli olmaların ı sağlama k yönetimi n sorumluluklar ı arasındadır .

Bilgi güvenliğ i kurallarını n değişme z kuralla r olmadığın ı belirtmekt e yarar vardır , i ş ortamlar ı değiştikçe , piyasay a yen i güvenli k teknolojiler i çıktıkça v e güvenli k açıklar ı evrimieştikç e kuralları n değiştirilmes i y a d a desteklenmesi gerekebilir . Düzenl i bi r gözde n geçirm e v e - güncellem e süreci devrey e alınmalıdır . Şirke t güvenli k kurallan m v e süreçlerin i intranet üzerinde n herkes e açı n y a d a b u tar z kurallar ı herkesi n ulaşa - bileceği bi r klasör e koyun . B u hareket , kuralları n v e süreçleri n dah a sı k okunma olasılığın ı artırı r v e çalışanları n bilg i

güvenliğiyl e ilgil i soruları - na dah a hızl ı yanı t bulmalar ı açısından etkil i bi r yönte m olur .

Sonuç olarak , eğitimlerdek i açıklar ı y a d a şirke t kura l v e süreçlerin e

uyumdaki eksikliğ i ortay a çıkarma k amacıyla , toplu m mühendisliğ i yön - tem v e taktikler i kullanılara k düzenl i delm e testler i v e açı k değer - lendirmeleri yapılmalıdır . Aldatıc ı delm e testler i uygulanmada n önc e b u tarz testleri n zama n zama n yapılacağ ı çalışanlar a duyurulmalıdır .

Bu Kuralla r Nası l Kullanılır ?

Bu bölümd e aytıntılarıyl a anlatıla n kurallar , tü m güvenli k risklerin i azaltması içi n öneml i olduğun a inandığı m bilg i güvenliğ i kurallarını n yal - nızca küçü k bi r parçasıdır . Bun a göre , burad a söz ü geçe n kuralları n kapsamlı bi r bilg i güvenliğ i kura l listes i olduğ u düşünülmemelidir . B u kurallar, dah a çok , şirketinizi n belirl i ihtiyaçların a uygu n olabilece k kap - samlı bi r güvenli k kurallar ı bütün ü oluşturabilme k içi n bi r temeldir .

Kuralları hazırlayanlar , şirketlerin e özgü , çevrelerin e v e i ş hedefle - rine uygu n kuralla r seçmelidirler . He r kuruluş , i ş gereksinimleri , yasa l yükümlülükleri, kuru m kültür ü ve kullandığ ı bilg i sistemlerin e gör e aşağıda anlatıla n kurallarda n ihtiyac ı olan ı alabilir , diğerlerin i bi r kenar a bırakabilir.

Her ver i sınıfındak i kuralları n n e kada r kat ı olacağıyl a ilgil i d e verile - cek kararla r vardır . Te k bi r binay a sığa n v e çalışanları n çoğunu n birbirin i tanıdığı küçü k bi r şirketin , telefo n edi p o şirkett e çalıştığın ı söyleye n bi r saldırgandan korkmasın a gere k yoktu r (anca k saldırgan , bi r satıc ı fir - madan aradığ ı ayağın a d a yatabilir) . Ayrıc a arta n riskler e karşı n raha t bi r kurum kültürün e sahi p bi r şirket , güvenli k hedeflerin e ulaşma k içi n öne - rilen kuralları n yalnızc a küçü k bi r bölümün ü kullanma k isteyebilir .

Veri Sınıflandırm a

Bir ver i sınıflandırm a politikas ı kuruluşu n bilg i varlıkların ı koruma k için önemlidi r v e hassa s bilgileri n yayılmasın ı denetleye n bi r sınıflandı"" - ma sistem i getirir . B u politika , tü m çalışanlar ı he r bilg i parçasını n has - saslık dereces i konusund a bilinçlendirere k şirke t bilgilerin i koruma k iç - bir çerçev e oluşturur .

Veri sınıflandırm a politikas ı olmada n çalışma k -bu , artı k günümüzc e pek ço k şirketi n olmazs a olmazıdır - kararları n çoğun u bireyse l düzeyc e çalışanlara bırakır . Doğa l olara k çalışa n kararları , bilgini n hassash î önemi v e değerinde n ço k büyü k ölçüd e öznel unsurlar a daya r - Çalışanlar bi r bilg i talebin e karşılı k vererek , bilgiy i bi r saldırganı n e ~ - rine tesli m edebilecekler i olasılığında n habersi z olduklar ı içi n d e t ; duyurulur.

Veri sınıflandırm a politikas ı pe k ço k düzeyden birind e değerl i c : - lerin sınıflandırılmas ı içi n yo l göstericidir . He r bilg i parça s ~ sınıflandırılmasıyla çalışanlar , hassa s bilgileri n kasıtsı z olara k şirker.e -

dışarı çıkmasın ı önleyece k bi r ver i kullanı m sürecin e uyabileceklerdir . Bu süreçle r çalışanları n hassa s bilgiler i yetkisi z kişiler e verme k içi n kandırılmaları olasılığını azaltacaktır .

Her çalışa n (norma l olara k bilgisaya r y a d a şirke t iletişi m ağların ı kullanmayanlar d a dahil) şirketi n ver i sınıflandırm a politikas ı konusund a eğitilmelidir. Şirke t işgücünü n -temizlikçiler , güvenli k görevlileri , fotokopicilerin yanısır a danışmanlar , taşeronla r v e hatt â stajyerle r d e aralarında olma k üzere - he r üyesini n hassa s bilgiler e erişim i olabile- ceğinden, herke s bi r saldırını n hedef i olabilir .

Yönetim, şirke t içind e halihazırd a kullanımd a ola n he r bilg i içi n bi r bilgi sahibi belirlemelidir . Diğe r şeyleri n yan ı sır a bilgi sahibi bilg i varlık - larının korunmasında n sorumludur . Bilgiy i korum a gereksinimin e gör e hangi derec e sınıflandırm a yapılacağın a o kara r veri r v e düzenl i olara k sınıflandırma derecelerin i yenide n değerlendiri r v e uygu n gördüğ ü değişiklikleri yapar . Bilgi sahibi, ver i korum a görevin i bi r vekile y a d a sorumluya d a devredebilir .

Sınıflandırmalar v e Tanımla r

Bilgi, hassaslığın a gör e değişe n sınıflandırm a düzeylerin e bölün - melidir. Bi r sınıflandırm a sistem i bi r ke z kuruldukta n sonr a bilgiy i yeniden sınıflandırma k zama n isteye n v e pahal ı bi r i ş halin e gelir . Örne k sınıflandırmamızda, orta-büyü k ölçekl i işletmeleri n çoğ u içi n uygu n ola - cak dör t sınıflandırm a düzey i seçtim . Hassa s bilgileri n sayıs ı ve çeşi - dine gör e işletmeler , belirl i bilg i çeşitlerin i d e kapsama k içi n yen i sınıflandırmalar ekleme k isteyebilirler . Dah a küçü k işletmelerd e ü ç düzeyli bi r sınıflandırm a sistem i yeterl i olacaktır .

Gizli: B u bilg i smıf ı e n hassa s olanıdır . Gizl i bilgile r yalnızc a kuru m iç i kullanım içindir . Çoğ u zama n kesinlikl e bilmes i şar t ola n sınırl ı sayıd a insan tarafında n bilinmelidir . Gizl i bilgi , herhang i bi r yetkisi z paylaşımı n şirkete, hissedarlara ve/vey a müşteriler e cidd i zararla r verebileceğ i bi r yapıdadır. B u bilgile r gene l olara k aşağıdak i gruplarda n birin e girerler : • Ticar i sırlar , tescill i kayna k kodları , tekni k y a d a işlevse l özellikle r

ya d a bi r rakibi n işin e yarayabilece k ürü n bilgiler i gib i bilgiler . • Halk a açılmamı ş finansa l y a d a pazarlamay a yöneli k bilgiler . • Gelecektek i i ş stratejiler i gib i şirketi n işler i içi n öneml i ola n diğe r

bilgiler.

Özel: B u sınıflandırma , kuru m içind e kullanılmas ı öngörüle n kişise l nitelikte - ki bilgiler i içerir . Öze l bilgini n yetkisi z dağıtım ı çalışanları n y a d a yetkisi z kişi - lerin (özellikl e toplu m mühendislerinin) elin e geçtiğ i zama n şirket e cidd i şe - kilde zara r verebilmektedir . B u tar z bilgileri n arasınd a çalışanları n tıbb î geçmişi, sağlı k yardımları , bank a hesa p bilgileri , ücre t geçmiş i y a d a halk a açı k olmayan diğe r kişise l tanımlamala r bulunmaktadır .

INVJ 1 1 "Dahili" olarak sınıflandırılmış bilgiler, güvenlik personeli tarafından sık sık "Hassas" olarak da adlandırılırlar, Ben Dahilî şeklinde kullanacağım çünkü terimin kendisi bilginin hitap ettiği kişileri tanımlıyor. Hassas terimini bir güvenlik sınıflandırması olarak değil de Gizli, Özel ve Dahili bilgilerinin tümünü anlatan bir terim olarak kullandım. Hassas, özellikle Genel olarak tanımlanmamış her türlü şirket bilgisine karşılık gelmektedir.

Dahilî: B u bilg i smıf ı kuramd a çalışa n herkes e rahatlıkl a dağıtılabilir . Dahilî bilgini n yetkisi z dağıtımını n çoğ u zama n şirkete , hissedarlara , i ş ortaklarına, müşteriler e y a d a çalışanlar a cidd i bi r zara r vermes i beklen - mez. Bun a karşın , toplu m mühendisliğ i becerilerin i kullanmakt a ust a ola n kişiler b u bilgiy i kullanara k yetkil i bi r çalışan , taşero n y a d a satıc ı firm a gibi davranı p hiçbi r şeyde n kuşkulanmaya n personel i hassa s bilgiler i ver - mesi doğrultusund a kandırabili r v e bu , şirke t bilgisaya r sistemlerin e yetki - siz bi r erişi m sağlanmasın a nede n olabilir .

Satıcı firmalara , taşeronlara , orta k şirketler e v e benzer i üçünc ü şahıslar a dahilî bilgi verilmede n önc e tarafla r arasınd a bi r gizlili k anlaşmas ı imza - lanmalıdır. Dahil î bilgile r genellikl e günlü k işlerd e kullanılan , dışarıy a ve - rilmemesi gereke n şirke t kurulu ş şemaları , a ğ bağlant ı numaralan , dahil î sistem adlan , uzakta n erişi m süreçleri , maliye t merkez i kodla n v e bunu n gibi herhang i bi r bilgiy i içerebilir .

Genel: Özellikl e kamuy a duyurma k üzer e belirlenmi ş bilgilerdir . Bası n açıklamaları, müşter i deste k iletişi m bilgile n y a d a ürü n broşürler i gib i b u tarz bilgile r herkes e serbestç e dağıtılabilir . Gene l olara k sınıflandırılmamı ş diğer tü m bilgileri n hassas bilgi olara k el e alınmas ı gerektiğ i unutulma - malıdır.

Sınıflandırılmış Ver i Terimler i

Sınıflandırmalarına gör e verile r bell i düzeylerdek i kişiler e dağıtıl - malıdırlar. B u bölümd e verile n baz ı kuralla r bilgini n onaylanmamış kişilere verilmesiyl e ilgilidir . B u ifadey i açma k gerekirs e onaylanmamış kişi, şirkett e hale n çalışmakt a y a d a bilgiy i alma k içi n doğr u konumd a olup olmadığını n y a d a güvenili r bi r üçünc ü şahsı n on a kefi l olu p olmadığının çalışa n tarafında n bilinmediğ i kişidir .

Bunun ta m ters i olan , güvenilir kişi, yüzyüz e karşılaştığınız , bilg i erişim i için yeterl i yetkiy e sahi p bi r şirke t çalışanı , müşter i y a d a şirke t danışman ı olarak tanıdığını z kişidir . Güvenilir kişi şirketinizl e uzu n süredi r çalışa n bi r şir - ketin eleman ı d a olabili r (örneğin , bi r müşteri , satıc ı y a d a sı r saklam a anlaş - ması imzalanmı ş bi r strateji k i ş ortağ ı gibi) .

Üçüncü şahı s kefaletinde , bi r güvenilir kişi, bi r kişini n i ş durum u v e kişinin bilg i y a d a i ş istemey e yetkil i olu p olmadığıyl a ilgil i kontro l veris ;

sağlar. Baz ı durumlard a b u kurallar , kefi l olduklar ı birinde n gele n bilg i y a da i ş taleplerin e karşılı k vermede n önc e güvenilir kişinin şirkett e çalış - maya deva m edi p etmediğin i d e doğrulamanız ı gerektirir .

Ayrıcalıklı hesap, teme l kullanıc ı hesabını n ötesind e bilgisaya r y a d a benzeri bi r ortam a erişi m izn i soran , siste m yönetic i hesab ı türünde n bi r hesaptır. Ayrıcalıkl ı hesaplar a sahi p ola n çalışanla r genellikl e kullanıc ı yetkilerini değiştirip , siste m işlevler i gerçekleştirebilirler .

Genel bölüm posta kutusu, bölü m adın a gene l bi r mesajl a açıla n bi r sesli mesa j kutusudur . Böyl e bi r kut u belirl i bi r bölümd e çalışanları n adlarını v e dahil i numaraların ı koruma k amacıyl a kullanılır .

Onay v e Yetkilendirm e Süreçler i

Bilgi hırsızları , gizl i şirke t bilgilerin e ulaşma k v e b u bilgiler i el e geçirmek içi n çoğunlukl a gerçe k çalışanlar , taşeronlar , satıcıla r y a d a i ş ortakları gib i davranara k aldatm a taktikler i kullanırlar . Etkil i bilg i güven - liğini sürekl i kılma k içi n bi r i ş yapmas ı y a d a hassa s bi r bilg i vermes i istenen bi r çalışan , arayanı n kimliğin i tespi t etmel i v e bi r istekt e bulun - ma yetkisini n olu p olmadığın ı onaylattırmalıdır .

Bu bölümd e önerile n süreçler , herhang i bi r iletişi m aracıyl a -telefon , faks y a d a e-posta - kendisinde n bi r şe y istenmi ş bi r çalışana , isteği n geçerli v e isteyeni n d e gerçe k olu p olmadığın ı belirlemekt e yardımc ı olmak üzer e tasarlanmışlardır .

Güvenilir Kişide n Gele n İstekle r

Bir güvenili r kişide n gele n i ş y a d a bilg i taleb i durumund a şunları n yapılması gerekebilir :

• Kişini n şirke t bünyesind e çalıştığını n y a d a sö z konus u sınıf a ai t

bilgilere erişi m koşulun u d a içere n bi r ilişkini n varlığını n kontro l

edilmesi. Bunu n amacı , ilişiğ i kesilmi ş çalışanların , satıcıların ,

taşeronların v e benze r kişileri n kendilerin i çalışıyo r olara k

göstermelerini önlemektir ,

• Kişini n bilm e gereksinimini n v e bi r i ş y a d a bilg i talebind e bulun -

maya yetkil i olu p olmadığını n kontro l edilmesi .

Onaylanmamış Bi r Kişide n Gele n İstekle r

Onaylanmamış bi r kiş i bi r istekt e bulunduğ u zaman , istekt e buluna n kişinin b u talept e bulunmay

a yetkil i olu p olmadığın ı belirleme k içi n uygun bi r ona y sürec i kullanılmalıdır . Özellikl e d e istek , bilgisayarla r y a da bilgisaya r donanımlarıyl a ilgiliyse . B u süreç , toplu m mühendisliğ i saldırılarının başarıl ı olmasın ı engelleme k içi n teme l bi r önlemdir . Eğe r

bu ona y süreçler i uygulanırsa , başarıl ı toplu m mühendisliğ i saldırını n sayısını büyü k ölçüd e azalacaktır .

Süreci maliye t artırıc ı y a d a çalışanları n on u boşvereceğ i kada r han - tal yapmamanı z d a önemlidir .

Aşağıda d a belirtildiğ i gib i ona y sürec i ü ç adımda n oluşur : • Kişini n olduğun u söylediğ i kiş i olu p olmadığını n kontro l edilmesi . • Tale p sahibini n hale n şirkett e çalıştığını n y a d a şirketl e bilm e

gereği oluşturabilece k bi r ilişkisini n olduğunu n belirlenmesi . • Kişini n ilgil i bilgiy i almay a y a d a ilgil i iş i tale p etmey e yetkil i olu p

olmadığının belirlenmesi .

Birinci Adım : Kimii k Tespit i

Önerilen ona y adımları , etkinliklerin e gör e aşağıd a sıralanmışlardır ; sayı n e kada r büyü k olurs a yönte m o kada r etkilidir . He r öğeyl e birlikte , ilgili yöntemi n zayıflığıyl a v e bi r toplu m mühendisini n çalışanlar ı kandırabilmek içi n b u yöntem i aşm a y a d a çevresinde n dolaşm a yoluy - la ilgil i bi r açıklam a bulunmaktadır .

1. Araya n Kimliğ i (b u özelliği n şirke t telefo n sistemind e va r

olduğunu varsayıyoruz) : Araya n numaray a bakarak , aramanı n

şirket içinde n m i yoks a dışında n m ı geldiğ i bulunabili r v e

arayanın verdiğ i kimliği n görüne n a d v e telefon numarasıyl a

uyuşup uyuşmadığın a bakılır .

Zayıflığı: Dışarıda n gele n aramay a ai t araya n kimliğ i bilgileri ,

dijital telefon hizmetlerin e bağl ı bi r PB X y a d a telefo n santralın a

erişimi ola n herhang i bir i tarafında n saht e bilgilerl e değiştirilebilir .

2. Ger i Arama : İste k sahibi , şirke t rehberinde n bulunu r v e

rehberde geçe n dahil î numar a aranara k istekt e buluna n kişini n

gerçekten şirkett e çalışı p çalışmadığ ı kontro l edilir .

Zayıflığı: Çalışan , listed e geçe n şirke t dahil î numarasın ı kontro l

amaçlı olara k aradığ ı zaman , yeterl i bilgiy e sahi p bi r saldırgan ,
aramayı kend i dı ş hattın a aktarılaca k şekild e yönlendirebilir .

3. Kefi l Olunması : iste k sahibin e kefi l olmu ş bi r güvenilir kişi istek -
te buluna n kişini n kimliğin i onaylamı ş olur .

Zayıflığı: Başk a bir i gib i davrana n saldırganlar , farkl ı bi r çalışan ı
kimliklerinin doğruluğun a çoğunlukl a inandırabilirle r v e o çalışa -
nın kendilerin e kefi l olmasın ı sağlayabilirler .

4. Gizl i Orta k Bilgi : Kuru m çapınd a kullanılan , parol a y a d a gün -
lük şifr e gib i bi r gizl i orta k bilgi .

Zayıflığı: Eğe r gizl i orta k bilgiy i ço k kiş i bilirse , saldırganı n on u
öğrenmesi dah a kola y olur .

5. Çalışanı n Yöneticisi/Müdürü : Çalışanı n bağl ı olduğ u yönetic i aranır v e ona y istenir .

Zayıflığı: Eğe r yöneticini n numaralarını istekt e buluna n şahı s vermişse, çalışa n o numaray ı aradığınd a ulaştığ ı kiş i gerçe k yönetici değ i l aslınd a saldırganı n su ç ortağ ı olabilir .

6. Güvenl i e-posta : Dijita l olara k imzal ı bi r mesa j istenir .

Zayıflığı: Eğe r saldırga n zate n çalışanı n bilgisayarın a girmi ş v e çalışanın imz a parolasın ı alabilme k içi n tu ş girişlerin i kaydeden bir progra m yüklemişse , b u durumd a çalışanda n geliyormu ş gib i görünen dijita l imzal ı bi r e-post a gönderebilir .

7. Ses i Şahse n Tanımak : Kendisin e iste k gele n kişini n iste k sahibiyle dah a öncede n çalışmı ş olmas ı (tercihe n yü z yüze) , bi r güvenilir kişi olduğunda n emi n olmas ı v e kişini n sesin i telefon - dan tanıyaca k kada r kişiy i tanıması .

Zayıflığı: B u oldukç a güvenl i bi r yöntemdi r v e bi r saldırga n tarafından kola y kola y aşılamaz , anca k kendisin e iste k gele n kiş i arayanı tanımıyors a y a d a dah a önc e onunl a hi ç konuşmamışs a bu yönte m bi r iş e yaramaz .

8. Değişke n Parol a Çözümü : İste k sahib i güvenli kimlik gib i bi r değişken parol a çözümüyl e kendin i tanıtır .

Zayıflığı: B u yöntem i aşma k içi n saldırganın , he m değişke n parola cihazlarında n birini , he m d e cihazı n ai t olduğ u çalışanı n kimlik numarasın ı el e geçirmes i gereki r y a d a bi r çalışan ı cihazı n

üzerinden bilgiy i okumas ı v e kimli k numarasın ı vermes i içi n

kandırabilir.

9. Kimliğiyl e Birlikt e Gele n Kişi : istekt e buluna n kiş i şahse n geli r

ve tercihe n resiml i persone l kartın ı y a d a başk a uygu n bi r kimli k

kartını gösterir .

Zayıflığı: Saldırganla r sı k sı k bi r çalışanı n kartın ı çalabili r y a d a

gerçek gib i görünen bi r sahtesin i yapabilirler . Anca k saldırganla r

çoğunlukla b u yaklaşım ı kullanmazla r çünk ü bi r yer e şahse n git-

mek saldırgan ı büyü k bi r tanınm a v e alıkonm a tehlikesin e sokar .

İkinci Adım : İ ş Dorumunu n Kontrol ü

En büyü k bilg i güvenliğ i tehdid i bi r profesyone l toplu m mühendisin - den y a d a becerikl i bi r bilgisaya r kırıcısında n gelmez . Ço k dah a yakın - daki birinden , kıs a sür e önc e işte n atılmış , intika m alma k isteye n y a d a şirketten çaldığı bilgiler i kullanara k kend i işin i kurmay ı ümi t ede n çalışandan geli r (B u süreci n başk a bir i türünün , satıcı , danışma n y a d a sözleşmeli işç i gib i şirketinizl e farkl ı bi r i ş ilişkis i ola n kişile r içi n d e kul - lanılabileceğini unutmayınız) .

Başka birin e Hassa s bilgile r vermede n y a d a bilgisaya r v e bilgisaya r donanımlarıyla ilgil i başk a birini n verdiğ i talimatlar a uymada n önc e konuştuğunuz kimseni n sizinl e ayn ı şirkett e çalışı p çalışmadığın ı ş u yöntemlerden birin i kullanara k kontro l edebilirsiniz .

Personel Telefo n Rehberinde n Kontrol : Eğe r şirket , çalışan - ların listesini n titizlikl e tutulduğ u bi r çevrimiç i telefo n rehber i bulunduruyorsa, arayanı n b u listed e olduğunda n emi n olun .

Arayanın Yöneticisinde n Kontrol : Arayanı n yöneticisini , arayanın verdiğ i numarada n değil , şirke t rehberind e geçe n numarasından arayın .

Arayanın Biri m y a d a İ ş Gurubunda n Kontrol : Arayanı n biri - mini y a d a i ş grubun u arayı n v e orad a çalışa n herhang i birinde n söz konus u kişini n orad a çalışmakt a olu p olmadığın ı öğrenin .

Üçüncü Âdım : Bilm e Gereğini n Kontrol ü

istekte buluna n kişini n hale n şirkett e çalışı p çalışmadığın ı y a d a şir - ketinizle bi r ilişkis i kalı p kalmadığın ı kontro l etmeni n yanısıra , bi r de , istek sahibini n istediğ i bilgiy i tale p etmey e y a d a bilgisayarlar ı vey a bil - gisayar donanımların ı etkileyece k belirl i işlemler i tale p etmey e yetkil i olup olmadığ ı konus u vardır .

Bunun kontrol ü ş u yöntemlerde n bir i kullanılara k yapılabilir :

İşyeri Unvan/İ ş Gurubu/Sorumlulukla r Listelerin e Başvurun : Bi r şirket hang i çalışanları n n e tü r bilgiler i almay a yetkil i olduğun u içere n listeler çıkarara k yetkilendirm e bilgilerin e hızl ı erişi m sağlayabilir . B u lis - teler çalışa n unvanına , birimin e v e i ş gurubuna , sorumluluklar a y a d a başka veriler e gör e sıralanmı ş olabilir . B u tar z listeleri n çevrimiç i tutul - ması v e sürekl i güncellenere k yetkilendirm e bilgilerin e hızl ı erişi m sağlaması gerekir . Çoğunlukl a bilgi sahipleri, denetimler i altınd a ola n bilgilere erişilebilmes i içi n listeleri n oluşturulmasında n ve güncellen - mesinden sorumludurlar .

Bir Yöneticide n Ona y Alın : Bi r çalışan , isteğ i yerin e getirme k üzer e onay alma k içi n kend i yöneticisiyl e y a d a iste k sahibini n yöneticisiyl e bağlantıya geçer .

IV| v ^ I * B u tarz listelerin toplum mühendisine davetiye çıkarmak olduğu da göz önünde bulundurulmalıdır. Düşünün: Eğer bir şirketi hedef- leyen bir saldırgan şirketin böyle listeler tuttuğunu öğrenecek olursa bir tanesini ele geçirmek için bir nedeni olacaktır. Ele geçirdikten sonra da bu tarz listeler saldırgana pek çok kapı açarlar ve şirket için ciddi bir tehlike V.oluştururlar. J

Şirket Bilg i Güvenliğ i Kurallar ı Öneriler i 25 1

Bilgi Sahibinde n y a d a Sorumlusunda n Ona y Aıın : Belirl i bi r kişinin bilgiy e erişim i olu p olmayacağıyl a ilgil i so n sö z hakk ı bilgi sahibi- nindir. Bilgisaya r tabanl ı erişi m kontro l süreci , va r ola n i ş tanımlarına uygun bilgiler e erişm e talebini n onay ı içi n çalışanı n kend i yöneticisin i aramasıdır. Eğe r böyl e bi r tanı m yoksa , ilgil i bilgi sahibini arayı p izi n istemek yöneticini n sorumluluğudur . B u emir-komut a zincirin e uyulmas ı gerekir, yoks a bilgi sahipleri sı k sı k gele n bi r tale p akının a uğrarlar .

Tescilli Bi r Yazılı m Paket i Aracılığıyl a Ona y Alın : Rekabetç i bi r ortamda çalışa n büyü k bi r şirketi n bilm e gereğ i yetkilerin i vere n tescill i bir yazılı m paket i geliştirmes i kullanışl ı olabilir . Böyl e bi r veritabanı , çalışan adların ı v e gizl i bilgiler e erişi m yetkilerin i tutar . Kullanıcıla r he r çalışanın erişi m yetkilerin i göremezle r am a onu n yerin e istekt e buluna n kişinin adın ı v e istene n bilgini n tanımlayıcısın ı girebilirler . Dah a sonr a yazılım, arana n kişini n ilgil i bilgiler i almay a yetkil i olu p olmadığın a dai r bir sonu ç çıkarır . B u seçenek , değerli , öneml i y a d a hassa s bilgiler e erişim yetkisin e sahi p persone l listelerini n çalınm a tehlikesin i bertara f eder.

Yönetim Kurallar ı

Aşağıdaki kuralla r yönetic i seviyesindek i çalışanlarl a ilgilidir . Ver i Sınıflandırılması, Bilg i Verilmesi , Telefo n İdares i v e Çeşitl i Kuralla r gib i konulara bölünmüşlerdir . He r kura l sınıf ı kuralları n raha t tanımlana - bilmeleri içi n kendin e özg ü bi r sayılandırm a içermektedir .

Veri Sınıflandırm a Kurallar ı

Veri Sınıflandırma, şirketinizi n hassa s verilerini n nası l sınıflandırıl - dığına v e b u bilgiler e kimleri n erişi m yetkisini n olmas ı gerektiğin e değinir. .

1-1 Ver i sınıflandırmas ı yapı n

Kural: Tü m değerli , hassa s y a d a öneml i i ş bilgiler i ilgil i bilgi sahibi ya d a vekili tarafında n bi r sınıflandırmay a tutulmalıdır .

Açıklamalar/Notlar: ilgil i bilgi sahibi y a d a vekili i ş hedeflerin e ulaş - mak içi n düzenl i olara k kullanıla n herhang i bi r bilgiy i uygu n ver i sınıfın a yerleştirecektir. Bilgi sahibi, b u tar z bilgiler e kimleri n erişebileceğini v e bu bilgilerl e nele r yapılabileceğin i denetler . Bilgi sahibi, sınıflandırmay ı yeniden yapabili r v e düzenl i olara k sınıflandırmanı n yenilenmes i içi n bi r zaman belirleyebilir .

Başka bi r şekild e sınıflandırılmamı ş he r bilg i hassas olara k sınıflandırılmalıdır.

1 - 2 Sınıflar a gör e kullanm a süreçler i çıkarı n

Kural: Şirke t he r sını f bilgini n verilmesin e yöneli k süreçle r oluşturmalıdır .

Açıklamalar/Notlar: Sınıflandırmala r yapıldıkta n sonra , bilgini n çalışanlara v e dışarda n kişiler e verilmesiyl e ilgili , dah a önc e b u bölümde Ona y v e Yetkilendirm e konusund a anlatıldığ ı gib i süreçle r oluşturulmalıdır. .

1 - 3 Tü m öğeler i işaretleyi n

Kural: Gizli , öze l ya da dahil î bilg i içere n he m basıl ı malzemeleri , hem d e bilgisaya r saklam a ortamların ı ilgil i ver i sınıflandırmasın ı gösterecek açı k bi r şekild e işaretleyin .

Açıklamalar/Notlar: Basıl ı belgelerin , üstünd e göz e çarpa n bi r ver i sınıfi işaret i ola n bi r kapa k sayfas ı olmalıdı r v e ver i sınıfi , belg e açıldığında görülece k şekild e he r sayfad a bulunmalıdır .

İlgili ver i sınıflarıyl a kolaylıkl a işaretlenemeye n tü m elektroni k dosyalar, (veritaban ı y a d a ha m ver i dosyaları) , uygunsu z bi r şekild e dağıtılmasını, değiştirilmesini , yo k edilmesin i y a d a erişileme z durum a getirilmesini önleme k içi n erişi m denetimleriyl e korunmalıdırlar .

Disketler, bantla r v e CD-ROM'la r gib i tü m bilgisaya r araçlarının , içlerindeki e n üs t sını f veriy e gör e işaretlenmeler i gerekmektedir .

Bilginin Verilmesi

Bilgi verilmesi , ki m oldukların a v e bilm e gereklerin e bakılara k bil - ginin çeşitl i şahıslar a verilmesin i kapsar .

2-1 Çalışa n kimliğini n tespit i sürec i

Kural: Gizl i y a d a hassa s bilgileri n verilmesin i y a d a herhang i bi r bil - gisayar donanımını n y a d a yazılımını n kullanılmasın ı içere n bi r işi n yapılmasından önc e kişini n kimliğinin , i ş durumunu n v e yetkilerini n kontrol edilebilmes i içi n çalışanları n kullanabileceğ i kapsaml ı süreçle r şirket tarafında n oluşturulmalıdır .

Açıkiamalar/Notlar: Şirketi n büyüklüğ ü v e güvenli k ihtiyaçların a uygun olarak , kimli k tespit i için , gelişmiş güvenli k teknolojiler i kullanıl - malıdır. E n iy i güvenli k uygulaması , tanımlam a anahtarın ı gizl i orta k bil - giyle birlikt e kullanara k istekt e buluna n kişiler i doğr u bi r şekild e tanımla - maktır. B u uygulama , risk i büyü k ölçüd e azalts a d a baz ı işletmele r içi n maliyeti ço k yükse k olabilir . Bu koşullard a şirket , günlü k bi r parol a ya da şifre gib i tü m şirke t çapınd a geçerl i bi r gizl i orta k bilg i kullanabilir .

2-2 Bilgini n üçünc ü şahıslar a verilmes i

Kural: Bi r diz i kendin i kanıtlamı ş bilg i verm e sürec i yürürlüğ e kon - malı v e tü m çalışanla r b u süreçler i izlemeler i konusund a eğitilmelidirler .

Şirket Bilg i Güvenliğ i Kurallar ı Öneriler i 25 3

Açıklamalar/Notlar: Dağıtı m süreçlerini n gene l olara k şunla r içi n oluşturulması gerekir ;

• Şirke t için e verilece k bilgiler ,

• Danışmanlara , geçic i işçilere , stajyerlere , şirketl e alıcı-satıc ı

ilişkisi y a d a strateji k ortaklı k anlaşmas ı ola n kuruluşları n

çalışanlarına v e bunu n gibi , şirketl e oturmu ş bi r ilişkis i ola n kuru -

luşların çalışanların a bilgini n verilmesi ,

• Şirke t dışın a verilece k bilgiler ,

• Bilg i şahsen , telefonla , e-postayla , faksla , sesl i mesajla , post a

aracılığıyla, imzal ı kuryeyl e v e elektroni k aktarıml a veriliyors a

her ver i sınıfiyl a ilgil i bilgiler .

2-3 Gizl i bilgileri n dağıtım ı

Kural: Yetkisi z kişileri n elin e geçtiğind e büyü k zararlar a nede n ola - bilecek şirke t bilgiler i ola n gizli bilgile r anca k almay a yetkil i bi r güvenilir kişiye verilebilir .

Açıklamalar/Notlar: Fizikse l (yan i basıl ı y a d a taşınabili r saklam a ortamı) olara k gizl i bilgile r ş u şekild e tesli m edilebilir :

• Şahsen ,

• Mühürl ü v e gizl i damgas ı vurulmu ş olara k dahil i kuryeyle ,

• Şirke t dışın a itibarl ı bi r kury e şirketini n hizmetiyl e y a d a taahhütl ü

veya onayl ı post a hizmet i kullanarak .

Elektronik (bilgisaya r dosyaları , veritaban ı dosyaları , e-posta) olara k gizli bilgile r ş u şekild e tesli m edilebilir :

• Şifrel i e-post a içeriğinde ,

• Şifrel i bi r dosy a olara k e-post a ekinde ,

• Şirke t dahil î ağındak i bi r sunucuy a elektroni k aktarımla ,

• Bi r fak s program ı kullanara k bilgisayardan . Anca k karş ı makinay ı

ilgili kişini n kullandığında n y a d a fak s gönderilirke n ilgil i kişini n

makinanın başınd a beklediğinde n emi n olunmas ı gerekir . Diğe r

bir seçene k ise , şifrel i bi r telefo n hattında n parol a korumal ı bi r

faks sunucusunda n gönderilmes i durumunda , faksı n alıc ı

olmadan gönderilmes i mümkündür .

Gizli bilgiler , karşılıklı, şirke t iç i telefonla , şirke t dışında n şifrel i tele - fonla, şifrel i uyd u aktarımıyla , şifrel i videokonferan s bağlantısıyl a v e şifreli interne t Protokol ü üzerinde n se s geçidiyl e (VolP) yapıla n karşılık - lı görüşmelerl e d e iletilebilirler .

Faksla gönderimlerd e önerile n yöntem, göndereni n bi r kapa k say -

fası göndermesini , alıcını n sayfay ı almas ı üzerind e karşılı k olara k başka bi r sayf a gönderere k fak s makinasını n başınd a olduğun u göster - mesini içermektedir . Gönderen , dah a sonr a faksı n tümün ü gönderir .

Şu iletişi m kanallar ı is e gizl i bilgileri n görüşülmes i y a d a dağıtılmas ı için kabu l edilebili r yöntemle r değillerdir : Şifresi z e-postalar , sesl i mesajlar, post a hizmetler i y a d a herhang i bi r telsi z iletişi m yöntem i (ce p telefonları, kıs a mesa j hizmetler i y a d a telsi z telefonlar)

2-4 Öze l bilgileri n dağıtım ı

Kural: Açığ a çıktıklar ı takdird e çalışanlar a y a d a şirket e zara r ver - mek üzer e kullanılabilecek , çalışa n y a d a çalışanlarl a ilgil i kişise l bilgi - leri ifad e ede n öze l bilgiler , yalnızc a on u almay a yetkil i bi r güvenilir kişiye tesli m edilebilir .

Açıklamalar/Notlar: Fizikse l (yan i basıl ı y a d a taşınabilir saklam a ortamı) olara k öze l bilgile r ş u şekild e tesli m edilebilir :

• Şahsen ,

• Mühürl ü v e öze l damgas ı vurulmu ş olara k dahil î kuryeyle ,

• Post a hizmetiyle ,

Elektronik (bilgisaya r dosyalan , veritaban ı dosyaları , e-posta) olara k özel bilgile r ş u şekild e tesli m edilebilir :

• Dahil î e-postayla ,

• Şirke t dahil î ağındak i bi r sunucuy a elektroni k aktarımla ,

• Bi r fak s program ı kullanara k bilgisayardan , anca k karş ı makinay ı

ilgili kişini n kullandığında n y a d a fak s gönderilirke n ilgil i kişini n

makinanın başınd a beklediğinde n emi n olunmas ı gerekir . Diğe r

bir seçene k ise , şifrel i bi r telefo n hattında n parol a korumal ı bi r

faks sunucusun a gönderilmes i durumunda , faksı n alıc ı olmada n

gönderilmesi mümkündür .

Özel bilgiler , karşılıklı , şirke t iç i telefonla , uyd u aktarımıyla , videokonferans bağlantısıyl a v e şifrel i İnterne t Protokol ü izerinde n se s geçidiyle (VolP) yapıla n karşılıkl ı görüşmelerl e d e iletilebilirler .

Şu iletişi m kanallar ı is e öze l bilgileri n görüşülmes i y a d a dağıtılmas ı için kabu l edilebili r yöntemle r değillerdir : Şifresi z e-postalar , sesl i mesajlar, post a hizmetler i y a d a herhang i bi r telsi z iletişi m yöntem i (ce p telefonları, kıs a mesa j hizmetler i y a d a telsi z telefonlar)

2-5 Dahil î bilgileri n dağıtım !

Kural: Dahil î bilgiler , yalnızc a şirke t içind e dağıtılabilece k y a d a gizlilik anlaşmas ı imzalamı ş güvenilir kişilere verilebilece k bilgilerdir . Dahilî bilgini n dağıtımın a yöneli k yönergele r hazırlamanı z gerekir .

Açiklamaiar/NotSar: Dahil î bilgiler , aralarınd a dahil î e-post a d a olmak üzer e he r yoll a iletilebilirler , anca k şifrel i olmadıklar ı sürec e e-postayla şirke t dışın a gönderilemezler .

2-6 Hassa s bilgileri n telefo n üzerinde n görüşülmes i

Kural: Gene l sınıfind a tanımlanmamı ş herhang i bi r bilgiy i telefo n üzerinde görüşmede n önce , bilgiy i verece k kişinin , karş ı tarafi n sesin i daha öncede n şahse n duymu ş olmas ı y a d a şirke t telefon sistemini n aramanın iste k sahibin e ai t dahil î bi r numarada n yapıldığın ı tespi t etmi ş olması gerekmektedir .

Açıklamaiar/Notlar: Eğe r istekt e buluna n kişini n ses i tanınmıyorsa , kayıtlı bi r se s mesajında n sesler i karşılaştırabilme k içi n arayanı n dahil î numarasını arayı n y a d a arayanı n yöneticisin e kimliğin i v e bilm e gereği - ni onaylattırın .

2-7 Girişt e y o d a danışmad a görevl i persone l süreçleri .

Kural: Giri ş görevlileri , şirkett e çalışı p çalışmadığın ı bilmedikler i herhangi birin e herhang i bi r paket i verirlerke n resiml i kimli k kontrol ü yapmalıdırlar. Kişini n adının , ehliye t numarasının , doğu m tarihinin , alı - nan paketi n v e alımı n gerçekleştiğ i gü n v e saati n işlendiğ i bi r kayı t def - teri tutulmalıdır .

Âçıklamaîar/Notlar: B u kura l dışar ı gönderile n paketleri n taşıyıcılara y a d a kury e hizmet i vere n şirketler e tesli m edilmesind e d e geçerlidir. B u şirketler , çalışanları n kimliklerini n kontro l edilebileceğ i kimlik kartlar ı çıkarırlar .

2-8 Üçünc ü şahıslar a yazılı m aktarım ı

Kural: Herhang i bi r yazılım , progra m y a d a bilgisaya r açıkla - malarının verilmesinde n y a d a aktarılmasında n önc e iste k sahibini n doğru kiş i olduğ u belirlenmel i v e b u aktarımın , sö z konus u bilgini n ver i sınıfıyla tutarl ı olu p olmadığ ı kesinleştirilmelidir . Şirke t bünyesind e kay - nak kod u biçimind e yapılmı ş yazılımla r çoğunlukl a şirke t mülk ü sayılı r ve gizl i olara k sınıflandırılırlar .

Açıklamalar/Kurallar: Yetk i belirlenmes i genellikl e istekt e buluna n kişinin işin i yapma k içi n yazılı m erişimin e ihtiyac ı olu p olmadığın a gör e yapılır.

2-9 Satı ş v e pazarlamanı n müşter i önerilerini n

incelemesi

Kural: Satı ş v e pazarlam a personeli , dahil î ger i aram a numaralarını , ürün planlarını , ürü n grub u iletişi m sorumluların ı y a d a diğe r hassa s bil - gileri olas ı bi r müşteriy e vermede n önc e verile n öneriler i incelemelidir .

Açıklamalar/Notlar: Satı ş v e pazarlam a temsilcisiyl e bağlant ı

kurup, on u ufukt a büyü k bi r alımı n olacağın a inandırmak , sanay i casus - larının sı k kullandıklar ı yöntemle r arasındadır . Satı ş firsatında n yarar - lanma çabasıyl a satı ş v e pazarlam a temsilcileri , saldırga n tarafında n hassas bilgiler e ulaşma k içi n poke r markas ı olara k kullanılabilece k bil - gileri sı k sı k verirler .

2-10 Dosy a v e verileri n aktarım ı

Kural: İste k sahibi , kimliğ i belirlenmi ş v e veriy i ilgil i taşınabili r ortam - da almas ı gerektiğ i anlaşılmı ş bi r güvenilir kişi olmadığ ı sürec e dosyala r ya d a diğe r elektroni k verile r hiçbi r taşınabilir ortam a aktarılmamalıdır .

Açıklama!ar/Not!ar: Bi r toplu m mühendis i hassa s bilgileri n bi r banda, disket e y a d a diğe r taşınabilir ortamlar a kopyalanmı ş olara k kendine gönderilmesin i y a d a birini n geli p almas ı içi n girişt e bek - letilmesini isteme k içi n akl a yatkı n bi r gerekç e sunara k çalışan ı kandıra - bilir.

Telefon İdares i

Telefon idares i kuralları , çalışanların , araya n kimliğin i kontro l ede - bilmelerini v e şirket i araya n kişiler e karş ı kend i iletişi m bilgilerin i koru - malarını sağlar .

3-1 Bilgisaya r bağlantıs ı y a d a fak s numaralarınd a

aramaların yönlendirilmes i

Kural: Aramalar ı dı ş ha t telefon numaraların a yönlendire n aram a yönlendirme hizmetler i şirke t içindek i herhang i bi r mode m y a d a fak s numarasına sağlanmamalıdır .

Açıklamalar/Notlar: Ço k yönl ü saldırganlar , dahil î numarala n saldırganın kontrol ü altındak i bi r dı ş ha t telefonun a yönlendirmeler i konusunda telefo n şirket i personelin i y a d a dahil î telekomünikasyo n çalışanlarını kandırmay a çalışabilirler . B u saldırı , saldırganın , fakslar a müdahale edebilmesine , gizl i bilgileri n şirke t için e fakslanmaların ı isteyebilmesine (çalışanla r kuru m için e birşe y fakslamanı n emi n olduğunu varsayarlar) y a d a bağlant ı hatların ı giri ş sürecini n aynısın ı taklit ede n tuza k bi r bilgisayar a yönlendirere k modeml e bağlana n kul - lanıcıların parolaların ı el e geçirmesin e yo l açacaktır .

Şirket içind e kullanıla n telefon hizmetin e gör e aram a yönlendirm e özelliği," telekomünikasyo n bölümünde n çok , iletişi m hizmet i sağlayıcısının kontrol ü altınd a olabilir . B u durumd a aram a yönlendirm e özelliğinin bağlant ı v e faks a ayrılmı ş telefon numaralarınd a bulunma - masını isteye n bi r talepl e iletişi m hizme t sağlayıcısın a gidilmes i gereke - cektir.

3-2 Araya n kimliğ i

Kural: Şirke t telefo n sistemi , tü m dahil î telefonlar a araya n ha t tanımlama (araya n kimliği) hizmetin i sağlamalıdı r v e eğe r münkünse , dışarıdan gele n aramalard a farkl ı bi r çalm a ses i kullanılmalıdır .

Açıklamalar/Notlar: Eğe r çalışanlar , şirke t dışında n gele n ara - maların kimde n geldiğin i görebilirlerse , b u onları n bi r saldırıy ı engellemelerine y a d a ilgil i güvenli k sorumlusun a saldırgan ı tari f etmelerine yardımc ı olabilir .

3-3 Nezake t telefonlar ı

Kural: Ziyaretçileri n şirke t çalışan ı gib i davranmaların ı önleme k içi n her nezake t telefonunu n nerede n edildiğ i (örneğin , "Danışma") arananın telefo n göstergesind e açıkç a görülebilmelidir .

Âçıkîamalar/Notlar: Eğe r dahil î aramaları n araya n kimlikler i yalnız - ca dahil i numaray ı gösteriyorsa , danışm a v e diğe r herkes e açı k yer - lerdeki şirke t telefonlarında n yapıla n aramalar a yöneli k uygu n önlemle r alınmalıdır. Bi r saldırganı n b u telefonlarda n birinde n aram a yapmas ı v e aramanın herhang i bi r başk a çalışanı n telefonunda n yapıldığ ı doğrul - tusunda aradığ ı kişiy i kandırmasını n mümkü n olmamas ı gerekmektedir .

3-4 Telefo n sistemler i il e gele n üretic i parolalar ı

Kural: Sesl i mesa j yöneticisi , şirke t çalışanlar ı tarafında n kullanıl - madan önc e telefo n sistemiyl e birlikt e gele n parolala r değiştirilmelidir .

Açıklamalar/Notlar: Toplu m mühendisleri , üreticilerde n il k parol a listelerini edinebili r v e bunlar ı yönetic i hesapların a erişme k içi n kulla - nabilirler.

3-5 Bölü m sesl i mesa j kutular ı

Kural: Dışarıyl a bağlantıs ı olabilece k he r bölüm e içi n bi r sesl i mesa j kutusu oluşturun .

Açıklamalar/Notlar: Toplu m mühendisliğini n il k adım ı hede f şirke t ve çalışanlar ı hakkınd a bilg i toplamaktır . Şirket , çalışanları n a d v e tele - fon numaraların a erişim i sınırlayarak , toplu m mühendisini n şirke t için - den hede f belirlemesin i y a d a çalışanlar ı kandırma k içi n başkalarını n adlarını kullanmasın ı güçleştirebilir .

3-6 Telefo n siste m satıcısını n onaylanmas ı

Kural: Satıc ı firmada n gele n hizme t teknisyenlerinde n hiçbirine , satıcı firm a bilgiler i v e gelenleri n yetkiler i onaylanmadan , şirke t telefo n sistemine uzakta n erişi m hakk ı tanınmamalıdır .

Açıklamalar/Notlar: Şirke t telefo n sistemlerin e gire n bilgisaya r kırıcıları sesl i mesa j kutus u yaratma , diğe r kullanıcılar a gele n mesajlar a

müdahale etm e y a d a parasın ı şirketi n ödediğ i telefon görüşmeler i yapabilme becerisin i kazanırlar .

3-7 Telefo n sistemini n ayarlanmas ı

Kural: Sesl i mesa j yöneticisi , telefo n sistemind e ilgil i güvenli k ayarlamalarını yapara k güvenli k gerekliliklerini n yerin e getirilmesin i sağlar.

Açıklamalar/Notlar: Telefo n sistemler i sesl i mesajla r içi n a z y a d a çok kapsaml ı güvenli k düzeylerin e gör e ayarlanabilirler . Yönetici , şirke t güvenlik anlayışını n bilincind e olmal ı v e sistem i hassa s bilgiler i koru - mak üzer e ayarlama k içi n güvenli k sorumlularıyl a birlikt e çalışmalıdır .

3-8 Aram a izlem e özelliğ i - ••..' .

Kural: iletişi m hizmetler i vere n firmanı n sınırlamaların a göre , çalışanların, arayanı n saldırga n olduğunda n kuşkulandıklar ı durumd a kıstırıp kovalaya n b u işlev i çalıştırabilmeler i sağlanabilece k şekilde , arama izlem e özelliğ i devrey e sokulmalıdır .

Âçsklamalar/Notlar: Çalışanlar , aram a izlem e işlevini n kullanım ı v e kullanılacağı durumla r konusund a eğitilmelidirler . Araya n kişi , açıkça , şirket bilgisaya r sistemlerin e yetkisi z girmey e y a d a hassa s bilgiler i el e geçirmeye çalışıyorsa , bi r aram a izlem e sürec i başlatılmalıdır . N e zaman bi r çalışa n aram a izlem e özelliğin i çalıştırırsa , Olay Bildirme Merkezi'ne d e heme n habe r verilmelidir . :

3-9 Otomati k telefo n sistemler i

Kural: Eğe r şirke t otomati k bi r yanı t verm e sistem i kullanıyorsa , sis - tem bi r çalışan a y a d a bölüm e aramay ı aktarırke n dahil î numaray ı söylemeyecek şekild e programlanmalıdır . .

Açıklamalar/Notlar: Saldırganla r bi r şirketi n otomati k telefo n sis - temini, çalışa n adların ı dahil î telefonlarl a karşılaştırma k içi n kullanabilir - ler. Dah a sonr a saldırganla r b u dahil î numar a bilgilerin i kullanara k aradıkları kişiler i şirke t iç i bilg i almay a yetkil i çalışanla r oldukların a inandırırlar.

3-10 Birbir i ardın a başarısı z girm e denemesinde n

sonra sesl i mesa j kutularını n kapatılmas ı

Kural: Peşpeş e belirl i bi r sayıd a başarısı z girm e denemesi olduğun - da sesl i mesa j hesapların ı kilitleyece k şekild e şirke t telefon sistemini n programlanması.

Açıklamalar/Notlar: Telekomünikasyo n yöneticis i ard ı ardın a be ş başarısız giri ş denemesinde n sonr a sesl i mesa j kutusun u kapatmalıdır . Yönetici dah a sonr a kilitl i sesl i mesa j kutuların ı te k te k kendis i açmalıdır .

Şirket Bilg i Güvenliğ i Kurallar ı Öneriler i 25 9

3-11 Smırlandmlmı ş dahil î telefonla r

Kural: Çoğ u zama n dışarıda n gele n aramalar ı kabu l etmeye n bölüm v e i ş grupların a ai t tü m dahil î telefonla r (yardı m masası , bilgisa - yar odası , çalışa n tekni k deste k vb.) yalnızc a diğe r dahil î telefonları n ulaşabileceği şekild e programlanmalıdır . Diğe r bi r seçene k is e parol a korumalı olmas ı v e dışarıda n araya n çalışanları n doğr u parolay ı gir - meleridir.

Açıklamalar/Notlar: He r n e kada r b u kura l amatö r toplu m mühendislerinin çoğ u girişimlerin i önleyebils e de , kararl ı bi r toplu m mühendisinin baze n bi r çalışan ı sınırl ı bi r hatt ı aramay a v e karş ı taraftan saldırgan ı ger i aramay a y a d a yalnızc a sınırl ı hatt â bi r topl u görüşme oluşturmay a ikn a edebileceğ i d e unutulmamalıdır . Saldırgan a yardımcı olaca k şekild e çalışanları n kandırılmas ı yöntem i b u taktiklerl e ilgili bilinc i artırma k amacıyl a güvenli k eğitimler i sırasınd a tartışılmalıdır .

Çeşitli . ,

4-1 Persone l kart ı tasarım ı

Kural: Persone l kartlar ı uzakta n tanınabilece k büyü k bi r fotoğra f içerecek şekild e tasarlanmalıdır .

Açıklamalar/Notlar: Sırada n tasarıml ı şirke t kimli k kartlarındak i fotoğraflar iş e yaramazda n bi r gömle k üstündür . Binay a gire n biriyle , kimlik kontrolün e yetkil i bi r güvenli k y a d a danışm a görevlis i arasındak i uzaklık o kada r fazladı r ki , kiş i yürüyü p geçerken , resim , seçilemeyece k kadar küçü k kalır . Böyl e bi r durumd a fotoğrafı n iş e yarayabilmes i içi n kartın yenide n tasarlanmas ı şarttır .

4-2 Konu m y a d a sorumlulu k değiştirirke n erişi m

haklarının gözde n geçirilmes i

Kural: N e zama n bi r şirke t çalışanını n konum u değişi r y a d a sorum - lulukları azalı r vey a çoğalırsa , çalışanı n yöneticisi , gerekl i güvenli k pro - filinin oluşturulmas ı içi n değişimde n Bİ'y ı haberda r eder .

Açıklamalar/Noîiar: Çalışanları n erişi m yetkilerini n yönetimi , korun - ması gereke n bilgileri n açığ a çıkmasın ı kısıtlama k içi n şarttır . E n düşü k yetki kural ı geçerl i olacaktır : Kullanıcılar a verile n erişi m yetkiler i işlerin i yapmalarında gerekl i ola n e n düşü k seviy e olacaktır . Yükseltilmi ş erişi m yetkileriyle sonuçlana n değişi m talepler i yükseltilmi ş erişi m yetkiler i veren bi r kurall a bağlantıl ı olmalıdır .

Hesap sahibini n erişi m yetkilerin i ihtiya ç doğrultusund a ayarlamalar ı için B İ birimin e habe r verm e sorumluluğu , çalışanı n yöneticisini n y a d a insan kaynakla n bölümünündür .

4-3 Şirke t çalışan ı olmayanla r içi n öze l kimli k

Kural: Şirketiniz , düzenl i olara k içerid e iş i ola n am a şirke t çalışan ı olmayan kişile r v e güvenili r kuryele r içi n öze l fotoğrafl ı şirke t kart ı çıkar - malıdır. . , .

Açıklamalar/Notlar: Düzenl i olara k binay a girmes i gereke n şirke t dışı kişile r (örneğin , kafeteryay a yiyece k v e içece k getirenler , fotokop i makinası tamirciler i y a d a telefo n bağlamay a gelenler) şirketini z içi n bi r tehdit oluşturabilirler . B u ziyaretçiler e kar t çıkarmay a e k olara k şirket - lerin, çalışanların a kartsı z bi r ziyaretç i gördüklerind e nası l davranmalar ı gerektiği konusund a d a eğiti m verilmelidir .

4-4 Taşeronları n bilgisaya r hesapların ı kapatma k

Kural: Kendisin e bi r bilgisaya r hesab ı açılmı ş bi r taşero n işin i bitirdikten y a d a sözleşmes i son a erdikte n sonra , soruml u yönetic i der - hal bilg i teknolojiler i bölümün ü haberda r edere k uzakta n erişi m içi n tele - fon bağlantıs ı y a d a interne t erişimler i v e veritaban ı erişi m hesapla n d a dahil olma k üzer e taşeronu n bilgisaya r hesapların ı kapattıracaktır .

Açıklamalar/Notlar: Bi r çalışanı n işin e so n verildiğind e veriler e ulaşmak içi n şirke t sistemler i v e süreçler i bilgisin i kullanm a tehlikes i vardır. Esk i çalışanı n kullandığ ı y a d a bildiğ i tü m bilgisaya r hesaplar ı hemen kapatılmalıdır . B u hesapları n arasınd a üreti m ver i tabanın a erişim, uzakta n bağlant ı v e bilgisaya r bağlantıl ı donanımlar a erişi m içi n kullanılan diğe r hesapla r d a bulunmalıdır .

4-5 Ola y bildirm e merkez i

Kural: Bi r ola y bildirm e merkez i kurulmal ı y a d a dah a küçü k şir - ketlerde, olas ı güvenli k olayların a yöneli k uyarılar ı alı p duyuraca k bi r olay bildirm e sorumlus u v e yardımcıs ı seçilmelidir .

Açıklamalar/Notlar: Şüphel i güvenli k olaylarını n bildirilmes i işlevin i merkezîleştirerek dah a önc e far k edilemeyece k türde n bi r saldırını n far k edilmesi sağlanabilir . Şirke t çapınd a düzenl i saldırıla r görülü r v e bunla r bildirilirse ola y bildirm e merkez i saldırganı n ney i hedeflediğin i bulabilir ; böylece ilgil i varlıklar ı koruma k içi n öze l bi r çab a harcanabilir .

• Ola y raporların ı almakl a görevlendirilmi ş çalışanla r toplu m mühendisliği yönte m v e taktiklerin e aşin a olmalıdırlar . Böylec e raporlar ı değerlendirip, deva m ede n ola n bi r saldırıy ı görebilirler .

4-6 Ola y bildirm e hatt s

Kural: Ola y bildirm e merkezin e hatırlamas ı kola y bi r dahil î numaras ı olan bi r ha t açılabilir .

Açıklamalar/Notlar: Çalışanla r bi r toplu m mühendisliğ i saldırısını n hedefi olduklarında n şüphelendiklerind e heme n ola y bildirm e merkezin i

haberdar edebilmelidirler . Haberi n zamanınd a verilebilmes i içi n ilgil i numara, tü m şirke t telefo n santral ı memurlarını n v e danışm a görevlilerinin önlerind e asıl ı olmal ı y a d a raha t ulaşabilecekler i bi r yerd e durmalıdır.

Şirket çapınd a bi r erke n uyar ı sistemi , sürmekt e ola n bi r saldırıy ı tespit edi p karşılı k vermey e büyü k ölçüd e yardımc ı olabilir . Yazıl ı tüzük - ler uyarınca , ola y bildirm e merkez i görevlileri , personeli n dikkatl i olmas ı için bi r saldırını n sö z konus u olduğ u doğrultusund a heme n hedeflene n gruplara uyar ı gönderirler . Uyarını n zamanınd a yapılabilmes i içi n merkez numarasını n şirke t bünyesind e herkes e dağıtılmı ş olmas ı gerekir.

4-7 Hassa s alanla r kapatılmalıdı r

Kural: Bi r güvenli k görevlis i hassa s y a d a güvenl i alanlar ı gözeti m altında tutaca k v e b u alanlar a giri ş ik i kademel i tanıtı m gerektirecektir .

Açıklamalar/Notlar: Kabu l edilebili r tanıtı m şekillerinde n bir i çalışanın kartın ı geçiri p bi r erişi m şifres i girmesini n istendiğ i dijita l elekt - ronik kilittir . Hassa s bölgeler i güvenli k altın a almanı n e n emi n yolu , kapıya kartl ı giriş i gözetleyece k bi r güvenli k görevlis i yerleştirmektir . Bunun ço k maliyetl i olduğ u kuruluşlard a kimli k kontrol ü içi n ik i kademel i tanıtım kullanılmalıdır . Risk e v e maliyet e gör e biyometri k özellikl i bi r giriş kart ı d a önerilir .

4-8 A ğ v e telefo n kutular ı

Kural: A ğ kabloları , telefo n kablolar ı y a d a a ğ erişi m noktalar ı bulu - nan kutular , dolapla r y a d a odala r he r zama n kapal ı tutulmalıdır .

Açıkiamalar/Motlar: Yalnızc a yetkil i personeli n telefo n v e a ğ kutu - larına, odalar a v e dolaplar a erişimin e izi n verilmelidir . Dışarıda n gele n onarım görevliler i y a d a satıc ı firm a sorumlularını n kimlikler i bilg i güven - liğinden soruml u bölümü n çıkardığ ı süreçle r kullanılarak , kuşk u bırak - mayacak biçimd e kontro l edilmelidirler . Telefo n hatlarına , a ğ bağlant ı noktalarına, düğmelere , köprüler e y a d a diğe r ilgil i cihazlar a erişi m olması, bilgisaya r v e a ğ güvenliğin i kırma k isteye n bi r saldırga n tarafın - dan kullanılabilir .

4-9 Şirke t iç i post a kutu!a n

Kural: Şirke t iç i post a kutular ı herkes e açı k yerler e konmamalıdır .

Açıklamalar/Notlar: Şirke t iç i post a alı m noktaların a erişim i ola n sanayi casuslar ı y a d a bilgisaya r kırıcıları , çalışanlar ı gizl i bilg i vermey e ya d a saldırgan a yardımc ı olaca k bi r işle m yapmay a yetkilendire n saht e yetki mektupların ı y a d a dahil î formlar ı rahatlıkl a gönderebilirler . Ayrıc a saldırgan, içind e bi r yazılı m güncellemes i yüklem e y a d a saldırganı n amaçları doğrultusund a yerleştirilmi ş makrola r içere n bi r dosyay ı açm a

talimatları içere n bi r diske t y a d a başk a elektroni k ortamla r gönderebilir . Şirket iç i postayl a gele n herhang i bi r paketin , doğa l olarak , alıcıla r tarafından güvenili r olduğun u varsayılır .

4-10 Şirke t bülte n panos u

Kural: Şirke t çalışanlar ı yararın a ola n bülte n panolar ı dışarıda n gelenlerin erişebileceğ i yerler e aşılmamalıdırlar .

Açıklamalar/Notlar: Pe k ço k işletmede , herkesi n okuyabilmes i içi n şir - kete y a d a çalışan a ai t öze l bilgileri n asıldığ ı bülte n panolar ı bulunur . Çalışan haberleri , çalışa n listeleri , dahil î mektuplar , ilanlard a ad ı geçe n çalışanların e v telefo n numarala n v e diğe r benzer i bilgile r panoy a asılırlar .

Bülten panoları , ziyaretçileri n giremeyeceğ i şirke t kafeteryalarını n yakınlarına, sigar a v e kahv e molas ı köşelerin e yerleştirilebilir . B u tar z bilgiler ziyaretçileri n y a d a geli p geçenleri n ulaşabileceğ i yerlerd e bulun - mamalıdır.

4-11 Bilgisaya r merkez i giriş i

Kural: Bilgisaya r odas ı y a d a ver i merkez i he r zama n kilitl i tutulmal ı ve çalışanları n içer i girerke n kimli k göstermeler i zorunl u olmalıdır .

Açıklamalar/Notlar: Şirke t güvenliği , tü m girişleri n elektroni k olara k kayıtlarının tutulabilmes i v e denetlenebilmes i içi n elektroni k kar t y a d a kart okuyuc u kullanm a seçeneğin i d e değerlendirmelidir .

4-12 Hizme t sağlayıcıiardak i müşter i hesapla n

Kural: Şirket e öneml i hizmetle r sağlaya n satıcılar a sipari ş vere n şir - ket çalışanlar ı yetkisi z kişileri n şirke t adın a sipari ş vermelerin i önleme k için parolal ı bi r hesa p açmalıdırlar .

Açıklamalar/Notlar: Siparişl e çalışa n şirketle r v e pe k ço k başk a firma, müşterilerini n parol a koymaların a izi n verirler . Şirke t is e iş e uygu n hizmet alabilme k içi n tü m satıcılarınd a parol a oluşturmalıdır . B u kura l özellikle telekomünikasyo n v e interne t hizmetler i içi n önemlidir . Kriti k hizmetlerin etkilendiğ i durumlarda , arayanı n sipari ş verme k içi n yetkil i olup olmadığın ı kontro l etme k içi n orta k bi r bilg i kullanılmas ı şarttır . Sosyal güvenli k numarası , şirke t verg i numarası , anneni n kızlı k soyad ı ya d a benzer i tanımlayıc ı bilgileri n kullanılmamas ı gerektiğ i d e unutul - mamalıdır.

Bir toplu m mühendisi , örneği n telefo n şirketin i arayı p mode m hatları - na yönlendirm e eklenmes i içi n talima t verebili r y a d a kullanıcıla r an a bil - gisayarı arattırdıklarınd a saht e bi r İ P numaras ı verme k içi n çevir i bilgi - lerinin değiştirilmesin i interne t Hizme t Sağlayıcısında n isteyebilir .

4-13 Bölü m bağlant ı sorumlus u

Kural: Şirketiniz , he r bölümde n y a d a i ş grubunda n bi r kişiy e bağlantı kurulaca k kiş i sorumluluğun u verdiğ i bi r progra m tesi s edebilir . Böylece herhang i bi r çalışan , o bölümde n olduğun u iddi a ede n bilin - meyen kişileri n gerçekliğini kolaylıkl a doğrulayabilir . Örneğin , yardı m masası deste k isteye n bi r çalışanı n kimliğin i onaylatma k içi n ilgil i bölümün bağlant ı kişisin i arayabilir .

Açıklamalar/Notlar: Kimliği n b u yönteml e tespiti , b u tar z çalışanlar parolaları yenileme k y a d a bilgisaya r hesabıyl a ilişkil i konulard a deste k almak istediğind e kend i bölümünde n diğe r çalışanlar a kefi l olaca k çalışan sayısın ı d a azaltır .

Toplum mühendisliğ i saldırılarını n başarıl ı olmalarını n bi r neden i d e teknik deste k çalışanlarını n yeterl i zamanlarını n olmamas ı v e iste k sahibinin kimli k tespitin i doğr u bi r yönteml e yapmamalarıdır . Bağlant ı kişisinin kefi l olması , tekni k deste k ekibini n ona y amacıyl a şahse n görüşmeleri gereke n kiş i sayısın ı azaltır .

4-14 Müşter i parolalar ı

Kural: Müşter i hizme t temsilcilerini n müşter i hesa p parolaların ı alma yetkile n olmayacaktır .

Açıklamalar/Notlar: Toplu m mühendisler i sı k sı k müşter i hizmetleri - ni arayı p parol a y a d a Sosya l Güvenli k Numaras ı gib i müşter i tanımla - ma bilgilerin i eld e etmey e çalışırlar . Bi r toplu m mühendis i b u bilgiy i kul - lanarak başk a bi r müşter i temsilcisin i arayıp , müşter i gib i davranı p bilg i elde etmey e y a d a saht e siparişle r vermey e çalışabilir .

Bu denemeleri n başarıy a ulaşmasın ı engelleme k içi n müşter i hizme t yazılımı yalnızc a arayanı n verdiğ i tanımlam a bilgilerini n girilebileceğ i şekilde tasarlanmalıdı r v e temsilci , sistemde n sadec e parolanı n doğr u olup olmadığın ı söyleye n bi r mesa j almalıdır .

4-15 Açıklı k testler i

Kural: Güvenli k bilinçlendirm e v e çalışa n intiba k eğitimler i sırasınd a güvenlik açıkların ı tes t etme k içi n şirketi n toplu m mühendisliğ i taktikler i kullanacağını bildirilmes i gerekmektedir .

Açıklamalar/Notlar: Toplu m mühendisliğ i delm e testler i öncede n bildirilmeden yapılırs a diğe r çalışanları n y a d a test i yapa n şirke t eleman - larının kendilerin e karş ı aldatıc ı taktikle r kullanmas ı nedeniyl e şirke t çalışanlarında öfke , utanm a y a d a başk a duygusa l sarsıntıla r oluşabilir .

4-16 Şirke t Gizl i bilgilerini n gösterilmes i

Kural: Halk a açıklanmas ı düşünülmeye n şirke t bilgiler i herkesi n görebileceği yerler e aşılmamalıdır .

AçıkSamalar/Notiar: Gizl i ürü n y a d a süre ç bilgilerin e e k olarak , dahilî telefo n numaralar ı vey a çalışa n listeler i gib i listele r y a d a he r bölümün yöneticilerini n listesin i içere n bin a göre v çizelgeler i gib i dahil î iletişim bilgilerini n d e gözlerde n uza k tutulmalar ı gerekmektedir .

4-17 Güvenli k bilinçlendirm e eğitim i

Kural: Şirketi n tü m çalışanları , çalışa n intiba k eğitimler i sırasınd a bi r güvenlik bilinçlendirm e eğitimin i d e tamamlamalıdırlar . Dahası , he r çalışan, o n ik i ay ı geçmeme k koşuluyl a güvenli k eğitimlerin i yürüte n bölümün belirlediğ i düzenl i aralıklarl a güvenli k bilincin i tazelem e eğitimler i almalıdır.

Açıklamalar/Notlar: Pe k ço k kurulu ş u ç kullanıc ı bilinçlendirm e eğitimini tamame n gö z ard ı eder . 200 1 Küresе l Bilg i Güvenliğ i Araştırması'na göre , araştırmay a katıla n kuruluşları n yalnızc a yüzd e 30'u kullanıcılar a yöneli k bilinçlendirm e eğitimlerin e par a ayırmaktadır . Bilinçlendirme eğitim i toplu m mühendisliğ i teknikler i kullanılara k başarıya ulaşabile n güvenli k ihlallerini n sayısın ı azaltmay a yöneli k önemli bi r gerekliliktir .

4-18 Bilgisaya r erişim i içi n güvenli k eğitim i dersler i

Kural: Çalışanla r herhang i bi r şirkette , bilgisaya r sistemin e erişi m hakkı eld e etmede n önc e bilg i güvenliğ i derslerin i başarıyl a ta'mam - lamış olmalıdırlar .

Açıklamalar/Notlar: Toplu m mühendisler i sı k sı k yen i iş e girenler i hedef alırla r v e onları n guru p olara k şirketi n güvenli k kurallarını , ver i sınıflandırma v e hassa s bilgileri n kullanımın a yöneli k doğr u süreçler i bilme olasılıklarını n düşü k olduğun u bilirler .

Eğitim, çalışanları n güvenli k kurallarıyl a ilgil i olara k sorula r sor - malarına d a olana k tanımalıdır . Eğitimi n ardında n hesa p sahibini n güvenlik kuralların ı anladığın ı v e kurallar a uyacağın ı taahhü t ede n bi r belge imzalamas ı zorunl u olmalıdır .

4-19 Çalışa n kart ı renkl i baskıl ı olmalıdı r

Kural: Kimli k kartları , kar t sahibini n çalışan , taşeron , geçic i satıcı , danışman, ziyaretç i y a d a stajye r olduğun u gösterece k şekild e renk - lendirilmiş olmalıdır .

Açık!ama!ar/Notlar: Kar t rengi , kişini n konumun u uzakta n anlama k için ço k iy i bi r yoldur . Diğe r bi r seçene k is e kar t sahibini n konumun u belirtmek içi n ir i harfle r kullanılmasıdır , anca k renkl i bi r tasarı m olmas ı hataya maha l verme z v e görmes i dah a kolaydır .

Binanın için e girebilme k içi n toplu m mühendislerini n sıkç a kullandık - ları bi r yönte m is e kury e y a d a tamirc i kılığın a girmektir . İçer i girebildik - ten sonr a saldırga n başk a bi r çalışa n olara k davranabili r y a d a hiçbi '

Şirket Bilg i Güvenliğ i Kurallar ı Öneriler i 26 5

şeyin farkınd a olmaya n çalışanları n işbirliğin i eld e etme k içi n unvanıyl a ilgili yala n söyleyebilir . Örneğin , binay a telefo n tamircis i olara k gire n bi r kişi bi r çalışa n gib i davranamaz , çünk ü kartını n reng i on u el e verir .

Bilgi İşle m Teknolojiler i Kurallar ı

Herhangi bi r şirketi n bilg i işle m teknolojiler i bölüm ü kuruluşu n bilg i varlıklarını korumad a yardımc ı olmas ı içi n kurallar a öze l bi r gereksini m duymaktadır. Bi r kuruluştak i B İ işlemlerini n özgü n yapısın ı yansıta - bilmek amacıyla , B İ kuralların ı Genel , Yardı m Masası , Bilgisaya r Yönetimi v e Bilgisaya r işlemler i olara k böldüm .

5-1 B İ bölüm ü çalışa n iletişi m bilgiler :

Kural: B İ bölüm ü çalışanlarını n telefo n numarala n v e e-post a adresleri, bilm e gereğ i olmaya n herhang i birin e verilmemelidir .

Açıklamalar/Notlar: B u kuralı n amacı , iletişi m bilgilerini n toplu m mühendisleri tarafında n el e geçirilmesin i engellemektir . B İ içi n yanızc a genel bi r iletişi m numaras ı y a d a e-post a adres i verilere k dışarıda n arayan - ların B İ bölüm ü çalışanların a doğruda n ulaşmas ı engellenecektir . Sit e yöneticisinin v e tekni k hizmetleri n e-post a adres i yalnızc a admin@compa - nyname.com gib i gene ! adlarda n oluşmalıdır . Verile n telefo n numarala n bireysel çalışanlar a değil , bölümü n sesl i mesa j kutusun a bağlanmalıdırlar .

Doğrudan iletişi m bilgiler i herkes e açı k olduğ u zama n bi r bilgisaya r kırıcısının belirl i B İ çalışanların a ulaşmas ı v e bi r saldırıd a kullanılabile - cek bilgiler i y a d a B İ çalışan ı gib i davranma k amacıyl a adların ı v e iletişim bilgilerin i vermeler i içi n onlar ı kandırmas ı kolaylaşacaktır .

5-2 Tekni k deste k talepler i

Kural: Tü m tekni k deste k talepler i b u tar z talepler i değerlendire n gruba yönlendirilmelidir .

Açıklamalar/Motiar: Toplu m mühendisleri , gene l olara k tekni k deste k konularıyla ilgilenmeye n v e b u tar z istekler e yanı t verebilme k içi n uygu n güvenlik süreçlerini n farkınd a olmaya n B İ çalışanların ı aramay ı deneye - bilirler. Bun a gör e B İ çalışanlar ı b u istekler i ger i çevirme k v e arayan ı destek vermekl e yüküml ü grub a yönlendirme k üzer e eğitilmelidirler .

Yardım Masas ı . ... .

6-1 Uzakta n erişi m süreçler i

Kural: Yardı m masas ı çalışanları , haric î a ğ erişi m noktala n y a d a

bağlantı numaralar ı d a aralarınd a olma k üzer e uzakta n erişiml e ilgil i bil - gileri v e ayrıntılar ı açıklamamalıdırlar . Ancak , iste k sahib i aşağıdak i koşullardan birin e uyuyors a duru m değişebilir :

• Dahil î bilg i alabileceğin e dai r yetkil i olduğunu n onaylanmı ş

olması. . , .•' .

• Haric î bi r kullanıc ı olara k şirke t ağın a bağlanmay a yetkil i olduğu -

nun onaylanmı ş olması . Kiş i şahse n tanınmadığ ı sürec e b u

bölümde anlatıla n Ona y v e Yetkilendirm e Süreçlerin e uygu n

olarak iste k sahibini n kimli k tespit i kuşk u bırakmayaca k şekild e

yapılmalıdır. :

Açıklamaiar/Notlar: He m işler i bilgisayarl a ilgil i konulard a kul - lanıcılara deste k verme k olduğu , he m d e arttırılmı ş siste m yetkiler i olduğu içi n şirke t yardı m masas ı sı k sı k toplu m mühendisini n başlıc a hedefi olur . Tü m yardı m masas ı çalışanları , şirke t kaynakların a yetkisi z kişilerin ulaşmasın a yo l açabilece k yetkisi z bilg i aktarımların ı engelleyen bi r insa n güvenli k duvar ı olaca k şekild e yetiştirilmelidirler . En basi t kural , kimli k tespitini n sonuc u oluml u çıkmada n hiçbi r zama n uzaktan erişi m süreçlerin i kimsey e açıklamamaktır .

6-2 Parolalar ı il k durum a döndürme k

Kural: Bi r kullanıc ı hesabın a ai t parol a yalnızc a hesa p sahibini n isteği doğrultusund a yenilenebilir .

Açıklamalar/Notlar: Toplu m mühendisler i tarafında n e n sı k oynanan oyun , başk a birini n hesabını n parolasın ı il k durum a döndürt - mek y a d a değiştirtmektir . Saldırgan , parolasın ı unutmu ş y a d a kaybet - miş bi r çalışa n gib i davranır . B u tar z bi r saldırını n başar ı şansın ı azalta - bilmek için , parolay ı il k durumun a döndürmey e yöneli k bi r tale p geldiğinde B İ çalışan ı herhang i bi r işle m yapmada n önc e taleb i vere n çalışanı ger i aramalıdı r v e b u aram a içi n çalışa n telefon rehberindek i numarayı kullanmalıdır . B u süreçl e ilgil i olara k Ona y v e Yetkilendirm e Süreçlerine bakınız .

6-3 Yetkileri n değişim i

Kural: Bi r kullanıcını n yetkilerin i y a d a erişi m hakların ı artırmay a yönelik tü m taleple r hesa p sahibini n yöneticis i tarafında n yazıl ı olara k onaylanmış olmalıdır . Ayrıc a b u tar z talepleri n Ona y v e Yetkilendirm e Süreçlerine uygu n olara k geçerlilikler i onaylanmalıdır .

Açıklamalar/Notlar: Bi r bilgisaya r kırıcıs ı standar t bi r kullanıc ı hesabına girdikte n sonr a bi r

sonrak i adım saldırganı n tü m siste m üzerinde ta m kontro l sağlamas ı içi n yetkilerin i artırmas ı olur . Yetkilendirme süreciyl e ilgil i bilgis i ola n bi r saldırga n e-postayla , faksl a ya d a telefonla , yetkil i gib i görüne n bi r talepte bulunabilir . Örneğin , saldırgan tekni k deste k y a d a yardı m masasın ı arayı p girebildiğ i hesa -

ba e k erişi m haklar ı alabilme k içi n bi r teknisyen i ikn a etmey e çalışabilir .

6-4 Yen i hesa p yetkis i

Kural: Çalışanlar , taşeronla r y a d a diğe r yetkil i kişileri n kullanım ı içi n açılacak yen i hesa p talepler i çalışanı n yöneticis i tarafında n imzalanmı ş yazılı bi r belgeyl e y a d a dijita l olara k imzalanmı ş elektroni k postayl a yapılmalıdır. B u istekle r şirke t iç i post a aracılığıyl a teyi t edilmelidir .

Açıklamalar/Notlar: Parolala r v e diğe r bilgile r bilgisaya r sistemle - rine girme k içi n faydal ı olduklarından , bilg i hırsızlarını n erişi m sağlama - da kullandıklar ı e n öncelikl i hedeflerdi r v e öze l önlemle r alınmas ı şarttır . Bu kuralı n amac ı bilgisaya r kırıcılarını n yetkil i persone l gib i davran - masını y a d a yen i hesa p taleplerini n sahtesin i oluşturmasın ı önleme k içindir. B u nedenl e tü m b u tar z istekle r Ona y v e Yetkilendirm e Süreçler i kullanılarak şüph e kalmayaca k biçimd e onaylanmalıdırlar .

6-5 Yen i parolaları n teslim i

Kural: Yen i parolala r şirke t gizl i bilgiler i olara k el e alınmal ı v e şah - sen, taahhütl ü post a gib i imzal ı teslimatl a y a d a güvenili r karg o şirket - leri gib i güvenl i yöntemle r kullanara k tesli m edilmelidirle r (bkz . gizl i bil - gilerin dağıtımı il e ilgil i kurallar) .

Açıklamalar/Notlar: Şirke t iç i post a d a kullanılabilir , anca k paro - ların, içeriğin i göstermeye n güvenl i zarflard a gönderilmes i gerekir . Önerilen bi r yönte m d e he r bölümde n bi r bilgisaya r iletişi m sorumlus u belirlemektir. B u kiş i yen i hesa p ayrıntılarını n dağıtımında n v e paro - larını kaybeden y a d a unuta n çalışanlar a kefi l olmakta n sorumludur . Bu durumda , deste k personel i he r zama n şahse n tanıdığ ı küçü k bi r gurupla birlikt e çalışıyo r olacaktır .

6-6 Bi r hesabı n kapatılmas ı

Kural: Bi r kullanıc ı hesabın ı kapatmada n önc e talebi n yetkil i birinden geldiğini n doğrulanmas ı gerekmektedir .

Açıklamalar/Notlar: B u kuralı n amacı , saldırganı n bi r hesabı n ka - patılmasını isteyi p sonr a d a kullanıcını n bilgisaya r sistemin e erişe - memesi sorunun u çözmey e çalışıyo r numaras ı yapmas ı engelleme k içindir. Toplu m mühendis i kullanıcını n sistem e girememesiyl e ilgil i önce - den bilgis i ola n bi r teknisye n gib i davranara k kurban ı aradığında , kur - ban, yapıla n kontrolle r sırasınd a parolas ı istendiğind e çoğ u zama n b u bilgiyi verir .

6-7 A ğ bağlant ı noktalarını n v e araçlarını n devr e dış ı

bırakılması

Kural: Hiçbi r çalışa n ki m olduğun u bilmedikler i bi r tekni k deste k çalışan ı için herhang i bi r a ğ aracın ı y a d a bağlant ı noktasın ı kapatmamalıdır .

Açıklamalar/Notlar: B u kuralı n amacı , bi r saldırganı n bi r a ğ bağlan - tısının kapatılmasın ı isteyi p sonr a d a ağ a erişi m sorunun u çözme k içi n çalışanı aramasın ı engellemektir . Yardımseve r bi r teknisye n kılığındak i toplum mühendisi , kullanıcını n a ğ sorunun a ilişki n ö n bilgis i varmı ş gib i davrandığında, kurban , yapıla n kontrolle r sırasınd a parolas ı istendiğin - de çoğ u zama n b u bilgiy i verir .

6-8 Telsi z erişim i süreçlerini n açıklanmas ı

Kural: Hiçbi r çalışa n telsi z ağın a bağlanmay a yetkil i olmaya n kimseler e telsiz ağ ı üzerinde n şirke t ağın a bağlanm a süreçlerin i açıklamamahdır .

Açıklamalar/Notlar: Telsi z erişi m bilgilerin i açıklamada n önc e kişinin haric i kullanıc ı olara k şirke t ağın a bağlanmay a yetkil i olu p olma - dığı he r zama n öncede n kontro l edilmelidi r (bkz . Ona y v e Yetkilendirm e Süreçleri).

6-9 Kullanıc ı gizliliğ i

Kural: Bilgisayarl a ilgil i soru n olduğun u bildire n çalışanları n adlar ı bilgi işle m bölüm ü dışında n kimsey e açıklanmamalıdır .

Açıklamalar/Notlar: Sırada n bi r saldırıd a toplu m mühendis i yardı m masasını ara r v e yakı n zamand a bilgisayarlarınd a soru n olduğun u bildiren çalışanları n adların ı ister . Araya n çalışan , taşero n y a d a telefo n şirketi eleman ı gib i davranabilir . Soru n olduğun u söyleye n kişileri n adlarını aldıkta n sonr a toplu m mühendis i yardı m masas ı y a d a tekni k destek personel i gib i davranı r v e çalışan ı arayara k sorun u çözme k içi n aradığını söyler . Aram a sırasınd a saldırgan , kurban ı istediğ i bilgiler i ver - mesi y a d a saldırgan ı hedefin e götürece k bi r işle m yapmas ı içi n kandırır.

6-10 Komu t girme k y a d a progra m çalıştırma k

Kural: B i bölümünd e ayrıcalıkl ı hesapla n ola n çalışanlar , şahse n tanımadıkları birini n isteğ i üzerin e herhang i bi r komu t y a d a proga m çalıştırmamalıdırlar.

Açıklamalar/Notlar: Saldırganları n bi r Truv a At ı y a d a başk a bi r kötü huyl u yazılı m yükleme k içi n sıkç a kullandıklar ı bi r yönte m d e va r olan bi r programı n adın ı değiştirme k v e sonr a d a yardı m masasın ı ara - yarak program ı çalıştırmay a uğraşırke n hat a mesaj ı verdiğin i söylemek - tir. Saldırgan , yardı m masas ı teknisyenin i program ı çalıştırmay a ikn a eder. Teknisye n program ı çalıştırdığınd a köt ü huyl u yazılı m çalıştıra n kullanıcının yetkilerin i görü r v e saldırgan a ayn ı yetkile n verdiğ i bi r işle m gerçekleştirir. Bu , saldırganı n şirke t sistemin i el e geçirmesin i sağlar .

Bu kura l deste k personelini n bi r isteğ e bağl ı olara k herhang i bi r prog - ramı çalıştırmada n önc e çalışa n konumunu n doğrulanmasın ı zorunl u tutarak yukarıd a bahsedile n taktiğ e karş ı bi r önle m getirmektedir .

Şirket Bilg i Güvenliğ i Kurallar ı Öneriler i 26 9

7-1 Gene l erişi m haklarını n değiştirilmes i

Kural: Bi r elektroni k i ş profiliyl e ilgil i gene i erişi m hakların ı değiştirme taleb i şirke t ağınd a erişi m hakların ı yönete n guru p tarafında n onaylanmalıdır.

Açıklamalar/Notlar: Yetkilile r he r değişi m talebini n bilg i güvenliğ i için bi r tehdi t unsur u oluşturu p oluşturmadığın ı değerlendireceklerdir . Eğer oluşturuyorsa , soruml u kiş i iste k sahibin i gerekl i konulard a uyara - cak v e yapılaca k değişiklikle r konusund a orta k bi r karar a varacaklardır .

7-2 Uzakta n erişi m talepler i

Kural: Uzakta n bilgisaya r erişim i yalnızc a şirke t dış ı noktalarda n bil - gisayar sistemlerin e girm e gerekliliğ i olduğun u göstere n çalışanlar a ver - ilecektir.

Açıklamalar/Notlar: Yetkil i persone l tarafında n şirke t ağın a dışarı - dan bağlanm a ihtiyacın a gör e b u tar z erişimi n yalnızc a gere k duyanlar a verilecek şekild e sınırlandırılmas ı uzakta n erişiml i kullanıcıları n yöneti - mini v e oluşa n risk i büyü k ölçüd e azaltacaktır . Dışarıda n bağlanm a yetkileri ola n kişileri n sayıs ı n e kada r a z olurs a saldırganı n hede f seçenekleri d e o kada r a z olacaktır . Saldırganı n şirke t ağın a girme k içi n bağlantılarını çalma k y a d a onları n kimliğin e bürünme k niyetiyl e uza k kullanıcıları hedefleyebileceğin' ! hiçbi r zama n unutmayınız .

7-3 Ayrıcalıkl ı hesa p parolalarını n il k durum a getirilmes i

Kural: Yetkil i bi r hesab a ai t parolanı n il k durumun a getirilmes i talebi , hesabın bulunduğ u bilgisayarda n soruml u siste m yöneticis i tarafında n onaylanmalıdır. Yen i parola , şirke t iç i postayl a gönderilmel i y a d a şah - sen iletilmelidir .

Açıklamalar/Notlar: Ayrıcalıkl ı hesapları n tü m siste m kaynakların a ve bilgisaya r sistemindek i dosyalar a erişim i vardır . Doğa l olara k b u hesaplarda mümkü n ola n e n güçl ü korum a kullanılmalıdır .

7-4 Dışarıda n gele n deste k personelini n uzakta n erişim i

Kural: Hiçbi r dışarıda n deste k personelin e (yazılı m y a d a donanı m satan firmada n gele n persone l gibi) ilgil i hizmetler i vermey e yetkil i olu p olmadıkları kontro l edilmede n v e kimli k tespit i yapılmada n şirke t bilgisa - yar sistemlerin e y a d a ilgil i araçlar a uzakta n erişm e hakk ı y a d a bilgis i verilmemelidir. Eğe r deste k hizmet i verme k üzer e satıc ı firm a yetkil i erişim tale p ediyorsa , verile n hizme t son a erdiğind e satıc ı firmanı n kul - landığı hesabı n parolas ı zama n kaybetmede n değiştirilmelidir .

Açıklamalar/Notlar: Bilgisaya r kırıcılar ı şirke t bilgisaya r y a d a telekomünikasyon ağın a girebilme k içi n satıcıymı ş gib i davranabilirler .

Bu nedenl e sistemd e herhang i bi r i ş gerçekleştirm e yetkilerini n yanısır a satıcının kimliğini n d e onaylanmas ı önemlidir . Ayrıc a i ş bittiğind e satıcının kullandığ ı hesa p parolas ı değiştirilere k siste m kapılar ı kapatıl - malıdır.

Hiçbir satıc ı firmanı n geçic i olara k bil e herhang i bi r hesa p içi n kend i istediği parolay ı kullanmasın a izi n verilmemelidir . Baz ı satıcıları n farkl ı bilgisayar sistemlerind e ayn ı y a d a benze r parolalar ı kullandıklar ı bilin - mektedir. Örneğin , bi r a ğ güvenli k şirket i tü m müşter i bilgisaya r sistem - lerindeki hesapların a ayn ı parol a il e erişmektedi r v e üstün e üstlü k dışarıya Telne t erişimin e d e izi n verilmiştir .

7-5 Şirke t sistemlerin e uzakta n erişi m içi n güçl ü tanımlam a

Kural: Şirke t ağın a uzakta n erişi m içi n kullanıla n tü m bağlant ı nok - taları değişke n parolala r y a d a biyometrikle r gib i güçl ü tanımlam a araçlarıyla korunmalıdırlar .

Açiklamaiar/Notlar: Pe k ço k işletme , uza k kullanıcılar ı tanımla - manın te k yol u olara k sabi t parolalar a güvenirler . B u uygulam a sakın - calıdır çünk ü güvensizdir . Bilgisaya r kırıcılar ı kurbanı n ağınd a olas ı e n zayıf bağlantıy ı oluşturabilece k uzakta n erişi m noktasın ı hedeflerler . Başka birini n parolanız ı öğreni p öğrenmediğin i hiçbi r zama n bile - mezsiniz.

Bu nedenl e uzakta n erişi m noktaları , zama n tabanl ı anahtarlar , akıl - lı kartla r y a d a biyometri k araçla r gib i güçl ü tanımlam a araçlarıyl a korun - malıdır, böylec e aray a girere k alınmı ş parolaları n saldırga n içi n hiçbi r değeri olmaz .

Değişken parolalar a dayal ı tanımlamala r kullanışsı z olduklarından , bilgisayar kullanıcıları , tahmi n edilmes i zo r parol a seçm e kuralın a sada - katle uymalıdırlar .

7-6 İşleti m sistem i ayarlar !

Kural: Siste m yöneticiler i mümkü n ola n he r noktad a işleti m sistem - lerinin tü m geçerl i güvenli k kura l v e süreçleriyl e tutarl ı bi r şekild e ayarlanmış olduğunda n emi n olmalıdırlar .

Açıklamalar/Notlar: Güvenli k kuralların ı hazırlama k v e dağıtma k tehlikeyi azaltmay a yöneli k öneml i bi r adımdı r am a çoğ u durumd a uyu p uymamak iste r isteme z bireyse l çalışan a kalmıştır . Anca k bilgisayarl a ilgili birço k kural , parolaları n sahi p olmas ı gereke n uzunlu k gibi , işletir r sistemi ayarlar ı sayesind e zorunl u durum a getirilebilir . Güvenli k kura - larını işleti m sistem i özelliklerin i ayarlayara k otomatikleştirmek , kararla " etkili bi r şekild e insa n unsurunu n elinde n alı p kuruluşu n gene l güvenli ğ - ni artırmaktadır .

7-7 Zorunl u sür e aşım ı

Kural: Tü m bilgisaya r hesaplar ı bi r yı l içerisind e kapanmay a ayarlanmalıdır.

Açıklamalar/Notlar: B u kuralı n amacı , bilgisaya r kırıcılar ı sı k sık , kullanılmayan hesaplar ı hedefledikler i için , artı k kullanılmaya n bilgisa - yar hesapların ı ortada n kaldırmaktır . B u süre ç esk i çalışanlar a y a d a taşeronlara ai t v e kazar a olduğ u gib i bırakılmı ş herhang i bi r bilgisaya r hesabının otomati k olara k kaldırılacağın ı garantiler . .

Yönetimin takdirin e bağl ı olara k yenilem e zamanınd a çalışanları n güvenlik tazelem e eğitim i almalar ı y a d a bilg i güvenli k kuralların ı göz - den geçiri p bunlar a uyacakların a dai r bi r taahhütnam e imzalamalar ı zorunlu tutulabilir .

7-8 Gene l e-post a adresler i

Kural: B İ bölüm ü dışarıyl a sürekl i iletişim i ola n he r bölü m içi n gene l bir e-post a adres i oluşturacaktır .

Açık!amalar/Notlar: Gene l e-post a adres i santra l memurlar ı tarafından y a d a şirketi n interne t sites i aracılığıyl a dışarıy a verilebilir . Böylece he r çalışa n kend i şahs î e-post a adresin i yalnızc a bilmes i gereken kişiler e verecektir .

Bir toplu m mühendisliğ i saldırısını n il k aşamasınd a saldırga n genel - likle çalışanları n telefo n numaralarını , adların ı v e unvanların ı öğren - meye çalışır . Çoğ u zama n b u bilg i şirke t interne t sitesind e bulunabili r y a da istendiğind e herkes e verilebilir . Gene l sesl i mesa j kutularını n ve/veya e-post a adreslerini n yaratılmas ı çalışa n adlarını n belirl i bölüm - ler y a d a sorumluluklarl a bağdaştırılmasın ı zorlaştırmaktadır .

7-9 Ala n tesciller i içi n iletişi m bilgiler i

Kural: interne t adre s alanlar ı y a d a ala n adlar ı alma k içi n kayı t olurken sağlana n iletişi m bilgiler i idarî , tekni k y a d a diğe r çalışanları n bireysel olara k adların ı vermemelidir . Onu n yerin e oray a gene l bi r e-posta adres i v e an a şirke t telefo n numaras ı girilmelidir .

Açîklamalar/Notlar: B u kuralı n amac ı iletişi m bilgilerini n bilgisaya r kırıcısı tarafında n kötüy e kullanılmasın ı önlemektir . Bireyleri n adlar ı v e telefon numaralar ı verildiğind e bi r saldırga n b u bilgiler i kullanara k kişi - lerle bağlant ı kurabili r v e onlar ı siste m bilgiler i vermeler i y a d a saldır - ganın amacın a uya n bi r işle m yapmalar ı doğrultusund a kandırabilir . Toplum mühendis i diğe r şirke t çalışanların ı kandırabilme k içi n ad ı geçen çalışanlarda n bir i gib i davranabilir .

Belirli bi r çalışanı n e-post a adres i yerine , iletişi m bilgis i administra - tor@company.com şeklind e olmalıdır . Telekomünikasyo n bölüm ü çalışanları, idar î v e tekni k iletişi m içi n gene l bi r sesl i mesa j kutus u oluş -

turarak bi r toplu m mühendisliğ i saldırısınd a iş e yarayabilece k bilgileri n gizliliğini korumu ş olurlar .

7-10 Güvenii k v e işleti m sistem i güncellemelerini n yük -

lenmesi

Kural: işleti m sistem i v e uygulam a yazılımların a yöneli k tü m güven - lik yamalan , çıktıklar ı zama n e n kıs a süred e yüklenmelidirler . Eğe r b u kural görev-kriti k üreti m sistemlerini n işleyişiyl e çatışıyors a b u tar z gün - cellemeler uygu n olduklar ı zama n yapılmalıdırlar .

Açıklamaîar/Motlar: Bi r açı k görüldüğünd e bi r yamanı n y a d a geçi - ci bi r çözümü n va r olu p olmadığın ı öğrenme k içi n yazılı m üreticis i zaman kaybetmede n aranmalıdır . Yamalanmamı ş bi r bilgisaya r sistem i kuruma e n büyü k güvenli k tehditlerinde n birini oluşturur . Siste m yöneti - cileri gerekl i çözümler i uygulamay ı geciktirirlers e pencer e o kada r açılı r ki saldırga n tırmanı p içer i girebilir .

Bulunan düzinelerc e güvenli k açığ ı haftalı k olara k internett e yayın - lanmaktadır. Bilg i işle m çalışanlar ı mümkü n ola n e n kıs a süred e güven - lik yamaların ı v e çözümlerin i yüklem e çabala n konusund a uyanı k davranana kadar , şirke t ağ ı he p bi r güvenli k ihlal i yaşam a tehlikesiyl e karşı karşıy a kalacaktır . İşletmed e kullanıla n uygulam a programla n v e işletim sistemini n zayıflıklarıyl a ilgil i yapıla n açıklamalarda n haberda r olmak oldukç a önemlidir .

7-11 İnterne t sayfalarındak i iletişi m bilgiler i

Kura!: Şirketi n haric î interne t sayfası, şirke t yapıs ı il e ilgil i hiçbi r bilg i vermemeli y a d a çalışanlar ı isi m isi m göstermemelidir .

Açıklamalar/Notlar: Kurulu ş şemaları , hiyerarş i şemaları , çalışa n ya d a bölü m listeleri , raporlam a yapısı, adlar , unvanlar , dahil i telefo n numaraları, çalışa n numarala n y a d a şirke t yapısın a yöneli k benzer i bil - giler interne t sayfalarınd a gene l erişim e açı k olmamalıdırlar .

Bilgisayar kırıcıları , yararl ı bilgiler i sı k sı k hedefi n interne t sayfasında n bulurlar. Saldırgan , çevirdiğ i bi r dolapt a konuy a haki m bi r çalışa n gib i görün - mek içi n b u bilgiy i kullanır . Elind e b u bilg i varke n toplu m mühendisini n inandırıcı olm a olasılığ ı dah a fazladır . Dahası , saldırgan , b u bilgiy i inceleyere k değerli, hassa s y a d a öneml i bilgiler e erişim i olabilece k hedefler i bulabilir .

7-12 Ayrıcalıkl ı hesapları n oluşturulmas ı

Kural: Siste m yöneticis i tarafında n onaylanmadığ ı sürec e hiçbi r ayrıcalıklı hesa p açılmamal ı y a d a herhang i bi r hesabı n siste m yetkiler i artırılmamahdır.

Açıklamalar/Notlar. Bilgisaya r kırıcılar ı sı k sı k donanı m y a d a yazılım satıcıs ı firm a yetkilis i gib i davranara k tekni k personel i onaylan -

mamış hesapla r açmalar ı doğrultusund a kandırmay a çalışabilirler . B u kuralın amacı , ayrıcalıkl ı hesapları n oluşurulmas ı üzerin e dah a büyü k bir deneti m getirere k b u saldırılar ı engellemektir . Yükse k yetkilerl e donatılmış bi r hesa p açm a talebin i siste m yöneticis i onaylamı ş olmalıdır.

7-13 Misafi r hesaplar ı

Kural: Herhang i bi r bilgisaya r sistemind e y a d a ilgil i a ğ araçlarınd a bulunan misafi r hesapları , yönetimi n onayladığ ı adsı z erişiml i FT P (dosya aktarı m protokolü) sunucus u hariç , devr e dış ı bırakılmal ı y a d a kaldırılmalıdır.

Açıklamalar/Notlar: Misafi r hesabı n amac ı kendilerin e ai t bi r hesa p açılmasına gere k olmaya n kişiler e geçic i erişi m sağlamaktır . Pe k ço k işletim sistem i misafi r hesapla r açılmı ş olara k gelir . Misafi r hesapla r he r zaman devr e dış ı bırakılmalıdır , çünk ü varlıklar ı kullanıc ı sorumluluğ u ilkesine aykırıdır . B İ tü m bilgisayarlardak i faaliyet i denetleyebilme n v e onları belirl i bi r kullanıcıyl a bağdaştırabilmelidir .

Toplum mühendisler i y a doğruda n kullanı p y a d a yetkil i personel i bi r misafir hesab ı kullanmay a ikn a edi p yetkisi z erişi m sağlama k içi n misa - fir hesaplarında n kolaylıkl a yararlanırlar .

7-14 Şirke t dışınd a tutula n yedekleri n şiîrelenmes i

Kural: Şirke t dışınd a tutula n herhang i bi r ver i yetkisi z erişim i engellemek içi n şifrelenmelidir .

Açıklamalar/Kurallar: Herhang i bi r bilgini n yenide n yerin e koyul - ması gerektiğ i durumlard a sorumlula r tü m bilgileri n ger i getirilebile - ceğinden emi n olmalıdırlar . B u da , verileri n ger i getirilebileceğinde n emin olma k içi n düzenl i olara k şifrel i dosyalarda n rastgel e bi r örneklem e deneme deşifrelemes i yapılmasın ı gerektirir . Ayrıc a veriler i şifreleme k için kullanıla n anahta r kaybolm a y a d a bulunamam a olasılığın a karş ı güvenilir bi r yöneticiy e emane t edilmelidir .

7-15 Â ğ bağlantıların a ziyaretç i erişim i

Kural: Herkes e açı k tü m etheme t erişi m noktala n dahil i ağ a yetkisi z ulaşımı engelleme k içi n parçal ı ağd a (segmente d network) bulundurul - malıdır.

Açıklamalar/Notlar: B u kuralı n amacı , dışarıda n kişileri n şirke t alanına girdiklerind e dahil î ağ a bağlanmaların ı önlemektir . Konferan s salonlarına, kafeteryaya , eğiti m merkezlerin e y a d a ziyaretçileri n erişim i olabilecek başk a yerler e yerleştirile n etherne t girişler i ziyaretçileri n şirke t bilgisayar sistemlerin e yetkisi z erişimin i engelleme k içi n filtreienmelidir .

Ağ ya da güvenli k sorumlusu , bu noktalarda n erişim i engelleye - bilmek için , eğe r varsa , sana l bi r LA N anahtar ı oluşturmay ı seçebilir .

7-16 Bağlant ı modemler i

Kural: Aramalar a açı k bağlant ı modemler i dördünc ü çalışta n önc e açılmayacak şekild e ayarlanmalıdırlar .

Açıklamalar/Notlar: Sava ş Oyunlar ı (Wa r Games) adl ı filmd e d e anlatıldığı gib i korsanla r mode m bağl ı telefo n hatların ı bulma k içi n savaş aramas ı olara k biline n bi r tekni k kullanırlar . Süreç , saldırganı n şir - ketin bulunduğ u bölged e kullanıla n ala n prefikslerin i tanımlamas ı il e başlar. B u prefiksl e başlaya n he r numara , mode m bağl ı hatlar ı bulma k için bi r taram a programını n d a yardımıyl a taranır . Sürec i hızlandırma k için b u programla r bi r sonrak i numaray ı denemede n önc e mode m yanıtını bi r y a d a ik i çalı ş süres i kada r bekleme k üzer e ayarlanmışlardır . Bir şirke t mode m hattını n otomati k yanı t seçeneğin i e n a z dör t çalı ş olarak ayarlars a taram a programlar ı modeml i hatlar ı bulamayacaklardır .

7-17 Virü s korum a yazılımlar ı

Kural: He r bilgisaya r sistemin e virü s korum a yazılımlarını n so n sürümleri yüklenmel i v e çalıştırılmalıdır .

Açıklamalar/Notlar: Virü s korum a yazılımların ı v e şablo n dosyalarını (yen i virüsler i bulma k içi n virü s yazılımların a özg ü şablonlar ı tanıyan programlar) kullanıc ı bilgisayarların a kada r otomati k olara k indi - rememiş şirketlerd e bireyse l kullanıcılar , yazılımı , şirke t ağın a uzakta n erişmek içi n kullanıla n bilgisaya r sistemlerindekile r d e dahil , kend i sis - temlerine yüklem e v e sürekl i güncellem e sorumluluğun u almalıdırlar .

Eğer uyguns a b u yazılı m virü s v e Truv a At ı imzalar ı içi n he r gec e otomatik olara k güncellenece k şekild e ayarlanmalıdır . Şablo n y a d a imza dosyala n kullanıc ı bilgisayarların a kada r indirilmezse , kullanıcıla r en azında n haftad a bi r şablo n dosyaların ı güncellem e sorumluluğun u taşıyacaklardır.

Bu uygulamala r şirke t bilgisaya r sistemlerin e bağlana n tü m masaüstü v e dizüst ü makinala r içi n geçerlidi r v e bilgisayarı n şirket e ai t ya d a şahs a ai t olu p olmadığın a gör e d e değişmez .

7-18 Gele n e-post a ekler i (yükse k güvenli k gereksinimi)

Kural: Yükse k güvenli k ihtiyaçlar ı ola n bi r kuruluşt a şirke t güvenli k duvarı tü m e-post a eklerin i eleyece k şekild e ayarlanmalıdır .

Açıklamalar/Notlar: B u kura l yalnızc a yükse k güvenli k gereksinim - leri ola n y a d a e-post a ekind e dosy a almay a ihtiyac ı olmaya n işletme - ler içi n geçerlidir .

7-19 Yazılı m onay ı

Kural: Tü m yen i yazılımlar , yazılı m çözümler i y a d a güncellemeleri , ister fizikse l ortamd a olsun , iste r interne t üzerinde n eld e edilmi ş olsu n

J Şirke t Bilg i Güvenliğ i Kurallar ı Öneriler i 27 5 %

f yüklenmede n önc e güvenilirlikler i doğrulanmalıdır . B u kural , özellikl e I siste m yetkile n gerektire n yazılımla r yüklenirke n bilg i işle m bölümün ü j|s ilgilendirir .

t>-

Açıklamalar/Notlar: B u kurald a söz ü edile n bilgisaya r yazılımlar ı

işletim sistem i parçalarını , uygulamaları , yazılı m çözümlerini , yamalar ı

ya d a herhang i bi r yazılı m güncellemesin i içerir . Pe k ço k yazılı m üreti -

cisi, müşterini n dağıtımı n içeriğin i genellikl e bi r dijita l imz a kullanara k

kontrol edebileceğ i yöntemle r yerleştirmişlerdir , içeriği n onaylanmadığ ı

her durumda , yazılımı n güvenilirliğin i doğrulama k içi n üreticiy e başvu -

rulmalıdır.

Bilgisayar saldırganlarını n yazılı m üreticisind e yapılmı ş v e şirket e postalanmış gib i görünen bi r paketl e kurban a yazılı m gönderdiğ i d e bi - linmektedir. Aldığını z he r yazılımın , özellikl e d e tale p etmediğini z bi r yazılımsa, şirke t sistemin e yüklemede n önc e güvenilirliğin i doğrula - manız önemlidir .

Becerikli bi r saldırganı n kurumunuzu n bi r üreticide n yazılı m sipari ş ettiğini öğrenebileceğin i unutmayın . Elind e b u bilg i varke n saldırgan , gerçek üreticiy e verile n sipariş i ipta l edebili r v e sipariş i kend i yerin e getirebilir. O zama n yazılım , köt ü huyl u bi r işle v gerçekleştirme k üzer e değiştirilmiş olu r v e şirketiniz e ası l paketinde , gerekirs e vakumlanmı ş olarak gönderilir . Ürü n yüklendikte n sonr a kontro l artı k saldırganı n elin e geçer.

7-20 Varsayıla n parolala r

Kura!: Varsayıla n bi r parolay a sahi p ola n tü m işleti m sistem i yazılımlarının v e donanımlarını n şirke t parol a kurallar ı doğrultusund a parolaları değiştirilmelidir .

Açıklamalar/Notiar: Pe k ço k işleti m sistem i ve bilgisayarl a ilgil i donanımlar varsayıla n parolalarl a gönderilirler ; diğe r bi r deyişl e satıla n her parç a ayn ı parolay a sahiptir . Varsayıla n parolaları n değiştirilmes i konusunu ihma l etmek , şirket i tehlikey e soka n cidd i bi r hatadır .

Varsayılan parolala r herkesç e bilinirle r v e interne t sayfalarınd a bulunurlar. Bi r saldır ı sırasınd a saldırganı n denediğ i il k parola , üreticini n koyduğu varsayıla n paroladır .

7-21 Başarısı z erişi m denemeler i sonuc u kilitlenm e

(düşük-orta düze y güvenlik)

Kural: Özellikl e düşü k v e ort a düze y güvenli k gereksinimler i ola n bi r kurumda ayn ı hesab a birbir i ardın a belirl i bi r sayıd a girm e girişim i olur - sa hesa p bi r süreliğin e kilitlenmelidir .

Açıklamalar/Notlar: Tü m şirke t bilgisayarlar ı v e sunucuların a birbir i ardına yapıla n başarısı z girm e denemelerin e bi r sını r getirilmelidir . B u

kural denem e yanılmayl a parol a tahmini , sözlü k saldırıs ı y a d a kab a kuvvetle yetkisi z erişi m sağlam a yöntemlerin i engelleme k içi n gereklidir .

Sistem yöneticis i güvenli k ayarlarını , peşpeş e başarısı z bağlanm a girişimi eşiğin e gelindiğind e hesab ı kilitleyece k şekild e yapmalıdır . Yed i başarısız denemede n sonr a bi r hesabı n e n a z otu z dakik a boyunc a kilit - lenmesi önerilir .

7-22 Başarısı z erişi m girişimler i sonuc u hesabı n

kapatılması (yükse k güvenlik)

Kural: Yükse k güvenli k gereksinimler i ola n bi r kurumd a ayn ı hesa - ba birbir i ardın a belirl i bi r sayıd a başarısı z girm e girişim i olurs a hesap , desteği vere n gru p tarafında n düzeltilen e kada r kapatılmalıdır .

AçtkSamalar/Notlar: Tü m şirke t bilgisayarlar ı v e sunucuların a birbir i ardına yapıla n başarısı z girm e denemelerin e bi r sını r getirilmelidir . B u kural denem e yanılmayl a parol a tahmini , sözlü k saldırıs ı y a d a kab a kuvvetle yetkisi z erişi m sağlam a yöntemlerin i engelleme k içi n gereklidir .

Sistem yöneticisi , güvenli k ayarlarını , be ş başarısı z bağlanm a girişi - minden sonr a hesab ı kapayaca k şekild e yapmalıdır . Böyl e bi r saldırını n ardından hesa p sahibini n hesab ı açtırma k içi n tekni k deste k birimin i y a da hesa p desteğinde n soruml u grub u aramas ı gerekir . Hesab ı yenide n devreye sokmada n önc e ilgil i birimi n Ona y v e Yetkilendirm e Süreçlerin e • uygun olara k hesa p sahib i içi n kesinlikl e bi r kimli k tespit i yapmas ı şarttır .

7-23 Ayrıcalıkl ı hesapları n parolalarını n düzenl i olara k

değiştirilmesi

Kural: Tü m ayrıcalıkl ı hesa p sahiplerini n e n ço k otu z günd e bi r parolalarını değiştirmeler i zorunluluğ u getirilecektir .

Açıklamalar/Notlar: İşleti m sistem i sınırlamaların a bağl ı olarak , sis - tem yöneticis i siste m yazılımını n güvenli k özelliklerin i ayarlayara k kul - lanıcıları b u kural a uymay a zorlayabilir .

7-24 Kullanıc ı parolalarını n düzenl i olara k değişim i

Kurai: Tü m hesa p sahipler i e n ço k altmı ş günd e bi r parolaların ı değiştirmelidirler.

Açıklamalar/Notlar: B u özelliğ e sahi p işleti m sistemler i kullanarak , sistem yöneticisi , yazılımı n güvenli k özelliklerini n ayarlanmasıyl a kul - lanıcıları b u kural a uymay a zorlayabilir .

7-25 Yen i hesa p parolas ı oluşturma k

Kural: Yen i bilgisaya r hesapları , süres i dolmu ş bi r parolayl a oluştu - rulmalı, böylec e hesa p sahibin e il k kullanı m içi n yen i bi r parol a belirlem e zorunluluğu getirilmelidir . ,

Şirket Bilg i Güvenliğ i Kurallar ı Öneriler i 27 7

Açıklamalar/Notlar: B u zorunlulu k kend i parolasın ı hesa p sahibinden başk a kimseni n bilmemesin i sağlar .

7-26 Açılı ş parolalar ı

Kural: Tü m bilgisaya r sistemler i açılışt a parol a isteyece k şekild e ayarlanmalıdırlar.

Açiklama!ar/Notlar: Bilgisayarla r açıldıklar ı zama n işleti m sistem i yüklenmeden önc e parol a soraca k şekild e ayarlanmalıdırlar . Bu , yetki - siz kimseleri n başk a birini n bilgisayarın ı açı p kullanmasın ı engeller . B u kural şirke t içindek i tü m bilgisayarla r içi n geçerlidir .

7-27 Ayrıcalıkl ı hesapla r içi n parol a zorunluluklar ı

Kural: Tü m ayrıcalıkl ı hesapları n güçl ü parolalar ı olmalıdır . Parol a aşağıdaki özellikler e uymalıdır .

• Herhang i bi r dildek i sözlüklerd e bulunmamalıdır .

• Büyü k v e küçü k harflerde n oluşmal ı v e e n a z bi r harf , bi r simg e

ve bi r say ı içermelidir .

» E n a z 1 2 karakte r uzunluğund a olmalıdır . . "

• Şirket e y a d a birey e herhang i bi r nedenl e verilmemelidir .

Açıklamalar/Notlar: Çoğ u durumd a bilgisaya r kırıcılar ı siste m yet - kileri eld e etme k içi n belirl i hesaplar ı hedeflerler . Zama n zama n saldır - gan, siste m üzerind e ta m kontro l sağlama k içi n başk a açıklar ı d a sömürür.

Saldırganın deneyeceğ i il k parolala r basit , sözlükt e buluna n sı k kul - lanılan kelimele r olacaktır . Güçl ü parolaları n seçilmesi , bi r saldırganı n deneme yanılma , sözlü k saldırıs ı y a d a kab a kuvve t saldırıs ı kullanara k parolayı bulm a olasılığın ı azaltı r v e güvenliğ i artırır .

7-28 Telsi z erişi m noktalar ı

Kural: Bi r telsi z ağın a erişim i ola n tü m kullanıcıla r şirke t ağların ı korumak içi n VP N (virtua l privat e netvvor k - sana l öze l ağ) teknolojis i kullanmalıdırlar.

Açıklamalar/Notlar: Telsi z ağlara , sava ş sürüş ü ad ı verile n yen i bi r yöntemle saldırılıyor . B u yönte m 802.11 B NI C kartıyl a donanmı ş bi r dizüstü bilgisayarl a telsi z ağ ı bulan a kada r yürüme k y a d a arabayl a dolaşmaktan ibaret .

Pek ço k şirke t telsi z bağlantısın ı şifreleyere k güvenc e altın a ala n VVEP'i (vvireles s equivalenc y protoko l - telsi z denkli k protokolü) bil e devreye sokmada n telsi z ağların ı kullanmay a

başladılar . Açı k olduğ u zaman bil e VVEP'i n geçerl i sürüm ü (2002'ni n ortalarında) yetersizdir .

Kırılıp ardın a kada r açılmıştı r v e pe k ço k interne t sites i açı k telsi z sis - temlerini bulma k içi n yöntemle r üretmey e v e WE P özelliğ i açı k telsi z erişim noktaların ı kırmay a adanmıştır .

Bu yüzden , VP N teknolojis i kullanara k 802.1 1 B protokolün e e k bi r koruma sağlanmas ı önemlidir .

7-29 Virü s şablo n dosyalarını n güncellenmes i

Kural: He r bilgisaya r sistemi virü s korum a yazılımlar ı içi n virüs/Truva At ı şablo n dosyaların ı otomati k olara k güncelleme k üzer e programlanmalıdır. . . . •

Açsklamalar/Notlar: B u tar z güncellemele r e n azında n haftad a bi r yapılmalıdır. Çalışanların , bilgisayarların ı açı k bıraktıklar ı işletmelerd e şablon dosyalarını n he r gec e güncellenmes i şiddetl e önerilir .

Virüs korum a yazılımlar ı yen i tü r köt ü huyl u yazılımlar ı görece k şe - kilde güncellenmezs e etkisi z kalır . Dese n dosyalar ı güncellenmediğind e virüs, soluca n v e Truv a At ı tehlikes i büyü k ölçüd e arttığ ı içi n virü s y a d a kötü huyl u yazılı m korum a ürünlerini n günce l tutulmas ı önemlidir .

Bilgisayar İşlemler i • "

8-1 Komu t girme k v e progra m çalıştırma k

Kural: Bilgisaya r işlemlerinde n soruml u personel , tanımadıklar ı birinden gele n tale p üzerin e komu t girmemel i v e progra m çalıştırma - malıdır. Onaylanmamı ş bi r kişini n istekt e bulunma k içi n geçerl i bi r nedeni varmı ş gib i görüne n durumla r ortay a çıkars a öncelikl e yöneticinin onay ı alınmada n b u iste k yerin e getirilmemelidir .

Açıklamalar/Notlar: Bilgisaya r işlemler i çalışanları , konumlar ı gereği çoğunlukl a ayrıcalıkl ı hesa p erişimler i olduğ u içi n toplu m mühendislerinin ço k kullandığ ı hedefle r arasındadırla r v e saldırga n onların diğe r B i çalışanlarına gör e şirke t süreçleriyl e ilgil i olara k dah a a z bilgili v e dah a a z deneyiml i oldukların ı düşünür . B u kuralı n amacı , toplum mühendislerini n bilgisaya r işlemler i çalışanların ı kandırmaların ı önlemek amacıyl a uygu n bi r kontro l v e deng e unsur u oluşturmaktır .

8-2 Ayrıcalıkl ı hesab i ola n çalışanla r

Kural: Ayrıcalıkl ı hesapla n ola n çalışanla r onaylanmamı ş kişiler e destek v e bilg i vermemelidirler . Özellikl e d e bilgisaya r yardım ı (bi r uygu - lamanın kullanım ı konusund a eğiti m gibi) , herhang i bi r şirke t veritabanı - na erişim , yazılı m indirm e y a d a uzakta n erişi m yeteneğin e sahi p çalışanların adlarını n açıklanmas ı gib i durumla r sö z konus u olduğund a bu geçerlidir .

Açıklamalar/Notlar: Toplu m mühendisler i çoğunlukl a ayrıcalıkl ı

hesaplan ola n çalışanlar ı hedeflerler . B u kuralı n amac ı ayrıcalıkl ı hesaplara sahi p B İ çalışanların ı toplu m mühendisliğ i saldırıs ı olabilece k telefonları başarıyl a el e almalar ı konusund a yönlendirmektir .

8-3 Dahil î siste m bilgiler i

Kural: Bilgisaya r işlemler i personeli , iste k sahibin e kimli k tespit i yapmadan, şirke t bilgisaya r sistemler i y a d a ilgil i donanımlarl a ilgil i değerli bilgiler i kesinlikl e açıklamamalıdır .

Açıklamalar/Notlar: Bilgisaya r kırıcılar ı siste m erişi m süreçleri , ha - ricî uzakta n erişi m noktalar ı v e telefo n bağlant ı numaralar ı gibi , saldır - gan içi n öneml i olabilece k değerli bilgiler i eld e edebilme k içi n sı k sı k bil - gisayar işlemler i personeliyl e iletişi m kurarlar .

Teknik deste k personel i y a d a yardı m masas ı ola n şirketlerde , bil - gisayar sistemler i y a d a ilgil i donanım a yöneli k soruları n bilgisaya r işlemleri personelin e gelmes i olağandış ı bi r duru m olara k görülmelidir . Herhangi bi r ver i talebi , şirke t ver i sınıflandırm a kurallar ı çerçevesind e istek sahibini n b u bilgiy i istemey e yetkil i olu p olmadığın ı belirleme k üzere incelenmelidir . Ver i sınıfin a kara r verilemediğind e bilg i dahilî olarak değerlendirilmelidir .

Bazı durumlard a satıc ı firmada n gele n tekni k deste k sorumlularının , şirketin bilgisaya r sistemin e erişim i ola n kişilerl e iletişi m kurmalar ı gerekir. B u tar z firmaların , şirketleri n B İ bölümlerind e iletişi m kurduklar ı belirli kişile r olmas ı gerekir , böylec e b u kişile r karşılıkl ı ona y açısından birbirlerini tanıyo r olurlar .

8-4 Parolaları n açıklanmas ı

Kural: Bilgisaya r işlemler i personel i hiçbi r zama n kendilerin e ai t olan y a d a onlar a emane t edilmi ş parolalar ı bi r bilg i işle m yöneticisini n onayı olmada n açıklamamalıdırlar .

Açıklamalar/Notlar: Gene l olara k başk a birin e parol a söyleme k yasaktır. Kural , aci l bi r durumd a bilgisaya r işlemler i personelini n üçünc ü şahıslara bi r parolay ı verebileceğ i durumun u gö z önünd e bulundurur . Herhangi bi r parolanı n açıklanmasın ı yasaklaya n gene l kural a gele n b u istisna, bi r bilg i işle m yöneticisini n öze l iznin i gerektirir . Dah a fazl a önle m almak adına , tanımlam a bilgilerin i açıklam a sorumluluğunun , ona y süreç - leriyle ilgil i öze l eğiti m almı ş bi r gru p kişiyl e sınırlandırılmas ı d a şarttır .

8-5 Elektroni k orta m

Kural: Dışar ı verilme k üzer e sınıflandırılmamı ş bilgile r içere n tü m elektronik ortamla r fizikse l olara k güvenl i bi r yer e kilitlenmelidirler .

Açıklamalar/Notlar: B u kuralı n amac ı elektroni k ortamlard a saklan - mış hassa s bilgileri n fizikse l olara k çalınmasın ı önlemektir .

8-7 Yedeklem e ortamlar ı

Kural: Bilgisaya r işlemler i personel i yedeklem e ortamların ı şirke t kasasında y a d a başk a bi r güvenl i yerd e saklamalıdır .

Açıklamalar/Notlar: Yedeklem e ortamlar ı bilgisaya r kırıcılarını n başlıca hedeflerindendir . Zinciri n zayı f halkas ı fizikse l olara k korun - mayan yedeklem e ortamlar ı olabilecekken , bi r saldırgan , bi r bilgisaya r sistemine girmey e çalışma k içi n zama n harcamayacaktır . Yedeklem e ortamları çalındıkta n sonr a saldırgan , verile r şifrel i olmadığ ı sürece , oraya kayıtl ı herhang i bi r dosyay a erişebilecektir . B u yüzde n yedeklem e ortamlarını fizikse l olara k güvenc e altın a alma k şirke t bilgilerini n gizliliği - ni koruma k içi n öneml i bi r süre ç olacaktır .

*

Tüm Çalışanla r İçi n Geçerl i Kurallar

Bilgi işlem , insa n kaynakları , muhaseb e y a d a deste k hizmetleri ; şir - ketin neresind e çalışıyo r olurlars a olsunla r he r çalışanı n bilmes i gereken belirl i güvenli k kurallar ı vardır . B u kurallar , genel , bilgisaya r kul - lanımı, e-post a kullanımı , evde n çalışanlar a yöneli k kurallar , telefo n kul - lanımı, fak s kullanımı , sesl i mesa j kullanım ı v e parolala r şeklind e sınıflandırılmıştır.

Genel

9-1 Şüphel i aramaları n rapo r edilmes i

Kural: Herhang i bi r şüphel i bilg i y a d a bilgisaya r işlem i talebind e bulunulması durum u d a dahi l olma k üzer e bi r güvenli k ihlalin e maru z kaldıklarından kuşkulana n çalışanla r heme n olay ı şirketi n ola y bildirm e grubuna bildirmelidirler .

Açıklamalar/Notlar: Toplu m mühendisi , isteklerin i yerin e getirmey e hedefini ikn a edemediğ i durumda , he r zama n başk a birin i deneyecektir . Şüpheii bi r aramay ı y a d a olay ı bildire n çalışan , bi r saldır ı olduğ u yolun - da şirket i bilgilendirme k içi n il k adım ı atmı ş olur . Böylece , çalışanlar , toplum mühendisliğ i saldırıların a karş ı il k savunm a hattın ı oluştururlar .

9-2 Şüphel i aramalar ı belgeleme k

Kural: Bi r toplu m mühendisliğ i saldırıs ı gib i görünen şüphel i bi r ara - mada, çalışan , uygu n olduğ u ölçüde , saldırganı n n e başarmay a çalıştığını anlataca k kada r ayrınt ı öğrenmey e çalışmal ı v e belgelem e amacıyla b u ayrıntılarl a ilgil i notla r almalıdır .

Açıklamalar/Notlar: B u tar z ayrıntılar , ola y bildirm e grubun a bildirildiğinde, saldırını n yönünü n y a d a amacını n bulunmasın a yardımc ı olur. '

Şirket Bilg i Güvenliğ i Kurallar ı Öneriler i 28 1

9-3 Bağlant ı numaralarını n verilmes i

Kural: Şirke t çalışanlar ı şirketi n mode m telefo n numaraların ı açıkla - mamah v e b u tar z istekler i he r zama n yardı m masasın a y a d a tekni k destek personelin e yönlendirmelidir .

Açıkîamalar/NotSar: Bağlant ı telefo n numaralan , yalnızc a i ş yüküm - lülüklerini yerin e getirebilme k içi n bunu n gib i bilgiler e gereksinim i ola n çalışanlara verilece k türde n bi r dahil î bilg i olara k değerlendirilmelidir .

Toplum mühendisler i düzenl i olara k biig i taleplerin e karş ı dah a a z korumacı davranaca k çalışanlar ı y a d a bölümler i hedeflerler . Örneği n saldırgan, bi r faturalam a sorunun u çözmey e çalışa n bi r telefo n şirket i çalışanı gib i kendin i gösteri p ödemele r bölümün ü arayabilir . Saldırga n daha sonr a sorun u çözebilme k içi n bildikler i başk a fak s y a d a bağlant ı numarası olu p olmadığın ı sorar . Toplu m mühendis i sı k sı k b u tar z bilgiy i vermenin oluşturduğ u tehlikeni n farkınd a olmaya n y a d a şirke t bilg i verm e kural v e süreçlerin e yöneli k yeterl i eğitim i almamı ş bi r çalışan ı seçer .

9-4 Şirke t kimli k kartlar ı

Kural: içind e bulunduklar ı ofi s bölges i haricinde , üs t v e ort a yöneti m de dahil , tü m şirke t çalışanlar ı he r zama n persone l kartların ı takmalıdırlar .

Âçıkiamaiar/Notlar: Şirke t yöneticiler i d e dahi l tü m çalışanlar , halk a açık yerle r y a d a kişini n kend i ofis i y a d a çalışm a alan ı dışındak i he r yerde, kimli k takmanı n zorunl u olduğun u anlamalar ı içi n eğitilmel i v e teşvik edilmelidirler . . . : .

9-5 Kimlik kart ı ihiaüerini n sorgulanmas ı

Kural: Tü m çalışanla r şirke t kimli k kart ı y a d a ziyaretç i kart ı tak - mayan tanımadıklar ı kişiler i heme n sorgulamalıdırlar .

Açıklamalar/Notlar: He r n e kada r hiçbi r şirket , açı k gö z çalışanları n kimliksiz koridor a çıka n başk a çalışanlar ı enseled iğ i bi r kültü r yaratma k istemese d e bilgilerin i korum a endişesin e sahi p herhang i bi r şirketin , bina içind e sorgulanmada n dolaşa n bi r toplu m mühendis i tehdidin i d e ciddiye almas ı gerekir . "He r zama n kartl ı dolaş " kuralın ı yerleştirme k içi n gayretli olduğun u göstere n çalışanlar ı teşvi k etme k içi n şirke t gazetesinde y a d a bülte n panosund a duyurulması , birka ç saatli k ücretl i izin y a d a şahs i dosyasın a konaca k bi r tavsiy e mektub u verilmes i gib i çeşitli uygulamala r kullanılabilir .

9-6 Peşpeş e geçme k (güvenlikl i girişlerde n geçişler)

Kural: Binay a gire n çalışanlar , içer i girme k içi n manyeti k kar t gib i güvenli araçla r kullandıklarınd a tanımadıklar ı hi ç kimseni n heme n arkalarından gelmesin e izi n vermemelidirle r (peşpeş e geçmek) .

Açıklamalar/Notlar: Çalışanlar , bi r tesis e y a d a güvenl i bi r alan a

girmeye çalışa n tanımadıklar ı kişileri n kendilerin i tanıtmaların ı iste - menin, kabalı k olmayacağın ı bilmelidirler .

Toplum mühendisler i peşpeş e geçm e olara k biline n bi r tekni k kul- lanırlar. B u teknikt e tesis e y a d a hassa s bi r alan a gire n birin i beklerle r ve onunla birlikt e içer i giriverirler . Çoğ u insan , büyü k olasılıkl a şirke t çalışanı oldukların ı varsaydığ ı diğe r kişiler i sorgulamakta n rahatsı z olur . Başka bi r peşpeş e geçm e tekniğ i is e bi r sür ü kutuy u birde n taşımaktır , böylece hiçbi r şeyi n farkınd a olmaya n bi r çalışan , yardı m etme k içi n kapıyı açа r y a d a tutar .

9-7 Hassa s belgeleri n kâğı t öğütücüde n geçirilmes i

Kural: Atılaca k hassa s belgele r çapra z öğütücüde n geçirilmelidir . Herhangi bi r zamand a hassa s bilgile r y a d a malzemele r içermi ş ola n sabit sürücüle r d e dahi l tü m taşınabili r ortamla r bilg i güvenliğinde n sorumlu gru p tarafında n belirlene n süreçle r gereğinc e yo k edilmelidir .

Açıklamalar/Notlar: Sırada n kâğı t öğütücüle r belgeler i yeterl i ölçüde parçalamazlar ; çapraz- öğütücüle r is e belgeler i tanınma z durum a getirirler. E n iy i güvenli k uygulaması , kuruluşun , başlıc a rakiplerinin , atılmış malzemeleri n arasınd a işlerin e yarayaca k bilgile r arayacakların ı varsaymasıdır.

Sanayi casuslar ı v e bilgisaya r sadırganlar ı hassa s bilgiler i sürekl i çöpe atılmı ş malzemelerde n çıkarırlar . Baz ı durumlard a raki p şirketleri n çöpleri vermeler i içi n temizlikçiler e rüşve t vermey e teşebbü s ettikler i d e bilinir. Yakı n bi r örnek , bi r sermay e piyasas ı arac ı kurum u çalışan ı içeri - den edinile n bilgiyl e yapıla n alı m satımlar a yöneli k çöpt e bi r takı m malzemeler bulmuştu .

9-8 Kişise l tanımlayıcıla r

Kural: Kimli k numarası , Sosya l Güvenli k Numarası , ehliye t numarası, doğu m tarih i v e yer i v e anneni n kızlı k soyad ı gib i kişise l tanımlayıcılar kimli k tespit i amacıyl a kullanılmamalıdırlar . B u tanım - layıcılar sı r değildi r v e sayısı z yönteml e eld e edilebilirler .

Açıklamalar/Notlar: Bi r toplu m mühendis i başk a insanları n kişise l tanımlayıcılarını bi r ücre t karşılığınd a edinebilir . Aslınd a gene l kanını n aksine interne t erişim i v e kred i kart ı ola n herhang i bir i b u kişise l tanımlam a bilgilerini el e geçirebilir . Açı k tehlikey e karşı n bankalar , hizme t şirketler i v e kredi kart ı şirketler i sı k sı k b u tanımlayıcılar ı kullanmaktadırlar . Sadec e b u nedenle kimli k hırsızlığ ı so n o n yılı n e n hızl ı arta n suç u olmuştur .

9-9 Kurulu ş şemalar ı

Kural: Şirketi n kurulu ş şemasınd a gösterile n ayrıntıla r şirke t çalışanları dışınd a kimsey e verilmemelidir .

Açıklamalar/Notlar: Şirke t yapıs ı bilgiler i kurulu ş şemalarını , hiye -

rarşi şemalarını , bölü m çalışa n listelerini , raporlam a yapısını , çalışa n adlarını, çalışa n unvanlarını , dahil î telefo n numaralarını , kimli k numa - ralarını y a d a benzer i bilgiler i içerir .

Toplum mühendisliğ i saldırısını n il k aşamasınd a ama ç şirketi n i ç yapısıyla ilgil i bilg i toplamaktır . Sonr a b u bilgile r bi r saldır ı plan ı yapma k için kullanılır . Saldırgan , hang i çalışanları n aradığ ı bilgiy e erişim i ola - bileceğine kara r verebilme k içi n b u bilgiy i inceler . Saldır ı sırasınd a bilgi , saldırganın işin e haki m bi r çalışa n olara k görünmesin i sağla r v e kur - banını i ş birliğ i yapmay a ikn a etm e olasılığını artırır .

9-10 Çalışanlarl a ilgil i öze l bilgile r

Kural: Çalışanları n öze l bilgilerin e yöneli k tü m taleple r insa n kay - naklarına yönlendirilmelidir .

Açıklamalar/Notlar: B u kuralı n bi r istisnası , işl e ilgil i bi r konud a bağlantı kurulmas ı gereke n y a d a karş ı tarafta n telefon bekleye n bi r çalışanın telefo n numarasını n verilmes i olabilir . Anca k numaray ı isteye n kişinin telefo n numarasını n alınmas ı v e çalışanı n on u ger i aramas ı he r zaman terci h edilmes i gereke n yoldur .

Bilgisayar Kullanım ı

10-1 Bilgisayar a komu t girme k

Kural: iste k sahibini n bilg i işle m bölümünü n bi r çalışan ı olduğ u onaylanmadığı sürec e şirke t çalışanları , başk a birini n isteğ i üzerin e bil - gisayara y a d a bilgisayarlarl a ilgil i donanım a hiçbi r zama n komu t girmemelidirler.

Açıklamalar/Notlar: Toplu m mühendislerini n sıkç a oynadığ ı bi r oyun , çalışandan siste m ayarların ı değiştire n bi r komu t girmesin i istemeleridir . Bu sayed e saldırgan , kendin i tanıtmada n kurbanı n bilgisayarın a girebili r ya d a tekni k bi r saldırıd a kullanılabilece k bilgiler e erişebilir .

10-2 Dahil î adlandırm a standartlar ı

Kural: iste k sahibini n şirkett e çalıştığ ı onaylanmada n çalışanla r bil - gisayar sistemlerini n y a d a ver i tabanlarını n adların ı açıklamamalıdırlar .

Açıklamalar/Notlar: Toplu m mühendisleri baze n şirke t bilgisaya r sistemlerinin adların ı eld e etmey e çalışırlar . Adlar ı öğrendikte n sonr a saldırgan, şirket i ara r v e sistemler i kullanmakt a soru n çeke n bi r çalışa n gibi davranır . Toplu m mühendis i o sistem e verile n dahil î ad ı bilere k inandırıcılığını artırır .

10-3 Progra m çalıştırm a talepler i

Kural: Şirke t çalışanları , başk a birini n isteğ i üzerin e herhang i bi r bil - gisayar uygulamasın ı y a d a programın ı çalıştırmamalıdırlar .

Açıklamalar/Notlar: Progra m vey a uygulam a çalıştırmay a y a d a bilgisayarda herhang i bi r işle m yapmay a yöneli k taleple r tale p sahibini n bilgi işle m bölüm ü çalışan ı olduğ u onaylanan a kada r reddedilmelidir . Eğer tale p bi r dosyadan y a d a elektroni k mesajdan , gizl i bilgileri n çe - kilmesiyle ilgiliyse , taleb e karşılı k vermek , gizl i bilg i verm e süreçleriyl e uyumlu olmalıdı r (bkz . Bilg i Verm e Kuralları) .

Bilgisayar saldırganlar ı sistem i el e geçirmelerin i sağlayaca k prog - ramları çalıştırmalar ı içi n insanlar ı kandırırlar . Hiçbi r şeyde n kuşkulan - mayan bi r kullanıcı , saldırganı n yerleştirdiğ i bi r program ı çalıştırdığında , ortaya çıka n sonuç , saldırganın , kurbanı n bilgisayarın a erişmesin e neden olabilir . Bi r toplu m mühendis i zara r verebilece k bilgisaya r komut - larını çalıştırmas ı içi n birilerin i kandırabilirken , tekni k tabanl ı bi r saldırı , benzer bi r zarar ı bilgisaya r programların ı çalıştırmas ı içi n bilgisayarı n işletim sistemin i kandırara k yapabilir .

10-4 Yazılı m indirme k y a d a yükleme k

Kural: iste k sahibini n bilg i işle m bölümünü n bi r çalışan ı olduğ u onaylanmadığı sürec e şirke t çalışanlar ı başk a birini n isteğ i doğrultusun - da hiçbi r zama n yazılı m indirmemel i y a d a yüklememelidir .

Açıklamalar/Notlar: Çalışanla r bilgisayarlarl a ilgil i donanım a yöne - lik herhang i bi r olağandış ı işle m talebin e karş ı he r zama n uyanı k olmalıdırlar.

Toplum mühendislerinin sıkç a kullandığ ı taktiklerde n birisi , hiçbi r şeyden kuşkulanmaya n kurbanların ı saldırgan a bilgisaya r y a d a a ğ güvenliğini aşm a amacınd a yardımc ı olaca k bi r progra m yüklemey e y a da indirmey e ikn a etmektir . Baz ı durumlard a progra m gizlic e kullanıcıy ı gözetleyebilir y a d a gizl i bi r uzakta n kontro l yazılımıyl a saldırganı n bil - gisayar sistemin i el e geçirmesin i sağlayabilir .

10-5 Dü z meti n parolala r y e e-post a

Kural: Şifrel i olmadıklar ı sürec e parolala r e-postayl a gönderilmeme - lidirler.

Açıklamalar/Notlar: He r n e kada r önerilmes e d e b u kura l aşağıda - ki gib i sınırl ı koşullard a e-ticare t sitelerind e d e kullanılabilir :

» Sitey e kaydolmu ş müşteriler e parolalarını n gönderilmesi .

• Parolasın ı unutmu ş y a d a kaybetmi ş müşteriler e parolalarını n

gönderilmesi.

10-6 Güvenlikl e ilgil i yazılımla r

Kural: Şirke t çalışanlar ı hiçbi r zama n virüs/Truv a At ı koruma , güvenli k duvarı y a d a diğe r güvenlikl e ilgil i yazılımlar ı bilg i işle m bölümünde n alın - mış bi r ona y olmada n devr e dış ı

bırakmamal ı y a d a kaldırmamalıdırlar .

Şirket Bilg i Güvenliğ i Kurallar ı Öneriler i 28 5

Açıklamalar/Notlar: Bilgisaya r kullanıcılar ı baze n güvenlikl e ilgil i yazılımları, başk a herhang i bi r neden i olmadan , bilgisayarlarının hızın ı artıracağını düşünere k kapatırlar .

Bir toplu m mühendisi , güvenlikl e ilgil i tehditlerde n şirket i koruma k için gerekl i ola n bi r yazılım ı kaldırmas ı y a d a devr e dış ı bırakmas ı içi n bir çalışan ı kandırmay a çalışabilir .

10-7 Modemleri n yüklenmes i

Kural: B i bölümünde n ona y alınmada n herhang i bi r bilgisayar a modem bağlanamaz .

Açıklamalar/Notlar: Çalışm a ortamınd a masalard a y a d a bilgisa - yarların üstünd e dura n modemleri n -özellikl e d e şirke t ağın a bağlarsa - ciddi bi r güvenli k tehdid i oluşturduklar ı bilinmelidir . Bun a göre , b u kura l modem bağlam a süreçlerin i düzenlemektedir .

Bilgisayar korsanlar ı bi r telefo n silsilesin e bağl ı çalışa n bi r mode m hattı olu p olmadığın ı anlama k içi n sava ş aramas ı dene n bi r tekni k kul - lanırlar. Ayn ı teknik , şirke t içind e modemler e bağl ı telefo n numaraların ı bulmak içi n d e kullanılabilir . Eğe r saldırgan , bilgisaya r sisteminin , kola y tahmin edilebili r bi r parolas ı ola n y a d a hi ç parolas ı olmaya n zayı f bi r uzaktan erişi m program ı kullana n bi r modem e bağl ı olduğun u görürse , kolaylıkla şirke t ağın a girebilir .

10-8 Modemle r v e otomati k yanı t verm e ayarlar ı

Kural: Birilerini n bilgisaya r sistemin e mode m bağlantısında n girmesini önleme k amacıyl a B İ onayl ı tü m bilgisayarların , mode m otomatik yanı t verm e özellikler i kapatılmalıdır . .

Açıkiamalar/NotSar: Bilg i işle m bölümü , uygu n olduğ u ölçüde , modem aracılığıyl a haric i bilgisaya r sistemlerin e bağlanmas ı gereke n çalışanlar içi n dı ş ha t bağlantılard a kullanılaca k bi r mode m havuz u tah - sis etmelidir .

10-9 Kırm a araçia n

Kural: Çalışanla r yazılı m korum a mekanizmaların ı al t etme k üzer e tasarlanmış yazılı m araçlar ı indirmeme!' ! y a d a kullanmamalıdırlar .

Açıkîama/Motlar: İnternett e ticar î yazılımlar ı v e paylaşı m yazılım - larını kırma k üzer e tasarlanmı ş programlar a adanmı ş düzinelerc e sit e vardır. B u araçları n kullanım ı yalnızc a yazılı m sahibini n teli f hakların ı çiğnemekle kalmamakta , ayn ı zamand a oldukç a d a büyü k bi r tehlik e oluşturmaktadır. B u programla r bilinmeye n kaynaklarda n geldiğ i içi n kullanıcının bilgisayarın a zara r verebilece k köt ü huyl u yazılımla r içere - bilir y a d a program ı yaza n kişinin , kullanıcını n bilgisayarın a erişebilme - si içi n birTruvaAt ı yerleştirebilir .

10-10 Çevrimiç i şirke t bilgile n

Kurai: Çalışanla r herhang i bi r herkes e açı k habe r gurubuna , forum a ya d a bülten e şirket e ai t donanı m y a d a yazılımlarl a ilgil i ayrıntıla r yaz - mamalı v e kurallar a uygu n olanla r dışınd a iletişi m bilgiler i vermeme - lidirler.

Açıklamalar/Notlar: Usenet'e , çevrimiç i forumlara , bülte n panoları - na y a d a yazışm a listelerin e bırakılmı ş herhang i bi r mesaj , hede f şirke t ya d a hede f bireyl e ilgil i bilg i toplarke n araştırılabilir . Bi r toplu m mühendisliği saldırısını n araştırm a aşamasında , saldırga n şirketle , ürünleriyle v e çalışanlarıyl a ilgil i yararl ı bilgile r bulabilme k içi n internet - teki mesa j guruplar ı taranabilir .

Bazı mesajla r saldırganı n saldırısın ı ilerletme k içi n kullanabileceğ i ufak tefe k bilgile r d e içerir . Örneğin , bi r a ğ yöneticis i belirl i bi r mark a v e model güvenli k duvar ı içi n güvenli k duvar ı filtrelerini n ayarlanmasıyl a ilgili bi r sor u mesaj ı bırakmı ş olabilir . B u mesaj ı bula n bi r saldırga n şir - ket ağın a girebilmes i içi n çevresinde n dolaşmasın ı sağlayacak , şirketi n güvenlik duvar ı ayarlar ı v e türüyl e ilgil i değerli bilgile r eld e edebilir .

Çalışanların habe r grupların a nerede n geldiğini n anlaşılmayacağ ı adsız hesaplarda n mesa j göndermelerin e izi n verere k b u soru n azaltıla - bilir y a d a önün e geçilebilir . Kural , doğa l olara k çalışanları n şirketl e iliş - kilendirilebilecek herhang i bi r iletişi m bilgis i bırakmamalar ı şartın ı d a getirmelidir.

10-11 Disketle r v e diğe r elektroni k ortamla r

Kural: Eğe r bilgisaya r bilgilerin i saklama k içi n kullanıla n diske t y a da CD-RO M gib i ortamlar , çalışm a alanınd a y a d a çalışanı n masasınd a bırakılmışsa v e bilinmeye n bi r kaynakta n geliyors a bilgisaya r sistemin e sokulmamalıdır.

Açıklamalar/Notlar: Saldırganları n köt ü huyl u yazılı m yükleme k için kullandıklar ı yöntemlerde n bir i programlar ı bi r disket e y a d a CD-ROM'a koyu p ilg i çekic i bi r şekild e etiketlemekti r (örneğin , "Personel Maa ş Verileri-Gizlidir") . Sonr a bunu n birka ç kopyasın ı çalışanların kullandıklar ı alanlar a bırakırlar . Yalnızc a bir i bi r bilgisayar a girer v e içindek i dosyala r açılırsa , saldırganı n köt ü huyl u yazılım ı çalış - maya başlar . Bu , sistem e girilmesin i sağlayaca k bi r ark a kap ı yaratabili r ya d a ağ a başk a türl ü zararla r verebilir . , • . • •

10-12 Taşınabili r ortamları n atılmas ı

Kural: Bilg i silinmi ş bil e ols a herhang i bi r zama n aralığınd a hassa s şirket bilgilerini n tutulduğ u bi r elektroni k ortam ı çöp e atmada n önc e ortam manyeti k olara k silinmel i y a d a kurtarılamayaca k şekild e zara r görmüş olmalıdır .

Açıkiamalar/Notiar: Basıl ı belgeleri n öğütülmes i bugünlerd e sıradan işlerde n bir i olduys a da , şirke t çalışanlar ı bi r zamanla r hassa s bilgiler içermi ş bi r elektroni k ortam ı çöp e atmanı n yaratabileceğ i tehdid i gözardı edebilirler . Bilgisaya r saldırganları , atılmış elektroni k ortamlard a bulunan bilgiler i ger i getirmey e çalışırlar . Çalışanlar , dosyala n silerek , bu dosyaları n ger i getirilemeyeceğin i varsayıyo r olabilirler . B u varsayı m tamamen yanlıştı r v e gizl i i ş bilgilerini n yanlı ş eller e düşmesin e nede n olabilir. B u nedenl e gene l olara k sınıflandırılmamı ş bilgile r içermekt e y a da bi r zamanla r içermi ş ola n tü m elektroni k ortamla r tamame n temizlen - meli y a d a soruml u grubu n onayladığ ı yöntemle r kullanılara k yo k edilmelidir.

10-13 Parol a korumal ı ekra n koruyucula r

Kura!: Tü m bilgisaya r kullanıcılar ı bi r ekra n koruyucus u parolas ı oluşturmalı v e bell i bi r sür e kullanılmadığ ı zama n bilgisayar ı kilitleye n bir zama n aşım ı süres i belirlemelidir .

Açıklamalar/Notlar: Tü m çalışanla r bi r ekra n koruyuc u parolas ı v e on dakikada n fazl a olmama k üzer e bi r zama n aşım ı süres i ayarla - malıdırlar. B u kuralı n amac ı yetkisi z kişileri n başk a birini n bilgisayarın ı kullanmasını önlemektir . B u nedenl e b u kura l şirke t bilgisaya r sistem - lerini, dışarıda n binay a girebile n kişiler e karş ı korur .

10-14 Parol a gizlili k taahhüd ü

Kural: Yen i bi r bilgisaya r hesab ı açılmada n önc e çalışa n y a d a taşeron, parolaları n hiçbi r zama n herhang i birin e açıklanmamas ı y a d a paylaşılmaması gerektiğin i v e b u kurallar a uymay ı kabu l ettiğin i gösteren yazıl ı bi r beya n imzalamalıdır .

Açıklamalar/NotSar: Anlaşmada , b u tar z bi r anlaşmay a uyulmadığ ı durumda bunun , cezas ı işte n çıkarmay a kada r vara n cidd i bi r disipli n suçu teşki l edeceğin i belirte n bi r madd e d e bulundurulmalıdır .

E-Posta Kullanım ı . •

11-1 E-Post a ekler i

Kural: E-post a ekler i güvenili r bi r kişide n gelmediğ i y a d a işl e ilgil i olarak beklenmediğ i sürec e açılmamalıdır .

Açıklamalar/Notlar: Tü m e-post a ekler i yakında n izlenmelidir . Alıcı , eki açmada n önc e güvenili r bi r kişini n ekl i bi r e-post a gönderileceğin e dair ö n bilg i vermesin i zorunl u tutabilirsiniz . Bu , saldırganları n toplu m mühendisliği taktikler i kullanara k insanlar ı ekler i açmalar ı doğrultusun - • da kandırabilm e riskin i azaltacaktır .

Bir bilgisaya r sistemin e girmeni n yöntemlerinde n biri , saldırganı n sisteme girebilmesin i sağlayaca k bi r açı k yarata n köt ü huyl u birprog -

ramı çalıştırmas ı içi n çalışan ı kandırmaktır . Saldırgan , çalıştırılabili r bi r kod y a d a makr o içere n bi r e-post a ek i gönderere k kullanıcını n bilgisa - yarının kontrolün ü el e geçirebilir .

Bir toplu m mühendis i köt ü huyl u e-post a ekler i gönderebilir , sonr a da telefonl a arayı p alıcıy ı ek i açmay a ikn a etmey e çalışabilir .

11 - 2 Haric î adresler e otomati k yönlendirm e

Kural: Gele n e-postaları n otomati k olara k haric i bi r e-post a adresin e yönlendirilmesi yasaktır .

Açıklamalar/Notiar: B u kuralı n amacı , dahil î bi r e-post a adresin e gönderilmiş bi r e-postay ı dışarıda n birini n almasın ı önlemektir .

Çalışanlar, ofiste n uza k olacaklar ı zama n gele n e-postaların ı baze n şirket dışında n bi r e-post a adresin e yönlendirirler . Y a d a bi r saldırgan , bir çalışan ı kandırara k e-postalar ı şirke t dışında n bi r adres e postalaya n bir dahil î e-post a adres i oluşturtabilir . Saldırgan , dah a sonr a dahil î e-posta adres i olan , içeride n bir i gib i davranarak , insanları n hassa s bil - gileri dahil î adres e göndermelerin i sağlayabilir .

11-3 E-postaîars n yönlendirilmes i

Kural: Onaylanmamı ş bi r kişide n gele n herhang i bi r başk a onaylan - mamış kişiy e e-post a aktarm a talebi , tale p sahibin e kimli k tespit i yapıl - masını gerektirir .

11-4 E-postaSan n onaylanmas ı

. Kural : Gene l olara k sınıflandırılmamı ş bi r bilg i taleb i içere n y a d a bilgisayarlarla ilgil i donanımlar a yöneli k bi r işle m yapılmasın ı isteye n v e güvenilir bi r kişide n geliyo r gib i görünen bi r e-post a mesaj ı içi n e k bi r tanımlama şekl i dah a gereklidi r (bkz . Ona y v e Yetkilendirm e Süreçleri) .

Âçıklamaîar/Notlar: Bi r saldırga n bire-postay ı v e başlığın ı kolaylık - la takli t edere k on u farkl ı bi r e-post a adresinde n geliyormu ş gib i gösterebilir. Ayrıc a girdiğ i bi r bilgisaya r sisteminde n d e e-post a gön - derebilir. E-postanı n başlığın ı inceleyere k bil e müdahal e edilmi ş bi r dahilî sistemde n gönderili p gönderilmediğin i ayır t edemezsiniz .

12-1 Telefo n anketlerin e katılma k

Kural: Çalışanlar , başk a kuruluşları n y a d a kişileri n sor u sorm a yoluyla yaptığ ı anketler e katılamazlar . B u tar z taleple r halkl a ilişkile r bölümüne y a d a diğe r soruml u kişiler e yönlendirilmelidir .

Açıklamalar/Notlar: Şirket e karş ı kullanılabilece k değerl i bilgiler i elde edebilme k içi n toplu m mühendislerini n kullandığ ı yöntemlerde n bir i

de çalışan ı arayı p bi r anke t yaptığın ı söylemektir . Yasa l bi r araştırmay a katkıda bulundukların a inandıklar ı zama n insanları n şirke t y a d a kendi - leriyle ilgil i yabancılar a bilg i verme k konusund a n e kada r raha t olduk - larına inanamazsınız . Saldırgan , zararsı z görünüml ü soruları n arasın a yanıtlarını bilme k istediğ i birka ç soruy u dah a sıkıştırır . Sonu ç olara k b u tarz bilgile r şirke t ağın a girme k içi n kullanılabilirler .

12-2 Dahil î telefo n numaralarını n verilmes i

Kurai: Eğe r onaylanmamı ş bi r kişi bi r çalışan a telefo n numarasın ı sorarsa, çalışan, şirke t işlerini n yönetilmes i il e ilgil i olara k numaray ı ver - menin gerekl i olu p olmadığ ı doğrultusund a uygu n bi r kara r verebilir .

Açıklamalar/Notlar: B u kuralı n amac ı dahil î telefo n numaraların ı vermenin gerekl i olu p olmadığ ı üzerind e düşünülmü ş bi r kara r vermey e çalışanları yönlendirmektir . Numaray ı öğrenme k içi n iy i bi r nedenler i varmış gib i görünmeye n insanlarl a uğraşırke n e n emi n yo l an a şirke t telefonunu aramalar ı v e orada n aktarılmaların ı söylemektir .

12-3 Sesl i mesa j parolalar ı

Kural: Herhang i birini n sesl i mesa j kutusun a parol a bilgiler i içere n mesajlar bırakma k yasaktır .

Açıklamalar/Notlar: Kola y tahmi n edilebili r bi r erişi m koduyl a yeter - siz bi r şekild e korunduklar ı içi n bi r toplu m mühendis i sı k sı k bi r çalışanı n sesli mesa j kutusun a erişebilir . Saldır ı türlerinde n birinde , bilgil i bi r bil - gisayar kırıcıs ı kend i saht e sesl i mesa j kutusun u yaratabili r v e başk a bi r çalışanı parol a bilgilerin i içere n bi r mesa j bırakmay a ikn a edebilir . B u kural b u tar z bi r oyunu n üstesinde n gelme k içindir .

Faks Kullanım ı

13-1 Fak s gönderilmes i

Kural: iste k sahibini n kimli k tespit i yapılmada n kimsede n fak s alına - maz v e kimsey e fak s gönderilemez .

Açıklamalar/Notlar: Bilg i hırsızları , güvenili r çalışanları , şirke t için - deki bi r fak s makinasın a hassa s bilgiler i göndermeler i doğrultusund a kandırabilirler. Kurban a fak s numarasın ı vermede n önc e saldırgan , sek - reter y a d a idar î yardımc ı gibi , hiçbi r şeyde n haber i olmaya n bi r çalışan ı arar v e dah a sonr a alınmas ı içi n kendilerin e bi r fak s gönderili p gönderi - lemeyeceğini sorar . Ardından , masu m çalışa n faks ı aldıkta n sonra , sal - dırgan çalışan ı ara r v e faksı n başk a bi r yer e fakslanmasın ı ric a eder . Arada, bunu n aci l bi r toplant ı içi n gerekl i olduğun u söylemey i d e ihma l etmez. Faks ı göndermes i istene n kişi , o bilgini n değer i konusund a bi r fikri olmadığ ı içi n isteğ i yerin e getirir .

13-2 Faksl a gönderilmi ş talimatları n onaylanmas ı

Kural: Faksl a gele n talimatlar ı yerin e getirmeden önce , göndereni n şirketin bi r çalışan ı y a d a bi r güvenili r kiş i olduğ u onaylanmalıdır .

Açıklamalar/Notlar: Fak s aracılığıyla , bilgisayar a komu t girilmes i y a d a bilgi istenmes i gib i olağandış ı istekle r gönderildiğ i zama n çalışanla r dikkatl i olmalıdırlar. Fakslanmı ş belgeleri n başlığınd a geçe n bilgile r gönderic i fak s makinasının ayarlarıyl a oynanara k değiştirilebilir . B u yüzde n fak s başlığ ı yetki y a d a kimli k tespit i içi n yeterl i bi r ver i olara k kabu l edilmemelidir .

13-3 Faksl a hassa s biigiieri n gönderilmes i

Kural: Başk a çalışanları n d a erişebileceğ i bi r yerd e dura n bi r fak s makinasına hassa s bilg i göndermede n önce , gönderen , bi r kapa k say - fası göndermelidir . Alıcı , kapa k sayfasın ı alı r alma z karşılı k olara k bi r sayfa gönderi r v e fak s başınd a olduğun u gösterir . Gönderici , dah a sonra faksı n tümün ü gönderir .

Açıklamalar/Notlar: B u tokalaşm a süreci , göndericinin , alıcını n makinanın başınd a bulunduğunda n emi n olmasın ı sağlar . B u süre ç ayrıca, mesaj ı alaca k fak s numarasını n başk a bi r numaray a yön - lendirilmediğini d e doğrular .

13-4 Parol a fakslama k yasaktı r

Kural: Parolala r hiçbi r koşuld a fak s aracılığıyl a gönderilmemelidir .

Açıklamalar/Notlar: Tanımlam a bilgilerin i faksl a gönderme k güven - li değildir . Çoğ u fak s makinası , ço k sayıd a çalışanı n birde n elini n altın - dadır. Dahası , faksla r gene l telefo n santrallar ı ağın a bağlıdırlar . Gönderilen fak s başk a bi r numarad a buluna n saldırgan a gidece k şe - kilde aram a yönlendirmes i yapılabilir .

14-1 Sesl i mesa j parolalar ı

Kural: Sesl i mesa j parolalar ı hiçbi r nedenl e başkaların a verilmeme - lidirler. Bun a e k olara k sesl i mesa j parolalar ı e n ço k doksa n günd e bi r değiştirilmelidir.

Açıklamalar/Notlar: Gizl i şirke t bilgiler i sesl i mesa j kutuların a bırakılabilir. B u bilgiy i koruma k içi n çalışanla r sesl i mesa j parolaların ı sı k sık değiştirmel i v e bunlar ı hiçbi r zama n başkaların a vermemelidirler . Ayrıca, o n ik i aylı k dönemle r içerisind e sesl i mesa j kullanıcılar ı ayn ı y a da benze r parolala r kullanmamalıdırlar .

14-2 Çokl u sistemlerd e parolala r

Kural: Sesl i mesa j kullanıcılar ı iste r dahil î isters e haricî , telefon y a

da bilgisaya r sistemlerind e kullandıklar ı parolay ı kullanmamalıdırlar .

Açıklamalar/Notlar: Sesl i mesa j v e bilgisaya r gib i farkl ı ortamlard a aynı y a d a benze r parolay ı kullanmak , bi r tanesin i tespi t ettikte n sonr a toplum mühendislerini n tü m parolalar ı tahmi n etmelerin i kolaylaştırır .

14-3 Sesl i mesa j parolalarını n ayarlanmas ı

Kural: Sesl i mesa j kullanıcılar ı v e yöneticile r tahmi n edilmes i zo r olan sesl i mesa j parolalar ı kullanmalıdırlar . Parolala r herhang i bi r şe - kilde kullana n kişiyl e y a d a şirketl e ilişkilendirilmemel i v e tahmi n edilm e olasılığı ola n öngörülebili r bi r düzend e olmamalıdır .

Açıklamalar/Notlar: Parolala r ardışı k y a d a tekrarlana n sayıla r (örneğin, 1111 , 1234 , 1010) içermemelidir . Dahil î telefon numaralarını n aynısı y a d a benzer i olmamalı , adres , post a kodu , doğu m tarihi , ara ç plakası, telefo n numarası , ağırlık , I Q y a d a başk a türl ü tahmi n edilebili r kişisel bilgilerl e ilişkil i olmamalıdırlar .

14-4 "Eski " olara k işaretlenmi ş mesajla r

Kural: Dinlenmemi ş sesl i mesajla r yen i mesa j olara k işaretlen - mediğinde sesl i mesa j yöneticisi , olas ı bi r güvenli k ihlalin e karş ı uyarıl - malı v e sesl i mesa j parolas ı heme n değiştirilmelidir .

Açıklamalar/Notlar: Toplu m mühendisler i çeşitl i yollarl a sesl i mesa j kutularına ulaşabilirler . Hi ç dinlemediğ i mesajları n yen i mesa j olara k geçmediği bi r durumda , çalışan , birini n sesl i mesa j kutusun a yetkisi z giriş yapı p mesajlar ı dinlediğin i varsaymahdır .

14-5 Haric î sesl i mesa j açılı ş notlar ı

Kural: Şirke t çalışanlar ı dışarıy a yöneli k sesl i mesa j açılı ş notların - da verdikler i bilgiy i sınırlamalıdırlar . Gene l olarak , çalışanı n günlü k işler i ya d a yolculu k tarihleriyl e ilgil i bilgile r verilmemelidir .

Açıklamalar/Notlar: Dışarıy a yöneli k açılı ş notları , soyad , dahil i telefon numaras ı y a d a yerind e bulunmam a nedenlerin i (yolculuk , tati l tarihleri y a d a günlü k progra m gibi) içermemelidir . Bi r saldırga n b u bil - giyi diğe r çalışanlar ı kandırmay a yöneli k akl a yatkı n bi r hikây e uydura - bilmek içi n kullanır .

14-6 Sesl i mesa j parol a düzenler i

Kural: Sesl i mesa j kullanıcılar ı bi r bölüm ü sabi t kalan , kalan ı öngörülebilir bi r şekild e değişe n parolala r seçmemelidirler .

Açıklamalar/Notlar: Örneğin , so n ik i basamağı n içind e bulunulan aya karşılı k geldiğ i 743501 , 743502 , 74350 3 gib i parolala r kullanılma - malıdır.

14-7 Gizl i y a d a öze l bilgile r

Kurai: Gizl i y a d a öze l bilgile r sesl i mesajlarl a aktarılmamalıdır .

Açıklamalar/Notlar: Şirke t telefo n sistem i çoğ u zama n şirke t bil - gisayar sistemlerinde n dah a fazl a saldırıy a açıktır . Parolalar , bi r saldır - ganın yaptığ ı tahminler i büyü k ölçüd e kolaylaştıra n bi r diz i sayıda n oluşur. Ayrıc a baz ı kuruluşlard a sesl i mesa j parolalar ı yöneticiler i adın a mesaj alm a sorumluluğ u ola n sekreterler e y a d a yönetic i asistanların a verilebilmektedir. Yukarıdak i bilgileri n ışığınd a kimseni n sesl i mesa j kutusuna hassa s bilgile r bırakılmamalıdır .

Parolalar

15-1 Telefo n güvenliğ i

Kural: Parolala r hiçbi r zama n telefond a verilmemelidir .

Açıklamaiar/Not!ar: Saldırganlar , y a şahse n y a d a teknoloji k bi r araç yardımıyl a telefo n görüşmelerin i dinlemeni n yolların ı bulabilirler .

15-2 Bilgisaya r parolalarını n verilmes i

Kural: Bilg i işle m yöneticisini n yazıl ı onay ı olmada n bilgisaya r kul - lanıcıları hiçbi r koşuld a parolaların ı başkaların a vermemelidirler .

Açıklamalar/Notlar: Pe k ço k toplu m mühendisliğ i saldırısını n amac ı hiçbir şeyde n kuşkulanmaya n kişileri n hesa p adların ı v e parolaların ı açık - lamaları doğrultusund a onlar ı kandırmaktır . B u kura l şirket e karş ı yapıla n toplum mühendisliğ i saldırılarını n başar ı olasılığın ı azaltma k içi n öneml i bi r adımdır. Sonu ç olarak , b u kural a şirke t bünyesind e harfiye n uyulmalıdır .

15-3 İnterne t parolalar ı

Kural: Çalışanlar , şirke t sistemind e kullandıklar ı parolanı n bi r ben - zerini y a d a aynısın ı interne t sitelerind e d e kullanmamalıdırlar .

Açıklamalar/Notlar: Köt ü amaçl ı interne t sites i sahipler i değerl i bi r şey suna n y a d a bi r ödü l kazanm a olasılığ ı olduğun u söyleye n bi r sit e yapabilirler. Ziyaretçileri n kayı t olabilme k içi n bi r e-post a adresi , kul - lanıcı ad ı v e parol a girmeler i gerekir . Çoğ u insa n ayn ı y a d a benze r kayıt bilgilerin i tekra r tekra r kullandıklar ı içi n köt ü amaçl ı interne t sitelerinin sahipler i kullanıla n parolay ı v e b u parolanı n çeşitl i şekillerin i hedefin e v "y a d a i ş bilgisayarın a saldırma k içi n kullanabilirler . Ziyaretçinin i ş bilgisayar ı kayı t işlem i sırasınd a girdiğ i e-post a adresin - den d e baze n bulunabilir .

15-4 Çokl u sistemlerd e parolala r

Kural: Şirke t çalışanlar ı ayn ı y a d a benzer i bi r parolay ı birde n fazl a sistemde

kullanmamalıdırlar . B u kura l çeşitl i araçlar ı (bilgisaya r y a d a

sesli mesaj) ; çeşitl i konumlar ı (e v y a d a iş) ; çeşitl i sistemleri , araçlar ı (yönlendirici y a d a güvenli k duvarı) y a d a programlar ı (veritaban ı y a d a uygulama) kapsayabilir .

Açıklamalar/Notlar: Saldırganla r bilgisaya r sistemlerin e y a d a ağlarına girme k içi n insa n doğasın ı kullanırlar . Çoğ u insanı n girdikler i her sistemd e bi r sür ü parolay ı akıld a tutm a keşmekeşinde n kurtulma k için ayn ı y a d a benze r parolala r kullandıkların ı bilirler . B u yüzde n saldır - gan, hedefi n hesabını n olduğ u sistemlerde n birini n parolasın ı öğren - meye çalışır . Parolay ı bî r ke z öğrendikte n sonr a ayn ı parolanı n y a d a bi r benzerinin çalışanı n kullandığ ı diğe r sistemler e v e araçlar a erişi m sağlama olasılığ ı yüksektir .

15-5 Parolaları n yenide n kullanılmas ı

Kural: Hiçbi r bilgisaya r kullanıcıs ı o n seki z aylı k sür e içerisind e ayn ı ya d a benze r bi r parol a kullanmamalıdır .

Açıklamalar/Notlar: Parolanı n sı k değiştirilmesi , bi r sadırganı n bi r kullanıcının parolasın ı keşfetmes i durumund a oluşabilece k zarar ı e n aza indirger . Yen i parolay ı öncek i parolalarda n farkl ı yapma k saldır - ganın tahmi n etmesin i zorlaştırır .

15-6 Parol a yapıs ı " ••••••

Kural: Çalışanlar , bi r bölüm ü sabi t kala n diğe r bölüm ü öngörülebili r bir şekild e değişe n parolala r seçmemelidirler .

Açıklamalar/Notlar: Örneğin , so n ik i basamağı n içind e bulunula n ay a karşılık geldiğ i KevinOl , KevinO2 , KevinO 3 gib i parolala r kullanılmamalıdır .

15-7 Parol a seçim i

Kural: Bilgisaya r kullanıcılar ı aşağıdak i koşullar ı sağlaya n bi r paro - la yaratmal ı y a d a seçmelidir .

• Standar t kullanıc ı hesaplar ı içi n e n a z seki z karakte r v e ayrı -

calıklı hesapla r içi n e n a z o n ik i karakte r uzunluğund a olmalıdır . • E n a z bi r sayı , bi r simg e ($, - , I , & gibi) , bi r küçü k har f v e bi r

büyük har f (işleti m sistemind e buluna n farkl ı yaz ı şekillerini n e l

verdiği ölçüde) içermelidir .

• Aşağıdakilerde n herhang i birin i d e içermemelidir : Herhang i bi r

dildeki sözlükt e bulunabilece k bi r kelime , çalışanı n soyadı , hobi -

leri, plak a numarası , Sosya l Güvenli k Numarası , adresi , telefo n numarası, evci l hayvanını n adı , doğu m gün ü y a d a b u kelimeler i içeren kelim e grupları .

• Dah a önc e kullanılmı ş bi r parolanı n bi r taraf ı sabi t bi r taraf ı değişmiş türde n farkl ı bi r şekl i d e olmamalıdır , kevin , kevini , kevin2 y a d a kevinocak , kevinşuba t gibi .

Açıklamalar/Notlar: Yukarıd a sıralana n özellikleri n kullanılmas ı toplum mühendisini n tahmi n etmesini n zo r olacağ ı bi r parol a ortay a çıkaracaktır. Diğe r bi r seçene k is e sesli-sessi z har f yöntemidir . B u yön - temle hatırlamas ı v e okumas ı kola y bi r parol a eld e edilebilir . Böyl e bi r parola oluşturabilme k içi n "ABABABAB " şablonund a B harflerin i sessi z harflerle, A harflerin i is e sesl i harflerle r değiştirin . Örne k verme k gerekirse, MIKOFAS O y a d a KUSOCEN A olabilir .

15-8 Parolalar ı no t etme k

Kural: Çalışanla r parolaların ı yalnızc a bilgisayarda n y a d a başk a parola korumal ı donanımda n uzakt a güvenl i bi r yer e koyacaklars a bi r yere no t edebilirler .

Açıklamalar/Notlar: Çalışanlar a parolaların ı hiçbi r zama n bi r yer e yazmamaları salı k verilmelidir . Anca k baz ı koşulla r altınd a b u gerekl i olabilir. Örneğin , çalışanı n farkl ı bilgisaya r sistemlerind e birde n fazl a hesabı varsa . Herhang i bi r yazıl ı parol a bilgisayarda n uzakt a güvenl i bi r yere konmalıdır . Hiçbi r koşuld a parol a klavyeni n altın a saklanmamal ı y a da monitör e yapıştırılmamalıdır .

15-9 Bilgisaya r dosyalarındak i şifrelenmemi ş parolala r

Kural: Şifrelenmemi ş parolala r herhang i bi r bilgisaya r dosyasınd a sak - lanmayacak y a d a bi r işle v tuşuyl a çağırılabilece k şekild e programlanmaya - caktır. Gerekl i olduğ u durumd a parolalar , B i bölümünü n yetkisi z erişimler i engellemek içi n onayladığ ı bi r şifrelem e yazılım ı kullanılara k saklanmalıdır .

Açıklamalar/Notlar: Parolala r şifrelenmemi ş olara k tutulduklar ı bil - gisayar ver i dosyalarından , topl u komu t dosyalarından , uçbiri m işle v tuşlarından, giri ş dosyalarından , makr o y a d a yaz ı programlarında n veya FT P sitelerini n parolaların ı içere n herhang i bi r ver i dosyasında n bi r saldırgan tarafında n kolaylıkl a bulunu p çıkarılabilir .

Dışarıdan Çalışanla r Içî n Kuralla r

Dışarıdan çalışanlar , şirke t güvenli k duvarını n dışındadırla r v e b u nedenle saldırılar a açıktırlar . B u kuralla r toplu m mühendisini n dışarıda n çalışan personeliniz i verileriniz e açıla n bi r kap ı olara k kullanmasın ı önlemenize yardımc ı olacaktır .

16-1 Küçü k istemcile r

Kural: Uzakta n erişi m yetkisin e sahi p tü m şirke t çalışanlar ı şirke t ağına bağlanma k içi n küçü k istemc i kullanmalıdırlar .

Açıklamalar/Notlar: Bi r saldırgan , saldır ı stratejisin i kurarken , dışarıdan şirke t ağın a erişim i ola n kullanıcılar ı bulmay a çalışır . B u nedenle dışarıda n çalışanla r başlıc a hedefler i oluştururlar . B u kişileri n

bilgisayarlarında sık ı güvenli k kontrollerini n olm a olasılığ ı zayıftı r v e bu , şirket ağın a girebilece k açı k bi r nokt a bırakır .

Güvenilir bi r ağ a bağlana n herhang i bi r bilgisayar , klavy e girişlerin i kaydeden programlarl a tuzaklanabili r y a d a bağlantılar ı kaçırılabilir . Bi r küçük istemc i stratejis i sorunlar ı çözme k içi n kullanılabilir . Küçü k istem - ci, sürücüs ü olmaya n bi r bilgisaya r y a d a apta l bi r uçbiri m gibidir . Uçbiri m gibi çalışa n b u bilgisayard a gerekl i saklam a ortamlar ı yoktu r anca k bun a karşılık işleti m sistemi , uygulam a programlar ı v e tü m verile r şirke t ağın - da durur . Küçü k istemc i üzerinde n ağ a erişilmesi , yamalanmamı ş sis - temlerin, eskimi ş işleti m sistemlerini n v e köt ü huyl u programları n oluştur - duğu risk i büyü k ölçüd e azaltmaktadır . Ayn ı zamand a dışarıda n çalışan - ların güvenliğin i sağlama k d a merkez i güvenli k kontroller i sayesind e daha kola y v e etkil i olur . Güvenli k konularıyl a ta m anlamıyl a ilgilenme k konusunda iş i deneyimsi z kullanıcılar a bırakmaktans a b u tar z yüküm - lülükler eğitiml i a ğ y a d a siste m yöneticilerin e bırakılmalıdır .

16-2 Dışarıda n çalışanları n bilgisayarlar ı içi n güvenli k

yazılımları

Kural: Şirke t ağın a bağlanma k içi n kullanıla n herhang i bi r haric î bil - gisayar sistemind e virü s v e Truv a At ı korum a programlar ı v e (donanım - dan y a d a yazılımda n gelen) kişise l bi r güvenli k duvar ı bulunmalıdır . Virü s ve Truv a At ı tanı m dosyala n e n azında n haftalı k olara k yenilenmelidir .

Açıklamalar/Notlar: Genellikl e dışarıda n v e evde n çalışanla r güven - lik konularınd a bilgil i değillerdi r v e dikkatsizli k y a d a ihmalkârlıkl a bilgisa - yar sistemlerin i y a d a şirke t ağların ı saldırıy a açı k bırakabilirler . B u nedenle dışarıda n çalışanla r düzgü n bi r şekild e eğitilmezlers e cidd i bi r güvenlik tehdid i oluşturmaktadırlar . Köt ü huyl u yazılımlar a karş ı korun - mak içi n virüste n v e Truv a Atında n korunm a programlarını n yüklenme - sine e k olarak , saldırganları n çalışanlar a sunula n herhang i bi r hizmet e dışarıdan erişebilmelerin i engelleme k içi n d e bi r güvenli k duvar ı şarttır .

Microsoft'a yapıla n bi r saldırını n d a gösterdiğ i gibi , köt ü huyl u yazılımların çoğalmasın a karş ı e n elze m güvenli k teknolojilerin i kullan - mamanın risk i hafif e alınmamalıdır . Dışarıda n çalışa n bi r Microsof t çalışanının bilgisaya r sistemin e bi r Truv a At ı bulaşır . Saldırga n y a d a saldırganlar çalışanı n güvenili r ağın ı kullanara k geliştirm e kayna k kod - larını çalma k içi n Microsoft'u n geliştirm e ağın a girebilmişlerdir .

İnsan Kaynaklar ı Kurallar ı

insan kaynakla n bölümlerinin , kend i çalışm a ortamlar ı aracılığıyl a kişisel bilgiler i eld e etmey e çalışanlar a karş ı personel i koruma k konusun - da öze l bi r görevler i vardır . İ K çalışanlarını n ayn ı zamand a şirketlerin i mutsuz v e esk i çalışanlar a karş ı korum a sorumluluklar ı d a vardır .

17-1 Ayrıla n çalışanla r

Kural: N e zama n bi r çalışa n şirkette n ayrılı r y a d a ilişkis i kesilirse , insan kaynaklar ı heme n aşağıdak i işlemler i yerin e getirmelidir :

• Çevrimiç i telefo n rehberinde n kişini n adın ı çıkarmal ı v e sesl i

mesajlarını ipta l etmel i y a d a yönlendirmelidir .

• Bin a girişlerind e y a d a şirke t lobilerind e görevl i personel i bil -

gilendirmelidir.

• Çalışanı n adın ı ayrıla n çalışanla r listesin e eklemel i v e b u liste ,

sıklığı bi r haftada n dah a a z olmayaca k şekild e tü m çalışanlar a

gönderilmelidir.

Açıklamalar/Kurallar: Bin a girişlerind e görevl i çalışanla r esk i bi r çalışanın binay a yenide n girmesin i önleme k üzer e uyarılmalıdırlar . Ayrıca, diğe r çalışanları n d a uyarılmas ı esk i çalışanı n hale n çalışıyor - muş gib i davranara k başkaların ı şirket e zara r verebilece k hareketlerd e bulunmaları doğrultusund a kandırmasın ı önleyecektir .

Bazı koşullard a esk i çalışanl a ayn ı bölümd e çalışa n herkesi n paro - lalarını değiştirmelerini n istenmes i gerekl i olabilir . (Yalnızc a bilgisaya r korsanlığı konusundak i ünü m nedeniyl e GTE'dek i işim e so n verildiğind e şirket tü m çalışanları n parolaların ı değiştirmelerin i zorunl u tutmuştu.)

17-2 B İ bölümünü n uyarılmas ı

Kural: Şirkett e çalışa n bi r kiş i işte n ayrıldığınd a y a d a işin e so n ve - rildiğinde insa n kaynakları , esk i çalışanın , aralarınd a ver i taban ı erişimi , uzaktan bağlant ı y a d a uza k noktalarda n interne t erişim i hesaplarını n da bulunduğ u tü m bilgisaya r hesapların ı ipta l etmes i içi n bilg i işle m bölümünü heme n haberda r etmelidir .

Açıklamalar/Notlar: Esk i bi r çalışanı n işl e ilişiğ i kesili r kesilme z tü m bilgisayar sistemlerine , a ğ araçlarına , veritabanların a y a d a herhang i bi r bilgisayar donanımın a erişimini n derha l kesilmes i önemlidir . Aks i durumda şirke t ki n dol u bi r çalışanı n şirke t bilgisaya r sistemlerin e giri p ciddi zararla r verebilmes i içi n kapıy ı ardın a kada r açı k bırakmı ş olur .

17-3 İş e alm a sürecind e kullanıla n gizl i bilgile r

Kural: ilanla r v e i ş boşlukların ı doldurma k içi n uygu n ada y bulmay a yönelik diğe r herkes e açı k davetle r mümkü n olduğ u ölçüd e şirketi n kul - landığı bilgisaya r donanı m v e yazılımlar ı konusund a bilg i vermemelidir .

Açıklamalar/Notlar: Yöneticile r v e insa n kaynaklar ı personel i yal - nızca nitelikl i adayları n özgeçmişlerin i almay a yetece k kada r şirke t bil - gisayar donanı m v e yazılımlar ı hakkınd a bilg i vermelidirler .

Bilgisayar kırıcılar ı açı k i ş listelerin i bulma k içi n gazeteleri v e şirke t basın açıklamaların ı okurlar , interne t sayfaların a girerler . Çoğ u zama n

şirketler, müstakbe l çalışanlar ı çekebilme k içi n kullandıklar ı donanı m v e yazılımlarla ilgil i ço k fazi a ayrınt ı açıklamaktadırlar . Saldırgan , hedefini n Bİ sistemleriyl e ilgil i bi r bilgiy i bi r ke z el e geçird i mi , saldırını n bi r sonra - ki adım ı içi n hazı r demektir . Örneğin , bi r şirketi n VM S işleti m sistem i kul- landığını öğrenen bi r saldırga n sistemi n hang i sürü m olduğun u öğren ^ mek içi n birka ç yer i arayabili r v e sonr a d a yazılı m şirketinde n geliyo r gibi saht e bi r aci l güvenli k yamas ı gönderebilir . Yam a bi r ke z yüklendik - ten sonr a saldırga n sistem e girer .

17-4 Çalışanları n kişise l bilgiler i

Kural: insa n kaynakla n bölümü , çalışanı n y a d a insa n kaynaklar ı yöneticisinin yazıl ı onay ı olmada n hale n çalışa n y a d a çalışmaya n hiç - bir personel , taşeron , danışman , geçic i işç i y a d a stajyeri n kişise l bilgi - lerini açıklamamalıdır .

Açıklamalar/Notlar: insa n avcıları , öze l dedektifle r v e kimli k hırsız - ları, kimli k numaraları , doğu m tarihleri , ücre t bilgileri , aralarınd a bank a hesap numaralar ı v e sağlı k yardımlar ı gib i bilgileri n d e olduğ u mal î veri - leri içere n kişise l çalışa n bilgilerin i hedeflerler . Toplu m mühendis i ilgil i birey gib i davranabilme k amacıyl a b u bilgiler i eld e edebilir . Ayrıc a yen i işe başlayanları n adlarını n açıklanmas ı d a bilg i hırsızlarını n ço k işin e yarayabilir. Yen i iş e başlayanla r esk i olduklarını , yetkil i oldukların ı y a d a şirket güvenliğinde n oldukların ı iddi a ede n kişilerde n gele n talepler i ye - rine getirmey e dah a eğilimlidirler .

17-5 Sici l taramalar ı

Kural: Kendilerin e bi r i ş önerilmede n y a d a sözleşmey e dayana n bi r iş ilişkisin e girmede n önc e tü m yen i iş e başlayanlar , taşeronlar , danış - manlar, geçic i işçile r y a d a stajyerle r içi n bi r sici l taramas ı zorunl u olmalıdır.

Açıklamalar/Notlar: Maliyetle r gö z önün e alındığınd a sici l tara - maları güve n teşki l etmes i gereke n belirl i konumlarl a sınırl ı tutulabilir . Ancak şirke t odaların a girm e hakk ı tanınmı ş herhang i birini n olas ı bi r tehdit oluşturabileceğ i d e unutulmamalıdır . Örneğin , temizli k ekiplerini n personel odaların a girm e hakk ı vardı r v e b u onlar a orad a buluna n bil - gisayar sistemlerin e girm e hakkın ı d a verir . Fizikse l olara k bi r bilgisa - yara erişi m eld e ede n bi r saldırga n parolalar ı yakalama k içi n bi r dakikadan kıs a bi r sür e içerisind e klavy e girişlerin i kaydede n bi r prog - ramı bilgisayar a yükleyebilir .

Bilgisayar kırıcılar ı hede f şirketi n bilgisaya r sistemlerin e v e ağın a girebilmek içi n şirkett e i ş bulm a yolun a bil e gidebilirler . Bi r saldırgan , hedef şirkettek i soruml u kişiy i arayara k şirketi n çalıştığ ı temizli k şirke - tinin adın ı kolaylıkl a eld e edebili r v e i ş teklifiyl e gelmi ş bi r temizli k fir - ması olduğun u söyleyere k b u hizmet i vermekt e ola n şirketi n adın ı öğrenir.

Fiziksel Güvenli k Kurallar ı

Her n e kada r toplu m mühendisler i hedefleme k istedikler i bi r işye - rinde şahse n bulunmakta n kaçmsala r d a zama n zama n bulunduğunu z mekâna d a gireceklerdir . B u kuralla r fizikse l ortamınız ı tehditlerde n korumanıza yardımc ı olacaktır .

18-1 Persone l olmayanları n kimli k tespit i

Kurai: Kuryele r v e düzenl i olara k şirke t binaların a girmeler i gereken, şirke t dışında n kişileri n şirke t güvenliğini n belirlediğ i kurallar a uygun olara k düzenlenmi ş öze l yak a kartlar ı y a d a benzer i bi r kimlikler i olmalıdır.

Açıklamalar/Notlar: Düzenl i olara k binalar a girmes i gereke n per - sonel olmaya n kişiler e (örneğin , kafeteryay a yiyece k v e içece k getiren - lere, telefo n bağlantıların ı yapanlar a y a d a fotokop i makinaların ı tami r edenlere) b u amaçl a çıkarılmı ş öze l bi r şirke t kimli k belges i verilmelidir . Ara sır a girmes i gereke n y a d a bi r kereli k iş i ola n kişile r ziyaretç i olara k değerlendirilmeli v e he r zama n yanlarınd a bi r refakatç i bulundurul - malıdır.

18-2 Ziyaretç i kimli k tespit i

Kural: Tü m ziyaretçile r içer i alınabilmele h içi n geçerl i bi r sürüc ü ehliyeti y a d a başk a bi r resiml i kimli k belges i göstermelidirler .

Açıklamalar/Notlar: Güvenli k görevliler i y a d a danışm a memur u ziyaretçi kart ı vermede n önc e kimli k belgesini n bi r fotokopisin i almal ı v e bu kopy a ziyaretç i defterind e saklanmalıdır . Diğe r bi r seçene k is e kim - lik bilgilerini n danışm a memur u y a d a güvenli k görevlis i tarafında n ziyaretçi defterin e kaydedilmesidir . Ziyaretçileri n kimli k bilgilerin i kendi - lerinin girmesin e izi n verilmemelidir .

Bir binay a girmey e çalışa n toplu m mühendisler i defter e he r zama n yanlış bilg i gireceklerdir . He r n e kada r saht e bi r kimli k eld e etme k v e ziyaret edileceğ i söylene n kişini n adın ı öğrenme k zo r olmas a d a çalışanın girişler i kaydetmesin i zorunl u tutma k güvenli k sürecin i bi r kademe dah a artırmaktadır .

18-3 Ziyaretçiler e eşli k edilmes i

Kural: Ziyaretçile r he r zama n bi r çalışanı n eşliğind e olmal ı y a d a yanlarında refakatç i bulunmalıdır .

Açıklamalar/Notlar: Toplu m mühendislerini n çevirmey i sevdikler i dolaplardan bir i bi r şirke t çalışanın ı ziyare t etmekti r (örneğin , strateji k ortaklığın olduğ u bi r firmada n geldiğini söyleyere k ürü n mühendisin i ziyaret etme k gibi) , il k görüşmey e refakatç i eşliğind e gittikte n sonr a toplum mühendis i konuştuğ u kişiy i kend i başın a lobiy e dönebileceğ i

konusunda ikn a eder . B u yönteml e binay ı serbestçe dolaşm a fırsat ı elde ede r v e büyü k olasılıkl a hassa s bilgiler e ulaşabilir .

18-4 Geçic i kimlikle r

Kural: Başk a bi r tesiste n gele n v e yanlarınd a persone l kartlar ı bulun - mayan şirke t çalışanlar ı geçerl i bi r sürüc ü ehliyet i y a d a benzer i resiml i bir kimli k göstermel i v e onlar a geçic i bi r ziyaretç i kart ı verilmelidir .

Açıklamalar/Notlar: Saldırganla r şirket e girebilme k içi n sı k sı k şir - ketin başk a bi r binasında n y a d a şubesinde n gele n çalışanla r gib i davranırlar.

18-5 Aci l tahliy e

Kural: Aci l bi r durumd a y a d a bi r tali m sırasınd a güvenli k görevliler i herkesin binalar ı terkettiğinde n emi n olmalıdırlar .

Açıklamalar/Notlar: Güvenli k görevliler i tuvaletlerd e yâ'd a odalar - da gerid e kalmı ş olabilece k kişile r olu p olmadığın ı kontro l etmelidirler . İtfaiyenin ya da ortay a çıka n durumd a yetkil i ola n diğe r kurumları n da belirttiği üzer e güvenli k kuvvetler i tahliyede n ço k sonr a binay ı ter k ede n kişilere karş ı uyanı k olmalıdırlar .

Sanayi casuslar ı y a d a deneyiml i bilgisaya r kırıcılar ı bi r binay a y a d a güvenli bi r alan a girebilme k içi n yanlı ş alar m verebilirler . Kullanıla n hile - lerden bir i havay a büti l merkapta n adınd a zararsı z bi r ga z vermektir . Çalışanlar tahliy e işlemin e başladıkta n sonr a göz ü kar a saldırga n b u fir - satı y a bilg i çalma k içi n y a d a şirke t bilgisaya r sistemin e girme k içi n kul - lanır. Bilg i hırsızlarını n kullandığ ı başk a bi r takti k de , baze n tuvalett e bazen bi r odada , ta m tahliy e talimini n başladığ ı saatt e y a d a aci l tahli - yeye nede n olaca k si s bombas ı y a d a başk a bi r gere ç kullandıkta n sonra gerid e kalmaktır .

1 8- 6 Post a odasınd a ziyaretçile r

Kural: Bi r şirke t çalışanını n gözetimind e olmada n hiçbi r ziyaretçini n posta odasın a girmesin e izi n verilmemelidir .

Açıklamalar/Notlar: B u kuralı n amac ı dışarda n birini n şirke t iç i postaları karıştırmasını , göndermesin i y a d a çalmasın ı önlemektir .

18-7 Ara ç plak a numaralar ı

Kural: Eğe r şirketi n bekçil i bi r otopark ı varsa , güvenli k görevliler i b u alana gire n tü m araçları n plakaların ı no t etmelidirler .

18-8 Çö p bidonlar ı

Kural: Çö p bidonlar ı he r zama n şirke t alanı n içind e bulunmal ı v e dışarıdan erişilebili r olmamalıdır .

Açıklamalar/Notlar: Bilgisaya r saldırganlar ı v e sanay i casuslar ı şir - ket çöplerinde n değerl i bilgile r eld e edebilirler . Mahkemele r çöpler i yasal olara k ter k edilmi ş ma l olara k değerlendirirle r v e b u yüzde n bidon - lar herkes e açı k bi r aland a durduklar ı sürec e çö p dalışlar ı tamamiyl e yasaldır. B u nedenl e çöplerin , şirketin , bidonlar ı v e içindekiler i korum a hakkının olduğ u şirke t alan ı içind e tutulmalar ı önemlidir .

Danışma Görevliler i içi n Kuralla r

Danışma görevlileri , i ş toplu m mühendisleriyl e uğraşmay a gel - diğinde çoğ u zama n ö n cephededirler . Anca k onlar a nadire n bi r saldır - ganı far k edi p durdurabilmelerin i sağlayaca k eğitimle r verilir . Danışm a görevlinizin şirketiniz i v e verilerin i dah a iy i koruyabilmes i içi n b u kural - ları yürürlüğ e koyun .

19-1 Dahil î telefo n rehber i

Kural: Dahil î telefo n rehberind e açıklana n bilgiler e yalnızc a şirke t çalışanları erişebilmelidir .

Açıklamalar/Notlar: Rehberd e buluna n tü m unvanlar , adlar , telefo n numaraları v e adresle r dahil î bilg i olara k değerlendirilmel i v e yalnızc a veri sınıflandırm a kurallar ı v e dahil î bilgiler e yöneli k kuralla r doğrul - tusunda verilmelidir .

Ayrıca araya n tarafı n elinde , ulaşmay a çalıştığ ı kişini n ad ı y a d a dahili numaras ı olmalıdır . Arayanı n dahil î numaray ı bilmediğ i bi r durum - da he r n e kada r danışm a görevlis i gerekl i bağlantıy ı sağlas a d a arayan a dahilî numaray ı vermes i yasa k olmalıdı r (Örnek : isteye n meraklılar , her - hangi bi r Birleşi k Devletle r devle t dairesin i arayı p santra l memurun a dahilî numaray ı sorara k b u sürec i deneyebilirler.) .

19-2 Belirl i bölümlerin/grupları n telefo n numarala n

Kural: Çalışanlar , arayanı n geçerl i bi r neden i olu p olmadığın ı kont - rol etmeden , şirke t yardırr j masasının , telekomünikasyo n bölümünün , bilgi işlemi n y a d a siste m yöneticisini n dı ş ha t telefo n numaraların ı ver - memelidirler. Danışm a görevlisi , b u gruplarda n birin e bi r telefo n aktarırken arayanı n adın ı mutlak a açıklamalıdır .

Açıklamalar/Notlar: Baz ı kuruluşla r b u kural ı fazl a baskılayıc ı bul - salar da , b u kura l bi r toplu m mühendisini n çalışa n gib i davranı p başkalarını kend i dahil î numaralarında n yönlendirm e yapmalar ı içi n kandırmasını (baz ı telefo n sistemlerind e b u işlem , aramanı n şirke t için - den yapılıyormu ş gib i görünmesin i sağlar) y a d a kendin i kanıtlaya - bilmek içi n kurbanın a b u numaralar ı bildiğin i göstermesin i güçleştirir .

19-3 Bilg i aktarım ı

Kural: Santra ! memurlar ı v e danışm a görevlileri , çalışa n olu p olmadığını şahse n bilmedikler i kişile r adın a no t almamal ı y a d a bilg i aktarmamalıdır.

Açıklamalar/Notlar: Toplu m mühendisleri , dikkatsizli k gösteri p kendilerine kefi l olmalar ı içi n çalışanlar ı kandırma k konusund a ustadır - lar. Toplu m mühendisliğ i hilelerinde n biri , danışmanı n numarasın ı eld e edip, danışm a görevlisin e kendis i içi n bırakılmı ş mesa j olu p olmadığın ı sormaktır. Dah a sonr a kurbanın ı ararke n saldırgan , bi r çalışa n gib i davranır v e hassa s bi r bilg i verilmesin i y a d a bi r işle m yapılmasın ı iste - yerek an a santra l numarasın ı ger i aram a numaras ı olara k verir . E n sonunda saldırga n danışm a görevlisin i ara r v e hiçbi r şeyde n kuşkulan - mayan kurbanı n kendis i içi n bıraktığ ı mesaj ı alır .

19-4 Alınma k üzer e bırakılmı ş malzemele r

Kural: Bi r kuryey e y a d a tanımlanmamı ş başk a bi r kişiy e herhang i bir şe y verirken , danışm a görevlis i y a d a güvenli k görevlis i resiml i bi r kimlik görmel i v e kimli k bilgilerin i kuralları n öngördüğ ü şekild e kayı t def - terine işlemelidir .

Açıklamalar/Notlar: Toplu m mühendisliğ i taktiklerinde n bir i de , has - sas malzemeler i danışm a görevlisin e y a d a danışm a masasın a bırak - tırarak güy a yetkil i ola n bi r başk a çalışan a vermes i içi n bi r çalışan ı kandırmaktır. Danışm a görevlis i y a d a güvenli k görevlis i de , doğa l olarak paketi n alınmasını n sakıncal ı olmadığın ı düşünür . Toplu m mühendisi y a kendis i geli r y a d a paket i almas ı içi n bi r kury e hizmetinde n yararlanır.

Olay Bildirm e Grub u İçi n Kurallar

Her şirket , şirke t güvenliğin e yöneli k herhang i bi r saldı n far k edildiğinde aranma k üzer e merkez i bi r guru p oluşturmalıdır . Aşağıda b u grubun faaliyetlerini n düzenlenmes i v e yapılandırılmasın a yöneli k birkaç yo l gösteric i kura l bulacaksınız .

20-1 Ola y bildirm e grub u

Kural: Bi r kiş i y a d a guru p b u i ş içi n görevlendirilmel i v e çalışanla r güvenlikle ilgil i olaylar ı onlar a iletme k üzer e bilgilendirilmelidir .

Açıklamalar/Notlar: Çalışanla r bi r güvenli k tehdidin i nası l ayır t ede- ceklerini bilmel i v e oluşaca k herhang i bi r tehdid i ilgil i ola y bildirm e grubuna bildirece k şekild e eğitilmelidir . Bi r tehdi t oluştuğund a böyl e bi r gurubun hareket e geçebilmes i içi n kuruluşu n belirl i süreçle r v e yetkile r belirlemesi d e önemlidir .

20-2 Sürmekt e ola n saldırıla r

Kural: Ola y bildirm e gurubuna , sürmekt e ola n bi r toplu m mühendis - liği saldırıs ı bildirildiğind e gurup , hedeflene n bölümlerd e görevl i v e b u i ş için belirlenmi ş çalışanlar ı uyarma k üzer e süreçler i başlatacaktır .

Açıklamalar/Notlar: Ola y bildirm e gurub u y a d a soruml u yönetici , şirket çapınd a bi r uyar ı gönderili p gönderilmeyeceğine d e kara r verme - lidir. Soruml u kiş i y a d a gurubun , bi r saldırını n deva m ettiğin e inanc ı tamsa, şirke t çalışanların ı tetikt e olmalar ı konusund a uyarara k zarar ı e n aza indirme k başlıc a öncelikler i olmalıdır .

BİR BAKIŞT A GÜVENLİ K

Aşağıda verile n listele r v e şemala r ikinc i bölümde n o n dördünc ü bölümün sonun a kada r anlatıla n toplu m mühendisliğ i yöntemlerini n v e on altınc ı bölümd e ayrıntılandırıla n ona y süreçlerini n bi r bakışt a görülebileceği bi r başvur u kılavuz u oluşturmaktadır . B u bilgiler i kuru - munuza uyarlayı n v e bi r bilg i güvenliğ i sorun u ortay a çıktığ ı zama n çalışanlarınızın başvurabilmes i içi n herkes e duyurun .

Bir Saldırını n Belirlenmes i

Bu tablola r v e kontro l listeler i bi r toplu m mühendisliğ i saldırısın ı tespit etmeniz e yardımc ı olacaklardır .

Toplum mühendisliğ i döngüs ü

HAREKET AÇIKLAM A

Araştırma Aralarınd a güvenli k delm e test i kayıtları , yıllı k

raporlar, pazarlam a broşürleri , paten t uygulamaları ,

basın kupürleri , sektö r dergileri , interne t sayfas ı

içeriği olabilir . Ayrıc a çö p dalışlar ı d a olabilir . Dostluk v e güve n İçeride n gele n bilgileri n kullanılması , başkasını n uyandırma kimliğin e bürünme , kurbanı n tanıdığ ı kişileri n

adlarının sıralanması , yardı m isteğ i y a d a otoritey e

sahip olma .

Güveni kötüy e Kurbandan , bi r bilg i vermesini n y a d a bi r işle m yap - kullanma masını n istenmesi . Ter s dalavered e kurban , saldır -

gandan yardı m ister .

Bilgi kullanm a Eğe r edinile n bilg i ası l amaçta n bi r adı m uzaktaysa ,

saldırgan, amacın a ulaşan a kada r döngüdek i önce -

ki adımlar a ger i döner .

En Ço k

Toplum Mühendisliğ i Yöntemler i

• Bi r çalışa n gib i davranma k

• Bi r satıc ı firmanın , orta k i ş yürütüle n bi r şirketi n y a d a güvenli k

güçlerinin bi r personel i gib i davranma k

• Yetkil i bir i gib i davranma k '

• Yardım a ihtiyac ı olan , iş e yen i girmi ş bir i gib i davranma k • Bi r siste m yamas ı y a d a güncellemes i sunma k içi n araya n bi r

satıcı y a d a siste m üreticis i gib i davranma k

• Soru n çıktığ ı takdird e yardı m edebileceğin i söyleyi p sonr a

sorunu kendis i yaratma k v e böylec e kurbanı n yardı m isteme k

için kendisin i aramasın ı sağlama k

• Kurbanı n yüklemes i içi n bedav a yazılı m y a d a yam a gönderme k • E-post a ekind e virü s y a d a Truv a At ı gönderme k

• Kullanıcını n yenide n bağlanmasın ı y a d a parol a girmesin i

isteyen saht e bi r pencer e kullanma k

• Gözde n çıkarılmı ş bi r bilgisaya r sistem i y a d a programıyla , kur -

banın klavyede n yaptığ ı girişler i kaydetme k

• içind e köt ü huyl u yazılı m buluna n diske t y a d a CD'ler i işyerind e

görünür bi r şekild e bırakma k

• Güve n kazanma k içi n şirke t iç i terimler i kullanma k

• Şirke t iç i teslimat a girmes i içi n post a odasın a bi r belg e y a d a

dosya bırakma k

• içerde n gönderildiğ i izlenimin i verebilme k içi n fak s makinasını n

başlığını değiştirme k

• Danışm a görevlisinden , alacağ ı faks ı başk a bi r yer e faksla -

masını ric a etme k

• Bi r dosyanı n şirke t iç i gib i görüne n bi r yer e gönderilmesin i isteme k • Ger i aramalard a şirke t mensub u gib i görünece k şekild e bi r sesl i

mesaj kutus u oluşturma k

• Şehi r dışındak i bi r ofiste n geldiğini söyleyi p bulunduğ u yerde n

e-postalarını okuyabilmey i isteme k

Bir Saldırını n Uyar ı Sinyaller i

• Bi r ger i aram a numaras ı vermekte n kaçınılmas ı

• Sıradış ı taleplerd e bulunulmas ı

• Yetkil i olunduğunu n ön e sürülmes i

• Aciliyeti n üzerin e vurg u yapılmas ı

• İsteği n yerin e getirilmemes i durumund a köt ü sonuçla r doğa -

cağının söylenmesi i • Sor u sorulduğund a rahatsı z olunmas ı

• Biline n adları n sıralanmas ı

• iltifa t edili p pohpohlanm a

• Ku r yapılmas ı

Bir Bakışt a Güvenli k 30 5

Saldırılarda en-sı k görüle n hedefle r

HEDEF TÜR Ü ÖRNEKLE R • - • • , . Bilginin Danışm a görevlileri , santra l memurları , idar î değerinden yardımcılar , güvenli k görevliler i

habersiz olanla r

Özel ayrıcalıklar a Yardı m masas ı y a d a tekni k destek , siste m yöneti - sahip olanla r çileri , bilgisaya r işletmenleri , telefo n sistemler i

yöneticileri

Üretici/Satıcı Bilgisaya r donanımı , yazılı m üreticileri , sesl i mesa j firmalar sistemler i satıcılar ı

Belli bölümle r Muhasebe , insa n kaynaklar ı

Şirketleri Saldırılar a Açı k Durum a Getire n Unsurla r • Ço k sayıd a çalışa n olmas ı . _ • e Birde n fazl a tesi s bulunmas ı

• Çalışanı n nered e olduğuyl a ilgil i sesl i mesajlard a bilg i verilmes i • Dahil î telefo n numarasını n verilmes i

• Güvenli k eğitimlerini n yetersizliğ i

• Ver i sınıflandırm a sistemini n bulunmamas ı

9 Bi r ola y bildirm e y a d a karş ı eyle m planını n yürürlükt e olmamas ı

Onaylama v e Ver i Sınıflandırm a

Bu tablola r v e şemala r toplu m mühendisliğ i saldırıs ı olabilece k bilg i ya d a işle m taleplerin e karşılı k vermeniz e yardımc ı olacaklardır .

Kimlik Tespit i Yapılm a Sürec i

HAREKET TANI M

Arayan kimliğini n Gele n aramanı n dahil î olu p olmadığın ı v e görüne n belirlenmesi numaranı n y a d a adın , arayanı n kimliğiyl e uyuşu p

uyuşmadığını kontro l edin .

Geri aram a İste k sahibin i şirke t telefo n rehberinde n bulup ,

rehberde geçe n numarada n on u ger i arayın . Kefil olm a Güvenili r bi r çalışanda n iste k sahibin e kefi l

olmasını isteyin .

Paylaşılan orta k Bi r parol a y a d a günlü k şifr e gib i şirke t içind e kul - anahtar lanıla n orta k anahtar ı tale p edin .

HAREKET

TANIM (Tablonun devamı) '

Müdür y a d a yönetici Güvenli e-post a Kişisel se s tanımlama Değişken parolalar

Şahsen görm e

Çalışanın bi r üs t yöneticisin i arayı n v e kimliğini n ve çalışm a durumunu n onaylanmasın ı isteyin . Dijital olara k imzalanmı ş bi r mesa j tale p edin . Çalışanın tanıdığ ı bir i arıyors a sesinde n tanımay a çalışın.

Güvenli kimli k y a d a başk a bi r güçl ü tanımlam a aracı kullanara k değişke n parol a çözümlerin e başvurun.

istek sahibini n persone l kartıyl a y a d a başk a bi r kimlik belgesiyl e şahse n gelmesin i isteyin .

Çalışma Durumunu n Onaylanm a Sürec i HAREKET AÇİKLAM A

Şirket telefo n Çevrimiçi rehberd e iste k sahibini n adını n geçi p rehberinden geçmediğini kontro l edin .

kontrol

İstek sahibini n Şirket rehberind e geçe n numaray ı kullanara k yöneticisinin istek sahibini n yöneticisin i arayın .

onayı

İstek sahibini n iste k sahibini n bölümün ü y a d a i ş grubun u bölümünün y a d a arayara k kişini n hale n şirkett e çalışı p iş grubunu n onay ı çalışmadığın ı kontro l edin .

Bilme Gereğin i Kontro l Sürec i

HAREKET TANI M

Unvan/iş Bell i gizl i bilgiler e hang i çalışanları n erişi m hakk ı grubu/sorumlu- olduğun u öğrenme k içi n öncede n yayınlanmı ş luklar listelerin e şirke t iç i listeler e başvurun .

başvurun

Yöneticiden Kendi yöneticiniz i y a d a iste k sahibini n yöneticisin i yetki alı n arayıp isteğ i yerin e getirme k içi n ona y isteyin . Bilgi sahibinde n Bilgi sahibinde n istekt e buluna n kişini n bilm e ya d a yede k gereği olu p olmadığın ı öğrenin .

sorumludan

yetki alı n

Otomatik bi r ara ç Yetkil i persone l içi n tescill i yazılı m ver i tabanların a kullanarak bakın .

yetki alı n

Bir Bakışt a Güvenli k 30 7

Şirket Çalışan ı Olmayanlar ı Belirleme k

İçin Kriterle r .. . -

KRİTER HAREKE T

İlişki istekte buluna n kişini n çalıştığ ı firmanı n bi r satıcı ,

stratejik orta k y a d a başk a bi r i ş ilişkis i ola n firm a

olduğundan emi n olun .

Kimlik istek sahibini n kimliğin i v e i ş durumun u satıcı/orta k

firmadan öğrenin .

Açığa vurmam a istek sahibini n yürürlükt e ola n bi r açığ a vurmam a

anlaşması imzaladığında n emi n olun .

Erişim Bilgi, dahil î vey a dah a üs t derec e olara k

sınıflandırılmışa taleb i yönetim e gönderin .

Veri Sınıflandırm a

SINIFLANDIRMA AÇIKLAM A

Genel Herkese serbestç e Onaylanmay a gere k yoktur ,

verilebilir.

Dahilî Şirket iç i kullanı m Şirket çalışanlarını n hale n

içindir çalışıp çalışmadıklarını n kontrol ü

ya d a şirke t çalışan ı olmayanla r

için yürürlükt e bi r açığ a vurma -

ma anlaşmasını n olmas ı v e

yönetici onayını n alınmas ı Özel Yalnızca kuru m

istek sahibini n faa l bi r çalışa n

içinde kullanılma k

ya d a dışarda n yetkil i bi r kiş i

üzere belirlenmi ş

olduğunun onaylanması . Yetkil i

kişisel nitelikl i

çalışanlara y a d a dışarda n

bilgiler. gelen talepler e öze l bilgile r ver -

meden önc e insa n kaynakların -

dan kontro l edilmesi , Gizli Kurum içind e yal -

ilgili bilg i sahibin e istekt e bulu -

nızca kesinlikl e

nan kişini n kimliğin i v e bilm e

bilmesi gereke n

gereğini onaylatın . Yalnızc a

kişilerce biline n

yöneticinin, bilg i sahibini n y a

bilgiler.

da sorumlusunu n yazıl ı izniyl e

isteği yerin e getirin . Yürürlükt e

olan bi r açığ a vurmam a anlaş -

ması olu p olmadığın ı kontro l

edin. Şirke t mensub u olmaya n

kişilere yalnızc a yöneticier

açıklama yapabilir .

308 Aldatm a Sanat ı

Bilgi Talebin e Karşılı k Verme k

Altın Sorula r

Bu kişini n söylediğ i kiş i olduğun u nası l bilebilirim ? Bu kişini n böyl e bi r istekt e bulunma k içi n yetkil i olu p olmadığın ı

Personel raporlam a yapısı , çalışan adla n v e unvanlar ı

Personelin kullandığ ı dahil î

teîefon numaraları , fak s numaraları, bin a iç i numarala r

ve bolu m üsteler i

Kişisel telefo n numarala n

(ev y a d a cep) , sosya l

güvenlik numarası , e v adresi, özgeçmiş i v e maaş ı

İşletim sistem i çeşidi , uzaktan erişi m süreçleri , uzak bağlant ı numarala n v ı

bilgisayar sistemlerin e

verilmiş adla r

Üretim süreçleri , strateji k planlar, tescill i kayna k kodları, müşter i Üsteler i v e

ticari sırla r

nasıl öğrenebilirim ?

istenen bilg i neyl e ilgili. .

Hayır

Kuruluş Şemas ı

Ayrıntıları

Hayır

Şirket Telefo n

Rehberi

Hayır

Kişisel Bilgile r

Hayır

g ı saya r

Sistemleri Süreçleri y a d aBilgile

Hayır

Gizli y a d a Öze l

Bilgiler

Parolanızı

HİÇBİR KOŞULD A başkalarına söylemeyin .

Dahilî bilgileri n açıklanmasıyla ilgil i

süreci izleyin .

Dahilî bilgileri n açıklanmasıyla ilgil i

süreci izleyin .

Dahilî bilgileri n açıklanmasıyla ilgil i

süreci izleyin .

Dahilî bilgileri n açıklanmasıyla ilgil i

süreci izleyin .

Veri sınıfların ı belirleyin ; bilgi vermey e yöneli k olara k ilgili süreçler i taki p edin .

Bir Bakışt a Güvenli k 30 9

İşlem Talebin e Karşılı k Verme k

• Altı n Kuralla r

rttılik tespit i yapılmada n kimsey e güvenilmemelidir . Gelen talepleri n sorgulanmas ı teşvi k edilmelidir .

Talep edile n işle m

Parola Değiştirme k

Tescilli kayna k kodlan , ticar î

sırlar, üreti m süreçleri , formüller, ürü n özellikleri , pazarlama veriler i y a d a

iş planla n

Dahilî Bilgiy i Elektronik Olara k

Aktarmak

Bİ boiüm ü tarafında n özellikl e onaylanmamışa herhang i bi r kimsenin İsteğ i doğrultusund a hiçbir zama n bilmediğini z

komutlar girmeyi n v e

program çalıştırmayın .

Herhangi Bi r Bilgisayara Komu t

Girmek

Yalnızca dijita l İmzayl a doğruluğu kanıtlanmış , güve - nilir kaynaklarda n edindiğini z

yazılımları yükleyin .

Yazılım

•İndirmelcYükJemeİ ^ya d a Devr e

.Bırakmak,

Bİ bölüm ü tarafında n özellikle onaylanmamışsa , BlOS'un, işleti m sistemini n

ya d a herhang i bi r uygulamanın (kişise l güven - lik duvar ı y a d a virü s koru - ma programlar ı d a dahil) ayarlarını değiştirmeyin .

Bilgisayar ^ "ya d a A ğ Ayarlarının 1

Değiştirilmesi

Beklediğiniz bi r şe y değils e ekleri açmayın ; tü m ekler i virüs korum a yazılımlarıyl a

tarayın.

HİÇBİR ZAMA N parolanız ı başkasının bildiğ i bi r şeyl e değiştirmeyin, bi r a n içi n

olsa bile !

Veri sınıfların ı belirleyin ; bilgi vermey e yöneli k olara k ilgili süreçler i taki p edin .

Böyle bi r tale p anca k B İ bölümünden gelebilir ; Çalışanın Kimli k Tespit i Süreçlerine bakınız .

Böyle bi r tale p anca k B İ bölümünden gelebilir ; Çalışanın Kimli k Tespit i Süreçlerine bakınız .

Böyle b/ r tale p anca k B İ bölümünden gelebilir ; Çalışanın Kimli k Tespit i Süreçlerine bakınız .

Başkaları aüma yaptığına tüm hareteJler .

Daima kontro l edin , kontro l edin , kontro l edin .