

Uticaj ljudskog faktora na bezbednost

UMETNOST

O B M A N E

O B M A N E

KEVIN D. MITNIK

i Vilijam L. Sajmon

O B M A N E

UMETNOST

Predgovor napisao Stiv Voznijak

Social Engineering

engleski termin *social engineering* označava manipulisanje ljudima ubedivanjem i lažnim predstavljanjem. Obmanjivač (engl. *social engineer*) zloupotrebljava ljude da bi došao do informacija, pri čemu može – ali ne mora – koristiti tehnološka sredstva.

sadržaj

Uvodna reč	vii
Predgovor	ix
Uvod	xv
Deo 1 Iza kulisa	1
Poglavlje 1 Najslabija tačka bezbednosnog sistema	3
Deo 2 Umeće napadača	13
Poglavlje 2 Kada bezazlena informacija nije tako bezazlena	15
Poglavlje 3 Direktan napad: samo tražite ono što vam treba	31
Poglavlje 4 Izgradnja poverenja	41
Poglavlje 5 „Dopustite da vam pomognem“	55
Poglavlje 6 „Možete li mi pomoći?“	77
Poglavlje 7 Lažne Web lokacije i opasni prilozi	93
Poglavlje 8 Iskorišćavanje sažaljenja, osećaja krivice i zastrašivanja	107
Poglavlje 9 Obrnuta žaoka	135
Deo 3 Uzbuna zbog uljeza	151
Poglavlje 10 Upad u prostorije	153
Poglavlje 11 Kombinovanje tehnologije i obmane	177
Poglavlje 12 Napadi na zaposlene u prijemnim odeljenjima	199
Poglavlje 13 Dobro osmišljene prevare	215
Poglavlje 14 Industrijska špijunaža	231

Deo 4 Pogled u suštinu problema	249
Poglavlje 15 Obuka za zaštitu podataka	251
Poglavlje 16 Preporučena bezbednosna pravila	265
Pregled bezbednosnih metoda	333
Bibliografija	341
Zahvalnica	343
Indeks	349

uvodna reč

Ij udi se rađaju sa željom da istražuju okolinu. Kao mladići, Kevin Mitnik i ja bili smo veoma radoznali; zanimao nas je svet i bili smo željni dokazivanja. Često su naši pokušaji da saznamo nešto novo, rešimo zagonetke i pobedimo u igrama bili nagrađivani. Istovremeno, društvo nas je naučilo pravilima ponašanja, koja su sputala naš istraživački nagon. Najsmelijim naučnicima i poznavaočima tehnologije, kao i ljudima poput Kevina Mitnika, prepuštanje tom unutrašnjem nagonu pruža izuzetno zadovoljstvo, jer im omogućava da postignu stvari za koje drugi veruju da su nemoguće.

Kevin Mitnik je jedan od najčestitijih ljudi koje poznajem. Samo ga pitajte, pa će vam otvoreno reći da ono čime se nekada bavio – obmanjivanje – podrazumeva varanje ljudi. On se time više ne bavi. Čak i dok je to činio, motiv mu nikada nije bio da se obogati ili naškodi drugima. To ne znači da ne postoje opasni i destruktivni kriminalci koji obmanjuju ljude da bi naneli pravu štetu. Upravo zato je Kevin napisao ovu knjigu – da bi vas upozorio na njih.

Umetnost obmane otkriva koliko smo svi podložni obmanama – državne institucije, kompanije i svako od nas ponaosob. Pošto smo svi svesni bezbednosnih pitanja, trošimo mnogo novca na tehnologiju da bismo zaštitili računarske mreže i podatke. U ovoj knjizi istaknuto je koliko je lako prevariti zaposlene u organizacijama i zaobići tehnološku zaštitu.

Bilo da radite u preduzeću ili državnoj instituciji, ova knjiga predstavlja jasan putokaz koji će vam pomoći da razumete kako obmanjivači rade i šta možete učiniti da ih osujetite. Pomoću zabavnih i poučnih izmišljenih

prča, Kevin i njegov saradnik Bil Sajmon predstavljaju vam tehnike računarskog podzemlja. Nakon svake priče nude vam praktične savete za odbranu od upada i pretnji koje opisuju.

U bezbednosnoj tehnologiji postoji mnogo propusta. Ljudi poput Kevina mogu nam pomoći da ih premostimo. Pročitajte ovu knjigu i možda ćete najzad shvatiti da svi moramo tražiti pomoć od nekog našeg Mitnika.

– Stiv Voznijak

predgovor

neki hakeri uništavaju ljudima datoteke ili celokupan sadržaj disko-
va – oni su *provalnici* ili *vandali*. Neki hakeri početnici se ne trude
da nauče tehnologiju, već koriste hakerske alate da bi provalili u
računarske sisteme – oni su *skriptaši*. Iskusniji hakeri razvijaju hakerske
programe i objavljuju ih na Webu i u diskusionim grupama. A tu su i osobe
koje tehnologija ne zanima, već računar koriste samo kao pomoćno sred-
stvo za krađu novca, dobra i usluga.

Uprkos mitu koji su o Kevinu Mitniku ispleli mediji, ja nisam zlona-
meran haker.

Ali, sad vam sve pričam unapred.

POČECI

Svoj put sam verovatno odabrao rano. Bio sam bezbrižno dete, ali sam se
dosadiwao. Nakon što nas je otac ostavio kada sam imao tri godine, moja
majka je radila kako konobarica da bi nas izdržavala. Pošto je morala
naporno da radi po ceo dan, ja sam uglavnom danju bio sam. Čuvao sam
sam sebe.

Budući da sam odrastao u San Fernando Veliju, mogao sam da istražu-
jem čitav Los Angeles, a do svoje dvanaeste godine pronašao sam način da
putujem besplatno po čitavoj teritoriji L.A. Jednog dana, dok sam se vozio
autobusom, shvatio sam da ispravnost karte za gradski prevoz zavisi od ne-
običnog rasporeda izbušenih rupica kojima su vozači označavali dan, vreme
i trasu. Jedan ljubazan vozač odgovorio je na moje pažljivo formulisano pi-
tanje. Objasnio mi je gde da kupim tu vrstu aparata za bušenje rupica.

Karte za presedanje omogućavaju putnicima da menjaju autobuse do
odredišta, ali ja sam smislio kako da pomoću njih besplatno putujem gde

god poželim. Nabaviti neoverene karte za presedanje bio je mačji kašalj. Karte za otpatke na autobuskim stajalištima bile su uvek pune delimično ispunjenih blokova karata za presedanje, koje bi vozači bacili na kraju smene. S blokom praznih karata i uređajem za bušenje rupica, mogao sam da označavam sopstvenu trasu i putujem kud god su išli autobusi u Los Andelesu. Ubrzo sam gotovo napamet znao red vožnje čitavog gradskog prevoza. (To je bio jedan od prvih primera mog začuđujućeg pamćenja određenih vrsta informacija: i danas mogu da se setim telefonskih brojeva, lozinki, i drugih naizgled beznačajnih pojedinosti iz detinjstva.)

U detinjstvu sam bio opčinjen opsenarstvom. Kad bih saznao kako se nov trik izvodi, vežbao bih, vežbao, i još malo vežbao dok ga ne bih naučio. U izvesnoj meri, upravo sam kroz mađioničarstvo otkrio radost saznavanja nečeg tajanstvenog.

Od prevaranta koji se služi telefonom do hakera

Moj prvi susret s onim što ću kasnije zvati *obmanjivanje*, dogodio se u srednjoj školi, kad sam se upoznao s učenicom čiji je hobi bio *zloupotrebljavanje telefona*. To je vrsta hakerisanja kojim se istražuje telefonska mreža. Koriste se telefonski sistemi i iskorišćavaju zaposleni u telefonskoj kompaniji. Pokazao mi je zgodne trikove koje je umeo da izvede preko telefona, poput dobijanja svih informacija koje telefonska kompanija ima o bilo kom klijentu, ili upotrebe tajnog probnog broja da bi se besplatno koristile međugradske veze. (Zapravo, samo je za nas to bilo besplatno. Mnogo kasnije sam saznao da to uopšte nije bio tajni probni broj. Pozivi su se naplaćivali preko MCI računa neke jadne kompanije.)

To me je uvelo u obmanjivanje – bilo je to, takoreći, moje obdanište. Moj prijatelj i još jedan takav prevarant, kojeg sam nedugo zatim upoznao, dozvoljavali su mi da slušam dok su pod nekim *izgovorom* pozivali telefonsku kompaniju. Čuo sam stvari koje su im govorili da bi zvučali verovatnije; naučio sam nešto o različitim ograncima telefonske kompanije, njihovu terminologiju i procedure. Ta obuka nije dugo trajala; nije ni bilo potrebno. Uskoro sam sve to radio sam, usput učeći, sve dok nisam postao bolji i od sopstvenih prvih učitelja.

Put kojim će se moj život odvijati tokom sledećih petnaest godina bio je zacrtan.

U srednjoj školi mi je jedna od omiljenih šala bila da neovlašćeno pristupim telefonskoj centrali i izmenim klasu usluge na liniji nekog drugog prevaranta. Kad bi pokušao da pozove od kuće, poruka bi ga obavestila da treba da ubaci novčić jer bi do telefonske centrale stizao signal koji znači da zove iz telefonske govornice.

Opčinjavalo me je sve o telefonima – ne samo elektronika, centrale i računari, već i organizacija telefonske kompanije, te njihove procedure i terminologija. Nakon izvesnog vremena, verovatno sam bolje poznavao telefonski sistem od bilo kog zaposlenog. Svoju veštinu obmane razvio sam do te mere da sam, sa sedamnaest godina, mogao da – lično ili telefonom – nagovorim većinu zaposlenih u telefonskoj kompaniji da učine gotovo bilo šta.

Moja hakerska karijera, o kojoj se mnogo govorilo u javnosti, počela je dok sam bio u srednjoj školi. Iako ovde ne mogu opisivati pojedinosti, reći ću da je jedna od linija vodilja u mojim ranim hakerskim danima bila da budem prihvaćen u krug ostalih hakera.

U to vreme, nama je izraz *haker* označavao osobu koja provodi mnogo vremena petljajući s hardverom i softverom, da bi razvio efikasnije programe ili da bi zaobišao nepotrebne korake i obavio posao brže. Taj izraz je sada postao pogrdan, i označava „zlomamernog kriminalca“. U ovoj knjizi ja ga koristim kao i uvek – u njegovom starijem, dobroćudnijem značenju.

Nakon srednje škole, studirao sam informatiku u Centru za računarsku obuku u Los Andelesu. Za nekoliko meseci, upravnik računarske mreže u školi otkrio je da sam pronašao propust u operativnom sistemu i dodelio sebi ovlašćenja administratora na njihovom IBM-ovom miniračunaru. Ni najbolji stručnjaci za računare koji su tamo predavali nisu mogli da shvate kako sam to učinio. Bio je to možda jedan od najranijih primera „unajmljivanja hakera“ – ponudu nisam mogao da odbijem. Tražili su da za diplomski rad uradim projekat za unapređivanje bezbednosti školskih računara, ili da budem izbačen zbog hakerskog upada u sistem. Naravno, odabrao sam prvo, pa sam na kraju diplomirao s najvećim ocenama.

Kako sam počeo da se bavim obmanjivanjem

Neki ljudi svakog jutra ustaju iz kreveta užasavajući se rutine svakodnevnog posla u „rudniku“, kako se kaže. Ja sam bio te sreće da sam uživao u poslu. Ne možete ni zamisliti izazov, nagradu i zadovoljstvo koje sam

dobijao za vreme koje sam proveo kao privatni istražitelj. Brusio sam svoj talenat u *umetnosti obmane* (u kojoj se ljudi navode da čine ono što obično ne bi uradili za neznanca), i bio sam za to plaćen.

Meni nije bilo teško da postanem vrstan obmanjivač. Očeva familija se generacijama bavila trgovinom, pa sam umetnost uticanja i ubeđivanja možda i nasledio. Kad spojite tu crtu s težnjom za varanjem ljudi, dobijate tipičan profil osobe koja može da se bavi obmanjivanjem.

Moglo bi se reći da postoje dve specijalnosti u okviru tog zanimanja. Onaj ko vara ljude i izmamљуje od njih novac pripada jednoj potkategoriji – *varalicama*. Onaj ko obmanjuje i ubeđuje zaposlene u kompanijama, i utiče na njih, obično s ciljem da se domogne njihovih informacija, pripada drugoj potkategoriji – *obmanjivačima*. Još od vremena kad sam izvodio svoj trik s kartama za autobus, kad sam bio isuviše mali da bih znao da to što radim nije u redu, počeo sam u sebi da prepoznajem talenat za otkrivanje tajni koje nije trebalo da saznam. Taj sam talenat nadogradio koristeći se obmanom, poznajući terminologiju, i razvijajući do majstorstva veštinu manipulacije.

Jedan od načina na koji sam razvijao veštinu svog zanata, ako ga tako mogu nazvati, bio je da izaberem neki podatak do kojeg mi nije zaista stalo, i da vidim mogu li nekog s druge strane žice nagovoriti da mi ga oda, tek da bih se kalio. Kao što sam uvećavao iluzionističke trikove – vežbao sam laganje preko telefona. Uskoro sam otkrio da mogu da dodem do gotovo bilo koje informacije koju poželim.

Kao što sam opisao u svedočenju pred senatorima Libermanom i Tomsonom godinama kasnije:

Neovlašćeno sam pristupao računarskim sistemima nekih od najvećih firmi na svetu, i uspešno sam upadao u neke od najotpornijih računarskih sistema koji su ikad napravljeni. Koristio sam tehnička i ostala sredstva da bih se domogao izvornog koda raznih operativnih sistema i telekomunikacionih uređaja, da bih proučavao njihove slabe tačke i način na koji rade.

Sve to sam činio da bih zadovoljio sopstvenu znatiželju; da bih video šta mogu; i da bih otkrio tajne informacije o operativnim sistemima, mobilnim telefonima, i svemu ostalom što bi zagolicalo moju ljubopitljivost.

ZAKLJUČAK

Nakon hapšenja, priznao sam da je to što sam činio nezakonito, i da sam narušavao tuđu privatnost.

Ta krivična dela vršio sam iz radoznalosti. Hteo sam da znam što više o tome kako rade telefonske mreže, kao i sve pojedinosti o obezbeđenju kompanija. Prešao sam put od momka koji voli da prikazuje iluzionističke trikove, do najozloglašnijeg svetskog hakera, kojeg se plaše i kompanije i vlade. Kad razmislim o svom životu u poslednjih 30 godina, priznajem da sam doneo neke veoma loše odluke, vođen ljubopitljivošću, željom da naučim nešto više o tehnologiji, kao i potrebom za odgovarajućim intelektualnim izazovima.

Sada sam druga osoba. Koristim svoj talenat i ogromno znanje o bezbednosti informacija i metodama obmane da bih pomogao državnim institucijama, kompanijama i pojedincima da spreče i otkriju opasnosti po bezbednost informacija, i da na to reaguju.

Ova knjiga je još jedan način da svojim iskustvom pomognem drugima da se odbrane od zlobnih kradljivaca informacija. Smatram da će vam priče biti zabavne, poučne i informativne.

uvod

Ova kniga sadrži obilje podataka o bezbednosti informacija i obmanjivanju. Da biste se lako snašli čitajući je, evo kratkog pregleda:

U prvom delu obelodaniću najslabiju tačku bezbednosnog sistema i pokazaću zašto ste vi i vaše preduzeće potencijalna žrtva obmanjivača.

U drugom delu videćete kako se napadači poigravaju vašim poverenjem, željom da nekome pomognete, sažaljenjem i lakovernošću, da bi došli do onoga što žele. U izmišljenim pričama o tipičnim napadima pokazaću vam da obmanjivači mogu da imaju razna lica. Ako mislite da se nikada niste susreli s varalicom, verovatno niste u pravu. Da li ćete prepoznati priče i zapitati se da li ste imali bliski susret sa obmanjivačem? Sasvim je moguće. Kad knjigu pročitate redom, od drugog do devetog poglavlja, znaćete kako da izađete kao pobednik ako do napada ponovo dođe.

U trećem delu saznaćete kako se u svetu obmane povećava ulog. U izmišljenim pričama opisano je kako može da se uđe u prostorije preduzeća, kako mogu da se dobiju poverljive informacije, ili da se naruše visokotehnološke bezbednosne mere. Zahvaljujući tim pričama postaćete svesniji raznih pretnji – od obične osvete zaposlenog, do terorizma preko Interneta. Ako su vam važne informacije od kojih vam zavisi posao i privatnost podataka, pažljivo pročitajte poglavlja od 10 do 14.

Bitno je imati na umu da su sve anegdote u ovoj knjizi u celosti izmišljene, ukoliko nije drugačije naglašeno.

U četvrtom delu pozabavio sam se sprečavanjem napada. U poglavlju 15 nalazi se program za uspešnu obuku o bezbednosti. A poglavlje 16 bi vam moglo spasti glavu – reč je o potpunom bezbednosnom pravilniku koju možete prilagoditi sopstvenoj organizaciji i odmah ga primeniti kako biste zaštitili važne informacije.

Na kraju knjige nalazi se i *Pregled bezbednosnih metoda*, u kome se nalaze spiskovi, tabele i grafikoni s ključnim informacijama koje vaši zaposleni mogu primeniti da bi onemogućili obmane na radnom mestu. Tu ćete pronaći i vredne podatke za osmišljavanje sopstvenog programa za obuku o bezbednosti.

U knjizi ćete naći još nekoliko korisnih elemenata: u okvirima označenim nazivom Terminologija, nalaze se definicije iz oblasti obmanjivanja i terminologija računarskih hakera; Mitnikove poruke su saveti za poboljšavanje bezbednosne strategije; u napomenama možete pročitati zanimljivosti ili dodatne informacije o temi.

deo

1

Najslabija tačka
bezbednosnog sistema

Iza kulisa

poglavlje

1

Najslabija tačka bezbednosnog sistema

preduzeće može da kupi najbolje dostupne bezbednosne tehnologije, obučiti ljude tako dobro da zaključavaju sve tajne informacije pre nego što uveće podu kući, i zaposli najbolje čuvaru zgrade.

Takva kompanija je ipak potpuno ranjiva.

Pojedinci se mogu pridržavati svakog visokobezbednosnog pravila koje preporučuju stručnjaci, revnosno instalirati svaki preporučeni proizvod iz oblasti bezbednosti, i mogu veoma pažljivo konfigurisati sistem i primenjivati bezbednosne zakrpe.

I ti pojedinci su ipak sasvim podložni napadima.

LJUDSKI ČINILAC

Kad sam svedočio pred Kongresom SAD, objasnio sam da sam često dolazio do lozinki i drugih poverljivih informacija pretvarajući se da sam neko drugi i *jednostavno tražeći*.

Prirodno je da čovek teži osećanju apsolutne sigurnosti, usled čega se mnogi uljuljkuju u lažno osećanje bezbednosti. Uzmite, na primer, odgovornog i brižnog kućevlasnika. Da bi zaštitio svoju ženu, decu i dom, na ulazna vrata ugrađuje bravu s prekidačem, za koju se misli da se ne može obiti. On se sada oseća mnogo prijatnije, budući da je njegova porodica

mного bolje zaštićena od uljeza. Ali šta ako provalnik razbije prozor ili otkrije šifru sistema za otvaranje garažnih vrata? Šta kažete na to da instalirate robustniji bezbednosni sistem? To je bolje, ali i dalje nema garancija. Sa skupim bravama ili bez njih, kućevlasnik je i dalje podložan napadima.

Zašto? Zato što je *ljudski* činilac zapravo najslabija tačka bezbednosnog sistema.

Bezbednost je suviše često samo iluzija, iluzija kojoj povremeno idu u prilog lakovernost, naivnost, ili neznanje. Najčuveniji svetski naučnik dvadesetog veka, Albert Ajnštajn, rekao je: „Samo su dve stvari bezgranične, univerzum i ljudska glupost, a za ono prvo nisam ni siguran“. Dakle, obmanjivanje može da uspe kada se naiđe na ljudsku glupost ili, češće, na nepoznavanje dobrih bezbednosnih pravila. Budući da imaju sličan stav kako i naš kućevlasnik koji pazi na bezbednost, mnogi stručnjaci iz oblasti informacionih tehnologija (IT) žive u zabludi da su u velikoj meri obezbedili preduzeće primenom standardnih bezbednosnih proizvoda – zaštitnih barijera, sistema za otkrivanje upada, ili moćnijih uređaja za identifikaciju poput onih sa šiframa koje se menjaju u vremenskim intervalima, ili biometričkih identifikacionih kartica. Svi koji smatraju da sami bezbednosni proizvodi nude pravu sigurnost, uljuljuju se u *iluziju* sigurnosti. Oni žive u svetu uobrazilje: pre ili kasnije, neizbežno će im se dogoditi bezbednosni incident.

Kao što priznati savetnik za bezbednost Brus Šnajer kaže: „Bezbednost se ne dobija od proizvoda; to je proces“. Štaviše, to nije tehnološki problem – već problem ljudi i uprave.

Kako se razvijaju sve bolje i bolje bezbednosne tehnologije, koje otežavaju pronalaženje tehničkih propusta, napadači će se sve više okretati ljudskom činiocu. Poražavanje ljudskog sigurnosnog bedema je često lako, ne zahteva nikakva ulaganja osim jednog telefonskog poziva, i podrazumeva minimalan rizik.

KLASIČAN SLUČAJ OBMANE

Šta je najveća pretnja bezbednosti vašeg poslovanja? Odgovor je jednostavan; to je obmanjivač – beskrupulozni mađioničar čiju levu ruku gledate dok vam desnom krade tajne informacije. Ta osoba je često tako prijateljski nastrojena, toliko je slatkorečiva i predusretljiva, da ste srećni što ste na nju naišli.

Evo primera obmane. Ne sećaju se mnogi danas mladog Stenlija Marka Rifkina i njegove male avanture sa sada nepostojećom bankom Security Pacific National Bank u Los Angelesu. Postoje razne priče o njegovim ludorijama, jer Rifkin (poput mene) nikada nije ispričao sopstvenu verziju. Priča koja sledi zasniva se na objavljenim izveštajima.

Otkrivanje šifre

Jednog dana 1978. Rifkin se odšetao do prostorije za transakcije banke Security Pacific. Pristup toj prostoriji bio je dozvoljen samo određenim zaposlenima. Službenici su tu slali i primali transakcije čija je ukupna vrednost dostizala i nekoliko milijardi dolara svakog dana.

Kompanija u kojoj je radio trebalo je da projektuje rezervni sistem za podatke, u slučaju da se glavni računar pokvari. Zahvaljujući toj ulozi imao je pristup proceduri rada pri transakcijama, uključujući i to kako činovnici banke šalju nalog da se novac prebaci na neki račun. Saznao je da se ovlašćenim činovnicima svakog jutra daje pomno čuvana dnevna šifra, koju koriste kad zovu sobu za transakcije.

Zaposleni u prostoriji za transakcije nisu se trudili da zapamte šifru: pisali su je na papiriće i kačili na vidna mesta. Tog novembarskog dana Rifkin je imao poseban razlog za posetu. Želeo je da osmotri taj papirić.

Stigavši u sobu za transakcije, zapisao je neke podatke, navodno da bi se uverio da će se rezervni sistem valjano uklopiti sa postojećim sistemima. U međuvremenu, potajno je pročitao bezbednosnu šifru s parčeta papira i zapamtio je. Izašao je nakon nekoliko minuta. Kako je kasnije rekao, osećao se kao da je upravo osvojio nagradu na lutriji.

U pitanju je taj bankovni račun u Švajcarskoj...

Napustivši prostoriju oko 3 časa poslepodne, uputio se pravo ka telefonskoj govornici u mermernom holu zgrade. Ubacio je novčić i okrenuo broj prostorije za transfere. Potom je preuzeo tuđ identitet, ne predstavljajući se više kao Stenli Rifkin, bankarski savetnik, nego kao Majk Hensen, član Međunarodnog odseka banke.

Prema jednom izvoru, razgovor se odvijao približno ovako:

„Zdravo, ovde Majk Hensen iz Međunarodnog“, rekao je mladoj ženi koja se javila na telefon.

Ona ga je upitala za broj kancelarije. To je bila uobičajena procedura, pa je on bio spreman: „286“, rekao je.

Devojka je pitala: „Koja je šifra?“

Rifkin je rekao da mu je u tom trenutku adrenalin pojurio venama a srce poskočilo. Ravnodušno je odgovorio: „4789“. Potom joj je dao nalog za prenos „tačno deset miliona i dve stotine hiljada dolara“ od firme Irvin Trast u Njujorku, na račun u banci Vochud Handels u Cirihu u Švajcar-skoj, gde je prethodno već otvorio račun.

Devojka potom reče: „U redu, zabeležila sam. A sad mi treba međukancelarijski identifikacioni broj.“

Rifkina je oblio znoj; bilo je to neočekivano pitanje, nešto što mu je promaklo za vreme priprema. Odglumio je da je sve u najboljem redu, i odmah je hladnokrvno odgovorio: „Sačekajte da proverim; odmah ću vas pozvati.“ Ponovo je promenio identitet i pozvao drugo odeljenje u banci, ovog puta predstavljajući se kao zaposleni u prostoriji za transakcije. Dobio je međukancelarijski identifikacioni broj i odmah pozvao devojku.

Zapisala je broj i zahvalila mu se. (Što je, u tim okolnostima, bilo veoma ironično.)

Privođenje kraju

Nekoliko dana kasnije Rifkin je odleteo u Švajcarsku i podigao gotovinu. Od jedne ruske agencije kupio je gomilu dijamanta za preko 8 miliona dolara. Vratio se avionom, i prošao kroz carinu Sjedinjenih Država s draguljima skrivenim u pojasu za novac. Uspela mu je najveća pljačka banke u istoriji – a počinio ju je bez pištolja, pa čak i bez računara. Začudo, njegova ludorija je na kraju dospela na stranice *Ginisove knjige svetskih rekorda* u kategoriji „najveća računarska prevara“.

Stenli Rifkin je primenio umetnost obmane – veštine i tehnike koje se danas, na engleskom, nazivaju *social engineering*. Detaljno planiranje i nadarenost za ophođenje s ljudima zapravo je sve što mu je bilo potrebno.

Upravo time se bavi ova knjiga – metodama obmane (za koje je pisac ovih redova pravi stručnjak) i načinima odbrane od njih.

PRIRODA PRETNJE

Priča o Rifkinu savršeno objašnjava kako osećaj sigurnosti može biti varljiv. Ovakvi slučajevi – možda ne krađa 10 miliona dolara, ali ipak nepoželjni – dešavaju se *svakodnevno*. Možda upravo sada gubite novac, ili

vam neko krađe planove o novom proizvodu, a da toga niste ni svesni. Ako se to vašem preduzeću još nije dogodilo, ne postavlja se pitanje *da li* će, već *kada* će to biti.

Sve veća zabrinutost

Institut za računarsku bezbednost objavio je u svom izveštaju o računarskom kriminalu iz 2001. godine da je 85% ispitanih organizacija otkrilo narušavanje računarskog bezbednosnog sistema u prethodnih dvanaest meseci. To je zapanjujuća cifra: samo petnaest od svakih sto ispitanih organizacija mogle su da kažu da kod njih nije bilo narušavanja bezbednosnog sistema tokom te godine. Podjednako zapanjujući bio je i broj organizacija koje su prijavile finansijske gubitke usled napada na računarski sistem: 64 procenta. Više od pola ispitanih organizacija podleglo je finansijskim gubicima usled toga. *I to samo u jednoj godini.*

Iz sopstvenog iskustva smatram da su brojke u ovakvim izveštajima pomalo preterane, pošto sumnjam u ispravnost načina anketiranja. Ali to ne znači da šteta nije ogromna – ogromna je. Preduzeća koja ne planiraju odbranu od napada sigurno će pretrpeti štetu.

Komercijalni proizvodi za bezbednost sistema, koji se koriste u većini kompanija, uglavnom štite od uljeza amatera, poput devojaka i mladića koji se nazivaju „skriptasi“. Ti klinici koji bi želeli da postanu hakeri, a koriste softver preuzet s Interneta, uglavnom predstavljaju sitnu smetnju. Veće gubitke nanose i pravu pretnju predstavljaju sofisticirani napadači. Njih motiv više finansijska dobit a mete su im dobro definisane. Oni se usmeravaju na jednu po jednu metu, umesto da, poput amatera, pokušaju da provale u što više sistema. Dok se amateri zadovoljavaju kvantitetom, profesionalci ciljaju na kvalitetne i vredne informacije.

Tehnološke mere poput uvođenja uređaja za identifikaciju, kontrole pristupa (za upravljanje pristupom datotekama i sistemskim resursima), i instaliranja sistema za otkrivanje upada (elektronski ekvivalent alarma koji upozoravaju na provalnike) neophodne su stavke u bezbednosnom sistemu jedne firme. Skoro po pravilu, u današnje vreme jedna kompanija troši više novca na kafu nego na mere zaštite od napada na bezbednosni sistem.

Upravo kao što um kriminalca ne može da odoli iskušenju, um hakera teži da zaobide moćne tehnološke bezbednosne sisteme. U mnogim slučajevima oni to čine usmeravajući se na korisnike tehnologije.

Načini obmane

Kaže se da je bezbedan računar samo onaj koji je isključen. Pametno rečeno, ali ipak netačno: *obmanjivač* nagovori nekoga da uđe u kancelariju i uključi računar. Neprijatelj koji želi određenu informaciju do nje može doći, obično na jedan od nekoliko načina. To je samo pitanje ličnosti, vremena, strpljenja i upornosti. A onda umetnost obmane stupa na scenu.

Da bi zaobišao mere bezbednosti, uljez, odnosno obmanjivač, mora naći načina da prevari lakovernog korisnika kako bi mu ovaj otkrio informacije, ili da na prevaru navede žrtvu, koja ništa ne sumnja, da mu odobri pristup. Kada neko prevari zaposlene, na njih izvrši pritisak, ili ih obmane da otkriju važne informacije ili stvore rupu u bezbednosnom sistemu, nikakva tehnologija ne može zaštititi poslovanje. Stručnjaci ponekad uspeju da dešifruju poruku tako što pronađu propust zahvaljujući kojem mogu da zaobiđu tehnologiju za šifriranje. Upravo tako i obmanjivači pokušavaju da prevare zaposlene da bi zaobišli bezbednosnu tehnologiju.

ZLOUPOTREBA POVERENJA

U većini slučajeva, uspešni obmanjivači umeju dobro da se ophode s ljudima. Šarmantni su, ljubazni i dopadljivi – a upravo su te osobine potrebne da bi se brzo uspostavili prisnost i poverenje. Iskusan napadač može pristupiti gotovo svakoj informaciji pomoću pomenute strategije i taktike.

Savesni stručnjaci za tehnologiju mukotrpno su razvijali bezbednosna rešenja kako bi sveli rizike na najmanju moguću meru, a ipak su ispustili najbitniju tačku podložnu napadima – ljudski faktor. Uprkos intelektu, mi ljudi – vi, ja, i svi ostali – i dalje predstavljamo najveću bezbednosnu pretnju jedni drugima.

Neiskvarenost u okviru organizacije

Prisetite se da je ARPANet (mreža Agencije za napredne istraživačke projekte Sekretarijata odbrane), prethodnik Interneta, projektovan za razmenu informacija između vlade, istraživačkih i obrazovnih institucija. Cilj je bio sloboda informisanja, kao i napredak tehnologije. Mnoge obrazovne institucije su, dakle, instalirale prve računarske sisteme uz malu ili nimalu zaštitu. Čuveni borac za slobodnu upotrebu softvera, Ričard Stolman, čak je odbio da zaštititi lozinkom sopstveni nalog.

No, budući da se Internet koristi za elektronsku trgovinu, opasnosti od slabe zaštite u ovom našem umreženom svetu znatno su se povećale. Ipak, upotrebom tehnologije neće se rešiti problem ljudskog faktora u obezbeđenju.

Pogledajte samo današnje aerodrome. Obezbeđenje je postalo najbitnije, pa ipak nas plaše izveštaji u medijima o putnicima koji su uspeali da zaobiđu mere bezbednosti i prenesu potencijalno oružje pored punktova za proveru. Kako je to moguće u vreme kad su nam aerodromi u takvom stanju pripravnosti? Da li detektori metala ne rade dobro? Ne. Problem nije u mašinama, već u ljudskom faktoru: u ljudima koji njima upravljaju. Aerodromski službenici mogu dovesti Nacionalnu gardu, instalirati detektore metala i sisteme za prepoznavanje lica, ali bi korisnije bilo obučiti obične službenike obezbeđenja da pravilno proveravaju putnike.

Isti problem se javlja u okviru državnih institucija, kompanija i obrazovnih institucija širom sveta. Uprkos naporima stručnjaka za bezbednost, informacije su ipak svugde ranjive, a obmanjivači će ih i dalje smatrati poželjnim metama, sve dok se najslabija karika u lancu obezbeđenja – ljudski činilac – ne ojača.

Sada, više nego ikada ranije, moramo naučiti da raskrstimo s pustim željama i postanemo svesniji metoda zlonamernika, koji pokušavaju da naruše poverljivost, integritet i dostupnost računarskih sistema i mreža. Bili smo primorani da prihvatimo opreznu vožnju; vreme je da prihvatimo i naučimo oprezan rad na računaru.

Pretnja da će neko narušiti vašu privatnost ili informacioni sistem vaše kompanije možda se ne čini stvarnom dok se napad zaista ne dogodi. Da bismo izbegli tako skupo otrežnjenje, moramo svi postati svesniji, obrazovaniji, oprezniji; moramo agresivno štititi vredne poslovne informacije, lične podatke, i najbitniju infrastrukturu. Te mere opreza moramo početi da sprovodimo danas.

TERORISTI I OBMANA

Naravno, prevara nije jedino sredstvo obmanjivača. Fizički terorizam je najveća vest u medijima, te smo shvatili, kao nikada ranije, da je svet opasan. Civilizovanost je, ipak, samo prividan sjaj.

Nedavno pojačani naponi američke vlade podigli su i nivo naše svesti o bezbednosti. Moramo biti u stanju pripravnosti i razumeti kako teroristi podlo menjaju identitet, preuzimaju ulogu studenata i suseda, i stapaju se u

masu. Prikrivaju svoja prava uverenja dok kuju planove protiv nas; tako koriste trikove obmane slične onima o kojima ćete čitati na ovim stranicama.

Koliko ja znam, teroristi još nisu primenili lukavstva obmane kako bi se uvukli u firme, postrojenja za navodnjavanje, elektrane ili druge najbitnije delove naše nacionalne infrastrukture, ali mogućnost postoji. Sasvim je lako. Nadam se da će ova knjiga početi da utiče na podizanje svesti o bezbednosti na viši nivo, te da će rukovodstva kompanija insistirati da se u bezbednosnom sistemu primene opisane procedure.

O OVOJ KNJIZI

Bezbednost preduzeća je pitanje ravnoteže. Usled suviše slabe zaštite, kompanija postaje ranjiva, ali i preterano naglašavanje bezbednosti smeta pri poslovanju – koči rast i prosperitet preduzeća. Izazov je naći ravnotežu između bezbednosti i produktivnosti.

Druge knjige o bezbednosti kompanija usredsređuju se na hardversku i softversku tehnologiju, a ne bave se u odgovarajućoj meri najozbiljnijom pretnjom od svih: obmanjivanjem ljudi. Cilj ove knjige je da objasni kako ste vi, vaši saradnici i ostali zaposleni u vašoj kompaniji predmet manipulacije i da informiše o bedemima koje možete podići da biste prestali da budete žrtva. Knjiga se uglavnom usredsređuje na ne-tehničke metode koje uljezi koriste da bi ukrali informacije, ugrozili celovitost podataka za koje se veruje da su bezbedni, ili uništili neki proizvod kompanije.

Moj zadatak otežava jednostavna istina: svakog čitaoca su već prevarili najveći stručnjaci svih vremena iz oblasti obmane – njegovi roditelji. Našli su načina da vas privole, „za sopstveno dobro“, da činite ono što su oni smatrali najboljim. Roditelji, odlični manipulatori, postupaju kao profesionalni obmanjivači koji izmišljaju vrlo uverljive priče, razloge i opravdanja za dostizanje sopstvenih ciljeva. Da, nas su oblikovali roditelji, koji nas dobronamerno (a ponekad i ne tako dobronamerno) obmanjuju.

Budući da smo vaspitavani uz obmane, postali smo podložni manipulaciji. Živeli bismo drugačije da smo stalno morali da budemo na oprezu, nepoverljivi prema drugima i zabrinuti da bismo mogli postati naivna meta nekoga ko pokušava da nas iskoristi. U savršenom svetu podrazumevalo bi se da verujemo drugima, uvereni da su ljudi koje srećemo iskreni i da im se može verovati. Ali ne živimo u savršenom svetu, pa moramo da uvećavamo određene mere opreza kako bismo sprečili pokušaje neprijatelja da nas prevare.

Glavne delove ove knjige, drugi i treći, sačinjavaju priče o obmani na delu. U tim delovima biće reči o sledećem:

- O onome što su telefonski prevaranti otkrili pre više godina: kako od telefonske kompanije dobiti broj koji ne postoji u imeniku.
- O nekoliko različitih metoda koje napadači primenjuju da bi naveli čak i oprezne, sumnjičave službenike da im obelodane svoja korisnička imena i lozinke.
- O tome kako je jedan upravnik računarskog centra sarađivao s napadačem i omogućio mu da ukrade informacije o najpoverljivijem proizvodu njegovog preduzeća.
- O postupcima kojima je službenica navedena da učita softver koji špijunira svaki njen pritisak na taster i elektronskom poštom šalje izveštaje napadaču.
- O tome kako privatni istražitelji dolaze do informacija o preduzećima i pojedincima, od čega ćete se, u to budite uvereni, naježiti.

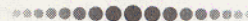
Dok budete čitali neke od priča u drugom i trećem delu, možda ćete pomisliti da nisu moguće, da niko ne može tako lagati, koristiti se prljavim trikovima i spletkama. Suština je da se opisani događaji mogu odigrati i zaista se dešavaju; mnogi od njih se svakodnevno zbivaju negde u svetu, a možda čak i u vašem preduzeću dok čitate ovu knjigu.

Ova knjiga će vam zaista otvoriti oči kad je u pitanju zaštita poslovanja. Naučiće vas da se branite od obmane na ličnom planu, da biste zaštitili integritet informacija u privatnom životu.

U četvrtom delu knjige preći ćemo na praktične teme. Moj cilj je da vam pomognem da napravite neophodne poslovne pravilnike i podignete nivo svesti službenika, kako biste na najmanju moguću meru sveli mogućnost da vaš zaposleni bude obmanut. Razumevanje strategija, metoda i taktike obmane pripremiće vas da upotrebite razumna sredstva za zaštitu informacija, ne dovodeći u pitanje produktivnost kompanije.

Ukratko, napisao sam ovu knjigu da bih podigao nivo svesti o ozbiljnoj pretnji koju obmanjivanje predstavlja, kako biste mogli da obezbedite firmu i zaposlene i budete sigurni da vas niko ne može obmanuti.

Ili bi možda trebalo da kažem da je mnogo manje verovatno da će vas ikada ponovo obmanuti.



deo

2

Umeće napadača

poglavlje

2

Kada bezazlena informacija nije tako bezazlena

Šta većina ljudi smatra pravom pretnjom obmane? Šta bi valjalo učiniti da biste bili na oprezu?

Ako je cilj napadača da se domogne nečeg veoma vrednog – recimo, izuzetno važne komponente intelektualnog vlasništva kompanije – onda je možda, figurativno govoreći, potreban samo čvršći sef i jače naoružano obezbeđenje. Je li tako?

Narušavanje bezbednosnog sistema preduzeća, zapravo, obično započinje tako što se „negativac“ domogne neke informacije ili dokumenta koji se čine toliko bezazlenim, svakodnevnim i nevažnim, da mnogi zaposleni u organizaciji ne vide zašto bi bili zaštićeni i poverljivi.

SKRIVENA VREDNOST INFORMACIJA

Obmanjivač smatra većinu naoko bezazlenih informacija vrednim, jer mogu igrati odlučujuću ulogu u njegovim pokušajima da se zaodene velom uverljivosti.

Na stranicama koje slede, pokazaću vam tehnike obmane tako što ću vam omogućiti da i sami „prisustvujete“ napadima. Ponekad ću prikazivati

događaje iz ugla žrtve, pa ćete moći da se poistovetite s njom i ocenite kako biste vi (ili možda neko od saradnika ili zaposlenih) reagovali u datoj situaciji. Većinu tih događaja posmatraćete i iz ugla napadača.

U prvoj priči reč je o ranjivosti finansijskog poslovanja.

CREDITCHEX

Britanci su dugo imali veoma krut bankarski sistem. Kao običan, pošten građanin niste mogli da uđete u banku i otvorite račun. Ne, banka bi razmotrila vaš zahtev tek kad bi vam njihov pouzdan klijent dao preporuku.

Sasvim je različito, naravno, prividno otvoreno savremeno bankarstvo. Lakoća s kojom se u današnje moderno vreme posluje, najbolje se očituje u prijateljskoj, demokratskoj Americi, gde gotovo svako može ući u banku i lako otvoriti tekući račun, je li tako? Pa, ne baš. Banke nerado otvaraju račune onima koji su možda ranije ispisivali čekove bez pokrića, što je i razumljivo – u banci je ček bez pokrića isto toliko dobrodošao kao i prijava zbog pljačke banke ili optužba za proneveru. Stoga je u svakoj banci standardna procedura da se brzo proverí novi klijent.

Jedna od glavnih kompanija koju banke unajmljuju radi ovakvih informacija jeste CreditChex. Oni svojim klijentima obezbeđuju dragocene usluge, ali poput mnogih preduzeća, mogu nesvesno pružiti zgodne usluge i obmanjivačima, koji znaju kako do njih da dođu.

Prvi poziv: Kim Endrjuz

„Nacionalna banka, Kim je kraj telefona. Da li biste želeli da otvorite račun?“

„Zdravo, Kim. Hteo bih nešto da vas pitam. Da li vi koristite usluge firme CreditChex?“

„Da.“

„Kad im telefonirate, kako zovete broj koji im saopštite – je li to 'Identifikacioni broj filijale'?“

Usledila je stanka; razmatrala je zahtev, pitajući se o čemu se radi i da li treba da odgovori.

Sagovornik je brzo nastavio, ne trepnuvši.

„Vidite, Kim, ja pišem knjigu o privatnim istražiteljima.“

„Da“, reče, odgovarajući na pitanje s novostečenom sigurnošću, zadovoljna što pomaže piscu.

„Dakle, to se zove identifikacioni broj filijale, je li tako?“

„A-ha.“

„Dobro, sjajno. Hteo sam da budem siguran da je to pravi izraz. Za knjigu. Hvala vam na pomoći. Do viđenja, Kim.“

Drugi poziv: Kris Talbert

„Nacionalna banka, odsek za nove račune, Kris je kraj telefona.“

„Zdravo, Kris. Ovde Aleks“, reče glas iz slušalice. „Ja sam iz odeljenja za korisničke usluge firme CreditChex. Sprovođimo anketu da bismo poboljšali uslugu. Možete li da mi posvetite nekoliko minuta?“

Pristala je, pa je nastavio.

„U koje vreme je vaš ogranak otvoren za klijente?“ Odgovorila je, i nastavila da odgovara na niz njegovih pitanja.

„Koliko zaposlenih u vašem ogranku koristi naše usluge?“

„Koliko često nam upućujete zahteve?“

„Koje od naših besplatnih brojeva smo vam dodelili?“

„Jesu li naši službenici uvek ljubazni?“

„Koliko brzo reagujemo na vaše zahteve?“

„Koliko dugo radite u ovoj banci?“

„Koji identifikacioni broj filijale trenutno koristite?“

„Da li ste ikada naišli na nedoslednosti u informacijama koje smo vam obezbedili?“

„Kako biste unapredili našu uslugu?“

„Da li biste popunili upitnike koje bismo poslali vašem ogranku?“

Ona se s tim složila, još malo su pročaskali, potom je on spustio slušalicu, a Kris se vratila svom poslu.

Treći poziv: Henri Mekinsi

„CreditChex, ovde Henri Mekinsi. Šta mogu da učinim za vas?“

Osoba s druge strane žice predstavila se kao službenik Nacionalne banke. Dao mu je odgovarajući identifikacioni broj filijale, a potom ime i broj socijalnog osiguranja osobe o kojoj su mu trebali podaci. Henri je pitao za datum rođenja, a on mu je i to rekao.

Nakon nekoliko trenutaka, Henri je pročitao podatke koji su mu se pojavili na ekranu.

„Vels Fargo, ispisao je čekove bez pokrića 1998. godine, jednom, na sumu od 2066 dolara.“ Ček bez pokrića je poznat bankarski izraz za čekove koji su upotrebljeni kad na računu nema dovoljno novca da ispisani iznos pokrije.

„Da li je kasnije bilo nečeg sličnog?“

„Ne.“

„Je li bilo drugih provera?“

„Da vidimo. Da, dvaput, i to oba puta prošlog meseca. Zahteve su uputili Third United Credit Union iz Čikaga i Schenectady Mutual Investments.“ Spetljao se pri potonjem nazivu, pa je morao da izgovori slovo po slovo. „Ovi drugi su iz države Njujork“, dodao je.

Kako radi privatni istražitelj

Sva tri puta poziv je uputila ista osoba: privatni istražitelj kojeg ćemo zvati Oskar Grejs. Grejs je imao novog klijenta. S obzirom na to da je do pre nekoliko meseci bio policajac, ustanovio je da mu ovaj novi posao leži, ali morao je više da se potruži i bude inventivniji. Posao je bio baš izazovan.

Detektivi iz priča – Sem Spejd, Filip Marlo i njima slični – provodili su duge noćne sate u kolima, čekajući da uhvate nevernog supružnika na delu. I pravi detektivi rade tako. No, oni istražuju za „zaraćene“ supružnike i na drugi način, o kojem se manje piše, a isto toliko je važan. Ta metoda se više oslanja na veštinu obmane nego na ubijanje dosade pri noćnom bdenju.

Oskarov klijent bila je dama koja je, činilo se, imala sasvim pristojan budžet za odeću i nakit. Jednog dana je ušetala u njegovu kancelariju i sela na kožnu stolicu, jedinu na kojoj nisu bili naslagani papiri. Smestila je svoju

veliku tašnu marke Guči na njegov radni sto s logotipom okrenutim prema njemu, i izjavila da planira da traži razvod od muža, ali je priznala da postoji „jedan mali problem“.

Činilo se da je njen muž bio korak ispred. Već je podigao gotovinu s njihove štedne knjižice, i još veću sumu s bankovnog računa. Htela je da zna gde je skrivena njihova imovina, a njen advokat za razvod uopšte joj nije bio od pomoći. Grejs je pretpostavljao da je advokat jedan od onih uspešnih savetnika iz bolje gradske četvrti, te da neće da prlja ruke u potrazi za novcem.

Da li Grejs može da pomogne?

Uverio ju je da nema nikakvih problema, rekao joj cenu, saopštio da će troškovi biti naplaćeni posebno i uzeo ček s prvim delom iznosa.

Tek potom se suočio s problemom. Šta učiniti ako se nikad ranije niste srela sa sličnim problemom i zapravo ne znate odakle da počnete da biste utvrdili kuda je novac nestao? Krenete korak po korak. Evo Grejsove priče, onako kako nam je ispričao naš izvor.



Znao sam za CreditChex i način na koji banke koriste tu organizaciju – moja bivša žena je nekad radila u banci. Ali nisam znao terminologiju i procedure, a da sam pitao svoju bivšu ženu, samo bih izgubio vreme.

Prvi korak: naučite pravilno terminologiju. Kad tražite informacije, trudite se da zvučite kao da znate o čemu pričate. U prvoj banci koju sam nazvao, prva gospodica, Kim, bila je podozriva kad sam je upitao kako se identifikuju kad pozovu CreditChex. Oklevala je; nije znala da li da mi kaže ili ne. Da li je to osujetilo moje namere? Nimalo. Zapravo, njeno oklevanje bilo je za mene važan signal da treba da pružim verodostojno obrazloženje. Kad sam joj rekao da istražujem za knjigu, prestala je da bude sumnjičava. Samo kažete da ste pisac ili scenarista, i svi vam jedu iz ruke.

Imala je ona i druge informacije koje bi mi bile korisne – poput podataka koje CreditChex zahteva radi identifikacije osobe koju proveravate, šta smete da ih pitate, i najvažnije, koji je identifikacioni broj njene filijale. Tako sam hteo da je ispitam, kad me je njeno oklevanje upozorilo da ne srljam. Poverovala je u priču o istraživanju za knjigu, ali je prethodno bila dosta sumnjičava. Da je od samog početka bila otvorenija, zatražio bih od nje još detalja o bankarskim procedurama.

Morate se voditi instinktom, i slušati pažljivo šta „žrtva“ govori i kako to izgovara. Ova mi je dama zvučala dovoljno pametno – verovatno bi se oglašio alarm da sam nastavio da joj postavljam suviše neobičnih pitanja. Iako nije znala ko sam, niti s kog broja zovem, u ovom poslu nikako ne želite da se pročuje da neko zove kako bi dobio informacije o poslovanju pa treba biti na oprezu. Razlog je što ne želite da vam se izvor ugasi – možda ćete ponovo morati da pozovete istu kancelariju neki drugi put.

terminologija

ŽRTVA Reč je o prevarenoj osobi.

UGASITI IZVOR (engl. burn the source) Kaže se da je napadač ugasio izvor kad dozvoli da žrtva prepozna da je reč o napadu. Kad žrtva postane svesna napada i o tome obavesti ostale zaposlene i rukovodstvo, izuzetno je teško ponovo upotrebiti isti izvor u budućim napadima.

Uvek obraćam pažnju na male signale. Pomoću njih procenjujem koliko je osoba spremna za saradnju, u opsegu od: „Zvučiš kao prijatna osoba i sve ti verujem“ do: „Zovite policiju, obavestite Nacionalnu gardu, ovaj nešto gadno smerā“.

Ocenio sam da je Kim pomalo napeta, pa sam zato pozvao nekoga iz drugog ogranka. Tokom drugog razgovora, s Kris, trik s anketom upalio je iz prve. Ovde je taktika da se važna pitanja ubace između nebitnih koja stvaraju osećaj uverljivosti. Pre nego što sam je pitao o identifikacionom broju njihove filijale kod firme CreditChex, testirao sam je u poslednjem trenutku postavivši joj pitanje lične prirode o tome koliko dugo radi u banci.

Pitanje lične prirode je poput nagazne mine – neki ga prekorače ništa ne primetivši, dok drugima eksplodira pa se brzo povuku na sigurno. Dakle, ako joj postavim takvo pitanje i ona odgovori, a ne promeni ton, to znači da verovatno nije sumnjičava. Slobodno mogu da postavim ključno pitanje. Neće posumnjati i najverovatnije će odgovoriti.

Evo još nečega što dobar privatni istražitelj zna: nikada ne prekidajte razgovor nakon što se domognete ključne informacije. Postavite još dva-tri pitanja, malo proćaskajte, i tek onda možete prekinuti. Kasnije će se žrtva verovatno setiti nekoliko poslednjih pitanja – ako se ičega seti. Ostalo se uglavnom zaboravlja.

I tako mi je Kris dala identifikacioni broj njihove filijale, kao i telefonski broj koji zovu kad proveravaju potencijalne klijente. Bio bih srećniji da sam uspeo da je pitam koliko podataka se može tražiti od firme CreditChex, ali sam smatrao da je bolje da ne preterujem.

Bilo je to kao da imam neispunjen ček kod firme CreditChex. Mogao sam ih nazvati i dobiti informacije kad god sam želeo. Nisam čak ni morao da platim za tu uslugu. Kako se ispostavilo, službenik kompanije CreditChex rado mi je dao upravo one podatke koje sam tražio: dve banke kod kojih je muž moje klijentinje nedavno predao molbu da mu se otvori račun. Pa, gde je bio novac koji traži njegova žena, koja će mu uskoro postati bivša? Gde drugde nego u bankama koje je momak iz kompanije CreditChex naveo.

Analiza prevare

Čitava ova prevara zasnovana je na jednoj od osnovnih taktika obmanjivanja: na pristupu informacijama koje zaposleni pogrešno smatraju bezazlenima.

Prva službenica je potvrdila termin za broj koji se koristi kad se zove CreditChex: identifikacioni broj filijale. Druga je obelodanila telefonski broj na koji se zove CreditChex, kao i najbitniju informaciju, identifikacioni broj te banke. Činilo se da su joj svi ti podaci potpuno bezazleni. Na kraju krajeva, ona je mislila da razgovara s nekim iz kompanije CreditChex, pa šta škodi ako im se kaže broj?

Sve ovo je bilo samo priprema za treći poziv. Grejs je imao sve što mu treba da bi telefonirao firmi CreditChex, predstavio se kao službenik jedne od banaka s kojom sarađuju, Nacionalne banke, i zatražio željene informacije.

Grejs je bio vešt u krađi informacija poput nekog prevaranta koji lako izmami novac, a imao je i pravog talenta da oceni ljude. Znao je da ključna pitanja valja smestiti između nebitnih. Znao je da će pitanjem lične prirode utvrditi koliko je druga službenica spremna za saradnju, pre nego što ju je „nevino“ upitao za identifikacioni broj filijale.

Da prva službenica nije potvrdila izraz za broj koji se koristi pri proveru kod firme CreditChex, bilo bi gotovo nemoguće nastaviti. Taj podatak je toliko rasprostranjen u bankarstvu, da se čini nevažnim – što je upravo klasičan primer naoko bezazlene informacije. Ali druga službenica, Kris, nije trebalo tako olako da odgovara na pitanja, a da prethodno ne proveru

da li je sagovornik onaj za koga se izdaje. Trebalo je, u najmanju ruku, da zapiše njegovo ime i telefonski broj i da ga ona pozove. Ako bi se kasnije pojavio problem, mogla je imati podatak o tome s kog je telefona osoba zvala. U tom slučaju bi napadaču bilo mnogo teže da se lažno predstavi kao službenik firme CreditChex.

mitnikova poruka

Identifikacioni broj filijale je u ovom slučaju isto što i lozinka. Kad bi se osoblje banke prema njemu odnosilo kao prema PIN kodu za bankomate, možda bi shvatili koliko je takva informacija poverljiva. Da li i u vašoj organizaciji postoji interni kôd ili broj kojem osoblje ne pridaje dovoljno značaja?

Još bolje bi bilo da je službenica pozvala CreditChex koristeći broj kojim se banka inače služi – a ne broj koji bi joj sagovornik eventualno dao – kako bi se uverila da on zaista radi u pomenutoj kompaniji, i da oni uistinu sprovode anketu među svojim klijentima. Međutim, kada se uzme u obzir da se danas, u realnom svetu, radi toliko da niko nema viška vremena, previše bi bilo očekivati poziv radi provere, osim u slučaju da zaposleni posumnja da je u pitanju napad.

ZAMKA ZA INŽENJERE

Svi znaju da agencije za zapošljavanje koriste metode obmanjivanja kako bi vrbovali talentovane kandidate. Evo primera kako se to radi.

Krajem devedesetih, jedna agencija za zapošljavanje, koja baš i ne drži do etike, potpisala je ugovor s novim klijentom, kompanijom koja traži inženjere elektrotehnike s iskustvom u telekomunikacijama. Vođa projekta bila je dama obdarena dubokim, seksi glasom koji je naučila da iskoristi da bi brzo uspostavila poverenje i prisnost preko telefona.

Odlučila je da izvrši pohod na davaoca usluga mobilne telefonije, da vidi može li tamo naći neke inženjere koji bi se našli u iskušenju da pređu na drugu stranu, kod konkurencije. Naravno, nije mogla da pozove centralu i kaže: „Spojite me sa svakim ko ima pet godina inženjerskog iskustva“. Umesto toga, iz razloga koji će uskoro postati jasni, započela je potragu za talentovanim osobljem tako što je zatražila jedan podatak koji naizgled nije uopšte bitan, i koji službenici te kompanije daju gotovo svakom ko ga zatraži.

Prvi poziv: prijemno odeljenje

Napadač, predstavljajući se kao Didi Sends, poziva upravu kompanije za telekomunikacione usluge. Evo kako je razgovor tekao.

Službenica prijemnog odeljenja: Dobar dan. Ovde Meri, šta mogu da učinim za vas?

Didi: Možete li me spojiti s odeljenjem za transport?

S: Nisam sigurna da li tako nešto kod nas postoji. Pogledaću u imeniku. Ko zove?

D: Didi.

S: Jeste li u zgradi, ili...?

D: Ne, van zgrade sam.

S: Kako se prezivate?

D: Sends. Didi Sends. Imala sam lokal transportnog odeljenja, ali sam ga zaboravila.

S: Trenutak.

Da bi odagnala sumnju, Didi je nonšalantno, radi same konverzacije, postavila pitanje osmišljeno tako da sagovornika uveri da je ona „domaća“, da poznaje firmu.

D: U kojoj se vi zgradi nalazite – u Lejkjuu ili u centrali?

S: U centrali. (*stanka*) Broj je 805 555 6469.

Da bi obezbedila rezervu u slučaju da putem poziva transportnom odeljenju ne dobije ono što joj treba, Didi je takođe zatražila da razgovara s odeljenjem za nekretnine. Službenica joj je dala i taj broj. Kad je Didi zamolila da je spoji s transportnim odeljenjem, ova je to pokušala, ali je veza bila zauzeta.

Tada je Didi zamolila da joj da *treći* telefonski broj, broj odeljenja za platni promet, smešten u prostorijama firme u Ostinu u Teksasu. Službenica ju je zamolila da malo sačeka i za trenutak spustila slušalicu. Da li je javila obezbeđenju da ima sumnjiv telefonski poziv i da misli da je u pitanju prevara? Ni slučajno. A ni Didi se nije nimalo brinula. Bila je malo dosadna, ali je to službenici bio deo običnog radnog dana. Prošao je otprilike minut, a potom je službenica ponovo uzela vezu, pogledala broj odeljenja za platni promet, pokušala da dobije vezu i spojila Didi s njima.

Drugi poziv: Pegi

Sledeći poziv je tekao ovako:

Pegi: Odeljenje za platni promet, ovde Pegi.

Didi: Zdravo, Pegi. Ovde Didi iz Tauzend Ouksa.

P: Zdravo, Didi.

D: Kako si?

P: Dobro.

Didi je potom upotrebila poznat izraz za kôd kojim se troškovi dodeljuju budžetu određene organizacije ili radne grupe:

D: Odlično. Kaži mi kako da dođem do konta za neko odeljenje.

P: Moraš se obratiti analitičaru budžeta tog odeljenja.

D: Znaš li ko analizira budžet za Tauzend Ouks – za upravu? Pokušavam da ispunim neki obrazac, a ne znam odgovarajući konto.

P: Ja samo znam da onaj kome treba konto zove svog analitičara budžeta.

D: Imaš li ti konto svog odseka tu u Teksasu?

P: Mi imamo svoj konto, ali nam ne daju čitav spisak.

D: Koliko cifara ima? Na primer, koji je vaš konto?

P: Čekaj, jesi li ti u okviru 9WC ili SAT?

Didi nije imala pojma na koje se odseke ili odeljenja te skraćnice odnose, ali nije bilo ni važno. Odgovorila je:

D: 9WC.

P: Onda obično ima četiri cifre. Gde reče da radiš?

D: U upravi – u Tauzend Ouksu.

P: Da, evo konta za Tauzend Ouks. 1A5N, N kao Nensi.

Zahvaljujući tome što je provela dovoljno dugo vremena s nekim ko je spreman da pomogne, Didi je dobila konto koji joj je bio potreban. A to je jedan od onih podataka koje niko i ne pomisli da zaštititi, jer se čini kao nešto što ljudima van firme ne može biti ni najmanje važno.

Treći poziv: koristan pogrešan broj

Sledeći Didin zadatak bio je da pretvori dobijeni konto u nešto zaista vredno, poput žetona za poker.

Otpočela je nazvavši odeljenje za nekretnine, pretvarajući se da je dobila pogrešan broj. Prvo je rekla: „Izvinite što smetam, ali...“, a potom izdeklamovala da je koleginica koja je izgubila telefonski imenik kompanije i pitala koga treba da zove da bi dobila nov. Muški glas je odgovorio da je štampana verzija zastarela, jer se imenik može naći na intranetu.

Didi odvrati da više voli da koristi štampanu verziju, a on joj na to reče da pozove Izdavaštvo. Potom je ljubazno potražio njihov broj i dao joj ga, a da ga ona to nije ni zamolila – možda samo da bi malo duže razgovarao s damom takvog glasa.

Četvrti poziv: Bart u Izdavaštvu

Nazvavši Izdavaštvo, razgovarala je s čovekom po imenu Bart. Rekla je da radi u Tauzend Ouksu i da imaju novog savetnika kojem treba štampana kopija telefonskog imenika kompanije. Rekla je da savetniku tako više odgovara, bez obzira na to što je štampana verzija unekoliko zastarela. Bart joj reče da mora da ispuni obrazac za trebovanje i pošalje ga njemu.

Didi odvrati da joj je nestalo obrazaca i da je u gužvi, i zamolila ga da bude tako dobar i ispuni ga umesto nje. Pristao je, nekako isuviše oduševljeno, a potom mu je Didi izdiktirala pojedine podatke. Što se tiče adrese izmišljenog savetnika, otegnuto je izdiktirala nešto što se u svetu obmane naziva lažna adresa. U ovom slučaju, navela je adresu firme Mail Boxes Etc., kod koje je njena kompanija iznajmljivala poštanske sandučice upravo za ovakve prilike.

Prethodni trud se sada isplatio. „Slanje imenika se naplaćuje.“ U redu – Didi mu je dala konto za Tauzend Ouks:

„1A5N, N kao Nensi.“

Nakon nekoliko dana, kad je telefonski imenik kompanije stigao, Didi je shvatila da joj se trud još više isplatio nego što je očekivala – u njemu se nisu nalazili samo puki spiskovi imena i telefonskih brojeva, već je bilo prikazano i ko za koga radi, dakle poslovna struktura čitave organizacije.

Dama promuklog glasa bila je spremna da telefonom vrbuje kadar. Na prevaru je došla do informacija neophodnih da bi otpočela s napadom, i to sve zahvaljujući svom talentu za ophođenje s ljudima, koji svaki obmanjivač mora da dovede do perfekcije. Sad je mogla da ubere plodove svog rada.

Analiza prevare

Ovu obmanu Didi je počela tako što je nabavila brojeve tri odeljenja u ciljnoj kompaniji. To je bilo lako, jer brojevi koje je tražila nisu tajna, a pogotovo zaposlenima. Obmanjivač nauči da zvuči kao „domaći“, a Didi je bila spretna u toj igri. Pomoću jednog od tih telefonskih brojeva došla je do kontnog broja, koji je potom upotrebila kako bi se domogla primerka firminog telefonskog imenika zaposlenih.

Bilo je potrebno: da zvuči prijateljski, da koristi određene poslovne izraze, i, kod poslednje „žrtve“, da ubaci malo verbalnog koketiranja.

Neophodno joj je bilo još nešto što se ne stiče lako – veština manipulacije, dovedena do visokog nivoa kroz dugu praksu, kao i samouverenost.

terminologija

LAŽNA ADRESA (engl. *mail drop*) U obmanjivanju, to je izraz za privremeni poštanski fah, uglavnom pod lažnim imenom, koji služi da u njega stižu dokumenta ili paketi koje „žrtve“ na prevaru pošalju.

mitnikova poruka

Baš kao i delići slagalice, svaka informacija ponaosob može biti nebitna. Međutim, kad se delovi slagalice spoje, dobija se jasna slika. U ovom slučaju, slika koju je manipulator video bila je čitava interna struktura kompanije.

JOŠ NEKE „BEZVREDNE“ INFORMACIJE

Osim kontnog broja i internih telefonskih lokala, koje još naizgled bezvredne informacije mogu biti izuzetno važne vašem neprijatelju?

Telefonski poziv za Pitera Ejblsa

„Zdravo“, kaže glas s druge strane žice. „Ovde Tom iz kompanije Parkharst Trevl. Vaše karte za San Francisco su spremne. Hoćete li da vam ih dostavimo, ili ćete sami doći po njih?“

„Za San Francisco?“ pita Piter. „Ja ne putujem u San Francisco.“

„Da li je to Piter Ejbls?“

„Da, ali ja ne planiram da putujem.“

„E pa“, kaže sagovornik prijazno se nasmejavši, „jeste li sigurni da ne želite da odete u San Francisco?“

„Ako mislite da možete nagovoriti mog šefa...“ odvrća Piter, nastavljajući ovaj prijateljski razgovor.

„Ovo je izgleda zabuna“, kaže sagovornik. „U našem sistemu rezervišemo putovanja pod brojem zaposlenih. Možda je neko dao pogrešan broj. Koji je vaš broj?“

Piter mu poslušno izdeklamuje broj. A zašto da ne? Taj broj se upisuje na gotovo svaki kadrovski obrazac, i mnogi iz kompanije mu imaju pristup – kadrovsko odeljenje, obračunsko odeljenje i, očigledno, ova turistička agencija. Niko ne smatra broj zaposlenog tajnom. Kakve ima veze?

Nije teško proniknuti u odgovor. Možda su za efektno prerušavanje, odnosno napadačevo preuzimanje tuđeg identiteta, potrebna samo dva-tri podatka. Ako se domogne imena službenika, njegovog telefonskog broja, broja zaposlenog i, bilo bi dobro, imena i telefonskog broja njegovog nadređenog, čak i manje uspešan obmanjivač imaće gotovo sve što mu je obično potrebno da zvuči uverljivo sledećoj žrtvi koju pozove.

Da je neko ko se predstavio da radi u drugom odeljenju vaše firme juče nazvao, dao vam neki verodostojan razlog i zatražio vaš broj zaposlenog, da li biste mu ga nerado dali?

Uzgred budi rečeno, koji je vaš matični broj?

mitnikova poruka

Pouka priče je ta da ne treba obelodanjivati lične podatke niti interne kompanijske informacije ili šifre nikome, ukoliko glas sagovornika ne zvuči poznato ili niste sigurni da li ima pravo da ih zatraži.

SPREČAVANJE PREVARE

Kompanija mora objasniti zaposlenima da može doći do ozbiljnih posledica ako se s informacijama, koje nisu javne prirode, ne postupa na pravi način. Dobro osmišljena politika zaštite informacija, zajedno sa odgovarajućim obrazovanjem i uvežbavanjem, naglo će podići na viši nivo svest zaposlenih o tome kako se valja odnositi prema poslovnim informacijama u okviru kompanije. Klasifikacija podataka pomoći će vam da primenite odgovarajuća pravila kad je u pitanju njihovo obelodanjivanje. Ako takva klasifikacija ne postoji, svi interni podaci moraju se smatrati poverljivima, ukoliko nije drugačije određeno.

Preduzmite sledeće korake da biste zaštitili svoju kompaniju od odavanja naizgled bezazlenih informacija:

- Odeljenje za bezbednost informacija treba da sprovede obuku s ciljem da do pojedinosti razjasne metode obmanjivanja. Jedna od metoda, kao što smo ranije opisali, jeste da se dođe do naizgled beznačajnog podatka, te da se on kasnije upotrebi kao žeton za poker kako bi se uspostavilo kratkotrajno poverenje. Svaki zaposleni mora znati da poznavanje kompanijske procedure, terminologije i internih kodova, ni u kom slučaju nije dovoljno za identifikaciju sagovornika, niti mu daje pravo da zahteva podatke. Sagovornik može biti i bivši zaposleni ili radnik po ugovoru koji ima potrebne interne informacije. Shodno tome, svaka firma mora da utvrdi odgovarajuće metode identifikacije koje se primenjuju kad zaposleni stupe u kontakt s ljudima koje lično ne poznaju ili s njima razgovaraju telefonom.
- Osoba ili osobe koje imaju ulogu i odgovornost da osmisle klasifikaciju podataka treba da razmotre tipove pojedinosti koje se mogu upotrebiti da bi se došlo do poverljivih informacija, a koje se zaposlenima

čine bezazlene. Iako nikada ne biste otkrili šifru kreditne kartice, da li biste ikome rekli koji server koristite za razvoj kompanijskog softvera? Da li bi tu informaciju mogao upotrebiti prevarant koji se izdaje za osobu kojoj je odobren pristup kompanijskoj mreži?

- Zahvaljujući pukom poznavanju interne terminologije, ponekad napadač ostavlja utisak autoritativne osobe koja se razume u posao. Zahvaljujući uvreženom poverenju u siguran nastup, prevarant često svojim nastupom nagovori „žrtvu“ da s njim sarađuje. Na primer, identifikacioni broj filijale je izraz koji osoblje u odeljenju za nove račune banke nonšalantno koristi svakog dana. Ali takav identifikator je potpuno isto što i lozinka. Kad bi svaki zaposleni shvatio njegov značaj – to da se koristi kako bi se podnosilac molbe identifikovao – možda bi se prema njemu odnosili s više poštovanja.
- Nijedna kompanija, ili bar veoma malo njih, ne daje direktne telefonske brojeve svojih generalnih direktora ili članova upravnog odbora. Ipak, u najvećem broju kompanija se i ne razmišlja o davanju telefonskih brojeva većine odeljenja i radnih grupa u okviru organizacije – a pogotovo nekome ko je zaposlen ili se tako predstavlja. Moguća protivmera bila bi da se uvede zabrana davanja internih telefonskih brojeva zaposlenih, radnika po ugovoru, savetnika i probnih radnika bilo kome van firme. Što je još važnije, valja osmisliti proceduru koja se sastoji iz više koraka, a kojom bi se tačno mogao utvrditi identitet sagovornika koji traži telefonske brojeve.

mitnikova poruka

Kako kaže stara izreka – čak i pravi paranoici verovatno imaju neprijatelje. Pretpostavićemo da i svaka firma ima svoje neprijatelje – napadače koji ciljaju na mrežnu infrastrukturu da bi ugrozili poslovne tajne. Ne dozvolite da i vi završite kao statistički podatak o računarskom kriminalu. Krajnje je vreme da podignete neophodne bedeme tako što ćete primeniti odgovarajuće, dobro osmišljene bezbednosne pravilnike i procedure.

- Brojevi računa radnih grupa i odeljenja, kao i primerci telefonskih imenika kompanija (u štampanoj verziji, u vidu datoteke ili kao elektronski imenik na intranetu) česta su meta prevaranata. Neophodno

je da svaka kompanija ima pisani i distribuirani pravilnik o obelodanjivanju informacija te vrste. U zaštitne mere treba uvrstiti i vođenje dnevnika u koji bi se zapisivalo odavanje poverljivih informacija ljudima van firme.

- Podaci poput broja zaposlenog ne treba da se samostalno koriste za identifikaciju. Svakog zaposlenog treba obučiti da utvrdi i identitet onoga ko informaciju traži i zašto je traži.
- U okviru obuke o zaštiti informacija, razmislite o tome da naučite zaposlene sledećem: kad god im nepoznata osoba postavi pitanje ili ih zamoli za uslugu, prvo treba ljubazno da je odbiju dok se zahtev ne odobri. A potom – pre nego što popuste pred prirodnim nagonom da budu predusretljivi – neka prate kompanijski pravilnik i procedure u vezi sa odobravanjem i objavljivanjem informacija koje nisu javne prirode. To može biti malo protivno našem prirodnom nagonu da pomognemo drugima, ali je možda neophodna mala doza zdrave paranoje da biste izbegli da baš vi upadnete u obmanjivačevu zamku.

Kao što smo u pričama iz ovog poglavlja videli, naizgled bezazlene informacije mogu biti ključ do najčuvanijih tajni vaše kompanije.



poglavlje

3

Direktan napad: samo tražite ono što vam treba

mnoge obmane su složene: sadrže brojne korake i zahtevaju pažljivo planiranje, te kombinovanje manipulacije i tehnološkog znanja. Ipak, prosto je neverovatno šta se sve može postići direktnim napadom. Kao što ćete videti, ponekad je dovoljno da samo zatražite prave informacije.

MCDL NA BRZAKA

Želite li da saznate telefonski broj nekoga koga nema u imeniku? Obmanjivač bi vam mogao navesti nekoliko načina (a neki od njih će biti opisani u drugim pričama u ovoj knjizi), ali je verovatno najjednostavniji scenario onaj za koji je potreban samo jedan telefonski poziv, kao u ovom slučaju.

Molim vas, dajte mi broj

Napadač je okrenuo broj privatne telefonske kompanije MCDL, Mehanizovanog centra za dodelu linija. Ženi koja se javila rekao je:

„Zdravo, ovde Pol Entoni. Ja razvodim kablove. Čujte, razvodna kutija je izgorela u požaru. Policija misli da je neki ludak pokušao da spali

sopstvenu kuću zbog novca od osiguranja. Poslali su me ovde samog da pokušam da dovedem u red čitav ovaj razvodnik s dvesta parica. Stvarno mi je potrebna pomoć. Šta bi trebalo da bude uključeno na adresi Saut Mejn 6723?“

U drugim delovima telefonske kompanije, osoba koja odgovori na poziv znala bi da se informacije o neobjavljenim brojevima smeju davati samo zaposlenima u kompaniji s posebnim odobrenjem. Ali trebalo bi da za MCDL znaju samo zaposleni u firmi. Iako oni nikad ne bi dali takve podatke javnosti, ko bi odbio da pomogne kolegi koji se hvata u koštac sa zadatkom u teškim uslovima? Sažaljeva ga, jer je i sama imala loših dana na poslu, pa će malo zaobići pravila kako bi pomogla kolegi koji ima problem. Ona mu izdiktira raspored kablova, parica i svih telefonskih brojeva na pomenutoj adresi.

Analiza prevare

Stalno ćete u ovim pričama primećivati da je poznavanje kompanijske terminologije i strukture preduzeća – raznih kancelarija i odseka, čime se ko bavi i ko vlada kakvim podacima – deo neophodnog skupa trikova za uspešan poduhvat obmanjivanja.

mitnikova poruka

U ljudskoj prirodi je da verujemo drugim ljudima, a pogotovo kad je zahtev u granicama normale. U obmanjivanju se ta činjenica koristi da bi se žrtve iskoristile i da bi se postigli ciljevi.

MLADIĆ U BEKSTVU

Čovek kog ćemo zvati Frenk Parsons u bekstvu je već godinama. Još uvek ga traži američka vlada zbog učestvovanja u jednoj ilegalnoj antiratnoj grupi šezdesetih godina. U restoranima je sedao naspram vrata i povremeno gledao preko ramena, što je drugima smetalo. Selio se svakih nekoliko godina.

Tako se jednom Frenk našao u gradu koji nije poznao, i počeo je da traži posao. Za nekog poput Frenka, ko dobro vlada računarima (i obmanjivanjem, mada ovo potonje nikada nije upisivao u prijavu za posao), pronalazjenje posla obično nije bilo problematično. Ukoliko ekonomska situacija nije veoma loša, osobe s velikim tehničkim znanjem o računarima obično se svugde traže i gotovo bez problema ponovo staju na noge. Frenk je brzo pronašao dobro plaćen posao u jednoj velikoj, dobrostojećoj firmi s dugoročnim planovima za zaposlene, blizu mesta na kom je stanovao.

Savršeno, pomislio je. Ali kad je počeo da popunjava podugačak obrazac za prijavljivanje, naišao je na teškoću: poslodavac je zahtevao da podnosioc aplikacije priloži primerak državnog izveštaja o kriminalnom dosijeu, koji je lično morao da zatraži od državne policije. U gomili papira za zapošljavanje nalazio se i obrazac kojim se mogao zatražiti taj dokument, a na njemu se nalazio i kvadrat za otisak prsta. Iako su tražili samo otisak desnog kažiprsta, ako bi se on poklopio s njegovim otiskom u bazi podataka FBI, verovatno bi uskoro radio u kantini neke federalne „institucije“.

S druge strane, Frenku se učinilo da bi možda ipak mogao da se izvuče. Možda država uopšte nije slala te uzorke otisaka prstiju u FBI. Kako to da sazna?

Kako? Bavio se obmanjivanjem – šta *mislite* kako je saznao? Pozvao je telefonom državnu policiju: „Zdravo. Vršimo istraživanje za Ministarstvo pravosuđa. Ispitujemo zahteve da bismo primenili nov sistem za identifikaciju otisaka prstiju. Mogu li da razgovaram s nekim ko zaista poznaje procedure i ko bi mogao da nam pomogne?“

Kad se lokalni stručnjak javio, Frenk mu je postavio niz pitanja o sistemima koje koriste i mogućnostima za pretraživanje i pohranjivanje podataka o otiscima prstiju. Jesu li imali ikakvih problema s opremom? Jesu li povezani sa sistemom za pretragu otisaka prstiju Nacionalnog centra za informacije o kriminalu, ili samo na neki lokalni sustem? Da li ljudi uglavnom lako nauče da koriste opremu?

Lukavo je ubacio ključno pitanje između ostalih.

Odgovor je bio upravo ono što je hteo da čuje: ne, nisu povezani s Nacionalnim centrom, i proveravaju samo državni Indeks kriminalnih informacija.

mitnikova poruka

Sposobni kradljivci informacija ne prežu od toga da pozovu službenike državnih institucija da bi saznali procedure u vezi s primenom zakona. Kad se domogne takvog podatka, on može uspeti da zaobiđe uobičajenu bezbednosnu proveru kompanije.

To je bilo sve što je Frank želeo da sazna. Nije imao dosije u toj državi, pa je predao prijavu, dobio posao i niko se nikada nije pojavio kraj njegovog radnog stola s rečima: „Gospoda su iz FBI i želeli bi da porazgovaraju s tobom.“

I, kako on tvrdi, pokazao se kao primeran radnik.

NA PRAGU

Uprkos pričama koje kruže o kancelarijama bez papira, u kompanijama se i dalje svakodnevno štampaju gomile papira. Štampane informacije se mogu ukrasti, čak i ako primenjujete preventivne bezbednosne mere i označite ih kao poverljive.

Evo priče u kojoj je opisano kako prevaranti obmanom mogu doći do najtajnijih dokumenata.

Obmana pomoću zaobilaznog broja

Svake godine američka telefonska kompanija objavljuje Imenik probnih brojeva (ili su bar to nekad radili, a budući da sam ja još uvek na uslovnoj slobodi, neću ih pitati da li to i dalje čine). Ovaj dokument je bio izuzetno značajan telefonskim prevarantima, jer je bio pun svih dobro čuvanih telefonskih brojeva koje koriste kompanijski stručnjaci, tehničari i drugi radi testiranja linija, ili provere brojeva koji stalno daju signal zauzeća.

Jedan od tih probnih brojeva, poznat u terminologiji kao *zaobilazni*, bio je posebno koristan. Prevaranti su ga koristili da bi pronašli istomišljenike s kojima bi ćaskali, na tuđ račun. Upotrebljavali su ga i kao broj koji bi davali, na primer, banci. Dali bi nekom zaposlenom u banci telefonski broj na koji ih mogu dobiti u kancelariji. Kad bi banka pozvala da proveri broj (zaobilazni) oni bi mogli da prime poziv, a bili bi zaštićeni jer su upotrebili broj koji se ne može povezati s njima.

U Imeniku probnih brojeva nalazilo se dosta zgodnih informacija koje bi mogao upotrebiti svaki telefonski prevarant željan informacija. Dakle, kad su novi imenici štampani svake godine, za njima su žudeli mnogi klinici čiji je hobi bio istraživanje telefonske mreže.

mitnikova poruka

Bezbednosna obuka o zaštiti važnih informacija mora biti obavezna za sve u okviru firme, a ne samo za zaposlene koji imaju elektronski ili fizički pristup kompanijskom računarskom sistemu.

Stivijeva prevara

Naravno, u telefonskim kompanijama ti imenici nisu lako dostupni, pa se prevaranti moraju dovijati da bi ih se domogli. Kako to mogu da učine? Mladić kome je stalo da dođe do imenika, mogao bi da učini nešto ovako.



Jedne prijatne jesenje večeri u južnoj Kaliforniji, mladić kojeg ćemo zvati Stivi pozove centralu male telefonske kompanije; iz te zgrade telefonske linije se račvaju do svih kuća i firmi u oblasti u kojoj oni pružaju usluge.

Kad se službenica javila, Stivi kaže da je iz ogranka iste telefonske kompanije koji objavljuje i distribuira štampani materijal. „Imamo nov Imenik probnih brojeva“, kaže. „Ali iz bezbednosnih razloga vam ne možemo dostaviti primerak dok ne preuzmemo stari, a isporuka kasni. Ako ostavite svoj primerak ispred vrata, raznosač će svratiti, pokupiti ga, ostaviti novi i produžiti.“

Službenica ništa ne sumnja i to joj zvuči razumno. Radi upravo ono što joj je rečeno, i ostavlja na prag zgrade primerak imenika, na čijim je korica-
ma velikim crvenim slovima ispisano upozorenje „**POVERLJIVO – KADA VIŠE NIJE POTREBAN, OVAJ DOKUMENT SE MORA UNIŠTITI**“.

Stivi se proveze pored zgrade i pažljivo osmatra ima li policajaca ili ljudi iz obezbeđenja telefonske kompanije skrivenih iza drveća, ili u parkiranim automobilima. Nonšalantno pokupi imenik i odveze se.

Eto još jednog primera kako obmanjivač lako može dobiti ono što želi ako se pridržava jednostavnog principa „samo traži ono što ti treba“.

BLIC NAPAD

Umetnost obmane se ne mora primenjivati samo na preduzeća. Ponekad su mete napada klijenti kompanije.

Rad sa strankama donosi frustracije, smeh, ali i naizgled bezazlene greške – od kojih neke mogu imati nepoželjne posledice po klijente.

Priča Dženi Ekton

Dženi Ekton je bila službenik za rad sa strankama u preduzeću Houmtaun Elekrik iz Vašingtona, tek nešto više od tri godine. Smatralo se da je jedna od boljih službenica, pametna i savesna.

Osoba s druge strane žice rekla je: „Ovde Eduardo iz odeljenja za naplatu. Imam na vezi sekretaricu jednog od potpredsednika; potrebne su joj neke informacije, a ja ne mogu da koristim svoj računar. Dobio sam elektronsku poruku od jedne devojke iz kadrovske u kojoj je pisalo „VOLIM TE“, a kad sam otvorio priloženu datoteku, više nisam mogao da pokrenem računar. Virus. Dobio sam glupi virus. No, bilo kako bilo, možeš li da mi pogledaš neke podatke o klijentima?“

„Naravno“, odgovori Dženi. „Uništio ti je računar? Pa to je strašno.“

„Ma, da.“

„Šta mogu da učinim?“ upita Dženi.

Tad je napadač zatražio informacije o kojima se prethodno obavestio kako bi zvučao autentičnije. Otkrio je da se traženi podatak nalazi u nečemu što se zove Sistem za informacije o naplati, i saznao kako ga zaposleni zovu. Upitao je: „Možeš li da pogledaš jedan račun iz SIN-a?“

„Da, koji je broj računa?“

„Ne znam broj. Treba da ga pronađeš prema imenu.“

„U redu, pod kojim imenom?“

„Heder Marning.“ Ponovio joj je ime slovo po slovo, a Dženi ga je otkucala.

„Dobro, tu je.“

„Sjajno. Je li račun aktuelan?“

„A-ha, aktuelan je.“

„Koji je broj?“ upitao je.

„Imaš li olovku?“

„Pišem.“

„Broj računa je BAZ6573NR27Q.“

Ponovio joj je broj, a potom kazao: „A koja joj je adresa?“

Dala mu je adresu.

„A telefon?“

Dženi mu je poslušno pročitala i taj podatak.

Sagovornik se zahvalio, pozdravio se i prekinuo vezu. Dženi se javila na sledeći poziv, nikad i ne pomislivši na prethodni.

Istraživački projekt Arta Silija

Art Sili je prestao da radi honorarno za male izdavačke kuće kad je ustanovio da može da zaradi više istražujući za pisce i kompanije. Uskoro je shvatio da se honorar povećava proporcionalno tome koliko mu se zadatak graniči s nelegalnim. Art je počeo da se bavi obmanjivanjem, primenjujući metode bliske svakom lovcu na informacije, a da to nije ni znao, a kamoli to tako nazivao. Ispostavilo se da ima urođeni talenat za poslovnost, sam je pronalazio metode koje su mnogi morali da uče od drugih. Nakon izvesnog vremena, prekoračio je granicu legalnog, a da se nimalo nije osetio krivim zbog toga.

Pozvao me je čovek koji je pisao knjigu o radu američke vlade u Niksonovo vreme; tražio je istraživača koji bi mogao da se domogne internih informacija o Vilijamu E. Sajmonu, Niksonovom sekretaru za finansije. Gospodin Sajmon je umro, ali je autor saznao ime jedne njegove službenice. Bio je prilično siguran da i dalje živi u Vašingtonu, ali nije uspeo da dođe do njene adrese. Nije imala telefon, ili bar nije bila navedena u imeniku. I tada je nazvao mene. Rekao sam mu da nema problema.

Taj posao se obično može obaviti pomoću jednog ili dva telefonska poziva, ako znate šta radite. Uglavnom se može računati na to da će svaka lokalna uslužna kompanija obelodaniti takvu informaciju. Naravno, morate malo da izvrćete istinu, ali šta je poneka laž iz nužde tu i tamo – je li tako?

Volim da svaki put upotrebim drugačiji pristup, tek da mi bude zanimljivo. Predstavljanje „Ovde taj-i-taj iz uprave“ uvek je dobro palilo. Isto tako i „Imam na vezi nekoga iz kancelarije nečijeg potpredsednika“, što je ovog puta dobro prošlo.

mitnikova poruka

Nikad nemojte misliti da svaka obmana mora biti toliko komplikovana da će je žrtva verovatno prepoznati pre nego što se privede kraju. Neke su munjevit, veoma jednostavni napadi u kojima se napadač samo pojavi i odmah nestane, pri čemu... pa, jednostavno traži ono što mu treba.

Morate na neki način razviti instinkt za obmanjivanje, odnosno osećaj za to koliko će osoba s druge strane žice sarađivati s vama. Ovoga puta imao sam sreće s ljubaznom damom spremnom da pomogne. Samo jednim telefonskim pozivom pronašao sam i adresu i telefonski broj. Zadatak je bio izvršen.

Analiza prevare

Dženi je sigurno znala da su informacije o klijentima poverljive. Nikada nije razgovarala o računu jednog klijenta s drugim klijentom, niti je davala podatke lične prirode javnosti.

Ali, za ljude iz kompanije važe drugačija pravila. Kad je u pitanju kolega, sve se svodi na timski rad i ispomaganje da bi se posao obavio. Čovek iz nplatnog mogao je i sam da proveri te podatke da mu računar nije zaražen virusom, i bilo joj je drago što može da pomogne kolegi.

Art se postepeno primicao informacijama koje je zaista želeo, postavljajući usput pitanja o stvarima koje mu zapravo i nisu bile potrebne, poput broja računa. Ipak, istovremeno mu je broj računa obezbeđivao zaleđinu: da je službenica nešto posumnjala, pozvao bi ih drugi put i imao bi veće šanse za uspeh, jer bi nekom drugom službeniku zvučao autentičnije, budući da zna broj računa.

Dženi nikad nije ni pomislila da bi neko mogao lagati tako uverljivo, te da njen sagovornik uopšte nije iz odeljenja za naplatu. Naravno, ne treba za to kriviti Dženi. Nisu je dobro naučili pravilu da se valja uveriti u identitet sagovornika pre nego što se saopšte informacije o klijentima. Nikad je niko nije upozorio na opasnost koja preti od poziva poput Artovog. To nije bila politika kompanije, niti deo njene obuke, a ni njen nadređeni to nikada nije pomenuo.

KAKO SPREČITI OBMANU

Evo nečega što valja uvrstiti u bezbednosnu obuku: ako neko, ko pozove telefonom ili dođe u kompaniju, zna imena pojedinih ljudi, ili poznaje kompanijsku terminologiju ili procedure, to ne znači da je taj osoba za koju se izdaje. Puko predstavljanje ga sigurno ne ovlašćuje da dobije interne informacije, niti pristup računarskom sistemu ili mreži.

U bezbednosnoj obuci mora se naglasiti: ako ste u nedoumici, obavezno proverite.

Ranije je pristup kompanijskim informacijama bio znak ranga i privilegija. Zaposleni su ložili, radili na mašinama, kucali slova i slali izveštaje. Poslovođa ili šef govorili su im šta da rade, kada i kako. Oni su znali koliko uređaja svaki radnik treba da proizvede u jednoj smeni, koliko uređaja i koje boje fabrika treba da izradi te nedelje, sledeće nedelje i do kraja meseca.

Radnici su se bavili mašinama, alatima i materijalima, a šefovi informacijama. Radnicima su bile potrebne samo specifične informacije o njihovom poslu.

Danas stvari stoje malo drugačije, zar ne? Mnogi fabrički radnici koriste računar ili mašinu kojom upravlja računar. Najbitnije informacije se spuštaju sve do krajnjih korisnika kako bi mogli da obave posao. U današnjem okruženju, bavljenje informacijama je gotovo sve što zaposleni rade.

Zato se pravila o kompanijskoj bezbednosti moraju distribuirati širom preduzeća, bez obzira na poziciju. Svako mora da shvati da nemaju samo šefovi i rukovodioci informacije koje napadaču možda trebaju. Danas radnici na svim nivoima, pa čak i oni koji ne koriste računare, mogu biti meta napada. Možda je upravo novozaposleni službenik u odeljenju za rad sa strankama slaba tačka na koju napadač cilja.

Bezbednosna obuka i kompanijska pravila trebalo bi da ojačaju tu slabu tačku.



poglavlje

4

Izgradnja poverenja

možda ćete zbog nekih od ovih priča pomisliti da ja smatram da su svi zaposleni potpune neznalice, spremni, pa čak i željni da odaju svaku tajnu koju znaju. Obmanjivači znaju da to nije istina. Zašto su onda napadi te vrste tako uspešni? Ne zato što su ljudi glupi ili se ne vode zdravim razumom, nego zato što svi, kao ljudska bića, možemo biti obmanuti, jer pogrešno ukazujemo poverenje ako nas na određen način izmanipulišu.

U obmanjivanju, napadač računa na sumnju i otpor, i uvek je spreman da pretvori nepoverenje u poverenje. Onaj ko je dobar u tome, planira napad poput igre šaha, predviđajući pitanja koja mu žrtva može postaviti, kako bi imao spremne odgovore.

Jedna od uobičajenih tehnika je izgradnja poverenja kod žrtve. Kako vas prevarant može navesti da mu poverujete? Verujte mi, on to može.

POVERENJE – KLJUČ OBMANE

Što je pokušaj obmane sličniji uobičajenom poslovnom razgovoru, to se lakše otklanja sumnja. Kad ljudi nemaju razloga da budu sumnjičavi, lako je zadobiti njihovo poverenje.

Kad napadač zadobije vaše poverenje, most je spušten, a vrata zamka širom otvorena tako da može da uđe i uzme koje god informacije želi.

napomena

Primitičete da koristim zamenicu „on“ u većini ovih priča kad je reč o obmanjivačima, telefonskim prevarantima i sličnima. Nije u pitanju šovinizam; to samo odslikava istinu da se obmanjivanjem uglavnom bave muškarci. No, iako u tom polju nema mnogo žena, njihov broj raste. Ima dovoljno žena obmanjivača da ne bi trebalo da ste neoprezni samo zato što čujete ženski glas. Zapravo, žene koje to čine su u prednosti jer lakše mogu da flertuju kako bi postigle saradnju. Na ovim stranicama biće zastupljen manji broj pripadnica lepšeg pola.

Prvi poziv: Andrea Lopez

Andrea Lopez se javila na telefon u videoteci u kojoj je radila, i odmah se nasmešila: uvek je lepo kad se mušterija potruži da pohvali uslugu. Ova je mušterija rekla da je imala odlično iskustvo s videotekom i da želi da upravniku pošalje pismo o tome.

Zatražio je upravnikovo ime i poštansku adresu, a ona je odgovorila da je to Tomi Elison, i dala mu adresu. Već je hteo da spusti slušalicu, kad mu je sinula još jedna ideja, pa je rekao: „Možda ću pisati i upravi vaše kompanije. Koji je broj vaše poslovnice?“ Dala mu je i tu informaciju. Zahvalio se, dodao nešto ljubazno o tome koliko je predusretljiva bila i oprostio se.

„Uvek se čini da smena brže prođe kad neko takav pozove“, pomislila je. „Kako bi bilo lepo kad bi češće zvali ljubazni ljudi.“

Drugi poziv: Džini

„Hvala vam što ste pozvali Studio Video. Kraj telefona je Džini, šta mogu da učinim za vas?“

„Zdravo, Džini“, reče glas oduševljeno. Zvučao je kao da razgovara sa Džini otprilike svake nedelje. „Ovde Tomi Elison, upravnik videoteke Forest Park broj 863. Imamo ovde jednu mušteriju koja želi da iznajmi kasetu *Roki 5*, a nama je nestalo kopija. Možete li da proverite da li je vi imate?“

Ponovo je uzela vezu nakon nekoliko trenutaka i kazala: „Da, imamo tri kopije.“

„U redu, videću da li želi da se odveze do vas. Čujte, hvala vam. Ako vam ikada zatreba pomoć iz naše videoteke, samo pozovite i tražite Tomija. Rado ću učiniti sve što je u mojoj moći.“

Tri ili četiri puta u sledećih nekoliko nedelja Tomi je zvao Džini tražeći pomoć u vezi sa ovim ili onim. Naizgled su to bili razumni zahtevi, i uvek je bio veoma ljubazan, a da nije zvučao kao neko ko pokušava da joj se nabaci. Usput je malo i ćaskao: „Jeste li čuli za veliki požar u Ouk Parku? Puno ulica je zatvoreno u toj oblasti“, i tome slično. Ti pozivi su joj pružali odušak od svakodnevnice rutine, i Džini je uvek bilo drago da razgovara s njim.

Jednog dana Tomi se javio i zvučao kao da je pod stresom. Pitao je: „Jeste li vi tamo imali problema s računarima?“

„Ne“, odvrati Džini. „Zašto?“

„Neki tip je udario u telefonski stub, a majstor iz telefonske kompanije kaže da čitav deo grada neće imati telefonske veze i veze s Internetom dok to ne poprave.“

„O, ne. Je li čovek povređen?“

„Odveli su ga kolima hitne pomoći. Bilo kako bilo, trebala bi mi mala pomoć. Imam ovde vašu mušteriju koja želi da iznajmi *Kuma II*, a nema uza se karticu. Možete li da proverite njegove podatke?“

„Da, svakako.“

Tomi joj je dao njegovo ime i adresu, a Džini ga je našla u računararu. Dalá je Tomiju broj pod kojim se mušterija vodi.

„Ima li nekih dugovanja ili kasete vraćenih uz kašnjenje?“, pitao je Tomi.

„Ne vidim ništa.“

„Dobro, sjajno. Ručno ću ga upisati ovde, pa ćemo ga ubaciti u vašu bazu podataka kasnije kad računari ponovo prorade. Želi da plati Visa karticom koju koristi u vašoj radnji, a nema je sad kod sebe. Koji je broj i datum do kojeg važi?“

Izdiktirala mu je i broj i datum. Tomi reče: „Hvala vam na pomoći. Čujemo se uskoro“, i prekinu.

Priča Dojla Lonegana

Lonegan nije mladić koga biste želeli da zateknete ispred svojih ulaznih vrata. Nekada je bio uterivač velikih kockarskih dugova, a danas još uvek učini poneku uslugu starim znancima, ako mu to ne predstavlja suviše velik problem. U ovom slučaju ponuđena mu je pozamašna suma novca za svega nekoliko poziva videoteci. Zvuči veoma jednostavno, a niko od njegovih „mušterija“ nije umeo da izvede ovu prevaru. Trebao im je neko s Loneganovim talentom i umećem.



Da bi se pokrio dug, kad nemate sreće ni pameti za kockarskim stolom, ne ispisuju se čekovi. Svi to znaju. Zašto su ovi moji prijatelji nastavili da igraju s prevarantom koji nije imao para na stolu? Ne pitajte. Možda im fali koja vijuga. Ali to su moji prijatelji – šta ću.

Momak nije imao novca, pa su prihvatili ček. Trebalo je da ga odvedu do aparata za gotovinu, ali ne, uzeli su ček. Na 3230 dolara.

Naravno, nije imao pokriće. Šta biste drugo i očekivali? A onda su pozvali mene i pitali mogu li im pomoći. Ja više ljudima ne prebijam prste vratima da bi vratili dug. Osim toga, danas ima boljih načina. Rekao sam im da ću za 30 procenata provizije videti šta mogu da uradim. I tako su mi dali njegovo ime i adresu, a ja sam otišao do prvog računara da proverim koja videoteka mu je najbliža.

Nisam žurio. Trebalo je da pozovem telefonom četiri puta da bih omekšao upravnika videoteke, a onda – pogodak! Dobio sam broj Visa kartice tog prevaranta.

Jedan moj prijatelj drži toples bar. Za pedeset dolara naplatio sam kockarski dug sa Visa kartice u tom baru. Neka to taj prevarant samo objasni svojoj ženi. Mislite da bi mogao objasniti kompaniji Visa da on nije napravio taj trošak? Razmislite ponovo. On zna da mi znamo ko je. Ako smo se domogli broja njegove Visa kartice, smislićemo kako da dodemo i do mnogo čega drugog. Nema brige.

Analiza prevare

Prvih nekoliko Tomijevih poziva Džini poslužili su da se izgradi poverenje. Kad je došlo vreme za sam napad, nije bila oprezna i poverovala je da je Tomi onaj za koga se izdaje, upravnik druge videoteke iz istog lanca.

A zašto i *ne bi* poverovala – već ga je poznavala. Upoznala ga je samo preko telefona, dakako, ali između njih se uspostavilo poslovno prijateljstvo koje je osnova poverenja. Kad ga je prihvatila kao čoveka koji ima autoritet, kao upravnika iz iste kompanije, poverenje je već bilo izgrađeno, a ostalo je bilo mačji kašalj.

mitnikova poruka

Metoda izgradnje poverenja radi prevare jedna je od najefektnijih u obmanjivanju. Morate razmisliti o tome da li zaista poznajete osobu s kojom razgovarate. U retkim slučajevima, ta osoba možda nije onaj za koga se izdaje. Shodno tome, svi moramo naučiti da posmatramo, razmišljamo i budemo skeptični prema osobama koje navodno imaju autoritet.

VARIJACIJA NA TEMU: OSVAJANJE KARTICE

Za izgradnju osećaja poverenja nije uvek neophodan niz telefonskih poziva žrtvi, kao u prethodnoj priči. Sećam se događaja kojem sam prisustvovao. Građenje poverenja je potrajalo svega pet minuta.

Iznenadenje, tata

Sedeo sam za stolom u restoranu s Henrijem i njegovim ocem. Tokom razgovora, Henri je grdio oca što je dao broj kreditne kartice kao da je broj telefona. „Naravno da moraš da daš broj kartice kad nešto kupuješ“, reče. „Stvarno je glupo dati ga u radnji koja snima brojeve u svoj zapisnik.“

„Jedino mesto gde se tako radi je Studio Video“, odgovori gospodin Konklin, navodeći isti lanac videoteke. „Svakog meseca proveravam izvod s Visa kartice. Da su počeli da troše s nje, znao bih.“

„Naravno“, reče Henri, „ali kad oni imaju tvoj broj, lako ga je ukrasti.“

„Misliš da bi to uradio neki nepošteni zaposleni.“

„Ne, *bilo ko*, a ne samo zaposleni.“

„Pričaš gluposti“, reče gospodin Konklin.

„Mogu da ih pozovem odmah i reći će im broj tvoje Visa kartice“, odvratila Henri.

„Ma, *ne možeš*“, reče njegov otac.

„Mogu to da uradim za pet minuta, tu pred tobom, a da se i ne maknem od stola.“

Lice gospodina Konkлина bilo je zategnuto; izgledao je kao neko ko se oseća samouvereno, ali ne želi to da pokaže. „Kažem ti da ne znaš šta pričaš“, obrecnuo se, vadeći novčanik i tresnuvši novčanicu od pedeset dolara na sto. „Ako uradiš to što tvrdiš, ovo je tvoje.“

„Ne treba mi tvoj novac, tata“, kaza Henri.

Izvadio je mobilni telefon, pitao oca u koju videoteku ide i nazvao službu informacija da bi dobio telefonski broj centrale, kao i broj videoteke blizu Šerman Ouksa.

Slično kao u prethodnoj priči, ubrzo je saznao ime upravnika i broj videoteke. Zatim je pozvao centralu, predstavio se kao upravnik i upotrebio istu prevaru: „Da li vam danas računari dobro rade? Naši malo rade, malo ne rade.“ Saslušao je njen odgovor, a potom rekao: „Vidite, jedna vaša mušterija hoće da iznajmi kasetu kod nas, ali nam računari trenutno ne rade. Potražite njegov korisnički račun i proverite da li je zaista vaša mušterija.“

Henri im je dao očevo ime. Zatim je, veoma malo izmenivši metodu, zatražio da mu pročitaju sledeće podatke: adresu, broj telefona i datum otvaranja računa. Onda reče: „Čujte, zadržavam mnogo mušterija. Koji mu je broj kreditne kartice i datum do kojeg važi?“

Pridržavao je mobilni telefon na uhu jednom rukom dok je drugom zapisivao na salvetu. Kad je završio razgovor, gurnuo je salvetu pred oca, koji je zurio u nju otvorenih usta. Jadnik je izgledao potpuno šokiran, kao da mu je čitav sistem poverenja poljuljan.

Analiza prevare

Razmislite o sopstvenom stavu kad vam neko koga ne znate zatraži nešto. Ako vam na vrata dođe pohaban neznanac, verovatno ga nećete pustiti unutra; ako dođe neko lepo obučen, uglancanih cipela, savršene kose, ljubazan i nasmejan, verovatno ćete biti mnogo manje sumnjičavi. Možda je on stvarno Džejson iz filmova *Petak 13*, ali ste spremni da odmah poverujete toj osobi sve dok izgleda normalno i nema nož u ruci.

Manje je očigledna činjenica da ljude s kojima razgovaramo telefonom procenjujemo na isti način. Da li ta osoba zvuči kao da želi nešto da mi proda? Je li ljubazan i otvoren, ili osećam nekakvu odbojnost ili pritisak?

Govori li kao obrazovana osoba? Takve stvari, i možda još mnogo drugih, ocenjujemo nesvesno, u trenutku, često u prvih nekoliko trenutaka razgovora.

mitnikova poruka

U ljudskoj prirodi je da mislimo kako je malo verovatno da nas obmanjuju, bar dok nemamo razloga da poverujemo u suprotno. Odmerimo rizike a onda, uglavnom, nad sumnjom prevagne poverenje. To je normalno ponašanje civilizovanih ljudi... bar onih civilizovanih ljudi koje nikad nisu prevarili, izmamulisali, niti od njih izmamili veliku sumu novca.

U detinjstvu, roditelji su nas učili da ne verujemo neznancima. Možda bismo u današnje vreme trebalo da svi vodimo računa o tom starom principu na radnim mestima.

Od nas se na poslu stalno nešto zahteva. Imate li adresu elektronske pošte ovog momka? Gde je najnovija verzija spiska mušterija? Ko radi honorarno na ovom delu projekta? Molim vas da mi pošaljete najnovije podatke o projektu. Potrebna mi je nova verzija izvornog koda.

A znate šta? Ponekad to traže osobe koje lično ne poznajete, koje rade za neki drugi ogranak kompanije, ili bar tako tvrde. Ako su informacije koje vam daju odgovarajuće i čini se da se razumeju u poslovanje („Merion je rekla...“; „Nalazi se na serveru K-16...“; „...26. Revizija planova za nove proizvode“), poverovaćete i bezbrižno im dati ono što traže.

Naravno, možda malo zastanemo, zapitavši se: „Zašto su nekom iz fabrike potrebni planovi naših novih proizvoda?“ ili „Može li da škodi ako kažem ime servera na kojem se nalazi?“ Zato postavite dodatnih nekoliko pitanja. Ako se čini da su odgovori razumni, a osoba deluje uverljivo, niste više oprezni i vraćate se svom prirodnom nahođenju. Imate poverenja u druge i činite (u granicama normale) sve što se od vas traži.

I nemojte ni za trenutak pomisliti da napadači ciljaju samo na one koji koriste kompanijske računarske sisteme. Šta je s momkom u prostoriji za poštu? „Možete li mi na brzinu učiniti uslugu? Ubacite ovo u internu kompanijsku vreću s poštom.“ Da li službenik iz prostorije za poštu zna da se u tom paketu nalazi disketa s posebnim programom za sekretaricu generalnog direktora? Sad taj napadač dobija primerak elektronske pošte generalnog direktora. Da li bi to zaista moglo da se desi u vašoj firmi? Odgovor glasi: u svakom slučaju.

MOBILNI TELEFON OD JEDNOG CENTA

Mnogi traže dok ne nađu bolju ponudu; obmanjivači ne traže bolju ponudu, već pronalaze načina da ponudu učine boljom. Na primer, ponekad je marketinška kampanja toliko dobra da joj je teško odoleti, a obmanjivač razmotri ponudu i gleda kako da je učini još primamljivijom.

Nedavno je jedna američka kompanija za mobilne telefone pripremala veliku promociju u kojoj su nudili potpuno nove telefone za samo jedan cent, kad potpišete ugovor.

Mnogi suviše kasno shvate da oštrouman kupac treba da postavi mnogo pitanja pre nego što potpiše ugovor za paket mobilne telefonije – da li je usluga analogna, digitalna, ili kombinacija te dve; broj minuta koji mesečno možete da koristite za razgovor; da li su uključene usluge rominga... i tako dalje. Posebno je važno jasno shvatiti broj meseci ili godina na koji morate da se obavezete ugovorom.

Zamislite prevaranta, kog privuče jeftin telefon koji kompanija nudi pri potpisivanju ugovora, ali mu se nikako ne dopada odgovarajući paket usluga. Nema problema. Evo jednog načina na koji bi mogao da razreši situaciju.

Prvi poziv: Ted

Napadač prvo pozove lanac prodavnica elektronske opreme u ulici Vest Žirard.

„Elektron Siti. Ted je kraj telefona.“

„Zdravo, Ted. Ovde Adam. Čujte, pre nekoliko večeri bio sam kod vas i razgovarao s jednim prodavcem o mobilnim telefonima. Rekao sam da ću mu se javiti kad odlučim koji paket želim, a zaboravio sam mu ime. Ko radi u tom ogranku u večernjoj smeni?“

„Ima ih više. Da nije bio Vilijam?“

„Nisam siguran. Možda je bio Vilijam. Kako izgleda?“

„Visok, pomalo mršav.“

„Mislim da je to bio on. Kako se ono preziva?“

„Hedli. H-E-D-L-I.“

„Da, to mi zvuči poznato. Kad počinje njegova smena?“

„Ne znam njegov raspored ove nedelje, ali večernja smena obično počinje oko pet.“

„Dobro. Pokušaću da ga dobijem večeras. Hvala, Tede.“

Drugi poziv: Kejti

Sledeći poziv upućuje prodavnicu istog lanca u ulici Nort Broud.

„Dobar dan, Elektron Siti. Kejti je kraj telefona. Izvolite.“

„Kejti, zdravo. Ovde Vilijam Hedli, iz prodavnice u ulici Vest Žirard. Kako ste?“

„Onako. U čemu je stvar?“

„Kupac je došao po onaj paket s telefonom koji košta jedan cent. Znae na šta mislim?“

„Da. Prodala sam nekoliko takvih prošle nedelje.“

„Imate li još tih telefona koji se dobijaju u paketu?“

„Čitavu gomilu.“

„Sjajno. Upravo sam prodao jedan. Čovek je platio i potpisao ugovor. Proverio sam inventar i video da nam je nestalo telefona. Tako mi je neprijatno. Možete li mi učiniti uslugu? Poslaću ga u vašu radnju da pokupi telefon. Možete li mu ga prodati za jedan cent i napisati mu račun? Trebalo bi da mi javi kad ga dobije, da mu objasnim kako da ga programira.“

„Da, naravno. Pošaljite ga.“

„Važi. Zove se Ted. Ted Jensi.“

Kad se momak pojavio i predstavio kao Ted Jensi, Kejti mu je napisala račun i prodala mobilni telefon za jedan cent, baš kao što ju je i zamolio „kolega“. U potpunosti je nasela na prevaru.

Na kasi, kupac ne nalazi sitninu u džepu, pa pruži ruku ka časici sa sitninom, uzme cent i da ga blagajnici. Dobija telefon, a da nije platio ni taj jedan cent za njega.

Potom slobodno može da ode u drugu kompaniju za mobilne telefone u kojoj se koristi isti model aparata, i da izabere paket usluga koji mu se dopada. Ako je moguće na mesečnoj osnovi, bez ikakvog obavezivanja.

Analiza prevare

Prirodno je da ljudi lakše prihvataju nekoga ko *tvrdi* da je kolega, i ko poznaje kompanijske procedure i terminologiju. Čovek koji je upotrebio metode obmane u ovoj priči saznao je pojedinosti o prodaji, predstavio se kao službenik kompanije, i zatražio uslugu iz drugog ogranka. To se događa između ogranaka maloprodajnih objekata i različitih odeljenja kompanije, gde su ljudi fizički razdvojeni i svakodnevno rade s kolegama koje nikad nisu sreli.

HAKERSKI UPAD U FBI

Ljudi obično nedovoljno razmišljaju o podacima koje njihova organizacija objavljuje na Webu. Za moj nedeljni program na stanici KFI Talk Radio u Los Angelesu, producent je pretražio mrežu i pronašao kopiju objašnjenja za pristup bazi podataka Nacionalnog informacionog centra za kriminal. Kasnije je otkrio i zvanično uputstvo na Mreži, a to je poverljiv dokument u kojem se nalaze sva uputstva za pretraživanje informacija iz nacionalne baze podataka FBI o kriminalu.

Pronašao je priručnik za kriminalističke službe u kom se nalaze formati i kodovi za pretraživanje informacija o kriminalcima i zločinima iz američke nacionalne baze podataka. Službe širom zemlje mogu da pretražuju tu istu bazu podataka i uzmu informacije koje bi im pomogle da reše kriminalne slučajeve za koje su nadležne. Uputstvo sadrži kodove iz baze podataka kojima se obeležava sve – od raznih vrsta tetovaža, do različitih brodskih trupova i apoena ukradenog novca i deonica.

Svako ko ima pristup priručniku može da potraži naredbe za dobijanje podataka iz nacionalne baze i njihovu sintaksu. Prateći instrukcije iz uputstva o procedurama, svako može izvući informacije iz baze, samo ako je dovoljno drzak. Uputstvo takođe sadrži telefonske brojeve službe tehničke podrške. Možda imate slične priručnike u firmi u kojima se nalaze kodovi proizvoda ili šifre za pretraživanje poverljivih podataka.

FBI gotovo sigurno nikada nije otkrio da su njihov poverljivi priručnik i uputstva o procedurama dostupni svima na mreži, i ne verujem da bi se obradovali kad bi to saznali. Jedan primerak je objavio ogranak vlade u Oregonu, a drugi jedna kriminalistička služba iz Teksasa. Zašto? U oba slučaja neko je verovatno mislio da ta informacija nije posebno značajna i da njeno objavljivanje nikome neće škoditi. Možda ju je neko objavio na

intranetu radi lakšeg korišćenja. Nikada nije shvatio da je učinio priručnik dostupnim svima na Internetu, koji imaju pristup dobrom pretraživaču mreže kao što je Google – uključujući i one koji su samo radoznali, one koji bi želeli da postanu policajci, hakere i vođe organizovanog kriminala.

Ulazak u sistem izmamljivanjem informacija

Princip upotrebe takvih informacija da bi se neko u državnoj službi ili poslovnom okruženju prevario isti je: budući da obmanjivač zna kako da pristupi određenim bazama podataka ili aplikacijama, odnosno zna nazive kompanijskih računarskih servera, ili nešto slično, postaje uverljiv. A uverljivost vodi do poverenja.

Kad se domogne takvih kodova, lako mu je da dođe do potrebnih podataka. U ovom primeru, mogao bi da počne tako što bi pozvao službenicu u lokalnoj stanici državne policije, i postavio joj pitanje o jednom kodu iz uputstva – na primer, o prekršajnom kodu. Mogao bi da kaže: „Kad podnesem OFF upit u NCIC-u, javlja mi se greška ‘Sistem ne radi’. Da li se i vama to dešava kad radite s OFF upitima? Hoćete li da probate, molim vas?“ Ili bi možda rekao da pokušava da pretraži WPF – što je policijski izraz za dosije tražene osobe.

Službenica s druge strane žice dobila bi jasan znak da njen sagovornik poznaje procedure i naredbe za pretraživanje NCIC-ove baze podataka. Ko bi drugi poznavao te procedure, ako nije prošao obuku?

Nakon što službenica potvrdi da njihov sistem dobro radi, razgovor bi se dalje mogao ovako odvijati:

„Trebala bi mi mala pomoć.“

„Šta tražite?“

„Treba mi da izvršite pretraživanje pomoću naredbe OFF za osobu po imenu Rirdon Martin. Datum rođenja je 10.18.1966.“

„Koji mu je broj soša?“ (Ponekad zaposleni u američkim kriminalnim službama broj socijalnog osiguranja nazivaju *soš*.)

„700-14-7435.“

Nakon pretraživanja spiska, mogla bi mu reći nešto ovako: „Ima 2602.“

Napadač bi u bazi na Mreži mogao otkriti šta taj broj znači: ta osoba u dosijeu ima ubeležen slučaj prevare.

Analiza prevare

Iskusni obmanjivač ne bi ni za trenutak razmišljao o tome kako da provali u bazu podataka NCIC-a. A i zašto bi, kad će se domoći željene informacije čim pozove lokalnu policijsku stanicu i razgovora biranim rečima tako da zvuči uverljivo kao „domaći“. Sledećeg puta nazove drugu policijsku stanicu i upotrebi isti izgovor.

terminologija

SOŠ (engl. *sosh*) Izraz iz slenga američkih kriminalističkih odeljenja za broj socijalnog osiguranja.

Možda se pitate da li je rizično pozvati policijsku stanicu, šerifovu kancelariju ili kancelariju saobraćajne policije. Zar napadač ne rizikuje previše?

Odgovor je negativan... i to iz određenih razloga. Ljudi iz kriminalnog odeljenja, kao i vojnici, od prvog dana u akademiji stiču uvreženo poštovanje prema starijem činu. Sve dok se napadač predstavlja kao vodnik ili poručnik – kao osoba višeg ranga od one s kojom razgovara – žrtva će se voditi dobro naučenim pravilom da se ljudi koji imaju veći autoritet ne ispituju. Drugim rečima, čin ima svoje privilegije, a pogotovo tu da ga osobe nižeg ranga ne proveravaju.

Kriminalistička služba i vojska nisu jedina mesta gde se zloupotrebljava poštovanje ranga. Pri napadima na kompanije, često se kao oružje koristi navodni autoritet – kao što se i vidi iz ovih priča.

SPREČAVANJE PREVARE

Koje korake može preduzeti vaša organizacija da bi smanjila verovatnoću da će prirodni instinkt poverenja u ljude kod zaposlenih biti iskorišćen u obmani? Evo nekih predloga.

Zaštitite svoje kupce

U ovom elektronskom dobu mnogi prodavci čuvaju brojeve kreditnih kartica kupaca. Postoje razlozi za to: kupac ne mora da daje podatke o kreditnoj kartici svaki put kad poseti prodavnicu ili Web lokaciju da bi nešto kupio. Međutim, to ne treba raditi.

Ako baš morate da čuvate brojeve kreditnih kartica, onda taj postupak treba da bude praćen merama zaštite koje se ne svode samo na upotrebu šifara i kontrole pristupa. Valja obučiti osoblje da prepoznaju pokušaje obmane poput onih opisanih u ovom poglavlju. Taj kolega kojeg niste upoznali, postao vam je prijatelj preko telefona, možda nije onaj za koga se izdaje. Možda on i ne treba da ima pristup poverljivim informacijama o korisnicima, jer i ne radi u vašoj kompaniji.

mitnikova poruka

Svako treba da je svestan metoda obmanjivanja: sakupi se što više informacija o meti, i iskoriste se da bi se zadobilo poverenje. A onda se ujeda pravo za vrat!

Mudro poklanjajte poverenje

Na odbranu od upada ne treba da budu spremni samo ljudi koji imaju pristup poverljivim informacijama – softverski inženjeri, osoblje u razvojnom odeljenju i tako dalje. Gotovo svakog u organizaciji valja obučiti, da bi se preduzeće zaštitilo od industrijskih špijuna i kradljivaca informacija.

Treba započeti ispitivanjem vrednih informacija širom preduzeća. Pojedinačno obratite pažnju na svaku poverljivu, bitnu ili vrednu informaciju, i razmislite o tome koje metode obmanjivanja napadač može da upotrebi kako bi ih ugrozio. Odgovarajuća obuka osoba kojima je poveren pristup takvim informacijama trebalo bi da se isplanira na osnovu odgovora na sledeća pitanja. Ako bih dao ovaj podatak najgorem neprijatelju, da li bi mogao da ga iskoristi da naudi meni ili mojoj kompaniji? Da li u potpunosti razumem kakav bi efekat mogle imati naredbe koje traže da unesem u računar?

Ne želimo da budemo sumnjičavi prema svakoj osobi koju upoznamo. Pa ipak, što smo poverljiviji, to je verovatnije da ćemo obmanjivaču odati poslovne informacije.

Šta treba da se nalazi na intranetu?

Neki delovi intraneta mogu biti otvoreni za javnost, dok drugima imaju pristup samo zaposleni. Koliko vaša kompanija vodi računa o pristupu

poverljivim informacijama? Kada je poslednji put iko iz vaše organizacije proverio da li su neke poverljive informacije na kompanijskom intranetu nenamerno postale dostupne svima preko delova Web lokacije koji su namenjeni javnosti?

Ako vaša firma štiti bezbednost mreže pomoću zastupničkih servera, da li ste nedavno proverili jesu li pravilno podešeni?

U stvari, da li je iko *ikada* proverio koliko je bezbedan vaš intranet?



poglavlje

5

„Dopustite da vam pomognem“

Svi smo zahvalni kada imamo problem a naiđe neko ko se u to razume, vešt je i predusretljiv i ponudi nam pomoć. To je poznato obmanjivačima, i oni znaju kako se može iskoristiti.

Obmanjivač zna i kako da *prouzrokuje* problem, da biste mu potom bili zahvalni što ga je rešio. Na kraju, igrajući na kartu vaše zahvalnosti, obmanjivač iz vas izvlači neke podatke ili dobija male usluge zbog čega će vaša kompanija (ili možda vi sami) proći mnogo lošije u toj razmeni. A možda nikada nećete ni saznati da ste izgubili nešto značajno.

Evo tipičnih metoda koji se primenjuju u obmanjivanju da bi se „pružila pomoć“.

PAD MREŽE

Vreme: ponedeljak, 12. februar, 15:25

Mesto: Kancelarije brodogradilišta Starbord

Prvi poziv: Tom Dilej

„Tom Dilej, računovodstvo.“

„Zdravo, Tome. Ovde Edi Martin iz tehničke podrške. Pokušavamo da rešimo problem s računarskom mrežom. Zna li da li se ikome u vašem odseku prekidala veza s mrežom?“

„Koliko ja znam – nikome.“

„A ni vi sami nemate problema?“

„Ne, čini se da je sve u redu.“

„Dobro. Čujte, zovemo ljude koje bi mogao pogoditi ovaj problem, pa je važno da nam odmah javite ako vam se prekine veza s mrežom.“

„To baš i ne zvuči dobro. Mislite da se tako nešto može dogoditi?“

„Nadamo se da neće, ali nazvaćete nas ako se ipak desi, zar ne?“

„Sasvim sigurno.“

„Znači li to da bi prekid mrežne veze za vas bio velik problem?“

„U to se možete *kladiti*.“

„U tom slučaju, daću vam broj mog mobilnog telefona dok radimo na tome. Tako me možete direktno pozvati ako vam zatrebam.“

„To bi bilo sjajno. Kažite.“

„555 867 5309.“

„555 867 5309. Zapisao sam. Hvala vam. Kako se ono zovete?“

„Edi. Čujte, ima još nešto – moram da proverim na koji je konektor vaš računar priključen. Pogledajte svoj računar i proverite da li se na njemu nalazi nalepnica na kojoj je napisano nešto poput 'Broj konektora'.“

„Sačekajte. ... Ne, ne vidim ništa slično.“

„Dobro, onda pogledajte zadnju stranu računara. Prepoznajete li mrežni kabl?“

„Da.“

„Pratite ga do mesta na kojem je priključen u računar. Da li na tom konektoru postoji neka oznaka?“

„Sačekajte samo malo. Da, čekajte malo – moram da čučnem da bih se dovoljno približio i pročitao je. U redu – piše konektor 6 povlaka 47.“

„Dobro – tako ste i kod nas ubeleženi. Samo proveravam.“

Drugi poziv: momak iz informatičkog odeljenja

Dva dana kasnije, upućen je poziv mrežnom centru iste kompanije.

„Zdravo, ovde Bob. Nalazim se u kancelariji Toma Dileja u knjigovodstvu. Pokušavamo da popravimo jedan problem s kablom. Potrebno nam je da isključite priključak 6-47.“

Momak iz informatičkog odeljenja rekao je da će to biti obavljeno za samo nekoliko minuta, i zamolio je da mu se javi kad treba ponovo da ga osposobi.

Treći poziv: zvanje neprijatelja u pomoć

Nakon otprilike jednog sata, momak koji se predstavljao kao Edi Martin kupovao je elektronsku opremu u prodavnici, kad mu je zazvonio mobilni telefon. Proverio je broj osobe koja ga zove, video da je poziv upućen iz brodogradilišta, i žurno otišao do mirnog mesta pre nego što se javio.

„Služba za tehničku podršku, Edi.“

„O, zdravo, Edi. Čujem neki odjek, gde se nalazite?“

„Ja sam, ovaj, u prostoriji s mrežnim priključcima. Ko je to?“

„Ovde Tom Dilej. Uh, baš mi je drago što sam vas našao. Možda se sećate da ste me nazvali pre nekoliko dana. Veza s mrežom mi je upravo nestala, baš kao što ste i rekli da bi se moglo dogoditi, i pomalo sam se uspaničio.“

„Da, imamo gomilu takvih slučajeva. Trebalo bi da to sredimo do kraja dana. Je li to u redu?“

„NE! Do đavola, ništa neću stići da uradim ako ne budem imao vezu tako dugo. Koliko bih morao da čekam u najboljem slučaju?“

„Koliko vam je hitno?“

„Mogao bih nešto drugo da radim trenutno. Ima li šanse da to sredite za pola sata?“

„ZA POLA SATA! Uh! Dobro, vidite, ostaviću ovo što trenutno radim i videću da li mogu to da popravim za vas.“

„Bio bih vam zaista zahvalan, Edi.“

Četvrti poziv: moj si!

Nakon četrdeset pet minuta...

„Tome, ovde Edi. Probajte da se uključite u mrežu.“

Nakon nekoliko trenutaka:

„Uh, dobro je, radi. To je sjajno.“

„Odlično, drago mi je da sam uspeo da vam to popravim.“

„Da, hvala vam mnogo.“

„Čujte, ako želite da budete sigurni da vam veza neće ponovo ispasti, imam softver koji bi trebalo da instalirate. Oduzeće vam svega nekoliko minuta.“

„Sad baš i nije najpogodniji trenutak.“

„Razumem ... ali moglo bi obojici da uštedi velike glavobolje sledeći put kad se dogodi ovaj problem s mrežom.“

„Pa, ako će mi oduzeti svega nekoliko minuta...“

„Evo šta treba da uradite...“

Edi je zatim postupno objasnio Tomu kako da preuzme malu aplikaciju s jedne Web lokacije. Nakon što je preuzeo program, Edi je rekao Tomu da ga samo dvaput pritisne mišem. Pokušao je, i rekao:

„Ne radi. Ništa se ne dešava.“

„Baš bez veze. Mora da program ne valja. Hajde da ga izbrišemo, pa ćemo ponovo pokušati drugi put.“ Objasnio je Tomu kako da ga izbriše tako da se ne može ponovo pokrenuti.

Ukupno potrošeno vreme, dvanaest minuta.

Napadačeva priča

Bobiju Volisu je uvek bilo smešno kad bi dobio neki dobar zadatak, a klijent bi okolišao da objasni očigledno – zašto su mu potrebne te informacije. U ovom slučaju, mogao je da smisli samo dva razloga. Možda neko ko želi da kupi brodogradilište Starboard, pa hoće da zna pravu finansijsku situaciju – a pogotovo sve one podatke koje bi uprava brodogradilišta krila od potencijalnog kupca. Ili je klijent, u stvari, investitor koji misli da se s novcem ne radi kako valja, pa hoće da otkrije da li neki od direktora uzima parče kolača za sebe.

Možda klijent nije hteo da kaže pravi razlog zato što bi Bobi, kad bi znao koliko je vredna informacija, verovatno tražio više novca za posao.



Ima više načina da se prodre do najtajnijih datoteka firme. Bobi je proveo nekoliko dana razmatrajući mogućnosti i malo se raspitujući pre nego što je napravio plan. Odlučio se za pristup koji mu se posebno dopadao, u kojem se žrtva tako obmane da ona pozove napadača za pomoć.

Prvo je Bobi kupio mobilni telefon za 40 dolara u jednoj velikoj radnji. Pozvao je čoveka kojeg je odabrao kao metu, predstavio se da radi u tehničkoj podršci u okviru firme, i tako sredio da ga službenik pozove mobilnim telefonom ako bude problema s mrežnom vezom.

Sačekao je dva dana da ne bi bilo očigledno, a potom je pozvao mrežni operativni centar u kompaniji. Kazao je da rešava problem koji ima Tom, njegova žrtva, i zamolio ih da isključe Tomovu vezu s mrežom. Bobi je znao da je to najteži deo čitave ludorije; u mnogim firmama osoblje iz službe za tehničku podršku tesno sarađuje s onima iz mrežnog centra. Zapravo, znao je da je služba podrške često deo informatičke službe. Nezainteresovani momak iz centra, s kojim je razgovarao, ponašao se kao da je poziv rutinski, nije pitao za ime osobe iz korisničke službe koja navodno rešava problem u mreži, i potvrdio je da će isključiti žrtvin mrežni priključak. Kad to učini, Tom će biti potpuno izolovan od kompanijskog intraneta, i neće moći da otvara datoteke sa servera, razmenjuje ih sa saradnicima, preuzima elektronsku poštu, niti da pošalje i jednu stranicu podataka do štampača. U današnjem svetu, to je kao da živite u pećini.

Kao što je Bobi i očekivao, nedugo zatim zazvonio mu je telefon. Naravno, potrudio se da zvuči tako kao da žarko želi da pomogne tom jadnom „kolegi“ u nevolji. Potom je nazvao centar i rekao im da ponovo uključe

vezu s mrežom. Konačno, nazvao ga je i ponovo ga izmanipulisao, ovog puta učinivši da se oseća krivim što ga je odbio nakon učinjene usluge. Tom je pristao na njegov zahtev da preuzme neki softver.

Naravno, ono na šta je on pristao nije bilo to što se činilo da jeste. Softver, za koji je Tomu rečeno da će rešiti buduće probleme s mrežom, zapravo je bio trojanski konj, aplikacija koja je Tomovom računaru učinila isto što je mitski konj učinio Trojancima: uveo je neprijatelja u logor. Tom je rekao da se ništa ne događa kad dvaput pritisne mišem ikonicu; činjenica je da je softver tako napravljen da se ne vidi ništa, iako ta mala aplikacija instalira tajni program koji će uljezu omogućiti pristup Tomovom računaru.

Dok softver radi, Bobi postupno kontroliše Tomov računar, preko *daljinskog komandnog okruženja*. Kad je Bobi pristupio Tomovom računaru, mogao je da potraži zanimljive knjigovodstvene datoteke i kopira ih. Potom će, kad bude imao vremena, proveriti da li sadrže tražene informacije.

terminologija

TROJANSKI KONJ Program koji sadrži zlonameran ili štetan kôd, napravljen tako da ošteti žrtvin računar ili datoteke, ili da se domogne informacija s računara ili mreže. Neki trojanski konji se kriju unutar operativnog sistema računara i špijuniraju svako pritiskanje tastera ili operaciju, ili čekaju na naredbe preko mreže kako bi izvršili neku funkciju. Žrtva nije ni svesna njegovog prisustva.

I to nije sve. Bobi je mogao da pogleda elektronske poruke i privatne memorandume rukovodilaca kompanije, tako što bi pretražio tekst na osnovu reči koje bi mogle da otkriju zanimljive informacije.

Kasnije te večeri, pošto je naveo žrtvu da instalira softver, Bobi je bacio svoj mobilni telefon u smeće. Naravno, bio je dovoljno pažljiv da prvo izbriše memoriju i izvadi mu bateriju pre nego što ga je bacio – uopšte nije želeo da neko slučajno pozove taj broj i da telefon zazvoni!

Analiza prevare

Napadač plete mrežu kako bi uverio žrtvu da ima problem koji, zapravo, ne postoji – ili, kao u ovom slučaju, problem koji se još nije dogodio, ali napadač zna da će se desiti jer će ga on i prouzrokovati. Potom se predstavi kao osoba koja može to da reši.

Ovakva prevara je posebno primamljiva obmanjivaču. Unapred je pripremio teren, pa kad žrtva otkrije da ima problem, sama ga poziva i traži pomoć. Napadač samo sedi i čeka da telefon zazvoni, a ta taktika se od milja naziva *obrnuto obmanjivanje*. Napadač koji nagovori žrtvu da pozove *njega*, odmah postaje uverljivija: ako ja pozovem nekoga za koga mislim da radi u tehničkoj podršci, neću proveravati njegov identitet. Tu napadač pobeđuje.

terminologija

DALJINSKO KOMANDNO OKRUŽENJE (engl. *remote command shell*) Konzolno okruženje koje na osnovu tekstualnih komandi izvršava određene funkcije ili pokreće programe. Napadač koji iskorišćava tehničke nedostatke, ili je u stanju da instalira trojanskog konja na žrtvin računar, može pomoću njega i da upravlja na daljinu.

OBRNUTA OBMANA (engl. *reverse social engineering*) Radi se o obmani u kojoj napadač dovodi žrtvu u problematičnu situaciju, pa žrtva traži pomoć od obmanjivača. Drugo značenje „obrnute obmane“ jeste da se obmanjivač nađe u nebranom grožđu. Žrtva prepozna napad i koristi psihološke principe ubeđivanja da bi od obmanjivača izvukla što više informacija i zaštitila kompaniju.

mitnikova poruka

Ako vam neznana učini uslugu, a potom zatraži protivuslugu, ne činite ništa dok detaljno ne razmislite o tome što od vas traži.

U ovakvoj prevari, obmanjivač pokušava da izabere nekoga ko slabo poznaje računare. Što više zna, to će biti sumnjičaviji, ili će shvatiti da njime manipulišu. Osobe koje ja nazivam računarskim neznaalicama, one koje malo znaju o tehnologiji i procedurama, lakše sarađuju. Oni mnogo češće nasednu na prevaru tipa „Samo učitajte ovaj mali program“, jer nemaju predstavu o potencijalnoj šteti koju program može da nanese. Štaviše, ima mnogo manje šanse da će shvatiti koliko je vredna informacija koju ugrožavaju.

MALA POMOĆ NOVOJ DEVOJCI

Tek zaposleni su sjajna meta za napadače. Još ne poznaju mnogo ljudi, ne znaju kompanijske pravilnike niti šta se sme, a šta ne sme činiti. Da bi ostavili dobar prvi utisak, željni su da pokažu koliko su kooperativni i koliko brzo reaguju.

Predusretljiva Andrea

„Kadrovsko, Andrea Kalhun.“

„Zdravo, Andrea. Ovde Aleks iz kompanijskog obezbeđenja.“

„Da?“

„Kako ste?“

„Nije loše. Kako mogu da vam pomognem?“

„Vidite, planiramo seminar o bezbednosnom sistemu za nove kolege i treba da sakupimo neke ljude kako bismo sve isprobali. Trebaju mi imena i telefonski brojevi svih novoza-poslenih u poslednjem mesecu. Možete li mi pomoći?“

„Neću to moći da uradim do poslepodneva. Je li u redu? Koji je vaš lokal?“

„Naravno. Lokal je 52 ... ali danas ću gotovo ceo dan biti na sastancima. Pozvaću ja vas kad se vratim u kancelariju, verovatno nakon četiri.“

Kad je Aleks nazvao oko 4:30, Andrea je već pripremila spisak i pročitala mu je imena i lokale.

Poruka za Rouzmeri

Rouzmeri Morgan je bila oduševljena novim poslom. Nikada ranije nije radila za časopis i imala je utisak da su tu ljudi mnogo ljubazniji nego što je očekivala. To ju je iznenadilo s obzirom na konstantan pritisak pod kojim su gotovo svi zaposleni završavali još jedan broj do kraja mesečnog roka. Poziv koji je dobila u četvrtak ujutru potvrdio je taj utisak.

„Da li je to Rouzmeri Morgan?“

„Da.“

„Zdravo, Rouzmeri. Ovde Bil Džordej, iz odeljenja za bezbednost informacija.“

„Da?“

„Da li je iko iz vašeg odseka razgovarao sa vama o najboljim bezbednosnim postupcima?“

„Mislim da nije.“

„Dobro, da vidimo. Kao prvo, ne dozvoljavamo nikom da instalira softver koji nije kupila kompanija, zato što ne želimo da preuzmemo odgovornost za korišćenje nelicenciranog softvera. Hoćemo da izbegnemo probleme sa softverom koji prenosi crve ili viruse.“

„U redu.“

„Da li ste obavešteni o radu s elektronskom poštom?“

„Ne.“

„Koja je vaša elektronska adresa?“

„Rouzmeri@ttrzine.net.“

„Da li je vaše korisničko ime Rouzmeri?“

„Ne. Korisničko ime mi je R-crta-Morgan.“

„U redu. Sve zaposlene uvek upozoravam da neočekivane priložene datoteke mogu biti opasne. Šalje se mnogo virusa i crva, a dobijaju se u elektronskim porukama koje naizgled šalju poznanici. Dakle, ako dobijete neočekivanu elektronsku poruku s prilogom, trebalo bi uvek da proverite da li je osoba navedena kao pošiljalac poruke zaista tu poruku i poslala. Razumete?“

„Da, čula sam za to.“

„Dobro. I uveli smo pravilo da se lozinka menja svakih devedeset dana. Kada ste je poslednji put promenili?“

„Ovde sam tek tri nedelje. Još uvek koristim prvu.“

„U redu, nema problema. Možete sačekati dok ne istekne devedeset dana. Moramo da proverimo da li zaposleni koriste lozinke koje se suviše lako mogu pogoditi. Da li se vaša lozinka sastoji i od brojeva i od slova?“

„Ne.“

„To moramo ispraviti. Kako glasi vaša sadašnja lozinka?“

„Koristim ime svoje kćerke – Anet.“

„Zaista nije bezbedna. Nikada ne treba koristiti lozinku zasnovanu na podacima iz kruga porodice. Pa, da vidimo... mogli biste da učinite isto što i ja. Koristite isto što i sada kao prvi deo lozinke, ali svaki put kad je budete menjali dodajte broj tekućeg meseca.“

„Ako bih to učinila sada, za mart, da li da upotrebim broj tri, ili nula-tri?“

„To je na vama. Šta bi vam više odgovaralo?“

„Pretpostavljam Anet-tri.“

„U redu. Hoćete li da vam objasnim kako da promenite lozinku?“

„Ne, to znam.“

„Dobro. O još nečemu treba da razgovaramo. Na svom računaru imate instaliran antivirusni softver, i bitno je da ga ažurirate. Nikada ne smete isključiti automatsko ažuriranje, čak i kad računar povremeno malo uspori. U redu?“

„Naravno.“

„Odlično. Imate li broj na koji nas možete nazvati ako budete imali problema s računarem?“

Nije ga imala. Dao joj je broj, ona ga je pažljivo zapisala, a potom se vratila poslu. Bila je zadovoljna što o njoj tako brinu.

Analiza prevare

U ovoj priči naglašena je osnovna tema s kojom ćete se susresti u ovoj knjizi: najčešće informacije koje obmanjivač želi da izmami od zaposlenog, bez obzira na krajnji cilj, jesu žrtvini identifikacioni podaci. Kad se napadač domogne broja naloga i lozinke samo jednog zaposlenog iz odgovarajuće oblasti kompanije, on već ima sve što je potrebno da se uvuče i pronađe potrebne informacije. Imati te podatke isto je što i pronaći ključeve prostorija; pomoću njih se može slobodno kretati po kompaniji i naći traženo blago.

mitnikova poruka

Pre nego što tek zaposlenima dozvolite pristup bilo kom kompanijskom računarskom sistemu, morate ih obučiti da se pridržavaju odgovarajućih bezbednosnih pravila, a pogotovo onog da nikada ne otkrivaju svoju lozinku.

NIJE TAKO BEZBEDNO KAO ŠTO MISLITE

„Kompanija koja ne uloži napore da zaštiti svoje poverljive informacije, nemarna je.“ Mnogi bi se složili s tom izjavom. Svet bi bio bolji kad bi sve bilo tako očigledno i jednostavno. Istina je da čak i one kompanije koje se zaista trude da zaštite poverljive informacije mogu biti izložene ozbiljnom riziku.

Evo priče koja još jednom ilustruje kako se preduzeća svakodnevno zavaravaju mislju da se ne mogu zaobići njihova bezbednosna pravila, koja su planirali iskusni i sposobni profesionalci.

Priča Stiva Kremera

To nije bio velik travnjak, ne jedno od onih dvorišta zasejano skupim semenom. Nije izazivalo zavist. I sigurno nije bilo dovoljno veliko da bi Stiv imao izgovor za kupovinu kosilice sa sedištem, što je i bilo u redu, jer je svakako ne bi koristio. Voleo je da kosi travu ručnom kosilicom, jer je trajalo duže, a i imao je zgodan izgovor da se usredsredi na sopstvene misli, umesto da sluša Anu kako mu priča o ljudima iz banke u kojoj radi, ili objašnjava šta još treba da obavi. Mrzeo je te spiskove zadataka koji su postali sastavni deo svakog njegovog vikenda. Kroz glavu mu je sinulo da je dvanaestogodišnji Pit bio vrlo pametan kad se priključio plivačkom timu. Sad je morao da ide na trening ili sastanak svake subote, pa ga nisu čekali subotnji poslovi.

Stiv je dizajnirao nove uređaje za firmu DžeminiMed. Neko bi pomislio da je taj posao dosadan; on je znao da spasava živote. Stiv je smatrao da ima kreativan posao. Slikari, muzičari, kompozitori, inženjeri – prema Stivovoj logici svi imaju pred sobom isti izazov kao i on: stvaraju nešto što niko pre njih nije učinio. Njegov najnoviji izum, neobično inteligentno projektovan aparat za srce, biće njegovo najveće dostignuće dosad.

Bilo je gotovo 11:30 te subote, i Stiv se iznervirao jer je skoro pokosio travu, a nije smislio kako da smanji količinu struje potrebnu za rad srčanog aparata, što mu je bila poslednja prepreka. Bila je to savršena tema za razmišljanje dok se kosi trava, ali do rešenja nije došao.



Ana se pojavila na vratima, kose pokrivene crvenom kaubojskom maramom od meke tkanine, koju je uvek nosila dok je brisala prašinu. „Telefon“, viknula mu je. „Neko s posla.“

„Ko?“ doviknuo je Stiv.

„Neki Ralf. Čini mi se.“

Ralf? Stiv nije mogao da se seti nijednog Ralfa iz firme, ko bi mogao da ga zove vikendom. Ana je verovatno pogrešno čula ime.

„Stiv, ovde Ramon Perez iz tehničke podrške.“ „Ramon – kako je, za ime sveta, Ana čula Ralf, kad je ime španskog porekla“, pitao se Stiv.

„Zovem samo da vas obavestim“, reče Ramon. „Tri servera ne rade, mislimo da je možda u pitanju crv, pa moramo da obrišemo čvrste diskove i ponovo sve obnovimo sa rezervnih kopija. Trebalo bi da vaše datoteke budu dostupne od srede ili četvrtka – ako budemo imali sreće.“

„To je apsolutno neprihvatljivo“, reče Stiv oštro, trudeći se da ne dozvoli da ga bes savlada. Kako mogu biti tako glupi? Zar zaista misle da on može bez pristupa svojim datotekama čitavog vikenda i skoro cele sledeće nedelje? „Nema govora. Treba da sednem za kućni računar kroz dva sata i biće mi potreban pristup datotekama. Je li to jasno?“

„Da, svako koga sam dosad zvao hoće da bude prvi na spisku. Odrekao sam se vikenda da bih došao na posao i radio na ovome, i uopšte nije zabavno to što su svi s kojima razgovaram ljuti na mene.“

„Imam kratke rokove, a kompanija računa na moj rad. Moram da završim posao danas poslepodne. Šta vam tu nije jasno?“

„Još uvek moram da obavestim mnogo ljudi pre nego što uopšte počnem“, reče Ramon. „Šta kažete na to da vam datoteke budu spremne u utorak?“

„Ne u utorak, niti u ponedeljak, nego danas. ODMAH!“ reče Stiv, pitajući se koga će da zove ako ne uspe tom momku da utuvi u glavu ono što misli.

„U redu, u redu“, reče Ramon, a Stiv je mogao da čuje kako se iznervirao. „Da vidim šta mogu da učinim kako bih vam omogućio rad. Vi koristite server RM22, je li tako?“

„RM22 i GM16. Oba.“

„U redu. Dobro, mogu da odvojim malo vremena – trebaće mi vaše korisničko ime i lozinka.“

Oho, pomisli Stiv. Šta se ovde dešava? Zašto mu treba moja lozinka? Zašto bi je baš neko iz tehničke podrške zahtevao?

„Kako ste rekli da se prezivate? Ko vam je pretpostavljeni?“

„Ramon Perez. Vidite, kad ste se zaposlili, ispunili ste formular da biste dobili korisnički nalog, i morali ste da napišete i lozinku. Mogao bih da ga potražim i da vam pokažem da ga imamo u dokumentaciji. U redu?“

Stiv je nekoliko trenutaka razmišljao o tome, a potom se složio. Čekao je sa sve većim nestrpljenjem, dok je Ramon tražio dokumenta iz ormara za kartoteku. Kad se ponovo javio, Stiv je mogao da čuje kako prebira po gomili papira.

„A-ha, evo ga“, reče Ramon najzad. „Naveli ste lozinku ‘Dženis’.“

Dženis, pomisli Stiv. Bilo je to ime njegove majke, i zaista ga je ponekad koristio kao lozinku. Možda ga je stvarno zapisao kao lozinku kad je popunjavao formulare za novozaposlene.

„Da, tako je“, potvrdi.

„Dobro, gubimo vreme. Znae da sam zaista iz firme, i ako hoćete da vam na brzinu povratim dokumenta, moraćete malo da mi izadete u susret.“

„Moj identifikacioni kôd je s, d, crta, krejmer – k-r-e-j-m-e-r. Lozinka mi je ‘pelikan1’.“

„Odmah ću se pozabaviti time“, kaza Ramon, najzad predusretljivim glasom. „Dajte mi nekoliko sati.“

Stiv je pokosio travu, ručao, a kad je seo za računar video je da su mu datoteke ponovo tu. Bio je zadovoljan što je tako energično ubedio tog nepredusretljivog momka iz tehničke podrške, i nadao se da je Ana čula kako je pun samopouzdanja. Bilo bi dobro pohvaliti tog momka ili njegovog šefa, ali je znao da je to jedna od stvari na koju se nikada zaista ne bi odlučio.

Priča Krega Kogburna

Kreg Kogburn je ranije bio trgovački putnik za jednu visokotehnološku kompaniju, i dobro mu je išlo. Nakon izvesnog vremena, počeo je da shvata da ima talenta da oceni kupca, razume zbog čega određena osoba pruža otpor, i uoči neke slabe ili ranjive tačke pomoću kojih bi lako sklopio posao. Počeo je da razmišlja na koje druge načine bi mogao da upotrebi svoj talenat, i put ga je konačno naveo na plodnije tle: industrijsku špijunažu.



Ovo je bio težak zadatak. Nije izgledalo da će mi oduzeti mnogo vremena, a činilo se da će se dovoljno isplatiti kako bih otputovao na Havaje. Ili možda na Tahiti.

Čovek koji me je unajmio, razume se, nije mi rekao ko je pravi klijent, mada sam pretpostavio da je to neka kompanija koja želi da sustigne konkurenciju jednim brzim, lakim i velikim korakom. Samo je trebalo da se

domognem planova i specifikacija proizvoda za novi uređaj pod nazivom srčani aparat, šta god to bilo. Firma se zvala DžeminiMed. Nikad za njih nisam čuo, ali bila je to jedna od 500 najuspešnijih firmi, kako tvrdi časopis Fortune, sa kancelarijama na 5–6 lokacija – zbog čega mi je posao bio još lakši nego da je u pitanju mala kompanija gde su veće šanse da se zaposleni poznaju. To bi vam, kao što piloti kažu za sudar u vazduhu, moglo uništiti čitav dan.

Klijent mi je poslao faks, isečak iz nekog medicinskog časopisa u kojem je pisalo da DžeminiMed radi na aparatu revolucionarnog dizajna i da će se zvati STH-100. Za ime sveta, neki izveštač je već odradio veći deo mog posla. Imao sam nešto što mi je bilo potrebno i pre nego što sam počeo – naziv novog proizvoda.

Prvi problem: nabaviti imena zaposlenih u kompaniji koji rade na proizvodu STH-100 ili baciti pogled na planove. Zato sam pozvao operatera na centrali i kazao: „Obećao sam jednom čoveku u vašem inženjerskom timu da ću mu se javiti, a ne sećam se njegovog prezimena, njegovo ime počinje sa S.“ Ona onda reče: „Imamo Skota Arčera i Sema Dejvidsona.“ Okušao sam sreću. „Ko od njih radi u timu STH-100?“ Nije znala, pa sam nasumice odabrao Skota Arčera, a ona ga je pozvala.

Kad se javio, rekao sam: „Zdravo, ovde Majk iz prostorije za poštu. Imamo pošiljku preko FedEx-a za projektantski tim srčanog aparata STH-100. Da li možda znate kome je to upućeno?“ Reče da se vođa projekta zove Džeri Mendel. Naveo sam ga čak i da mi da njegov telefonski broj.

Okrenuo sam broj. Mendel nije bio tamo, ali je ostavio poruku na sekretarici da će biti na odmoru do trinaestog, što znači da je odvojio još nedelju dana za skijanje, ili nešto slično, i da svi kojima je nešto potrebno u međuvremenu treba da pozovu Mišel na 9137. Baš su predusretljivi ti ljudi. Jako su ljubazni.

Spustio sam slušalicu i pozvao Mišel, ona se javila na telefon, a ja joj rekoh: „Ovde Bil Tomas. Džeri mi je rekao da vas pozovem kad budem imao spremne specifikacije koje momci iz njegovog tima treba da revidiraju. Vi radite na srčanom aparatu, je li tako?“ Odgovorila je potvrdno.

Sad dolazimo do gadnog dela prevare. Da je zvučala sumnjičavo, bio sam spreman da igram na tu kartu kako samo pokušavam da učinim Džeriju uslugu za koju me je zamolio. Upitah: „Koji sistem koristite?“

„Sistem?“

„Koje servere koristi vaš tim?“

„A-ha“, reče „RM22. Neki iz grupe takođe upotrebljavaju GM16.“

Dobro. Ta informacija mi je bila potrebna. Izvukao sam je a da ništa nije posumnjalo. Omeškala je, pa sam važno pitanje postavio što sam nonšalantnije mogao. „Džeri reče da mi možete dati spisak adresa elektronske pošte osoba u razvojnom timu“, rekoh, i zadržah dah.

„Naravno. Distribucioni spisak je suviše dugačak da bih vam ga pročitao. Mogu li da vam ga pošaljem elektronskom poštom?“

Oprez. Svaka adresa elektronske pošte koja nije na kompanijskoj mreži predstavljala bi ogroman znak za uzbunu. „A šta kažete na to da mi ga pošaljete faksom?“ upitah.

Za nju to nije predstavljao nikakav problem.

„Faks mašina nam trenutno ne radi dobro. Moraću da pronađem broj neke druge. Ponovo ću vas pozvati za trenutak“, rekoh i spustih slušalicu.

Možda ćete pomisliti da sam se uplašio teškog problema, ali je to samo još jedan trik. Sačekao sam malo, da moj glas ne bi zazvučao poznato službenici na centrali, a potom sam je nazvao i kazao: „Zdravo, ovde Bil Tomas. Naša faks mašina ne radi. Mogu li da preusmerim jedan faks na vašu mašinu?“ Odgovorila je da nema problema i dala mi broj.

A onda samo uđem i kupim faks, je li tako? Naravno da ne. Pravilo broj jedan: nikad se ne pojavljuj lično ako baš ne moraš. Teško vas identifikuju samo ako zovete telefonom. Ako ne mogu da vas identifikuju, ne mogu ni da vas uhapse. Teško je navući lisice glasu preko žice. Zato sam ponovo pozvao službenicu na centrali nakon izvesnog vremena i pitao je da li je moj faks stigao. Odgovorila je da jeste.

„Čujte“, rekoh joj „faks moram da pošaljem jednom savetniku koji s nama sarađuje. Možete li to da uradite umesto mene?“ Pristala je. Zašto ne bi? Kako bi se od jedne službenice na centrali moglo očekivati da prepozna poverljive podatke? Dok je ona slala faks „savetniku“, ja sam, da bih se malo razmrdao, odšetao do obližnje knjižare, one na kojoj je istaknut znak „Primanje i slanje faksova“. Trebalo je da moj faks stigne pre mene i, kao što sam očekivao, čekao me je kad sam ušao. Šest strana po ceni od 1,75 dolara. Za novčanicu od 10 dolara i nešto sitnine dobio sam potpun spisak članova tima i njihove adrese elektronske pošte.

Upad u sistem

Dobro, dosad sam razgovarao s troje ili četvero ljudi za samo nekoliko sati, i već sam bio veoma blizu tome da uđem u računarski sistem kompanije. No, trebale su mi još neke informacije.

Broj jedan bio je telefon za uspostavljanje veze s inženjerskim serverom kad se zove van firme. Ponovo sam nazvao DžeminiMed, i zatražio od operatera na centrali da me spoji s informatičkim odeljenjem, te zamolio momka koji se javio da me poveže s nekim ko bi mogao da mi pomogne oko računara. Prebacio je liniju, a ja sam se pravio zbunjen i pomalo glup za sve što se tiče tehnike. „Nalazim se kod kuće, upravo sam kupio nov prenosiv računar, i treba da ga podesim tako da mogu da se spolja uključim u mrežu.“

Postupak je bio očigledan, ali sam ja strpljivo dopustio da mi objasni korak po korak, dok nije došao do telefonskog broja. Dao mi je broj kao da je to samo još jedna rutinska informacija. Onda sam ga naterao da sačeka dok sve ne isprobam. Savršeno.

Dakle, sad sam prevazišao i prepreku uključivanja u mrežu. Povezao sam se i otkrio da imaju server terminala, pomoću kojeg se korisnik može povezati sa svakim računarom u njihovoj internoj mreži. Nakon nekoliko pokušaja, naleteo sam na računar kojem je bio dodeljen privremeni nalog bez lozinke. Neki operativni sistemi, kad se prvi put instaliraju, nalažu korisniku da unese identifikacioni kôd i lozinku, ali nude i privremene naloge. Administrator treba da upiše lozinku za privremeni nalog ili da ga isključi, ali mnogi to ne znaju, ili ih to ne zanima. Ovaj sistem je verovatno tek instaliran, a administrator se nije potrudio da isključi privremeni nalog.

Zahvaljujući tome, sad sam imao pristup jednom računar, koji je, kako se ispostavilo, radio pod starijom verzijom operativnog sistema UNIX. Operativni sistem UNIX sadrži datoteku s lozinkama, u kojoj se nalaze *šifrovane lozinke* svih korisnika. Tekstualna lozinka se šifruje u niz alfanumeričkih znakova pomoću jednosmerne heš-funkcije.

terminologija

ŠIFROVANA LOZINKA (engl. *password hash*) Niz nerazumljivih znakova koji se dobija jednosmernim šifrovanjem lozinke. Trebalo bi da se proces ne može odvijati u drugom smeru; to jest, smatra se da se tekstualna lozinka ne može rekonstruisati iz šifrovanog oblika.

Kad momak, čija je kancelarija u dnu hodnika, želi da preuzme neke datoteke, on se mora identifikovati tako što unese korisničko ime i lozinku. Sistemski program koji proverava identifikaciju šifruje unetu lozinku, a potom upoređuje rezultat sa šifrovanom lozinkom u datoteci s lozinkama; ako se ta dva niza poklope, pristup se odobrava.

Budući da su lozinke u datoteci šifrovane, sama datoteka je dostupna svakom korisniku, jer se teorijski smatra da nema poznatog načina da se lozinke dešifruju. To je smešno – preuzeo sam datoteku, upotrebio rečnik (pogledajte poglavlje 12 da biste saznali nešto više o ovoj metodi), i otkrio da Stiven Krejmer trenutno ima nalog na datom računaru, čija je lozinka „Dženis“. Tek da probam, pokušao sam da unesem njegov nalog i tu lozinku na jednom od razvojnih servera; da je upalilo, uštedelo bi mi nešto vremena i rizika. Ali nije.

To je značilo da moram na prevaru da ga nateram da mi kaže svoje korisničko ime i lozinku. Za to ću sačekati vikend.

Ostalo već znate. U subotu sam pozvao Krejmera, i izložio mu priču o crvu i datotekama koje treba obnoviti iz rezervnih kopija da bih otklonio njegovu sumnju.

Šta je s onom pričom o tome da je naveo lozinku kad je ispunjavao obrasce pri zapošljavanju? Računao sam na to da se neće setiti da se to ikada desilo. Novozaposleni ispunjavaju tako mnogo obrazaca; ko bi se toga sećao godinama kasnije? U svakom slučaju, da nisam uspeo s njim, odabrao bih drugo ime s dugačkog spiska.

Pomoću njegovog korisničkog imena i lozinke, povezao sam se na server, malo tumačio njime, a potom utvrdio gde se nalaze datoteke s planovima za STH-100. Nisam znao koje su ključne, pa sam preneo sve datoteke na tajnu FTP lokaciju u Kini, gde se datoteke mogu čuvati, a da niko ništa ne posumnja. Neka klijent pretura po tome i pronade ono što želi.

terminologija

TAJNA LOKACIJA Skladište za informacije koje drugi verovatno neće pronaći. U svetu tradicionalnih špijuna, to bi mogao biti prostor iza nekog labavog kamena u zidu; u svetu računarskih hakera, to je često lokacija na Internetu u stranoj zemlji.

Analiza prevare

Za čoveka koga ovde zovemo Kreg Kogburn, ili bilo koga sličnog njemu i podjednako veštog u nepoštenim, ali ne uvek nelegalnim metodama obmanjivanja, ovaj izazov bio je gotovo rutinski. Njegov cilj je bio da pronađe i preuzme datoteke sa kompanijskog računara, koji je zaštićen barijerom i svim uobičajenim bezbednosnim tehnologijama.

Veći deo posla bio je prost kao pasulj. Počeo je tako što se predstavio kao neko ko radi u prostoriji za poštu i rekao da ima FedEx-ov paket koji čeka da bude isporučen. Iz te obmane dobio je ime vođe tima inženjera koji rade na srčanom aparatu. Vođa je bio na odmoru, ali – što je zgodno za svakog obmanjivača koji pokušava da ukrade informacije – ljubazno je ostavio ime i telefonski broj svoje pomoćnice. Pozvavši je, Kreg je otklonio svaku sumnju rekavši da se on samo javlja na zahtev vođe tima. S obzirom na to da je Džeri otputovao, Mišel nije imala načina da proveriti Kregovu tvrdnju. Prihvatila ju je kao istinitu i bez problema mu je obezbedila spisak osoba u timu – što su Kregu bile neophodne, i veoma vredne informacije.

Nije ništa posumnjala čak ni kad je Kreg zamolio da mu se spisak pošalje faksom umesto elektronskom poštom – iako je slanje elektronskom poštom obično zgodnije za oboje. Zašto je bila tako lakoverna? Poput mnogih zaposlenih, nije želela da se njen šef vrati i vidi da je odbila sagovornika koji samo pokušava da učini nešto što ga je njen pretpostavljeni zamolio. Osim toga, sagovornik je rekao da šef nije samo odobrio taj zahtev, već je i tražio njegovu pomoć. Još jednom, evo primera nekoga ko pokazuje žarku želju da bude timski igrač, zbog čega je, kao i mnogi drugi, podložan obmani.

Kreg je izbegao rizik da fizički uđe u zgradu tako što je organizovao da se faks pošalje službenici prijemnog odeljenja, znajući da će ona verovatno biti spremna da pomogne. Takvi službenici se, uostalom, obično biraju zbog toga što su šarmantni i ostavljaju dobar utisak. Male usluge kao što su primanje i prosledjivanje faksa deo su njihovog posla, a tu je činjenicu Kreg uspeo da iskoristi. Informacije koje je slala van firme uzbunile bi svakog ko zna koliko su vredne – ali kako se od službenice prijemnog odeljenja može očekivati da zna koje su informacije bezopasne, a koje poverljive?

Primenjujući drugačiji stil manipulacije, Kreg se pravio da je naivan kako bi ubedio osobu u računarskom odeljenju da mu otkrije broj za spoljni pristup kompanijskom serveru terminala. Taj uređaj se koristi za povezivanje na ostale računarske sisteme u okviru interne mreže.

mitnikova poruka

Svima je na poslu glavno da obave zadatak. Pod tim pritiskom, bezbednosne procedure često zauzimaju tek drugo mesto; ljudi ih ignorišu ili previde. Obmanjivači se oslanjaju na tu činjenicu.

Kreg je uspeo lako da se uključi tako što je isprobao podrazumevanu lozinku koja nikada nije izmenjena, a to je jedna od očiglednih, zjapećih rupa što postoje u mnogim internim mrežama koje se oslanjaju na zaštitnu barijeru. U suštini, podrazumevane lozinke mnogih operativnih sistema, usmerivača i mnogih vrsta proizvoda, uključujući i lokalne telefonske centrale, mogu se naći na Webu. Svaki obmanjivač, haker, industrijski špijun, ili puki radoznalac, može naći taj spisak na adresi <http://www.phenonelit.de/dpl/dpl.html>. (Potpuno je neverovatno koliko Internet olakšava život onima koji znaju gde da traže. A sad i vi to znate.)

Kogburn je potom zaista ubedio opreznog, podozrivog čoveka („Kako ste rekli da se prezivate? Ko vam je pretpostavljeni?“) da obelodani svoje korisničko ime i lozinku za pristup serverima koje koristi razvojni tim za srčani aparat. Bilo je to kao da je Kregu ostavio otvorena vrata da pretražuje najstrože čuvane tajne preduzeća i preuzme planove za nov proizvod.

A šta da je Stiv Krejmer i dalje sumnjao u verodostojnost Kregovog poziva? Verovatno ne bi prijavio da mu je nešto sumnjivo dok se u ponedeljak ujutro ne pojavi na poslu, što bi bilo suviše kasno da se napad spreči.

Ključni trenutak u poslednjem delu prevare: Kreg je isprva zvučao neodlučno i nezainteresovano za Stivove probleme, a potom se izmenio i zvučao kao da želi da pomogne Stivu da obavi svoj posao. Uglavnom, ako žrtva veruje da pokušavate da joj pomognete ili učinite neku uslugu, odaće poverljive informacije koje bi inače pažljivo čuvala.

SPREČAVANJE PREVARE

Jedan od najmoćnijih trikova u obmanjivanju je zamena uloga. To ste videli u ovom poglavlju. Napadač stvori problem, a potom ga magično reši, na prevaru izmamljujući od žrtve pristup najstrože čuvanim tajnama kompanije. Da li bi vaši zaposleni poverovali ovakvoj prevari? Da li ste se potrudili da napišete i objavite posebna bezbednosna pravila koja bi mogla to da spreče?

Obrazujte, obrazujte i obrazujte...

Postoji priča o strancu u Njujorku koji zaustavi čoveka na ulici i pita: „Kako da dođem do Karnegi Hola?“ Čovek odgovori: „Vežbajte, vežbajte, vežbajte.“ Svi su toliko podložni obmanama, da je jedina efikasna odbrana kompanije da obrazuje i obuči ljude, obezbeđujući im potrebnu praksu kako bi uočili prevaru. Potom stalno podsećajte ljude na to što su naučili na obuci.

Svako u organizaciji mora se obučiti da bude sumnjičav i oprezan kad lično ne poznaje sagovornika, a pogotovo kad taj zahteva bilo kakav pristup računaru ili mreži. U ljudskoj prirodi je da želimo da verujemo drugima ali, kao što Japanci kažu, poslovanje je rat. Vaša firma ne može dozvoliti da ne bude opreznna. U kompanijskom bezbednosnom sistemu mora se jasno definisati primereno i neprimereno ponašanje.

Bezbednosna pravila ne mogu biti ista za sve, ima različitih uloga i odgovornosti, i svaka pozicija je ranjiva na svoj način. Potreban je osnovni nivo obuke koji bi pohađali svi zaposleni, a potom ljude valja naučiti, prema njihovom poslu, da se drže odgovarajućih postupaka koji će umanjiti šanse da budu uvučeni u problem. Oni koji rade s poverljivim informacijama ili su na odgovornim položajima trebalo bi da pohađaju dodatnu obuku.

Zaštita poverljivih informacija

Kad neznata ponudi pomoć, kao što smo videli u pričama iz ovog poglavlja, zaposleni se moraju osloniti na bezbednosne mere firme koje su osmišljene prema potrebama poslovanja, veličini i običajima kompanije.

Nikada nemojte sarađivati s neznancem koji vas zamoli da potražite informacije, unesete nepoznate naredbe u računar, podesite softver ili, što je možda najopasnije od svega, da otvorite datoteke priložene uz elektronsku poruku ili učitate neproveren softver. Svaki program – čak i onaj koji naizgled ništa ne radi – možda nije tako bezazlen kakvim se čini.

napomena

Smatram da ni u jednoj kompaniji ne treba da bude dozvoljeno obelodanjivanje lozinki. Mnogo je lakše ustanoviti čvrsto pravilo koje zabranjuje osoblju da ikada daje ili razmenjuje poverljive lozinke. To je sigurnije. Ali, svaka firma mora da oceni sopstvene običaje i bezbednosna pitanja pri donošenju odluka.

Izvesne postupke obično vremenom zanemarimo, bez obzira na kvalitet obuke. Potom zaboravimo na obuku u odsudnom času, baš kad nam je potrebna. Pomislili biste da svako zna (ili bi trebalo da zna) da se korisničko ime i lozinka ne daju, i da to i ne treba pominjati – da tako nalaže zdrav razum. Zapravo, svakog zaposlenog treba često podsećati da je davanje korisničkog imena i lozinke kancelarijskog računara, kućnog računara, ili čak i mašine za štampanje taksenih marki u prostoriji za poštu, jednako obelodanjivanju PIN koda kreditne kartice.

Povremeno, *samo* povremeno, zaista postoje okolnosti kad je neophodno, pa čak i važno, otkriti nekom poverljive informacije. Zato se to „nikad“ ne sme postaviti kao apsolutno pravilo. Pa ipak, vaš bezbednosni pravilnik mora sasvim detaljno da propiše okolnosti pod kojima zaposleni može da otkrije svoju lozinku, i što je najvažnije, ko ima pravo da traži informacije.

Uzmite u obzir izvor informacija

U mnogim organizacijama, pravilo bi trebalo da bude da se informacija koja može da naudi kompaniji ili kolegi, može dati samo onom koga znate lično, ili onom čiji je glas toliko poznat da ga bespogovorno prepoznajete.

U situacijama gde je obezbeđenje na visokom nivou, treba uvažiti zahteve samo ako odgovorna osoba lično dođe po informacije, ili zahteve koji su na neki siguran način odobreni – na primer, pomoću dva podatka kao što su grupna lozinka i privatni kôd koji se periodično menja.

U procedurama za klasifikaciju podataka mora biti naznačeno da ljudi koji rade s poverljivim podacima ne smeju odavati *nikakve* informacije nikome koga lično ne poznaju, niti osobi za koju se na neki način ne garantuje.

Dakle, kako se ponašati kad vam kolega iz firme zatraži informacije kao što su spisak imena i adrese elektronske pošte u vašem timu, i to vama zazvuči logično? Zapravo, kako da podignete svest toliko da se takva informacija, koja je očigledno manje važna nego, recimo, specifikacije proizvoda u razvoju, prepozna kao nešto što je samo za internu upotrebu? Jedan veliki deo rešenja: odredite zaposlene u svakom odeljenju koji će voditi računa o svim informacijama koje treba slati van tima. Potom se mora obezbediti program na visokom nivou za te zaposlene, kako bi vodili računa o specijalnim postupcima za utvrđivanje identiteta kojih treba da se pridržavaju.

napomena

Neverovatno, čak ni ako potražite ime i telefonski broj sagovornika u bazi podataka zaposlenih u vašoj kompaniji i vi njega nazovete, niste potpuno sigurni – obmanjivači poznaju metode unošenja imena u kompanijske baze podataka ili preusmeravanja telefonskih poziva.

Nemojte nikoga zaboraviti

Svako može brzo da izdeklamuje one odeljke kompanije kojima je potrebna zaštita na visokom nivou od zlonamernih napada. Često se previde manje očigledna, a ipak jako ranjiva mesta. U jednoj od priča, zahtev da se faks pošalje na telefonski broj u okviru kompanije činio se bezazlenim i sasvim bezbednim, pa ipak je napadač iskoristio taj propust u bezbednosnom sistemu. Lekcija koju smo iz toga naučili: svako, od sekretarice i administrativnog pomoćnika, do rukovodstva kompanije i direktora mora pohađati posebnu bezbednosnu obuku, da bi uočio ovakve trikove. I ne zaboravite da zaštitite ulazna vrata: službenici prijemnog odeljenja su često odlične mete obmanjivača, i njima se moraju navesti metode za obmanjivanje koje koriste neki posetioci i sagovornici preko telefona.

Kompanijsko obezbeđenje bi trebalo da uspostavi jedinstveno mesto za prijavljivanje, vrstu šaltera za zaposlene koji misle da su možda bili obmanuti. Jedinstveno mesto gde će se prijavljivati incidenti narušavanja bezbednosti, omogućava da se napravi efikasan sistem, koji će dovoljno rano upozoravati zaposlene i jasno staviti do znanja svima kada dođe do isplaniranog napada, tako da se bilo kakva šteta može odmah regulisati.



poglavlje

6

„Možete li mi pomoći?“

Videli ste kako obmanjivači varaju ljude tako što se nude da im pomognu. Još jedan omiljeni pristup je potpuno suprotan: napadač obmanjuje žrtvu tako što se pretvara da mu je potrebna pomoć. Svi mi saosećamo s onima koji su u škripcu, a taj pristup je uvek efikasan i omogućava obmanjivačima da dođu do cilja.

NOVAJLIJA

U poglavlju 3 prikazano je kako napadač može da nagovori žrtvu da mu otkrije svoj identifikacioni broj. U ovoj priči je upotrebljena drugačija metoda s istim ciljem, a potom je prikazano kako napadač može da iskoristi tu informaciju.

Nadmudrivanje

U Silicijumskoj dolini postoji globalna kompanija čije ime nećemo navoditi. Razni prodajni centri i drugi terenski objekti širom sveta povezani su s rukovodstvom te kompanije preko mreže širokog područja. Brajan Eterbi pametan i drzak uljez, znao je da je gotovo uvek lakše ući u mrežu na jednoj od udaljenih lokacija, gde je obezbeđenje gotovo sigurno slabije, nego u upravi.



Uljez je pozvao kancelariju u Čikagu i zamolio da razgovara s gospodinom Džounsom. Službenica na centrali ga je pitala da li zna ime gospodina Džounsa. Odgovorio je: „Imao sam ga ovde negde, upravo ga tražim. Koliko osoba s prezimenom Džouns imate?“ Odgovorila je: „Tri. U kom odeljenju se nalazi?“

On reče: „Ako mi pročitate njihova imena, možda ću ga prepoznati.“ Ona je to i učinila: „Beri, Džozef i Gordon.“

„Džo. Gotovo sam siguran da je to on“, reče. „U kom je odeljenju?“

„U razvojnom.“

„Dobro. Možete li me spojiti s njim, molim vas?“

Prosledila je poziv. Kad se Džouns javio, napadač reče: „Gospodin Džouns? Zdravo, ovde Toni iz obračunskog. Upravo smo realizovali vaš zahtev da vam se plata isplaćuje direktno na račun u štedionici.“

„MOLIM???!!!! Mora da se šalite. Nisam podneo takav zahtev. Čak i nemam račun u štedionici.“

„Uh, do đavola, već sam ga realizovao.“

Džouns je bio veoma uznemiren pri pomisli da mu plata možda upravo odlazi na nečiji tuđ račun, i pomislio je da je momak s druge strane žice sigurno priglup. Pre nego što je i uspeo da odgovori, napadač reče: „Bolje da proverim šta se dogodilo. Izmene u platama se vrše prema identifikacionom broju. Koji je vaš broj?“

Džouns mu ga je dao. Njegov sagovornik reče: „Da, u pravu ste, niste vi uputili zahtev.“ „Svake godine su sve glupliji“, mislio je Džouns.

„Čujte, postaraću se da se to sredi. Odmah ću uneti ispravke. Ne brinite – sve će biti u redu s vašom sledećom platom“, reče momak uverljivo.

Poslovno putovanje

Nedugo zatim, administrator sistema u prodajnom centru kompanije u Ostinu u državi Teksas primio je telefonski poziv. „Ovde Džozef Džouns“, reče osoba s druge strane žice. „Ja radim u razvojnom odeljenju. Dolazim kod vas na nedelju dana, i biću u hotelu Driskil. Hteo bih da mi obezbedite privremeni nalog kako bih mogao da pristupam svojoj elektronskoj pošti, a da ne moram da zovem međugradski.“

„Kažite mi ponovo kako se zovete, i dajte mi svoj identifikacioni broj“, reče administrator sistema. Čovek koji se izdavao za Džounsa dade broj i nastavi: „Imate li brojeve za brzu vezu?“

„Sačekajte malo. Moram da proverim vaše podatke.“ Nakon izvesnog vremena, rekao je: „U redu, Džo. Recite mi broj zgrade.“ Napadač je prethodno uradio domaći zadatak, pa je imao spreman odgovor.

mitnikova poruka

Kad osiguravate informacije, ne oslanjajte se na sisteme za zaštitu mreže, niti na barijere. Usredsredite se na najranjivije mesto. Obično ćete otkriti da su ranjivi vaši ljudi.

„Dobro“, odvrati mu administrator sistema, „ubedili ste me.“

Bilo je tako jednostavno. Administrator sistema je proverio ime Džozefa Džounsa, njegovo odeljenje, broj zaposlenog, a „Džo“ je dao tačan odgovor na test pitanje. „Vaše korisničko ime biće isto kao i ono koje obično koristite, jbjones“, saopšti mu administrator sistema, „a ja vam dodeljujem podrazumevanu lozinku ‘promenime’.“

Analiza prevare

Pomoću nekoliko telefonskih poziva, za petnaestak minuta, napadaču je omogućen pristup mreži kompanije. Ta kompanija, kao i mnoge druge, primenjuje ono što ja nazivam *bezbednost poput bombone*; taj izraz su prvi put upotrebila dva istraživača iz laboratorije Bel, Stiv Belovin i Stiven Čezvik. Oni su takvo obezbeđenje opisali kao „tvrdu, krckavu ljusku s mekim srcem koje se topi“ – poput M&M bombone. Spoljna ljuska, odnosno zaštitna barijera, tvrdili su Belovin i Čezvik, ne predstavlja dovoljnu zaštitu, jer kad je uljez zaobiđe, interni računarski sistemi imaju slabu zaštitu koja se prosto topi. Uglavnom su nedovoljno zaštićeni.

Ova priča se uklapa u definiciju. Kad je dobio telefonski broj i nalog, napadač nije morao čak ni da se potruži da zaobiđe zaštitnu barijeru na Internetu; kad se povezao, lako je mogao da ugrozi većinu sistema u internoj mreži.

Iz svojih izvora saznajem da je jedan od najvećih svetskih proizvođača računarskog softvera prevaren na baš ovakav način. Pomislili biste da su administratori sistema u takvoj kompaniji obučeni da otkriju takvu vrstu prevare. Iz sopstvenog iskustva tvrdim da niko nije potpuno bezbedan od dovoljno pametnog i ubedljivog obmanjivača.

terminologija

BEZBEDNOST POPUT BOMBONE (engl. *candy security*) Ovaj izraz skovali su Belovin i Čezvik iz laboratorije Bel da bi opisali obezbeđenje čija je spoljašnjost, poput zaštitne barijere, čvrsta, ali je infrastruktura ispod nje slaba. Izraz aludira na M&M bombonu, koja ima čvrstu spoljnu ljusku i meko srce.

BEZBEDNOST UZ LOZINKU (engl. *speakeasy security*) Sistem bezbednosti koji se zasniva na tome da se zna gde se željena informacija nalazi i da se za pristup toj informaciji ili računarskom sistemu upotrebljava tajna reč ili ime.

BEZBEDNOST UZ LOZINKU

Nekada davno, u doba prohibicije, u noćnim klubovima je džin „iz kade“ tekao u potocima. Ko je hteo nešto da popije morao je da stane pred prava vrata i pokuca. Za nekoliko trenutaka otvorio bi se prozorčić na vratima, i iz njega bi provirilo grubo, zastrašujuće lice. Ako je posetilac znao o čemu se radi, izgovorio bi ime nekog redovnog posetioca tog mesta (često se govorilo „Poslao me je Džo“), na šta bi izbacivač otključao vrata i pustio ga.

Pravi trik je bio u tome da saznate gde se ilegalan bar nalazi, jer vrata nisu bila obeležena, a vlasnici nisu baš privlačili posetioce neonskim reklamama. U većini slučajeva, bilo je dovoljno samo pojaviti se na pravom mestu da biste ušli unutra. Isti nivo bezbednosti, nažalost, primenjuje se naširoko u poslovnom svetu; ja taj nivo nazivam *bezbednost uz lozinku*.

Video sam to u filmovima

Evo primera iz omiljenog filma kojeg će se mnogi setiti. U filmu *Tri dana kondora*, glavni lik, Tarner (kojeg igra Robert Redford), radi za malu istraživačku firmu koju upošljava CIA. Jednog dana on se vraća s ručka i nalazi sve svoje kolege ubijene. Ostaje mu da otkrije ko je to učinio i zašto, i sve vreme zna da loši momci, ko god bili, traže i njega.

Kasnije, Tarner uspeva da se domogne telefonskog broja jednog od loših momaka. Ali ko je ta osoba, i kako Tarner da sazna gde se nalazi?

Junak ima sreće. Po scenariju Dejvida Rejfiela, Tarner je u vojsci bio vezista, pa je poznavao tehnike i rad telefonskih kompanija. Kad je dobio telefonski broj lošeg momka, Tarner je tačno znao šta da radi. U scenariju, ta scena ide ovako:

TARNER DOBIJE SLOBODAN SIGNAL I UNESE DRUGI BROJ.

ZVRRR! ZVRRR! A potom:

ŽENSKI GLAS (KROZ FILTAR)

IAK, na telefonu gospođa Kolman.

TARNER (govori u slušalicu)

Ovde Harold Tomas, gospođu Kolman. Iz korisničke službe. Molim vas IAK za 202-555-7389.

ŽENSKI GLAS (KROZ FILTAR)

Samo trenutak, molim vas.

(*gotovo odmah*)

Lenard Etvud, Mekenzi Lejn 765, Čevi Čejs, Merilend.

Ako izuzmemo činjenicu da je scenarista pogrešno upotrebio pozivni broj za Vašington za adresu u Merilendu, vidite li šta se dogodilo?

Budući da je obučen kao vezista, Tarner je znao koji broj da okrene kako bi dobio IAK, biro za Imena i adrese klijenata. IAK postoji da bi olakšao rad instalaterima i drugom ovlašćenom osoblju telefonske kompanije. Instalater može da pozove IAK i da im telefonski broj. Službenik u IAK-u mu potom kaže ime i adresu osobe na čije ime je telefon.

Obmana službenika telefonske kompanije

U realnosti, telefonski broj IAK-a je strogo čuvana tajna. Iako su telefonske kompanije konačno shvatile u čemu je stvar, pa danas mnogo teže izdaju informacije, tada su bili obezbeđeni kao ilegalni klubovi – što stručnjaci za bezbednost nazivaju *bezbednost na osnovu tajnovitosti*. Smatrali su da je svako ko nazove IAK i vlada odgovarajućom terminologijom („Korisnička služba. Molim vas IAK za 555-1234“, na primer) osoba kojoj se sme dati informacija.

terminologija

BEZBEDNOST NA OSNOVU TAJNOVITOSTI (engl. *security through obscurity*) Nedelotvorna metoda računarske bezbednosti koja se zasniva na tome da se pojedinosti rada sistema (protokoli, algoritmi i interni sistemi) čuvaju u tajnosti. Ova vrsta bezbednosti oslanja se na pogrešno verovanje da niko osim grupe ljudi od poverenja neće moći da nadmudri sistem.

mitnikova poruka

Bezbednost na osnovu tajnovitosti nema *nikakvog* uticaja u slučaju obmane. Svaki računarski sistem na svetu koristi bar jedan čovek. Dakle, ako napadač uspe da prevari ljude koji upotrebljavaju sisteme, tajnost sistema ne igra nikakvu ulogu.

Niko se nije morao predstaviti, dati identifikacioni broj, niti lozinku koja se svakodnevno menja. Ako ste znali koji broj da pozovete i zvučali autentično, morali ste dobiti informacije.

Takvo pravilo i nije baš bilo primereno jednoj telefonskoj kompaniji. Njihovo jedino ulaganje u bezbednost bilo je da povremeno izmene telefonski broj, bar jednom godišnje. Uprkos tome, važeći broj su u svakom trenutku znali telefonski prevaranti, koji su uživali u iskorišćavanju ovog zgodnog izvora informacija, kao i u razmeni metoda prevare s ostalim varalicama. Trik sa biroom IAK bio je jedna od prvih stvari koje sam naučio kad sam u pubertetu počeo da se bavim telefonskim prevarama.

U poslovnom svetu i državnim institucijama, bezbednost uz lozinku još uvek preovlađuje. Verovatno je da se bilo koji iole vešt uljez može predstaviti kao ovlašćena osoba – dovoljno je da sakupi informacije o ograncima, ljudima i terminologiji kompanije. Često je dovoljno i manje od toga: na primer, jedan interni telefonski broj.

NEOPREZNI DIREKTOR

Iako su mnogi zaposleni u organizacijama nemarni, nezainteresovani, ili nesvesni opasnosti po bezbednosni sistem, očekivali biste da neko sa zvanjem direktora računskog centra preduzeća koje se nalazi među 500

najuspešnijih po proceni časopisa Fortune zna sve o najboljim bezbednosnim merama, zar ne?

Ne biste očekivali da upravnik računskog centra – neko ko pripada informatičkom odeljenju svoje firme – postane žrtva u prostoju i očiglednoj igri obmane. A *naročito* ne ako je obmanjivač tek nešto stariji od deteta, jedva da je izašao iz puberteta. Očekivanja ponekad varaju.

Prisluškivanje radio-prijemnika

Pre nekoliko godina mnogi su iz zabave podešavali radio-prijemnike na frekvencije lokalne policije ili vatrogasne službe, prisluškujući povremeno naelektrisanе razgovore o pljački banke koja je u toku, požaru u poslovnoj zgradi, ili jurnjavi, dok se događaji odvijaju. Radio-frekvencije koje koriste kriminalističke i vatrogasne službe nekada su se mogle naći u knjigama u obližnjoj knjižari; danas se njihovi spiskovi nalaze na Webu – frekvencije lokalnih, oblasnih, državnih i, u nekim slučajevima, čak i federalnih službi.

Naravno, nisu prisluškivali samo radoznalci. Provalnici koji pljačkaju prodavnicu usred noći mogli su da se uključe na određenu frekvenciju i čuju da li je već poslato policijsko vozilo. Dileri droge mogli su da proveravaju aktivnosti lokalnih agenata službe za suzbijanje narkotika. Palikuća je mogao još više da uživa – podmetnuo bi požar, a potom slušao gužvu na radiju dok vatrogasci pokušavaju da ga ugase.

Poslednjih godina, razvoj računarske tehnologije omogućio je šifrovanje glasovnih poruka. Budući da inženjeri pronalaze načina da mikročip učine sve moćnijim, počeli su da prave male, šifrovane radio-prijemnike za kriminalističku službu, koji su sprečili loše momke i radoznalce da se priključuju na njihove frekvencije.

Deni prisluškuje

Fanatik za skenere i vešt haker kog ćemo zvati Deni odlučio je da proba da se domogne izvornog koda supertajnog softvera za šifrovanje od jednog od glavnih proizvođača bezbednih radijskih sistema. Nadao se da će proučavanjem koda saznati kako da prisluškuje kriminalističku službu, a hteo je da primeni tu tehnologiju tako da ni najjače državne agencije ne mogu da prisluškuju njegove razgovore s prijateljima.

Ljudi poput Denija pripadaju svetu hakera iz senke svrstavaju se negde između radoznalih i sasvim bezazlenih, i onih opasnih. Oni imaju znanje stručnjaka i želju nestašnog hakera da provaljuje u sisteme i mreže radi

intelektualnog izazova i sopstvenog zadovoljstva u otkrivanju kako tehnologija radi. Njihovi elektronski upadi upravo su samo podvizi. Ti ljudi, ti bezazleni hakeri, nezakonito upadaju na lokacije iz čiste zabave i ushićenja što sebi mogu da dokažu da su sposobni. Oni ništa ne krađu, ne zarađuju novac svojim majstorijama; ne uništavaju datoteke, ne prekidaju mrežne veze, niti obaraju računarske sisteme. Samom činjenicom što su tamo, što uzimaju kopije dokumenata i pretražuju elektronsku poštu da bi pronašli lozinke iza leđa obezbeđenja i mrežnih administratora, oni vuku za nos ljude odgovorne za čuvanje tih podataka od ljudi poput njih. Preimućstvo igra veliku ulogu u njihovom osećaju zadovoljstva.

Deni, koji se uklapa u ovaj opis, želeo je da ispita pojedinosti najstrože čuvanog proizvoda u odabranoj kompaniji, samo da bi utolio svoju znatiželju i divio se pametnim novinama koje je proizvođač smislio.

Planovi proizvoda bili su, suviše je reći, u kompaniji pažljivo čuvana tajna, vredna i zaštićena kao i bilo šta drugo u posedu kompanije. Deni je to znao. I nije hajao nimalo. Konačno, bila je to samo jedna velika, bezimena firma.

Ali kako se domoći izvornog koda softvera? Kao što se ispostavilo, krađa „krunskih dragulja“ kompanijskog tima za bezbedne komunikacije pokazala se suviše jednostavnom, iako je kompanija jedna od onih koje koriste *dvostepenu identifikaciju*, gde se od ljudi traži da ne upotrebljavaju jedan, nego dva posebna identifikatora kako bi dokazali ko su.

Evo primera s kojim ste verovatno već upoznati. Kad vam stigne obnovljena kreditna kartica, trebalo bi da pozovete izdavača da biste im javili da je koverta stigla neotvorena. U uputstvu koje stiže s karticom uglavnom stoji da treba zvati *od kuće*. Kad pozovete, softver u kompaniji koja izdaje kreditne kartice analizira broj pozivaoca.

Računar upoređuje broj stranke koja zove s brojem koji se nalazi u bazi podataka o vlasnicima kartica. Pre nego što se službenik javi na telefon, na ekranu mu se prikazuju informacije iz baze podataka o klijentu. Tako službenik već zna da je poziv upućen iz klijentovog doma; to je jedan oblik identifikacije.

On potom odabere jedan od podataka iz prikazanih informacija o klijentu – najčešće matični broj, datum rođenja, ili majčino devojачko ime – i postavi klijentu odgovarajuće pitanje. Ako odgovor bude tačan, to je drugi oblik identifikacije – zasnovan na informacijama koje klijent mora znati.

terminologija

DVOSTEPENA IDENTIFIKACIJA (engl. *two-factor authentication*)

Upotreba dva različita identifikatora da bi se utvrdio identitet. Na primer, osoba bi se mogla identifikovati tako što pozove s poznate lokacije i zna lozinku.

U kompaniji koja proizvodi bezbedne radijske sisteme u našoj priči, svaki zaposleni s pristupom računaru imao je svoje uobičajeno korisničko ime i lozinku, ali je uz to imao i vremenski žeton, mali elektronski uređaj pod nazivom Secure ID. Postoje dve varijante takvih uređaja: jedni su upola manji od kreditne kartice, ali su malo deblji, dok su drugi dovoljno mali da se mogu nositi kao privezak za ključeve.

Nastala u svetu šifara, ova sprava ima prozorčić na kojem je prikazano šest cifara. Svaki šezdeset sekundi prikaz na ekranu se menja, i pojavljuje se nov šestocifren broj. Kada ovlašćena osoba treba da pristupi mreži s nekog mesta van firme, mora se identifikovati kao ovlašćeni korisnik tako što unese svoj tajni PIN kôd i cifre prikazane na vremenskom žetonu. Kad mu interni sistem odobri pristup, on se identifikuje pomoću korisničkog imena i lozinke.

Da bi se mladi haker Deni domogao izvornog koda za kojim je toliko žudeo, morao je da sazna nečije korisničko ime i lozinku (što i nije izazov za iskusnog obmanjivača), ali i da reši problem vremenskog žetona.

Nadigrati dvostepenu identifikaciju pomoću vremenskog žetona i tajnog korisničkog PIN koda zvuči kao izazov iz *Nemoguće misije*. Ali za obmanjivača, izazov je sličan onom s kojim se susreće pokeraš neuobičajeno obdaren za procenu suparnika. Uz malo sreće, kad sedne za sto, on pouzdano zna da će od stola ustati s velikom gomilom tuđeg novca.

Juriš na utvrđenje

Deni je počeo da radi domaći zadatak. Ubrzo je uspeo da sakupi dovoljno podataka da bi se predstavio kao službenik kompanije. Imao je ime zaposlenog, njegovo odeljenje, telefonski broj i identifikacioni broj, kao i ime pretpostavljenog i njegov telefon.

Tad je nastalo zatišje pred buru. Bukvalno. Prema razrađenom planu, Deniju je bila potrebna još jedna stvar pre nego što preduzme sledeći korak, a to nije mogao da naruči. Trebala mu je snežna oluja ili slična nepogoda koja bi sprečila radnike da dođu na posao.

Niko ko se nadao lošem vremenu u Južnoj Dakoti, gde je fabrika iz priče bila smeštena, nije zimi morao dugo da čeka. U petak uveče oluja je stigla. Sneg se brzo pretvorio u ledenu kišu, tako da su do jutra putevi bili presvučeni, opasnim slojem leda. Za Denija je to bila savršena prilika.

Telefonirao je firmi, zamolio da ga spoje s računarskim odeljenjem i dobio običnog radnika u informatičkom odeljenju, računarskog operatera koji se predstavio kao Rodžer Kovalski.

Predstavljajući se kao čovek zaista tamo zaposlen, čije je ime prethodno saznao, Deni reče: „Ovde Bob Bilings. Radim u timu za obezbeđenje komunikacija. Trenutno sam kod kuće i ne mogu da se dovezem do firme zbog oluje. Problem je u tome što moram da pristupim radnoj stanici i serveru od kuće, a ostavio sam svoj Secure ID na radnom stolu. Možete li ga uzeti? Ili neko drugi? Hoćete li mi očitati kôd kad bude trebalo da se uključim? Moj tim ima veoma važan rok i moram završiti posao kako god znam i umem. Nema načina da dođem do kancelarije – putevi kojima idem su suviše opasni.“

Operater je rekao: „Ne smem da napuštam računski centar.“

Deni na to odvrati: „Imate li vi Secure ID?“

„Postoji jedan u računskom centru“, rekao je. „Držimo ga za rad u hitnim slučajevima.“

„Čujte“, reče Deni, „možete li mi učiniti veliku uslugu? Kad bude trebalo da se priključim na mrežu, da li biste mi pozajmili svoj Secure ID? Samo dok ne postane bezbedno za vožnju?“

„Kako ste rekli da se zovete?“

„Bob Bilings.“

„Za koga radite?“

„Za Eda Trentona.“

„A, da, njega znam.“

Kad očekuje da će naići na tanak led, dobar obmanjivač istražuje više nego što je uobičajeno. „Radim na drugom spratu“, nastavi Deni. „Pored Roja Taker.“

To ime mu je takođe bilo poznato. Deni počeo ponovo da ga obrađuje. „Bilo bi mnogo lakše kad biste samo otišli do mog stola i doneli moj Secure ID.“

Deni je bio prilično siguran da momak neće nasesti na to. Kao prvo, verovatno neće želeći da napušta računski centar usred svoje smene da bi tumačio hodnicima i stepenicama do udaljenog dela zgrade. Nije hteo ni da čeprka po tuđem radnom stolu, narušavajući nečiji lični prostor. Ne, Deni se slobodno mogao opkladiti da ovaj to neće učiniti.

Kovalski nije hteo da odbije čoveka kome je bila potrebna pomoć, ali nije hteo ni da pristane, pa da se uvali u nevolje. Zato je zaobišao odluku: „Moraću da pitam šefa. Pričekajte.“ Spustio je slušalicu, a Deni je mogao da čuje kako podiže slušalicu drugog telefona, bira broj i objašnjava zahtev. Kovalski je zatim učinio nešto neobjašnjivo: on je garantovao za čoveka pod imenom Bob Bilings. „Poznajem ga“, reče on svom pretpostavljenom. „Radi za Eda Trentona. Možemo li da mu dopustimo da upotrebi Secure ID iz računskog centra?“ Deni, koji je držao slušalicu, bio je zapanjen tom izvanrednom i neočekivanom podrškom. Nije mogao da veruje svojim ušima, i sreći.

Nakon nekoliko trenutaka, Kovalski je ponovo uzeo vezu i kazao: „Moj pretpostavljeni želi da razgovara s vama lično“, i dao mu je čovekovo ime i telefonski broj.

Deni ga je nazvao i još jednom mu ispričao celu priču, dodajući pojedinosti o projektu na kom radi, te zašto njegov proizvodni tim mora to da završi do tog izuzetno važnog roka. „Bilo bi lakše kad bi neko otišao po moj identifikator“, reče. „Mislim da sto nije zaključan, trebalo bi da je tamo negde u levoj fioci.“

„Dobro“, kaza rukovodilac, „mislim da bismo mogli da vam dopustimo da koristite uređaj u računskom centru samo za ovaj vikend. Reći ću dežurnim momcima da vam pročitaju nasumično generisani kôd za pristup kad pozovete“, i dao mu je PIN kôd koji ide uz njega.

Čitavog vikenda, Deni je mogao da pristupa računarskom sistemu kompanije, čim pozove računski centar i zamoli ih da mu pročitaju šest cifara prikazanih na vremenskom žetonu.

Interni posao

Ušao je u računarski sistem kompanije, i šta sad? Kako da pronađe server na kom se nalazio traženi softver?

Već se pripremio za to.

Mnogi korisnici računara znaju za diskusione grupe, u kojima se upućuju pitanja, pronalaze odgovori, ili upoznaju virtuelni prijatelji istih interesovanja – za muziku, računare, ili bilo koju od stotina drugih tema.

Malo ko shvata da poruka poslana na lokaciju diskusione grupe ostaje dostupna na mreži godinama. Na lokaciji Google, na primer, trenutno se nalazi arhiva od sedam stotina miliona poruka, od kojih su neke stare dvadeset godina! Deni je istraživanje počeo na Web lokaciji <http://groups.google.com>.

Deni je potražio poruke koje sadrže reči „šifrovane radio-komunikacije“, kao i naziv kompanije, i pronašao je godinama staru poruku o toj temi od jednog zaposlenog. Poslata je još kad je firma počela da razvija taj proizvod, verovatno mnogo pre nego što su policija i federalne agencije razmišljale o tome da kodiraju radio-sigale.

U poruci se nalazio potpis pošiljaoca, s njegovim imenom i telefonskim brojem, pa čak i nazivom njegove radne grupe – tim za obezbeđenje komunikacija.

Deni je podigao slušalicu i okrenuo broj. Činilo se da je to nesiguran potez – da li on još radi u istoj organizaciji nakon toliko godina? Da li je na poslu tog olujnog vikenda? Telefon je zazvonio jedanput, dvaput, triput, a potom se začuo glas. „Ovde Skor“, reče.

Predstavljajući se da je iz informatičkog odeljenja kompanije, Deni je naveo Skota (na jedan od načina koje ste upoznali u ranijim poglavljima) da mu otkrije imena servera koji se koriste za razvoj. Moglo se očekivati da se na njima nalazi izvorni kôd za jedinstveni algoritam šifrovanja i upravljački softver smešten u čipu, koji se upotrebljava u bezbednim radijskim proizvodima.

Deni se približavao cilju, i bio je sve uzbuđeniji. Predosećao je navalu emocija, ushićenje koje bi uvek osetio kad bi uspeo u nečemu što samo mali broj ljudi može da postigne.

Pa ipak, posao još nije priveo kraju. Tokom vikenda uspeće da se priključi na kompanijsku mrežu kad god poželi, zahvaljujući predusretljivom upravniku računskog centra. Znao je i kojim serverima treba da pristupi. Ali kad se uključio, server terminala na koji se povezao nije mu dozvolio da pristupi razvojnim sistemima tima za bezbedne komunikacije. Mora da postoji interna barijera ili usmerivač koji štite računarske sisteme tog tima. Moraće da pronađe drugi ulaz.

Za sledeći potez trebalo je biti pomalo drzak. Deni se ponovo javio Kovalskom u računskom centru, požalio se da ne može da se poveže sa serverom, i rekao: „Trebalo bi da mi obezbedite nalog na jednom od računara u vašem odeljenju kako bih se povezao na svoj sistem preko Telnet.“

Upravnik je već odobrio da mu se kaže kôd za pristup vremenskom žetonu, pa ovaj novi zahtev nije delovao nerazumno. Kovalski mu je napravio privremeni nalog i lozinku na jednom od računara iz računskog centra, i rekao Deniju da ga ponovo pozove kad mu više ne bude potreban, da bi ga uklonio.

Kad se povezao preko privremenog naloga, Deni je uspeo da pristupi računarskim sistemima tima za bezbedne komunikacije. Nakon jednog sata rada na mreži u potrazi za tehničkim propustima, pomoću kojih bi mogao da pristupi glavnom razvojnom serveru, sreća mu se osmehnula. Čini se da administrator sistema ili mreže nije bio oprezan, te nije pratio najnovije vesti o bezbednosnim propustima u operativnom sistemu koji omogućavaju daljinski pristup. Ali Deni jeste.

Za kratko vreme pronašao je datoteke s izvornim kodom za kojima je tragao i preneo ih je na jednu lokaciju za elektronsku trgovinu na kojoj se nudio besplatan prostor. Čak i ako bi datoteke bile otkrivene na toj lokaciji, nikad se ne bi mogle povezati s njim.

Trebalo je povući još jedan konačan potez pre nego što se izgubi. Valjalo je metodično izbrisati tragove. Završio je pre kraja šoua Džeja Lenoa. Deni je bio veoma zadovoljan zbog obavljenog posla tog vikenda. Uza sve, nijednom nije morao lično da se izlaže riziku. Bilo je to očaravajuće uzbuđenje, bolje od skijanja na dasci ili skakanja iz aviona s padobranom.

Deni je te noći bio opijen, ne od viskija, džina, ili piva, nego od osećaja moći i uspeha dok je prebiraio po ukradenim datotekama, i došao do neuhvatljivog, izuzetno tajnog radio-softvera.

Analiza prevare

Kao i u prethodnoj priči, ova prevara je upalila samo zato što je jedan zaposleni bio isuviše spreman da prihvati, zdravo za gotovo, da je njegov sagovornik zaista kolega za kojeg se izdaje. Želja da se pomogne kolegi koji ima problem je, s jedne strane, deo mašinerije koja pokreće industriju, i deo onoga što čini osoblje jedne kompanije spremnijim na saradnju nego zaposlene neke druge firme. S druge strane, ta ljubaznost može biti glavna slaba tačka koju će obmanjivač pokušati da iskoristi.

Jedan oblik manipulacije koji je Deni upotrebio bio je sjajan – kad je zahtevao da neko uzme njegov vremenski žeton sa stola, stalno je ponavljao da bi hteo da neko ode i donese ga. Takva se naredba daje psu i niko ne želi da mu se komanduje da ide i donese nešto. Tom jednom rečju, Deni je obezbedio da njegov zahtev bude odbijen, te da se neko drugo rešenje prihvati, a upravo je to i želeo.

Deni je obmanuo operatera u računskom centru, Kovalskog, tako što je pominjao imena ljudi koje je on slučajno poznavao. Ali zašto bi njegov *pretpostavljeni* – ni manje, ni više nego upravnik informatičkog odeljenja – dozvolio nekoj nepoznatoj osobi da pristupi internoj računarskoj mreži? Zato što poziv u pomoć može biti moćno, ubedljivo oružje u arsenalu obmanjivača.

mitnikova poruka

U ovoj priči je pokazano da vremenski žetoni i slični oblici identifikacije nisu odbrana od lukavih metoda obmane. Jedina odbrana je savestan zaposleni koji prati bezbednosna pravila i razume kako drugi mogu zlonamerno da utiču na njega.

Da li bi se nešto tako ikada moglo dogoditi u *vašoj* kompaniji? Da li se već desilo?

KAKO SPREČITI PREVARU

Čini se da se u ovim pričama često ponavlja opis jednog postupka. Napadač pripremi teren tako da može da se spolja poveže na računarsku mrežu kompanije, a osoba koja mu u tome pomaže ne primeni odgovarajuće mere i proveru da li je sagovornik zaista zaposleni i da li mu je odobren pristup? Zašto se tako često vraćam na tu temu? Zato što je to zaista bitan činilac mnogih obmana. Napadaču je to najlakši način da dođe do cilja. Zašto bi provodio sate pokušavajući da provali u mrežu, kad to može da uradi jednim telefonskim pozivom?

Jedna od najmoćnijih metoda obmanjivanja je pretvaranje da vam treba pomoć – i taj pristup napadači često koriste. Ne želite da sprečite zaposlene da budu predusretljivi prema saradnicima i klijentima, pa ih zato morate naoružati posebnim postupcima za utvrđivanje identiteta koje će primeniti

kad bilo ko zatraži pristup računaru ili poverljivim informacijama. Na taj način mogu biti predusretljivi sa onima koji zaslužuju pomoć, a istovremeno će zaštititi važne podatke i računarske sisteme.

U bezbednosnim pravilima mora biti detaljno opisano koje metode se koriste za proveru identiteta u različitim okolnostima. U poglavlju 16 nalazi se detaljan spisak postupaka, ali evo nekih osnovnih ideja koje valja imati na umu:

- Dobar način da se proveru identitet osobe koja postavlja zahtev jeste da se nazove telefonski broj te osobe koji je naveden u telefonskom imeniku kompanije. Ako je osoba koja vam je postavila zahtev zapravo obmanjivač, pomoću tog poziva ćete ili moći da razgovarate s pravom osobom dok uljez čeka na vezi, ili će se uključiti glasovna poruka tog zaposlenog, pa ćete moći da mu čujete glas i uporedite ga s napadačevim.
- Ako se u vašoj firmi za utvrđivanje identiteta koriste identifikacioni brojevi zaposlenog, onda se s njima mora ophoditi kao s poverljivim informacijama, koje se brižljivo čuvaju i ne daju nepoznatim osobama. Isto važi i za sve druge interne identifikatore, poput internih telefonskih brojeva, kontnih brojeva odeljenja, pa čak i adresa elektronske pošte.
- Na kompanijskoj obuci trebalo bi da se svima obrati pažnja na činjenicu da se nepoznate osobe često prihvataju kao pravi zaposleni samo zato što zvuče autoritativno ili tako da se razumeju u poslove firme. To što neko poznaje kompanijske procedure ili koristi internu terminologiju nije razlog da se pretpostavi da njegov identitet ne treba potvrditi na druge načine.
- Službenici obezbeđenja i administratori sistema ne smeju se usredsrediti samo na to koliko se svi *ostali* pridržavaju bezbednosnih pravila. I oni sami moraju poštovati ista pravila i procedure.
- Lozinke i tome slično se, naravno, nikada ne smeju obelodanjivati, ali je ta zabrana još važnija kada su u pitanju vremenski žetoni i drugi sigurni oblici utvrđivanja identiteta. Zdrav razum bi trebalo da nam kaže da se saopštavanjem bilo kakve slične informacije narušava čitav smisao instaliranja zaštitnog sistema u kompaniji. Ako se takve informacije objavljuju, onda nema odgovornosti. U slučaju da se dogodi bezbednosni problem ili se nešto pokvari, nećete moći da utvrdite ko je odgovoran za to.

poglavlje

7

Lažne Web lokacije i opasni prilozi

kaže se da u životu ništa nije besplatno. Ipak, obmana da se nešto nudi besplatno i dalje privlači kupce kako u zakonitim („Pričekajte samo – ima još nešto! Pozovite odmah i dodaćemo vam komplet noževa i aparat za kokice!“), tako i u nezakonitim radnjama („Kupite hektar močvare u Floridi i dobićete drugi besplatno!“).

Skoro svi toliko želimo da dobijemo nešto besplatno, da nas to može ometi pri proceni ponude ili obećanja. Poznato nam je upozorenje: „kupče, čuvaj se“, ali je vreme da poslušamo još jedno upozorenje: čuvajte se priloženih datoteka uz neočekivane elektronske poruke, kao i besplatnog softvera. Pametan napadač će upotrebiti gotovo bilo koje sredstvo da provali u računarsku mrežu, uključujući i vašu prirodnu želju da dobijete besplatan poklon. Evo nekoliko primera.

„ZAR NE BISTE ŽELELI BESPLATAN...?“

Baš kao što su virusi prokletstvo ljudskog roda i lekara od kad je sveta i veka, i računarski virus (primereno nazvan tako) predstavlja slično prokletstvo za korisnike tehnologije. Najistaknutiji računarski virusi dospevaju u centar pažnje i nanose najviše štete. Takve viruse prave računarski vandali.

- Kao što stalno ponavljam, zaposleni se moraju upoznati sa strategijama i metodama obmanjivanja da bi pažljivo analizirali zahteve koji im se postavljaju. Razmislite o tome da uobičajeni deo bezbednosne obuke bude igranje scena iz stvarnog života, kako bi zaposleni bolje shvatili postupak obmanjivanja.



Računarski vandali, tj. računarski zaludenici koji su postali zlobni, trude se da pokažu kako su pametni. Ponekad su njihovi napadi poput obreda inicijacije, sa namerom da zadive starije i iskusnije hakere. Ti ljudi prave crve ili virus motivisani namerom da nanese štetu. Ako njihovo delo uništi datoteke, pokvari čvrste diskove i pošalje se hiljadama ljudi koji ništa ne sumnjaju, vandali se ponose svojim dostignućima. Kad virus učini toliko štete da novine pišu o njemu i pominju ga u vestima na televiziji, vandal je još zadovoljniji.

Mnogo knjiga je napisano o vandalima i njihovim virusima. Postoje softverski programi i kompanije koje nude zaštitu, pa se ovde nećemo baviti tehničkom odbranom od napada. Nas trenutno manje interesuje destruktivno ponašanje vandala, a više naponi njegovog daljeg rođaka, obmanjivača.

Stiglo je s elektronskom poštom

Verovatno svakodnevno primete neželjene elektronske poruke s reklamama ili besplatnim ponudama. Znači o čemu govorim. U njima se nude saveti za investiranje, popusti na računare, televizori, kamere, vitamini, putovanja, ponude za kreditne kartice koje vam ne trebaju, uređaj pomoću kojeg ćete besplatno gledati televizijske kanale koji se inače plaćaju, načini da poboljšate zdravlje ili seksualni život i tako dalje.

Povremeno se u vašem elektronskom sandučetu pojavi ponuda za nešto što vam skrene pažnju. To može biti besplatna igra, ponuda fotografija vaše omiljene zvezde, besplatan program za kalendar, ili jeftin server koji će zaštititi vaš računar od virusa. Šta god ponuda bila, elektronska poruka vas upućuje na preuzimanje datoteke s dakonijama koje želite da isprobate.

Ili možda primite poruku čiji naslov glasi „Done, nedostaješ mi“, ili „Ana, zašto mi nisi pisala“, ili „Zdravo, Time, evo seksi fotografije koju sam ti obećao“. To ne može biti neželjena reklamna poruka, pomislite, jer se u njoj nalazi vaše ime i zvuči tako prisno. Zato otvarate priloženu datoteku da biste videli fotografiju ili pročitali poruku.

Svi ti postupci – preuzimanje softvera o kojem ste saznali iz reklamne elektronske poruke, pritiskanje mišem veze koja vas odvodi na lokaciju za koju niste nikada čuli, ili otvaranje priložene datoteke koju vam je poslao neko koga ne poznajete – mogu vas uvaliti u nevolje. Svakako, uglavnom dobijate upravo ono što ste očekivali ili, u najgorem slučaju, nešto razočaravajuće ili uvredljivo, ali bezopasno. Ipak, ponekad je ono što dobijete delo vandala.

Slanje štetnog softvera vašem računaru samo je mali deo napada. Napadač mora da vas ubedi da učitate priloženu datoteku kako bi napad uspeo.

Najopasniji oblici štetnog koda – crvi kao što su Ljubavno pismo, Sir-Cam, i Ana Kurnikova, pored ostalih – oslanjali su se na tehniku obmane i na iskorišćavanje naše želje da dobijemo nešto besplatno. Crv stiže u obliku datoteke priložene uz elektronsku poruku u kojoj se nudi nešto što vas dovodi u iskušenje, poput poverljivih informacija, besplatne pornografije ili, veoma lukavo, kao poruka u kojoj piše da je priložena datoteka račun za neki skup predmet koji ste navodno naručili. Ovo poslednje lukavstvo vas navede da otvorite priloženu datoteku iz straha da vam je preko kreditne kartice naplaćeno nešto što niste naručili.

napomena

Jedna vrsta programa poznata u računarskom podzemlju kao RAT, ili Remote Access Trojan (trojanski konj za daljinski pristup), omogućava napadaču pun pristup vašem računaru, baš kao da sedi za vašom tastaturom!

Zapanjujuće je koliko ljudi se upeca na ove trikove; čak i kad im se stalno iznova govori o opasnostima koje nosi otvaranje priloženih datoteka, svest o opasnosti vremenom izbledi, pa svako od nas postaje ranjiv.

Kako primetiti štetan softver

Druga vrsta štetnog softvera instalira na vaš računar program koji radi bez vašeg znanja ili odobrenja, ili obavlja neke zadatke a da vi toga niste ni svesni. Štetan softver može delovati sasvim bezazleno, i može biti čak i u obliku Word dokumenta, PowerPoint prezentacija, ili bilo kog drugog dokumenta koji sadrži makroe. Takav softver, po pravilu, bez vašeg odobrenja instalira neke programe. Na primer, takav softver može biti verzija trojanskog konja o kojem je bilo reči u poglavlju 6. Kad se taj softver instalira na računar, može napadaču poslati podatke o svakom pritisku tastera, uključujući i sve lozinke i brojeve kreditnih kartica koji se unose s tastature.

Postoje još dve vrste zlonamernog softvera, koje će vas možda zapanjiti. Jedan napadaču može da pošalje svaku reč koju izgovorite u dometu vašeg računarskog mikrofona, čak i kad mislite da je mikrofonski isključen. Štaviše,

ako na računar imate priključenu Web kameru, koristeći varijaciju ove tehnike napadač može i da vidi sve što se odvija ispred računara, čak i kad mislite da je kamera isključena, i danju, i noću.

terminologija

ŠTETAN SOFTVER (engl. malware) To je izraz za softver napravljen s lošim namerama, tj. računarski program kao što je virus, crv, ili trojanski konj, koji izvršava štetne zadatke.

mitnikova poruka

Čuvajte se zaludenika, čak i kad poklone nose, inače će vašu kompaniju snaći ista sudbina kao i Troju. Zaštitite se da biste izbegli viruse i crve.

Haker s čudnim smislom za humor mogao bi da pokuša da na vaš računar instalira programčić napravljen da vas užasno nervira. Na primer, možda bi vam se CD uređaj stalno otvarao, ili bi vam se datoteka na kojoj radite stalno smanjivala. Ili bi reprodukovao audio datoteku vriska najglasnije što može usred noći. Ništa od toga nije smešno kad pokušavate da se naspavate ili da obavite posao... ali bar ne nanosi trajniju štetu.

PORUKA OD PRIJATELJA

Situacija može biti još gora, uprkos oprezu. Zamislite samo! Odlučili ste da ne rizikujete. Više nećete preuzimati nikakve datoteke osim sa bezbednih lokacija koje poznajete i u koje imate poverenja, kao što su SecurityFocus.com ili Amazon.com. Više ne pritiskate mišem veze u elektronskim porukama koje dolaze iz nepoznatog izvora. Nikako ne otvarate neočekivane datoteke priložene uz elektronsku poštu. I proveravate prozor čitača Web-a da biste se uverili da postoji sigurnosni simbol na svakoj lokaciji za elektronsku trgovinu koju posetite.

A onda jednog dana dobijete elektronsku poruku s prilogom od prijatelja ili poslovnog saradnika. Ne može biti ništa zlonamerno ako dolazi od nekog koga dobro poznajete, zar ne? Pogotovo zato što biste znali koga da okrivite ako vam se podaci na računaru oštete.

Otvorite priloženu datoteku, a onda... BUM! Upravo vas je pogodio crv ili trojanski konj. Zašto bi vam neko koga poznajete to učinio? Zato što nije sve onako kakvim se čini. Čitali ste o tome: crv se instalira na nečiji računar, a potom se pošalje elektronskom poštom svima u adresaru te osobe. Svako dobije elektronsku poruku od nekoga koga poznaje i veruje mu, a u svakoj od tih poruka nalazi se crv, koji se umnožava kao talasi od kamena bačenog u mirno jezero.

Ova tehnika je uspešna jer ubija dve muve jednim udarcem: virus može da se umnoži i pošalje drugim žrtvama koje ništa ne sumnjaju, i čini se da poruka potiče od poznate osobe.

mitnikova poruka

Čovek je izmislio mnoge divne stvari koje su izmenile svet i naš način života. Ali neko će uvek naći načina da za sopstvene ciljeve upotrebi svaku korisnu tehnologiju bio to računar, telefon, ili Internet.

Tužna je činjenica da možete dobiti elektronsku poruku od nekoga ko vam je blizak, a ipak se pitati da li je bezbedno da je otvorite.

VARIJACIJE NA TEMU

U eri Interneta postoji prevara u kojoj vas pogrešno upute na Web lokaciju koja nije ono što ste očekivali. To se redovno dešava, u raznim oblicima. Kao ilustraciju navodimo sledeći primer zasnovan na stvarnom događaju.

Srećan Božić...

Edgar, penzionisani prodavac osiguranja primio je jednog dana elektronsku poruku od firme PayPal, koja nudi brz i lak način plaćanja na Webu. Ta usluga je posebno zgodna kad osoba koja živi u nekom udaljenom delu zemlje (ili sveta) kupuje nešto od osobe koju ne poznaje. PayPal naplaćuje iznos pomoću kupčeve kreditne kartice i prebacuje novac direktno na račun prodavca.

Edgar je sakupljao starinske staklene tegle i stalno je trgovao preko Web lokacije za aukcije eBay. Često je koristio usluge preduzeća PayPal, ponekad i više puta nedeljno. Zato je bio zainteresovan kad je, u vreme praznika 2001. godine, primio elektronsku poruku za koju se činilo da dolazi od

firme PayPal, u kojoj mu se nudi nagrada zato što je obnovio svoj račun kod njih. U poruci je pisalo:

Srećni praznici, dragi korisniče firme PayPal;

Kako se Nova godina približava i svi se pripremamo da još jednu godinu ostavimo za sobom, PayPal bi želeo da vam pokloni 5 dolara. Uplat ćemo ih na vaš račun!

Da biste dobili svih 5 dolara, ažurirajte svoje podatke na našoj bezbednoj lokaciji do 1. januara 2002. Svaka godina donosi mnogo promena, pa ćete nam ažuriranjem svojih podataka omogućiti da vama i ostalim korisnicima naših usluga i dalje obezbeđujemo naše cenjene usluge, kao i da uvek imamo ažurnu evidenciju!

Da biste odmah ažurirali svoje podatke i primili 5 dolara na svoj račun kod firme PayPal, pritisnite ovu vezu:

<http://www.paypal-secure.com/cgi-bin>

Hvala vam što koristite PayPal.com i pomažete nam da se razvijemo i postanemo najveći u svom poslu!

Od srca vam želimo srećnu Novu godinu i božićne praznike!

Tim firme PayPal

Napomena o Web lokacijama za elektronsku trgovinu

Verovatno poznajete ljude koji nerado kupuju robu na Webu, čak i od poznatih kompanija kao što su Amazon i eBay, ili s Web lokacija Old Navy, Target, ili Nike. Skoro da imaju pravo što su sumnjičavi. Ako vaš čitač Weba koristi 128-bitno šifrovanje, podaci koje šaljete do bilo koje bezbedne lokacije sa vašeg računara odlaze šifrovani. Ti podaci se mogu dešifrovati uz mnogo muke, ali se to verovatno ne može učiniti u nekom razumnom vremenskom intervalu, osim, možda, u američkoj Agenciji za nacionalnu bezbednost (a ta agencija, koliko nam je poznato, do sada nije pokazala interesovanje da krađe brojeve kreditnih kartica od građana, niti da pokuša da otkrije ko naručuje pornografske filmove ili seksi donje rublje).

Te šifrovane datoteke bi, zapravo, mogao da dešifruje ko god ima vremena i sposobnosti. Ali, u suštini, ko je tako glup da se toliko muči kako bi ukradio broj samo *jedne* kreditne kartice, kad mnoge kompanije za elektronsku trgovinu greše tako što sve finansijske podatke o svojim klijentima čuvaju u bazama podataka u nešifrovanom obliku. Da stvar bude gora, neke kompanije nikad ne zamene podrazumevanu lozinku administratora SQL baze podataka. Kada su instalirali softver lozinka je bila prazna, i dan danas je ista. Dakle, sadržaj baze podataka je dostupan svakom na Internetu ko odluči da se poveže na server baza podataka. Takve lokacije se stalno napadaju i informacije se zaista krađu, a niko da izvuče pouku.

S druge strane, isti ti ljudi koji ne kupuju na Internetu jer se plaše da će neko ukrasti podatke o njihovim kreditnim karticama, bez problema kupuju tom istom karticom u prodavnicama građevinskog materijala, plaćaju ručak, večeru ili pića – čak i u sumnjivim barovima i restoranima u koje ne bi odveli ni rođenu majku. S tih mesta se priznanice za kreditnu karticu stalno krađu, ili se vade iz kanti za otpatke u stražnjim uličicama. Svaki beskrupulozni službenik ili konobar može da zabeleži vaše ime i podatke o kartici, ili da upotrebi čitač kartica koji se može naći svugde na Internetu.

Kupovina na Webu nosi svoje opasnosti, ali je verovatno isto toliko bezbedna kao i kupovina u prodavnici građevinskog materijala. A izdavači kreditnih kartica vam nude istu zaštitu i kada koristite karticu na Webu.

Dakle, moje mišljenje je da je strah od kupovine na Webu samo još jedna nepotrebna briga.

Edgar nije primetio nijedan od znakova koji bi mu nagoveštavali da nešto nije u redu s njegovom elektronskom porukom (na primer, tačka i zarez nakon uvodnog reda, i čudan tekst o „našoj cenjenoj usluzi korisnicima naših usluga“). Pritisnuo je vezu, uneo tražene podatke – i zavalio se, čekajući da mu se na sledećem izvodu s računa kreditne kartice pokaže priliv od pet dolara. Umesto toga, pojavio se spisak naplata za stvari koje nikada nije kupio.

Analiza prevare

Edgar je postao žrtva uobičajene obmane na Internetu. Ona se javlja u nekoliko vidova. U jednom od njih (o čemu se više govori u poglavlju 9) napadač napravi lažnu stranu za prijavljivanje koja izgleda kao prava. Razlika je u tome što se pomoću lažne strane ne pristupa očekivanom računarskom sistemu, već se uneto korisničko ime i lozinka šalju hakeru.

Edgar je naseo na obmanu. Prevaranti su registrovali Web lokaciju pod nazivom „paypal-secure.com“, koja zvuči kao da je bezbedna strana na stvarnoj lokaciji firme PayPal, ali nije. Kad je uneo podatke, napadači su dobili upravo ono što su i želeli.

mitnikova poruka

Kad god posećujete neku lokaciju na kojoj se traže lični podaci, uvek proverite da je veza zaštićena i šifrovana – iako ni to nije savršeno bezbedno (nijedna zaštita nije). Što je još važnije, nemojte automatski pristiskati opciju Yes u okvirima za dijalog koji možda upućuju na problem sa bezbednosnim sistemom, poput nevažećeg, zastarelog, ili opozvanog digitalnog sertifikata.

JOŠ NEKE VARIJACIJE

Koliko drugih načina još postoji da se korisnici računara na prevaru navedu na neku lažnu Web lokaciju i tamo obelodane svoje poverljive informacije? Pretpostavljam da niko nema pravi, tačan odgovor, ali „previše“ će poslužiti svrsi.

Veza koje zapravo nema

Jedan trik se stalno javlja: pošalje se elektronska poruka u kojoj se nudi neki primamljiv razlog da posetite lokaciju, direktna veza s njom. Ali, ta veza vas ne vodi do ponuđene lokacije, jer ona samo liči na pravu vezu do nje. Evo još jednog primera koji je zaista primenjen na Internetu, ponovo zloupotrebom imena PayPal:

www.PayPal.com

Na prvi pogled, čini se da piše PayPal. Čak i ako žrtva primeti, možda pomisli da je to samo mala greška u tekstu zbog koje slovo „l“ iz reči Pal izgleda kao „i“. I ko bi na prvi pogled primetio da je u adresi:

www.PayPal.com

upotrebljen broj 1 umesto malog slova L? Dovoljno ljudi previdi ovakve slovne greške i druge omaške, pa je ova prevara stalno popularna među kradljivcima kreditnih kartica. Lažna lokacija izgleda poput originalne, pa korisnici bezbrižno unesu podatke o kreditnim karticama. Da bi se izvela takva obmana, napadač samo treba da registruje lažno ime domena, pošalje elektronske poruke, i čeka da se lakovernici pojave, spremni da budu obmanuti.

Sredinom 2002. primio sam elektronsku poruku, navodno samo jednu od mnogih, na kojoj je pisalo da je poslata sa adrese Ebay@ebay.com. Poruka je prikazana na slici 8.1.

msg: Dear eBay User,

It has become very noticeable that another party has been corrupting your eBay account and has violated our User Agreement policy listed:

4. Bidding and Buying

You are obligated to complete the transaction with the seller if you purchase an item through one of our fixed price formats or are the highest bidder as described below. If you are the highest bidder at the end of an auction (meeting the applicable minimum bid or reserve requirements) and your bid is accepted by the seller, you are obligated to complete the transaction with the seller, or the transaction is prohibited by law or by this Agreement.

You received this notice from eBay because it has come to our attention that your current account has caused interruptions with other eBay members and eBay requires immediate verification for your account. Please verify your account or the account may become disabled. Click Here To Verify Your Account – http://error_ebay.tripod.com

Designated trademarks and brands are the property of their respective owners. eBay and the eBay logo are trademarks of eBay Inc.

Slika 8.1: Veze u bilo kojoj elektronskoj poruci valja koristiti oprezno.

Žrtve koje su mišem pritisnule datu vezu upućene su na Web lokaciju koja izgleda sasvim slično lokaciji eBay. Zapravo, strana je bila dobro dizajnirana, sa autentičnim logotipom kompanije eBay, a opcije „Browse“, „Sell“ i druge veze za navigaciju odvele bi korisnika do prave lokacije firme eBay, ako ih pritisne mišem. U donjem desnom uglu nalazio se i bezbednosni logotip. Da bi prevario i oštroomne žrtve, dizajner je čak upotrebio i HTML šifrovanje, čime je prikrrio lokaciju na koju se korisnički podaci zapravo šalju.

Bio je to savršen primer računarske obmane s lošim namerama. Pa ipak, nije bio bez mane.

Elektronska poruka nije bila dobro napisana; ljudi odgovorni za ovakve obmane nikada ne angažuju profesionalne lektore, i to se uvek vidi. Takođe, svako ko zaista obrati pažnju posumnjao bi zašto eBay traži posetiočeve podatke iz firme PayPal; nema razloga zašto bi eBay od korisnika tražila ove lične podatke u vezi s drugom firmom.

Svako ko se razume u Internet verovatno bi prepoznao da hiperveza nije povezana sa domenom kompanije eBay, nego sa domenom tripod.com, koji nudi besplatnu uslugu ugošćavanja lokacije na Webu. To je bio očiti znak da je ta elektronska poruka zlonamerna. Pa ipak, kladim se da je mnogo ljudi unelo svoje podatke, uključujući i brojeve kreditnih kartica.

napomena

Zašto se dozvoljava registrovanje lažnih ili nepodesnih imena domena? Zato što prema trenutnom zakonu i pravilima upotrebe Mreže, svako može da registruje bilo koje ime koje nije već upotrebljeno.

Kompanije pokušavaju da se bore protiv upotrebe lažnih, a sličnih adresa, ali pogledajte samo s čime se hvataju u koštac. General Motors je podneo tužbu protiv kompanije koja se registrovala pod nazivom f**kgeneralmotors.com (odgovarajuća slova umesto zvezdica), i čija je hiperveza vodila do Web lokacije General Motorsa. GM je izgubio parnicu.

Budite oprezni

Svaki korisnik Interneta mora biti oprezan, i svesno odlučivati o tome kada je ispravno uneti lične podatke, lozinke, brojeve računa, PIN kodove i tome slično.

Koliko ljudi poznajete koji bi vam mogli reći da li neka strana na Internetu odgovara bezbednosnim zahtevima? Koliko zaposlenih u vašoj kompaniji znaju šta da traže?

Svako ko koristi Internet trebalo bi da prepozna sličicu katanca koja se često pojavljuje negde na Web strani. Trebalo bi da znaju da je lokacija označena kao bezbedna kad je katanac zatvoren. Kad je otvoren, ili takve sličice nema, Web lokacija nije pouzdana, i svi podaci koji se na nju prenose mogu se prisluškivati – odnosno, nisu šifrovani.

Napadač koji uspe da iskoristi privilegije administratora na kompanijskom računaru, može izmeniti ili zakrpati kôd operativnog sistema tako da utiče na korisnikovo viđenje onoga što se zaista događa. Na primer, čitač Weba se može izmeniti tako da se isključi provera ispravnosti digitalnog sertifikata. Ili se čitav sistem može promeniti pomoću administratorskog paketa, koji otvara *mala vrata* na nivou operativnog sistema.

Bezbedna veza identifikuje lokaciju kao pouzdanu i šifrira podatke koji se prenose, tako da napadač ne može da iskoristi ukradene informacije. Možete li verovati bilo kojoj Web lokaciji, čak i onoj koja upotrebljava bezbednu vezu? Ne, zato što vlasnik lokacije možda ne instalira ažurne bezbednosne zakrpe, ili pak ne insistira dovoljno na tome da korisnici ili administratori poštuju bezbednosna pravila. Zato ne možete podrazumevati da je svaka navodno bezbedna lokacija otporna na napade.

terminologija

MALA VRATA (engl. *back door*) Tajno mesto kroz koje se može dospeti do korisnikovog računara, a da on za to ne zna. Koriste ih i programeri dok razvijaju softver, da bi mogli da poprave greške u programu.

Bezbedan HTTP (engl. *hypertext transfer protocol* – protokol za prenos hiperteksta) ili SSL (engl. *secure sockets layer* – sloj bezbedne veze) obezbeđuju automatski mehanizam u kom se koriste digitalni sertifikati i za šifrovanje komunikacije i za identifikaciju (da bi vas uverili da ste uspostavili vezu s pravom Web lokacijom). Ipak, taj mehanizam ne može da zaštiti korisnike koji ne obraćaju pažnju na to da li je u adresnom polju zaista prikazana tačna adresa lokacije kojoj pokušavaju da pristupe.

Još jedan bezbednosni problem, koji se uglavnom ignoriše, ispoljava se u vidu poruke upozorenja u kojoj piše nešto ovako: „Ova lokacija nije bezbedna, ili je bezbednosni sertifikat zastareo. Da li ipak želite da odete na lokaciju?“ Mnogi korisnici ne razumeju poruku pa, kad se ona pojavi, pritisnu dugme OK ili Yes i nastave da rade, nesvesni da su možda na tankom ledu. Upozoravam vas – nikada ne unosite poverljive informacije poput adrese ili broja telefona, kreditne kartice ili bankovnog računa, niti bilo šta drugo što želite da sačuvate u tajnosti na Web lokaciju koja ne upotrebljava bezbednosni protokol.

Tomas Džeferson je rekao da je za održavanje slobode potreban „večan oprez“. Ništa manje od toga nije potrebno ni za održavanje privatnosti i bezbednosti u društvu koje koristi informacije kao valutu.

Upoznajte viruse

Evo posebne napomene o antivirusnom softveru – takav softver je izuzetno važan za kompanijski intranet, kao i za svakog zaposlenog koji koristi računar. Osim toga što im se antivirusni softver instalira, korisnici moraju da ga uključe (što mnogi ne vole jer se neminovno usporavaju neke funkcije računara).

Što se tiče antivirusnog softvera, treba imati na umu još jedan bitan postupak – opisi virusa moraju biti ažurni. Ukoliko vaša kompanija distribuira svim korisnicima softver ili ažurirane verzije preko mreže, svako mora biti odgovoran za preuzimanje najnovijih opisa virusa. Moj predlog je da svako podesi programe tako da se opisi novih virusa automatski ažuriraju svakodnevno.

terminologija

SLOJ BEZBEDNE VEZE (engl. *secure sockets Layer*) Protokol razvijen u firmi Netscape koji nudi identifikaciju klijenta i servera radi bezbedne komunikacije na Internetu.

Jednostavno rečeno, ranjivi ste ukoliko se opisi virusa ne ažuriraju redovno. Čak i kad se ažuriraju, ipak niste sasvim zaštićeni od virusa i crva koje proizvođači antivirusnog softvera još nisu registrovali, ili još nisu objavili datoteku sa šemom za njihovo otkrivanje.

Svi zaposleni koji daljinski pristupaju računarima preduzeća sa svojih prenosivih ili kućnih računara trebalo bi, u najmanju ruku, da na tim računarima imaju ažuriran antivirusni softver i ličnu zaštitnu barijeru. Iskusan napadač će sagledati sliku u celini kako bi otkrio najslabiju tačku, i tu će napasti. Kompanija je odgovorna za to da redovno podseća zaposlene na lične zaštitne barijere i ažurirani, aktivni antivirusni softver, jer se ne može očekivati da će svi zaposleni, upravnici, prodavci, i drugi koji su udaljeni od informatičkog odeljenja zapamtiti koja opasnost prethodi nezštićenih računara.

Osim toga, iskreno preporučujem manje uobičajene, ali ne manje važne, softverske pakete koji štite od napada trojanskih konja – takozvane anti-trojanske programe. Dok ovo pišem, dva poznatija programa su The Cleaner (www.moosoft.com) i Trojan Defense Sweep (www.diamondcs.com.au).

Na kraju, verovatno najbitnija poruka o bezbednosti upućena kompanijama koje ne proveravaju viruse u elektronskoj pošti na sopstvenim serverima glasi: budući da smo svi obično zaboravni ili nehajni u vezi s onim što se čini sporednim u obavljanju posla, zaposleni se moraju stalno podsećati, na razne načine, da ne otvaraju priloge elektronskih poruka osim ako nisu sigurni da potiču od pouzdane osobe ili organizacije. Rukovodstvo takođe mora da podseća osoblje da koriste aktivan antivirusni i anti-trojanski softver, koji nudi važnu zaštitu od pošte koja je naizgled bezazlena, a može sadržati razorno oružje.

poglavlje

8

Iskorišćavanje sažaljenja, osećaja krivice i zastrašivanja

Kao što će biti reči u poglavlju 15, obmanjivači psihološki utiču na žrtve kako bi ih naveli da pristanu na njihove zahteve. Vešti obmanjivači veoma stručno planiraju obmane u kojima se poigravaju tuđim emocijama, poput straha, uzbuđenja, ili osećaja krivice. Izazivaju ih pomoću psiholoških mehanizama koji navode ljude da odgovaraju na zahteve bez temeljne analize svih dostupnih informacija.

Svi želimo da izbegnemo teške situacije, a to želimo i drugima. Na osnovu tog pozitivnog impulsa, napadač može da igra na kartu nečijeg sažaljenja, izazivanja osećaja krivice, ili zastrašivanja.

Evo nekih srednjoškolskih lekcija o uobičajenim metodama iskorišćavanja emocija.

POSETA STUDIJU

Jeste li ikada primetili kako neki ljudi prođu pored čuvara na vratima, recimo, balske dvorane hotela u kojoj se odvija neki sastanak, privatna zabava, ili promocija knjige, a da im niko ne zatraži kartu ili propusnicu?

Na sličan način, obmanjivači mogu da smisle priču pomoću koje će se uvući na mesta za koja ne biste mislili da je to moguće. Primer je sledeća situacija.

Telefonski poziv

„Kancelarija Rona Hiljarda, ovde Doroti.“

„Zdravo, Doroti. Zovem se Kajl Belami. Upravo sam počeo da radim na razvoju animacije kod Brajana Glasmena. Vi stvarno drugačije poslužete ovde.“

„Pretpostavljam da je tako. Nikad nisam radila na nekom drugom filmu, pa ne znam kako je. Šta mogu da učinim za vas?“

„Istinu govoreći, osećam se pomalo glupo. Treba da mi dođe pisac danas poslepodne na razgovor, a ja ne znam s kim treba da popričam da bi ga pustili unutra. Ljudi ovde u Brajanovoj kancelariji su zaista ljubazni, ali ne mogu stalno da im smetam pitajući ih kako se radi ovo ili ono. Osećam se kao da sam tek pošao u gimnaziju i da ne mogu da nađem put do toaleta. Znete na šta mislim?“

Doroti se nasmejala.

„Treba da razgovarate s obezbeđenjem. Okrenite 7, a potom 6138. Ako vam se javi Lorin, recite joj da joj Doroti poručuje da vas dobro pazi.“

„Hvala, Doroti. Ako ne budem mogao da nađem toalet, možda ću vam se ponovo javiti!“

Prigušeno su se nasmejali, a potom prekinuli vezu.

Priča Dejvida Herolda

Obožavam filmove i kad sam se preselio u Los Anđeles, mislio sam da ću sretati razne ljude iz sveta filma i da će me oni odvoditi na žurke i pozivati me na ručkove u studije. Živeo sam u gradu već godinu dana, punio sam dvadeset i šest godina, a najviše sam se približio filmadžijama na razgledanju studija Universal, sa svim tim finim ljudima iz Feniksa i Klivlenda. Tako sam konačno došao do tačke kad sam odlučio – ako neće oni da me pozovu, pozvaću se sam. Upravo sam to i učinio.

Kupio sam *Los Angeles Times*, čitao kulturnu hroniku nekoliko dana i zapisivao imena producenata u raznim studijama. Odlučio sam da ću prvo pokušati s jednim od velikih studija.

Tako sam pozvao centralu i zamolio da me spoje s kancelarijom producenta o kojem sam čitao u novinama. Sekretarica koja se javila bila je majčinski tip, pa sam pomislio da imam sreće. Da sam naišao na mladu devojkicu koja tu radi u nadi da će je neko otkriti, verovatno ne bi sa mnom tako ćaskala.

Ta Doroti je delovala kao neko ko bi odveo kući napušteno maće, neko ko bi se sažalio na novog momka koji se nije snašao na novom poslu. I sigurno je da sam pogodio pravu žicu u razgovoru s njom. Ne događa se svakog dana da pokušate da prevarite nekoga, a on vam pruži i više od onoga što ste tražili. Iz samilosti, dala mi je ime osobe zaposlene u obezbeđenju i po meni poručila toj dami da mi pomogne.

Naravno, ja sam u svakom slučaju planirao da upotrebim njeno ime. Ovako je bilo još bolje. Lorin se odmah odobrovoljila i nikad se nije ni setila da potraži ime koje sam joj dao u bazi podataka o zaposlenima.

Kad sam se tog poslepodneva odvezao do kapije, imali su moje ime na spisku posetilaca, i čak su mi sačuvali mesto za parkiranje. Kasno sam ručao u bifeu, pa sam se muvao naokolo do kraja dana. Čak sam se i uvukao u nekoliko studija i gledao kako snimaju filmove. Otišao sam tek u 7 sati. Bio je to jedan od najuzbudljivijih dana u mom životu.

Analiza prevare

Svako je nekad bio novajlija na poslu. Svi se sećamo kako je izgledao taj prvi dan još kad smo bili mladi i neiskusni. Kad novi zaposleni zatraži pomoć, može očekivati da će se mnogi – a naročito oni koji rade na prijemnim odeljenjima – prisetiti sopstvenih osećanja kao novajlije u kraju i učiniti sve što je u njihovoj moći da pomognu. U svetu obmane to je poznato, pa se podrazumeva da se može i iskoristiti kad se igra na kartu sažaljenja.

Mi omogućavamo uljezima da sasvim lako na prevaru uđu u kompanijska postrojenja i kancelarije. Čak i kad postoje čuvari na ulazu i zahteva se da se potpiše svako ko nije zaposleni, u raznim varijacijama obmane opisane u ovoj priči uljez uspeva da dobije propusnicu posetioca i jednostavno ušeta. A ako se u vašoj kompaniji zahteva da se posetiocima dodeli

pratnja? To je dobro pravilo, ali deluje samo ako su vaši zaposleni zaista savesni pa zaustave svakog ko je došao sam, imao on značku ili ne, i ispita-ju ga. Otkriju li da posetiočevi odgovori nisu zadovoljavajući, vaši zaposle-ni moraju biti voljni da pozovu obezbeđenje.

Ako je nepoznatim osobama lako da se uvuku u vaše prostorije pomoću izmišljene priče, to ugrožava poverljive kompanijske informacije. U današnje vreme, kad se nad našim društvom nadvila pretnja od terorističkih napada, mnogo više od informacija može biti ugroženo.

„UČINITE TO ODMAH“

Nisu baš svi obmanjivači tako uspešni. Svako ko poznaje neku kompaniju može postati opasan po nju. Rizik je čak i veći u kompanijama koje u da-totekama i bazama podataka drže privatne podatke o zaposlenima, a takve su skoro sve.

Kad radnici nisu obrazovani, niti obučeni da prepoznaju obmanu, od-lučni ljudi poput ostavljene dame u priči koja sledi, mogu da učine stvari koje čestiti ljudi smatraju nemogućim.

Dagova priča

Sa Lindom ionako nije baš sve išlo kako treba, pa sam znao čim sam sreo Erin da je ona prava osoba za mene. Linda je, recimo, pomalo... pa, ne baš nestabilna, ali nekako može da izgubi živce kad se uznemiri.

Kazao sam joj, što sam nežnije mogao, da mora da se iseli, pomogao joj da se spakuje, i čak joj dozvolio da ponese nekoliko mojih muzičkih dis-kova. Čim se iselila, otišao sam do gvoždare po novu Mediko bravu za ula-zna vrata i stavio sam je iste večeri. Sledećeg jutra sam nazvao telefonsku kompaniju, zamolio ih da mi promene broj i da ga ne objavljuju.

Tako sam bio slobodan da potražim Erin.

Lindina priča

Ionako sam rešila da odem, samo nisam odlučila tačno kada. Ali niko ne voli da se oseća odbačenim. Morala sam nešto da uradim da mu stavim do znanja kakav je kretan.

Brzo sam smislila i šta. Sigurno je postojala druga devojka, ili me ne bi izbacio u takvoj žurbi. Tako sam rešila da malo sačekam, a onda da

počnem da ga zovem kasno uveče. Znete, u vreme kad bi najmanje želeli da ih neko zove telefonom.

Sačekala sam sledeći vikend i pozvala oko 11 uveče u subotu, ali on je promenio telefonski broj. Novi broj nije bio objavljen. To samo potvrđuje kakav je pokvarenjak bio.

Nije to bio tako velik problem. Počela sam da prebiram po papirima koje sam uspeła da odnesem kući pre nego što sam napustila posao u tele-fonskoj kompaniji. Bio je tu – sačuvala sam račun o popravci kad je jed-nom Dagova telefonska linija bila u kvaru, a na isečku su bili odštampani kabl i parica za njegov telefon. Vidite, možete menjati broj telefona koliko vam je volja, ali i dalje imate isti par bakarnih žica koje vode od vaše kuće do centrale telefonske kompanije. Par bakarnih žica iz svake kuće i stana identifikuje se tim brojevima, koji se nazivaju kabl i parica. Ako znate način rada u telefonskoj kompaniji, a ja to znam, sve što vam je potrebno da biste saznali neki telefonski broj jeste kabl i parica te osobe.

Imala sam spisak svih centrala u gradu, sa adresama i telefonskim broje-vima. Potražila sam broj centrale u kraju u kom sam ranije živela s Dagom pokvarenjakom, i nazvala ali, naravno, nikoga nije bilo. Gde je operater na centrali kad vam zaista treba? Trebalo mi je čak dvadeset sekundi da smislim plan. Počela sam da zovem druge centrale i konačno ga pronašla. On je bio miljama daleko i verovatno je sedeo s nogama podignutim na sto. Zнала sam da neće hteti da učini ono što mi treba. Imala sam spreman plan.

„Ovde Linda iz Centra za popravke“, rekoh. „Imamo hitan slučaj. Veza u jednoj medicinskoj ustanovi se prekinula. Tehničar na terenu pokušava da ponovo uspostavi liniju, ali ne može da pronađe u čemu je problem. Treba da se odmah odvezete do centrale Webster i pogledate da li centrala odašilje signal.“

A onda sam mu rekla: „Nazvaću vas kad stignete tamo“ jer, naravno, nisam mogla da dozvolim da on pozove Centar za popravke i traži mene.

Zнала sam da neće želeći da napušta udobnu centralu, morao bi da se ušuška, očisti led s vetrobranskog stakla, a potom vozi kroz bljuzgavicu kasno uveče. Ali bio je u pitanju „hitan slučaj“, pa nije baš mogao da mi kaže kako je suviše zauzet.

Kad sam ga, četrdeset i pet minuta kasnije, pozvala u centrali Webster, rekla sam mu da proverio kabl 29 i paricu 2481, a on je otišao do ormarića, proverio, i kazao da signal postoji. To sam, svakako, već znala.

Onda reko: „Dobro, potrebno mi je da potvrdite vezu“, što znači da identifikuje telefonski broj. To se radi tako što se okrene poseban broj koji očita broj sa koga se zvalo. Čovek nije znao da broj nije objavljen, niti da je nedavno bio promenjen, pa je učinio to što sam ga zamolila, a ja sam čula broj koji mu je objavljen preko test opreme za montere linija. Divno. Sve je išlo kao po loju.

Rekoh mu: „Pa, mora da je problem negde na terenu“, kao da sam broj znala sve vreme. Zahvalila sam mu se, kazala da ćemo raditi na tome, i poželeva mu laku noć.

mitnikova poruka

Kad obmanjivači poznaju način rada neke kompanije, lako će upotrebiti to znanje da ostvare prisnost sa zaposlenima. Firme se moraju pripremiti za takve napade sadašnjih ili bivših zaposlenih koji možda gledaju svoje lične interese. Može biti korisno da se proveri istorijat osoblja kako bi se otkrilo ko ima sklonosti ka takvom ponašanju. U većini slučajeva, takvi se ljudi teško otkriju. Pre nego što se bilo koji podaci otkriju nekome za koga se lično ne zna da li još uvek tu radi, jedino je razumno proveriti identitet i status tog zaposlenog u okviru firme.

Toliko o Dagu i njegovom pokušaju da se od mene sakrije pomoću neobjavljenog broja. Zabava će uskoro uslediti.

Analiza prevare

Mlada dama iz ove priče došla je do željenih informacija radi osвете jer je poznavala telefonsku kompaniju: telefonske brojeve, procedure i terminologiju. Uspela je da otkrije nov, neobjavljen telefonski broj, i izvela je to usred vetrovite noći, šaljući operatera telefonske centrale na drugi kraj grada.

„GOSPODIN BIG TO TRAŽI“

Popularan i vrlo uspešan oblik zastrašivanja – popularan uglavnom zato što je tako jednostavan – zasniva se na uticanju na ljudsko ponašanje pomoću autoriteta.

I samo pominjanje imena asistenta generalnog direktora može biti vredno. To stalno koriste privatni istražitelji, pa čak i kompanije za zapošljavanje. Nazovu operatera na centrali i kažu da žele da ih spoji s kancelarijom

generalnog direktora. Kad se javi sekretarica ili asistent, oni kažu da imaju neki dokument ili paket za generalnog direktora, ili pitaju da li mogu da pošalju nešto elektronskom poštom na štampanje. Pitaju koji je broj faksa, a usput i kako se sagovornik zove?

Potom nazovu nekog drugog i kažu: „Džanin iz kancelarije gospodina Biga mi je rekla da vas nazovem da biste mi pomogli u vezi s ovim.“

Ova metoda se naziva „imenovanje ljudi na položaju“, a obično se koristi da bi se brzo ostvarila prisnost a žrtva navela da poveruje kako je napadač povezan s nekom osobom od autoriteta. Žrtva će pre učiniti uslugu nekome s kim ga vezuju zajednički poznanici.

Ako je napadač bacio oko na veoma poverljive informacije, može upotrebiti ovakav pristup da bi žrtvi podstakao emocije, kao što je strah od ulaska u sukob s pretpostavljenima. Evo primera.

Skotova priča

„Skot Ejbrems.“

„Skote, ovde Kristofer Dalbridž. Upravo sam razgovarao s gospodinom Biglijem – veoma je nezadovoljan. Kaže da vam je pre deset dana poslao poruku da nam dostavite primerke svih vaših istraživanja tržišta radi analize. Uopšte ih nismo dobili.“

„Istraživanje tržišta? Niko mi ništa nije rekao o tome. Iz kog ste odseka?“

„Mi smo savetnička firma koju je unajmio, i već kasnimo.“

„Čujte, upravo sam pošao na sastanak. Kažite mi svoj broj telefona, pa...“

Napadač je tad zazvučao kao da je gotovo potpuno iznerviran: „Da li želite da to prenesem gospodinu Bigliju?! On očekuje naše analize sutra ujutru, a mi moramo da radimo na tome noćas. Hoćete li da mu ja kažem da to nismo mogli da učinimo jer nismo dobili vaš izveštaj, ili hoćete to sami da mu kažete?“

Besan generalni direktor vam može upropastiti nedelju. Žrtva će verovatno odlučiti da problem treba rešiti pre nego što ode na sastanak. Još jednom, napadač je pritisnuo pravo dugme da bi dobio odgovarajući odgovor.

Analiza prevare

Obmana zastrašivanjem tako što se navede ime nadređenog posebno dobro uspeva ako je sagovornik na prilično niskom nivou u firmi. Kad se upotrebi ime neke važne osobe, prevaziđe se uobičajena rezerva ili sumnja,

a sagovornik je uglavnom željan da pomogne; prirodan instinkt da se pomaže pojačava se kad mislite da je osoba kojoj pomažete važna ili uticajna.

Zna se, međutim, da je najbolje u ovakvom tipu obmane upotrebiti ime nekoga ko je na višem nivou od šefa žrtve. I to lukavstvo je teško primeniti u okviru male organizacije. Napadač ne želi da njegova žrtva slučajno pomene nešto potpredsedniku odeljenja za marketing. Na komentar poput ovog: „Poslao sam onaj marketinški plan za proizvode zbog kojeg ste zamolili onog momka da me nazove“, sasvim lako se dobija odgovor tipa: „Kakav marketinški plan? Kog momka?“ To bi moglo dovesti do otkrića da je izvršen napad na firmu.

mitnikova poruka

Zastrašivanje obično izaziva bojazan od kazne – zato ljudi sarađuju. Može potaći i bojazan od neugodne situacije, ili gubitka nove, više pozicije.

Ljudi se moraju obučavati da je provera autoriteta prihvatljiva i očekivana kad je u pitanju bezbednost. Obuka za obezbeđivanje informacija trebalo bi da nauči osoblje kako da provere autoritet, a da istovremeno budu ljubazni prema klijentima i da ne naruše odnose. Štaviše, ta očekivanja mora prvenstveno podržati rukovodstvo. Ako se zaposleni ne podržavaju u tome da proveravaju sagovornike nezavisno od statusa, normalna reakcija je da se prestane s proverom – a upravo to ne želite.

ŠTA SOCIJALNO OSIGURANJE ZNA O VAMA

Obično se smatra da državne agencije koje imaju dosijea o građanima čuvaju te podatke na sigurnom mestu, zaključane, daleko od osoba kojima nije odobren pristup. U stvarnosti, čak ni američka savezna vlada nije tako otporna na upade kako bismo želeli.

Telefonski poziv za Mej Lin

Mesto: Regionalna kancelarija Socijalnog osiguranja

Vreme: 10:18, četvrtak ujutru

„Mod broj tri. Ovde Mej Lin Vong.“

Glas s druge strane žice zvučao je kao da se izvinjava, gotovo uplašen.

„Gospođice Vong, ovde Artur Erondejl, iz kancelarije glavnog inspektora. Mogu li vas zvati Mej?“

„Zovem se Mej Lin“, reče.

„Pa, ovako stoje stvari, Mej Lin. Zaposlili smo novog momka za kojeg još nemamo računar, a trenutno radi na veoma važnom projektu, pa koristi moj. Mi predstavljamo Vladu Sjedinjenih Država, za ime sveta, a oni kažu da nemaju dovoljno novca u budžetu da kupe tom momku računar. I sad moj šef misli da ja zaostajem s poslom i neće da čuje nikakva opravdanja, znate.“

„Znam tačno na šta mislite.“

„Možete li mi pomoći da na brzinu proverim nešto u MCS-u?“, upita, upotrebivši ime računarskog sistema u kom se pretražuju podaci o poreskim obveznicima.

„Naravno, šta vam treba?“

„Prvo mi treba abecedna provera Džozefa Džonsona, datum rođenja 7/4/69.“ (Abecedna provera znači da se u računaru pronađe račun abecedno pohranjen prema imenu poreskog obveznika, a datum rođenja služi kao dodatni identifikator.)

Nakon kratke stanke, upitala je:

„Šta vam treba?“

„Koji je broj njegovog računa?“, upita, upotrebivši skraćeni izraz za broj socijalnog osiguranja, koji koriste samo zaposleni firme. Pročitala ga je.

„U redu, očitajte mi stavke tog računa“, reče njen sagovornik.

Zapravo ju je zamolio da mu pročita osnovne podatke o poreskom obvezniku, a Mej Lin mu je na to dala mesto rođenja, majčino devojčako ime i očevo ime. Njen sagovornik je pažljivo slušao dok mu je iščitavala i mesec i godinu kad je kartica izdata, te regionalnu kancelariju u kojoj je izdata.

Potom je zatražio i detaljnu proveru primanja.

Pitala je: „Za koju godinu?“

Sagovornik je odgovorio: „Za 2001.“

Mej Lin reče: „Suma je bila 190286 dolara, a uplatila ju je firma Džonson Mikrotek.“

„Da li je bilo drugih primanja?“

„Ne.“

„Hvala vam“, kaza. „Bili ste veoma ljubazni.“

Potom je pitao da li može da je pozove kad mu ponovo zatrebaju informacije a ne može da dođe do svog računara. Ponovo je upotrebio omiljen trik obmanjivača: uvek treba uspostaviti vezu kako bi se mogla stalno zvati ista osoba; tako se izbegava neprijatno pronalaženje nove žrtve uvek iznova.

„Ne sledeće nedelje“, rekla mu je, jer je išla u Kentaki na sestrino venčanje. U svako drugo doba, učiniće sve što je u njenoj moći.

Kad je spustila slušalicu, Mej Lin se osećala dobro što je mogla malo da pomogne kolegi koji je naišao na nerazumevanje.

Priča Kita Kartera

Ako je suditi po filmovima i popularnim kriminalističkim romanima, privatni detektivi ne drže mnogo do etike, a odlično poznaju načine da dođu do sočnih podataka o ljudima. To čine pomoću potpuno nezakonitih metoda, i jedva uspevaju da izbegnu hapšenje. Istina je, naravno, da većina privatnih detektiva legalno posluje. Budući da su mnogi od njih započeli karijeru kao zakleti službenici kriminalističke službe, oni savršeno dobro znaju šta je legalno, a šta nije, i uglavnom ne dolaze u iskušenje da pređu tu granicu.

Ipak, postoje izuzeci. Neki privatni istražitelji – a to je više nego šačica njih – zaista odgovaraju opisu tipova iz kriminalističkih priča. U ovom poslu su poznati kao mešetari informacijama, što je eufemizam za osobe koje su spremne da krše pravila. Oni znaju da svaki zadatak mogu da obave mnogo brže i lakše ako pođu prečicama. Činjenica da su te prečice zapravo prekršaji zbog kojih bi mogli odležati nekoliko godina u zatvoru ne sprečava beskrupuloznije.

Uspešni privatni detektivi – oni koji rade u luksuznim kancelarijama u otmenom delu grada – ne obavljaju sami ilegalne poslove. Obično za to unajme nekog mešetara informacijama.

Čovek koga ćemo zvati Kit Karter bio je privatni detektiv neopterećen etikom.

Bio je to tipičan slučaj u kom se traži „Gde je sakrio novac?“ Ponekad je u pitanju i „Gde je ona sakrila novac?“ Ponekad neka bogata dama želi da sazna gde je muž sakrio njen novac (mada je Kitu Karteru bila misterija zašto bi se žena koja ima novca ikada udala za čoveka koji ga nema; o tome je povremeno razmišljao, ali nikada nije našao dobar odgovor.)

U ovom slučaju je muž, Džo Džonson, skrivao novac. Bio je to pаметan momak. Osnovao je visokotehnološku firmu sa deset hiljada dolara koje je pozajmio od ženine porodice, i razvio je u kompaniju od sto miliona dolara. Kako tvrdi njen advokat za razvod, uspeo je da na savršen način sakrije svoj imetak, a advokat je želeo detaljan izveštaj.

Kit je smatrao da bi trebalo da počne od socijalnog osiguranja, konkretno od njihovog dosijea o Džonsonu, koji je verovatno prepun vrlo korisnih informacija za ovakve situacije. Naoružan njihovim podacima, Kit se mogao pretvarati da je žrtva i navesti banke, mešetarske firme i inostrane institucije da mu kažu sve.

Prvi poziv uputio je lokalnoj službi socijalnog osiguranja, koristeći besplatni broj koji je naveden u telefonskom imeniku. Kad se službenica javila, tražio je da ga spoje s nekim u odeljenju za potraživanja. Ponovo je sačekao, a potom se neko javio. Sad je Kit ubacio u drugu brzinu; „Zdravo“, počeo je. „Ovde Gregori Adams, Mesna kancelarija 329. Vidite, pokušavam da dobijem službenika za potraživanja koji radi s brojevima koji se završavaju s 6363, a na broj koji su mi dali odgovara faks mašina.“

„To vam je Mod broj tri“, odvrati čovek. Potražio je broj i dao ga Kitu.

Zatim je nazvao Mod broj tri. Kad se Mej Lin javila, promenio je ulogu i ispričao joj priču o tome kako zove iz kancelarije glavnog inspektora, i problemu koji ima s tim što neko drugi mora da koristi njegov računar. Dala mu je tražene podatke i pristala da učini sve što može kad mu ubuduće zatreba pomoć.

Analiza prevare

Uspeh ovog pristupa leži u tome što je napadač igrao na kartu sažaljenja zaposlenog zbog priče da mu neko drugi koristi računar, a da „šef nije zadovoljan“. Ljudi ne pokazuju često osećanja na poslu; kad se to dogodi, može da oslabi nečiju uobičajenu odbranu od obmana. Za uspeh je bila potrebna samo emotivna obmana tipa „Imam problema, da li biste mi pomogli?“

Socijalno (ne)osiguranje

Neverovatno! Socijalno osiguranje je objavilo na Webu čitavo njihovo Uputstvo za rad. Prepun je korisnih informacija za osoblje, ali su te informacije takođe izuzetno bitne prevarantima. Ono sadrži skraćenice, terminologiju i uputstva za to kako treba tražiti ono što vam je potrebno, na način koji je opisan u ovoj priči.

Želite da saznate više internih informacija o socijalnom osiguranju? Pretražite Web pomoću lokacije Google, ili unesite sledeću adresu u čitač Web: <http://policy.ssa.gov/poms.nsf/>. Ukoliko socijalno osiguranje nije već pročitao ovo i uklonilo Uputstvo, tu ćete naći čak i detaljne informacije o tome koje podatke njihovi službenici smeju da saopšte kriminalističkom odeljenju. To praktično znači da ih može dobiti i svaki prevarant koji uspe da ubedi njihovog službenika da radi u kriminalističkoj službi.

Napadač se nije mogao uspešno domoći tih informacija od službenika koji odgovara na pozive običnih ljudi. Vrsta obmane koju je Kit izveo uspeva samo kad telefonski broj osobe koja prima poziv nije dostupan javnosti. Takva osoba stoga očekuje da svako ko je pozove mora biti neko iz firme – što je još jedan primer bezbednosti uz lozinku.

U elemente koji su pomogli da ovaj napad uspe spadaju:

- Poznavanje telefonskog broja za Mod.
- Poznavanje terminologije koju oni koriste – očitavanje stavki, abecedna provera...
- Pretvaranje da je poziv došao iz kancelarije glavnog inspektora, za koju svaki zaposleni iz federalne vlade zna da je veoma moćna vladina istraživačka agencija. Tako je napadač stekao auru autoriteta.

Evo još jednog zanimljivog dodatnog podatka – čini se da obmanjivači znaju kako da podnesu zahtev tako da gotovo niko ne pomisli: „Zašto zovete mene?“ – čak i kad bi, logično, imalo više smisla da je poziv upućen nekoj drugoj osobi u sasvim drugom odeljenju. Možda poziv u pomoć prekida monotoniju svakodnevnog sagovornikovog posla, pa žrtva i ne razmišlja koliko je poziv neobičan.

Najzad, napadač iz ove priče, nije bio zadovoljan samo zadobijenim informacijama. Želeo je da uspostavi kontakt na koji se mogao redovno pozivati. Da nije hteo trajniju vezu sa žrtvom, mogao je primeniti uobičajenu obmanu u napadu u kom se računa na nečije sažaljenje – „Prosuo sam kafu na tastaturu“. Međutim, to ovde ne bi upalilo, jer se tastatura može zameniti za dan. Stoga je izmislio priču o tome da neko koristi njegov računar, što je slobodno mogao da razvuče na nekoliko nedelja: „Da, mislio sam da je juče trebalo da dobije svoj računar, a kad je stigao, neki drugi momak je nekako uspeo da organizuje da ga on dobije. I tako taj tip još uvek dolazi da radi na mom radnom mestu.“ I tako dalje.

„Jadan ja, potrebna mi je pomoć.“ Uvek upali!

JEDAN JEDNOSTAVAN POZIV

Jedan od glavnih problema jeste formulisanje razumnog zahteva, koji liči na uobičajene zahteve s kojima se žrtva svakodnevno sreće, tako da se on ili ona ne uznemiri suviše. Kao i sve drugo u životu, i trud da vam zahtev zvuči logično nekad može biti pravi izazov, dok je drugi put prosto kao pasulj.

Telefonski poziv za Meri H.

Vreme: ponedeljak, 23. novembar, 07:49

Mesto: Mersbi Storč, Njujork

Mnogima se čini da se računovodstvo svodi na rad s brojkama i računanje, i uglavnom se smatra krajnje nezanimljivim poslom. Na sreću, ne misli svako isto. Na primer, Meri Heris je njen posao glavnog knjigovođe bio sasvim zanimljiv, što je delom bio razlog da je postala jedan od najmarljivijih računovođa u firmi.

Tog ponedeljka, Meri je stigla rano da bi na vreme započela jedan dug dan, kako se činilo. Iznenadila se kad joj je zazvonio telefon. Podigla je slušalicu i predstavila se.

„Zdravo, ovde Piter Šepard. Ja radim u kompaniji Erbakl; mi pružamo tehničku podršku vašoj firmi. Preko vikenda nam je od vaših ljudi pristiglo nekoliko žalbi da imate problema s računarima. Mislio sam da mogu sad ujutru to da popravim pre nego što svi stignu na posao. Imate li vi nekih problema s računarom ili povezivanjem na mrežu?“

Rekla mu je da još ne zna. Uključila je računar, a on joj je objasnio šta treba da uradi, dok se operativni sistem podizao.

„Hteo bih nešto da proverim, uz vašu pomoć“, reče. „Ja na svom ekranu mogu da vidim šta pritiskate na tastaturi, pa želim da se uverim da signali ispravno stižu na mrežu. Čim pritisnete taster, recite mi koji je, pa ću videti da li se isto slovo ili broj pojavljuje i ovde. U redu?“

Pred očima su joj se pojavile slike užasa – njen računar ne radi, a čitav dan joj je upropašćen jer ne može da završi posao; zato joj je bilo veoma drago što joj ovaj čovek pomaže. Nakon nekoliko trenutaka, kazala mu je: „Pojavio se ekran za prijavljivanje za rad, pa ću uneti svoju identifikaciju. Upravo pritiskam tastere – M...A...R...Y...D.“

„Zasad odlično ide“, odvrati on. „To i ja ovde vidim. Sad slobodno unesite lozinku, ali mi nemojte reći koja je. Nikad nikom ne govorite lozinku, čak ni tehničkoj podršci. Meni će se ovde pojaviti samo zvezdice – vaša lozinka je zaštićena, tako da ja ne mogu da je vidim.“ Naravno da je to sve bila čista laž, ali se Meri činilo logičnim. A onda je rekao: „Kazite mi kad vam se računar potpuno pokrene.“

Kad mu je to kazala, zamolio ju je da otvori dve aplikacije, a ona mu je javila da rade sasvim dobro.

Meri je osetila olakšanje kad je ustanovila da sve radi normalno. Piter reče: „Drago mi je što sam se uverio da ćete normalno moći da radite na računaru. Znači“, nastavi, „upravo smo instalirali nov program pomoću kojeg možete menjati lozinke. Da li biste hteli da odvojite nekoliko minuta za mene da bih proverio radi li kako valja?“

Bila mu je zahvalna za pomoć, pa je odmah pristala. Piter joj je potanko objasnio kako da pokrene aplikaciju pomoću koje korisnici mogu da menjaju lozinke, standardni program Windowsa 2000. „Unesite lozinku“, kaza, „ali nemojte je izgovoriti naglas.“

Kad je to učinila, Piter reče: „Samo da bismo na brzinu izvršili test, kad vam zatraži novu lozinku, unesite 'test123'. Potom to ponovo unesite u polje Verification, i pritisnite Enter.“

Objasnio joj je postupak prekidanja veze sa serverom. Zamolio ju je da sačeka nekoliko minuta, potom da se ponovo poveže, ovoga puta pokušavajući da se prijavi za rad pomoću nove lozinke. Odmah je upalilo, i činilo se da je Piter veoma zadovoljan. Objasnio joj je kako da ponovo vrati svoju staru lozinku ili da izabere novu – još jednom je upozorivši da je ne kaže naglas.

„Pa, Meri“, reče joj Piter, „nismo ustanovili nikakav problem, i to je sjajno. Čujte, ako se ipak pojavi neki problem, samo pozovite firmu Erbakl. Obično radim specijalne projekte, ali svaki naš zaposleni koji vam se javi može vam pomoći.“ Zahvalila mu se, pa su se oprostili.

Piterova priča

O Piteru se raširila priča – mnogi njegovi školski drugovi iz kraja čuli su da se pretvorio u nekakvog računarskog maga koji često može da pronađe korisne informacije do kojih drugi nisu mogli da dođu. Kada ga je Elis Konrad zamolila za uslugu, prvo ju je odbio. Zašto bi joj pomogao? Kad su se jednom ranije sreli, pozvao ju je da izađu zajedno, ali ga je hladno odbila.

Nije se činilo da ju je njegovo odbijanje iznenadilo. Rekla je da misli da on to ionako ne može da izvede. To je bilo poput izazova, jer je, svakako, bio siguran da može. I tako je ipak pristao.

Elis je ponuđen ugovor za posao savetnika u jednoj marketinškoj kompaniji, ali uslovi ugovora nisu baš izgledali povoljno. Pre nego što je ponovo otišla da pregovara o boljim uslovima, htela je da zna kakve uslove drugi savetnici imaju u svojim ugovorima.

Evo Piterove priče.



Nisam hteo da kažem Elis da sam počeo ovim da se bavim jer su mi ljudi tražili da nešto uradim ne verujući da to mogu, kad sam ja znao da će biti lako. Pa, ne baš lako, ne ovog puta. Valjalo se malo potruditi. Ali to ne smeta.

Pružala mi se prilika da joj pokažem šta znači biti pametan.

Nešto nakon 7:30 u ponedeljak ujutru, nazvao sam marketinšku kompaniju i javila mi se službenica na centrali. Kazao sam joj da radim u firmi koja se bavi njihovim penzionim planovima i da želim da razgovaram s nekim iz računovodstva. Da li je primetila da je neko iz računovodstva već stigao? Odgovorila je: „Mislim da je Meri ušla pre nekoliko minuta. Pokušaću da vas spojim s njom.“

Kad je Meri podigla slušalicu, ispričao sam joj svoju priču o računarskim problemima, što je trebalo da je uplaši i nagna na saradnju. Čim sam joj objasnio kako da promeni lozinku, odmah potom sam se brzo prijavio za rad u sistemu pomoću iste te privremene lozinke koju sam je zamolio da upotrebi, test123.

A evo i majstorskog dela posla – instalirao sam jedan mali program pomoću kojeg sam, koristeći sopstvenu tajnu lozinku, mogao da pristupam računarskom sistemu kompanije kad god poželim. Nakon što sam prekinuo razgovor s Meri, prvo sam izbrisao trag o događajima kako niko nikad ne bi saznao da sam bio u njihovom sistemu. Bilo je lako. Pošto sam dodelio sebi administratorska ovlašćenja, uspeo sam da učitam besplatan program pod nazivom clearlogs koji sam našao na jednoj Web lokaciji posvećenoj obezbeđenju, na adresi www.ntsecurity.nu.

Tad je došlo vreme za pravi posao. Pretražio sam sva dokumenta koja u imenu datoteke imaju reč „ugovor“, i preuzeo ih. Potom sam još malo tražio i naišao na pravu stvar – direktorijum u kom se nalaze svi izveštaji o isplata-ma savetnika. Tako sam spojio sve datoteke s ugovorima i spisak isplata.

Elis je sad mogla da prouči ugovore i vidi koliko plaćaju druge savet-nike. Neka sama obavi taj dosadni deo posla, neka iščita sve te datoteke. Ja sam učinio ono što me je zamolila.

Sa diskova na koje sam snimio podatke odštampao sam neke datoteke kako bih joj pokazao dokaz. Naterao sam je da se sastane sa mnom i plati mi večeru. Trebalo je da joj vidite izraz lica dok je prelistavala hrpu papira. „Nemoguće“, govorila je. „Nemoguće.“

Nisam poneo diskove. Oni su bili mamac. Rekao sam joj da će morati da dođe kod mene da bi ih dobila, nadajući se da će možda želeći da mi se lično zahvali za uslugu koju sam joj upravo učinio.

mitnikova poruka

Zapanjujuće je koliko obmanjivači, na osnovu toga kako formulišu zahtev, lako navode ljude da nešto učine. Ideja je da se izazove automatski odgovor na osnovu psiholoških principa. Obmanjivač se oslanja na mentalne prečice kojima se služimo kad shvatimo da je sagovornik na našoj strani.

Analiza prevare

Piterov telefonski poziv marketinškoj kompaniji predstavlja najosnovniji oblik obmane – to je jednostavan pokušaj za koji nije potrebna velika priprema, upalio je iz prve, i trajao je samo nekoliko minuta.

Što je još bolje, Meri, njegova žrtva, nije imala razloga da pomisli da ju je sagovornik prevario ili obmanuo, pa nije podigla uzbunu.

Trik je upalio jer je Piter upotrebio tri metode obmane. Prvo je ostvario saradnju uplašivši Meri – naveo je da poveruje kako možda neće moći da koristi računar. Potom ju je bez žurbe zamolio da otvori dve svoje aplikacije da bi se uverila da dobro rade, čime je učvrstio prisnost između njih, odnosno osećaj da su na istoj strani. Konačno, ponovo ju je naveo da s njim sarađuje u najbitnijem delu zadatka. Igrao je na kartu njene zahvalnosti za pomoć koju joj je pružio proveravajući da li njen računar dobro radi.

Rekavši joj da nikad ne treba da otkriva svoju lozinku, pa čak ni njemu, Piter je na fini način i u potpunosti uspeo da je ubedi da on brine o bezbednosti dokumenata njene kompanije. Bila je još sigurnija da nije prevarant, jer štiti nju i preduzeće.

POLICIJSKA RACIJA

Zamislite ovu scenu: vlada pokušava da uhvati Artura Sančeza, koji besplatno distribuirao filmove na Internetu. Holivudski studiji kažu da narušava njihova autorska prava, a on odgovara da samo pokušava da ih natera da priznaju kako neumitno postoji još jedno tržište, te da konačno omogućće preuzimanje novih filmova s Interneta. On (tačno) ističe da bi to mogao biti ogroman izvor zarade za studije koji, čini se, tu zamisao potpuno ignorišu.

Molim vas, nalog za pretres

Kad je jedne večeri kasno došao kući, pogledao je prozore svog stana s druge strane ulice i video da su svetla ugašena, iako on uvek ostavi jedno upaljeno kad izlazi iz kuće.

Lupao je i udarao na susedova vrata dok ga nije probudio, i saznao je da je zaista bila policijska racija u zgradi. Naterali su komšije da ostanu u dnu zgrade, pa još uvek nije siguran u koji su stan ulazili. Zna samo da su odneli neke teške stvari. Bile su umotane, pa nije video šta nose. I nikoga nisu odveli s lisicama.

Arturo je proverio stan. Loša vest je bila ta što je našao obaveštanje od policije da im se odmah mora javiti i zakazati razgovor u roku od tri dana. Još lošija vest bila je ta što su mu nestali računari.

Arturo je odjurio da prespava kod prijatelja. Nesigurnost je rasla. Koli-ko policija zna? Jesu li mu najzad doskočili, ili su mu ostavili šansu da pobegne? Ili se radi o nečem sasvim drugom, što bi mogao da razjasni, a da ne napušta grad?

Pre nego što nastavite da čitate, zastanite malo i razmislite: pada li vam na pamet kako biste mogli otkriti šta policija zna o vama? Uz pretpostavku da nemate nikakve političke veze, prijatelje u policiji, niti u tužilačevoj kancelariji, mislite li da postoji način da vi, kao običan građanin, dobijete te informacije? Da li bi to mogao da sazna vešt obmanjivač?

Obmana policije

Arturo je uspeo na sledeći način: za početak, nabavio je telefonski broj obližnje fotokopirnice, nazvao ih, i zamolio da mu daju svoj broj faksa.

Potom je nazvao kancelariju okružnog javnog tužioca i zamolio da ga spoje s arhivom. Kad su to učinili, predstavio se kao detektiv iz okruga Lejk, i kazao da želi da razgovara sa službenikom koji zavodi aktuelne naloge za pretres.

„Ja to činim“, reče gospoda. „O, odlično“, odgovori on. „Jer juče uveče smo izvršili raciju na jednog osumnjičenog, pa pokušavam da ustanovim gde se nalazi pismena izjava.“

„Zavodimo ih prema adresi“, kaza ona.

Dao joj je svoju adresu, a glas joj je zazvučao gotovo uzbuđeno. „A, da“, reče ushićeno, „za to znam. ‘Narušavanje autorskih prava‘.“

„To je to“, reče. „Potrebna mi je izjava i kopija naloga za pretres.“

„Evo imam ga ovde.“

„Odlično“, kaza. „Čujte, trenutno sam na terenu, a za petnaestak minuta imam sastanak s tajnom službom u vezi s ovim slučajem. U poslednje vreme sam toliko rastrojen, pa sam ostavio dosije kod kuće, i nikako neću uspeti da odem do stana i vratim se na vreme. Možete li mi vi poslati kopije?“

„Naravno, nema problema. Napraviću kopije; možete doći i pokupiti ih.“

„Sjajno“, na to će on. „To je sjajno. Ali, vidite, na drugoj sam strani grada. Možete li mi ih poslati faksom?“

Tu se ispostavio mali problem, ali ne takav da se ne može prevazići. „Ovde u arhivi nemamo faks mašinu“, kaza ona. „Ali dole u sobi za referente imaju jednu, pa će mi možda dozvoliti da je upotrebim.“

Na to će on: „Pustite da ja nazovem sobu za referente i sredim to.“

Gospoda u sobi za referente rekla je da će se rado pobrinuti za to, ali je želela da zna ko će to da plati. Trebao joj je kontni broj.

„Potražiću šifru, pa ću vam se javiti.“

Onda je nazvao kancelariju okružnog javnog tužioca, ponovo se predstavio kao policajac i upitao službenicu na centrali: „Koji je kontni broj kancelarije okružnog javnog tužioca?“ Ona mu ga je dala bez oklevanja.

Kad je ponovo nazvao sobu za referente da bi im dao konto, imao je izgovor da tu gospodu još više zloupotrebi – nagovorio ju je da ode na sprat i uzme papire koje valja poslati faksom.

Brisanje tragova

Arturu je preostalo da učini još nekoliko stvari. Uvek je postojala mogućnost da neko nešto posumnja, pa bi u fotokopirnici mogao naići na nekoliko detektiva, neformalno obučениh, koji se pretvaraju da imaju posla dok se ne pojavi neko ko traži baš taj faks. Malo je pričekao, a potom je ponovo pozvao sobu za referente da bi proverio da li je službenica poslala faks. Sve je teklo po planu.

napomena

Kako obmanjivač zna pojedinosti toliko mnogo procedura – u policiji, tužilačevoj kancelariji, telefonskim kompanijama, i raznim drugim zanimljivim firmama, poput telekomunikacionih i računarskih preduzeća? Posao mu je da to sazna. To mu je specijalnost, jer informacije koristi pri pokušaju obmane.

Nazvao je drugu fotokopirnicu iz istog lanca na drugom kraju grada i za njih smislio priču o tome kako je zadovoljan njihovom uslugom, te želi da pošalje upravnici pismo zahvalnosti, pa mu zato treba njeno ime. S tom izuzetno bitnom informacijom nazvao je ponovo prvu fotokopirnicu i kazao da želi da razgovara s upravnikom. Kad se on javio, Arturo reče: „Zdravo, ovde Edvard iz objekta broj 628 u Hartfildu. Moja uprava, Ana, rekla mi je da vas nazovem. Imamo veoma nezadovoljnu mušteriju – neko mu je dao faks broj pogrešnog objekta. On ovde čeka važan faks, ali su mu dali broj vaše radnje.“ Upravnik je obećao da će zamoliti radnika da pronađe taj faks i prosledi ga odmah do radnje u Hartfildu.

Arturo je već čekao u drugoj radnji kad je faks stigao. Kad ga je imao u rukama, pozvao je ponovo sobu za referente da se zahvali onoj gospodi, i da joj kaže: „Ne morate da vraćate te primerke na gornji sprat, slobodno ih bacite“. Potom je nazvao upravnika prve fotokopirnice i kazao i njemu da

baci svoj primerak faksa. Tako neće biti dokaza o tome što se dogodilo, u slučaju da neko dođe kasnije i počne da postavlja pitanja. Iskusni obmanjivači znaju da nikada ne možete biti suviše oprezni.

Na ovaj način Arturo čak nije ni morao da plati prvoj fotokopirnici što su primili faks i ponovo ga poslali drugoj radnji. Ako se policija zaista pojavila u prvoj radnji, Arturo je već imao svoj faks i biće već daleko kad policajci odu do druge lokacije.

Kraj priče: u izjavi i nalogu za pretres stajalo je da policija ima dobro dokumentovane dokaze da Artur kopira filmove. To je hteo da zna. Do ponoći je već prešao državnu granicu. Arturo je bio na putu da započne nov život, negde drugde, s novim identitetom, spreman da ponovo otpočne svoju kampanju.

Analiza prevare

Ljudi koji rade u bilo kojoj kancelariji okružnog javnog tužioca u stalnoj su vezi sa zaposlenima iz kriminalističke službe – odgovaraju na pitanja, ugovaraju sastanke, primaju poruke. Svakom ko je dovoljno drzak da ih pozove i predstavi se kao policajac, zamenik šerifa, ili nešto slično, verovatno će poverovati na reč. Ako obmanjivač očigledno poznaje terminologiju, nije nervozan i ne zamuckuje, i zvuči autentično, moguće je da mu neće postaviti nijedno jedino pitanje da bi potvrdili njegov identitet. Upravo to se dogodilo u ovoj priči, sa dva različita službenika.

Neophodan kontni broj dobio je pomoću jednog telefonskog poziva. Potom je Arturo odigrao na kartu sažaljenja službenice onom pričom o sastanku s tajnom službom za petnaestak minuta, te kako je rastrojen, pa je ostavio dosije kod kuće. Naravno, sažalila se nad njim i učinila sve što može da mu pomogne.

mitnikova poruka

Istina je da niko nije imun na obmanu veštog prevaranta. Zbog tempa normalnog života, nemamo uvek vremena za promišljene odluke, pa čak i u stvarima koje su važne. Složene situacije, nedostatak vremena, emocionalna stanja ili zamor, mogu nas lako omesti. Zato napravimo mentalnu prečicu, pa donesemo odluku ne analizirajući podatke pažljivo i u celini; taj se mentalni proces naziva automatsko reagovanje. To važi i za federalne, državne i lokalne pripadnike kriminalističke službe. Svi smo mi ljudi od krvi i mesa.

Arturo se dvostruko obezbedio kada je išao da preuzme faks, tako što je tražio da ga proslede u drugu radnju. Varijacija toga, usled čega bi se faksu još teže ušlo u trag, bila bi sledeća – umesto da se dokument pošalje u drugu fotokopirnicu, napadač im može dati broj koji liči na faks broj, ali je adresa besplatne službe na Internetu za primanje faksova i njihovo automatsko prosleđivanje do adrese elektronske pošte. Obmanjivač može direktno preuzeti dokument na svoj računar, i nikada ne mora da se pojavi lično, pa ga kasnije niko ne bi mogao identifikovati. Elektronska adresa i broj elektronskog faksa mogu se isključiti čim se misija okonča.

ZAMENA ULOGA

Mladić kojeg ću ovde zvati Majkl Parker bio je jedan od onih koji suviše kasno shvate da bolje plaćene poslove uglavnom dobijaju ljudi koji su završili fakultet. Imao je priliku da pohađa lokalni koledž i da prima delimičnu stipendiju i kredit za obrazovanje, ali je to značilo da treba da radi noću i vikendima kako bi otplatio zakupninu stana, hranu, gas i osiguranje kola. Majkl, koji je uvek voleo da ide prečicom, pomislio je da možda postoji drugi način, koji se isplati brže, a sa manje truda. Budući da je o računarima učio od kad je počeo da se na njima igra u desetoj godini i postao opsednut njima, odlučio je da izradi sebi ubrzanu fakultetsku diplomu iz računarskih nauka.

Diploma – bez pohvala

Mogao je ući u računarske sisteme državnog univerziteta, tamo pronaći dosije nekoga ko je diplomirao s lepim prosekom, kopirati diplomu, upisati na nju sopstveno ime, i dodati je ostalim diplomama klase koja je te godine diplomirala. Pošto je o tome razmislio, nekako se osećao nelagodno, pa je shvatio da mora postojati još dokaza o tome da je jedan student živeo u univerzitetskom gradu – dokaz o plaćenju školarini, domu, i ko zna čemu drugom. Kad bi se napravio samo dokaz o položenim ispitima i ocenama, ostalo bi isuviše mnogo rupa.

Razmišljajući dalje, planirajući šta da radi, setio se da bi mogao postići cilj ako bi proverio da li je fakultet pohađao diplomirani student koji se zove isto kao i on, a diplomirao je iz informatike u odgovarajućem raspornu godina. Ako je tako, mogao bi da upiše broj socijalnog osiguranja tog drugog Majkla Parkera u obrasce za zapošljavanje; ako neka kompanija i

proveri ime i broj socijalnog osiguranja na univerzitetu, biće im rečeno da zaista poseduje tu diplomu. (Većini ne bi bilo očigledno, ali njemu jeste, da može uneti jedan broj socijalnog osiguranja u molbu za posao, a potom, ako ga unajme, može upisati svoj pravi broj na obrasce za novo-zaposlene. U većini firmi ne bi se ni setili da provere da li je novi službenik upisao isti broj na oba obrasca.)

Prijavljivanje za rad

Kako u univerzitetskoj dokumentaciji pronaći nekog ko se zove Majkl Parker? Učinio je to na sledeći način.

Otišao je do glavne biblioteke u univerzitetskom gradu, seo je za terminal, uključio se na Internet, i pristupio Web lokaciji univerziteta. Potom je nazvao arhivu. Osobu koja se javila proveo je kroz poznatu rutinu obmane: „Zovem iz računskog centra. Trenutno menjamo mrežnu konfiguraciju, pa želimo da se uverimo da vam nećemo prekiniti pristup mreži. Kom serveru pristupate?“

„Kako mislite 'serveru'?“ usledilo je pitanje.

„Na koji se računar povezujete kad tražite akademske informacije o nekom studentu?“

U odgovoru koji je glasio: admin.rnsu.edu, dobio je ime računara na kome se nalazi dokumentacija o studentima. To je bio prvi deo zagonetke. Sad je znao koji mu je ciljni računar.

Uneo je URL adresu u računar, ali nije dobio odgovor – kao što je i očekivao, pristup je blokirala zaštitna barijera. Zato je uključio neki program da vidi može li pronaći bilo koju uslugu na tom računaru, i pronašao je slobodan priključak za Telnet; na taj način se računar može povezati s drugim udaljenim računarem i pristupiti mu kao da su direktno povezani *glupim terminalom*. Sve što mu je trebalo za pristup bili su standardan korisnički identifikator i lozinka.

Ponovo je pozvao arhivu, ovog puta pažljivo osluškujući da bi se uverio da razgovara s drugom osobom. Javila mu se neka gospođa, a on se ponovo predstavio kao službenik računskog centra. Upravo instaliraju nov sistem za administrativnu dokumentaciju, rekao joj je. Zamolio je da mu učini uslugu i poveže se na novi sistem, koji je još uvek u probnom režimu, kako bi proverila da li može normalno da pristupi akademskoj dokumentaciji studenata. Dao joj je IP broj na koji treba da se poveže, i objasnio joj postupak.

Naime, pomoću tog IP broja ona se povezala s računarem za kojim je Majkl sedeo u biblioteci studentskog grada. Koristeći postupak koji je već opisan u ovom poglavlju napravio je simulator – lažni ekran za prijavljivanje – koji je izgledao potpuno isto kao onaj koji je ona obično vidala. „Ne radi“, rekla mu je. „Stalno mi javlja 'Pristup neispravan'.“

Do tada je Majkl već saznao njeno korisničko ime i lozinku; misija je bila izvršena. Kazao joj je: „Da, neki nalozi nisu još prebačeni na ovaj računar. Napraviću vam nov nalog, pa ću vas ponovo pozvati“. Majkl je pazio da ne ostavi nedovršen posao, što bi svaki dobar obmanjivač trebalo da čini, pa je pozvao kasnije da kaže da probni sistem još ne radi dobro te da će, ako se ona slaže, pozvati kasnije nju ili nekog drugog ko tu radi kad otkriju u čemu je problem.

terminologija

GLUPI TERMINAL (engl. *dumb terminal*) Terminal koji nema sopstveni mikroprocesor. Takvi terminali mogu da primaju samo jednostavne naredbe i prikazuju tekstualne znakove i brojeke.

Ljubazna službenica arhive

Sad je Majkl znao kom računarskom sistemu treba da pristupi, a imao je i korisničko ime i lozinku. Ali koje naredbe se koriste za pretraživanje datoteke studenata? Baza podataka o studentima verovatno je napravljena na univerzitetu, prema njihovim specifičnim potrebama. Sigurno postoji jednostven način pristupanja podacima u bazi.

Prvi korak u prevazilaženju ove poslednje poteškoće: mora pronaći nekoga ko bi ga proveo kroz misterije pretraživanja baze podataka o studentima. Ponovo je pozvao arhivu, i ovaj put mu se javila druga osoba. Gospođa je rekao da zove iz kancelarije dekana Elektrotehničkog fakulteta, i upitao je: „Koga treba da pozovemo da nam pomogne ako imamo problema s pristupanjem akademskim dokumentima studenata?“

Nakon nekoliko trenutaka razgovarao je s administratorom univerzitetske baze podataka, kod kog je igrao na kartu sažaljenja: „Ovde Mark Selers, iz arhive. Da li biste se sažalili na novajliju? Izvinjavam se što vas zovem, ali svi su na nekom sastanku danas poslepodne, pa nema ko da mi pomogne. Treba da pronađem spisak svih studenata koji su diplomirali informatiku

od 1990. do 2000. godine. Moram da završim izveštaj do kraja dana, a ako to ne uradim, možda neću dugo zadržati posao. Da li biste pomogli momku u nevolji?" Pomaganje ljudima bilo je deo posla ovog administratora baze podataka, pa je izuzetno strpljivo, korak po korak, objašnjavao Majklu postupak.

Kad su završili razgovor, Majkl je već učitao čitav spisak onih koji su pomenutih godina diplomirali informatiku. Za nekoliko trenutaka počeo je pretraživanje, pronašao dva Majkla Parkera, odabrao jednog, našao njegov broj socijalnog osiguranja i druge bitne informacije u bazi podataka.

Analiza prevare

U ovoj prevari primenjen je trik o kojem ranije nisam govorio: napadač je zamolio administratora baze podataka da mu potanko objasni kako da izvrši jednu proceduru na računaru koju nije umeo da izvede. To je moćna i efikasna zamena uloga, i isto je kao da ste zamolili vlasnika radnje da vam pomogne da do kola odnesete kutiju u kojoj se nalazi roba koju ste upravo ukrali s njegovih polica.

mitnikova poruka

Ponekad korisnici računara nemaju predstavu o tome koliko je današnji tehnološki svet ranjiv i koje opasnosti vrebaju. Oni imaju pristup informacijama, ali ne poznaju pojedinosti potencijalnog narušavanja bezbednosti. Obmanjivači će odabrati zaposlenog koji slabo shvata značaj tražene informacije, jer će takva osoba lakše udovoljiti zahtevu neznanca.

SPREČAVANJE PREVARE

Sažaljenje, osećaj krivice i zastrašivanje jesu tri veoma popularna psihološka momenta koja se upotrebljavaju u obmanama, a u ovim pričama pokazali smo vam kako se te metode primenjuju u stvarnosti. Šta vi i vaša kompanija možete učiniti da biste izbegli takve napade?

Zaštitite podatke

U nekim pričama u ovom poglavlju naglašeno je koliko je opasno slati dokumenta nekome koga ne poznajete, pa čak i ako je ta osoba kolega (ili se

tako čini), a dokument šaljete *interno*, na adresu elektronske pošte ili faks mašinu u okviru firme.

Kompanijska pravila bezbednosti treba jasno da propišu način izdavanja vrednih podataka bilo kome koga pošiljalac ne poznaje lično. Valja ustanoviti tačne procedure za prenos poverljivih dokumenata. Kad podatke zahteva neko koga zaposleni ne poznaje lično, moraju postojati jasno definisani koraci za utvrđivanje identiteta, različitog nivoa, u zavisnosti od poverljivosti informacija.

Evo nekih metoda koje valja razmotriti:

- Utvrdite zašto su nekome potrebne date informacije (za šta može biti neophodna dozvola od vlasnika te informacije).
- Vodite zapisnik o tim transakcijama za sebe ili čitavo odeljenje.
- Napravite spisak osoba koje su posebno obučene za takve procedure i kojima je povereno da odobre slanje poverljivih informacija. Zahtevajte da samo te osobe smeju da šalju podatke bilo kome van radne grupe.
- Ako se zahtev za podatke pošalje napismeno (elektronskom poštom, faksom, ili pismom), preduzmite dodatne bezbednosne mere da biste proverili da li je zahtev zaista uputila osoba koja je navodno poslala dopis.

O lozinkama

Svi zaposleni koji mogu da pristupe bilo kakvim poverljivim informacijama – a danas je to gotovo svaki radnik koji koristi računar – treba da shvate da jednostavne stvari, poput izmene lozinke, čak i na samo nekoliko trenutaka, mogu dovesti do velikog narušavanja bezbednosnog sistema.

U bezbednosnu obuku treba uvrstiti i temu o lozinkama, a tu se delom valja usredsrediti na to kako i kada promeniti lozinku, od čega se sastoji prihvatljiva lozinka, i koje su opasnosti ako dopustite da iko bude prisutan za vreme tog postupka. U obuci, svim zaposlenima treba posebno preneti da sumnjaju u *svaki* zahtev u vezi s lozinkama.

Na prvi pogled, čini se da je to jednostavna poruka koju valja preneti zaposlenima. Ali ona to nije jer, da bi je zaposleni razumeli, moraju shvatiti kako nešto jednostavno poput izmene lozinke može dovesti do narušavanja bezbednosnog sistema. Detetu možete govoriti: „Gledaj na obe strane pre nego što pređeš ulicu“, ali sve dok ono ne shvati zašto je to važno, oslanjate

se na slepu poslušnost. Pravila koja zahtevaju slepu poslušnost uglavnom se ignorišu ili zaboravljaju.

napomena

Lozinke su toliko bitne u obmanama, da smo toj temi posvetili poseban odeljak u poglavlju 16, gde ćete pronaći preporučena pravila za rad s lozinkama.

Centralno mesto za prijavljivanje

U svom pravilniku bezbednosnog sistema trebalo bi da odredite jednu osobu ili grupu kojoj će se prijavljivati sumnjive radnje, tj. one koje izgledaju kao pokušaji da se neko uvuče u vašu organizaciju. Svi zaposleni treba da znaju koga da pozovu kad posumnjaju na pokušaj elektronskog ili fizičkog upada. Telefonski broj tog mesta treba uvek da bude zaposlenima pri ruci, kako ne bi morali da ga traže ako posumnjaju da se napad upravo odvija.

Zaštite mrežu

Zaposleni treba da shvate da ime računarskog servera ili mreže nisu beznačajne informacije, već da napadaču mogu obezbediti osnovno saznanje pomoću kojeg će zadobiti nečije poverenje ili pronaći mesto na kojem su smešteni željeni podaci.

Osobe poput administratora baza podataka, koji rade sa softverom, pripadaju kategoriji onih koji imaju tehnološko znanje. Takvi pojedinci moraju poštovati posebna i veoma stroga pravila u vezi sa utvrđivanjem identiteta osoba koje ih zovu radi informacija ili saveta.

Radnici koji redovno drugima pomažu s računarima moraju se dobro obučiti da prepoznaju pokušaj prevare i koje zahteve treba da smatraju signalima za uzbunu.

Ništa ne vredi to što je iz perspektive administratora baze podataka iz poslednje priče u ovom poglavlju napadač zadovoljio kriterijume da bi se smatrao legitimnim: zvao je iz studentskog grada, i očigledno se nalazio na lokaciji na intranetu za koju mu je bilo potrebno korisničko ime i lozinka. To samo iznova naglašava koliko je važno imati standardizovane procedure

za utvrđivanje identiteta svakoga ko zahteva informacije, a pogotovo u ovakvom slučaju, kad sagovornik traži pomoć da bi pristupio poverljivim dokumentima.

Sve ove savete treba shvatiti dvostruko ozbiljnije na koledžima i univerzitetima. Svi znaju da je hakerisanje omiljena razbibriga mnogim studentima, pa takođe ne bi trebalo da vas začudi to što je studentska dokumentacija – a ponekad i dokumentacija profesora – primamljiva meta. Takva zloupotreba je veoma česta. Neka preduzeća smatraju studentske računarske sisteme opasnim, te podižu zaštitne barijere kojima blokiraju pristup iz obrazovnih institucija sa adresama koje se završavaju na .edu.

Na kraju, zaključak je da svu dokumentaciju o studentima i osoblju treba smatrati mogućom metom napada, te da je valja dobro zaštititi kao poverljive informacije.

Saveti za obuku

Od većine obmana može se odbraniti izuzetno lako... svako ko zna na šta da obrati pažnju.

Kad su preduzeća u pitanju, neophodna je dobra obuka. Ali potrebno je i nešto drugo: razni načini da se ljudi *podsete* na ono što su naučili.

Na ekranu koji se pojavi svaki put kad se korisnikov računar upali, svakog dana prikazujte drugačiju poruku o bezbednosti. Poruka ne treba da nestaje sama – korisnik mora da pritisne nekakvo dugme i potvrdi da ju je pročitao.

Preporučujem vam da napravite seriju podsetnika na bezbednosna pitanja. Česti podsetnici su važni; program za podizanje svesti o nečemu mora da traje i nikada ne sme da prestane. Podsetnike ne treba uvek sročiti na isti način. Studije su pokazale da se takve poruke bolje prihvataju kad su sročene drugačije od prethodnih, ili kad se koriste u različitim primerima.

Odličan pristup je da se koriste balončići u kompanijskim biltenima. To ne treba da bude čitav članak o datoj temi, iako bi strana o bezbednosti sigurno bila bitna. Umesto toga, dizajnirajte umetak širine dva ili tri stupca, poput male reklame u lokalnom biltenu. U svakom izdanju objavite nov podsetnik o bezbednosti u ovom kratkom i atraktivnom obliku.



poglavlje

9

Obrnuta žaoka

U filmu *Žaoka*, koji se pominje i drugde u ovoj knjizi (i koji je, po meni, verovatno najbolji film o prevari), prevara je prikazana do zapanjujućih pojedinosti. Operacija žaoka u filmu verno oslikava kako glavni prevaranti organizuju „mrežu“, a to je jedna od tri vrste velikih obmana poznatih kao „velike prevare“. Ako želite da saznate kako se tim profesionalaca na prevaru domogne ogromne sume novca za jedno veče, nema boljeg udžbenika od tog filma.

Prevaranti starog kova, kakva god obmana bila u pitanju, vladaju se po nekom šablonu. Ponekad se prevara dogodi na obrnut način, što se naziva *obrnuta žaoka*. U ovom zanimljivom preokretu napadač tako organizuje situaciju da žrtva *njega* nazove tražeći pomoć, ili kolega ima neki zahtev, na koji napadač odgovori.

Kako se to postiže? Uskoro ćete saznati.

UMETNOST PRIJATELJSKOG UBEĐIVANJA

Kad prosečna osoba zamisli hakera, obično joj prvo padne na pamet slika usamljenog, povučenog čudaka čiji je najbolji prijatelj računar, i ko ima problema s konverzacijom opširnijom od, razmene kratkih poruka. Obmanjivači često poznaju hakerske veštine, ali, s druge strane, umeju da se ophode i s ljudima – oni imaju visokorazvijene sposobnosti za iskorišćavanje ljudi i manipulisanje njima, na osnovu čega uspevaju rečima da se domognu informacija, na načine za koje nikada ne biste poverovali da su mogući.

terminologija

OBRNUTA ŽAOKA (engl. *reverse sting*) Prevara u kojoj žrtva moli napadača za pomoć.

Anđelin sagovornik

Mesto: filijala Veli, Industrijska federalna banka

Vreme: 11:27

Anđela Visnovski se javila na telefon. Njen sagovornik je rekao da upravo treba da nasledi pozamašnu svotu novca, te da su mu potrebne informacije o različitim vrstama štednih knjižica, potvrdama o depozitu, kao i o drugim investicijama koje bi mogla da mu predloži a da su sigurne i da donose pristojnu kamatu. Objasnila mu je da postoji mnogo mogućnosti i upitala ga da li bi došao i natenane porazgovarao. On odlazi na put čim novac stigne, rekao je, i ima još mnogo poslova da posvršava. Tako je ona počela da mu preporučuje neke od mogućnosti, da mu daje detalje o kamatama, obaveštava o tome šta se dešava ako se potvrde o depozitu prodaju ranije, i tako dalje, istvremeno pokušavajući da utvrdi svrhu njegovog investiranja.

Učinilo joj se da ima nekog napretka, kad on reče: „Izvinite, moram da se javim, imam drugu vezu. Kada bismo mogli da nastavimo ovaj razgovor da bih doneo odluke? Kada imate pauzu za ručak?“ Odgovorila je da ruča u 12:30, pa je rekao da će pokušati da je ponovo nazove sutradan, pre tog vremena.

Luisov sagovornik

Velike banke koriste interne bezbednosne kodove koji se menjaju svakodnevno. Kad su neke iz jedne filijale potrebni podaci iz druge, kao dokaz ovlašćenja navodi se kôd za taj dan. Radi dodatne sigurnosti i fleksibilnosti, neke velike banke svakodnevno objavljuju nekoliko kodova. U banci na Zapadnoj obali koju ću nazvati Industrijska federalna banka, svaki zaposleni svakog jutra na računaru nalazi spisak od pet šifara za taj dan, koje se identifikuju slovima od A do E.

Mesto: isto.

Vreme: 12:48, istog dana.

Luis Hepbern nije poklonio posebnu pažnju pozivu koji je primio tog poslepodneva. Bio je to poziv kao i drugi koje je primao redovno, nekoliko puta nedeljno.

„Halo“, reče glas s druge strane žice. „Ovde Nil Vebster. Zovem iz filijale 3182 u Bostonu. Molio bih Anđelu Visnovski.“

„Na ručku je. Mogu li ja da vam pomognem?“

„Pa, ostavila nam je poruku da joj faksom pošaljemo informacije o jednom od naših klijenata.“

Zvučalo je kao da sagovornik ima loš dan.

„Osoba koja se obično bavi takvim zahtevima je na bolovanju“, reče. „Imam ovde čitavu hrpu takvih zahteva, skoro je četiri sata, a ja treba već da pođem jer imam zakazan lekarski pregled za pola sata.“

Manipulacija – davanje svih mogućih razloga zbog kojih bi ga druga osoba sažaljevala – bila je deo omekšavanja žrtve. Nastavio je: „Ko god da je primio njenu telefonsku poruku, broj faksa je nečitljiv. Počinje sa 213. Kako ide dalje?“

Luis mu je dao broj faksa, a sagovornik reče: „U redu, hvala. Pre nego što pošaljem ovo faksom, moram vas zamoliti za kôd B.“

„Ali vi ste mene nazvali“, reče on dovoljno oštro da bi čovek iz Bostona shvatio poruku.

Ovo je dobro, pomisli sagovornik. Baš je sjajno kad ljudi ne nasednu na prvu loptu. Ako ne pruže bar malo otpora, posao je suviše lak i mogao bih da se ulenjim.

Varalica nastavi: „Upravnik naše filijale je postao paranoičan u vezi s traženjem identifikatora pre nego što išta pošaljemo; to je sve. Ali čujte, ako vam trebaju te informacije, u redu je. Nema ni potrebe za identifikacijom.“

„Čujte“, odvrati Luis. „Anđela se vraća za otprilike pola sata. Mogu joj reći da vas nazove.“

„Ja ću joj reći da danas nisam mogao da joj pošaljem podatke jer niste hteli da potvrdite da je to legitiman zahtev tako što biste mi dali kôd. Ako sutra ne budem na bolovanju, nazvaću je.“

„U redu.“

„Na poruci stoji 'Hitno'. Nije važno, ja ne mogu ništa da učinim bez identifikacije. Reći ćete joj da sam pokušao da ih pošaljem, ali da niste hteli da mi date kôd, u redu?“

Luis je popustio pod pritiskom. Njegov ljutiti uzdah začuo se kroz telefonsku liniju.

„Dobro“, rekao je, „sačekajte trenutak; moram da odem do računara. Koji kôd vam treba?“

„B“, reče sagovornik.

Spustio je slušalicu, a potom je za nekoliko trenutaka ponovo podigao. „Kod je 3184.“

„To nije taj kôd.“

„Jeste – B je 3184.“

„Nisam rekao B nego E.“

„Oh, do đavola. Sačekajte malo.“

Usledila je još jedna stanka dok je ponovo tražio kodove.

„E je 9697.“

„9697 – tako je. Poslaću faks. U redu?“

„Naravno. Hvala.“

Volterov sagovornik

„Industrijska federalna banka, ovde Volter.“

„Zdravo, Voltere, ovde Bob Grabovski iz Studio Sitija, filijala 38“, reče njegov sagovornik. „Treba da pronađete karticu s potpisom za jedan korisnički račun i da mi je pošaljete faksom.“

Kartica s potpisom ne sadrži samo potpis klijenta. Na njoj se takođe nalaze podaci za identifikaciju, te uobičajeni podaci poput broja socijalnog osiguranja, datuma rođenja, majčinog devojčkog prezimena, a ponekad čak i broja vozačke dozvole. To može biti vrlo korisno obmanjivačima.

„Naravno. Koji je kôd C?“

„Drugi blagajnik trenutno koristi moj računar“, reče sagovornik. „Ali upravo sam upotrebio kodove B i E, pa ih se sećam. Pitaj me za jedan od njih.“

„U redu, koji je kod E?“

„E je 9697.“

Za nekoliko minuta, Volter je faksom poslao traženu karticu s potpisom.

Sagovornik Done Plejs

„Dobar dan, ovde gospodin Anselmo.“

„Kako vam danas mogu pomoći?“

„Koji ono broj koji počinje sa 800 treba da pozovem kad hoću da proverim da li je uplata stigla na račun?“

„Jeste li vi klijent banke?“

„Da, a nisam upotrebio taj broj već dugo, pa sad ne znam gde sam ga zapisao.“

„Broj je 800-555-8600.“

„Hvala vam.“

Priča o Vinsu Kapeliju

S obzirom na to da je bio sin uličnog policajca iz Spokejna, Vins je odmalena znao da neće provesti život mukotrpno radeći do kasno i rizikujući glavu za minimalnu platu. Dva osnovna cilja u životu su mu postala da ode iz Spokejna, i da osnuje sopstveni posao. To što su mu se drugovi podsmevali tokom čitave srednje škole samo ga je još više podstaklo – smatrali su da je užasno smešno što je toliko ponosan na svoj budući biznis, a još ne zna kakav bi to posao mogao biti.

Vins je potajno znao da su u pravu. Bio je dobar samo kao hvatač u srednjoškolskom bejzbol timu. Ali nije bio dovoljno dobar da bi dobio stipendiju za koledž, a ni približno dovoljno dobar za profesionalnog igrača bejzbola. Pa kojim će onda poslom moći da se bavi?

Momci koji su se s Vinsom družili nikako nisu mogli da shvate kako bilo šta što neko od njih ima, a Vinsu se dopada – postaje Vinsovo, bio to nov mož skakavac, sjajan par novih rukavica, ili nova. Nije krao, niti se ikome prikradao iza leđa; nije morao. Drug bi mu svojevolljno dao šta želi, a potom se pitao kako se to dogodilo. Čak ni kad biste ga pitali ne biste ništa saznali, jer ni on sam to nije znao. Činilo se da ljudi Vinsu prepuštaju sve što poželi.

Vins Kapeli se počeo baviti obmanjivanjem od malena.

Prijatelji su prestali da mu se podsmevaju kad su svi maturirali. Dok su se drugi muvali gradom tražeći poslove u kojima se nije moralo govoriti „Želite li i prženi krompir s tim?“ Vinsa je otac poslao da porazgovara s jednim starim prijateljem koji je napustio policiju i osnovao privatnu detektivsku agenciju u San Francisku. Ubrzo je uvideo Vinsov talenat za posao, i primio ga.

To je bilo pre šest godina. Mrzeo je traženje dokaza o nevernim supružnicima, kada se satima dosađivao, mukotrpno sedeći i osmatrajući. Stalni izazov je predstavljalo iskopavanje informacija o nečijoj imovini što treba advokatima da utvrde da li je neki jadnik dovoljno bogat da bi ga vredelo tužiti. U takvim zadacima imao je dovoljno prilika da upotrebi svoju umešnost.

Kao što je postupio kad je trebalo da proveriti bankovni račun Džoa Markovica. Džo je možda ranije obmanuo nekadašnjeg prijatelja, koji je sad želeo da sazna da li je Markovic dovoljno bogat, kako bi ako ga tuži, možda izvukao bar deo sopstvenog novca.

Vinsov prvi korak bio je da otkrije bar jedan, ili još bolje dva bančina bezbednosna koda za taj dan. To zvuči kao gotovo nemoguć izazov. Šta bi, za ime sveta, navelo jednog bankarskog službenika da oslabi sopstveni bezbednosni sistem? Zapitajte se – kad bi ste vi želeli to da učinite, da li biste imali ideju kako to da izvedete?

Za ljude poput Vinsa, to je sasvim lako.



Ljudi vam veruju ako poznajete internu terminologiju njihovog posla i kompanije. To je kao da dokazujete da pripadate tom zatvorenom krugu. Kao tajno rukovanje.

Nije mi trebalo mnogo toga za ovakav posao. Svakako nisam razbijao glavu. Za početak mi je trebao samo broj filijale. Kad sam nazvao filijalu u ulici Bikon u Bafalu, glas čoveka koji se javio zvučao je kao mašina.

„Ovde Tim Ekerman“, rekoh. Moglo je doći u obzir bilo koje ime, jer ga neće zapisati. „Koji vam je broj filijale?“

„Telefonski broj ili broj filijale?“ hteo je da zna, što je bilo prilično glupo jer sam upravo pozvao taj telefonski broj, zar ne?

„Broj filijale.“

„3182“, odgovori. Tek tako. Nije rekao: „Zašto to želite da znate?“, niti bilo šta slično. Jer to nije poverljiva informacija; nalazi se na gotovo svakom papiru koji koriste.

Drugi korak – nazvao sam filijalu koju koristi naša žrtva, dobio sam ime jedne od njihovih službenica i saznao kad će ta osoba biti na ručku. Zvala se Andela. Odlazi u 12:30. Zasad – odlično.

Treći korak – pozvao sam istu filijalu za vreme Andeline pauze za ručak, rekao da zovem iz filijale čiji je broj taj-i-taj iz Bostona, da Andeli treba faksom da se pošalju neke informacije, te da mi daju kôd za taj dan. To je bio problematičan deo zadatka; osetio sam otpor. Da ja sastavljam testove iz obmane, uvrstio bih u njih nešto ovako, gde žrtva postane sumnjičava – s punim pravom – a vi se i dalje ne date sve dok je ne slomite i izvučete iz nje potrebne podatke. To se ne može uraditi deklamovanjem rečenica iz scenarija; morate biti sposobni da procenite žrtvu, prepoznate njeno raspoloženje, da se igrate njom kao kad se lovi riba, pa se struna malo popusti, a onda opet zategne, popusti, pa zategne. Sve dok ga ne uhvatite mrežom i ubacite u čamac – pljus!

Tako sam ga upecao i dobio jedan od kodova za taj dan. Bio je to velik korak. U mnogim bankama koristi se samo jedan, pa bi ovaj zadatak bio okončan. U Industrijskoj federalnoj banci koristi se pet kodova, a ja sam imao jedan od njih, što mi je davalo loše izgleda. Sa dva od pet imao bih mnogo bolje šanse da okončam i sledeći čin ove male drame. Svida mi se onaj deo kad sam rekao „Nisam rekao B, nego E.“ Kad upali, to je sjajno. Uglavnom uvek uspe.

Da sam dobio i treći kôd, bilo bi još bolje. Jednom sam zaista uspeo da dobijem sva tri koda jednim telefonskim pozivom – „B“, „D“ i „E“ zvuče toliko slično da možete tvrditi kako su vas ponovo pogrešno razumeli. Ali sagovornik vam mora biti neko ko je zaista slab protivnik. Ovaj čovek to nije bio. Odlučio sam se za dva.

Kodovi za taj dan bili su mi adut da se domognem kartice s potpisom koju sam tražio. Pozvao sam, a čovek me je upitao za kôd. Hteo je kôd C, a ja sam imao samo B i E. Ali nije to kraj sveta. U takvim trenucima morate ostati prisebni, zvučati samouvereno, i nastaviti igru. Mirno sam ga obradio rekavši: „Neko koristi moj računar, pa me pitaj za jedan od ovih.“

Svi smo mi zaposleni u istoj firmi, svi smo u ovome zajedno, treba olakšati posao ovom momku – nadate se da žrtva tako razmišlja u ovakvim trenucima. A on je odigrao baš prema scenariju. Odabrao je jedan od

ponuđenih kodova, ja sam mu tačno odgovorio, a on mi je poslao faks kartice s potpisom.

Još malo pa gotovo. Pomoću još jednog poziva, dobio sam broj koji korisnici pozivaju radi automatskog očitavanja stanja na računima. Na kartici s potpisom imao sam sve žrtvine brojeve računa i njegov PIN kôd, jer se u toj banci upotrebljavalo prvih pet ili poslednje četiri cifre broja socijalnog osiguranja. S olovkom u ruci, nazvao sam taj telefonski broj, i nakon nekoliko minuta pritiskanja dugmića imao sam najsvežiji izveštaj o stanju na sva četiri njegova računa, a kao dopunu i najsvežije uplate i isplate na svakom od njih.

To je bilo sve što moj klijent traži, pa i više od toga. Ja uvek volim da dodam malo, kao dopunu. To klijente čini srećnima. Najzad, stalne mušterije su ono što održava posao, je li tako?

Analiza prevare

Ključ za čitavu ovu epizodu ležao je u tome da se dođe do izuzetno važnih dnevnih kodova, a da bi to učinio, Vins je primenio nekoliko različitih tehnika.

Počeo je s malo verbalnog iznudiivanja kad se ispostavilo da Luis ne želi da mu dâ kôd. Luis je s pravom bio sumnjičav, jer se kodovi koriste na drugačiji način. Znao je da obično nepoznat sagovornik *njemu* daje bezbednosni kôd. To je bio presudni trenutak, od kojeg je zavisio Vinsov uspeh.

Uprkos Luisovoj sumnjičavosti, Vins je na to sve nastavio s manipulacijom, apelujući na njegovo sažaljenje („idem kod lekara“), potom vršeći pritisak („Imam ovde čitavu hrpu takvih, a skoro je četiri sata“), pa opet manipulišući („Recite joj da niste hteli da mi date kôd“). Vins je bio dovoljno pametan da mu ne zapreti. Pretnja se samo podrazumevala: ako mi ne date bezbednosni kôd, neću poslati informacije o klijentu koje su potrebne vašoj kolegici, i reći ću joj da sam hteo to da učinim, ali da vi niste hteli da sarađujete.

Pa ipak, nemojmo suviše olako okriviti Luisa. Na kraju krajeva, osoba s druge strane žice znala je (ili se bar tako *činilo*) da je njegova kolegica Andela zatražila faks. Njegov sagovornik je znao za bezbednosne kodove, kao i to da se identifikuju pomoću slova. Rekao je da to zahteva upravnika njegove filijale radi veće sigurnosti. Naizgled, nije bilo nikakvog razloga da mu ne da potvrdu koju traži.

Nije u pitanju samo Luis. Bankarski službenici svakodnevno odaju bezbednosne kodove obmanjivačima. To je neverovatno, ali istinito.

Postoji granica, poput linije povučene u pesku, iza koje tehnike privatnih istražitelja prestaju da budu zakonite i postaju nezakonite. Vins je i dalje vršio zakonitu radnju kad se domogao broja filijale. Bilo je zakonito čak i to što je na prevaru od Luisa dobio dva bezbednosna koda za taj dan. Prešao je granicu kad su mu faksom poslate poverljive informacije o klijentu banke.

No, za Vinsa i njegovog poslodavca takvo krivično delo nosi malo rizika. Kad ukradete novac ili robu, neko će primetiti da je nema. Kad ukradete informacije, uglavnom niko ne primeti, jer su one i dalje tamo gd su bile.

mitnikova poruka

Verbalni bezbednosni kodovi su isto što i lozinke; oni su zgodno i pouzdano sredstvo za zaštitu podataka. Ipak, zaposleni moraju biti obavešteni o trikovima koje koriste obmanjivači, i moraju biti obučeni da nikom ne predaju ključeve kraljevstva.

NAIVNI POLICAJCI

Sumnjivim privatnim istražiteljima i obmanjivačima često bi bilo zgodno da znaju broj nečije vozačke dozvole (koja se u SAD koristi umesto lične karte) – na primer, ako žele da se predstavljaju kao neko drugi da bi dobili podatke o izvodima s bankovnih računa.

Ako izuzmemo krađu novčanika te osobe, ili virenje preko ramena u zgodnoj prilici, domoći se broja nečije vozačke dozvole trebalo bi da bude gotovo nemoguće. Za prosečnog obmanjivača to i nije neki izazov.

Konkretno, jednom obmanjivaču – zvaću ga Erik Mantini – redovno su trebali brojevi vozačkih i saobraćajnih dozvola. Erik je pomislio da će se nepotrebno izložiti većem riziku ako pozove auto-moto savez i uvek iznova primeni isti trik kad god mu trebaju informacije. Pitao se da li postoji način da se postupak pojednostavi.

Verovatno se niko toga nije setio pre njega, a on je u tren oka smislio kako da dođe do informacija kad god mu trebaju. To je postigao iskoristivši uslugu koju pruža auto-moto savez njegove države. Mnogi državni

auto-moto savezi (ili slične organizacije, kako god se zvale u vašoj državi) obelodanjuju poverljive informacije o građanima osiguravajućim društvima, privatnim istražiteljima i drugima, koji po zakonu imaju pravo na njihovu upotrebu zarad dobrobiti čitavog društva.

Naravno, AMS ima odgovarajuća pravila o tome kakvi se podaci mogu obelodanjivati. Osiguravajuća društva mogu dobiti samo određene vrste informacija iz dosijea. Drugačiji skup pravila odnosi se na privatne istražitelje, i tako dalje.

Što se tiče kriminalističke službe, uglavnom se primenjuje drugačije pravilo – AMS će dati sve podatke iz dosijea svakom policajcu pod zakletvom koji se identifikuje na odgovarajući način. U državi u kojoj je Erik tada živio, potrebna identifikacija se zvala Šifra podnosioca molbe, a izdavao ga je AMS, zajedno s brojem vozačke dozvole dotičnog policajca. Zaposleni u AMS uvek proveravaju identitet tako što uporede ime policajca sa brojem njegove vozačke dozvole i još nekim podatkom – obično datumom rođenja – pre nego što izdaju informacije.

Erik, iskusan obmanjivač, želeo je, ni više ni manje, nego da preuzme identitet nekoga iz kriminalističke službe.

Kako mu je to pošlo za rukom? Tako što je izveo trik obrnute žaoke s policajcima!

Erikova žaoka

Prvo je nazvao odgovarajuću službu informacija i zatražio telefonski broj glavne filijale AMS-a u glavnom gradu te države. Dobio je broj 503-555-5000, što je, razume se, broj za pozive običnih građana. Potom je nazvao obližnju šerifovu kancelariju i zamolio da ga spoje s Teletajpom – kancelarijom preko koje se održavala komunikacija s drugim kriminalističkim službama i nacionalnom bazom podataka o krivičnim delima. Odatle su se slali lokalni nalozi za pretres i hapšenje, i tako dalje. Kad su ga spojili s Teletajpom, rekao je da mu treba telefonski broj koji kriminalistička služba koristi kad zove glavnu filijalu AMS-a u državi.

„Ko ste vi?“ upita policajac iz Teletajpa.

„Ovde Al. Zvao sam 503-555-5753“, odgovori. To je delom bila pretpostavka, a delom broj koji mu je tek pao na pamet; sigurno specijalna kancelarija AMS-a koja prima pozive iz kriminalističke službe ima isti

pozivni broj kao i broj koji je namenjen običnim građanima, a bilo je gotovo isto tako sigurno da su i sledeće tri cifre, takozvani prefiks, iste. Samo je trebalo da sazna poslednje četiri cifre.

U šerifovu kancelariju Teletajp ne stižu pozivi od običnih građana. A sagovornik je znao veći deo broja. Očigledno je bio pravi policajac.

„Broj je 503-555-6127“, odvrati policajac.

Tako je Erik sada imao specijalan telefonski broj na koji policajci zovu AMS. Eriku nije bio dovoljan jedan broj; ta kancelarija verovatno ima mnogo više telefonskih linija, a Eriku je trebalo da sazna koliko ih je, i koji su im brojevi.

Centrala

Da bi izveo svoj plan, trebalo je da pristupi telefonskoj centrali koja radi s telefonskim linijama što dolaze iz kriminalističke službe u AMS. Nazvao je državne Telekomunikacije i predstavio se da je iz Nortela, firme koja proizvodi DMS-100, jednu od najrasprostranjenijih komercijalnih telefonskih centrala. Rekao je: „Možete li me, molim vas, spojiti s jednim od tehničara za centrale koji radi na tipu DMS-100?“

Kad se tehničar javio, predstavio se da je iz Nortelovog centra za tehničku podršku u Teksasu, i objasnio da prave matičnu bazu podataka kako bi ažurirali softver na svim centralama. Sve će se izvršiti na daljinu – nema potrebe da u tome učestvuje ijedan tehničar. Ali potreban im je broj koji se zove da bi se priključili na centralu i ažurirali je direktno iz Centra za podršku.

Zvučalo je sasvim verovatno, pa je tehničar dao Eriku telefonski broj. Sad je mogao direktno da se priključi na jednu od državnih telefonskih centrala.

Radi odbrane od uljeza, takve komercijalne centrale zaštićene su lozinkom, baš kao i svaka kompanijska računarska mreža. Svaki obmanjivač koji se nekada bavio telefonskim prevarama zna da za Nortelove centrale postoji podrazumevano korisničko ime za ažuriranje softvera: NTAS (to je skraćenica za Nortelova tehnička podrška, engl. *Nortel Technical Assistance Support*; nije baš promućurno). A šta je s lozinkom? Erik se priključio nekoliko puta, svaki put pokušavajući s nekom logičnom i često korišćenom lozinkom. Kad je kao lozinku uneo korisničko ime, NTAS, nije mu uspelo. Nije upalila ni reč „pomagač“. Nije ni „zakrpa“.

Potom je pokušao „ažuriranje“... i uključio se. Kako je to tipično. Koristiti očiglednu lozinku koja se lako može pogoditi samo je malo bolje nego nemati nikakvu lozinku.

Zgodno je kad ste dobri u svom poslu; Erik je verovatno znao isto toliko o toj centrali kao i tehničari – kako da je programira ili popravi problem. Kad je uspeo da joj pristupi, mogao je potpuno da kontroliše telefonske linije. Sa svog računara, na centrali je potražio dobijeni telefonski broj, na koji policajci iz kriminalističke službe pozivaju AMS – 555-6127. Otkrio je postoji još devetnaest drugih telefonskih linija za isti odsek. Očito su primali velik broj poziva.

Centrala je bila programirana tako da pri svakom pozivu traži slobodnu liniju od postojećih dvadeset.

Odabrao je liniju broj osamnaest, i uneo kôd pomoću kojeg su se pozivi s te linije mogli prosledivati dalje. Kao broj za prosleđivanje poziva, uneo je telefonski broj svog novog, jeftinog mobilnog telefona s pretplatnom karticom, kakav rasturači droge vole da koriste, jer su dovoljno jeftini da bi se mogli baciti nakon što se obavi posao.

Pošto je prosleđivanje poziva uključeno na osamnaestoj liniji, čim u kancelariji postane dovoljno prometno tako da istovremeno odgovaraju na sedamnaest poziva, sledeći poziv neće se oglasiti u kancelariji AMS-a, nego će biti prosleđen do Erikovog telefona. Zavalio se u stolici i čekao.

Poziv AMS-u

Malo pre osam sati tog jutra, zazvonio je mobilni telefon. Taj deo mu je bio najbolji, najdraži. Eto, Erik prevarant razgovara s policajcem koji može da dođe i uhapsi ga, ili da dobije nalog za pretres i izvrši raciju kako bi pokupio dokaze protiv njega.

Nije pozvao samo jedan policajac, već više njih, jedan za drugim. Jednom prilikom, Erik je sedeo u restoranu, ručao s prijateljima, i primao pozive otprilike svakih pet minuta, zapisujući podatke na salvetu pozajmljenom olovkom. Još uvek mu je to užasno smešno.

Razgovor s policajcima ni najmanje ne zbunjuje pravog obmanjivača. Štaviše, usled uzbuđenja što je obmanuo kriminalističke službe verovatno još više uživa u svemu tome.

Kako Erik tvrdi, pozivi su zvučali otprilike ovako:

„AMS, šta mogu da učinim za vas?“

„Ovde detektiv Endru Kol.“

„Zdravo, detektive. Šta danas mogu da učinim za vas?“

„Potreban mi je Saundeks za vozačku dozvolu broj 005602789“, rekao bi, na primer, upotreбивši izraz za fotografiju poznat u kriminalističkoj službi – a slika je korisna, na primer, kad policajci treba da uhapsu osumnjičenog, pa žele da znaju kako izgleda.

„Svakako, sačekajte da pogledam dosije“, odvratio bi Erik. „Detektive Kol, iz koje ste vi službe?“

„Iz okruga Džeferson.“ Potom bi Erik postavio škakljiva pitanja: „Detektive, koja je vaša šifra?“ „Koji je broj vaše vozačke dozvole?“ „Kad ste rođeni?“

Sagovornik bi mu otkrio lične podatke za identifikaciju. Erik bi naizgled proveravao informacije, a potom rekao sagovorniku da su podaci za identifikaciju odobreni, te bi pitao o pojedinostima koje je želeo da sazna od AMS-a. Pretvarao se da traži dotično ime, dok je slušalac mogao da čuje kako pritiska tastere, a onda bi rekao nešto poput: „O, do đavola, računar mi se ponovo pokvario. Izvinite, detektive, računar mi ne radi dobro čitave nedelje. Da li biste nas ponovo pozvali, i zatražili pomoć od drugog službenika?“

Na taj način bi okončao poziv ne ostavljajući nedovršen posao, a da policajac ništa ne posumnja o tome zašto nije mogao da mu odgovori na zahtev. U međuvremenu, Erik bi saznao pojedinosti koje je mogao upotrebiti kako bi dobio poverljive informacije od AMS-a kad god mu zatrebaju.

Nakon što je nekoliko sati primao pozive i domogao se šifri desetine podnosilaca molbi, Erik se ponovo povezao na centralu i deaktivirao prosleđivanje poziva.

Mesecima nakon toga, obavljao je zadatke koje su mu slali pravi privatni istražitelji, koji nisu želeli da znaju kako dolazi do informacija. Kad god je bilo potrebno, on bi se ponovo povezao na centralu, aktivirao prosleđivanje, i sakupio još jednu gomilu identifikacionih podataka policajaca.

Analiza prevare

Vratimo se malo unazad i pogledajmo iz početka kako je Erik prevario niz ljudi da bi mu ova obmana uspeła. U prvom uspešnom koraku, naveo je šerifovog zamenika u sobi za komunikacije da oda poverljivi broj AMS-a potpunom neznancu, jer je pretpostavljao da mu je sagovornik isto zamenik šerifa, pa nije tražio nikakvu identifikaciju.

SPREČAVANJE PREVARE

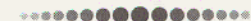
Sigurnosna šifra, kad se ispravno koristi, dodaje vredan sloj zaštite. Nepravilno korišćenje lozinke može biti gore od nepostojanja lozinke, jer stvara iluziju bezbednosti tamo gde je zapravo nema. Šta vrede lozinke ako ih vaši zaposleni ne čuvaju u tajnosti?

Svaka kompanija kojoj su neophodne verbalne sigurnosne lozinke treba jasno da stavi do znanja zaposlenima kada i kako se one koriste. Da je imao odgovarajuću obuku, službenik iz prve priče u ovom poglavlju ne bi morao da se oslanja na svoj instinkt, na koji se lako utiče, kad je od njega zatraženo da neznancu kaže bezbednosni kôd. Osetio je da u datim okolnostima ne bi trebalo da ga pitaju za taj podatak, ali s obzirom na to da nisu postojala jasna bezbednosna pravila – niti zdrav razum – lako je popustio.

U bezbednosnim procedurama takođe bi trebalo odrediti korake po kojima se valja vladati ako se zaposlenom uputi neodgovarajući zahtev za bezbednosni kôd. Svi zaposleni moraju biti obučeni da odmah prijave svaki sumnjiv zahtev za identifikaciju, kao što su dnevni kôd ili lozinka. Trebalo bi takođe da podnesu prijavu kada pri pokušaju provere identiteta podnosilac zahteva pruži neodgovarajuće podatke.

U najmanju ruku, zaposleni bi trebalo da zapiše ime sagovornika, njegov telefonski broj i kancelariju ili odeljenje, a potom da prekine vezu. Pre nego što pozove, trebalo bi da proveri da li zaista postoji zaposleni pod tim imenom, da li se telefonski broj slaže s brojem u kompanijskom telefonskom imeniku, kako na mreži, tako i u štampanoj verziji. Uglavnom će ta jednostavna metoda biti dovoljna da se potvrdi identitet sagovornika.

Malo je teže utvrditi identitet kad firma ima štampani telefonski imenik, a nema verziju na mreži. Ljudi se zapošljavaju i odlaze, menjaju odeljenja, pozicije na poslu i telefonske brojeve. Štampana verzija imenika je zastarela već prvog dana kad se on objavi, čak i pre nego što se distribuira. Čak se ni na mrežne imenike ne možete uvek osloniti, jer prevaranti znaju kako da ih izmene. Ako zaposleni ne može da potvrdi broj telefona iz nezavisnog izvora, treba ga uputiti da to učini na drugi način, na primer stupanjem u kontakt s pretpostavljenim sumnjive osobe.



Potom je neko u Telekomunikacijama učinio isto to, prihvatajući Erikovu tvrdnju da radi za firmu koja proizvodi opremu, i dajući neznancu broj za povezivanje na telefonsku centralu koja opslužuje AMS.

Erik je uspeo da se poveže na centralu u velikoj meri zbog slabog obezbeđenja koje je postavio proizvođač, tako što je zadao isto korisničko ime za sve centrale. Usled te nepažnje, budući da je bio iskusen obmanjivač, veoma lako je pogodio lozinku znajući, još jednom, da tehničari, baš kao i gotovo svako drugi, biraju lozinke koje će sigurno zapamtiti.

Kad je pristupio centrali, podesio je da se pozivi prosleđuju s jedne telefonske linije AMS-a određene za kriminalističku službu, do njegovog mobilnog telefona.

A potom, u poslednjem i najbezočnijem delu, varao je jednog policajca za drugim i navodio ih da mu otkriju i svoje šifre i sopstvene podatke za identifikaciju. Na osnovu skupljenih podataka, Erik se uspešno lažno predstavljao.

Iako je za ovu obmanu svakako bilo potrebno tehničko znanje, ne bi uspela bez pomoći niza ljudi koji nisu uopšte znali da razgovaraju s prevarantom.

U ovoj priči još jednom je prikazan fenomen da ljudi ne pitaju: „Zašto baš ja?“ Zašto bi službenik u Teletajpu dao informacije nekom nepoznatom zameniku šerifa – ili, u ovom slučaju, neznancu *koji se izdaje* za šerifovog zamenika – umesto da mu savetuje da podatke potraži od nekog kolege ili pretpostavljenog? Ponovo, jedini odgovor koji ja znam glasi: ljudi retko sebi postavljaju to pitanje. Možda se ne sete da pitaju? Ili ne žele da zvuče nadobudno i neljubazno? Možda. Sva dalja objašnjenja bila bi čista pretpostavka. Ali obmanjivačima nije bitno zašto žrtve tako reaguju. Njima je važno samo to da im taj fenomen olakšava da se domognu informacija do kojih bi inače teško došli.

mitnikova poruka

Ako u okviru firme imate lokalnu telefonsku centralu, šta bi osoba zadužena za nju učinila kad bi primila poziv od proizvođača koji traži broj za povezivanje? Uzgred budi rečeno, da li je ta osoba ikada promenila podrazumevanu lozinku? Da li je lozinka neka reč koja se nalazi u svakom rečniku i lako se može pogoditi?

deo

3

Uzbuna zbog uljeza

poglavlje

10

Upad u prostorije

Zašto nepoznata osoba lako preuzima identitet zaposlenog u kompaniji i predstavlja se toliko ubedljivo da obmane čak i ljude koji brinu o bezbednosti? Zašto je toliko lako prevariti osobe koje možda odlično poznaju bezbednosne procedure, sumnjičave su prema ljudima koje ne poznaju lično, i štite interese svoje kompanije?

Razmišljajte o tim pitanjima dok čitate priče u ovom poglavlju.

POSTIĐENI ČUVAR

Vreme: četvrtak, 17. oktobar, 2:16 ujutru

Mesto: Skajvočer, proizvodno postrojenje u predgrađu Tusona u Arizoni.

Čuvareva priča

Dok je osluškivao kuckanje svojih potpetica o pod u hodnicima gotovo napuštenog postrojenja, Liroj Grin se osećao mnogo bolje nego ispred monitora u kancelariji obezbeđenja za dugih sati u noćnoj smeni. Tamo mu nije bilo dozvoljeno da radi išta drugo osim da zuri u ekrane; nije smeo čak ni da čita časopis, niti Bibliju. Morao je samo da sedi i posmatra slike na ekranu na kojima se nikada ništa nije pomeralo.

Šetajući hodnicima bar bi protegao noge, a kad bi se setio da radi i rukama i ramenima, malo bi i provežbao, iako se to nije stvarno moglo

nazvati vežbom za nekoga ko je igrao u srednjoškolskom ragbi timu i osvojio titulu gradskog šampiona. „Pa ipak“, pomislio je, posao je posao.

Skrenuo je na jugozapad i krenuo galerijom iznad proizvodne hale dugačke pola milje. Pogledao je dole i ugledao dvoje ljudi pored niza delično završenih helikoptera. Ta dvojica su zastala i činilo se da jedan drugom nešto pokazuju. Bio je to neobičan prizor u ovo doba noći. „Bolje da proverim“, pomislio je.

Liroj se uputio ka stepeništu kojim će se spustiti u halu iza te dvojice, a oni nisu primetili da im se približava sve dok nije istupio pored njih. „Dobro jutro. Mogu li da vidim vaše propusnice, molim vas?“ upita. Liroj se uvek trudio da mu glas zvuči opušteno u ovakvim trenucima; znao je da verovatno izgleda preteće zbog svoje građe.

„Zdravo, Liroj“, reče jedan od njih, pročitavši mu ime s oznake. „Ja sam Tom Stilton, iz marketinškog odeljenja u centrali u Finiksu. Došao sam ovamo na sastanak, pa sam hteo prijatelju da pokažem kako se prave najbolji svetski helikopteri.“

„Da, gospodine. Molim vas, pokažite propusnicu.“, odvrati Liroj. Nije mogao a da ne primeti kako mladoliko izgledaju. Činilo se da je momak iz marketinškog odeljenja tek izašao iz srednje škole, dok je drugi imao dugu kosu do ramena i izgledao je kao da ima petnaest godina.

Ošišani dečko je posegao u džep a potom počeo da se hvata za ostale džepove. Liroj je odjednom imao loš predosećaj. „Do đavola“, reče momak. „Mora da sam je ostavio u kolima. Doneću je – trebaće mi samo deset minuta da odem do parkinga i vratim se.“

Liroj je već tad izvadio notes. „Kako ste rekli da se zovete, gospodine?“ upitao je, i pažljivo zapisao odgovor. Potom ih je zamolio da pođu s njim do kancelarije obezbeđenja. U liftu do trećeg sprata Tom je čavrljao o tome kako za firmu radi tek šest meseci, te da se nada da zbog ovoga neće upasti u nevolje.

U prostoriji za nadgledanje, Liroju su se u ispitivanju dvojice momaka pridružila druga dva čuvara iz noćne smene. Stilton im je dao svoj broj telefona, rekao da mu je šef Džudi Andervud, i dao im njen telefonski broj, a podaci na računaru su se poklapali s tim. Liroj je odveo drugu dvojicu iz obezbeđenja na stranu, pa su popričali o tome šta da rade. Niko nije želeo nesporazum; sva trojica su se složila da bi bilo najbolje da pozovu Tomovu pretpostavljenu, bez obzira na to što će je probuditi usred noći.

Liroj je lično pozvao gospođu Andervud, objasnio joj ko je, i upitao da li za nju radi izvesni Tom Stilton. Zvučala je kao da se još uvek nije razbula. „Da“, odgovorila je.

„Pa, našli smo ga u proizvodnoj hali u 2:30 ujutru bez identifikacione propusnice.“

Gospođa Andervud reče: „Dajte da ja razgovaram s njim.“

Stilton se javio i rekao: „Džudi, zaista mi je žao što su vas ovi momci probudili usred noći. Nadam se da mi nećete to uzeti za zlo.“

Slušao je njen odgovor, a potom rekao: „U pitanju je samo to da sam svakako morao doći ovamo ujutro, na onaj sastanak u vezi s novom objavom za štampu. Uzgred, da li ste dobili elektronsku poruku o poslu s Tomsonom? Moramo se naći s Džimom u ponedjeljak ujutro da nam to ne bi promaklo. Još uvek važi dogovor da zajedno ručamo u utorak, zar ne?“

Slušao je šta govori još neko vreme, a onda se oprostio i prekinuo vezu.

To je iznenadilo Liroja; mislio je da će mu dati slušalicu kako bi gospođa mogla da mu kaže da je sve u redu. Razmišljao je da li bi možda trebalo ponovo da je nazove i pita, ali je odustao. Već ju je jednom uznemirio usred noći; kad bi je nazvao još jednom, možda bi se naljutila i žalila se njegovom šefu. „Zašto da tražim nevolje?“ pomislio je.

„Mogu li da pokažem prijatelju ostatak proizvodnog procesa?“ upita Stilton Liroja. „Hoćete li da podete s nama, da nas držite na oku?“

„Izvolite“, odvrati Liroj. „Razgledajte. Samo sledeći put nemojte zaboraviti propusnicu. I obavestite obezbeđenje ako treba da uđete u postrojenje nakon radnog vremena – to je pravilo.“

„Zapamtiću to, Liroj“, kaza Stilton, a potom su otišli.

Nije prošlo ni deset minuta kad je telefon zazvonio u kancelariji obezbeđenja. Na vezi je bila gospođa Andervud. „Ko je to bio?!“ htela je da zna. Kazala je da je pokušavala da mu postavi pitanja, ali je on samo pričao o tome kako će ručati s njom, a ona ga uopšte ne poznaje.

Čuvari su pozvali ulazni hol i čuvara na kapiji parkinga. Obojica su saopštila da su dva mladića otišla pre nekoliko minuta.

Prepričavajući ovaj događaj, Liroj bi uvek ovako završio priču govoreći: „Gospode, kako me je šef izribao. Sreća moja što sam zadržao posao.“

Priča Džoa Harpera

Šedamnaestogodišnji Džo Harper je krišom ulazio u zgrade već više od godinu dana, nekad danju, a nekad noću, samo da bi video šta mu sve

može poći za rukom. S obzirom na to da su njegovi roditelji, muzičar i konobarica, radili noću, suviše je vremena provodio sam. Priča o tom istom incidentu iz njegovog ugla objašnjava nam kako se sve dogodilo.



Imam jednog prijatelja, Kenija, koji želi da postane pilot helikoptera. Pitao me je mogu li ga uvesti u fabriku Skajvočer da vidi proizvodnu halu u kojoj ih prave. Zna da sam i ranije ulazio na zabranjena mesta. Adrenalin vam pojuri venama kad pokušavate da se uvučete na mesta na kojima ne bi trebalo da budete.

Ne možete se tek tako ušetati u fabriku ili kancelarije. Morate da razmislite, dobro sve da isplanirate, i izvidite metu. Na kompanijskoj Web strani treba potražiti imena zaposlenih i njihove pozicije, organizacionu strukturu, kao i telefonske brojeve. Valja pročitati isečke iz novina i članke u časopisima. Iz predostrožnosti, uvek sam sprovodio detaljno istraživanje, tako da sam mogao da razgovaram sa svakim ko bi me eventualno ispitivao kao da sam jedan od zaposlenih.

Dakle, gde početi? Prvo sam na Internetu pogledao gde se nalaze kancelarije, i video da je centrala u Finiksu. Savršeno. Nazvao sam ih i tražio marketinško odeljenje – svaka firma ga ima. Javila se neka gospođa, a ja sam rekao da zovem iz firme Blu Grafiks i želim da im ponudim naše usluge. Upitao sam je s kim o tome mogu da razgovaram. Rekla je da je za to zadužen Tom Stilton. Zatražio sam njegov telefonski broj, a ona je odvrtila da ne saopštavaju takve informacije, ali će me spojiti s njim. Javila mi se snimljena poruka: „Ovde Tom Stilton, lokal 3147. Molim vas, ostavite poruku.“ Naravno da ne daju brojeve lokala, ali je ovaj momak ostavio svoj u glasovnoj poruci. To je bilo sjajno. Sad sam imao ime i broj lokala.

Pozvao sam ponovo istu kancelariju. „Zdravo, tražim Toma Stiltona, a on nije u kancelariji. Hteo bih nešto da pitam njegovog pretpostavljenog.“ Ni pretpostavljeni nije bio tu, ali sam do kraja razgovora saznao njeno ime. A i ona je zgodno ostavila broj lokala u svojoj glasovnoj poruci.

Verovatno bih mogao da nas provučem pored čuvara u holu bez problema ali, vozeći se pored fabrike, primetio sam ogradu oko parkinga. Ograda znači da postoji čuvar koji vas proverava kad pokušate da se uvezete. Uveče možda i zapisuju broj tablice, pa moram da kupim neke stare tablice na buvljoj pijaci.

Ipak, prvo moram saznati broj telefona u stražarskoj kućici. Malo sam sačekao, tako da me ista službenica na centrali ne bi prepoznala, ako bi mi se ona javila. Nakon izvesnog vremena sam pozvao i kazao: „Stigla nam je žalba da se telefonska veza sa stražarskom kućicom na Ridž Roudu povremeno prekida – da li još uvek imaju problema s njom?“ Rekla je da ne zna, ali da će me spojiti s njima.

Čuvar se javio: „Kapija na Ridž Roudu, ovde Rajan.“ Rekoh: „Zdravo Rajane, ovde Ben. Jeste li imali problema s telefonima?“ On je samo nisko plaćeni čuvar, ali pretpostavljam da je donekle obučen jer je odmah odvratio: „Koji Ben, kako se prezivate?“ Ja sam nastavio, kao da ga nisam čuo. „Neko je prijavio problem.“

Čuo sam kako udaljava slušalicu i uzvikuje: „Hej, Brus, Rodžere, jeste li imali problema s ovim telefonom?“ Ponovo se javio i odgovorio: „Ne, mi ne znamo ni za kakav problem.“

„Koliko telefonskih linija imate tu?“

Zaboravio je da me pita za ime. „Dve“, odvrati.

„Koju sad koristite?“

„3140.“

Moj si! „I obe su ispravne?“

„Tako se čini.“

„U redu“, rekoh. „Čujte, Rajane, ako imate ikakvih problema s telefonom, slobodno nas pozovite u svako doba. Tu smo da vam pomognemo.“

Moj prijatelj i ja odlučili smo da posetimo postrojenje sledeće noći. Kasno tog poslepodneva nazvao sam stražarsku kućicu, koristeći ime onog momka iz marketinškog odeljenja. Rekoh: „Zdravo, ovde Tom Stilton iz marketinškog odeljenja. Imamo kratak rok za projekat, pa će neki momci doći da mi pomognu. Verovatno neće stići do jedan ili dva ujutru. Hoćete li još uvek biti na dužnosti tada?“

Odgovori da odlazi u ponoć i zvučao je radosno.

Odvratih: „Dobro, samo ostavite poruku sledećoj smeni, u redu? Kad se dva momka pojave i kažu da su došli kod Toma Stiltona, samo im pokažite da uđu, važi?“

Rekao je da nema problema. Zapisao je moje ime, odeljenje i lokal, i rekao da će se postarati za to.

Dovezli smo se do kapije malo nakon dva ujutru, ja sam se predstavio kao Tom Stilton, a pospani čuvar nam je samo pokazao da prođemo kroz kapiju i gde da parkiram.

Kad smo ušli u zgradu, u holu se nalazila još jedna stražarska stanica, s uobičajenom knjigom za upisivanje nakon radnog vremena. Rekao sam čuvaru da moram da završim jedan izveštaj do jutra, a da moj prijatelj želi da vidi postrojenje. „On obožava helikoptere“, rekoh. „Želi da postane pilot.“ Zatražio mi je propusnicu. Posegao sam u džep, potom se potapšao po ostalima i kazao da sam je sigurno ostavio u kolima, te da ću otići po nju. Rekoh: „Trebaće mi oko deset minuta.“ On na to odvrati: „Nema veze, u redu je. Samo se potpišite.“

Razgledanje proizvodne hale bilo je pravo ushićenje dok nas nije zaustavio taj Liroj, kao od brega odvaljen.

U kancelariji obezbeđenja pomislio sam da bi neko kome tu nije bilo mesto izgledao nervozno i uplašeno. Kad zagusti, ja se ponašam kao da sam ljut. Kao da sam zaista onaj za koga se izdajem i da me žesti što mi ne veruju.

Kad su počeli da razgovaraju o tome kako bi možda trebalo da pozovu gospođu za koju sam tvrdio da mi je pretpostavljeni, i kad su otišli da pronadu njen telefonski broj na računaru, stajao sam tamo misleći: „Sad je pravo vreme da izjurimo odavde.“ Ali bila je tu i kapija na parking; čak i kad bismo pobjegli iz zgrade, zatvorili bi kapiju, pa nikako ne bismo uspjeli da izađemo.

Kad je Liroj nazvao tu gospođu, Stiltonovog pretpostavljenog, a potom mi dao slušalicu, ona je počela da viče na mene: „Ko je to? Ko ste vi?“ A ja sam samo pričao i pričao kao da prijatno ćaskamo, a onda sam spustio slušalicu.

Koliko je vremena potrebno da se pronade neko ko vam može dati broj firme usred noći? Pretpostavio sam da imamo manje od petnaest minuta da se izgubimo odatle pre nego što ta gospođa pozove kancelariju obezbeđenja i kaže im šta se dogodilo.

Izašli smo odatle što smo brže mogli, tako da ne izgleda kao da žurimo. Kako mi je samo bilo drago kad nam je momak na kapiji rukom pokazao da prodemo.

Analiza prevare

Nema nikakvog značaja to što su u pravom incidentu, na kojem je ova priča zasnovana, uljezi zaista bili pubertetlije. Upad je bio šala, tek da vide da li će uspeti da izvedu tako nešto. Ali ako su dvojica pubertetlija to tako lako izveli, bilo bi čak i jednostavnije odraslim kradljivcima, industrijskim špijunima ili teroristima.

Kako su tri iskusna čuvara dozvolila dvojici uljeza da izađu odatle? I to ne bilo kakvim uljezima, nego toliko mladim osobama da bi svako razuman bio veoma sumnjičav?

Liroj je isprva i *bio* sumnjičav u odgovarajućoj meri. Ispravno je postupio kad ih je odveo u kancelariju obezbeđenja, i kad je ispitao momka koji se predstavljao kao Tom Stilton, i kad je proverio imena i telefonske brojeve koje mu je taj momak dao. Svakako je bio u pravu kad je pozvao pretpostavljenog.

Na kraju ga je obmanulo mladićevo samopouzdanje i ogorčenost. Takvo ponašanje ne bi očekivao od kradljivca ili uljeza. Samo bi se pravi zaposleni tako ponašao – mislio je. Liroj je trebalo da proveri identifikaciju, a ne da se oslanja na opažanja.

Zašto nije nešto posumnjao kad je mladić spustio slušalicu? Zašto nije insistirao da Džudi Andervud potvrdi „Tomov“ identitet i uveri ga da momak ima razloga što se nalazi u postrojenju tako kasno noću?

Liroj je poverovao u toliko bestidnu obmanu, da je trebalo da bude očigledna. Ali razmislite o tome iz njegovog ugla: imao je samo srednjoškolsku diplomu, bio je zabrinut za svoj posao, i nije bio siguran da li bi mogao upasti u nevolje što uznemirava rukovodioca kompanije po drugi put usred noći. Da ste vi bili na njegovom mestu, da li biste ponovo pozvali?

Naravno, drugi poziv nije bio jedini mogući izlaz. Šta je još čuvar mogao da učini?

Čak i pre nego što je pozvao, mogao je da zamoli obojicu da pokažu neakvu legitimaciju sa slikom; dovezli su se do fabrike, pa valjda bar jedan od njih ima vozačku dozvolu. Činjenica da su se lažno predstavili odmah bi bila očigledna (profesionalac bi se obezbedio lažnom vozačkom dozvolom, ali ovi mladići nisu preduzeli te mere opreza). U svakom slučaju, trebalo je da im Liroj pogleda legitimacije i zapiše te podatke. Ako bi obojica tvrdili da ih nemaju, trebalo je onda da ih otprati do kola po kompanijsku propusnicu koju je „Tom Stilton“ navodno ostavio tamo.

Nakon telefonskog poziva, trebalo je da jedan od čuvara ostane uz dvojicu momaka sve dok ne napuste zgradu a potom da ih isprati do kola i zapiše broj tablice. Da je bio dovoljno pažljiv, primetio bi da tablice (one koje je napadač kupio na buvljoj pijaci) nemaju odgovarajuću registracionu nalapnicu – a to bi bilo sasvim dovoljno da se ta dvojica zadrže radi daljeg ispitivanja.

mitnikova poruka

Manipulatori su obično šarmantne ličnosti. Uglavnom su snalažljivi i elokventni. Vešto odvrćaju misli da bi ljudi sarađivali s njima. Ako mislite da neko nije podložan takvoj manipulaciji, onda potcenjujete vještinu i pobjednički instinkt iskusnih obmanjivača.

S druge strane, uspješan manipulator nikada ne potcenjuje svog protivnika.

KOPANJE PO SMEĆU

Ovaj izraz se odnosi na traženje vrednih podataka po žrtvinom smeću. Tako možete saznati zapanjujuću količinu informacija.

Ljudi ne razmišljaju mnogo o tome šta bacaju kod kuće: telefonske račune, izvode s računa kreditnih kartica, flašice od lekova, izvode iz banke, poslovne materijale, i još mnogo toga.

Zaposlenima se mora staviti do znanja da prevaranti zaista pregledaju smeće kako bi došli do korisnih informacija.

Tokom srednje škole, ja sam obično kopao po smeću iza kancelarija lokalne telefonske kompanije – najčešće sâm, ali povremeno i sa prijateljima koje je takođe zanimalo da saznaju nešto više o toj organizaciji. Kad se već izveštite u tome, naučite nekoliko trikova; na primer, kako da posebno obratite pažnju na vreće iz toaleta i izbegnete ih, i obavezno nosite rukavice.

Kopanje po smeću nije uživanje, ali je ono što za uzvrat dobijete izvanredno – interne telefonske imenike kompanije, uputstva za računare, spisake zaposlenih, bačena uputstva za programiranje centrala, i još mnogo toga – i sve je to vaše.

Obilazio bih kante one noći kad su iz štampe izlazila nova uputstva, jer bi se u kontejnerima sa smećem našlo puno starih, bačenih bez razmišljanja. A išao bih tamo i u drugim prilikama, nasumično, tražeći memorandume, pisma, izveštaje, i tako dalje, u kojima bi se mogle naći neke zanimljive i veoma vredne informacije.

Kad bih stigao, našao bih kartonske kutije, izvukao ih i stavio sa strane. Ako bi me iko pitao šta radim, što se povremeno dešavalo, rekao bih da mi se prijatelj seli, pa tražim kutije da mu pomognem da se spakuje. Čuvar nikada nije primetio gomilu dokumenata koje sam stavljao u kutije i nosio

kući. U nekim slučajevima bi me oterao, pa bih se premestio do kancelarija neke druge telefonske kompanije.

terminologija

KOPANJE PO SMEĆU (engl. *dumpster diving*) Preturanje po smeću iz preduzeća (često napolju, po javnom kontejneru) da bi se pronašle bačene informacije koje su značajne ili se mogu koristiti u obmanama, a takvi su interni telefonski brojevi ili podaci o radnicima.

Ne znam kakva je situacija danas, ali u to vreme bilo je lako prepoznati vreće u kojima se možda nalazi nešto zanimljivo. Smeće počišćeno s poda i otpaci iz restorana nalazili su se u nezatvorenim velikim vrećama, dok su sve kancelarijske kante za otpatke bile obložene belim vrećama za smeće za jednokratnu upotrebu. Njih bi čistači vadili jednu po jednu i vezivali ih.

Jednom prilikom, dok sam pretraživao smeće s prijateljima, naišli smo na neke papire pocepane rukom. Ne samo da su bili pocepani – neko se potrudio da ih pokida na komadiće. Svi su bili zgodno bačeni u jednu vreću. Odneli smo vreću u obližnju prodavnicu krofni, prosuli deliće na sto, i počeli da ih slažemo jedan po jedan.

Svi smo voleli da sklapamo slagalice, pa nam je ovo bio poticajan izazov, poput rada na ogromnoj slagalici... za koju se ispostavilo da je više od obične dečje igre. Kad smo završili, sastavili smo čitav spisak korisničkih naloga i lozinki za jedan od najbitnijih računarskih sistema kompanije.

Da li je naše kopanje po smeću bilo vredno rizika i truda? Možete se u to kladiti. Čak i više nego što mislite, jer nije bilo nikakvog rizika. I u to vreme, kao i danas, istina je sledeća: sve dok se ne nalazite na nečijem privatnom posedu, pretraživanje tuđeg smeća je 100% legalno.

Naravno, u kante za smeće ne zabijaju glavu samo hakeri i telefonski prevaranti. Policajci širom zemlje redovno pretražuju smeće, pa je niz ljudi, počev od šefova mafije do sitnih prevaranata, osuđen delimično na osnovu dokaza sakupljenih iz njihovog smeća. Obaveštajne službe, uključujući i američku, godinama su pribegavale toj metodi.

Možda je ta metoda suviše prizemna za Džemsa Bonda, jer bi bioskopska publika mnogo radije gledala kako nadmudruje negativca i odvodi lepoticu u krevet, nego kako pretura po kontejneru. Pravi špijuni su manje

gadljivi ako pretpostavljaju da se nešto vredno nalazi u vreći zajedno s korama banane, talogom od kafe, novinama i spiskovima za kupovinu – naročito ako takvo sakupljanje informacija nije rizično.

Gotovina u zamenu za smeće

I kompanije kopaju po smeću. Novine su juna 2000. objavile da je firma Oracle (čiji je generalni direktor, Leri Elison, verovatno najotvoreniji protivnik Microsofta u Americi) unajmila istražiteljsku firmu koja je uhvaćena na delu. Čini se da su istažitelji želeli da se domognu smeća organizacije ACT, pripadnice lobija koji podržava Microsoft, ali nisu hteli da rizikuju da ih uhvate. Prema izveštajima iz štampe, istražiteljska firma je poslala jednu ženu, koja je ponudila domarima 60 dolara za smeće ACT-a. Odbili su je. Sledeće večeri se vratila, podigavši ponudu na 500 dolara za čistače i 200 za njihovog nadzornika.

Odbili su je, a potom i prijavili.

Vodeći novinar na Webu, Deklan Mekulah, nazvao je u biltenu *Wired News* svoj članak o tom događaju: „Oracle je špijunirao Microsoft“. Časopis *Time* je, okomivši se na Elisona, nazvao svoj članak „Leri viri kroz ključaonicu“.

Analiza prevare

Na osnovu mog ličnog iskustva i iskustva firme Oracle, možda se pitate zašto bi iko rizikovao krađu nečije smeće.

Odgovor je da rizika nema, a da korist može biti velika. Dobro, možda pokušaj podmićivanja domara povećava šanse da osetite posledice, ali ako ste voljni da se malo isprljate, mito vam ne treba.

Za obmanjivače, kopanje po smeću ima svojih prednosti. Mogu sakupiti dovoljno podataka za napad na ciljnu kompaniju, uključujući memorandum, dnevni red sa sastanka, pisma i slične stvari koje otkrivaju imena, ogranke, pozicije, telefonske brojeve i zadatke na projektima. U smeću se mogu naći organizaciona struktura firme, podaci o strukturi poslovanja, zakazana putovanja i tako dalje. Sve te pojedinosti možda deluju beznačajno zaposlenima, ali napadaču mogu biti izuzetno važne.

Mark Džozef Edvards u svojoj knjizi *Bezbednost na Internetu pri radu s Windowsom NT* govori o „čitavim izveštajima bačenim zbog slovnihi grešaka, lozinkama zapisanim na papirićima, porukama s telefonskim brojevima

za odsutne kolege, fasciklama u kojima se dokumenti još uvek nalaze, disketama i trakama koje nisu izbrisane, niti uništene – što bi sve moglo koristiti onom ko namerava da se uvuče u firmu.“

Pisac dalje pita: „Ko su vaši čistači? Odlučili ste da se čistačima neće odobriti ulaz u prostoriju s računarima, ali ne zaboravite ostale kante za smeće. Ako američke obaveštajne službe smatraju da je neophodno proveriti prošlost ljudi koji imaju pristup njihovim kantama za smeće i aparatima za uništavanje poverljivih dokumenata, verovatno bi trebalo i vi isto da učinite.“

mitnikova poruka

Vaše smeće je možda blago za vašeg neprijatelja. Ne obraćamo dovoljno pažnje na stvari koje bacamo u privatnom životu, pa zašto bismo smatrali da ljudi imaju drugačiji stav na radnom mestu? Sve se svodi na obučavanje zaposlenih o opasnostima (kad beskrupulozne osobe kopaju po smeću tražeći vredne informacije) i slabim tačkama (kad se poverljive informacije ne unište ili ne izbrišu na odgovarajući način).

PONIŽENI ŠEF

Nikom se nije činilo neobičnim kad je Harlan Fortis, kao i obično, došao na posao u ponedeljak ujutru u Okružnu saobraćajnu službu i rekao da je iz kuće izašao u žurbi, pa je zaboravio propusnicu. Čuvarka je videla Harlana kako dolazi i odlazi svakog radnog dana u prethodne dve godine, koliko je tamo radila. Zamolila ga je da se potpiše da bi dobio privremenu propusnicu, dala mu je propusnicu, i on je otišao svojim putem.

Tek dva dana kasnije sve je izbilo na videlo. Priča se širila čitavom službom kao požar. Pola onih koji su je čuli govorili su da to nikako nije moguće. Ostali, činilo se, nisu znali da li da se naglas smeju ili da sažaljevaju jadnika.

Na kraju krajeva, Džordž Adamson je bio dobra i saosećajna osoba, najbolji šef odseka kojeg su ikad imali. Nije zaslužio da mu se to dogodi. Naravno, uz pretpostavku da je priča istinita.

Nevolje su počele kad je Džordž pozvao Harlana u svoju kancelariju jednog petka popodne i rekao mu, što je pažljivije mogao, da će od ponedeljka Harlan imati nov posao. Radiće u sanitetskoj službi. Harlan to nije doživeo kao otkaz. Bilo je još gore – ponižavajuće. Nije hteo s tim tek tako da se pomiri.

Iste večeri sedeo je na svojoj verandi i posmatrao automobile koji prolaze. Najzad je spazio Dejvida momka iz susedstva, kojeg svi zovu „Majstor za ratne igre“. Dejvid je prošao na mopedu na povratku kući iz srednje škole. Zaustavio ga je, dao mu igricu Code Red Mountain Dew, koju je kupio posebno za tu priliku, i ponudio mu posao: daće mu najnoviji uređaj za video igre i šest igara u zamenu za malu pomoć s računarima i obećanje da o tome nikome neće reći ni reći.

Nakon što mu je Harlan objasnio projekat, ne odajući mu kompromitujuće pojedinosti, Dejvid je pristao. Rekao je Harlanu šta treba da učini. Treba da kupi modem, ode u kancelariju, pronađe računar blizu slobodnog priključka za telefon, i priključi ga. Neka ga ostavi pod stolom, gde ga verovatno niko neće primetiti. Došao je do rizičnog dela. Trebalo je da Harlan sedne za računar, instalira softverski paket za daljinski pristup, i pokrene ga. Osoba koja radi u toj kancelariji mogla je da naiđe u svakom trenutku, ili bi neko mogao proći hodnikom i videti ga u tuđoj kancelariji. Bio je toliko napet da je jedva pročitao uputstva koja mu je momak napisao. Ali uspeo je to da uradi, i neopaženo se izvukao iz zgrade.

Podmetanje bombe

Dejvid je svratio posle večere. Njih dvojica su seli za Harlanov računar, i za nekoliko minuta dečko se priključio na modem, dobio pristup i dospao do računara Džordža Adamsona. To uopšte nije bilo teško, jer Džordž nikada nije imao vremena za predostrožnosti kao što je izmena lozinki, i često bi zamolio nekog kolegu da učitava elektronsku poštu ili neku datoteku umesto njega. Ubrzo su, svi iz te službe znali njegovu lozinku.

Nakon kratkog pretraživanja, pronašli su prezentaciju o budžetu, koju je mladić preneo na Harlanov računar. Harlan mu je potom rekao da ode kući, i da se vrati za nekoliko sati.

Kad se Dejvid vratio, Harlan ga je zamolio da se ponovo uključi u računarski sistem saobraćajne službe i da vrati istu datoteku tamo gde ju je i našao, prebrisavši prethodnu verziju. Pokazao je Dejvidu uređaj za video igre, i rekao da će ga dobiti sutradan, ako sve pođe po planu.

Iznenadenje za Džordža

Ne biste pomislili da bi nešto što zvuči tako dosadno, kao što je izjava o budžetu, ikoga zainteresovalo, ali je sala za sastanke u Okružnom veću bila

puna novinara, predstavnika raznih grupa, a bile su tu čak i dve televizijske ekipe.

Džordž je uvek imao osećaj da od tih sastanaka puno toga zavisi. Okružno veće je držalo novac, pa će budžet za saobraćaj biti umanjen, ukoliko on Džordž ne bude održao ubedljivu prezentaciju. A onda će svi početi da se žale na rupe na putevima, semafore koji ne rade i opasne raskrsnice, a optužice njega, pa će mu život čitave sledeće godine biti zagorčan. Kada su ga te večeri najavili, ustao je siguran u sebe. Radio je šest nedelja na ovoj prezentaciji i slajdovima u PowerPointu, i sve je isprobao pred svojom ženom, glavnim saradnicima i nekim prijateljima. Svi su se složili da mu je to najbolja prezentacija koju je ikada napravio.

Prve tri slike u PowerPointu bile su dobro prikazane. Za promenu, svi članovi veća su obraćali pažnju. Efektivno je isticao najvažnije delove.

A onda je odjednom sve pošlo nizbrdo. Trebalo je da četvrta slika bude divna fotografija zalaska sunca iznad novog dela autoputa otvorenog prošle godine. Umesto toga nalazila se neka druga slika, nešto veoma nepristojno. Bila je to fotografija iz časopisa poput *Penthouse* ili *Hustler*. Mogao je da čuje kako se publika iščuđava, dok je užurbano pritiskao dugme na svom prenosivom računaru kako bi prešao na sledeću fotografiju.

Ta je bila još gora. Na njoj ništa nije bilo prepušteno mašti.

Još uvek je pokušavao da pritiskom na dugme pređe na sledeću sliku, kad je neko iz publike izvukao strujni priključak za projektor iz zida. Glasno udarajući čekićem, predsedavajući je viknuo da bi nadglasao buku. Sastanak je završen.

Analiza prevare

Iskoristivši znanje mladog hakera, nezadovoljni radnik je uspeo da pristupi računaru šefa svog odeljenja, preuzme važnu prezentaciju u PowerPointu, i zameni neke slajdove slikama koje će ga sigurno osramotiti. Potom je vratio prezentaciju na njegov računar.

Pošto je modem bio povezan na telefonski priključak i jedan od kancelarijskih računara, mladi haker je uspeo da pristupi tom računaru daljinski. Momak je unapred podesio softver za daljinski pristup tako da ima pun pristup svakoj datoteci u čitavom sistemu. S obzirom na to da je računar bio povezan u lokalnu mrežu organizacije i da je napadač već znao šefovo korisničko ime i lozinku, lako je mogao da pristupi njegovim dokumentima.

Za čitav poduhvat bilo je potrebno samo nekoliko sati, uključujući i vreme za skeniranje slika iz časopisa. Koliko je ugled jednog primernog građanina narušen usled toga, ne može se ni zamisliti.

mitnikova poruka

Ogromna većina zaposlenih koji budu prebačeni na drugi posao, otpušteni, ili postanu tehnološki višak, nikad ne predstavljaju problem. Pa ipak je dovoljan samo jedan takav, pa da kompanija isuviše kasno shvati koje su korake mogli preduzeti da bi sprečili katastrofu.

Iskustvo i statistike su jasno pokazali da najveću pretnju preduzećima predstavljaju *zaposleni*. Oni dobro znaju gde se nalaze značajne informacije, i gde da udare da bi izazvali najveću štetu.

KARIJERISTA

Jednog prijatnog jesenjeg jutra, Piter Milton je ušao u hol regionalne kancelarije firme Honorable Auto Parts u Denveru, koja se bavi veleprodajom automobilskih rezervnih delova širom Amerike. Čekao je na prijemnom odeljenju dok je jedna mlada dama upisivala posetioca, objašnjavala sgovorniku preko telefona kako da dođe kolima do njih, i komunicirala s čovekom iz UPS-a, sve to manje-više istovremeno.

„Pa gde ste naučili da radite toliko stvari odjednom?“ upita Pit kad je imala malo vremena da mu se posveti. Nasmešila se, očigledno polaskana što je to primetio. Rekao joj je da je iz marketinškog odeljenja ogranka u Dalasu, te da će imati sastanak s komercijalistom Majkom Talbotom iz Atlante. „Treba zajedno da posetimo jednog klijenta danas poslepodne“, objasnio joj je. „Samo ću ga sačekati ovde u hodniku.“

„Marketing.“ Izgovorila je to gotovo čežnjivo, a Pit joj se nasmešio, čekajući da čuje šta još želi da kaže. „Da sam mogla da idem na koledž, to bih izabrala“, rekla je. „Jako bih volela da radim u marketingu.“

Ponovo se nasmešio. „Kajla“, reče on, čitajući njeno ime s oznake na stolu, „u ogranku u Dalasu imamo jednu damu koja je bila sekretarica. Uspela je da se prebaci u marketing. To je bilo pre tri godine, a sad je pomoćnik direktora marketinga, i zarađuje dvostruko više nego ranije.“

Kajli kao da su zasijale oči. Nastavio je: „Umete li da koristite računar?“ „Naravno“, odvrati.

„Šta kažete na to da vas prebacim na sekretarski posao u marketingu?“ Ozarila se. „Radi toga bih se čak i preselila u Dalas.“

„Dalas će vam se izuzetno dopasti“, rekao je. „Ne mogu da vam obećam da će odmah biti slobodnih mesta, ali videću šta mogu da uradim.“

Pomislila je da bi ovaj uglađeni čovek u odelu s kravatom i urednom trizurinom mogao da joj pomogne da napravi veliki pomak u karijeri.

Pit je seo u drugi kraj hola, otvorio svoj prenosivi računar, i počeo nešto da radi. Nakon deset ili petnaest minuta, ponovo je prišao pultu. „Čujte“, reče, „čini se da se Majk zadržao. Postoji li ovde neka sala za sastanke u koju bi mogao da sednem i proveravam elektronsku poštu dok čekam?“

Kajla je pozvala čoveka koji organizuje raspored korišćenja sale za sastanke, i dogovorila se da Pit ode u jednu koja nije zauzeta. Prema ideji preuzetoj od kompanija iz Silicijumske doline (firma Apple je verovatno prva to uvela) neke sale za sastanke dobile su imena po likovima iz crtanih filmova, a druge prema lancima restorana, filmskim zvezdama, ili junacima iz stripova. Rečeno mu je da potraži salu pod imenom Mini Maus. Zamolila ga je da se potpiše, i objasnila mu kako da dođe do Mini Maus.

Pronašao je prostoriju, smestio se, i povezao svoj prenosivi računar na lokalnu mrežu.

Da li vam je već jasno?

Tako je – uljez se uključio u mrežu *iza kompanijske zaštitne barijere*.

Antonijeva priča

Pretpostavljam da biste Antonija Lejka mogli nazvati lenjim biznismenom. Ili bi izraz „nepošten“ više odgovarao.

Umesto da radi za druge, odlučio je da radi za sebe; hteo je da otvori radnju u kojoj bi mogao da boravi čitav dan, a da ne mora da juri po unutrašnjosti. Samo, želeo je da ima posao koji će mu sasvim sigurno donositi zaradu.

Kakvu radnju da otvori? Nije mu trebalo dugo da smisli. Razumeo se u popravku automobila – dakle, otvoriće prodavnicu auto-delova.

Kako biti siguran da će posao uspeti? Odgovor mu je samo sinuo: valja ubediti firmu koja se bavi veleprodajom auto-delova, Honorable Auto Parts, da mu prodaju svu potrebnu robu po nabavnim cenama.

Svakako, oni to ne bi svojevoljno uradili. Ali Antoni je znao kako da obmane ljude, njegov prijatelj Miki je znao kako da provali u tuđ računar, pa su zajedno skovali mudar plan.

Tog jesenjeg dana uverljivo se predstavio kao zaposleni pod imenom Piter Milton, na prevaru se domogao kancelarija kompanije Honorable Auto Parts, i već je priključio prenosivi računar na njihovu mrežu. Za sada, odlično, ali to je bio samo prvi korak. Ono što mu je preostalo da učini nije bilo lako, pogotovo što je Entoni sebi odredio vremensko ograničenje od petnaest minuta – ako bi čekao duže, smatrao je da bi rizik da ga neko razotkrije bio isuviše velik.

Prethodno se preko telefona predstavio kao službenik korisničke podrške njihovog dobavljača računara, a ulogu je odigrao savršeno do detalja. „Vaša firma je kupila dvogodišnji paket podrške, pa želimo da vas uvrstimo u bazu podataka, kako bismo znali kada izlazi zakrpa ili nova, ažurirana verzija nekog programa koji koristite. Dakle, treba da mi kažete koje aplikacije koristite.“ Kao odgovor je dobio spisak programa, a jedan prijatelj knjigovođa preporučio je da se usredsredi na program pod nazivom MAS 90 – u njemu se verovatno nalazi spisak njihovih preprodavača, kao i popusti i uslovi plaćanja za svakog od njih.

mitnikova poruka

Naučite radnike da nije zlato sve što sija – ne treba u ljude imati više poverenja samo zato što su dobro obučeni i imaju urednu frizuru.

S tim saznanjem, upotrebio je jedan program kako bi pronašao sve računare koji su trenutno povezani na mrežu, i nije mu trebalo dugo da pronađe odgovarajući server računovodstva. Pokrenuo je alatku iz arsenala hakerskih alata na prenosivom računaru, da bi popisao sve autorizovane korisnike servera. Pomoću druge alatke i spiska često korišćenih lozinki pokušao je da provali u neki nalog. Reč „password“ se poklopila s lozinkom jednog naloga. To ga nije iznenadilo. Ljudima ponestane kreativnog nadahnuća kad biraju lozinke.

Proteklo je samo šest minuta, a posao je bio do pola završen. Priključio se.

Bilo je potrebno još tri minuta da spisku mušterija veoma pažljivo doda naziv svoje nove firme, adresu, telefonski broj, i ime osobe za kontakt. Zatim je uneo ključnu stavku, onu od koje sve zavisi, u kojoj piše da mu svu robu valja prodati po ceni koja je za 1 procenat veća od nabavne.

Završio je za manje od deset minuta. Dovoljno se zadržao da bi se zahvalio Kajli, jer je okončao proveravanje poruka. I razgovarao je s Majkom

Talbotom; plan je promenjen, pa on žuri na sastanak kod klijenta. Neće zaboraviti da je preporučio za taj posao u marketingu.

Analiza prevare

Uljez koji se predstavio kao Piter Milton primenio je dve subverzivne psihološke metode – jednu planiranu, a drugu improvizovanu na licu mesta.

Obukao se kao rukovodilac koji dobro zarađuje. Odelo i kravata, pažljivo začešljana frizura – čine se samo pojedinostima, ali ostavljaju dobar utisak. To sam i lično slučajno otkrio. Dok sam kratko vreme radio kao programer u velikoj telefonskoj kompaniji GTE California, koja više ne postoji, primetio sam da me zaustave i ispituju ako dođem na posao bez propusnice, uredno, ali neformalno obučen – recimo u sportskoj majci, platnenim pantalonama i grubim cipelama. „Gde vam je propusnica, ko ste vi, gde radite?“ Drugi put bih došao, ponovo bez propusnice, ali u odelu i s kravatom; izgledao sam vrlo poslovno. Primenio bih varijaciju stare tehnike švercovanja: utopiti se u gomilu na ulasku u zgradu ili kroz čuvani ulaz. Prikačio bih se nekim ljudima dok se približavaju glavnom ulazu, i ušao bih časkajući, kao da sam jedan od njih. Prošao bih pored čuvara, a čak i kad bi primetili da nemam propusnicu, ne bi me uznemiravali jer sam izgledao kao rukovodilac i bio sam s ljudima koji su imali propusnice.

Na osnovu tog iskustva, shvatio sam koliko je predvidljivo ponašanje čuvara. Kao i svi mi, i oni ljude ocenjuju prema izgledu – što je ozbiljan propust koji obmanjivači nauče da iskoriste.

Napadačevo drugo psihološko oružje stupilo je na scenu kad je primetio koliko se službenica prijemnog odeljenja trudi. Dok je obećavala nekoliko stvari odjednom, nije izgledala mrzovoljno – svi su imali utisak da im se u potpunosti posvetila. Shvatio je to kao znak da je ambiciozna i željna dokazivanja. Kad je rekao da radi u marketinškom odeljenju, posmatrao je njenu reakciju, tražeći signale koji bi mu ukazali na to da li uspeva da uspostavi prisan odnos s njom. Pošlo mu je za rukom. Prevarantu je sve to značilo da je može izmanipulisati obećanjem da će joj pomoći da pređe na bolje radno mesto. (Naravno, da je rekla kako želi da se premesti u računovodstvo, on bi tvrdio da ima veze u tom odeljenju.)

Uljezi vole još jedno psihološko oružje koje je upotrebljeno u ovoj priči: poverenje grade u dve faze. Prvo je časkao o radnom mestu u marketinškom odeljenju, i spomenuo je poznato ime – ime nekog zaposlenog, stvarne osobe – upravo kao što je i osoba za koju se izdavao bila stvarno zaposlena.

Odmah nakon početnog razgovora mogao je zatražiti da ga puste u salu za sastanke. Umesto toga, sedeo je neko vreme pretvarajući se da radi, navodno čekajući svog saradnika, što je još jedan način da se odagna moguća sumnja, jer se uljez ne bi zadržavao. Međutim, nije sedeo predugo; obmanjivači znaju da se ne sme ostajati na mestu zločina duže nego što je neophodno.

Samo da se zna: prema važećem zakonu u vreme pisanja ove knjige, Entoni nije počinio zločin kad je ušao u hol. Nije ga počinio ni kad se predstavio kao pravi zaposleni. Nije počinio zločin ni kad je na prevaru ušao u salu za sastanke, niti kad se priključio na kompanijsku mrežu i tražio željeni računar.

Tek kad je zaista provalio u računarski sistem – prekršio je zakon.

mitnikova poruka

Dozvoliti neznancu da uđe u prostoriju u kojoj može priključiti prenosivi računar na kompanijsku mrežu povećava rizik od narušavanja bezbednosnog sistema. Savršeno je razumljivo da zaposleni, a pogotovo oni koji ne rade na toj lokaciji, žele da provere elektronsku poštu iz sale za sastanke. Ukoliko se za posetioca pouzdano ne zna da je radnik od poverenja, ili ako mreža nije podeljena da bi se sprečilo neodobreno priključivanje, to može biti slaba tačka preko koje se kompanijska dokumenta ugrožavaju.

NEKO ŠPIJUNIRA KEVINA

Pre mnogo godina, dok sam radio u jednom malom preduzeću, primetio sam da momak (kojeg ću ovde zvati Džo) brzo okrene ekran svog monitora ka drugom prozoru svaki put kad uđem u kancelariju. Odmah mi je to bilo sumnjivo. Kad se to isto dogodilo još dvaput istog dana, bio sam uveren da se događa nešto što bi trebalo da znam. Šta je on smerao a nije hteo da vidim?

Džo je radio na terminalu za pristup kompanijskim miniračunarima, pa sam instalirao program za nadgledanje na VAX miniračunaru, pomoću kojeg sam mogao da ga špijuniram. Program je radio kao da mu je televizijska kamera postavljena iza leđa, prikazujući mi tačno ono što on vidi na svom ekranu.

Moj sto je bio pored njegovog; okrenuo sam svoj ekran koliko god sam mogao da ne bi video šta radim, ali mogao je da pogleda u svakom trenutku i shvati da ga špijuniram. To nije predstavljalo problem – bio je suviše zaokupljen svojim poslom da bi išta primetio.

Zinuo sam kad sam video šta radi. Gledao sam, opčinjen, dok je taj prokletnik pregledao podatke o *mojoj* plati. Gledao je kolika mi je plata!

Bio sam tu tek nekoliko meseci, u to vreme, pa sam pretpostavio da Džo nije mogao da podnese pomisao da možda zarađujem više od njega.

Nekoliko minuta kasnije video sam da preuzima hakerske alate koje koriste manje iskusni hakeri, koji ne znaju dovoljno o programiranju da bi razvili sopstvene alate. Dakle, Džo nije ništa znao; nije imao pojma da pored njega sedi jedan od najiskusnijih hakera u Americi. To mi je bilo strašno smešno.

Već je imao podatke o mojoj plati, pa je bilo isuviše kasno da ga sprečim. Osim toga, svaki zaposleni koji preko računara ima pristup poreskoj službi ili socijalnom osiguranju može da pogleda koliko zarađujete. Naravno da nisam želeo da se razotkrijem tako što bih mu stavio do znanja da sam otkrio šta smerao. Tada je moj glavni cilj bio da se ne ističem, jer vešt obmanjivač ne otkriva svoje mogućnosti i sposobnosti. Uvek želite da vas potceni, a ne da vas smatraju pretnjom.

Zato nisam reagovao, i nasmejao sam se u sebi što Džo misli da zna neku moju tajnu, dok je zapravo bilo obrnuto: ja sam bio u prednosti jer sam znao šta smerao.

Vremenom sam otkrio da se sva tri moja saradnika u informatičkom odeljenju zabavljaju gledajući koliko zarađuje ova ili ona zgodna sekretarica ili momak kojeg su spazili. I svi su znali plate i bonuse svih zaposlenih u kompaniji koji su ih interesovali, uključujući i više rukovodstvo.

Analiza prevare

U ovoj priči prikazan je zanimljiv problem. Datoteke s platama bile su dostupne osobama zaduženim za održavanje računarskih sistema firme. Dakle, sve se svodi na osoblje, odnosno na odluku u koga se može imati poverenja. U nekim slučajevima, informatičari ne mogu da odole želji da njuškaju okolo. Mogućnost da to učine imaju jer im ovlašćenja dozvoljavaju da zaobiđu kontrolu pristupa tim dokumentima.

Jedan vid zaštite bio bi da se proverava pristup naročito osetljivim datotekama, poput onih s platama. Naravno, svako s potrebnim ovlašćenjima mogao bi da isključi sistem nadgledanja, ili možda i da ukloni odrednice koje ukazuju na provalu, ali je potrebno više energije da bi beskrupulozni radnik sakrio svoja dela.

SPREČAVANJE PREVARE

Prevaranti mogu fizički ući u firmu na razne načine, od toga da kopaju po smeću, do toga da prevare čuvara ili službenicu prijemnog odeljenja. Ipak, biće vam drago da čujete da postoje preventivne mere koje možete preduzeti.

Zaštita nakon radnog vremena

Sve zaposlene bez propusnice treba zadržati kod stola u holu ili u kancelariji obezbeđenja da bi im se izdala privremena propusnica za taj dan. Incident iz prve priče u ovom poglavlju mogao se završiti sasvim drugačije da su se kompanijski čuvari pridržavali određenog postupka u slučaju da zaposleni nema potrebnu propusnicu.

U preduzećima ili odeljenjima kompanije gde obezbeđenje nije preko potrebno, možda nije toliko važno insistirati na tome da svaka osoba uvek nosi vidljivu propusnicu, ali bi u važnim odeljenjima to trebalo da bude standardan zahtev koji se strogo primenjuje. Zaposleni se moraju obučiti i motivisati da provere identitet osoba koje nemaju propusnicu, a osobe na visokim pozicijama moraju se naučiti da prihvate takve provere i da ne dovode u neopasnost osobe koje ih zaustave.

U kompanijskom pravilniku trebalo bi da postoje kazne za radnike koji često ne nose propusnicu; kazna bi mogla biti ta da se radnik pošalje kući tog dana bez plate, ili napomena u njegovoj dokumentaciji. U nekim firmama uvodi se niz sve strožih kazni, koje mogu biti i obaveštavanje pretpostavljenog te osobe o problemu, a potom davanje zvaničnog upozorenja.

Pored toga, kompanija bi trebalo da osmisli postupke za ovlašćivanje osoba koje moraju da budu fizički prisutne u važnim prostorijama van radnog vremena. Jedno od rešenja: zahtevajte da ovlašćenja izdaje obezbeđenje ili neka specijalna radna grupa. Ta grupa bi rutinski utvrđivala identitet svakog zaposlenog koji najavi dolazak van radnog vremena. Pozivali bi pretpostavljenog te osobe, ili bi upotreбили neku drugu relativno bezbednu metodu.

Ophodite se prema smeću s dužnim poštovanjem

Priča o kopanju po smeću prikazala je mogućnost da se zloupotrebi otpadni materijal. Evo osam ključnih ideja na ovu temu:

- Klasifikujte sve osetljive informacije na osnovu stepena njihove poverljivosti.
- Širom firme uspostavite postupke za bacanje osetljivih podataka.
- Insistirajte na tome da se sve osetljive informacije koje će se baciti prvo unište, a obezbedite i neki siguran način za uklanjanje važnih informacija na papirićima koji su suviše mali da bi se mogli uništiti u mašini. Uređaji za uništavanje papirnih dokumenata ne smeju biti oni jeftini, koji seku papir u trake. Takve trake odlučni napadač, uz dovoljno strpljenja, može da složi. Umesto toga, koristite uređaje za potpuno uništavanje dokumenata, koji papir pretvaraju u beskorisnu masu.
- Nadite načina za onemogućavanje dalje upotrebe ili *potpuno* brisanje računarskih medija – disketa, Zip diskova, CD i DVD diskova, izmenljivih traka, starih čvrstih diskova i sličnog – pre nego što se bace. Upamtite da se datoteke brisanjem zapravo *ne* uklanjaju; i dalje se mogu povratiti, što su rukovodioci Enrona, kao i mnogi drugi, iskusili na sopstvenoj koži. Kad bacite neki računarski medij u smeće, pozivate svog lokalnog, prijateljski nastrojenog kopača po smeću. (U poglavlju 16 pročitajte posebna uputstva o bacanju medija i uređaja.)
- Na odgovarajućem nivou nadgledajte izbor čistača i ako treba, proveravajte i njihovu prošlost.
- Povremeno podsećajte zaposlene da razmisle o prirodi materijala koje bacaju u smeće.
- Zaključavajte kontejnere za smeće.
- Upotrebljavajte posebne posude za izbacivanje osetljivih materijala, i unajmite neku specijalizovanu firmu da uklanja takve materijale.

Ispraćanje zaposlenih

Ranije u ovoj knjizi istaknuto je da se moraju strogo definisati bezbednosni postupci pri prestanku rada zaposlenog koji je imao pristup osetljivim informacijama, lozinkama, brojevima za daljinsko povezivanje na sistem

i tome sličnom. Vaše bezbednosne procedure moraju omogućiti vođenje računa o tome kome je dozvoljen pristup raznim sistemima. Možda je teško osujetiti namere obmanjivača da se provuče pored vaših bezbednosnih barijera, ali nemojte to olakšavati bivšim zaposlenima.

Evo još jednog koraka koji se lako previdi: kad firmu napusti zaposleni koji je bio ovlašćen da radi s trakama za rezervne kopije, morate odmah da obavestite kompaniju koja obezbeđuje trake da ukloni njegovo ime sa spiska ovlašćenih lica.

U poglavlju 16 nalaze se detaljne informacije o ovoj veoma važnoj temi, ali korisno je da ovde nabrojimo neke ključne bezbednosne mere kojih se valja pridržavati, kao što se videlo iz ove priče. Trebalo bi uspostaviti:

- Potpun i detaljan spisak koraka koje valja preduzeti pri odlasku zaposlenog, sa posebnim merama za radnike koji su imali pristup osjetljivim podacima.
- Pravilo da se tom zaposlenom *odmah* zabranjuje pristup računaru – najbolje i pre nego što je napustio zgradu.
- Postupak za preuzimanje propusnice te osobe, kao i ključeva i elektronskih uređaja za pristup.
- Mere u kojima se zahteva od čuvara da pogledaju lični dokument sa slikom pre nego što prime zaposlenog bez propusnice, kao i da potraže njegovo ime na spisku da bi proverili da li je još uvek zaposlen.

Neki dodatni koraci učiniće se preteranim ili suviše skupim za neke firme, ali su primereni drugima. U te strože bezbednosne mere ubrajaju se:

- Elektronske propusnice sa skenerima na ulazima; svaki zaposleni provuče svoju propusnicu kroz skener, i trenutno se elektronski proveriti da li ta osoba još uvek radi za firmu i da li mu je dozvoljeno da uđe u zgradu. (Imajte na umu da se čuvari ipak moraju obučiti da pažljivo nadgledaju provlačenje kartice. Dešava se da neovlašćeno lice uđe odmah iza zaposlenog i zaobiđe elektronsku proveru.)
- Zahtev da svi zaposleni u radnom timu osobe koja odlazi (a naročito ako je otpuštena) promene lozinke. (Da li se to čini preteranim? Mnogo godina nakon što sam kratko vreme radio u kompaniji General Telephone, saznao sam da su se stručnjaci za računarsku bezbednost kompanije Pacific Bell valjali po podu od smeha kad su čuli da

me je General Telephone zaposlio. U prilog firmi General Telephone ide činjenica da su, nakon što su saznali da je čuveni haker radio za njih i pošto su me otpustili, zahtevali da *svi u kompaniji* promene lozinke!)

- Ne želite da vam preduzeće liči na zatvor. Istovremeno, morate se odbraniti od osobe koja je juče otpuštena, ali se danas vratila s nametom da vam naškodi.

Ne zaboravite nikoga

U bezbednosnim merama obično se previde službenici koji rade sa strankama, na primer u prijemnim odeljenjima, a ne rade s poverljivim informacijama. I ranije smo videli da su te osobe zgodna meta za napadače, a priča o upadu u kompaniju auto-delova daje još jedan primer: prijatna osoba, obučena poput profesionalca, koja tvrdi da je zaposlena u nekom drugom ogranku, možda nije onaj za koga se izdaje. Službenice prijemnog odeljenja treba dobro obučiti da ljubazno zatraže kompanijsku propusnicu u odgovarajućem trenutku, a obuka treba da obuhvati i glavne službenice i svakoga ko ih zamenjuje na prijemnom odeljenju za vreme pauze.

Što se tiče posetilaca koji ne rade u preduzeću, u pravilniku treba da stoji da valja zatražiti dokument s fotografijom i zabeležiti podatke. Nije teško domoći se lažne lične karte, ali se tako potencijalni napadač još više osujećuje.

U nekim preduzećima ima razloga da se posetioци otprate iz hola, od sastanka do sastanka. U postupku treba naglasiti da pratilac mora da razjasni da li je osoba ušla u zgradu kao zaposleni ili nezaposleni, kad ga otprati do prvog sastanka. Zašto je to važno? Jer će se, kao što smo videli u prethodnim pričama, prevarant često izdavati za jednu osobu prvom zaposlenom na kojeg naiđe, a za neku drugu sledećoj. Uljez sasvim lako može da se pojavi u holu i ubedi službenicu prijemnog odeljenja da ima sastanak sa nekim inženjerom. Kad ga otprate do kancelarije tog inženjera, može da se predstavi kao trgovački putnik iz druge kompanije, a potom, nakon sastanka s inženjerom, slobodan je da tumara zgradom.

Pre nego što se zaposleni iz drugog ogranka pusti u zgradu firme, mora se utvrditi da li on zaista radi u kompaniji; službenici prijemnog odeljenja i čuvari moraju poznavati metode koje prevaranti upotrebljavaju izdajući se za zaposlene.

A šta kažete na to da se zaštitite od prevaranta koji uđe u zgradu i uspe da uključi svoj prenosivi računar na mrežni priključak iza zaštitne barijere kompanije? Imajući u vidu današnju tehnologiju, to je pravi izazov: mrežni priključci u sobama za konferencije, obuku i u sličnim prostorijama treba da budu zaštićeni barijerama ili usmerivačima. Bolja zaštita bi se postigla primenom sigurne metode identifikacije svakog korisnika koji se priključuje na mrežu.

Bezbedan informatički tim!

Ne treba dvaput reći: u vašoj kompaniji svaki informatičar verovatno zna ili može da otkrije za nekoliko trenutaka koliko zarađujete vi, koliko generalni direktor, a ko koristi kompanijski avion za odlazak na skijanje.

U nekim kompanijama je čak moguće da informatičari ili računovođe sebi povećaju plate, uplate novac nepostojećem prodavcu, uklone negativne ocene iz dokumentacije o zaposlenima ili isplate nepostojećeg prodavca i tako dalje. Ponekad su poštteni samo zato što se plaše da će ih uhvatiti... a onda jednog dana dođe neko ko se zbog pohlepe i urođenog nepoštenja ne obazire na rizike i poduzima sve za šta misli da mu može poći za rukom.

Svakako, i za to postoje rešenja. Poverljiva dokumentacija može se zaštititi odgovarajućom kontrolom pristupa tako da ih samo ovlašćena lica mogu otvoriti. U nekim operativnim sistemima postoji mogućnost za nadgledanje događaja i zapisivanje podataka o svakoj osobi koja pokuša da pristupi zaštićenoj datoteci, bez obzira na to da li je pokušaj uspeo ili nije.

Ako je vaša kompanija razumela ovaj problem, primenila odgovarajuće kontrole pristupa i aktivirala nadgledanje pristupa osetljivim datotekama, krupnim koracima ste krenuli pravim putem.



poglavlje

11

Kombinovanje tehnologije i obmane

Obmanjivači žive od svoje sposobnosti da manipulišu ljudima koji će im pomoći da dođu do cilja, ali je za uspeh često neophodno i veliko znanje i veština pri radu s računarskim i telefonskim sistemima. Evo primera tipičnih obmana u kojima je tehnologija igrala važnu ulogu.

HAKERISANJE IZ ZATVORA

Koje su najbezbednije institucije koje možete da zamislite – zaštićene od fizičkih i elektronskih provala? Fort Noks? Naravno. Bela kuća? Apsolutno. NORAD, Severnoamerički štab za odbranu od vazдушnih napada, koji je ukopan duboko u planini? Svakako.

A šta mislite o istražnim zatvorima i kazneno-popravnim ustanovama? Mora da su i oni bezbedni kao sva slična mesta u zemlji, zar ne? Ljudi iz njih retko pobegnu, a kad se to i dogodi, obično ih odmah uhvate. Pomislili biste da na takvim mestima ni obmane ne prolaze. Ne biste bili u pravu – nigde ne postoji savršeno obezbeđenje.

Pre nekoliko godina, dvojica profesionalnih prevaranata naišli su na problem. Ispostavilo se da su ukrali veliku sumu novca u gotovini od lokalnog sudije. Ta dvojica su godinama povremeno imali problema sa zakonom, ali su se ovog puta savezne vlasti zainteresovale za njih. Uhapsili

su jednog od njih, Čarlsa Gondorfa, i strpali ga u zatvorsku ustanovu blizu San Dijega. Savezni sud mu je odredio pritvor zbog mogućnosti bekstva i opasnosti po okolinu.

Njegov prijatelj Džoni Huker znao je da će Čarliju trebati dobar advokat. Ali odakle mu novac za to? Kao i većina lopova, i oni su novac uvek trošili na dobru odeću, luksuzne automobile i dame. Džoni je jedva imao dovoljno za goli život.

Novac za dobrog advokata morao je nabaviti još jednom prevarom. Džoni to nije umeo da izvede sam. Čarli Gondorf je oduvek smišljao njihove zaverе. Ali Džoni se nije usuđivao da poseti Čarlija u zatvoru i pita ga šta da radi, jer su istražitelji znali da postoji i saučesnik, i jedva su čekali da se domognu i njega. Naročito to nije smeo da učini kad je dozvoljena poseta samo članovima porodice, što bi značilo da mora da pokaže lažnu vozačku dozvolu i predstavi se kao njegov rođak. Nije mu se činilo baš pametno da pokuša da upotrebi lažnu ispravu u saveznom istražnom zatvoru.

Ne, moraće da stupi u vezu s Gondorfom na neki drugi način.

Neće biti lako. Nijednom licu u bilo kom saveznom, državnom, ili lokalnom istražnom zatvoru nije dozvoljeno da prima telefonske pozive. Na znaku koji se nalazi pored svakog telefonskog uređaja u savezним istražnim zatvorima napisano je: „Ovim se obaveštavaju korisnici da se svi razgovori s ovog telefona nadgledaju; ko upotrebi telefon, automatski pristaje na to.“ Ako vam vladini službenici prisluškuju telefonski razgovor dok činite krivično delo, sigurno će vam se „odmor“ u toj saveznoj ustanovi produžiti.

Ipak, Džoni je znao da se određeni telefonski pozivi ne nadgledaju: na primer, razgovori između zatvorenika i njegovog advokata, jer su američkim Ustavom zaštićeni kao komunikacija između pravobranioca i njegovog klijenta. Zapravo, u zatvoru su i telefoni direktno povezani s kancelarijom javnog pravobranioca. Podignite slušalicu na jednom od tih aparata, i direktno dobijate vezu s odgovarajućim telefonom u pomenutoj kancelariji. Telefonska kompanija tu uslugu naziva *Direktna veza*. Vlasti koje ništa ne sumnjaju smatraju da je ta usluga bezbedna i da se ne može zloupotребiti, jer izlazni pozivi stižu samo u kancelariju javnog pravobranioca, a dolazni pozivi se blokiraju. Čak i ako neko sazna taj telefonski broj, on je blokiran u telefonskoj centrali.

S obzirom na to da je svaki iole pristojan prevarant dobro potkovан u umetnosti obmane, Džoni je pomislio da mora postojati rešenje tog

problema. Iz zatvora, Gondorf je već jednom podigao slušalicu jednog od telefona priključenih na kancelariju javnog pravobranioca, i rekao: „Ovde sam iz servisa telefonske kompanije. Proveravam ovu liniju, pa vas molim da okrenete broj devet, a potom nula-nula.“ Pomoću broja devet dobio bi izlaznu liniju, a kad bi službenik okrenuo nula-nula, javio bi mu se operater za međugradske pozive. Nije upalilo – osoba koja se javila na telefon u kancelariji već je poznavala taj trik.

terminologija

DIREKTNА VEZA (engl. *direct connect*) Izraz telefonske kompanije za telefonsku liniju kojom se direktno poziva određeni broj kad se slušalica podigne.

BLOKIRANI BROJ (engl. *deny terminate*) Usluga telefonske kompanije kojom se na centrali blokiraju dolazni pozivi.

Džoni je imao više uspeha. Lako je saznao da u istražnom zatvoru postoji deset spavaonica i da je svaka povezana direktnom telefonskom linijom s javnim pravobraniocem. Džoni je naišao na probleme ali je, kao i svaki obmanjivač, uspeo da smisli način da zaobiđe te dosadne prepreke. U kojoj se spavaonici nalazi Gondorf? Koji je telefonski broj službe za direktno povezivanje u toj spavaonici? I kako će preneti poruku Gondorfu tako da zatvorski čuvari ništa ne primete?

Za ono što se običnim ljudima čini nemogućim, kao što je otkrivanje tajnih telefonskih brojeva zatvorskih institucija, obmanjivaču je često potrebno samo nekoliko telefonskih poziva. Nakon nekoliko besanih noći tokom kojih je smišljao šta da preduzme, Džoni se jednog jutra probudio s detaljnim planom u glavi, u pet koraka.

Prvo će saznati telefonske brojeve tih deset telefona direktno povezanih s kancelarijom javnog pravobranioca.

Potom će izmeniti svih deset tako da prihvataju dolazne pozive.

Saznaće u kojoj se spavaonici nalazi Gondorf.

Potom će otkriti telefonski broj te spavaonice.

Konačno, ugovoriće s Gondorfom kada da očekuje njegov poziv, tako da država ništa ne posumnja.

Mačji kašalj, pomislio je.

Poziv telefonskoj kompaniji

Džoni je počeo od poziva poslovnom ogranaku telefonske kompanije pod izgovorom da zove iz agencije General Services Administration, odgovorne za nabavku roba i usluga za američku vladu. Rekao je da naručuje dodatne usluge, te da mu trebaju informacije o svim direktnim vezama koje se trenutno koriste, uključujući i njihove telefonske brojeve i mesečne račune u istražnom zatvoru u San Dijegu. Gospođa mu je rado pomogla.

Radi provere, pokušao je da okrene jedan od brojeva, ali javio mu se tipičan snimak koji se ponavlja: „Ova linija je isključena, ili se više ne koristi.“ On je znao da to nije istina; linija je programirana tako da blokira dolazne pozive, baš kao što je i očekivao.

Budući da je dobro poznao procedure i rad telefonske kompanije, znao je da mora pozvati njihov Centar za memorisanje i ovlašćivanje nedavno izmenjenih brojeva (Recent Change Memory Authorization Center, RCMAC). Nikad mi neće biti jasno ko smišlja te nazive! Najpre je nazvao poslovni ogranak telefonske kompanije, rekao da zove iz servisa i da mu je potrebno da zna broj RCMAC-a koji je zadužen za pozivni broj i početnih nekoliko brojeva koje im je dao. Te linije su bile povezane na istu centralu kao i sve telefonske linije u istražnom zatvoru. Bio je to rutinski zahtev, na koji se odgovara tehničarima na terenu kojima je potrebna pomoć, pa službenik nije oklevao i dao mu je broj.

Nazvao je RCMAC, lažno se predstavio i rekao da radi u servisu. Zamolio je damu koja mu se javila da pristupi jednom od brojeva do kojih je na prevaru došao u jednom od prethodnih telefonskih razgovora. Kad je uspela, Džoni ju je upitao: „Da li su dolazni pozivi tog broja blokirani?“

„Jesu“, odgovorila je.

„Pa, eto objašnjenja zašto klijent ne može da prima pozive!“ Džoni reče: „Čujte, možete li mi učiniti uslugu? Treba da izmenite klasifikacioni kôd ove linije, ili da deblokirate dolazne pozive, u redu?“ Usledila je pauza dok je ona u drugom računarskom sistemu proveravala da li postoji odgovarajuć nalog za izvršenje. Odgovori: „Taj broj *i treba* da bude ograničen samo na izlazne pozive. Ne postoji nalog za izvršenje izmene.“

„Da, to je greška. Trebalo je da pošaljemo nalog juče, ali se koleginica koja se bavi naložima ovog korisnika razbolela i otišla kući. Zaboravila je da obavesti nekog drugog da se pobrine o tome. Naravno, sad je korisnik pobesneo.“

Dama je nakratko razmotrila zahtev, koji bi bio vanredan i neprimeren standardnim radnim procedurama, i odgovorila: „U redu“. Mogao je čuti kako kuca, unoseći izmenu. Nekoliko sekundi kasnije završila je.

Probio je led, a oni kao da su sada bili u dosluhu. Procenjujući njen stav i spremnost da pomogne, Džoni nije oklevao da ide do kraja. Rekao je: „Imate li još nekoliko minuta da mi pomognete?“

„Da“, odgovorila je. „Šta vam treba?“

„Imam još nekoliko linija koje pripadaju istom korisniku, i sa svima je isti problem. Pročitaću vam brojeve, a vi se postarajte za to da dolazni pozivi ne budu blokirani, u redu?“ Rekla je da nema problema.

Nakon nekoliko minuta, svih deset telefonskih linija „podešeno“ je tako da prihvataju dolazne pozive.

Kako pronaći Gondorfa

Dalje, valjalo je pronaći u kojoj se spavaonici Gondorf nalazi. Tu informaciju osoblje istražnih zatvora i kazneno-popravnih ustanova zasigurno ne želi da objavi. Džoni je ponovo morao da se osloni na svoju veštinu obmane.

Pozvao je savezni zatvor u drugom gradu – pozvao je Majami, ali poslužio bi bilo koji grad – i kazao da zove iz istražnog zatvora u Njujorku. Zamolio je da razgovara s nekim ko radi s računarima Uprave straže, čiji sistem sadrži podatke o svakom zatvoreniku koji se nalazi u nekoj od institucija pod nadležnošću Zatvorske uprave širom zemlje.

Kad se ta osoba javila na telefon, Džoni je progovorio bruklinskim naglaskom. „Zdravo“, reče. „Ovde Tomas iz federalnog istražnog zatvora u Njujorku. Naša veza sa sistemom Straže se stalno prekida. Možete li mi reći gde se nalazi jedan zatvorenik? Mislim da je možda u vašoj instituciji“, i dao mu je Gondorfovo ime i registracioni broj.

„Ne, nije ovde“, reče čovek nakon nekoliko trenutaka. „Nalazi se u istražnom zatvoru u San Dijegu.“

Džoni je glumio iznenađenje. „San Dijego! Trebalo je da ga prebace u Majami državnim letom prošle nedelje! Govorimo li o istom čoveku – koji mu je datum rođenja?“

„12/3/60“, pročitao je sagovornik.

„Da, to je ista osoba. U kojoj je spavaonici?“

„U desetoj severnoj“, odvrati ovaj bezbrižno, iako nema nijednog razloga zašto bi zatvorskom službeniku u Njujorku bio potreban taj podatak.

Džoni je sad uspeo da podesi telefone tako da primaju pozive, i znao je u kojoj se spavaonici Gondorf nalazi. Trebalo je otkriti telefonski broj povezan sa desetom severnom spavaonicom.

To je bilo relativno teško. Džoni je pozvao jedan od brojeva. Znao je da je zvučnik telefona isključen, te da niko neće znati da zvoni. Zato je sedeo i čitao *Fodorov vodič kroz velike gradove Evrope*, slušajući stalnu zvonjavu na svom telefonu sa zvučnikom sve dok neko najzad nije podigao slušalicu. Zatvorenik s druge strane slušalice, naravno, pokušava da dobije svog advokata kojeg mu je dodelio sud. Džoni je bio spreman na očekivani odgovor. „Kancelarija javnog pravobranioca“, izdeklamovao je.

Kad je čovek s druge strane žice zatražio da razgovara sa svojim advokatom, Džoni reče: „Proveriću da li je slobodan; iz koje spavaonice zovete?“ Zapisao je njegov odgovor, spustio slušalicu, ponovo je podigao za pola minuta i rekao: „U sudu je, moraćete da pozovete kasnije“, i prekinuo je vezu.

Proveo je tako dobar deo prepodneva, ali moglo je biti i gore; ispostavilo se da je četvrti poziv upućen iz desete severne spavaonice. Sada je Džoni znao broj telefona u Gondorfovoj spavaonici.

Sinhronizujmo satove

Sada valja preneti poruku Gondorfu kada da podigne slušalicu. To je bilo lakše nego što zvuči.

Džoni je nazvao istražni zatvor, i službenim glasom se predstavio kao zaposleni i zamolio da ga spoje s desetom severnom spavaonicom. Odmah su to učinili. Kada je zatvorski službenik podigao slušalicu, Džoni ga je obmanuo upotrebivši jedan lokalni izraz za prijemno i otpusno odeljenje: „Ovde Tajson iz PO-a“, reče. „Moram da razgovaram sa zatvorenikom Gondorfom. Treba da otpremimo njegove stvari, pa nam je potrebna adresa na koju želi da je pošaljemo. Možete li ga pozvati na telefon?“

Džoni je čuo kako čuvar više kroz sobu za dnevni boravak. Nakon nekoliko minuta nestrpljenja, začuo je poznat glas.

Džoni mu reče: „Nemoj ništa da kažeš dok ti ne objasnim o čemu je reč.“ Objasnio mu je pod kojim ga izgovorom zove, da bi mogao da zvuči kao da razgovara o tome gde da mu pošalju imovinu. Džoni zatim reče: „Ako možeš da upotrebiš telefon javnog pravobranioca u jedan danas poslepodne, nemoj ništa da odgovoriš. Ako ne možeš, reci mi u koliko sati možeš biti pored telefona.“ Gondorf nije ništa odgovorio. Džoni je nastavio: „Dobro, onda budi tamo u jedan. Pozvaću te. Podigni slušalicu. Ako se oglasi u kancelariji javnog tužioca, prekidaj vezu svakih dvadeset sekundi. Pokušavaj sve dok me ne budeš čuo.“

U jedan sat Gondorf je podigao slušalicu, a Džoni ga je čekao s druge strane žice. Zadovoljno su časkali, bez žurbe, a usledio je niz sličnih razgovora u kojima su planirali prevaru da bi obezbedili novac za Gondorfovog branioca – i sve to bez državnog nadgledanja.

Analiza prevare

Ova epizoda odlično ilustruje kako obmanjivač može da učini nešto što je naizgled nemoguće. Dovoljno je da navede nekoliko ljudi da učine nešto što se, samo po sebi, čini nevažnim. Zapravo, iz svakog tog čina nastaje jedan mali deo slagalice sve dok se prevara ne upotpuni.

Prva službenica telefonske centrale mislila je da daje informacije neko- me iz Službe društvenog knjigovodstva američke vlade.

Sledeća službenica iste kompanije znala je da ne bi smela da menja klasifikaciju telefonskih usluga bez naloga, ali je, bez obzira na to, pomogla ljubaznom sagovorniku. Tako je omogućila da pozivi stižu na svih deset linija direktno povezanih s javnim pravobraniocem u istražnom zatvoru.

Čoveku u istražnom zatvoru u Majamiju činilo se savršeno razumnim da pomogne kolegi iz druge kazneno-popravne ustanove koji ima problema s računarom. Iako nije bilo jasno zašto bi želeo da zna broj spavaonice zatvorenika, zašto ne odgovoriti na pitanje?

A šta reći o čuvaru u desetoj severnoj spavaonici, koji je poverovao da ga sagovornik zaista zove iz iste ustanove, po službenoj dužnosti? Bio je to savršeno uverljiv zahtev, pa je pozvao zatvorenika Gondorfa na telefon. U čemu je problem?

Bio je to niz dobro isplaniranih priča koje su se jedna na drugu nado- vezivale da bi upotpunile žaoku.

BRZO PREUZIMANJE

Deset godina nakon što su završili pravni fakultet, Ned Rejsin je video da njegove bivše kolege žive u lepim kućama s travnjacima, da su učlanjeni u privatne klubove, i igraju golf jednom ili dvaput nedeljno, dok on još uvek vodi sitne slučajeve za stranke koje nikada nisu imale dovoljno novca da ga plate. Zavist može biti opasna. Najzad, jednog dana, Nedu je bilo dosta svega.

Jedini dobar klijent kojeg je ikada imao bila je mala, ali veoma uspešna knjigovodstvena kompanija koja se specijalizovala za integracije i kupovine preduzeća. Nedove usluge im dugo nisu bile potrebne, dovoljno dugo da on shvati da su upleteni u takve poslove koji bi, kad bi dospeli do novina, uticali na cene akcija nekoliko preduzeća. Bile su to akcije male vrednosti, od onih koje se javno oglašavaju, ali je to u neku ruku bilo čak i bolje – mali skok cena odrazio bi se kao procentualno velik dobitak u odnosu na investiciju. Kad bi samo mogao da zaviri u njihova dokumenta i otkrije na čemu rade...

Poznavao je čoveka koji je poznavao nekoga ko se razumeo u delimično nezakonite radnje. On je saslušao plan, zagrejao se za njega, i prihvatio da mu pomogne. Za nadoknadu manju nego što obično naplaćuje, i procenat od Nedove dobiti na berzi, čovek je uputio Neda šta mu valja činiti. Takođe mu je dao i jednu zgodnu spravicu, nešto sasvim novo na tržištu.

Nekoliko dana za redom Ned je osmatrao parking malog poslovnog centra u kojem su bile neupadljive kancelarije pomenute knjigovodstvene kompanije. Većina zaposlenih je odlazila s posla između 5:30 i 6. Do 7 sati parking bi se potpuno ispraznio. Čistači su dolazili oko 7:30. Savršeno.

Sledeće večeri, nekoliko minuta pre 8 sati, Ned se parkirao u ulici preko puta parkinga. Kao što je i očekivao, na parkingu nije bilo nikoga, osim kamiona čistača. Ned je prislonio uho na vrata i čuo kako radi usisivač. Pokucao je na vrata veoma glasno, a potom sačekao stojeći tako u odelu i kravati, u ruci držeći svoju izlisanu aktovku. Nije bilo odgovora, ali on je bio strpljiv. Ponovo je pokucao. Konačno se pojavio jedan od čistača. „Zdravo“, povika Ned kroz staklena vrata, pokazujući mu posetnicu jednog od poslovnih partnera koju je uzeo nešto ranije. „Zaključao sam ključeve u kolima, pa moram da dođem do svog radnog stola.“

Čovek mu je otključao vrata, ponovo ih zaključao kad je Ned ušao, a potom pošao niz hodnik i upalio svetla kako bi Ned mogao da vidi kuda

ide. A zašto da ne – čistač je samo bio ljubazan prema jednom od ljudi od kojih zavisi njegova egzistencija. Ili je bar imao razloga da tako razmišlja.

Ned je seo za računar jednog od poslovnih partnera i uključio ga. Dok se pokretao, povezao je onaj mali uređaj na USB priključak računara. Taj uređaj je toliko mali da se može nositi kao privezak za ključeve, pa ipak može da sadrži više od 120 megabajta podataka. Priključio se na mrežu pomoću korisničkog imena i lozinke partnerove sekretarice, jer su bile zgodno zapisane na papiriću zalepljenom za ekran. Za manje od pet minuta Ned je preuzeo sve tabele i dokumente s te radne stanice i iz jednog mrežnog direktorijuma, i bio je već na putu kući.

mitnikova poruka

Industrijski špijuni i računarski prevaranti ponekad pokušaju fizički da uđu u kancelarije žrtve. Umesto da pajserom razvale vrata, obmanjivači utiču na osobu s druge strane vrata da ih otvori.

LAK PLEN

Kad sam se prvi put susreo s računarima u srednjoj školi, morali smo preko modema da se povežemo na centralni miniračunar DEC PDP 11 u centru Los Anđelesa koji su delile sve srednje škole iz tog grada. Operativni sistem na tom računaru zvao se RSTS/E, i na njemu sam naučio da radim.

U to vreme, 1981. DEC je organizovao godišnju konferenciju za svoje korisnike. U popularnom časopisu za korisnike operativnog sistema RSTS/E nalazilo se obaveštenje o novom bezbednosnom proizvodu pod imenom LOCK-11. Proizvod su promovisali putem pametno osmišljene reklamne kampanje koja je glasila otprilike ovako: „3:30 je ujutru, a vaš komšija Džoni otkrio je vaš broj za povezivanje na mrežu, 555-0336, iz 336-og pokušaja. Sad je on u igri, a vi ste van nje. Nabavite LOCK-11.“ Taj sistem se nije mogao prevariti, tvrdilo se u reklamama. I biće prikazan na konferenciji u Los Angelesu.

Žarko sam želeo da sam vidim taj proizvod. Moj školski drug i prijatelj, Vini, koji je zajedno sa mnom hakerisao nekoliko godina, a kasnije je postao doušnik u slučaju protiv mene, bio je, kao i ja, zainteresovan za taj novi DEC-ov proizvod, pa me je podsticao da pođem na konferenciju s njim.

Prokockani ulog

Kad smo stigli, već su svi na konferenciji pričali o proizvodu LOCK-11. Činilo se da se proizvođači kockaju sopstvenim novcem. Opkladili su se da niko ne može da porazi njihov proizvod. Zvučilo je kao izazov kojem nisam mogao odoljeti.

Uputili smo se pravo ka štandu na kom se nalazio LOCK-11. Tu su stajala trojica autora. Prepoznao sam ih, kao i oni mene – već kao pubertetliju pratio me je glas da sam haker i telefonski prevarant, zbog velikog članka koji je *LA Times* objavio o mom prvom maloletničkom sukobu s vlastima. U članku je pisalo da sam uspeo nekog da ubedim da me pusti u zgradu kompanije Pacific Telephone usred noći i da sam iz nje izašao s priručnicima za računare, pred nosom njihovog čuvara. (Čini se da je *Times* želeo da štampa senzacionalističku priču, pa im je odgovaralo da objave moje ime. Budući da sam bio maloletan, u članku je prekršen običaj, ako ne i zakon, da se imena maloletnika optuženih za krivična dela ne objavljuju.)

Kad smo Vini i ja prišli, pokazali su interesovanje, a i mi. Oni su bili zainteresovani za nas, jer su me prepoznali kao hakera o kojem su čitali, i bili su pomalo zapanjeni što me vide. Nas je privuklo to što je svaki od tri tvorca stajao tamo s novčanicom od 100 dolara koja je virila ispod konferencijske značke. Nagrada za svakog ko bi uspeo da porazi njihov sistem bila je svih 300 dolara, što je bilo mnogo novca za dvojicu pubertetlija. Jedva smo čekali da počnemo.

LOCK-11 je bio dizajniran na utvrđenom principu koji se oslanjao na dva nivoa bezbednosti. Korisnik je, kao i obično, morao imati važeće korisničko ime i lozinku, ali su uz to identifikacija i lozinka obezbeđivali pristup samo ako se unesu na ovlašćenim terminalima; taj se pristup zove *bezbednost zasnovana na terminalu*. Da bi porazio sistem, haker osim poznavanja korisničkog imena i lozinke, mora i da unese te podatke na odgovarajućem terminalu. Ta metoda je već bila proverena, pa su tvorci proizvoda LOCK-11 bili ubeđeni da će sprečiti loše momke da provaljuju u sisteme. Odlučili smo da ih naučimo pameti, i uz to zaradimo tri stotine dolara.

Mladić koga su smatrali stručnjakom za sistem RSTS/E već nas je pretekao pred štandom. Nekoliko godina ranije on je bio jedan od momaka koji su me izazvali da provalim u DEC-ov interni računar za razvoj, nakon čega su me njegovi prijatelji prijavili. Kasnije je postao čuveni programer. Saznali smo da je pokušao da porazi bezbednosni program LOCK-11

nedugo pre nego što smo mi stigli, ali da nije uspeo. Zbog toga su proizvođači bili još sigurniji da je njihov proizvod zaista bezbedan.

Pravila takmičenja bila su jednostavna: onaj ko provali u sistem dobija novac. Bio je to dobar štos za dobijanje publiciteta... osim ako neko ne uspe da ih posrami i odnese novac. Bili su toliko sigurni u svoj proizvod i dovoljno drski da su pored štanda okačili odštampan spisak s brojevima nekih naloga u sistemu i odgovarajućim lozinkama. Nisu to bili samo obični korisnički, već svi privilegovani nalozi.

terminologija

BEZBEDNOST ZASNOVANA NA TERMINALU (engl. *terminal-based security*) Bezbednosni sistem koji se delom zasniva na identifikaciji korišćenog računarskog terminala; ova bezbednosna metoda bila je naročito popularna na IBM-ovim velikim računarima.

Prihvatili smo izazov

Vini i ja smo otišli odatle, porazgovarali o izazovu i smislili plan. Tumarali smo oko neobavezno, iz daljine motreći na štand. Za vreme ručka, kad se gužva smanjila, tri autora su iskoristila pauzu i otišla zajedno da nešto pojedju, ostavivši za štandom neku ženu koja je mogla biti supruga ili devojka jednog od njih. Odšetali smo se tamo, a ja sam ženi odvrtao pažnju, časkajući s njom o svemu i svačemu: „Koliko dugo radite za ovu firmu?“ „Koje druge proizvode vaša kompanija ima na tržištu?“ i tako dalje.

U međuvremenu se Vini, kojeg nije mogla da vidi, bacio na posao. Osim toga što smo bili opčinjeni provaljivanjem u računarske sisteme, i što je mene interesovalo mađioničarstvo, obojicu je zanimalo da naučimo kako da otvaramo brave. Kao dečak, pretražio sam sve police jedne malo poznate knjižare u dolini San Fernando, koja je imala gomile knjiga o tome kako obiti bravu, izvući se iz lisica, napraviti lažnu ličnu kartu – sve što jedno dete ne treba da zna.

Vini je, kao i ja, vežbao obijanje brava sve dok nismo postali zaista dobri. Bili smo u stanju da obijemo svaku bravu koja se mogla kupiti u prosečnoj gvoždari. Jedno vreme sam uživao u korišćenju brava da bih se našalio na tuđ račun. Na primer, primetio bih da neko koristi dve brave radi dodatne zaštite, obio ih i vratio u suprotna ležišta, što bi zbunilo i iznerviralo vlasnika kad pokuša da ih otključa.

U izložbenoj sali, ja sam i dalje odvrćao pažnju devojci, dok je Vini, čučajući iza štanda kako ga niko ne bi video, obio bravu na ormaru u kom se nalazio njihov PDP-11 miniračunar i završni kablovski otpornici. Bilo je smešno kako su zaključali ormar. Na njemu se nalazila prosta brava, poznata po tome što je lako obijaju čak i relativno smušeni amateri poput nas.

Vini je čitav minut otvarao bravu. Unutar ormara našao je upravo ono što je očekivao: niz priključaka u koje se uključuju korisnički terminali, i jedan priključak za konzolni terminal. Taj terminal koriste operater na računaru ili administrator sistema da bi upravljali svim računarima. Vini je priključio kabl koji vodi od konzolnog terminala u jedan terminal na konferencijskom podijumu.

To je značilo da taj terminal sada predstavlja konzolni terminal. Seo sam za prespojeni računar i prijavio se na sistem pomoću lozinke koju su tvorci programa tako drsko objavili. S obzirom na to da je softver LOCK-11 tada prepoznao da se prijavljujem s ovlašćenog terminala, odobrio mi je pristup, pa sam se priključio s privilegijama administratora sistema. Na operativni sistem sam instalirao zakrpu koja ga je izmenila tako da mogu da se prijavim za rad kao privilegovani korisnik sa svakog terminala na podijumu.

Kad sam instalirao tajnu zakrpu, Vini je vratio terminalski kabl tamo gde se isprva nalazio. Potom je ponovo obio bravu da bi zaključao vrata ormarića.

Pogledao sam programski kôd da bih prelistao dokumenta na računaru, tražeći program LOCK-11 i datoteke u vezi s njim, pa sam nabasao na nešto što me je zapanjilo jer nije trebalo da bude na ovom računaru. Tvorci programa bili su isuviše samouvereni, toliko ubeđeni da je njihov softver nepobediv, da se nisu potrudili da uklone izvorni kôd svog novog proizvođa. Prešavši na susedni terminal sa štampačem, počeo sam da štampam delove izvornog koda na neprekidnu traku računarskog papira sa zelenim prugama, koji se u to vreme koristio.

Vini je jedva uspeo da ponovo zaključa bravu i pridruži mi se pre nego što su se momci vratili s ručka. Zatekli su me kako sedim za računarem i pritiskam tipke dok je štampač stalno zujao. „Šta radiš, Kevine?“, upitao me je jedan od njih.

„Samo štampam vaš izvorni kôd“, rekoh. Mislili su da se šalim, sve dok nisu pogledali štampač i videli da je to *zaista* taj ljubomorno čuvani izvorni kôd njihovog proizvođa.

Nisu verovali da sam se prijavio za rad kao privilegovani korisnik. „Pritisni tastere Control-T“, naložio mi je jedan od proizvođača. Učinio sam to. Poruka koja se pojavila na ekranu potvrdila je ono što sam im rekao. Čovek se lupio po čelu, a Vini reče: „Trista dolara, molim vas.“

mitnikova poruka

Evo još jednog primera kako pametni ljudi potcenjuju neprijatelja. A šta je s vama – jeste li vi toliko sigurni u obezbeđenje svoje kompanije da biste se kladili u 300 dolara da napadač ne može da ga probije? Ponekad se ne očekuje zaobilazanje tehnološkog bezbednosnog uređaja.

Isplatili su nas. Vini i ja smo se šetali po konferencijskom podijumu do kraja dana sa novčanicama od stotinu dolara zadnutim za konferencijske značke. Svako ko ih je video znao je šta znače.

Naravno, Vini i ja nismo pobedili njihov softver. Da je razvojni tim razmislio o tome da postavi bolja pravila takmičenja, ili da su upotreбили zaista sigurnu bravu, ili da su pažljivije motrili na opremu, ne bi doživeli poniženje dana. Ovako su ih ponizila dvojica pubertetlija.

Kasnije sam saznao da je razvojni tim morao da svrati u banku po gotovinu: te novčanice od sto dolara bile su sav džeparac koji su imali uza se.

REČNIK KAO ORUŽJE

Kad se neko domogne vaše lozinke, u stanju je da vam napadne sistem. U većini slučajeva, nikad i ne saznate da se nešto loše dogodilo.

Jedan mlad napadač kog ću zvati Ivan Piters želeo je da dođe do izvornog koda nove elektronske igre. Bez problema se povezao na kompanijsku regionalnu mrežu, jer se jedan njegov prijatelj haker već ranije uključivao na njihove servere za Web. Kad je pronašao propust u softveru Web servera i shvatio da računar ima dve mrežne adrese, njegov prijatelj je gotovo pao sa stolice. Pronašao je mesto preko kojeg se moglo ući u internu mrežu.

Kad se Ivan povezao, susreo se s problemom pomalo nalik na traženje Mona Lize u Luvru. Bez mape, mogli biste lutati nedeljama. Kompanija je bila globalna, sa stotinama poslovnica i hiljadama računarskih servera, a nisu baš obezbedili indeks razvojnih sistema, niti uslugu turističkog vodiča koji bi vodio do cilja.

Umesto da primeni tehnički pristup kako bi pronašao željeni server, Ivan je upotrebio metodu obmane. Obavio je nekoliko telefonskih razgovora po metodama opisanim u ovoj knjizi. Prvo je pozvao tehničku podršku i tvrdio da je službenik koji ima problem s interfejsom proizvoda koji njegov tim dizajnira, i zamolio ih za telefonski broj vođe projekta razvojnog tima za igre.

Potom je nazvao čoveka čije su mu ime dali, predstavljajući se kao neko ko radi u tehničkoj službi. „Kasnije večeras“, rekao je „zamenićemo usmerivač, pa treba da se postaram za to da vaš tim ne izgubi vezu sa serverom. Zato treba da znamo koje servere koristi vaš tim.“ Mrežu stalno nadograđuju. Ako dâ ime servera, to nikom ne može škoditi, zar ne? Budući da je zaštićen lozinkom, ime servera ne može pomoći provalniku da se na njega poveže. Tako je čovek dao napadaču ime servera. Nije se čak ni potrudio da ga pozove kako bi proverio njegovu priču, niti da mu zapiše ime i telefonski broj. Samo mu je dao imena servera: ATM5 i ATM6.

Potruga za lozinkom

Tada je Ivan prešao na tehnički pristup da bi došao do podataka za identifikaciju. Prvi korak u većini tehničkih napada na sisteme pomoću kojih se dobija mogućnost daljinskog pristupa čini traženje naloga s jednostavnom lozinkom koji predstavlja početno mesto za ulazak u sistem.

Kad napadač upotrebi hakerske alatke da bi daljinski isprobavao lozinke, može ostati priključen na kompanijsku mrežu satima bez prekida. Jasno je da to čini na sopstveni rizik: što duže ostane na vezi, to je veći rizik da ga otkriju i uhvate.

Kao pripremni korak, Ivan je popisao naloge da bi saznao pojedinosti o ciljnom sistemu. Na Internetu je pronašao odgovarajući softver (na adresi <http://ntsleuth.Ocatch.com>; znak ispred reči „catch“ je nula). Ivan je na Webu našao nekoliko javno dostupnih hakerskih alatki kojima se automatski popisuju nalozi. Izbegao je ručno popisivanje za šta bi trebalo više vremena, i bilo bi rizičnije. Znajući da pomenuta organizacija koristi uglavnom servere pod Windowsom, preuzeo je alatku NBTEnum, uslužni program za popisivanje NetBIOS-a. Uneo je IP adresu servera ATM5, i pokrenuo program. Alatka za popisivanje uspeła je da otkrije nekoliko postojećih naloga na serveru.

terminologija

POPISIVANJE (engl. enumeration) Postupak otkrivanja postojećih usluga na ciljnom sistemu, operativnog sistema i spiska imena korisnika.

Kad popišete postojeće naloge, istom alatkom možete pokrenuti napad pomoću rečnika. Za napad pomoću rečnika znaju mnogi stručnjaci za bezbednost računara, kao i uljezi, ali ostali se uglavnom zapanje kad čuju da je to moguće. Cilj takvog napada je da se otkriju lozinke svakog korisnika sistema primenom često korišćenih reči.

Svi smo u nekom pogledu lenji, ali uvek me iznova zapanjuje to što ljudima ponestaje kreativnosti i mašte kad treba da izaberu lozinku. Većina zeli lozinku koja će štititi, ali koja se istovremeno lako pamti, pa se najčešće bira blizak pojam. Na primer, česte lozinke su inicijali, srednje ime, nadimak, ime supružnika, omiljena pesma, film, ili piće. Lozinke su često i ime ulice ili grada u kojima živimo, marka automobila koji vozimo, mesto na moru u kojem volimo da letujemo, ili omiljeni potok u kojem se najbolje pecaju pastrmke. Prepoznajete li šablon? Lozinke su uglavnom lična imena, nazivi mesta ili reči iz rečnika. Napadom pomoću rečnika pročešljaju se uobičajene reči veoma brzo, i svaka od njih se isproba kao lozinka na jednom ili više korisničkih naloga.

Ivan je podelio napad pomoću rečnika u tri stepena. U prvom je upotrebio jednostavan spisak od oko 800 najčešćih reči; na spisku su se nalazile i reči *tajna*, *posao*, i *lozinka*. Program je i permutovao reči iz rečnika kako bi isprobao svaku reč s pridodatom cifrom, ili dodajući joj broj tekućeg meseca. Program je svaku kombinaciju isprobavao na svim popisanim korisničkim naložima. Nije bilo sreće.

U sledećem pokušaju, Ivan je na pretraživaču Google potražio spiskove reči. Pronašao je hiljade lokacija s dužim spiskovima reči i rečnicima za engleski i nekoliko stranih jezika. Preuzeo je čitav elektronski rečnik engleskog jezika. Potom je rečniku dodao i više spiskova reči koje je pronašao pomoću pretraživača Google. Ivan je odabrao lokaciju na adresi www.outpost9.com/files/WordLists.html.

Sa te lokacije mogli su se preuzeti (a sve to *besplatno*) delovi datoteka u kojima su se nalazila prezimena i imena, imena i reči u vezi s Kongresom, imena glumaca, kao i reči i imena iz Biblije.

Jednu od mnogih lokacija na kojima se nude spiskovi reči održava Oksfordski univerzitet, na adresi <ftp://ftp.ox.ac.uk/pub/wordlists>.

Na drugim lokacijama nalaze se spiskovi likova iz crtanih filmova, reči koje je koristio Šekspir ili Tolkin, reči iz *Odiseje* i serije *Zvezdane staze*, kao i iz nauke i religije i tako dalje. (Jedna kompanija na Internetu za samo 20 dolara prodaje spisak od 4,4 miliona reči i imena.) Napadački program se takođe može podesiti tako da isprobava anagrame reči iz rečnika, što je još jedna omiljena metoda korisnika računara, za koju se misli da povećava bezbednost.

Brže nego što mislite

Kad je Ivan odlučio koji spisak da upotrebi i započeo napad, softver je radio automatski. Mogao je da se usredsredi na nešto drugo. A evo i neverovatnog dela priče: pomislili biste da bi haker za vreme takvog napada mogao da prespava nekoliko godina kao Rip van Vinkl, a da bi softver i dalje slabo napredovao kad bi se probudio. Zapravo, u zavisnosti od platforme koju napada, bezbednosne konfiguracije sistema, i mrežne veze, sve reči u rečniku engleskog jezika mogu se, neverovatno, isprobati za manje od trideset minuta!

Za vreme ovog napada, Ivan je na drugom računaru započeo sličan napad na drugi server koji koristi razvojni tim – ATM6. Nakon dvadesetak minuta, napadački softver je učinio ono što mnogi korisnici smatraju nemogućim: obelodanio je da je jedan od korisnika izabrao lozinku „Frodo“, ime Hobita iz knjige *Gospodar prstenova*.

Pomoću ove lozinke, Ivan je uspeo da se poveže na server ATM6.

Za našeg napadača postojala je jedna dobra, i jedna loša vest. Dobra vest je bila ta da nalog koji je provalio ima ovlašćenja administratora, što je neophodno za sledeći korak. Loša vest je bila ta što izvornog koda igre nije bilo nigde. Mora da je izvorni kôd, ipak, na drugom računaru, za koji je već znao da se ne može pokoriti napadom pomoću rečnika. Ali Ivan još uvek nije odustajao; i dalje je mogao da isproba još nekoliko trikova.

Na nekim računarima pod Windowsom i UNIX-om, šifrovane lozinke su javno dostupne svakom ko ima pristup računaru. Razlog je taj što se šifrovane lozinke ne mogu dešifrovati, pa se stoga ne moraju ni zaštititi. Ta teorija je pogrešna. Pomoću alatke `pwdump3`, koja se takođe može naći na Internetu, uspeo je da izvuče šifrovane lozinke sa računara ATM6.

Tipična datoteka šifrovanih lozinki izgleda ovako:

```
Administrator:500:95E4321A38AD8D6AB75E0C8D76954A50:2E48
927A0B04F3BFB341E26F6D6E9A97:::
akasper:1110:5A8D7E9E3C3954F642C5C736306CBFEF:393CE7F90
A8357F157873D72D0490821:::
digger:1111:5D15C0D58DD216C525AD3B83FA6627C7:17AD564144
308B42B8403D01AE256558:::
ellgan:1112:2017D4A5D8D1383EFF17365FAF1FFE89:07AEC950C2
2CBB9C2C734EB89320DB13:::
tabeck:1115:9F5890B3FECCAB7EAAD3B435B51404EE:1F0115A728
447212FC05E1D2D820B35B:::
vkantar:1116:81A6A5D035596E7DAAD3B435B51404EE:B933D36DD
12258946FCC7BD153F1CD6E:::
vwalwick:1119:25904EC665BA30F4449AF42E1054F192:15B2B795
3FB632907455D2706A432469:::
mmcdonald:1121:A4AED098D29A3217AAD3B435B51404EE:E40670F
936B79C2ED522F5ECA9398A27:::
kworkman:1141:C5C598AF45768635AAD3B4358B51404EE:DEC8E82
7A121273EF084CDBF5FD1925C:::
```

Na šifrovane lozinke koje je sada preneo na svoj računar, Ivan je primenio alatku koja drugačije pretražuje lozinke, tehnikom koja se zove *pogađanje lozinke na silu*. U takvom napadu isprobava se svaka kombinacija alfanumeričkih znakova i većine specijalnih simbola.

Ivan je upotrebio uslužni program `L0phtcrack3` (izgovara se kao *loft-krek*, a može se naći na lokaciji www.atstake.com; još jedan izvor odličnih alata za pogađanje lozinke je www.elcomsoft.com). Administratori sistema koriste `L0phtcrack3` da bi proverili postoje li suviše jednostavne lozinke, dok ga napadači upotrebljavaju da bi saznali lozinke. `LC3` isprobava lozinke pomoću kombinacije slova, brojeva i većine simbola, uključujući i `!@#%&^&`. On sistematski proverava svaku moguću kombinaciju većine znakova. (Međutim, imajte na umu da `LC3` neće moći da otkrije lozinku ako sadrži znakove koji se ne mogu odštampati.)

Program radi gotovo neverovatnom brzinom, koja može dostići i do 2,8 miliona pokušaja u sekundi na računaru s procesorom od 1 GHz. Čak i tom brzinom, pa i ako je administrator sistema ispravno podesio operativni sistem (onemogućivši upotrebu LANMAN šifrovanja), pogađanje lozinke može potrajati dosta dugo. Zbog toga napadač često preuzme šifrovane lozinke i pogađa ih na svom računaru, umesto da ostane na mrežnoj ciljnoj kompaniji i rizikuje da ga otkriju.

terminologija

POGAĐANJE LOZINKE NA SILU (engl. *brute force attack*) Tehnika za otkrivanje lozinke kojom se isprobava svaka moguća kombinacija alfanumeričkih znakova i specijalnih simbola.

Ivan nije morao da čeka tako dugo. Za nekoliko sati, program mu je poklonio lozinke svakog člana razvojnog tima. Ali to su bile lozinke korisnika s računara ATM6, a on je već znao da izvorni kôd igre koji traži nije na tom serveru.

Šta sad učiniti? Još uvek nije uspeo da pronađe lozinku za nalog na računaru ATM5. Posluživši se hakerskom logikom, budući da je znao loše navike tipičnih korisnika pretpostavio je da je neko od članova tima možda upotrebio istu lozinku za oba računara.

Upravo je to i otkrio. Jedan od članova tima koristio je istu lozinku i na računaru ATM5 i na računaru ATM6.

Ivanu su se vrata širom otvorila – mogao je da luta dok ne nađe željene programe. Kad je pronašao stablo s izvornim kodom i radosno ga preuzeo, preduzeo je još jedan korak tipičan za provalnike: promenio je lozinku jednog neupotrebljenog administratorskog naloga, za slučaj da jednom poželi da dođe do ažurirane verzije softvera.

Analiza prevare

U ovom napadu zloupotrebljeni su i tehnički propusti i ljudski činilac. Napadač je telefonskim pozivom saznao lokaciju i imena servera na kojima se nalaze skrivene informacije.

Potom je upotrebio uslužni program da bi odredio imena svih korisničkih naloga na razvojnom serveru. Zatim je na dva načina pokušao da pogodi lozinke, uključujući i napad rečnikom, pri kome se pogađaju često korišćene lozinke tako što isprobavaju sve reči u rečniku engleskog jezika, ponekad proširenom spiskovima imena, naziva mesta i drugih značajnih pojmova.

Budući da i besplatne i komercijalne hakerske alate mogu nabaviti svi, za koju god svrhu, još je važnije da budete na oprezu kad štitite računarske sisteme preduzeća i mrežnu infrastrukturu.

Nikada ne možete biti isuviše oprezni kad je ta pretnja u pitanju. Prema časopisu *ComputerWorld*, analiza bezbednosti u institutu Oppenheimer Funds u Njujorku dovela je do začuđujućeg otkrića. Potpredsednik firme za mrežnu bezbednost i oporavak sistema probao je da otkrije lozinke zaposlenih pomoću jednog standardnog softverskog paketa. Za tri minuta je pogodio lozinke 800 zaposlenih.

mitnikova poruka

Rečeno terminologijom igre Monopol, ako upotrebite neku reč iz rečnika kao svoju lozinku – idete pravo u Zatvor. Ne prolazite do polja Kreni, niti dobijate 200 dolara. Morate naučiti svoje zaposlene da izaberu lozinke koje će zaista zaštititi vašu imovinu.

SPREČAVANJE PREVARE

Obmane mogu postati još destruktivnije kad napadač doda tehnološki element. Za sprečavanje takvog napada moraju se zaštititi i tehnika i ljudi.

Jednostavno recite „ne“

U prvoj priči iz ovog poglavlja, službenica telefonske kompanije nije trebalo da aktivira dolazne pozive sa deset telefonskih linija bez naloga koji bi odobrio izmenu. Nije dovoljno da zaposleni *poznaju* bezbednosna pravila i procedure – oni moraju razumeti koliko su ta pravila važna da bi se predupredila šteta.

Bezbednosna pravila bi trebalo podržavati sistemom nagrada i posledica. Naravno, pravila moraju biti realna. Ako budu suviše teška, zaposleni će ih verovatno ignorisati. Takođe, programom za podizanje svesti o bezbednosti treba ubediti zaposlene da, iako je bitno završiti poslovne zadatke na vreme, moraju se ispoštovati odgovarajuće bezbednosne procedure. Zaobilaženje utvrđenih pravila može biti kobno po kompaniju i saradnike.

Sa istim takvim oprezom treba pristupiti kada se informacije daju nepoznatoj osobi preko telefona. Bez obzira na to koliko se ubedljivo osoba predstavi, i nezavisno od njegovog ili njenog statusa ili pozicije u kompaniji, apsolutno *nikakve* tajne informacije se ne smeju davati, sve dok se

ne potvrdi identitet sagovornika. Da su se ljudi strogo držali ovih pravila, prevara u ovoj priči ne bi uspjela, a zatvorenik Gondorf nikada ne bi uspeo da u istražnom zatvoru planira novu obmanu sa svojim prijateljem Džonijem.

Ovo je toliko bitno da stalno ponavljam kroz knjigu: proveravajte, proveravajte, proveravajte. Nikada ne treba prihvatati zahteve koji nisu podnesheni lično, bez prethodne provere identiteta podnosioca zahteva – i tačka.

Čišćenje

U svakoj kompaniji koja nema čuvaru 24 časa dnevno, sprečavanje ulaska u kancelarije nakon radnog vremena predstavlja pravi izazov. Čistači se uglavnom odnose s poštovanjem prema svakom ko izgleda kao pravi zaposleni. Najzad, to je neko ko bi ih mogao dovesti u neprilike ili otpustiti. Iz tog razloga, čistače, bez obzira na to da li su zaposleni ili rade po ugovoru s drugom agencijom, morate obučiti o bezbednosti.

Za posao čistača nije baš potrebno fakultetsko obrazovanje, a u uobičajenu obuku, ako je ima, uvrštena su pitanja o poslu, kao, na primer, koje se sredstvo za čišćenje koristi za različite zadatke. Ti ljudi najčešće ne dobijaju uputstva poput ovog: „Ako vas neko zamoli da ga pustite unutra nakon radnog vremena, treba da pogledate njihovu kompanijsku propusnicu, a potom da pozovete agenciju za čišćenje, objasnite situaciju i da sačekate njihovo odobrenje.“

Organizacija treba unapred da planira šta učiniti u takvoj situaciji, i da obučiti ljude na odgovarajući način. Lično sam otkrio da su mnoge, ako ne i sve firme iz privatnog sektora veoma ranjive u ovoj oblasti fizičkog obezbeđenja. Možete pokušati i da pristupite problemu iz drugog ugla, premeštajući breme na same zaposlene. U kompaniji u kojoj ne postoji dvadesetčetvoročasovno obezbeđenje, trebalo bi reći zaposlenima da moraju poneti sopstvene ključeve ili elektronske propusnice ako žele da uđu u kancelariju nakon radnog vremena. Čistači nikada ne smeju odlučivati ko sme da uđe unutra. Potom naložite čistačima da nikada ne primaju nikoga u vaše prostorije. To je jednostavno pravilo: nikada ne otvaraj vrata nikome. Ako je podesno, to se može i zapisati kao jedan od uslova ugovora s kompanijom za čišćenje.

Takođe, čistače valja obavestiti o tehnikama provlačenja (kada neovlašćena osoba prati ovlašćenu kroz obezbeđeni ulaz). Treba im i staviti do znanja da ne dopuste da druga osoba uđe za njima u zgradu samo zato što izgleda kao službenik.

Neka to bude praćeno povremenim (recimo tri ili četiri puta godišnje) insceniranjem probnog upada, ili proverom slabih tačaka obezbeđenja. Neka se neko pojavi na vratima dok čistači rade i pokuša da ih nagovori da ga puste u zgradu. Umesto da za to angažujete sopstvene radnike, unajmite firmu specijalizovanu za takve probe.

Prosledite poruku svima: zaštitite svoje lozinke

Organizacije sve više pokazuju oprez i primenjuju bezbednosna pravila u koja su uključene i tehničke mere; na primer, podešavaju operativni sistem tako da se moraju upotrebljavati lozinke, i ograničavaju broj neuspešnih pokušaja prijavljivanja pre zaključavanja naloga. U poslovne platforme Microsoft Windowsa uglavnom su ugrađene te funkcije. Poznato je da se korisnici lako iznerviraju zbog funkcija za koje je potreban dodatan napor, pa se proizvodi uglavnom isporučuju sa isključenim bezbednosnim opcijama. Zaista je krajnje vreme da proizvođači softvera prestanu da isporučuju proizvode u kojima su bezbednosne funkcije podrazumevano isključene, kad bi trebalo da bude suprotno. (Mislim da će uskoro to shvatiti.)

Naravno, u bezbednosnom pravilniku firme treba naložiti administratorima sistema da primenjuju tehničke mere obezbeđenja kad god je moguće, s ciljem da se ljudske greške ne tolerišu više nego što je neophodno. Činjenica je da, kada ograničite broj uzastopnih neuspešnih pokušaja prijavljivanja za rad na određenom nalogu, na primer, napadaču znatno zagorčavate život.

Svaka organizacija se susreće s problemom balansiranja između jakog obezbeđenja i produktivnosti zaposlenih, usled čega radnici ignorišu bezbednosna pravila, ne shvatajući koliko su te zaštitne mere važne za integritet osetljivih kompanijskih informacija.

Ako se iz kompanijskog pravilnika izostave neka pitanja, zaposleni će ići linijom manjeg otpora i raditi onako kako im je najjednostavnije. Neki zaposleni se odupiru promenama, pa će otvoreno prenebregavati dobru bezbednosnu politiku. Možda ste se već susreli s takvim radnikom, koji se pridržava nametnutih pravila o dužini i složenosti lozinke, a potom je zapiše na komadić papira i prkosno zakači za monitor.

Upotreba lozinki koje se teško mogu otkriti, u sprezi sa temeljnim tehnološkim podešavanjima radi obezbeđenja sistema, predstavlja osnovnu bezbednosnu meru.

Detaljne preporuke o lozinkama pronaći ćete u poglavlju 16.

.....●.....

poglavlje

12

Napadi na zaposlene u prijemnim odeljenjima

Kao što se videlo iz mnogih priča u ovoj knjizi, dobri prevaranti često ciljaju na osoblje na nižim nivoima u hijerarhijskoj lestvici organizacije. Ti se ljudi mogu ubediti tako da otkriju naizgled bezazlene informacije koje napadač kasnije upotrebi da bi se približio cilju.

Zaposleni u prijemnim odeljenjima obično nisu svesni vrednosti određenih kompanijskih informacija, niti mogućih posledica svojih postupaka. Takođe, na njih se često lako utiče uobičajenim metodama manipulacije – pozivanjem na autoritet, ljubaznim i simpatičnim predstavljanjem, pominjanjem imena zaposlenih kompanije koje i žrtva zna, insistiranjem da je zahtev hitan, ili navođenjem na to da će žrtva za svoju uslugu dobiti neku protivuslugu ili priznanje.

Evo primera napada na zaposlene na nižim nivoima.

LJUBAZNI ČUVAR

Prevaranti se nadaju da će naići na gramzivu osobu, jer je takve lakše prevariti. Kada im je meta čistač ili čuvar, oni se nadaju da će naići na dobrodušnu, ljubaznu i lakovernu osobu. Takvi ljudi najčešće žele da pomognu. Upravo to je napadač imao na umu u sledećoj priči.

Priča iz Eliotovog ugla

Vreme: 3:26, utorak ujutru, februara 1998.

Mesto: prostorije firme Merčand Majkrosistems, Našua, Nju Hempšir

Eliot Stenli je znao da ne sme da napušta svoje radno mesto osim kad ide u uobičajene obilaske. Ali bilo je gluvo doba noći, za ime boga, a on nije video nikoga od kad je došao na posao. U svakom slučaju, bližilo se vreme za obilazak. Čovek s kojim je razgovarao telefonom zvučao je kao da mu zaista treba pomoć, a svako se dobro oseća kad može nešto da učini za drugog.

Bilova priča

Bil Gudrok je imao jednostavan cilj i slepo ga se pridržavao još od svoje dvanaeste godine – da se penzioniše u dvadeset četvrtoj godini, a da ne upotrebi ni dolar iz svog fonda. A sve to da bi pokazao ocu, svemoćnom i nemilosrdnom bankaru, da može i sam uspeti u životu.

Ostalo mu je samo još dve godine, a postalo je savršeno jasno da se neće obogatiti u sledećih dvadeset četiri meseca čak ni ako radi kao sjajan ekonomista, ili pametno uloži novac. Jednom je razmišljao i o tome da opljačka banku pištoljem, ali to se dešava samo u filmovima – rizik da ga uhvate mnogo je veći od koristi. Sanjario je da ponovi Rifkinov podvig – da opljačka banku elektronskim putem.

Poslednji put kad je Bil bio u Evropi s porodicom, otvorio je bankovni račun u Monaku položivši 100 franaka. Na njemu je još uvek ista suma, ali on ima plan da je za kratko vreme izmeni u sedmocifren broj. Ako bude imao sreće, možda i u osmocifren.

Bilova devojka En radila je u odeljenju za marketing velike bostonske banke. Jednog dana, dok je u bančnim prostorijama čekao da En izađe s kasnog sastanka, podlegao je ljubopitljivosti i povezao je svoj prenosivi računar na Ethernet priključak sale za sastanke u kojoj se nalazio. Ušao je u njihovu unutrašnju mrežu, priključio se... iza zaštitne barijere. To mu je dalo ideju.

Udružio je svoj talenat sa školskim drugom koji je poznao izvesnu Džuliju. Ona je pripremala doktorat iz računarskih nauka i stažirala je u Merčandu. Činilo se da će Džulija biti odličan izvor najvažnijih unutrašnjih informacija. Kazali su joj da pišu scenario za film, a ona im je poverovala. Mislila je da je zabavno izmišljati priču s njima i dati im sve

pojediniosti o tome kako bi se zamišljena ludorija zaista mogla izvesti. Zapravo, smatrala je da je ideja izvanredna, i stalno ih je gnjavila da i nju potpišu kao scenaristu filma.

Upozorili su je na to da se ideje za scenario često krađu, pa su je naterali da se zakune da nikada nikome neće ispričati ovu ideju.

Bill, kojeg je podučavala Džulija, sam je izveo rizični deo plana, uopšte ne sumnjajući da će mu poći za rukom.



Pozvao sam poslepodne i saznao da je nadzornik noćnih čuvara izvesni Ajzea Adams. Pozvao sam u 9:30 te večeri. Javio mi se čuvar iz hola. Moja priča se zasnivala na užurbanosti, pa sam namerno zvučao pomalo uznemiren. „Imam problema s kolima, pa ne mogu da dođem do zgrade“, rekao. „Slučaj je hitan, i zaista mi je potrebna vaša pomoć. Pokušao sam da pozovem nadzornika, Ajzeu, ali nije kod kuće. Možete li mi učiniti uslugu, samo ovaj put? Bio bih vam veoma zahvalan.“

Prostorije u toj velikoj zgradi bile su obeležene šifrom, pa sam mu dao šifru računarske laboratorije i upitao ga da li zna gde se nalazi. Odgovorio je potvrdno i pristao da ode tamo. Rekao je da će mu trebati oko pet minuta, a ja sam odgovorio da ću ga ponovo pozvati u laboratoriji, pod izgovorom da imam samo jednu telefonsku liniju, a da mi ona treba da se uključim u mrežu kako bih rešio problem.

Već je bio tamo i čekao kad sam ga pozvao i rekao mu gde da nađe konzolu koja mi je bila potrebna, onu na kojoj se nalazi papirna nalepnica s oznakom „elmer“. Džulija mi je rekla da se taj računar koristi za sklapanje konačnih verzija operativnog sistema njihove kompanije. Kad je rekao da ga je našao, bio sam uveren da nam je Džulija davala prave informacije, a srce je počelo brže da mi lupa. Zamolio sam ga da pritisne taster Enter nekoliko puta, na šta je on rekao da se pojavljuje znak tarabice. Na osnovu toga sam zaključio da je za rad na računaru prijavljen administrator. Loše je kucao na tastaturi, pa ga je oblio znoj dok sam mu objašnjavao kako da unese moju sledeću naredbu, koja uopšte nije bila jednostavna:

```
echo 'fix:x:0:0:::/bin/sh' >> /etc/passwd
```

Konačno je uspeo, pa smo tako napravili nov korisnički nalog. Onda sam ga zamolio da unese:

```
echo 'fix::10300:0:0' >> /etc/shadow
```


Tako sam definisao šifrovanu lozinku, čije je mesto između dvostruke dve tačke. To što se između dva pomenuta znaka ne nalazi ništa znači da novi korisnik neće imati nikakvu lozinku. Dakle, te dve naredbe su bile dovoljne da se u datoteku s lozinkama doda nalog s praznom lozinkom. Što je najbolje, novi korisnik ima administratorska ovlašćenja.

Zatim sam ga zamolio da unese naredbu za izlistavanje direktorijuma koja štampa dugačak spisak imena datoteka. Potom sam mu rekao da malo povuče papir iz štampača, pocepa ga, i ponese do pulta za obezbeđenje „jer će možda biti potrebno da mi nešto pročita sa njega kasnije“.

U svemu tome bilo je izvanredno što on nije ni slutio da je napravio nov nalog. A zahtevao sam od njega da ispiše spisak imena datoteka jer sam se morao uveriti da će naredbe koje je prethodno uneo izaći iz računarske sobe zajedno s njim. Na taj način ni administrator sistema, ni operater neće sledećeg jutra primetiti ništa što bi ih moglo upozoriti na narušavanje bezbednosti sistema.

Sada sam imao nalog, lozinku i administratorska ovlašćenja. Malo pre ponoći sam se uključio u mrežu prateći uputstva koja je Džulija pažljivo otkucala „za scenario“. U tren oka sam pristupio jednom od razvojnih sistema u kojem se nalazio originalni primerak izvornog koda nove verzije operativnog sistema kompanije.

Poslao sam na mrežu *zакrpu* koju je Džulija napisala, za koju je rekla da menja rutinu jedne od biblioteka operativnog sistema. Ta *zакrpa* će, zapravo, napraviti *mala vrata* koja će omogućiti daljinski pristup pomoću tajne lozinke.

Pažljivo sam pratio uputstva koja mi je zapisala – prvo sam instalirao *zакrpu*, pa uklonio nov korisnički nalog i izbrisao zapise iz dnevnika događaja, tako da se uopšte ne vidi šta sam radio. Izbrisao sam svoje tragove.

napomena

Mala vrata koja se ovde koriste ne menjaju program za prijavljivanje na sistem. Umesto toga, zameni se određena funkcija u dinamičkoj biblioteci koju koristi program za prijavljivanje, i tako se stvori tajni ulaz. Obično računarski uljezi zamene ili *zакrpe* program za prijavljivanje, ali oštroumni administratori sistema mogu da otkriju promenu upoređivanjem sa originalnom verzijom programa, ili na druge načine.

Uskoro će kompanija početi da šalje novu verziju operativnog sistema svojim klijentima – finansijskim institucijama širom sveta. U svakoj kopiji koju isporuče nalaziće se mala vrata koja sam stavio u originalni primerak pre distribucije, što mi omogućava da pristupim svakom računarskom sistemu svake banke i posredničke kompanije koja instalira ažuriranu verziju.

terminologija

ZAKRPA Dodatni kôd koji ispravlja grešku u izvršnom programu.

Naravno, to nije bio kraj – trebalo je još dosta toga obaviti. I dalje sam morao da pristupim unutrašnjoj mreži svake finansijske institucije koju sam želeo da „posetim“. Zatim, valjalo je otkriti koji računar koriste za prenos novca, i instalirati softver za nadgledanje da bih saznao pojedinosti o njihovim procedurama i o tome kako se tačno novac prenosi.

Sve to se može uraditi daljinski, s računara koji se nalazi bilo gde u svetu. Recimo, tamo gde imam pogled na peščanu plažu. Tahiti, dolazim!

Ponovo sam pozvao čuvara, zahvalio mu se na pomoći, i rekao mu da sad može da baci odštampani materijal.

Analiza prevare

Čuvar je imao uputstva o dužnostima, ali ni temeljna, dobro osmišljena uputstva ne mogu da predvide sve moguće situacije. Niko mu nije predložio štetu koja se može naneti pritiskanjem nekoliko tastera računara na molbu osobe za koju misli da je zaposlena u kompaniji.

Uz čuvarovu saradnju, bilo je relativno lako pristupiti najbitnijem sistemu u kome se nalazio glavni primerak za distribuciju, uprkos tome što je bio iza zaključanih vrata bezbedne laboratorije. Čuvar, naravno, ima ključeve od svih zaključanih vrata.

Čak se i čestiti zaposleni (ili, u ovom slučaju, budući doktor nauka i stazista u preduzeću, Džulija) ponekad mogu podmititi ili obmanuti da otkriju izuzetno važne podatke – na primer, gde se nalazi određeni računarski sistem i, što je bilo ključno za uspeh ovog napada, kada će napraviti novu verziju softvera. To je važno jer, kad se takva izmena unese suviše rano, veće su šanse da će je otkriti ili poništiti, ako se operativni sistem bude ponovo proizvodio iz originalnog izvornog koda.

Jeste li zapazili da je čuvar odneo odštampani materijal sa sobom do pulta za obezbeđenje i kasnije ga uništio? To je bio važan korak. Napadač nije želeo da operateri nađu dokaze na terminalu za štampanje, niti da ih primete u korpi za otpatke, kada sledećeg radnog dana dođu na posao. Dajući čuvaru uverljiv izgovor da ponese odštampani materijal, izbegao je taj rizik.

mitnikova poruka

Kada uljez ne može fizički da priđe računarskom sistemu, niti mreži, pokušaće da navede drugu osobu da to učini umesto njega. U slučajevima gde je za izvršenje plana neophodan fizički pristup, bolje je iskoristiti žrtvu kao posrednika nego učiniti to sam, jer napadač tako preuzima mnogo manje rizika da će ga otkriti ili uhvatiti.

HITNA ZAKRPA

Pomislili biste da ljudi iz tehničke podrške shvataju potencijalnu opasnost ako se neznancu dozvoli pristup računarskoj mreži. Kada je taj uljez pame-tan i lažno se predstavlja kao ljubazni prodavac softvera, može se dogoditi neočekivano.

Ljubazan poziv

Osoba s druge strane žice želela je da zna ko je odgovoran za računare kod njih, pa ga je službenica na centrali spojila sa zaposlenim u tehničkoj podršci, Polom Ejhernom.

Sagovornik se predstavio: „Ovde Edvard iz firme Sirver, vašeg proizvođača baza podataka. Navodno mnogo naših kupaca nije primilo elektronsku poruku o hitnoj zakrpi, pa zato nasumično zovemo radi kontrole kvaliteta, da bismo proverili da li je bilo problema s instaliranjem zakrpe. Jeste li je već instalirali?“

Pol odvrati da je sasvim siguran da nije video ništa slično.

Edvard reče: „To bi moglo da prouzrokuje povremene katastrofalne gubitke podataka, pa vam preporučujemo da je instalirate što pre.“ „Da, to ću sigurno učiniti“, odgovori Pol. „U redu“, odvrati sagovornik, „možemo vam poslati traku ili CD sa zakrpom, i moram vam reći da je zaista izuzetno važno – dve kompanije su već izgubile podatke snimane tokom nekoliko

dana. Zato bi *zaista* trebalo to da instalirate čim stigne, pre nego što se isto dogodi i vašoj firmi.“

„Zar ne mogu da je preuzmem s vaše Web lokacije?“ upita Pol.

„Trebalo bi uskoro i na taj način da bude dostupna – naše tehničko osoblje se time bavi. Ako želite, naš centar za podršku korisnicima može vam je daljinski instalirati. Možemo to učiniti telefonskim uključenjem u vaš sistem, ili preko Telnet-a, ako ga podržavate.“

„Upotrebu Telnet-a ne dozvoljavamo, a naročito ne sa Interneta, jer nije bezbedan“, odgovori Pol. „Ako možete da koristite SSH, to bi bilo u redu“, reče, pomenuvši protokol za bezbedan prenos datoteka.

„Da. Imamo SSH. Koja vam je IP adresa?“

Pol mu je dao IP adresu, a kad ga je Edvard upitao: „Koje korisničko ime i lozinku da upotrebim?“, Pol mu je i to saopštio.

Analiza prevare

Naravno, taj poziv je mogao zaista uputiti proizvođač baze podataka. Ali u tom slučaju priči ne bi bilo mesta u ovoj knjizi.

Obmanjivač je uticao na žrtvu prouzrokujući osećaj straha od gubitka važnih podataka, i ponudivši trenutno rešenje koje bi otklonilo problem.

Kada napadač cilja na nekoga ko je svestan vrednosti informacija, mora smisliti veoma ubedljive i verodostojne argumente da bi dobio daljinski pristup. Ponekad mora odglumiti užurbanost, da bi žrtvi odvratio pažnju, te da bi sarađivala s njim pre nego što stigne da malo bolje razmisli o zahtevu.

NOVA SLUŽBENICA

Kakvim bi informacijama u dokumentima vaše kompanije napadač želeo da pristupi? Ponekad to može biti i nešto što smatrate da uopšte ne treba zaštititi.

Poziv za Saru

„Kadrovsko odeljenje, ovde Sara.“

„Zdravo, Sara. Ovde Džordž iz garaže. Znete onu propusnicu koju koristite da biste ušli u garažu i liftove? Imali smo problema, pa moramo da ponovo programiramo kartice svih službenika koji su primljeni u poslednjih petnaest dana.“

„Da li vam trebaju njihova imena?“

„I telefonski brojevi.“

„Mogu da proverim spisak novoprimljenih osoba i da vas pozovem. Koji je vaš broj?“

„Ja sam na 73... Ali idem na pauzu. Mogu li ja vas ponovo da nazovem za pola sata?“

„U redu.“

Kada je ponovo nazvao, rekla mu je:

„Pa, imamo samo dvoje. Ana Mirtl, u finansijama. Ona je sekretarica. I novi potpredsednik, gospodin Andervud.“

„A koji su njihovi lokali?“

„Telefonski broj gospodina Andervuda je 6973, a Ane Mirtl 2127.“

„Mnogo ste mi pomogli. Hvala.“

Poziv za Anu

„Finansije, Ana je kraj telefona.“

„Drago mi je da sam našao nekoga ko radi do kasno. Čujte, ovde Ron Vitaro. Ja radim u poslovnom odeljenju. Mislim da se nismo upoznali. Dobro došli u kompaniju.“

„O, hvala vam.“

„Ana, nalazim se u Los Anđelesu i imam hitan slučaj. Moram vam oduzeti deset minuta vremena.“

„Svakako. Šta vam je potrebno?“

„Idite u moju kancelariju. Znete li gde je?“

„Ne.“

„Dobro, to je kancelarija na uglu na petnaestom spratu – soba 1502. Pozvaću vas tamo za nekoliko minuta. Kada uđete u kancelariju, pritisnite dugme za prosleđivanje poziva na mom telefonu da se ne bi odmah uključila telefonska sekretarica kad pozovem.“

„U redu, krećem.“

Nakon deset minuta nalazila se u njegovoj kancelariji, isključila je funkciju prosleđivanja poziva na telefonu i čekala da pozvoni. Rekao joj je da sedne za računar i pokrene Internet Explorer. Kada se uključio, kazao joj je da unese adresu: www.geocities.com/ron_insen/rukopis.doc.exe.

Pojavio se okvir za dijalog, a on joj je rekao da pritisne dugme Open. Činilo se da je računar počeo da prima rukopis, a potom se na ekranu nije videlo ništa. Kad mu je javila da nešto izgleda ne valja, odgovorio je: „O, *ne*, ne ponovo. Često sam imao problema s preuzimanjem datoteka s te Web lokacije, ali mislio sam da je problem otklonjen. No, dobro, ne brinite, kasnije ću na drugi način doći do tog dokumenta.“ Onda ju je zamolio da ponovo pokrene računar, da bi se uverio da će se ispravno uključiti nakon problema koji joj se upravo dogodio. Objasnio joj je korak po korak kako da to uradi.

Kada se računar ponovo ispravno uključio, srdačno joj se zahvalio i spustio slušalicu. Ana se vratila u finansijsko odeljenje da završi posao na kojem je radila.

Priča Kurta Dilana

Urednici izdavačke kuće Milard-Fenton bili su oduševljeni autorkom s kojom tek što nisu potpisali ugovor. Bila je to penzionisana generalna direktorka jedne od najboljih 500 kompanija na svetu, prema procenama časopisa Fortune, koja je želela da ispriča fascinantnu priču. Angažovala je jednog poslovnog menadžera da pregovara s izdavačkom kućom umesto nje. Menadžer nije želeo da prizna da ne zna ništa o autorskim ugovorima, pa je unajmio starog prijatelja da mu pomogne. Taj prijatelj, nažalost, nije bio baš dobar izbor. Kurt Dilan se služio onim što bismo mogli nazvati neobičnim metodama istrage, odnosno metodama koje nisu u potpunosti etičke.

Kurt je dobio besplatan prostor na Web lokaciji Geocities, pod imenom Ron Vitari, i preneo je *špijunski softver* na nju. Promenio je ime programa u `rukopis.doc.exe`, da bi ime naizgled upućivalo na dokument u Wordu, i da ne bi izazivalo podozrenje. Zapravo, to je uspelo i bolje nego što je Kurt predviđao, jer pravi Vitari nikada nije promenio podrazumevane parametre Windowsa. Jedan od tih parametara je i: „Sakrij nastavke imena datoteka svih poznatih tipova dokumenata“. Zahvaljujući tom parametru, datoteka je bila prikazana pod imenom `rukopis.doc`.

Zatim je zamolio jednu prijateljicu da pozove Vitarovu sekretaricu. Dilan ju je uputio da kaže: „Ovde izvršni pomoćnik Pola Spadonea, predsednika lanca knjižara iz Toronta. Gospodin Vitaro je upoznao mog šefa na sajmu knjiga pre izvesnog vremena, i zamolio ga da pozove kako bi razmotrili moguć zajednički projekat. Gospodin Spadone je često na putu, pa me je zamolio da saznam kada će gospodin Vitaro biti u kancelariji.“

Kada su njih dvoje uporedili rasporede, prijateljica je imala dovoljno informacija da napadaču obezbedi spisak datuma kada će gospodin Vitaro biti u kancelariji. To je takođe značilo da je saznala i kada *neće* biti tamo. Prijateljica nije morala još mnogo da časka da bi došla do podatka da će Vitarova sekretarica iskoristiti njegovo odsustvo da ode na kratko skijanje. Oboje će biti odsutni nakratko. Savršeno.

Prvog dana kada je trebalo da budu odsutni, nazvao je pod izgovorom da mora hitno da razgovara s njima, samo da bi se uverio da nisu tu. Službenica prijemnog odeljenja ga je obavestila da „Gospodin Vitaro nije u kancelariji, kao ni njegova sekretarica. Ne očekujemo ih danas, niti sutra, a ni prekosutra.“

Njegov prvi pokušaj da na prevaru navede novog zaposlenog da učestvuje u njegovom planu bio je uspešan. Činilo se da ona nema baš ništa protiv toga da mu pomogne da preuzme „rukopis“, a to je zapravo bio popularan, javnosti dostupan špijunski program koji je napadač podesio tako da se *tajno instalira*. Na taj način, instalaciju neće otkriti nijedan antivirusni softver. Iz nepoznatih razloga, antivirusni softver ne otkriva javno dostupne špijunske programe.

terminologija

ŠPIJUNSKI PROGRAM (engl. *spyware*) Specijalizovan softver koji se koristi za tajno nadgledanje žrtvinog rada na računaru. Jedan njegov oblik se koristi za praćenje posećenih Web lokacija, da bi se reklame na Webu mogle prilagoditi navikama korisnika. Drugi oblik je identičan uređaju za prisluškivanje, samo što se prisluškuje računar. Softver nadgleda rad korisnika, uključujući lozinke, pritisnute tastere, elektronsku poštu, časkanje preko mreže, kratke poruke, sve posećene Web lokacije i snimke ekrana.

TAJNA INSTALACIJA (engl. *silent install*) Metoda instaliranja softverske aplikacije tako da korisnik računara ili operater nisu svesni instalacije.

Odmah nakon što je devojka preuzela program na Vitarov računar, Kurt je ponovo otišao na lokaciju Geocities i zamenio datoteku rukopisom knjige koji je našao na Internetu. U slučaju da neko otkrije prevaru i vrati se na pomenutu lokaciju da proveri o čemu je reč, samo bi našao bezazlen, amaterski rukopis knjige koja nije dovoljno dobra da bi bila objavljena.

Posle instaliranja i ponovnog pokretanja računara, špijunski program se automatski aktivirao. Ron Vitaro će se vratiti s puta za nekoliko dana, počće da radi, a špijunski program će prosleđivati svaki pritisak na tastere njegovog računara, kao i sve elektronske poruke koje šalje i snimke ekrana. Sve će se to slati u pravilnim vremenskim razmacima na lokaciju davaoca besplatnih usluga elektronske pošte u Ukrajini.

Nekoliko dana nakon Vitarovog povratka, Kurt je iščitavao dnevnike događaja koji su se nagomilavali u njegovom sandučetu za elektronsku poštu u Ukrajini, i ubrzo je pronašao poverljive poruke u kojima je naznačeno koliko izdavačka kuća Milard-Fenton želi da plati da bi sklopila ugovor s autorkom. Naoružana tim saznanjem, autorka je u pregovorima lako dobila mnogo bolje uslove nego što su joj isprva bili ponudeni, a da se nijednog trenutka nije upustila u rizik da dogovor propadne. To je, naravno, značilo da će ona dobijati veći procenat od prodaje.

Analiza prevare

U ovoj prevari, napadač je osigurao uspeh tako što je odabrao novog zaposlenog kao svog posrednika, računajući na to da će ona bolje sarađivati i želeti da bude timski igrač, te da je manje verovatno da poznaje kompaniju, ljude u njoj, i odgovarajuća bezbednosna pravila.

Budući da se u razgovoru s Anom, službenicom u finansijama, Kurt predstavio kao potpredsednik kompanije, znao je da verovatno neće posumnjati u njegov autoritet. Štaviše, možda će ona pomisliti da će imati nešto od toga što je potpredsedniku učinila uslugu.

Postupak instaliranja špijunskog programa nije delovao nimalo sumnjivo. Ana nije ni sanjala da će njeni, na prvi pogled bezazleni postupci pomoći napadaču da zadobije vredne informacije koje mogu naštetiti firmi.

Zašto je napadač odlučio da prosledi potpredsednikove poruke do naloga elektronske pošte u Ukrajini? Iz više razloga – napadača je teže pronaći i pokrenuti postupak protiv njega kada koristi udaljene lokacije. U zemlji kakva je Ukrajina takva krivična dela smatraju se manje bitnima. Tu

policija ima stav da krivično delo preko Interneta nije prestup vredan pažnje. Upravo je zato privlačno korišćenje lažnih adresa elektronske pošte u zemljama koje nerado sarađuju sa američkom kriminalističkom službom.

SPREČAVANJE PREVARE

Prevarant uvek radije odabere zaposlenog koji verovatno neće primetiti da je njegov zahtev sumnjiv. To mu olakšava posao, a i čini ga manje rizičnim – kao što se vidi iz priča u ovom poglavlju.

mitnikova poruka

Često se dešava da se saradnik ili podređeni zamoli za uslugu. Prevaranti znaju kako da iskoriste prirodnu želju ljudi da pomognu i budu timski igrači. Napadač iskorišćava tu pozitivnu ljudsku osobinu da bi naveo naivne zaposlene da mu pomognu u približavanju cilju. Važno je razumeti ovu jednostavnu ideju, da biste mogli lakše da prepoznate kada neko pokušava da vas prevari.

Obmanjivanje neopreznih

Ranije sam naglasio kako je neophodno temeljno obučiti zaposlene tako da ne dozvole da ih neznanac nagovori da izvrše njegova uputstva. Svi zaposleni takođe moraju shvatiti opasnosti od ispunjavanja zahteva koji obuhvata rad na tuđem računaru. To treba zabraniti kompanijskim pravilnikom osim kada pretpostavljeni izričito odobri. U situacije u kojima se to može dozvoliti spadaju:

- Kada vas lično zamoli osoba koju dobro poznajete, ili kada preko telefona bezrezervno prepoznate glas sagovornika.
- Kada zasigurno utvrdite identitet podnosioca zahteva putem odobrenih procedura.
- Kada vaše postupke odobri nadređeni ili druga osoba višeg ranga koja lično poznaje podnosioca zahteva.

Zaposleni se moraju obučiti da ne pružaju pomoć osobama koje ne poznaju lično, čak ni ako se podnosilac zahteva predstavi kao rukovodilac. Kada se odrede bezbednosna pravila u utvrđivanju identiteta osoba, rukovodstvo mora podržati zaposlene da ih se pridržavaju, čak i ako to znači da

će se zaposleni suprotstaviti članovima rukovodstva koji ih zamole da zao-
biđu bezbednosna pravila.

Svako preduzeće mora definisati pravila i postupke pomoću kojih će za-
posleni reagovati na zahteve u vezi s računarima ili opremom. U priči o izda-
vačkoj kući, napadač je odabrao novu radnicu koja nije bila obučena o
bezbednosnim pravilima i postupcima. Da bi se sprečio takav napad, svim
zaposlenima, i starim i novim, mora se objasniti da se pridržavaju jedno-
stavnog pravila: ne koristite računarski sistem da biste ispunili zahtev nepo-
znate osobe, i tačka.

Zapamtite da svaki zaposleni koji ima fizički ili elektronski pristup
računaru ili delu opreme u vezi s računarima može biti zloupotrebljen
tako da učini nešto što će ići u korist napadača.

Zaposleni, a pogotovo informatičko osoblje, moraju shvatiti da je omo-
gućavanje pristupa računarskoj mreži nepoznatoj osobi isto što i davanje
broja bankovnog računa agentu za prodaju preko telefona, ili broja kredit-
ne kartice neznancu u zatvoru. Radnici moraju obratiti pažnju na to da li
ispunjavanje zahteva može dovesti do otkrivanja osetljivih informacija, ili
ugrožavanja računarskog sistema kompanije.

Informatičari takođe moraju biti oprezni kad ih pozivaju nepoznati
sagovornici koji se izdaju za proizvođače računarskog hardvera i softvera. U
načelu, firma bi trebalo da odredi pojedince za kontaktiranje s proizvođa-
čima. Uz to, pravilnikom bi trebalo propisati da ostali zaposleni ne smeju
da odgovaraju na zahteve proizvođača koji traže neke podatke, ili žele da
izmene delove telefonske ili računarske opreme. Na taj način, pojedinci će
poznavati zaposlene proizvođača koji zovu telefonom ili dolaze u posetu, pa
će ih prevaranti teže obmanuti. Ako nazove proizvođač s kojim kompanija
nije sklopila ugovor o podršci, to bi takođe trebalo da bude sumnjivo.

Svi u organizaciji moraju postati svesni opasnosti koje prete informacija-
ma, i slabih tačaka u njihovom obezbeđenju. Imajte na umu da čuvari i
slično osoblje, pored fizičkog obezbeđenja, moraju pohađati i obuku iz bez-
bednosti *informacija*. S obzirom na to da čuvari često imaju fizički pristup
svim prostorijama u zgradi, moraju naučiti da prepoznaju obmanjivače.

Čuvajte se špijunskog softvera

Komercijalne špijunske programe uglavnom su koristili roditelji da bi
vodili računa o tome šta im deca rade na Internetu. Upotrebljavali su ga i
poslodavci, navodno da bi utvrdili koji se radnici zabavljaju krstareći po

Internetu. Ozbiljnije se primenljivao u otkrivanju potencijalne krađe informacionih dobara, ili u industrijskoj špijunaži. Proizvođači špijunskog softvera reklamiraju svoje proizvode kao sredstvo za zaštitu dece, ali njihovi pravi kupci su industrijski špijuni. U današnje vreme, prodaja špijunskog softvera je veoma porasla zahvaljujući tome što ljudi žele da znaju da li ih supružnik, ili druga draga osoba, vara.

Neposredno pre nego što sam počeo da pišem priču o špijunskom softveru za ovu knjigu, osoba koja umesto mene prima elektronsku poštu (jer meni nije dozvoljeno da koristim Internet) pronašla je u mom sandučetu neželjenu elektronsku poruku u kojoj se reklamira porodica proizvoda špijunskog softvera. Jedan od ponuđenih proizvoda opisan je ovako:

SVAČIJI OMILJENI PROGRAM! NE SMETE GA PROPUSTITI:

Ovaj moćan program za nadgledanje i špijuniranje tajno, u tekstualnu datoteku, snima podatke o svakom pritisnutom tasteru, kao i vreme i naziv svih otvorenih prozora, dok radi skriven u pozadini. Dnevni događaja se mogu šifrovati i automatski poslati elektronskom poštom, ili se mogu snimiti na čvrsti disk. Pristup programu je zaštićen lozinkom, i može se ukloniti iz liste poslova.

Upotrebite ga da biste nadgledali unete hiperveze, časkanje, elektronsku poštu, kao mnogo toga drugog (čak i lozinke ;-)).

Instalirajte ga neupadljivo na bilo koji PC računar i pošaljite dnevni događaja na svoju elektronsku adresu!!!!!!

Nedostatak antivirusnih programa

Antivirusni softver obično ne otkriva komercijalne špijunske programe, jer oni nisu definisani kao zlonamerni, bez obzira na to što im je cilj špijuniranje drugih ljudi. Tako računarska verzija prisluskiivača prolazi neprimećena, čime se stvara rizik da bi svako od nas bilo kada mogao nezakonito biti pod prismotrom. Naravno, proizvođači antivirusnog softvera mogu tvrditi da se špijunski softver može koristiti i u zakonite svrhe, pa ga zato ne treba smatrati zlonamernim. Ipak, određene alatke koje su nekad upotrebljavali samo hakeri, a danas se javno distribuiraju ili prodaju kao softver za bezbednost, smatraju se zlonamernim. Očigledno se radi o dvostrukim standardima, a ja se pitam zašto.

U istoj elektronskoj poruci reklamirao se još jedan proizvod koji navodno može da prenosi slike ekrana korisnikovog računara, baš kao da mu video kamera snima preko ramena. Za neke od tih softverskih proizvoda čak nije neophodno da fizički dođete do korisnikovog računara. Daljinski instalirajte i podesite aplikaciju, i dobićete trenutni računarski prislušivač! FBI mora da obožava tehnologiju.

Budući da je špijunski softver svima javno dostupan, vaše preduzeće se mora zaštititi na dva nivoa. Trebalo bi da instalirate softver za otkrivanje špijunskih programa, kao što je SpyCop (koji se može preuzeti s lokacije www.spycop.com), na sve radne stanice, i trebalo bi da zahtevate od svih zaposlenih da povremeno proveravaju računar. Pored toga, morate predložiti zaposlenima koliko je opasno ako ih neko na prevaru navede da preuzmu neki program s Interneta, ili otvore datoteku priloženu uz elektronsku poruku, iz koje bi se mogli instalirati zlonamerni softver.

Osim što bi valjalo sprečiti da se špijunski softver instalira za vreme pauze za kafu, ručka ili sastanka, pravilo u kom bi se zahtevalo da svi radnici zaključavaju svoje računare lozinkom čuvara ekrana ili nekom sličnom metodom značajno će umanjiti rizik da neovlašćena osoba pristupi nečijem računaru. Niko ko se uvuče u tuđu kancelariju neće moći da pristupi dokumentima, pročita elektronsku poštu, niti da instalira špijunski softver ili neki drugi. Čuvari ekrana se mogu uključiti bez dodatnih ulaganja, a korist od zaštite radnih stanica zaposlenih je velika. Računica u tim okolnostima je očigledna.



Dobro osmišljene prevare

dosad ste shvatili da, kada nepoznata osoba pozove telefonom, zahtevajući poverljive informacije ili nešto drugo što bi moglo biti korisno u eventualnom napadu, osoba koja primi poziv mora biti obučena da zapiše telefonski broj sagovornika. Zatim treba da pozove taj broj kako bi utvrdila da li je sagovornik zaista onaj za koga se izdaje – radnik iste firme, zaposlen kod poslovnog partnera, ili osoba iz tehničke podrške jednog od proizvođača računarske opreme, na primer.

Čak i kada kompanija uvede postupke kojih se zaposleni strogo pridržavaju da bi utvrdili identitet sagovornika, vrsni prevaranti će ipak uspeti da trikovima navedu žrtve da poveruju u njihov lažni identitet. Sledećim metodama mogu se obmanuti čak i radnici koji vode računa o bezbednosti.

NETAČNA IDENTIFIKACIJA POZIVA

Svako ko je ikada primio poziv na mobilni telefon, primetio je funkciju poznatu kao identifikacija poziva, kada se na ekranu prikaže telefonski broj pozivaoca. U poslovnom okruženju, ta funkcija nudi mogućnost da radnik na brzinu zaključi da li je poziv uputio drugi zaposleni iste firme, ili neko van nje.

Pre mnogo godina, ambiciozni telefonski prevaranti upoznali su čudesne mogućnosti identifikacije poziva, pre nego što je telefonskoj kompaniji bilo dopušteno da ponudi tu uslugu javnosti. Sjajno su se zabavljali

iznenađujući ljude tako što bi se javili na telefon i pozdravili sagovornika po imenu pre nego što bi ovaj rekao i reč.

I baš zato što mislite da je identitet sagovornika sigurno potvrđen, jer verujete svojim očima – onome što vidite na ekranu – upravo to napadač može pokušati da iskoristi.

Telefonski poziv za Lindu

Vreme: utorak, 23. juli, 15:12

Mesto: Kancelarije finansijskog odeljenja preduzeća Starbit

Telefon Linde Hil je zazvonio dok je pisala dopis za svog šefa. Pogledala je identifikator poziva, na kom je stajalo da poziv dolazi iz centrale u Nju-jorku. Uputio ga je izvesni Viktor Martin, čije ime joj nije bilo poznato.

Pomislila je da pusti da se uključi telefonska sekretarica, kako joj ne bi prekidali tok misli dok piše dopis. Ali ljubopitljivost je preovladala. Podigla je slušalicu, a osoba s druge strane žice se predstavila, i rekla da je iz odeljenja za odnose s javnošću, te da radi na nekom materijalu za generalnog direktora. „On je trenutno na putu za Boston, da se nađe s nekim našim bankarima. Potrebni su mu najsvežiji finansijski izveštaji za poslednji kvartal“, reče. „I još nešto. Potrebni su mu i finansijski predračuni za projekat Apač“, dodao je Viktor, upotrebivši interno ime za proizvod koji je u proleće trebalo da bude glavna novost na tržištu.

Zatražila mu je adresu elektronske pošte, ali on reče da ima problema s primanjem poruka, i da na tome radi tehnička podrška, pa ju je zamolio da mu sve pošalje faksom. Odgovorila je da nema problema, a on joj je dao interni telefonski lokal svog faksa.

Nakon nekoliko minuta poslala je faks.

Ali Viktor nije radio za odeljenje za odnose s javnošću. Zapravo, nije čak ni bio zaposlen u istoj firmi.

Džekova priča

Džek Dokins je još u detinjstvu započeo svoju profesionalnu karijeru kao džeparoš. Krao je na utakmicama na stadionu Jenkija, na prepunim stajalištima metroa, i noću u masi turista na Tajms skveru. Pokazalo se da je toliko spretan i lukav, da je mogao da skine nekom sat s ruke, a da to ovaj i ne primeti. Ali u pubertetu je postao nespretan, pa su ga uhvatili.

U popravnom domu za maloletnike izučio je nov zanat u kom je rizik da ga uhvate bio mnogo manji.

Njegov trenutni zadatak bio je da se domogne bilansa poslovanja Starbita za poslednji kvartal, kao i informacija o protoku sredstava, pre nego što se ti podaci dostave Berzanskoj komisiji i javno objave. Klijent je bio jedan zubar, koji nije želeo da objašnjava zašto su mu potrebne te informacije. Džeku se njegov oprez činio smešnim. I ranije se s tim susretao – verovatno je prokockao novac, ili ima zahtevnu ljubavnicu za koju njegova žena još uvek ne zna. Ili se možda samo hvalio pred ženom kako pametno ulaže na berzi; sada je izgubio pozamašnu sumu, pa želi da investira krupan ulog u nešto sigurno, tako što će saznati čije će cene berzanskih akcija skočiti kad se objave kvartalni rezultati.

Ljudi se iznenade kad vide koliko je malo vremena potrebno promišljenom prevarantu da smisli način na koji će pristupiti nepoznatoj situaciji. Kada je Džek stigao kući sa sastanka sa zubarom, već je osmislio plan. Njegov prijatelj Čarls Bejts je radio za firmu Panda Importing, koja ima privatnu telefonsku centralu (PBX).

Govoreći jezikom razumljivim onima koji poznaju telefonske sisteme, PBX je bio priključen na digitalnu telefonsku uslugu poznatu kao T1, koja je bila podešena kao PRI ISDN. To znači da su, prilikom svakog poziva iz prostorija preduzeća Panda, informacije o pozivu odlazile preko kanala podataka do centrale telefonske kompanije. U informacije je spadao i broj pozivaoca, koji stiže do uređaja za identifikaciju poziva osobe koja prima poziv (ukoliko ta funkcija nije isključena).

Džekov prijatelj je znao kako da programira centralu tako da osoba koja prima poziv vidi identifikator koji je on uneo, a ne broj kancelarije u firmi Panda. Taj trik uspeva jer se lokalne telefonske kompanije ne trude da provere da li identifikator pozivaoca odgovara telefonskom broju pretplatnika.

Džek Dokins je samo trebalo da pristupi takvoj telefonskoj usluzi. Na sreću, njegov prijatelj i nekadašnji partner u krađi, Čarls Bejts, uvek mu je rado pomagao, uz simboličnu nadoknadu. Ovog puta, Džek i Čarls su privremeno programirali telefonsku centralu tako da pozivi s određene linije u kancelarijama preduzeća Panda prenose identifikator broja Viktora Martina i izgledaju kao da dolaze iz preduzeća Starbit.

Činjenica da se identifikator poziva može podesiti tako da prikazuje bilo koji broj toliko je malo poznata, da se identifikator retko proverava. Linda je rado poslala faksom tražene informacije čoveku koji je navodno radio u odeljenju za odnose s javnošću.

Kada je Džek spustio slušalicu, Čarls je ponovo programirao telefonsku centralu, i vratio prvobitne parametre.

Analiza prevare

Neke kompanije ne žele da kupci ili prodavci znaju telefonske brojeve njihovih zaposlenih. Na primer, osoblje iz Fordovog centra za podršku kupcima moglo bi odlučiti da identifikator poziva prikazuje besplatan broj centra i natpis kao što je „Fordova podrška“, umesto stvarnog direktnog telefonskog broja službenika. Microsoft bi svojim zaposlenima mogao da ponudi da sami kažu svoj telefonski broj kome hoće, umesto da svako koga pozovu sazna njihov lokal pogledavši na identifikator poziva. Na taj način, kompanija može da obezbedi poverljivost internih brojeva.

Ispostavilo se da je ta ista mogućnost reprogramiranja zgodna za šaljivdžije, poverioce, agente prodaje preko telefona i, naravno, za prevarante.

VARIJACIJA NA TEMU: NA TELEFONU JE PREDSEDNIK SJEDINJENIH DRŽAVA

Bio sam voditelj radio-emisije „Tamna strana Interneta“ na radio-stanici KFI Talk Radio u Los Angelesu. Pretpostavljeni mi je bio direktor programa stanice, Dejvid, jedan od najprilježnijih i najmarljivijih ljudi koje sam ikada upoznao, pa ga je bilo veoma teško dobiti telefonom jer je stalno zauzet. On se ne javlja na telefon ukoliko na identifikatoru poziva ne vidi da ga zove neko s kim zaista treba da razgovara.

Kada bih ga ja nazvao, nije mogao da razazna ko ga zove, jer sam blokirao identifikaciju poziva na svom mobilnom telefonu. Ne bi se javio, uključila bi se telefonska sekretarica, a to je za mene postalo veoma neprijatno.

Razgovarao sam sa dugogodišnjim prijateljem koji je suvlasnik agencije za prodaju nekretnina o tome šta da učinim. Zajedno smo smislili plan. On je imao pristup telefonskoj centrali Meridian svoje kompanije, pa je mogao da programira telefonski broj pozivaoca, kao što je već opisano u prethodnoj priči. Kad god je trebalo da razgovaram s direktorom programa, a nije se javljao na moj poziv, zamolio bih prijatelja da podesi centralu tako da se pojavi identifikator koji ja izaberem. Ponekad bih ga zamolio da podesi centralu tako da izgleda kao da je poziv uputio Dejvidov pomoćnik, a ponekad holding preduzeće koje poseduje stanicu.

Omiljeni trik mi je bio da programiramo razvodnik tako da se čini da je poziv upućen s Dejvidovog kućnog telefona, na šta bi se uvek javio. Ipak, skidam mu kapu. Uvek bi se našalio kad bi podigao slušalicu i shvatio da sam ga ponovo prevario. Najbolje od svega je bilo to što bi potom razgovarao sa mnom dovoljno dugo da bih mogao da mu saopštim šta mi treba, i da bi rešio problem koji imam.

Kad sam demonstrirao ovaj mali trik u emisiji Arta Bela, našalio sam se tako da se na mom identifikatoru poziva pojavio naziv i broj glavnog štaba losandeleskog Federalnog istražnog biroa. Art je zbog toga bio zatečen i prekoreo me je što činim nezakonite radnje. Otkrio sam mu da je to potpuno legalno, sve dok nije pokušaj obmane. Nakon programa, primio sam nekoliko stotina elektronskih poruka u kojima su me ljudi pitali da im objasnim kako sam to učinio. Sad znate.

To je savršen alat kojim prevaranti grade sebi verodostojnost. Ako, na primer, u pripremnoj fazi napada prevarant otkrije da se žrtva oslanja na identifikator poziva, napadač bi mogao da kamuflira sopstveni broj kao da pripada proverenoj kompaniji ili poverljivom zaposlenom. Poverioci mogu da postignu da njihov poziv naizgled dolazi iz vaše firme.

Razmislite malo o posledicama. Neko ko želi da provali u računarski sistem mogao bi vas pozvati kući tvrdeći da je iz informatičkog odeljenja vaše kompanije. Osobi s druge strane žice hitno je potrebna vaša lozinka da bi povratila vaša dokumenta nakon pada servera. Ili se na identifikatoru poziva pojave ime i broj vaše banke ili posredničke kuće, a devojka zavodljivog glasa samo treba da proveri vaš broj računa i majčino devojačko prezime. Pored toga, takođe mora da proveri i PIN kôd vaše kartice zbog nekog problema u sistemu. Berzanski mešetari mogli bi da postignu da njihovi pozivi naizgled dolaze iz kompanija Merrill Lynch ili Citibank. Neko ko želi da se domogne vaših identifikacionih podataka mogao bi, navodno, da pozove iz firme Visa, i ubedi vas da mu kažete broj svoje Visa kartice. Osoba koja je kivna na nekoga mogla bi da pozove i predstavi se da je iz poreske službe ili Federalnog istražnog biroa.

Ako imate pristup telefonskom sistemu povezanom na PRI, kao i programersko znanje, uz neke podatke koje možete dobiti na Web lokaciji proizvođača sistema, ovom tehnikom izvodićete sjajne trikove sa svojim prijateljima. Zna li nekoga ko ima prevelike političke ambicije? Mogli biste da programirate referentni broj Bele kuće.

Pomisliće da ga zove američki predsednik!

Pouka priče je jednostavna: identifikatoru poziva se ne može verovati, osim kad se koristi za identifikaciju internih poziva. Kako na poslu, tako i kod kuće, svako mora biti svestan trikova sa identifikatorima poziva i shvatiti da se ime i telefonski broj na ekranu ne smeju upotrebljavati kao sredstvo utvrđivanja identiteta.

mitnikova poruka

Sledeći put kada vas neko pozove, a na identifikatoru poziva vam se pojavi broj drage mame, nikad se ne zna – možda vas ipak zove običan prevarant.

220

Deo 3: Uzbuna zbog uljeza

NEVIDLJIVI ZAPOSLENI

Širli Katlas je pronašla nov i uzbudljiv način da brzo zaradi novac. Više neće morati mukotrpno da radi u „rudniku“. Priključila se stotinama drugih varalica koje se bave najisplativijim kriminalom decenije. Ona je kradljivac identiteta.

Danas je odlučila da pokuša da se domogne poverljivih informacija iz odeljenja za korisničku uslugu kompanije koja izdaje kreditne kartice. Nakon uobičajene pripreme, nazvala je ciljnu kompaniju i rekla operateru na centrali da je spoji s odeljenjem za telekomunikacije. Kad ih je dobila, zatražila je da razgovara s administratorom glasovne pošte.

Koristeći pripremljene podatke, predstavila se kao Norma Tod, zaposlena u njihovom ogranku u Klivlendu. Primenivši trik koji bi dosad trebalo da vam je poznat, rekla mu je da putuje u centralu firme na nedelju dana, pa će joj biti potrebno da tamo prima glasovne poruke, da ne bi morala da proverava poruke međugradskim pozivima. „Ne treba fizički instalirati telefonsku liniju“, kaže ona, „nego samo otvoriti sandučće za glasovnu poštu.“ Rekao je da će se pobrinuti za to, i da će joj se javiti kad bude sve podesio, da bi joj dao potrebne informacije.

Ona na to odvrti, zavodljivim glasom: „Pošla sam na sastanak. Mogu li ja vas da pozovem za sat vremena?“

Kad se ponovo javila, obavestio ju je da je sve spremno, i dao joj podatke – broj lokala i privremenu lozinku. Upitao ju je da li zna kako da promeni lozinku glasovne pošte, a ona mu je dopustila da joj objasni sve korake, iako ih je poznavala u najmanju ruku isto tako dobro kao on.

„Uzgred budi rečeno“, upita ona, „koji broj treba da zovem iz hotela da bih proveravala poruke?“ On joj izdiktira broj.

Širli okrene taj broj, promeni lozinku, i snimi svoj novi pozdrav.

Širli u akciji

Zasad je sve bila laka priprema. Sada je spremna da primeni umetnost obmane.

Poziva odeljenje za korisničku uslugu. „Radim u naplatnom odeljenju u Klivlendu“, kaže, a potom primeni varijaciju dosad poznatog izgovora. „Moj računar trenutno popravlja tehnička podrška. Molim vas, pošaljite mi sledeće informacije.“ Pročitala je ime i datum rođenja osobe čije identifikacione podatke želi da ukrade i navela koji joj podaci trebaju: adresa, majčino devojačko prezime, broj kartice, ograničenje kredita, odobreni kredit i istorijat plaćanja. „Nazovite me na ovaj broj“, kaže ona, dajući im interni lokal koji joj je administrator glasovne pošte podesio. „Ako nisam tu, ostavite podatke u glasovnoj poruci.“

Oblavljala je druge stvari do kraja prepodneva, a potom proverila poruke tog poslepodneva. Sve je tu, sve što je tražila. Pre nego što je spustila slušalicu, Širli je izbrisala svoj pozdrav na glasovnoj pošti; bilo bi neoprezno da ostavi snimak svog glasa.

Uskoro će još jedna osoba postati žrtva krađe identiteta, najpopularnijeg krivičnog dela novog veka. Širli je upotrebila informacije o kreditnoj kartici i lične podatke koje je upravo dobila i počela da troši novac sa žrtvine kartice.

Analiza prevare

Širli je prvo navela administratora glasovne pošte da poveruje u njen identitet i da privremeno aktivira uslugu. Da se potrudio da proveri ko je, saznao bi da ime i telefonski broj koji mu je dala odgovaraju navedenim podacima u kompanijskoj bazi podataka o zaposlenima.

Nakon toga, jednostavno je navela realan izgovor o tome kako ima problema s računarom, zatražila je željene informacije, i zamolila da joj se odgovor ostavi u glasovnoj poruci. Zašto bilo koji zaposleni ne bi želeo da podeli informacije s kolegom? Budući da je telefonski broj koji je Širli dala očigledno bio interni lokal, nije bilo razloga za sumnju.

Pokušajte s vremena na vreme sami sebi da ostavite glasovnu poruku; ako čujete pozdrav koji niste vi snimili, možda ste upravo naišli na prvog prevaranta.

LJUBAZNA SEKRETARICA

Haker Robert Džordej je redovno provaljivao u računarske mreže globalne kompanije, Rudolfo Šiping. U firmi su konačno primetili da neko stalno neovlašćeno pristupa njihovom serveru terminala, i da se pomoću tog servera korisnik mogao povezati s bilo kojim računarskim sistemom u kompaniji. Da bi obezbedili mrežu, u firmi su odlučili da postave lozinku na svakom serveru terminala za pristupanje putem telefonske veze.

Robert je pozvao Mrežni centar predstavljajući se kao advokat u pravnom odeljenju, i rekao da ima problema s povezivanjem na mrežu. Administrator mreže je objasnio da je u poslednje vreme bilo bezbednosnih problema, pa svi korisnici treba da traže lozinku za taj mesec od svog pretpostavljenog. Robert se pitao na koji način se rukovodstvu šalju mesečne lozinke i kako bi ih se mogao domoći. Kako se ispostavilo, odgovor je bio da se lozinke za sledeći mesec šalju dopisom preko interne pošte svakom rukovodiocu kompanije.

To mu je olakšalo posao. Robert se malo pripremao i nazvao kompaniju nedugo nakon prvog dana u mesecu. Javila mu se sekretarica jednog od rukovodilaca, koja se predstavila kao Dženet. On reče: „Zdravo, Dženet. Ovde Rendi Goldstin, iz razvoja. Znam da sam verovatno dobio dopis s novom mesečnom lozinkom za daljinski pristup serveru terminala, ali nigde ne mogu da ga nađem. Jeste li vi dobili dopis ovog meseca?“

Potvrdila je.

Zamolio ju je da mu ga faksom pošalje, a ona je pristala. Dao joj je broj faksa službenice prijemnog odeljenja u holu druge zgrade u okviru firme, gde se već dogovorio da se faksovi za njega čuvaju, pa će potom organizovati da se faks s lozinkom prosledi dalje. Međutim, ovog puta je Robert primenio drugačiju metodu prosleđivanja faksa. Dao je službenici prijemnog odeljenja broj faks usluge na Internetu. Kada na taj broj stigne faks, sistem ga automatski prosledi do korisnikove adrese elektronske pošte.

Nova lozinka je stigla do lažne adrese elektronske pošte koju je Robert otvorio na besplatnoj lokaciji u Kini. Ako se faksu ikada uđe u trag, bio je siguran da će se istražitelj hvatati za glavu, pokušavajući da sarađuje s kineskim vlastima, koje, znao je, dosta nevoljno pomažu u ovakvim stvarima. Što je najbolje, nikada nije morao fizički da se pojavi da bi ga preuzeo.

mitnikova poruka

Vešti prevaranti pametno navode druge ljude da im učine uslugu. Primiti faks i proslediti ga čini se tako bezazlenim, da je sasvim lako ubediti službenicu prijemnog odeljenja ili nekog drugog da to učini. Kad vas neko zamoli za uslugu u vezi sa informacijama, ako ga ne poznajete i ne možete da utvrdite njegov identitet, odbijte ga.

223

Poglavlje 13: Dobro osmišljene prevare

PREKRŠAJNI SUD

Verovatno je svako ko je ikada bio kažnjen zbog brze vožnje sanjao o tome da pronade načina da izbegne kaznu. Ne tako što će pohađati kurs vožnje, niti što će platiti, ili pokušati da ubedi sudiju u neku tehničku grešku, na primer, koliko dugo niko nije proverio brzinometar ili radar. Ne, najbolji scenario bi bio izbeći kaznu nadmudrivanjem sistema.

Prevara

Iako vam ne bih preporučio da na ovaj način pokušate da izbegnete saobraćajnu kaznu (kao što se kaže, ne pokušavajte ovo kod kuće) ipak, to je dobar primer kako umetnost obmane može biti od pomoći prevarantima.

Nazvaću momka koji je napravio prekršaj Pol Duria.

Prvi korak

„Losanđeleska policija, odsek Holenbek.“

„Dobar dan, želeo bih da razgovaram s nekim iz odeljenja za uručivanje sudskih poziva.“

„Ja sam zadužen za to.“

„Dobro. Ovde advokat Leri Parker iz kancelarije Mičam, Mičam i Talbot. Hteo bih da uručim poziv za suđenje jednom policajcu u vezi sa slučajem na kom radim.“

„U redu, kome?“

„Radi li u vašem odseku policajac Kendal?“

„Koji mu je serijski broj?“

„21349.“

„Da. Kada vam je potreban?“

„Sledećeg meseca, ali moram da uručim pozive i drugim svedocima, pa tek potom da saopštim sudu koji nam dani odgovoraju. Kada će policajac Kendal biti odsutan sledećeg meseca?“

„Da vidimo... Na odmoru je od 20. do 23., a obuku ima 8. i 16.“

„Hvala vam. To je sve što mi je trenutno potrebno. Pozvaću vas ponovo kad budem znao datum suđenja.“

Opštinski sud, prijemno odeljenje

Pol: „Hteo bih da zakažem suđenje u vezi s ovim saobraćajnim prekršajem.“

Službenik: „U redu. Slobodan je 26. sledećeg meseca.“

„Želeo bih da ugovorim saslušanje.“

„Saslušanje o saobraćajnom prekršaju?“

„Tako je.“

„Dobro. Možemo ugovoriti saslušanje za sutra ujutru ili poslepodne. Šta vam više odgovara?“

„Poslepodne.“

„Saslušanje će biti sutra u 13:30 u sudnici broj šest.“

„Hvala. Biću tamo.“

Opštinski sud, sudnica broj šest

Vreme: četvrtak, 13:45

Službenik: „Gospodine Duria, molim vas pristupite sudiji.“

Sudija: „Gospodine Duria, jeste li razumeli prava koja sam vam objasnio danas poslepodne?“

Pol: „Da, gospodine sudijo.“

Sudija: „Želite li da iskoristite priliku da pohađate kurs vožnje? Vaš slučaj će biti zaključen nakon uspešnog pohađanja osmočasovnog kursa. Proverio sam vaš dosije, i vidim da ste podobni za to.“

Pol: „Ne, gospodine sudijo. S dužnim poštovanjem, molio bih vas da se slučaj iznese na suđenje. Još nešto, gospodine sudijo. Putovaću u inostranstvo, ali mogu da budem tu 8. ili 9. Možete li da mi zakažete suđenje jednog od tih dana? Sutra odlazim na poslovno putovanje u Evropu, a vraćam se za četiri nedelje.“

Sudija: „U redu. Suđenje se zakazuje za 8. jun u 8:30, u sudnici broj četiri.“

Pol: „Hvala vam, gospodine sudijo.“

Opštinski sud, sudnica broj četiri

Pol je stigao u zgradu suda rano 8. juna. Kada je sudija ušao, službenik mu je dao spisak slučajeva za koje se policajci nisu pojavili. Sudija je pozvao optužene, uključujući Pola, i rekao im da se postupci protiv njih obustavljaju.

Analiza prevare

Kada policajac napiše prijavu, potpiše je i napiše svoj serijski broj (taj broj ima različite nazive u različitim službama), uopšte nije teško pronaći njegovu stanicu. Za početak je dovoljno pozvati službu za informacije o telefonskim brojevima, dajući im ime policijske službe u zaglavlju priznanice (patrola auto-puta, kancelarija okružnog šerifa, ili tome slično). Kad pozovete policijsku službu, mogu vam dati telefonski broj odgovarajućeg službenika zaduženog za sudske pozive.

Policajci redovno primaju sudske pozive; to je deo posla. Kada okružni javni pravobranilac ili advokat optuženog želi da pozove policajca da svedoči, ako zna kako sistem funkcioniše, on prvo proveriti da li će biti slobodan tog dana. To je lako; treba samo pozvati službenika zaduženog za sudske pozive u toj stanici.

Obično tokom takvog razgovora advokat pita službenika da li će dotični policajac biti slobodan određenog datuma. U ovoj prevari, Pol je morao biti taktičan; morao je da ponudi verovatan razlog zbog kog bi mu službenik rekao kada policajac neće moći da se pojavi.

Kada je Pol prvi put ušao u zgradu suda, zašto nije rekao sudskom službeniku koji datum želi? Odgovor na to je lako dati – koliko ja znam, službenici prekršajnog suda uglavnom ne dozvoljavaju običnim građanima da biraju datume suđenja. Ako datum koji službenik predloži ne odgovara, ponudiće jednu ili dve opcije, ali dalje neće ići. S druge strane, svako ko je voljan da potroši nešto više vremena i pojavi se na saslušanju, verovatno će biti bolje sreće.

Pol je znao da ima prava da traži saslušanje. Znao je i da su sudije često voljne da odobre zahtev za određeni datum. Pažljivo je odabrao datume koji se poklapaju s obukom policajca, znajući da u njegovoj državi obuka ima prednost u odnosu na pojavljivanje na prekršajnom sudu.

mitnikova poruka

Ljudski um je sjajan. Zanimljivo je koliko ljudi mogu biti maštoviti kada planiraju nečasne metode pomoću kojih će doći do nečega što žele ili se izvući iz nezgodne situacije. Morate primeniti istu takvu kreativnost i maštovitost da biste obezbedili informacije i računarske sisteme. Dakle, kada planirate bezbednosna pravila, budite kreativni i otvoreni.

Na prekršajnom sudu, kada se policajac ne pojavi – postupak se obustavlja. Ne plaća se kazna. Ne pohađa se kurs vožnje, niti se dobijaju kazneni poeni. A što je najbolje, prekršaj se ne beleži u dosije!

Pretpostavljam da će neki policajci, sudski službenici, okružni pravobranioци i njima slični negodovati kad pročitaju ovu priču, jer znaju da takve prevare zaista uspeavaju. Ali negodovaće uzalud. Ništa se neće promeniti. Mogao bih se kladiti u to. Kao što kaže Kozmo, junak filma *Pri-slušivači* iz 1992. godine: „Radi se samo o jedinicama i nulama.“ To znači da se na kraju sve svodi na informacije.

Sve dok u policijskim stanicama budu praktično svakome ko pozove davali informacije o terminima kad su im kolege zauzete, mogućnost da se neko izvuče od prekršajne kazne uvek će postojati. Imate li vi sličnih propusta u procedurama kompanije ili organizacije, koje bi pametan prevarant mogao da iskoristi da bi dobio informacije koje biste radije čuvali u tajnosti?

SAMANTINA OSVETA

Samanta Gregson je bila ljuta.

Naporno je učila i radila da bi dobila diplomu više poslovne škole, i uzela je čitavu gomilu studentskih kredita da bi to postigla. Uvek su joj govorili da se pomoću diplome dolazi do prave karijere, a ne do običnog posla; da se tako zarađuje velik novac. Diplomirala je i nigde nije mogla da nađe pristojan posao.

Bilo joj je drago kad je dobila ponudu od firme Lembek. Naravno, bilo je ponižavajuće prihvatiti sekretarski posao, ali je gospodin Kartrajt rekao da im je jako potrebna, te da će je na poziciji sekretarice lako uočiti kada se ukaže prilika za neki drugi posao.

Dva meseca kasnije, čula je da jedan od Kartrajtovih nižih direktora proizvodnje odlazi. Te noći je jedva spavala, zamišljajući sebe na petom spratu, u sopstvenoj kancelariji, kako odlazi na sastanke i donosi odluke.

Sledećeg jutra odmah je otišla da razgovara s gospodinom Kartrajtom. Rekao je da smatra da treba još da uči o proizvodnji pre nego što bude spremna za takvu poziciju. Potom su zaposlili amatera koji prethodno nije radio u kompaniji, i koji je o proizvodnji znao još manje od nje.

Tad je počela da shvata: u kompaniji je bilo zaposleno dosta žena, ali su gotovo sve bile sekretarice. Neće joj dati posao rukovodioca. Nikad.

Samanta uzvraća udarac

Trebalo joj je gotovo nedelju dana da isplanira osvetu. Pre mesec dana momak iz nekog časopisa pokušao je da joj se nabaci kad je došao na promociju novog proizvoda. Nekoliko nedelja kasnije nazvao ju je na posao i zamolio je da mu pošalje unapred neke podatke o proizvodu Kobra 273, poslao joj je cveće i rekao da će doći iz Čikaga specijalno da bi je izveo na večeru, ako mu pošalje zaista sveže informacije za časopis.

Nedugo nakon toga, nalazila se u kancelariji mladog gospodina Johansona dok se on povezivao na kompanijsku mrežu. Bez razmišljanja je posmatrala njegove prste (to se ponekad zove i *gledanje preko ramena*). Uneo je lozinku „marty63“.

Počela je da osmišljava plan. Prisetila se jednog dopisa koji je otkucala nedugo nakon što je počela da radi u firmi. Našla je kopiju među dokumentima i napravila novu verziju, koristeći fraze iz originala. U njenoj verziji je stajalo:

PRIMA: C. Pelton, Informatičko odeljenje

ŠALJE: L. Kartrajt, Razvoj

Martin Johanson će raditi u timu za specijalne projekte u mom odeljenju.

Ovim putem ga ovlašćujem da dobije pristup serverima koje koristi inženjerski tim. Bezbednosni profil gospodina Johanson treba ažurirati tako da dobije ista prava pristupa kao i inženjeri koji rade na razvoju proizvoda.

Luis Kartrajt

terminologija

GLEĐANJE PREKO RAMENA (engl. *shoulder surfing*) Posmatranje kako druga osoba kuca na tastaturi svog računara, da bi se došlo do njene lozinke ili drugih korisničkih informacija.

Kada su gotovo svi otišli na ručak, isekla je potpis gospodina Kartrajta sa originalnog dopisa, zalepila ga na sopstvenu verziju, i stavila malo belila na ivice. Fotokopirala ga je, a potom napravila kopiju kopije. Ivice oko potpisa bile su jedva primetne.

Poslala je faks sa mašine blizu kancelarije gospodina Kartrajta.

Tri dana kasnije, ostala je da radi duže i čekala da svi odu. Ušla je u Johansonovu kancelariju i pokušala da se poveže na mrežu pomoću njegovog korisničkog imena i lozinke, marty63. Uspela je.

Za nekoliko minuta pronašla je datoteke sa specifikacijama za Kobru 273, i snimila ih na Zip disk.

Disk je stavila na sigurno, u svoju tašnu, a onda se odšetala do parkinga po prijatnom večernjem povetarcu. Iste večeri će ga poslati novinaru.

Analiza prevare

Sve što je potrebno je nezadovoljan radnik, pretraživanje datoteka, seckanje, lepljenje i beljenje na brzinu, malo kreativnog kopiranja, slanje faksom, i eto! Uspela je da dođe do poverljivih reklamnih specifikacija proizvoda.

Nekoliko dana kasnije, novinar iz specijalizovanog časopisa prvi je izveštio o specifikacijama i marketinškim planovima sasvim novog proizvoda, i to mesecima pre nego što je proizvod pušten u prodaju. Konkurentske

firme su imale nekoliko meseci prednosti da razviju slične proizvode i pripreme reklamne kampanje tako da podriju uspeh Kobre 273.

Naravno, časopis nikada neće otkriti svoj izvor.

SPREČAVANJE PREVARE

Kada zaposlenima neko zatraži vredne, osetljive ili bitne informacije koje bi mogle biti korisne konkurenciji ili drugim firmama, oni moraju biti svesni da identifikator pozivaoca ne sme da se koristi za utvrđivanje identiteta osobe koja zove izvan preduzeća. Moraju se upotrebiti drugi načini identifikacije. Na primer, valja pitati pretpostavljenog da li je zahtev opravdan i da li je korisnik ovlašćen da primi informacije.

Za postupak identifikacije potrebna je ravnoteža bezbednosti i produktivnosti koju svaka kompanija mora definisati za sebe. Da li će bezbednosne mere imati prednost? Da li će se zaposleni nerado povinovati bezbednosnim pravilima, pa će ih čak zaobilaziti da bi ispunili zahteve svog posla? Da li radnici shvataju zašto je bezbednost važna za firmu i njihov same? Na ta pitanja valja odgovoriti da bi se napravio bezbednosni pravilnik zasnovan na preovlađujućem mišljenju i potrebama poslovanja.

Većina ljudi neizbežno smatra uznemiravanjem sve što se kosi sa samim poslom, pa mogu zaobilaziti mere obezbeđenja koje se čine gubljenjem vremena. Ključno je motivisati radnike da uključe bezbednosna pitanja u svakodnevne odgovornosti.

Iako se identifikator pozivaoca nikada ne sme koristiti kao sredstvo provere identiteta osoba koje zovu van firme, sme se primenjivati druga metoda koja se zove automatska identifikacija broja (engl. *automatic number identification, ANI*). Ta usluga pouzdano identifikuje pozivaoca. Nasuprot identifikatoru pozivaoca, centrala telefonske kompanije u ovoj usluzi ne koristi informacije koje šalje pretplatnik. ANI prikazuje pretplatni broj pozivaoca.

Imajte na umu da je nekoliko proizvođača modema svojim proizvodima dodalo funkciju identifikacije poziva. Mrežu preduzeća možete zaštititi dozvoljavanjem daljinskih poziva samo sa spiska unapred odobrenih brojeva. Modemi sa identifikacijom poziva su prihvatljivo sredstvo provere u okruženju u kom nije potrebno jako obezbeđenje, ali, kao što bi dosad trebalo da bude jasno, računarski hakeri relativno lako mogu da zamene identifikatore poziva, pa se zato na njih ne treba ozbiljno oslanjati.

Rešenje problema upotrebe tuđeg identiteta, kao u priči u kojoj je žena obmanula administratora da joj instalira glasovnu poštu u kompanijskom telefonskom sistemu, jednostavno je. Nametnite pravilo da se sve telefonske usluge, sva glasovna pošta i svaki unos podataka u firmin telefonski imenik, kako u štampanom obliku, tako i na mreži, moraju zatražiti napismeno, na namenskom obrascu. Zahtev treba da potpiše pretpostavljeni, a administrator glasovnih poruka bi trebalo da proveri potpis.

U bezbednosnom pravilniku valjalo bi zahtevati da se novi računarski nalozi ili proširenja prava pristupa dodeljuju tek nakon što se proveri podnosilac zahteva. To se može učiniti tako što se pozove rukovodilac ili administrator sistema, odnosno njegov ili njen zamenik. Ako firma koristi zaštićen sistem elektronske pošte, pa zaposleni mogu digitalno da potpisuju poruke, može se koristiti i ta metoda provere.

Upamtite da svaki zaposleni, imao ili nemaao pristup računarskim sistemima kompanije, može biti meta prevaranata. Svi moraju biti uključeni u obuku o bezbednosti. Sekretarice, službenici prijemnih odeljenja, telefonski operateri i čuvari moraju se upoznati s vrstama mogućih napada, da bi se bolje pripremili za odbranu.



Industrijska špijunaža

Opšte je poznato da državnim institucijama, kompanijama i univerzitetima preta opasnost od krađe informacija. Gotovo svakog dana u medijima se piše o novim računarskim virusima, uskraćivanju usluga ili krađi podataka o kreditnim karticama s komercijalnih Web lokacija.

Čitamo o slučajevima industrijske špijunaže, kao kad je Borland optužio Symantec da je ukrao njihove poslovne tajne, ili kad je firma Cadence Design Systems tužila konkurenta za krađu izvornog koda. Mnogi poslovni ljudi čitaju ove priče i misle da se to u njihovoj kompaniji nikada ne bi moglo desiti.

Događa se svakog dana.

VARIJACIJA NA TEMU

Prevara opisana u sledećoj priči je verovatno mnogo puta uspevala, bez obzira na to što zvuči kao scenario nekog holivudskog filma ili roman Džona Grišama.

Grupna tužba

Zamislite da je pokrenuta ogromna grupna parnica protiv velike farmaceutske kompanije. U optužbi se tvrdi da su znali da jedan njihov lek ima ozbiljna neželjena dejstva, koja izlaze na videlo posle dugogodišnjeg korišćenja.

Navodi se da su imali rezultate nekoliko istraživačkih studija koje su upozorile na pomenutu opasnost, ali da su zataškali dokaze i nikada ih nisu predali državnoj komisiji za lekove.

Vilijam (Bili) Čejni, cenjeni advokat na čelu njujorške advokatske kancelarije koja je pokrenula grupnu parnicu, ima pismene izjave dva lekara koji podržavaju optužbu. Obojica su u penziji, nijedan ne raspolaže dokumentacijom, i nijedan ne bi bio dobar i ubedljiv svedok. Bili zna da stvari ne stoje baš najbolje. Ukoliko ne bude uspeo da se domogne kopije jednog izveštaja, ili nekog internog dopisa ili beleške koji su razmenili rukovodioci firme, slučaj će propasti.

Zato je najmilio privatne istražitelje čije je usluge koristio i ranije – firmu Andreson. Bili ne zna kako Pit i njegovi ljudi dolaze do potrebnih podataka, i ne želi da zna. Bitno je samo da je Pit Andreson dobar istražitelj.

Andreson ovakve zadatke zove poslići na crno. Prvo pravilo je da advokatske kancelarije i firme koje ga unajmljuju nikada ne smeju saznati kako dolazi do informacija da bi uvek mogli u potpunosti sve da demantuju, a da im ljudi poveruju. Ako će se neko opeći, biće to Pit, a on smatra da su nadoknade koje dobija za velike poslove vredne rizika. Osim toga, on lično uživa u nadmudrivanju ljudi.

Ako dokumenti koje Čejni želi da pronade zaista postoje i nisu uništeni, biće da su negde u dokumentaciji farmaceutske kompanije. Naći ih u ogromnoj dokumentaciji velike firme, bio bi težak zadatak. S druge strane, šta ako su dali kopije tih dokumenata svojim advokatima, Dženkinsu i Petriju? Ako advokati optuženih znaju da ti dokumenti postoje, a nisu ih predali sudu kao deo istražiteljskog postupka, narušili su etičke kanone svoje profesije i prekršili zakon. Zato Pit smatra da je bilo kakav napad na informacije moralan.

Pitov napad

Pit je naložio svojim ljudima da započnu istragu i za nekoliko dana je saznao koju kompaniju Dženkins i Petri koriste za čuvanje rezervnih kopija podataka. Znao je da takve kompanije imaju spiskove imena osoba koje je advokatska kancelarija ovlastila da preuzimaju trake iz skladišta. Takođe je znao da svaka od tih osoba ima svoju lozinku. Pit je poslao dva svoja čoveka da obave poslić na crno.

Njih dvojica su obili bravu pomoću pištolja za obijanje kupljenog sa Web lokacije www.southord.com. Iza 3 sata po ponoći, za samo nekoliko minuta, ušunjali su se u kancelarije kompanije za čuvanje rezervnih kopija i pokrenuli su PC računar. Nasmešili su se kada su videli logotip Windowsa 98, jer je to značilo da će posao biti sasvim lak. Za korišćenje Windowsa 98 nisu potrebna nikakva ovlašćenja. Tragajući za dokumentima, pronašli su bazu podataka u Microsoft Accessu sa imenima ovlašćenih osoba. Dodali su izmišljeno ime spisku ovlašćenih osoba za advokatsku kancelariju Dženkins i Petri. Jedan od te dvojice je već imao odgovarajuću lažnu vozačku dozvolu. Da li su mogli provaliti u zaključano skladište i potražiti trake koje klijentu trebaju? Svakako, ali onda bi svi klijenti firme, uključujući i advokatsku kancelariju, zasigurno bili obavješteni o upadu u prostorije. Napadači bi izgubili prednost: profesionalci uvek vole da ostave otvor za pristupe u budućnosti, ako se za to ukaže potreba.

Prateći standardnu proceduru industrijskih špijuna da sačuvaju nešto što će im možda kasnije zatrebati, za svaki slučaj su na disketu snimili kopiju datoteke sa spiskom ovlašćenih osoba. Nijedan nije znao kako bi im to moglo koristiti, ali nisu hteli da propuste priliku kad su već tu. S vremena na vreme se ispostavi da su takve stvari vredne.

Jedan od te dvojice sutradan je nazvao kompaniju za izradu rezervnih kopija, predstavio se imenom koje su dodali spisku ovlašćenih osoba, i izgovorio odgovarajuću lozinku. Zatražio je sve trake advokatske kancelarije Dženkins i Petri iz poslednjeg meseca, i kazao da će kurir doći po paket. Do poslepodneva Andreson je imao trake. Njegovi ljudi su učitali sve podatke u sopstveni računarski sistem, da bi ih na miru pretražili. Andreson je bio veoma zadovoljan što advokatska kancelarija, poput mnogih drugih preduzeća, nije vodila računa o šifrovanju podataka na rezervnim kopijama.

Trake su sutradan vraćene kompaniji koja ih čuva, i niko nije znao šta se dogodilo.

Analiza prevare

S obzirom na to da je fizičko obezbeđenje bilo slabo, loši momci su lako obili bravu firme za čuvanje rezervnih kopija, pristupili računaru i izmenili bazu podataka sa spiskom ovlašćenih osoba. Prevaranti su dodali ime spisku pa su došli do traka sa rezervnim kopijama računarskih podataka, i nisu morali da provale u skladište firme. Budući da većina kompanija ne šifrira podatke, do informacija su došli lako.

Vredne informacije valja zaštititi, bez obzira na to u kom se obliku nalaze i gde su smeštene. Spisak klijenata neke firme ima istu vrednost, bilo da je odštampan ili je u elektronskoj datoteci u kancelariji ili u skladištu. Prevaranti uvek biraju najslabije mesto za napad, ono koje se najlakše može zaobići. Smatra se da je napad na skladište u kome se čuvaju rezervne kopije podataka manje rizičan, te da se teže može otkriti. Svaka organizacija koja čuva vredne, osetljive, ili veoma važne podatke van preduzeća trebalo bi da ih šifrira radi zaštite.

Ovaj incident je još jedan primer toga kako kompanija koja ne preduzme dovoljne mere bezbednosti može olakšati napadaču da ugrozi vredne informacije njihovih klijenata.

NOVI POSLOVNI PARTNER

Obmanjivači imaju prednost nad običnim kradljivcima i varalicama, jer rade na daljinu. Obični kradljivci vas mogu prevariti samo lično, iz blizine, što vam omogućava da ih kasnije dobro opišete, ili čak da pozovete policiju ako na vreme primetite prevaru.

Obmanjivači izbegavaju taj rizik poput kuge. Ponekad je rizik neopodan, i opravdan, kada se uzme u obzir nagrada.

Džesikina priča

Džesika Andover se osećala sjajno jer je dobila posao u dobrostojećoj kompaniji koja se bavi robotikom. Naravno, bio je to tek početak i nisu mogli da joj plate mnogo, ali firma je mala, ljudi ljubazni, a bila je uzbudljiva pomisao da bi joj cene akcija mogle porasti i učiniti je bogatom. Možda ne milionerom kao osnivače kompanije, ali dovoljno bogatom.

Zbog toga je Rik Dagot dobio širok osmeh kada je tog avgustovskog utorka ujutru ušao u hol. Pojavio se u skupom odelu (Armanijevom), s velikim zlatnim satom na ruci (marke Rolex President), i besprekornom frizurom. Izgledao je kao samouveren muškarac kojeg su obožavale sve devojke u srednjoj školi.

„Zdravo“, reče. „Ja sam Rik Dagot i došao sam na sastanak s Lerijem.“

Džesika se uozbiljila. „S Lerijem?“ upita. „Leri je na odmoru cele nedelje.“

„Imam zakazan sastanak s njim u jedan. Upravo sam doleteo iz Lujvila zbog toga“, reče Rik. Izvadio je ručni računar, uključio ga i pokazao joj raspored.

Pogledala ga je i blago odmahнула glavom. „Dvadesetog“, reče. „To je sledeće nedelje.“ Uzeo joj je ručni računar i netremice zurio u njega. „O, ne!“ zakuka. „Ne mogu da verujem kakvu sam glupu grešku napravio.“

„Mogu li bar da vam rezervišem povratnu kartu?“ upita ona, sažaljevujući ga.

Dok je telefonirala, Rik joj se poverio da će on i Leri organizovati savez za strateški marketing. Rikova firma izrađuje delove za proizvodne i montažne trake, koji bi savršeno nadopunjavali njihov nov proizvod, C2Alfa. Rikovi proizvodi i C2Alfa će zajedno predstavljati moćno rešenje koje će otvoriti značajna industrijska tržišta obema kompanijama.

Kada mu je Džesika rezervisala let kasnim poslepodnevnim letom, Rik reče: „Pa, bar bih mogao da razgovaram sa Stivom ako je tu.“ Ali ni Stiv, potpredsednik kompanije i jedan od njenih osnivača, nije bio tu.

Rik, koji je bio ljubazan prema Džesiki i pomalo joj se udvarao, potom je predložio da bi, kad je već tu, a kući putuje tek kasno poslepodne, mogao da izvede neke od važnih ljudi na ručak. Dodao je: „Uključujući i vas, naravno – može li neko da vas zameni u vreme ručka?“

Pocrvenela je kad je čula da poziva i nju, i upitala ga: „Koga želite da izvedete?“ Ponovo je kucnuo po svom ručnom računar i naveo imena nekoliko ljudi – dvojice inženjera iz razvoja, novog zaposlenog u prodajnom i marketinškom odeljenju i momka iz finansija dodeljenog njihovom projektu. Rik je predložio da im ona objasni ko je Rik, i kako je povezan s firmom i da naglasi da bi rado upoznao svu četvoricu. Naveo je najbolji restoran u okolini, u koji je Džesika oduvek želela da ode, kazao da će sam rezervisati sto za 12:30, da će je pozvati i potvrditi dogovor.

Kada su se okupili u restoranu – njih četvorica i Džesika – sto im još nije bio spreman, pa su se smestili za šankom, a Rik im je stavio do znanja da on plaća piće i ručak. Rik je imao stila. U njegovom prisustvu ste se od samog početka osećali prijatno, baš kao sa nekim koga znate godinama. Činilo se da uvek zna šta treba da kaže, ubacio bi veselu opasku ili nešto smešno kad bi razgovor utihnuo, pa ste se dobro osećali samo zato što ste u njegovom prisustvu.

Rekao im je tek toliko detalja o proizvodima svoje kompanije da bi sebi predočili zajedničko marketinško rešenje za koje je bio toliko zagrejan.

Naveo je nekoliko kompanija koje je časopis Fortune svrstao među 500 najboljih u svetu, i rekao da njima već isporučuje proizvode, sve dok svi za stolom nisu počeli da zamišljaju kako će njihov proizvod postići velik uspeh čim prvi primerci izađu iz fabrike.

Potom je Rik nasamo porazgovarao sa inženjerom Brajanom. Izvukao je iz njega jedinstvene osobine proizvoda C2Alfa, kao i ono što ga je izdvajalo od konkurencije. Saznao je za nekoliko osobina proizvoda koje firma namerno nije isticala, a na koje je Brajan bio ponosan, i smatrao je da su zaista „zgodne“.

Rik je sa svakim ponaosob tiho popričao. Čovek iz marketinga je drage volje pričao o datumu promocije i marketinškim planovima. Taj prilježni momak je izvukao kovertu iz džepa i na njoj zapisao pojedinosti materijala i cenu proizvodnje, finalnu cenu i očekivani profit, kao i planirane pogodbe s svakim proizvođačem ponaosob, a naveo ih je poimence.

Kad im je sto bio spreman, Rik je već porazgovarao sa svakim i svi ređom su mu se divili. Kad su završili ručak, svi su se rukovali s njim i zahvalili mu se. Rik je sa svakim razmenio posetnice i usput pomenuo Brajanu, inženjeru, da želi sa njim detaljnije da razgovara kada se Leri vrati.

Kada je Brajan sutradan podigao telefonsku slušalicu, prepoznao je glas. Rik reče da je upravo razgovarao s Lerijem. „Vratiću se u ponedeljak da završim rad na nekim specifikacijama s njim“. „Želi da imam sve naj-svežije informacije o vašim proizvodima. Poručio je da mu elektronskom poštom pošalješ najnovije planove i specifikacije, a on će izdvojiti delove koje želi da ja pogledam i proslediće mi ih.“

Inženjer je odgovorio da nema problema. „Dobro“, odvrati Rik. Nastavio je: „Leri ti poručuje da ne može da čita elektronsku poštu. Organizovao je da mu poslovni centar hotela otvori nalog za elektronsku poštu na lokaciji Yahoo. Kaže da mu pošalješ datoteke na adresu larryrobotics@yahoo.com umesto na njegov uobičajen nalog.“

Sledećeg ponedeljka ujutru, kada je Leri ušao u kancelariju pocrneo i vidno opušten, Džesika je želela odmah da mu ispriča sve o Riku. „Kakav sjajan momak. Izveo je na ručak četvoricu službenika i mene.“ Leri je izgledao zbunjen. „Rik? Ko je, do đavola, Rik?“

„O čemu vi to pričate? Vaš nov poslovni partner.“

„Šta!!!!?“

„Sve su zadivila prava pitanja koja je postavljao.“

„Ne poznajem nijednog Rika...“

„Šta vam je? Je li ovo neka šala, Leri – samo se šalite sa mnom, zar ne?“

„Pozovite rukovodstvo u salu za sastanke. *Odmah!* Bez obzira na to šta rade. I sve koji su bili na tom ručku. Dodite i vi.“

Sedeli su za stolom neraspoloženi, jedva progovarajući. Leri je ušao, seo i saopštio: „Ne poznajem nikoga po imenu Rik. Nemam novog poslovnog partnera koga sam tajio od svih vas. Mislim da je to očigledno. Ako se neko od vas našalio na tuđ račun, neka se *odmah* javi.“

Ni glasa ni od koga. Činilo se da je sala tonula u tamu iz trena u tren.

Konačno Brajan reče: „Zašto niste ništa rekli kad sam vam poslao onu elektronsku poruku sa specifikacijama proizvoda i izvornim kodom?“

„*Koju* poruku!“

Brajan se ukočio. „O, ne!“

Klif, drugi inženjer, ubacio mu se u reč. „Svima je dao svoje posetnice. Samo treba da ga pozovemo i vidimo šta se dešava.“

Brajan je izvadio svoj ručni računar, otvorio okvir za dijalog, i gurnuo uređaj preko stola do Lerijsa. I dalje se nadajući u toj beznadežnoj situaciji, svi su gledali kao opčinjeni dok je Leri unosio brojeve telefona. Nakon nekoliko trenutaka, pritisnuo je dugme za zvučnik i svi su mogli da čuju da je veza zauzeta. Pošto je dvadeset minuta okretao broj, kivni Leri je pozvao operatera da ga zamoli za hitan prekid veze.

Nešto kasnije, operater se ponovo javio. Reče mu ispitivački: „Gospodine, odakle vam ovaj broj?“ Leri odgovori da ga je pročitao sa posetnice čoveka s kojim hitno mora da razgovara. Operator reče: „Žao mi je. To je probni broj telefonske kompanije. Uvek daje zauzeće.“

Leri je počeo da sastavlja spisak informacija koje je Rik saznao. Rezultati nisu bili sjajni.

Došla su dva policijska detektiva da naprave izveštaj. Nakon što su saslušali njihovu priču, objasnili su im da prema državnom zakonu nije počinjeno nikakvo krivično delo, te da ne mogu ništa da učine. Savetovali su Lerijsu da stupi u vezu s FBI-jem jer su oni nadležni za sva poslovna krivična dela u svim državama. Kada je Rik Dagot zamolio inženjera da mu prosledi probne rezultate lažno mu se predstavivši, možda je prekršio savezni zakon, ali bi to samo FBI mogao da utvrdi.

Tri meseca kasnije, Leri je sedeo u kuhinji i čitao jutarnje novine uz doručak. Skoro je prosuo kafu! Ono čega se pribojavao još od kad je čuo za Rika obistinilo se – bila je to njegova najgora noćna mora. Bilo je tu, crno na belo, na naslovnoj strani poslovne rubrike: kompanija za koju nikada

nije čuo najavila je promociju novog proizvoda koji je izgledao potpuno isto kao C2Alfa na kome je njegov tim radio prethodne dve godine.

Putem obmane, ti ljudi su ga pretekli na tržištu. Njegov san je uništen. Milioni dolara uloženi u istraživanje i razvoj bili su uzalud potrošeni. A verovatno neće moći ništa da dokaže protiv njih.

Priča Semija Senforda

Semi Senford je uspeo u životu, kada se uzme u obzir da je bio dovoljno pametan da zaradi veliku platu na zakonitom radnom mestu, ali i dovoljno nepošten da je radije izabrao život prevaranta. Vremenom ga je primetio špijun koji je bio primoran da se rano penzionise zbog alkoholizma. Ogorčen i osvetoljubiv, pronašao je način da upotrebi svoj talenat koji je usavršio radeći za državu. Stalno je promatrao ljude tražeći one koji bi mu mogli biti od koristi, pa je tako primetio Semija. Semiju je bilo lako, i veoma isplativo, da se usredsredi na krađu poslovnih tajni, umesto novca.



Mnogi ne bi imali petlje da učine ono što ja radim. Pokušajte da ćaskate s ljudima preko telefona ili Interneta – tu vas niko ne vidi. Svaki dobar prevarant starog kova, koji se sa žrtvom susreće licem u lice (a takvih još ima veoma mnogo, više nego što biste poverovali), može vas gledati u oči, ispričati vam koještarije, i navesti vas da mu poverujete. Poznajem nekoliko tužilaca koji smatraju da je to zločin. Ja mislim da je u pitanju talenat.

Ne možete se tek tako ušetati; prvo morate sve isplanirati. Ulični prevaranti mogu da ocene čoveka tokom kratkog ljubaznog razgovora... Postave nekoliko pažljivo formulisanih pitanja i ako dobiju prave odgovore – pogodak! Ulovili su vas!

Kad je reč o preduzećima, to zovemo velikim prevarama. Morate se prvo pripremiti. Valja pronaći šta im je najbitnije, šta žele, i šta im je potrebno. Isplanirajte napad. Budite strpljivi, pripremite se. Osmislite ulogu koju ćete odigrati i naučite tekst. Nemojte se pojaviti dok ne budete spremni.

Proveo sam više od tri nedelje pripremajući ovu prevaru. Klijent me je dva dana obučavao šta da kažem – čime se „moja“ firma bavi, i kako da objasnim zašto će to biti tako dobar zajednički marketinški savez.

Onda mi se posrećilo. Nazvao sam kompaniju i predstavio se kao službenik investitorske firme koja želi da ugovori sastanak. Pokušavao sam da organizujem sastanak u vreme kada će svi naši partneri biti slobodni u sledećih nekoliko meseci, pa sam pitao da li postoji neko vreme koje bi trebalo izbegavati, na primer kada Leri nije tu. Sekretarica je potvrdno odgovorila, rekavši da nije uzimao slobodno u poslednje dve godine od kada su osnovali kompaniju, ali da ga supruga u prvoj nedelji avgusta vodi na odmor na kom će igrati golf.

To je bilo za samo dve nedelje. Mogao sam toliko da sačekam.

U međuvremenu, iz jednog poslovnog časopisa saznao sam ime kompanije za odnose s javnošću pomenutog preduzeća. Kazao sam im da mi se dopada koliko se u novinama pominje njihov klijent iz oblasti robotike, pa želim da razgovaram sa osobom zaduženom za njih, da bi vodila marketinšku kampanju i mog preduzeća. Ispostavilo se da je u pitanju energična mlada dama kojoj se dopalo to što će možda pridobiti još jednog klijenta. Za skupim ručkom, nakon čašice više, svojski se trudila da me ubedi da oni izuzetno dobro razumeju probleme klijenata i pronalaze odgovarajuća rešenja za odnose s javnošću. Pretvarao sam se da me je teško ubediti. Bili su mi potrebni detalji. Uz malo podsticanja, ispričala mi je o novom proizvodu i problemima firme više nego što sam se mogao nadati, i to pre nego što su sklonili tanjire sa stola.

Sve se odvijalo po planu. Službenica prijemnog odeljenja u potpunosti je poverovala u priču o tome koliko mi je neprijatno što je sastanak *sledeće* nedelje, ali da bih ipak mogao da se sastanem s timom, kad sam već tu. Čak me je i sažaljevala. Ručak me je koštao čitavih 150 dolara, plus napojnica, ali dobio sam šta sam želeo – telefonske brojeve i pozicije. Čak sam pridobio i ključnog čoveka koji je poverovao u moj lažni identitet.

Priznajem, Brajan me je prevario. Činilo se da je osoba koja će mi poslati sve što mu tražim. Zvučao je malo suzdržano kad sam poveo razgovor o tome. Isplati se biti spreman na sve. Taj nalog za elektronsku poštu na Lerijevo ime čuvao sam za svaki slučaj. Policija verovatno i sad čeka da neko ponovo upotrebi taj nalog, pa da ga uhvate. Dosta će se načekati. Ja sam svoje završio. Prelazim na drugi projekat.

Analiza prevare

Svako ko se bavi prevarama u kojima se fizički pojavljuje, mora da se maskira tako da ga žrtva lakše prihvati. Obući će se na jedan način da bi se pojavio na hipodromu, na drugi da bi se ušao u lokalni kafić, a na treći da bi otišao u otmeni bar luksuznog hotela.

Isto je i u industrijskoj špijunaži. Za napad može biti potrebno odelo, kravata i skupa aktovka, ako se špijun lažno predstavlja kao rukovodilac dobrostojeće firme, savetnik, ili prodavac. Kada se prevarant izdaje za softverskog inženjera, tehničara, ili nekoga iz sobe za poštu, odeća, uniforma – zapravo čitav njegov izgled – biće drugačiji.

Da bi se uvukao u firmu, čovek koji se lažno predstavio kao Rik Dagot znao je da mora odati utisak samouverenog i sposobnog čoveka, koji dobro poznaje proizvod i industriju te kompanije.

Nije bilo teško domoći se potrebnih informacija. Osmislio je jednostavnu varku da bi otkrio kada će generalni direktor biti odsutan. Pomalo izazovno, ali i dalje ne veoma teško, bilo je saznati dovoljno pojedinosti o projektu kako bi mogao da zvuči kao da se razume u ono što rade. Često takve podatke znaju razni dobavljači firme, kao i investitori od kojih su pokušali da dobiju sredstva, banke i njihova advokatska kancelarija. Međutim, napadač mora biti oprezan: pronaći nekoga ko će vam odati interne tajne može biti teško, ali ako na nekoliko mesta pokušate da nađete osobu iz koje možete iscediti informacije, rizikujete da će neko shvatiti šta smerate. To može biti opasno. Ljudi slični Riku Dagotu moraju birati pažljivo i upotrebljavati svaki izvor informacija samo jednom.

Ručak je bio još jedan nesiguran predlog. Prvo se postavio problem organizacije. Kako bi mogao da provede po nekoliko minuta nasamo sa svakim a da drugi ne čuju? Džesiki je rekao da je ručak u 12:30, ali je rezervisao sto za 1. Nadao se da će zbog toga morati da popiju po piće za šankom, što se upravo i dogodilo. Bila je to savršena prilika da se kreće i časka sa svakim ponaosob.

Ipak, bilo je toliko prilika gde bi jedan pogrešan korak – pogrešan odgovor, ili neoprezna primedba – obelodanio da je Rik prevarant. Samo bi se izuzetno samouveren i lukav industrijski špijun usudio da se na taj način izloži riziku. Budući da je godinama „radio“ na ulici, Rik se izveštio i stekao samopouzdanje da će, čak i ako načini grešku, moći da je zataška dovoljno dobro da niko ništa ne posumnja. To je bio najizazovniji, najopasniji deo čitave operacije, a kada je osetio ushićenje što mu je takva obmana uspela,

shvatio je zašto ne mora da vozi brza kola, skače iz aviona s padobranom, niti da vara ženu – imao je dovoljno uzbuđenja i dok je obavljao posao. Koliko ljudi, pitao se, može to da kaže za sebe?

mitnikova poruka

Iako se većina prevara odigra preko telefona ili elektronskom poštom, nemojte misliti da se odvažan napadač nikada neće lično pojaviti u vašem preduzeću. U većini slučajeva, uljez izradi lažnu propusnicu pomoću svima dostupnog softvera kao što je Photoshop i upotrebi neku tehniku obmanjivanja da bi ušao u zgradu.

A šta kažete na posetnice na kojima je broj probne linije telefonske kompanije? U televizijskoj seriji o privatnom istražitelju, *Rokfordov dosije*, prikazana je oštroumna i ponešto smešna tehnika. Rokford (igrao ga je Džems Garner) imao je u kolima prenosiv uređaj za štampanje posetnica, koji bi koristio da odštampa odgovarajuću posetnicu za svaku priliku. Danas prevaranti mogu da izrade posetnice za jedan sat u svakoj fotokopirnici, ili da ih odštampaju na laserskom štampaču.

napomena

Džon le Kare, autor romana *Špijun koji se sklonio u zavetrinu*, *Savršen špijun*, i mnogih drugih odličnih knjiga, odrastao je uz oca, uglađenog i privlačnog prevaranta. Le Kare je u mladosti pogodilo saznanje da mu je otac, bez obzira na to što je uspešno obmanjivao druge, bio takođe lakoveran, te da je više puta bio meta drugih prevaranata. To samo pokazuje da se svako može obmanuti, pa čak i sam prevarant.

Zbog čega grupa pametnih osoba prihvati uljeza? Situacije ocenjujemo kako insitinktivno, tako i razumom. Ako je priča realna – to procenjuje razum – a prevarant izgleda uverljivo, obično nismo više oprezniji. Upravo taj uverljivi izgled odvaja uspešnog prevaranta od onog koji se ubrzo nađe iza rešetaka.

Zapitajte se da li biste poverovali u priču kao što je Rikova? Ako ste zaista sigurni, zapitajte se da li vas je iko *ikada* prevario u bilo čemu. Ako je odgovor na drugo pitanje potvrđan, onda isti odgovor verovatno važi i za prvo pitanje.

NAMEŠTALJKA

Ovo je izazov za vas: sledeća priča se ne odnosi na industrijsku špijunažu. Dok je budete čitali, pokušajte da razumete zašto sam odlučio da je uvrstim u ovo poglavlje!

Heri Tardi je ponovo živio kod kuće, i bio je ogorčen zbog toga. Činilo se da je mornarica pravo rešenje za njega, dok nije pretrpeo neuspeh za vreme obuke. Sada se vratio u rodni grad koji je mrzeo, pohađao je kurseve računara u lokalnoj višoj školi, i tražio je načina da se svima osveti.

Konačno je smislio plan. Pijuckajući pivo s jednim momkom koji je takođe pohađao predavanja, žalio se na sarkastičnog predavača sveznalicu, pa su zajedno smislili podao plan da ga nauče pameti: ukrasće izvorni kôd popularnog ručnog računara i poslati ga na predavačev računar, a pri tom će namerno ostaviti trag kako bi kompanija pomislila da je predavač krivac.

Njegov novi prijatelj, Karl Aleksandar, reče da „zna neke trikove“ i da će naučiti Herija kako to da izvede, a da ga ne uhvate.

Priprema

Tokom početnog istraživanja, Heri je saznao da se proizvod pravi u razvojnom centru u Evropi, u centrali firme koja proizvodi ručne računare. Postojale su i prostorije razvojnog odeljenja u Sjedinjenim Državama. To je dobar znak, istakao je Karl, jer im je za uspešan napad bio neophodan kompanijski ogranak u Sjedinjenim Državama, čiji zaposleni pristupaju izvornom kodu.

Tada je Heri bio spreman da nazove razvojni centar u Evropi. Zakukao je da mu pomognu: „Oh, bože, imam problema, potrebna mi je pomoć, molim vas, molim vas, pomozite mi.“ Naravno, molbu je uputio na prefinjeniji način. Karl je napisao tekst koji treba da kaže, ali je Heri zvučao potpuno izveštačeno dok ga je izgovarao. Na kraju je morao da vežba s Karlom da bi mogao da izgovori napisano prirodnim glasom.

Konačno, Heri je rekao sledeće, dok je Karl sedeo kraj njega:

„Zovem iz razvojnog odeljenja u Miniapolisu. Naš server je zaražen crvom koji je inficirao čitavo odeljenje. Morali smo ponovo da instaliramo operativni sistem, a kad smo pokušali da obnovimo podatke sa rezervnih kopija, nijedna kopija nije bila ispravna. Pogodite ko je trebalo da proveriti ispravnost rezervnih kopija? Ja, glavom i bradom. I tako se moj šef izvikao na mene, a čitavo rukovodstvo je ljutito što smo izgubili podatke. Čujte,

potrebna mi je najnovija verzija izvornog koda što je brže moguće. Trebalo bi da komprimujete izvorni kôd pomoću *gzipa* i pošaljete mi ga.“

Tada mu je Karl napisao nešto na ceduljici, a Heri je rekao čoveku s druge strane žice da samo treba da prosledi datoteku interno, u razvojno odeljenje u Miniapolisu. To je bilo izuzetno važno; kada je čoveku bilo jasno da od njega traže da samo pošalje datoteku u drugi deo kompanije, nije ga grizla savest – šta bi u tome moglo biti loše?

terminologija

GZIP GNU alatka za komprimovanje datoteka.

Pristao je da ga komprimuje i da ga pošalje. Korak po korak, Heri je objašnjavao čoveku kako da započne postupak komprimovanja ogromnog izvornog koda u jedinstvenu, kompaktnu datoteku, dok je Karl sve vreme bio tik kraj njega. Rekao mu je i kako da nazove novu komprimovanu datoteku, „novipodaci“, objašnjavajući mu da će na taj način izbeći mešanje sa njihovim starim dokumentima s greškom.

Karl je morao Heriju dvaput da objasni sledeći korak pre nego što ga je ovaj shvatio, ali to je bilo ključno za ovu nameštaljku. Trebalo je da Heri pozove razvojno odeljenje u Miniapolisu i kaže da će im poslati jedan dokument, a da ga oni proslede na drugu adresu – naravno, sve uvijeno u razloge zbog kojih bi zahtev zvučao uverljivo. Herija je zbunilo sledeće što treba da kaže: „Poslaću vam datoteku“, a zapravo je neće poslati on. Morao je da ubedi osobu s kojom razgovara u razvojnom centru da datoteku šalje on, a zapravo će je poslati neko iz Evrope. „Zašto da im kažem da ja šaljem datoteku, kad ona zapravo dolazi iz Evrope?“ želeo je Henri da zna.

„Osoba u razvojnom centru je samo posrednik“, objasni Karl. „On mora da misli da samo čini uslugu kolegi, tako što će primiti datoteku, a potom je proslediti dalje.“

Heri je konačno shvatio. Nazvao je razvojni centar i zamolio službenicu na centrali da ga poveže s računarskim centrom, gde je zatražio da razgovara s operaterom. Javio se momak koji je zvučao kao da je mlad koliko i Heri. Heri ga je pozdravio, predstavio se kao radnik iz čikaškog proizvodnog odeljka firme, i rekao da pokušava da pošalje neku datoteku jednom od partnera koji rade s njima na projektu, ali da ima problem s usmerivačem,

pa ne može da se uključi u njihovu mrežu. „Hteo bih da pošaljem datoteku vama, a kada je primite, nazvaću vas da vam objasnim kako da je prosledite do partnerovog računara.“

Dosad je sve bilo u redu. Heri je potom upitao mladića da li njegov računarski centar ima *anoniman FTP* nalog, koji omogućava bilo kome da šalje i preuzima datoteke. Da, postoji anoniman FTP nalog, i mladić je dao Heriju njegovu internu IP adresu.

terminologija

ANONIMAN FTP (engl. *anonymous FTP*) Program koji obezbeđuje pristup dokumentima na udaljenom računaru bez važećeg korisničkog imena i lozinke. Iako se anonimnom FTP nalogu može pristupiti bez lozinke, uglavnom su ograničena prava pristupa određenim direktorijumima.

Došavši do tih informacija, Heri je ponovo pozvao razvojni centar u Evropi. Komprimovana datoteka je tada već bila spremna, a Heri im je dao uputstva kako da je pošalju na anonimnu FTP lokaciju. Za manje od pet minuta, datoteka sa komprimovanim izvornim kodom bila je poslata momku u razvojnom centru.

Konačan potez

Pola posla je bilo obavljeno. Sada su Heri i Karl morali da sačekaju da bi se uverili da je datoteka stigla pre nego što nastave dalje. Dok su čekali, odšetali su se do predavačevog stola i preduzeli još dva neophodna koraka. Prvo su instalirali anoniman FTP server na predavačevom računaru, koji će biti konačno odredište datoteke u poslednjem delu njihovog plana.

U drugom koraku pronašli su rešenje za jedan velik problem. Očigledno nisu mogli da kažu momku u razvojnom centru da pošalje datoteku na adresu kao što je, na primer, `voren@rms.ca.edu`. Domen „.edu“ bi ih odmah izdao, jer bi ga svaki iole razuman računarski operater prepoznao kao adresu škole, što bi odmah upropastilo celu operaciju. Da bi to izbegli, otvorili su Windows na predavačevom računaru i potražili IP adresu računara, koju će dati kao adresu na koju valja poslati datoteku.

Tada je već bilo vreme da se pozove računarski operator u razvojnom centru. Heri ga je nazvao telefonom i rekao: „Upravo sam poslao datoteku o kojoj sam vam govorio. Možete li da proverite da li ste je primili?“ Da, stigla je. Heri ga je potom zamolio da je prosledi, i dao mu IP adresu. Ostao je na vezi dok se mladić povezivao i počeo da prenosi datoteku, pa su sa širokim osmesima na licu gledali iz drugog dela prostorije kako lampice na čvrstom disku trepere – to je značilo da računar prima datoteku.

Heri je još malo procaskao s momkom s druge strane žice o tome kako će možda jednog dana računari i pomoćni uređaji biti pouzdaniji, zahvalio mu se i oprostio se od njega.

Obojica su kopirala datoteku s predavačevog računara na par Zip diskova, da bi kasnije mogli da ih pogledaju, kao da su ukrali sliku iz muzeja u kojoj mogu da uživaju nasamo, ali se ne bi usudili da je prikažu prijateljima. Moglo bi se reći da su ukrali reprodukciju slike, a u muzeju je ostao original.

Karl je potom Heriju podrobno objasnio kako da ukloni FTP server sa predavačevog računara i izbriše dnevnik događaja kako ne bi bilo dokaza o tome što su učinili – ostao je samo ukradeni dokument, na lako dostupnom mestu.

Najzad, objavili su deo izvornog koda na Usenetu, direktno s predavačevog računara. Samo deo, da ne bi naneli veliku štetu kompaniji, ali ostavljajući tragove koji su očigledno upućivali na predavača. Imaće poteškoća da to objasni.

Analiza prevare

Iako je za uspeh ovog nestašluka bilo potrebno više elemenata, to se ne bi dogodilo da nisu vešto igrali na kartu sažaljenja i pomoći: na mene više šef, a rukovodstvo je ljutito, i tako dalje. To, zajedno sa smišljenim objašnjenjem kako da osoba s druge strane žice pomogne, pokazalo se kao izuzetno uspešna prevara. Uspela je njima, kao i mnogim drugima.

Drugi izuzetno važan element bio je što su čoveka koji je znao koliko je datoteka značajna zamolili da je pošalje na adresu unutar firme.

I treći deo slagalice: operater računarskog centra je video da mu je datoteka prosleđena u okviru kompanije. To je moglo da znači samo jedno – ili se bar tako činilo – da je čovek koji mu je poslao datoteku mogao sam da je uputi do konačnog odredišta, ali mu spoljna mrežna veza nije radila. Šta bi moglo biti loše u tome što mu pomaže da je pošalje?

A zašto su komprimovanom dokumentu dodelili drugo ime? To je bio naizgled mali korak, ali veoma bitan. Napadač nije smeo da rizikuje da datoteka stigne sa imenom koje bi je označilo kao izvorni kôd, ili nazivom vezanim za proizvod. Zahtev da se datoteka s tim nazivom pošalje van firme mogao je prouzrokovati uzbunu. Bilo je neophodno da ime datoteke bude bezazleno. Kao što su napadači i planirali, drugi mladić nije se kolebao da pošalje datoteku van firme. Teško i da bi mogao posumnjati u datoteku s nazivom kao što je „novipodaci“, koji ni na koji način ne odaje pravu prirodu informacija.

Da li ste shvatili zašto sam ovu priču uvrstio u poglavlje o industrijskoj špijunaži? Ako niste, evo odgovora: ono što su ova dva studenta izvela kao zlobnu šalu lako je mogao učiniti profesionalni industrijski špijun, kojeg možda plaća konkurencija. U svakom slučaju, šteta po kompaniju bi mogla biti poražavajuća, i opasno bi ugrozila prodaju njihovog novog proizvoda kada bi se konkurentski proizvod pojavio na tržištu.

Koliko lako bi se takav napad mogao izvesti na vašu firmu?

mitnikova poruka

Osnovno pravilo koje svaki zaposleni mora uvek imati na umu je sledeće: ne šaljite datoteke osobama koje ne poznajete lično, čak i ako se čini da se odredište nalazi u okviru interne mreže firme, ukoliko vam pretpostavljeni to posebno ne odobri.

SPREČAVANJE NAPADA

Industrijska špijunaža, koja je dugo opterećivala kompanije, postala je glavni posao tradicionalnih špijuna, nakon prestanka hladnog rata. Državne institucije i preduzeća sada angažuju industrijske špijune da krađu informacije. U mnogim slučajevima to su bivši vojni špijuni koji su prešli na mešetarenje industrijskim informacijama; oni imaju potrebno znanje i iskustvo, pa lako iskorišćavaju organizacije, naročito one koje ne primenjuju mere obezbeđenja podataka i ne obrazuju kadar.

Bezbednost van prostorija preduzeća

Šta je moglo da pomogne kompaniji koja je čuvala rezervne kopije van svojih prostorija? Opasnost se mogla izbeći da su podaci bili šifrovani. Da, za šifrovanje je potrebno dodatno vreme i novac, ali je vredno napora. Šifrovanje datoteke valja redovno proveravati da bi se utvrdilo da li šifrovanje i dešifrovanje dobro rade.

Uvek postoji opasnost da će se ključevi za šifrovanje izgubiti, ili da će jedinu osobu koja zna ključeve pregaziti autobus. Potencijalne nepravilnosti se predupređuju, i svako ko poverljive informacije čuva van svojih prostorija bez šifrovanja je, izvinjavam se na izrazu, idiot. To je kao da šetate ulicom po lošem kraju, dok vam iz džepa viri novčanica od dvadeset dolara, koja prosto traži da je neko ukrade.

Ostaviti medij sa rezervnim kopijama podataka tamo odakle bi ga neko mogao odneti uobičajen je propust u obezbeđenju. Pre nekoliko godina radio sam za preduzeće koje je moglo bolje da zaštiti informacije o klijentima. Osoblje je svakodnevno kuriru ostavljalo trake sa rezervnim kopijama podataka *izvan* zaključane prostorije s računarima. Svako je mogao da se odšeta sa tim trakama, na kojima su se nalazili svi tekstualni dokumenti firme u nešifrovanom obliku. Ako su podaci na rezervnim kopijama šifrovani, gubitak podataka je tek smetnja; ako nisu šifrovani – pa, sami možete da zamislite koliko bi to uticalo na vašu kompaniju, bolje nego što bih vam ja predstavio.

Činjenica da veće kompanije moraju imati pouzdano skladište podataka u udaljenom objektu uglavnom se podrazumeva. Ali u bezbednosnim procedurama mora se naznačiti i provera preduzeća za skladištenje da bi se videlo koliko prilježno primenjuju sopstvene mere obezbeđenja. Ako nisu toliko posvećeni tome kao vaša firma, svi vaši naponi da zaštitite podatke mogli bi pasti u vodu.

Manje kompanije imaju dobru alternativu za izradu rezervnih kopija podataka: svake večeri pošaljite nove i izmenjene datoteke na neko skladište na Mreži. Izuzetno je važno da se podaci šifriraju. U suprotnom, informacije će biti dostupne nepoštenim radnicima preduzeća za skladištenje podataka i svakom uljezu koji uspe da provali u njihove računarske sisteme ili mrežu.

Naravno, kada rezervne kopije podataka šifrujete, morate primeniti i izuzetno bezbednu proceduru skladištenja ključeva šifrovanja ili lozinki koje ih otključavaju. Tajne ključeve pomoću kojih se podaci dešifruju valja smestiti u sef ili trezor. U standardnom kompanijskom pravilniku treba uzeti u obzir mogućnost da zaposleni koji radi sa tim podacima naglo ode iz firme, umre, ili preuzme neko drugo radno mesto. Uvek moraju postojati bar dve osobe koje znaju mesto skladištenja, procedure za šifrovanje i dešifrovanje, kao i pravila o tome kada i kako izmeniti ključeve. U pravilniku mora stajati i to da se ključevi za šifrovanje moraju izmeniti neposredno nakon što bilo koji zaposleni koji im je pristupao napusti preduzeće.

Ko je to?

Primer ugladenog prevaranta koji šarmira zaposlene da mu odaju informacije ponovo nas podseća na to koliko je važna provera identiteta. Iz priče u kojoj je zahtevano da se izvorni kôd prosledi na FTP lokaciju takođe izvlačimo zaključak da je izuzetno bitno poznavati podnosioca zahteva.

Poglavlje 16 sadrži konkretna pravila za proveru identiteta svake nepoznate osobe koja zatraži informacije, ili zahteva da nešto učinite za nju. U knjizi je već bilo reči o tome kako je neophodno proveriti identitet podnosioca zahteva; u poglavlju 16 naći ćete konkretne savete kako to da učinite.



deo 4

Obuka za održivu
podjelu

Pogled u suštinu problema

Obuka za zaštitu podataka

Kradljivcu je naloženo da se domogne planova vašeg potpuno novog proizvoda koji treba da se pojavi na tržištu za dva meseca. Šta će ga sprečiti?

Vaš zaštitni bedem? Ne.

Moćni uređaji za identifikaciju? Ne.

Sistemi za otkrivanje uljeza? Ne.

Šifrovanje? Ne.

Ograničen pristup modemima za daljinski pristup? Ne.

Kodirana imena servera koja otežavaju uljezu da odredi na kom se od njih nalaze planovi proizvoda? Ne.

Istina je da ne postoji tehnologija koja može sprečiti napad na informacije.

OBEZBEĐENJE POMOĆU TEHNOLOGIJE, OBUKE I PRAVILA

Po podacima preduzeća za proveru bezbednosnih sistema, pokušaji provala u sisteme klijenata pomoću obmane skoro su uvek uspešni. Bezbednosne tehnologije mogu otežati takve napade izuzimanjem ljudi iz posupka donošenja odluka. Međutim, jedini zaista efikasan način da se umanj

pretnja od krađe podataka jeste korišćenje bezbednosne tehnologije *„sprezi sa bezbednosnim pravilima u kojima su definisani postupci zaposlenih, kao i sa odgovarajućim obrazovanjem i obukom.*

Proizvodne planove možete da zaštitite samo ako radnici budu obučeni, svesni opasnosti koje prete, i ako savesno primenjuju pravila. U to se ubraja i obuka o pravilima ponašanja i definisanje bezbednosnih postupaka, kao i – što je možda još važnije – stalni program za informisanje o opasnostima. Neki stručnjaci preporučuju da se 40 procenata predviđenog budžeta za obezbeđenje uloži u informisanje zaposlenih.

Prvi korak je da se svima u preduzeću stavi do znanja da postoje beskrupulozni ljudi koji će ih obmanuti koristeći psihološke metode. Zaposleni se moraju obučiti o tome koje informacije i kako valja zaštititi. Kad ljudi shvate na koje načine ih neko može obmanuti, mnogo lakše mogu da prepoznaju napad.

Informisanje o bezbednosti takođe znači obrazovanje svih zaposlenih o propisanim bezbednosnim pravilima i postupcima. Kao što piše u poglavlju 16, pravila ponašanja su neophodne smernice zaposlenima da bi se zaštitili informacioni sistemi i osetljivi podaci.

U ovom i sledećem poglavlju naći ćete detaljan plan obezbeđenja koji bi vas mogao spasti od napada sa skupim posledicama. Ako vaši radnici nisu obučeni i stalno na oprezu, i ako ne postupaju prema dobro osmišljenim pravilima, nije pitanje *da li*, već *kada* će vam prevaranti ukrasti vredne podatke. Ne čekajte da se napad dogodi pa da primenite ova pravila; to bi moglo da šteti vašem poslovanju i radnicima.

SHVATITE KAKO NAPADAČI ISKORIŠĆAVAJU LJUDSKU PRIRODU

Da biste osmislili uspešan program obuke, morate shvatiti zašto su ljudi uopšte podložni manipulaciji. Isticanjem tih slabih tačaka u obuci – na primer, tako što ćete se usredsrediti na njih za vreme rasprava o probnim napadima koje su izveli učesnici obuke – možete pomoći radnicima da razumeju zašto nas prevaranti mogu izmanipulisati.

Sociolozi proučavaju manipulaciju bar pedeset godina. Robert B. Cialdini je objavio sažetak tog istraživačkog rada u časopisu *Scientific American* (februara 2001). Naveo je šest „osnovnih tendencija ljudske prirode“ koje se javljaju kada neko pokuša da navede osobu na saradnju ili ispunjenje zahteva.

Kradljivci informacija se oslanjaju na tih šest tendencija, nekada svesno, a najčešće nesvesno.

Autoritet

Ljudi obično sarađuju sa podnosiocima zahteva koji su na visokom položaju. Kao što smo već napomenuli, osoba se može navesti da se povinuje zahtevu ako veruje da je podnosilac zahteva osoba na visokom položaju, ili neko ko je za to ovlašćen.

U svojoj knjizi *Uticaj*, dr Cialdini piše o studiji sprovedenoj u tri bolnice na srednjem zapadu. Čovek koji se predstavljao kao bolnički lekar zvao je 22 sobe za medicinske sestre i nalogao da daju lek pacijentu na odeljenju. Sestre koje su primile poziv nisu poznavale sagovornika. Nisu čak ni znale da li je zaista lekar (nije bio). Primile su uputstva za davanje leka telefonom, što je bilo kršenje bolničkog pravilnika. Nije bila odobrena upotreba navedenog leka na odeljenju, a navedena doza bila je dvostruko veća od najveće dozvoljene dnevne doze, pa je zbog toga mogla ugroziti život pacijenta. Cialdini tvrdi da su, u 95 odsto slučajeva, „sestre uzele potrebnu dozu iz ormarića za lekove na odeljenju, i krenule da ga daju pacijentu“. Tada bi ih presreo posmatrač i obavestio da je reč o eksperimentu.

Primeri napada: Obmanjivač pokušava da se zaodene velom autoriteta predstavljajući se da je iz informatičkog odeljenja, da je rukovodilac, ili radi za nekog na visokoj poziciji u kompaniji.

Dopadljivost

Ljudi obično sarađuju sa osobama koje im se dopadnu, ili navedu da imaju slične interese, uverenja i stavove kao žrtva.

Primeri napada: Kroz razgovor, napadač sazna hobije ili interesovanja žrtve, a potom tvrdi da ga zanima isto, kaže da je iz iste države, da je išao u istu školu, ili da ima slične ciljeve. Obmanjivač će takođe pokušati da imitira ponašanje žrtve da bi stvorio privid sličnosti.

Uzvratanje ljubaznosti

Često automatski pristanemo na zahtev kad nam se obeća ili pokloni nešto vredno. Poklon može biti materijalna stvar, savet, ili pomoć. Kada neko nešto učini za vas, osećate nagon da mu uzvratite. Ta jaka tendencija da se uzvрати istom merom javlja se čak i kada osoba koja je dala poklon nije ništa

tražila za uzvrat. Jedan od najefikasnijih načina da se ljudi navedu da učine „uslugu“ (tj. da se povinuju zahtevu) jeste da im se nešto pokloni ili da im se pomogne, pošto se podrazumeva da su obavezni da uzvrate istom merom.

Članovi sekte Hare Krišna veoma su efikasno navodili ljude da im uplate novac tako što bi im prvo dali knjigu ili cvet na poklon. Ako bi neko pokušao da im vrati poklon, odvrćali bi ga rečima: „To je naš poklon vama.“ Taj princip uzajamnog davanja pripadnici sekte upotreбили su da bi značajno uvećali donacije.

Primeri napada: Zaposleni primi poziv od osobe koja se predstavi kao informatičar iste firme. Sagovornik mu objasni da su neki kompanijski računari zaraženi novim virusom koji antivirusni softver nije prepoznao, a koji može da uništi sve datoteke na računaru. Potom mu ponudi objašnjenje kako da spreči problem. Nakon toga, sagovornik zamoli osobu da proveri nedavno ažuriran uslužni program pomoću koga korisnici mogu da menjaju lozinke. Radnik ne sme da odbije, jer je sagovornik upravo pomogao njemu, navodno zaštitivši računar od virusa. On mu uzvraća tako što pristaje na njegov zahtev.

Doslednost

Ljudi obično sarađuju pošto su se javno obavezali. Kada obećamo da ćemo nešto učiniti, ne želimo da nas smatraju neodgovornima ili odbojnim, pa se često držimo započetog da bismo dosledno sproveli izjavu ili obećanje.

Primeri napada: Napadač uspostavi kontakt s novozaposlenim i obavesti ga o pridržavanju bezbednosnih pravila i postupaka, koji su uslov za odobranje pristupa informacionim sistemima. Nakon što su porazgovarali o nekoliko bezbednosnih pravila, napadač zatraži od korisnika lozinku „da bi proverio da li ispunjava uslove“ prema kojima se moraju birati lozinke koje se teško pogađaju. Kada mu korisnik otkrije lozinku, sagovornik predloži da ubuduće koristi lozinke koje će napadači teško pogoditi. Žrtva se povinuje zahtevu jer je prethodno pristala da se pridržava firminih pravila obezbeđenja, i smatra da sagovornik samo proverava.

Društvena potvrda

Ljudi se povinuju zahtevu kad se čini da to i drugi rade. Ono što drugi rade prihvata se kao ispravno i odgovarajuće.

Primeri napada: Osoba s druge strane žice kaže da sprovodi anketu i pomene imena nekoliko drugih osoba iz istog odeljenja, koje su navodno već saradivale s njim. Žrtva, verujući da saradnja drugih potvrđuje ispravnost zahteva, pristane da učestvuje. Sagovornik mu potom postavi niz pitanja, među kojima su i ona koja navedu žrtvu da otkrije svoje korisničko ime i lozinku.

Oskudica

Često pristajemo da ispunimo zahtev kada se nadmećemo s drugima da bismo se domogli nečega, ili kada je željena stvar navodno dostupna samo u kratkom vremenskom periodu.

Primeri napada: Napadač pošalje elektronske poruke u kojima tvrdi da će prvih 500 osoba koje se registruju na novoj Web lokaciji preduzeća dobiti besplatne karte za nov, popularan film. Kada se naivni radnik registruje na lokaciji, od njega se traži da unese adresu elektronske pošte svoje firme i da izabere lozinku. Mnogi upotrebe istu lozinku koju inače koriste u svakom računarskom sistemu, ili sličnu, jer im je jednostavnije. Znajući to, napadač potom pokuša da provali u žrtvin poslovni i kućni računarski sistem pomoću unetog korisničkog imena i lozinke.

OSMIŠLJAVANJE PROGRAMA OBUKE I INFORMISANJA

Objavljivanjem brošure sa pravilima obezbeđenja informacija, ili upućivanjem zaposlenih na Web stranu s pravilima na intranetu, nećete umanjiti rizik. Svako preduzeće mora definisati pravila napismeno i uputiti *svakoga* ko radi s informacijama ili računarskim sistemima da nauči pravila i pridržava ih se. Štaviše, morate se uveriti da je svako shvatio zašto su sva pravila neophodna i proveriti da ih ljudi ne zaobilaze jer im je jednostavnije. U suprotnom, radnici će uvek koristiti neznanje kao izgovor, a upravo će to obmanjivači iskorišćavati.

Osnovni cilj svakog programa za informisanje jeste da utiče na ljude da izmene svoje ponašanje i stavove tako što će motivisati svakog od njih da *svojevoljno* doprinese zaštiti informacionih resursa preduzeća. U ovom slučaju, radnici se mogu sjajno motivisati ako im se objasni da će svojim učesćem doneti dobrobit i kompaniji, ali i kolegama. S obzirom na to da se u preduzeću čuvaju lični podaci o svakom radniku, kad zaposleni

ispune svoj deo obaveze o zaštiti informacija ili informacionih sistema, oni zapravo štite i sopstvene podatke.

Za program bezbednosne obuke potrebna je znatna podrška. Svako s pristupom osetljivim informacijama ili računarskim sistemima mora biti obučen. Obuka mora biti stalna, i mora se redovno unapređivati da bi se osoblje obavestilo o novim pretnjama i opasnostima. Zaposleni moraju videti da uprava u potpunosti podržava takav program. Njihova podrška mora biti stvarna, a ne samo u obliku dopisa sa pečatom u kom daju svoj blagoslov. Za planiranje, objavljivanje, proveru i merenje uspeha programa, takođe se moraju izdvojiti dovoljna sredstva.

Ciljevi

Prilikom planiranja obuke i pravljenja programa za informisanje zaposlenih o bezbednosti podataka, osnovna ideja treba da bude informisanje svih zaposlenih da bi kompanija u bilo kom trenutku mogla biti napadnuta. Moraju shvatiti da svaki zaposleni igra ulogu u odbrani od provale u računarske sisteme ili krađe osetljivih podataka.

Budući da su mnogi vidovi obezbeđenja informacija tehnološki, radnici olako veruju da taj problem rešavaju zaštitne barijere i druge bezbednosne tehnologije. Osnovni cilj treninga trebalo bi da bude informisanje svih zaposlenih da su oni sami u prvim redovima odbrane čitave organizacije.

Bezbednosna obuka mora imati znatno više ciljeve nego što je puko saopštavanje pravila. Osoba koja planira program obuke mora biti svesna toga da su zaposleni, pod pritiskom da obave zadatke na vreme, stalno u iskušenju da prenebregnu ili ignorišu svoje odgovornosti u vezi sa bezbednošću. Važno je poznavati taktike obmanjivanja i načine odbrane od napada, ali to ne vredi ništa ako se obuka ne usredsredi prvenstveno na *motivisanje* zaposlenih da upotrebe to znanje.

Možete da smatrate da je program zadovoljio osnovne ciljeve ako su svi koji su ga pohađali sasvim ubeđeni u to da je obezbeđenje informacija deo njihovog posla i motivisani da primene propisana pravila.

Radnici moraju shvatiti i prihvatiti činjenicu da su prevare realna opasnost, i da bi ozbiljan gubitak osetljivih informacija mogao ugroziti preduzeće, kao i njihove lične podatke i poslove. Ako neko ne brine o bezbednosti informacija na poslu, to je isto kao da ne vodi računa o svom PIN kodu za bankomate, ili o broju kreditne kartice. Ovo poređenje moglo bi podstaći zaposlene da primenjuju bezbednosne mere.

Organizovanje programa obuke i informisanja

Osoba odgovorna za organizovanje programa za zaštitu podataka mora razumeti da to nije projekat koji se na sve zaposlene može primeniti na isti način. Obuku treba isplanirati tako da odgovara posebnim zahtevima nekoliko različitih grupa u okviru preduzeća. Dok se mnoge bezbednosne mere navedene u poglavlju 16 odnose na sve zaposlene u firmi, druge su jedinstvene. U većini kompanija različiti programi obuke moraju se, u najmanju ruku, osmisliti za sledeće grupe: upravu, informatičko osoblje, korisnike računara, netehničko osoblje, sekretare, službenike prijemnih odeljenja i čuvare. (Pogledajte u poglavlju 16 spiskove pravila prema opisu radnog mesta.)

S obzirom na to da se od radnika iz obezbeđenja najčešće ne očekuje da umeju da koriste računare, i da se smatra da ne dolaze u dodir s njima (ili retko), oni se obično izostavljaju kada se planira ovakva obuka. Međutim, obmanjivači umeju da prevare čuvare i druge zaposlene da ih puste u zgradu ili kancelariju, pa i da ih navedu da provale u računarski sistem. Iako čuvarima sigurno ne treba čitava obuka za osoblje koje radi s računarima, oni se ipak ne smeju prevideti u programu informisanja o zaštiti podataka.

U poslovanju verovatno postoji veoma mali broj tema o kojima treba obrazovati sve zaposlene. Iako su te teme važne, zaposlenima su uglavnom dosadne. Takvo je i pitanje bezbednosti. Najbolje osmišljeni programi obuke za zaštitu podataka moraju biti informativni, zanimljivi i podsticajni.

Cilj bi trebalo da bude da se obuka i informisanje o zaštiti podataka učine zanimljivim i praktičnim. U tehnike se mogu svrstati sledeće: demonstriranje metoda obmanjivanja kroz probne napade, pregled izveštaja u medijima o skorašnjim napadima na druge, manje srećne firme i razgovor o načinima na koje su mogli sprečiti gubitak, ili prikazivanje video materijala koji je istovremeno i obrazovnog i zabavnog karaktera. Postoji nekoliko kompanija za informisanje o bezbednosti podataka koje prave takve video materijale.

Priče iz ove knjige daju dovoljno materijala da se objasne metode i tehnike obmanjivanja, da se informiše o pretnji od napada, i da se prikažu slabe tačke u ljudskom ponašanju. Neka ove priče budu osnova za probne napade prilikom obuke. Priče su dovoljno živopisne da nude različite mogućnosti za rasprave o tome kako su žrtve mogle drugačije reagovati i osujetiti napade.

napomena

Neka preduzeća nemaju sredstava da organizuju program u svojim prostorijama. Zato postoji nekoliko kompanija koje nude usluge obuke i informisanja o zaštiti podataka. Do njih možete doći na sajmovima kao što je Secure World Expo (www.secureworldexpo.com).

Vešti organizatori i predavači naići će na mnoge izazove, ali će uvideti i mnoge mogućnosti da učine obuku zanimljivijom, kao i da motivišu ljude da učestvuju u rešavanju problema.

Struktura obuke

Osnovni program obuke za zaštitu podataka valja planirati tako da bude obavezan za sve zaposlene. Od novih zaposlenih treba tražiti da obavezno pohađaju takvu obuku u okviru upoznavanja s organizacijom. Savetujem vam da se nijednom radniku ne dozvoli pristup računaru dok ne završi osnovni kurs za zaštitu informacija.

Predlažem da ta početna obuka bude dovoljno usredsređena na suštinu da bi održala pažnju polaznicima, te da bude dovoljno kratka da se zapamte bitne poruke. Iako količina materijala koji treba obraditi sigurno zahteva dužu obuku, smatram da je mnogo bitnije informisati i motivisati ljude, i preneti im umeren broj najvažnijih poruka, nego organizovati poludnevna ili celodnevna predavanja s kojih ljudi odlaze opterećeni prevelikim brojem informacija.

Za vreme obuke treba se usredsrediti na to da zaposleni shvate kolika se šteta može naneti preduzeću i pojedincima ukoliko se svi radnici ne budu pridržavali propisanih bezbednosnih pravila. Motivisanje zaposlenih da prihvate ličnu odgovornost za bezbednost još je važnije od podučavanja o određenim pravilima.

Ako neki zaposleni ne mogu da pohađaju klasičnu obuku, program informisanja treba sprovesti na druge načine: pomoću video traka, računara, Interneta, ili pisanih materijala.

Nakon početne kratke obuke valjalo bi organizovati duže kurseve na kojima bi se zaposleni obavestili o slabim tačkama i tehnikama napada koji se odnose na njihovo radno mesto u firmi. Trebalo bi zahtevati da svako

osveži svoje znanje iz te oblasti bar jednom godišnje. Priroda napada i metode za iskorišćavanje ljudi stalno se menjaju, pa sadržaj programa treba redovno ažurirati. Štaviše, ljudi vremenom postaju sve manje oprezni, pa se obuka mora ponavljati u određenim intervalima da bi se radnici podsetili bezbednosnih principa. Pri tome, naglasak ponovo treba da bude na obaveštavanju zaposlenih o značaju pravila i njihovom motivisanju da ih se pridržavaju. Pored toga, obratite pažnju i na prikazivanje vrsta napada i metoda obmanjivanja.

Uprava radnicima mora odobriti dovoljno vremena da se upoznaju s bezbednosnim pravilima i postupcima, kao i da učestvuju u informativnom programu. Ne bi trebalo očekivati od zaposlenih da uče pravila bezbednosti ili pohađaju časove u slobodno vreme. Novim zaposlenim treba dati dosta vremena da shvate bezbednosna pravila i postupke pre nego što preuzmu odgovornosti svog radnog mesta.

Od osoba koje promene radno mesto i dobiju pristup osetljivim informacijama ili računarskim sistemima, trebalo bi, naravno, zahtevati da pohađaju program za zaštitu podataka osmišljen posebno za njihove nove odgovornosti. Na primer, kada operater na računarima postane administrator sistema, ili kada službenica prijemnog odeljenja postane sekretarica, neophodna je nova obuka.

Sadržaj kursa

U osnovi, svi napadi lažnim predstavljanjem imaju jedan zajednički činilac: obmanu. Žrtva se navede da poveruje da je napadač kolega ili druga osoba koja je ovlašćena da pristupi osetljivim informacijama, ili da od žrtve zahteva da uradi nešto na računaru ili na pratećoj opremi. Gotovo svi ti napadi bi se mogli osujetiti kada bi se zaposleni pridržavali dva jednostavna pravila. Morali bi proveriti:

- identitet podnosioca zahteva – da li je osoba koja od njih nešto zahteva zaista onaj za kog se izdaje.
- da li je ta osoba ovlašćena – smeju li joj se saopštiti informacije, odnosno je li joj odobreno da podnese zahtev.

napomena

Budući da obuka za zaštitu informacija nikada nije savršena, koristite zaštitne tehnologije gde je god moguće da biste napravili višeslojan sistem odbrane. To znači da se obezbeđenje oslanja pre na tehnologiju nego na pojedine zaposlene, na primer, kada je operativni sistem podešen tako da spreči zaposlene da preuzimaju softver s Interneta, ili da izaberu kratku lozinku koja se može lako pogoditi.

Kada bi obuka za zaštitu podataka mogla izmeniti ponašanje zaposlenih tako da svako od njih uvek proveri svaki zahtev prema pomenuta dva kriterijuma, rizik od napada obmanjivača bio bi znatno umanjen.

Praktičan program obuke i informisanja o zaštiti podataka u kome se obrađuju pitanja ljudskog ponašanja i veština obmanjivanja trebalo bi da sadrži sledeće:

- Opis toga kako napadači koriste veštine obmanjivanja da bi prevarili ljude.
- Metode koje se upotrebljavaju pri sistematskom obmanjivanju da bi se postigli ciljevi.
- Kako prepoznati potencijalan napad.
- Postupke ponašanja kada se sumnja na napad.
- Kome treba prijaviti pokušaj obmane ili uspešan napad.
- Koliko je važno da se proveri identitet svake osobe koja podnese sumnjiv zahtev, bez obzira na njenu navodnu poziciju ili značaj.
- Činjenicu da ne treba verovati drugima bez provere, čak i kad prirodno poverenje prevagne nad sumnjom.
- Koliko je bitno proveriti identitet i autoritet svakoga ko zahteva podatke ili uslugu. (Pogledajte postupke za proveru i ovlašćivanje u poglavlju 16 da biste saznali kako da proverite nečiji identitet.)
- Postupke zaštite osetljivih informacija, uključujući i upoznavanje sa sistemom za klasifikaciju podataka.
- Mesto na kom se nalaze bezbednosna pravila i postupci firme, kao i koliko su oni važni za zaštitu podataka i informacionih sistema kompanije.

- Sažetak ključnih bezbednosnih pravila i objašnjenje njihovih značenja. Na primer, svaki zaposleni treba da nauči kako da osmisli lozinku koja se teško pogađa.
- Svaki zaposleni se mora obavezati da će se pridržavati pomenutih pravila i preuzeti odgovornost ako ih se ne pridržava.

Obmanjivanje po svojoj definiciji podrazumeva neki oblik interakcije među ljudima. Napadači često upotrebljavaju razne metode komunikacije i tehnologije da bi došli do cilja. Zato bi dobro osmišljen informativni program trebalo da dotakne neke od sledećih tema ili sve:

- Bezbednosna pravila u vezi sa lozinkama za pristup računarima i glasovnoj pošti.
- Postupke obznajivanja osetljivih informacija i materijala.
- Pravila upotrebe elektronske pošte, uključujući i mere zaštite od zlonamernih napada virusima, crvima i trojancima.
- Zahteve fizičkog obezbeđenja, kao što je stalno nošenje identifikacione kartice.
- Odgovornost da se proveri identitet osoba koje u prostorijama firme ne nose oznaku.
- Načine klasifikovanja podataka, i odgovarajuće mere zaštite osetljivih informacija.
- Odgovarajuće uklanjanje osetljivih dokumenata i računarskih medija na kojima se nalaze, ili su se ranije nalazili, poverljivi materijali.

Ako firma planira da obavi probna testiranja da bi proverila koliko efikasno deluje odbrana od obmanjivačkih napada, trebalo bi obavestiti zaposlene o tome. Stavite im do znanja da će ih u okviru takvog testa neko možda zvati telefonom ili na drugi način stupiti u vezu s njima. Rezultate takvih testova nemojte koristiti da kažnjavate, već da biste odredili oblasti za dodatnu obuku.

Pojedinosti o svim prethodno pomenutim temama nalaze se u poglavlju 16.

TESTIRANJE

Možda će vaša firma želiti da proveri koliko su zaposleni naučili na obuci za zaštitu podataka, pre nego što im se dozvoli pristup računarskom sistemu. Ako pripremite testove koji će se polagati preko mreže, rezultate testova možete odmah analizirati programom za automatsko ocenjivanje, da biste utvrdili oblasti na koje obuka treba da se posebno usredsredi.

Možda ćete odlučiti i da izdajete sertifikate kao dokaz da je zaposleni uspešno završio bezbednosnu obuku, što bi bila vrsta nagrade i motivisalo bi radnike.

Preporučuje se da u okviru programa svaki zaposleni potpiše sporazum u kojem se obavezuje da će se pridržavati bezbednosnih pravila i postupaka o kojima je bilo reči u obuci. Istraživanja pokazuju da osobe koje se obavežu potpisivanjem takvog ugovora ulažu veće napore da se pridržavaju procedura.

REDOVNO INFORMISANJE

Ljudi su uglavnom svesni da znanje, čak i o važnim stvarima, blede ako se povremeno ne osveži. Budući da je veoma bitno da radnici budu obavešteni o novinama u oblasti odbrane od napada obmanjivača, redovno informisanje je suštinski značajno.

Jedna od metoda kojom se obezbeđuje da radnici stalno misle na bezbednost jeste da se zaštita informacija definiše kao posebna odgovornost obuhvaćena opisom radnog mesta *svake* osobe koja radi u preduzeću. Tako radnici bolje shvataju koliko je važna njihova uloga u opštoj bezbednosti firme. U suprotnom, većina smatra da obezbeđenje „nije njihov posao“.

Iako se za program zaštite podataka uglavnom zaduži osoba iz obezbeđenja ili informatičkog odeljenja, verovatno je najbolje da se program informisanja o zaštiti podataka organizuje kao zajednički projekat sa odeljenjem za obuku.

Program redovnog informisanja mora biti kreativan i primenjivati sve moguće načine za prenošenje poruka o bezbednosti tako da ih ljudi lako pamte i stalno se podsećaju pravilnih bezbednosnih postupaka. U metode se ubrajaju sve tradicionalne tehnike, kao i sve druge kojih se seti osoblje određeno za organizovanje programa. Kao i uvek kada je u pitanju reklama, humor i oštroumnost su od pomoći. Ako menjate način na koji su poruke izražene, sprečićete da postanu toliko poznate da ih ljudi ignorišu.

Program za redovno informisanje mogao bi obuhvatiti sledeće metode:

- Obezbediti primerke ove knjige svim zaposlenima.
- Uvrstiti obaveštenja u bilten kompanije: članke, uokvirene podsetnike (najbolje je da budu kratki i da privlače pažnju), ili karikature.
- Objaviti sliku Najpožrtvovanijeg zaposlenog u oblasti obezbeđenja tog meseca.
- Okačiti postere u kancelarije zaposlenih.
- Staviti obaveštenja na oglasne table.
- Staviti odštampane podsetnike u kovertu s platom.
- Slati podsetnike elektronskom poštom.
- Upotrebljavati čuvare ekrana s porukama o obezbeđenju.
- Emitovati bezbednosne podsetnike preko sistema glasovnih poruka.
- Štampati nalepnice za telefone s porukama kao što je „Da li je vaš sagovornik zaista onaj za kog se izdaje?“
- Podesiti računare tako da prikazuju podsetnike kada se korisnik prijavljuje za rad, u kojima piše nešto poput „Ako šaljete poverljive informacije elektronskom poštom, šifrujte ih.“
- Uvrstiti posvećenost obezbeđenju kao standardno merilo u izveštajima o radu zaposlenih i u godišnjim pregledima.
- Postaviti podsetnike o zaštiti podataka na intranet. Uz dozu humora, karikaturama, ili na neki drugi način, podstaknite zaposlene da ih pročitaju.
- Koristiti table za elektronske poruke u kantini, na kojoj bi se često smenjivali podsetnici o bezbednosti.
- Distribuirati letke ili brošure.
- Razmisliti o trikovima kao što su besplatni kolačići sudbine u restoranu, od kojih svaki – umesto proročanstva – sadrži podsetnik o bezbednosti.

Pretanja uvek postoji, pa se i podsetnici moraju stalno koristiti.

ŠTA JA TIME DOBIJAM?

Pored informativnih programa i obuke, toplo preporučujem i aktivan i dobro promovisan program nagrađivanja. Morate nagraditi radnike koji su otkrili i sprečili pokušaj obmane, ili su na neki drugi način značajno doprineli uspehu programa za zaštitu podataka. Trebalo bi zaposlenima prisutnim na svim informativnim predavanjima objaviti da postoji program nagrađivanja, a narušavanja bezbednosnog sistema valja javno istaći širom organizacije.

S druge strane, ljudima se mora objasniti koje su posledice slučajnog ili namernog nepridržavanja pravila za zaštitu informacija. Svi mi grešimo, ali se višestruko narušavanje bezbednosnih postupaka ne sme tolerisati.

poglavlje

16

Preporučena bezbednosna pravila

Svaka deveta velika firma ili državna institucija bila je meta napada na računarske sisteme, ako je suditi po rezultatima ankete koju je sproveo FBI, a objavio je Associated Press aprila 2002. Zanimljivo je to da je, prema istraživanju, tek svaka treća firma prijavila ili javno objavila napad. Većina organizacija ne prijavljuje javno slučajeve provala u računarske sisteme da ne bi izgubili poverenje korisnika i da bi sprečili buduće napade.

Čini se da nema statističkih podataka o napadima obmanjivača, a kad bi ih i bilo, brojke bi bile sasvim nepouzdanе. U većini slučajeva, kompanija nikad i ne sazna da je neko ukrao podatke, pa mnogi napadi prolaze neprimećeni i neprijavljeni.

Protiv većine takvih napada mogu se primeniti efikasne mere zaštite. Ali, budimo realni – ukoliko svi u preduzeću ne shvate da je bezbednost važna, i ukoliko se svi ne potrudе da nauče bezbednosna pravila i pridržavaju ih se, obmane će uvek predstavljati velik rizik za preduzeće.

Kako se tehnološka zaštita od narušavanja sistema poboljšava, gotovo je sigurno da će lovci na informacije sve češće koristiti veštinu obmane da bi iskorišćavanjem ljudi dospeli do tajnih podataka, ili pristupili mreži preduzeća. Industrijski špijun će, naravno, pokušati da dođe do cilja na najlakši i najmanje rizičan način. Istinu govoreći, preduzeće koje je zaštitilo svoje

računarske sisteme i mrežu najmodernijim bezbednosnim tehnologijama možda je izloženo većem riziku od napadača koji se služe veštinama, tehnikama i metodama obmanjivanja.

U ovom poglavlju naći ćete pravila naročito osmišljena da svedu rizik od obmana na najmanju moguću meru. Pravila se odnose na napade u kojima se ne iskorišćavaju samo tehničke slabosti firme. U njima se upotrebljavaju trikovi i lažno predstavljanje da bi se od pouzdanog radnika na prevaru izmamile informacije, ili da bi se naveo na postupke koji obmanjivaču omogućavaju pristup osetljivim poslovnim podacima ili računarskim sistemima i mrežama firme.

ŠTA SU BEZBEDNOSNA PRAVILA?

Bezbednosna pravila su jasna uputstva kojih se zaposleni pridržavaju radi zaštite informacija. To je osnova za razvoj efikasnih mera za sprečavanje potencijalnih pretnji bezbednosnom sistemu. Još su važnija kada je u pitanju sprečavanje i otkrivanje obmane.

Efikasne bezbednosne mere se primenjuju tako što se radnici obučavaju do bro dokumentovanim pravilima i postupcima. Međutim, važno je shvatiti da bezbednosna pravila nisu garancija da će svaki pokušaj obmanjivanja biti sprečen, čak i ako ih se zaposleni u potpunosti pridržavaju. Umesto toga, realan cilj bi trebalo da bude smanjivanje rizik na prihvatljivu meru.

U pravila iz ovog poglavlja uvrstili smo i mere koje tu pripadaju zato što se odnose na tehnike koje se često koriste u obmanjivanju. Na primer, pravila o otvaranju priloga elektronskih poruka odnose se na metode koje prevaranti često koriste da bi instalirali programe na računar žrtve.

Razvoj bezbednosnog programa

Sveobuhvatan program za zaštitu podataka obično započinje procenom rizika pomoću kojih se utvrđuju odgovori na sledeća pitanja:

- Koje informacije u preduzeću valja zaštititi?
- Šta konkretno pretni tim podacima?
- Kakva bi se šteta nanela preduzeću ako bi se te potencijalne pretnje realizovale?

Osnovni cilj procene rizika jeste određivanje informacija koje treba odmah zaštititi, kao i da li će troškovi za mere obezbeđenja biti opravdani.

Jednostavno govoreći, treba odrediti koje informacije valja prvo zaštititi, i koliko novca treba potrošiti na to.

Izuzetno je važno da uprava potpuno podrži razvoj bezbednosnih pravila i programa za zaštitu podataka. Kao i u svemu drugom, ako želimo da program bezbednosti uspe, rukovodstvo mora dati lični primer, a ne samo obezbediti sredstva.

Zaposleni moraju biti uvereni da uprava smatra da je obezbeđenje informacija suštinski značajno za rad firme, da je zaštita poslovnih podataka izuzetno bitna za dalju konkurentnost i da svačiji posao zavisi od uspeha programa.

Osoba zadužena za pisanje bezbednosnih pravila mora imati na umu da tekst pravila ne sme biti opterećen tehničkim žargonom, tako da ga lako može razumeti netehničko osoblje. Takođe je važno da se u dokumentu objasni zašto je svako pravilo bitno inače bi zaposleni mogli zanemariti neka od njih jer im, navodno, uzalud troše vreme. Valjalo bi sačiniti pravilnik, i poseban dokument u kom su objašnjene procedure, jer će se pravila verovatno menjati mnogo ređe nego postupci za njihovu primenu.

Pored toga, osoba koja piše pravilnik mora biti obaveštena o tome kako se *tehnološka* rešenja mogu upotrebiti da bi se ljudi primorali na zaštitu informacija. Na primer, u većini operativnih sistema moguće je zahtevati da lozinke korisnika zadovolje određene zahteve, na primer, da ne budu kraće od zadate dužine. U nekim firmama se zabrana preuzimanja programa s Interneta može kontrolisati pomoću lokalnih ili globalnih parametara operativnog sistema. U pravilniku se mora insistirati da se zaštitna tehnologija koristi kad god je isplativa, da bi se ljudi isključili iz donošenja odluka.

Zaposlenima se moraju predložiti posledice nepridržavanja bezbednosnih pravila i postupaka. Trebalo bi sačiniti i objaviti spisak posledica narušavanja pravila bezbednosti. Takođe, valjalo bi osmisлити program nagrađivanja za one koji primenjuju propisana bezbednosna pravila, ili prepoznaju i prijave narušavanje bezbednosnog sistema. Kad god se radnik nagradi zbog osujećivanja napada, to valja javno razglasiti širom firme, na primer u kompanijskom biltenu.

Jedan od ciljeva programa informisanja o zaštiti podataka jeste da se ljudima saopšti koliko su važna bezbednosna pravila i da im se predloži šteta koja se može prouzrokovati nepridržavanjem tih pravila. U ljudskoj je prirodi da se povremeno ignorišu ili zaobiđu pravila koja se čine neopravdanim

ili koja oduzimaju suviše vremena. Uprava mora da uveri zaposlene koliko su pomenuta pravila bitna i da ih motiviše da ih se pridržavaju, umesto da ih oni smatraju preprekama koje valja zaobići.

Bitno je naglasiti da pravila zaštite podataka ne smeju biti nepromenljiva. Kako se menjaju potrebe poslovanja, na tržištu se pojavljuju nove bezbednosne tehnologije, a kako se pojavljuju propusti u obezbeđenju, pravila treba prilagoditi ili ih proširiti. Potrebno je odrediti postupak za redovni pregled i ažuriranje pravila. Neka kompanijska bezbednosna pravila budu svima dostupna preko intraneta, ili ih držite u registratoru, na javnom mestu. Tako je verovatnije da će se pravila i postupci češće revidirati, a i zaposlenima je zgodno da brzo nađu odgovor na svako pitanje u vezi sa obezbeđenjem.

Konačno, povremeno sprovedite probne upade i ocenjujte slabe tačke sistema pokušajima obmanjivanja, da biste pronašli oblasti na koje obuka treba više da se usredsredi, odnosno pravila i postupke kojih se zaposleni ne pridržavaju. Pre nego što primenite probne upade, objavite zaposlenima da povremeno mogu očekivati takvo testiranje.

Kako primenjivati pravila

Pravila iz ovog poglavlja samo su deo neophodnog skupa propisa da bi se ublažili rizici od narušavanja bezbednosnog sistema. Dakle, nemojte smatrati ova pravila sveobuhvatnim. Ona su osnova za sačinjavanje obimnijeg bezbednosnog pravilnika koji odgovara vašim konkretnim potrebama.

Osobe zadužene za pisanje pravilnika u vašoj organizaciji moraće da izaberu pravila na osnovu jedinstvenog okruženja i poslovnih ciljeva vaše firme. Budući da svaka organizacija ima drugačije bezbednosne zahteve koji zavise od potreba poslovanja, pravnih zahteva, atmosfere u organizaciji i postojećih informacionih sistema, iz ovog poglavlja proberite odgovarajuća pravila, a zanemarite nepotrebna.

Osim toga, trebalo bi odrediti koliko se strogo treba pridržavati pravila u različitim kategorijama. Manja firma koja nema više ogranaka i u kojoj se zaposleni uglavnom međusobno poznaju ne mora mnogo brinuti o tome da će neko pozvati telefonom i lažno se predstaviti kao kolega (iako bi se, naravno, mogao izdavati za poslovnog partnera). Takođe, iako postoje veliki rizici, ukoliko bi primenjivanje strogih pravila previše narušilo radnu atmosferu, preduzeće može usvojiti samo manji skup preporučenih pravila.

KLASIFIKACIJA PODATAKA

Klasifikacija podataka je neophodna za zaštitu kompanijskih informacija. To je postupak pravljenja kategorija za kontrolu objavljivanja osetljivih informacija. Svim zaposlenima se stavlja do znanja koliko je svaka pojedina informacija osetljiva.

Ako se podaci ne klasifikuju, donošenje odluka se uglavnom prepušta pojedincima. Svakako, na odluke zaposlenih velikim delom utiče njihova subjektivnost, umesto da se oslanjaju na osetljivost, značaj i vrednost informacija. Podaci se obelodanjuju i zato što radnici nisu svesni toga da ih možda daju obmanjivaču.

Klasifikacijom podataka, vredne informacije se smeštaju u jednu od više kategorija. Kada znaju klasu svake informacije, zaposleni mogu da se pridržavaju postupaka kojima se kompanija štiti od nenamernog ili nepažljivog odavanja osetljivih informacija. Ti postupci umanjuju mogućnost da se zaposleni na prevaru navedu da odaju osetljive informacije neovlašćenim osobama.

Svaki radnik mora da nauči klasifikaciju kompanijskih podataka, uključujući i radnike koji obično ne koriste računare, niti komunikacione sisteme firme. S obzirom na to da svaki radnik, uključujući čistače, čuvare, osobe koje fotokopiraju dokumenta, kao i savetnike, privremene radnike, pa čak i stažiste, može imati pristup osetljivim informacijama, svako od njih može biti meta napada.

Pretpostavljeni mora odrediti osobu *odgovornu za informacije*. Ta osoba će biti zadužena za upravljanje svim podacima koji se trenutno koriste u preduzeću. Između ostalog, to lice je zaduženo za zaštitu informacija. Najčešće on odlučuje o nivou klasifikacije podataka. U zavisnosti od toga koliko ih treba zaštititi, povremeno objavljuje izmene u klasifikaciji, i odlučuje o promenama. Upravnik za informacije može preneti svoja zaduženja i na *Čuvara* ili *Pomoćnika*.

Klasifikacione kategorije i definicije

Podatke treba odvojiti u različite nivoe u zavisnosti od njihove osetljivosti. Promena klasifikacionog sistema posle uspostavljanja je skupa i dugotrajna. Ja sam izabrao četiri nivoa klasifikacije, što je primereno većini srednjih i većih preduzeća. U zavisnosti od broja i vrsta osetljivih informacija, preduzeća mogu dodati još kategorija da bi bolje nadgledali pojedine tipove

podataka. U manjim preduzećima je možda dovoljna i trostepena klasifikacija. Upamtite – što je klasifikaciona šema složenija, to je obuka i primena sistema skuplja.

Poverljivo. Ova kategorija informacija je najosetljivija. Poverljive informacije se koriste samo u okviru organizacije. U većini slučajeva, samo veoma ograničen broj ljudi zna za njih. Priroda poverljivih podataka je takva da bi svako neovlašćeno obelodanjivanje prouzrokovalo ozbiljnu štetu firmi, njenim deoničarima, poslovnim partnerima i/ili klijentima. Poverljive informacije uglavnom spadaju u jednu od sledećih kategorija:

- Poslovne tajne, izvorni kodovi programa, tehničke ili funkcionalne specifikacije, ili informacije o proizvodu koje bi mogle koristiti konkurenciji.
- Informacije marketinške i finansijske prirode koje nisu namenjene javnosti.
- Sve druge informacije koje su suštinski značajne za rad firme, kao što su buduće poslovne strategije.

Privatno. U ovu kategoriju spadaju privatni podaci namenjeni internoj upotrebi u okviru organizacije. Svako neovlašćeno otkrivanje privatnih podataka (a naročito obmanjivačima) moglo bi ozbiljno oštetiti zaposlene ili firmu. U privatne podatke ubrajamo zdravstvene podatke o zaposlenima, podatke o njihovim bankovnim računima, istorijat o plati, kao i sve druge slične informacije koje nisu za javnost.

napomena

Interne informacije se često nazivaju osetljivima. Ja sam odabrao izraz „interne“ zato što govori i o tome kome su informacije namenjene. Izraz „osetljive“ nisam koristio kao bezbednosnu klasifikaciju, već kao zgodan način da ukažem na sve poverljive, privatne i interne informacije. Drugim rečima, „osetljive“ informacije su sve one kompanijske informacije koje nisu posebno namenjene javnosti.

Interno. Ovi podaci se mogu slobodno davati svim zaposlenima u organizaciji. Obično se ne očekuje da će neovlašćeno objavljivanje internih informacija naneti ozbiljnu štetu firmi, deoničarima, poslovnim partnerima, klijentima, ili zaposlenima. Međutim, vešti obmanjivači mogu da upotrebe takve informacije da bi se predstavili kao zaposleni, privremeni radnici, ili dobavljači, i na taj način izmamili osetljivije podatke od nepripremljenog osoblja i tako neovlašćeno pristupili računarskim sistemima firme.

Pre nego što se interne informacije saopšte trećim licima (kao što su osoblje dobavljača, privremeni radnici, poslovni partneri i tako dalje) mora se potpisati dogovor o poverljivosti podataka. Internim informacijama uglavnom pripada sve što se svakodnevno koristi u poslovanju, a što se ne sme saopštavati trećim licima, kao što su organizaciona struktura firme, pozivni brojevi za priključenje na mrežu, interni nazivi sistema, postupci za daljnjski pristup, kontni brojevi i tako dalje.

Javno. To su podaci posebno namenjeni javnosti. Oni se mogu slobodno davati svima, u izjavama za štampu, u kontaktu s korisnicima, ili u brošurama o proizvodima. Imajte na umu da sve informacije koje nisu naročito definisane kao javne treba smatrati osjetljivima.

Terminologija u klasifikaciji podataka

Klasifikacija podataka određuje kategorije ljudi kojima se može dati neka informacija. U nekim pravilima u ovom poglavlju govori se o tome da informacije ne treba davati *neproverenoj osobi*. Neproverena osoba je kolega koga radnik ne poznaje lično, za koga nije siguran da je ovlašćen za pristup informacijama, odnosno neko za koga ne garantuje osoba od poverenja.

Ovde *osobom od poverenja* nazivamo nekoga koga ste lično upoznali ili ga poznajete kao kolegu, klijenta ili savetnika kompanije koji ima odgovarajuću poziciju da bi pristupio informacijama. Osoba od poverenja bi takođe mogla biti u nekom odnosu s vašim preduzećem (na primer, kupac, dobavljač ili poslovni partner koji je potpisao ugovor o poverljivosti informacija).

Garancija trećeg lica znači da osoba od poverenja potvrđuje identitet i status zaposlenog, kao i to da li je ovlašćen da pristupi informacijama ili podnese zahtev. Imajte na umu da je neophodno proveriti da li osoba od poverenja još uvek radi u preduzeću pre nego što odobri davanje informacija nekome za koga garantuje.

Privilegovan nalog je računarski ili drugi nalog za koji je potrebna dozvola, na primer nalog administratora sistema. Zaposleni s privilegovanim nalogima uglavnom mogu da menjaju ovlašćenja korisnika ili upravljaju sistemskim funkcijama.

Glasovna pošta odeljenja služi za ostavljanje glasovnih poruka za ceo odelsek. Koristi se da bi se zaštitila imena i brojevi lokala radnika u tom odeljenju.

POSTUPCI ZA PROVERU I OVLAŠĆIVANJE

Kradljivci informacija obično upotrebljavaju veštine obmanjivanja da bi pristupili poverljivim poslovnim informacijama ili ih zadobili. Izdaju se za zaposlene privremene radnike, dobavljače, ili poslovne partnere. Da bi se informacije efikasno zaštitile, zaposleni od kog se zahteva da nešto uradi ili saopšti osetljive informacije mora tačno identifikovati sagovornika i proveriti njegova ovlašćenja.

Postupci preporučeni u ovom poglavlju osmišljeni su da pomognu zaposlenom od koga se nešto zahteva putem komunikacionih medija kao što su telefon, elektronska pošta, ili faks.

Zahtevi koje podnosi osoba od poverenja

Kada osoba od poverenja zahteva informacije ili usluge, obično se postupa na sledeći način:

- Proverava da li ta osoba još uvek aktivno radi u preduzeću, odnosno da li ispunjava uslove za pristup određenoj kategoriji informacija. To se radi da se bivši zaposleni, dobavljači, privremeni radnici i drugi koji više nisu u vezi sa kompanijom ne bi predstavljali kao aktivno osoblje.
- Proverava da li je ta osoba ovlašćena da primi podatke, i da pristupi informacijama, odnosno da zahteva uslugu.

Zahtevi koje podnosi neproverena osoba

Kada zahtev podnosi neproverena osoba, mora se zasigurno utvrditi identitet podnosioca zahteva, odnosno ovlašćenja za pristup željenim podacima, a naročito kada je zahtev u bilo kakvoj vezi s računarima ili pratećom opremom. To je osnovno sredstvo za sprečavanje obmanjivanja.

Važno je da postupak ne bude toliko mukotrpan da prestane da bude isplativ i da ga zaposleni ignorišu.

Kao što je ovde objašnjeno, postupak provere ima tri faze:

- Proveru identiteta osobe.
- Utvrđivanje da li je podnosilac zahteva trenutno zaposlen ili je u takvoj vezi s firmom da mu je odobren pristup podacima.
- Proveru da li je osoba ovlašćena da primi određene informacije, ili da zahteva usluge.

Prvi korak: provera identiteta

Koraci preporučeni za proveru identiteta navedeni su prema efikasnosti – što im je redni broj veći, to su efikasniji. Uz svaki postupak navedeni su i nedostaci, kao i način na koji obmanjivač može nadmudriti ili prevariti zaposlene.

1. **Identifikator poziva** (uz pretpostavku da ta funkcija postoji u telefonskom sistemu kompanije). Sa ekrana identifikatora utvrdite da li poziv dolazi iz firme ili izvan nje, i da li ime i telefonski broj sagovornika odgovaraju podacima kojima se sagovornik predstavio.

Nedostatak: Podatke prikazane na identifikatoru poziva upućenog izvan firme može falsifikovati svako ko može pristupiti lokalnoj centrali povezanoj s digitalnom centralom.

2. **Uzvratanje poziva.** Potražite podnosioca zahteva u imeniku preduzeća, i pozovite navedeni lokal da biste proverili da li je zaista zaposlen u kompaniji.

Nedostatak: Dovoljno vešt napadač može preusmeriti pozive upućene lokalu tako da, kada zaposleni uzvratu poziv da bi proverio broj naveden u imeniku, dobije napadačev spoljni telefonski broj.

3. **Garantovanje.** Osoba od poverenja koja garantuje za podnosioca zahteva treba da potvrdi njegov identitet.

Nedostatak: Napadači koji se lažno predstavljaju često mogu da ubede drugog zaposlenog u svoj navodni identitet, te da ga navedu da garantuje za njih.

4. **Deljena tajna.** Upotrebljavajte tajnu koju znaju svi u preduzeću, kao što je lozinka ili dnevni kôd.

Nedostatak: Ako mnogo ljudi zna tajnu, i napadač lako može doći do nje.

5. **Nadzornik/predpostavljeni zaposlenog.** Telefonirajte pretpostavljenom zaposlenog i proverite njegov identitet.

Nedostatak: Ako je podnosilac zahteva dao telefonski broj svog pretpostavljenog, osoba koja se javi kada se pozove navedeni broj možda nije pravi rukovodilac, već je saučesnik u napadu.

6. Bezbedna elektronska pošta. Zahtevajte digitalno potpisane poruke.

Nedostatak: Ako je napadač već pristupio računaru zaposlenog i instalirao program za snimanje tastature da bi se domogao njegove lozinke, može poslati poruku s digitalnim potpisom zaposlenog.

7. Prepoznavanje glasa osobe. Osoba koja primi poziv već se susretala s podnosiocem zahteva, sigurno zna da je to osoba od poverenja, i dovoljno je poznaje da bi prepoznala njen glas preko telefona.

Nedostatak: To je prilično bezbedna metoda koju napadač ne može lako da zaobiđe, ali ničemu ne služi ako se osoba od koje se nešto zahteva nikada nije susrela s podnosiocem niti je razgovarala s njim.

8. Upotreba promenljive lozinke. Podnosilac zahteva se identifikuje pomoću uređaja na kome se lozinke periodično menjaju.

Nedostatak: Da bi nadmudrio ovu metodu, napadač bi morao da se domogne jednog uređaja na kome se lozinke periodično menjaju, kao i odgovarajućeg PIN koda zaposlenog kome pomenuti uređaj pripada, ili bi morao da na prevaru navede zaposlenog da mu pročita podatke prikazane na uređaju i da mu kaže svoj PIN kôd.

9. Lično pojavljivanje uz identifikacioni dokument. Podnosilac zahteva se pojavi lično i pokaže propusnicu ili drugi odgovarajući identifikacioni dokument, po mogućstvu sa slikom.

Nedostatak: Napadači mogu da ukradu propusnice, ili naprave lažne propusnice koje izgledaju kao prave. Međutim, oni se često klone toga. Kada se lično pojave, dovode sebe u rizičnu situaciju jer ih mogu razotkriti i uhvatiti.

Drugi korak: provera statusa zaposlenog

Najveću opasnost po bezbednosni sistem ne predstavljaju profesionalni obmanjivači, niti vešti napadači na računarske sisteme, već bliski ljudi: nedavno otpušteni radnici koji žele da se osvete ili se nadaju da će imati koristi od informacija ukradenih iz bivše firme. (Imajte na umu da se verzija ovog postupka može primeniti i da bi se proverilo da li je neko još uvek u vezi s vašom kompanijom, poput dobavljača, savetnika ili radnika po ugovoru.)

Pre nego što obelodanite osetljive informacije ili pristanete na nečija uputstva u vezi s računarima ili pratećom opremom, na jedan od sledećih načina proverite da li je podnosilac zahteva još uvek zaposlen u firmi:

Provera zaposlenog pomoću imenika. Ako je preduzeće objavilo imenik zaposlenih na mreži, koji se aktivno ažurira, proverite da li je podnosilac zahteva još uvek na spisku.

Provera preko pretpostavljenog podnosioca zahteva. Pozovite pretpostavljenog podnosioca zahteva na telefonski broj koji se nalazi u imeniku preduzeća, a ne na onaj koji vam je sagovornik dao.

Provera preko odeljenja u kom radi podnosilac zahteva ili preko njegove radne grupe. Pozovite odeljenje u kom radi podnosilac zahteva ili njegovu radnu grupu i proverite u razgovoru s bilo kim iz dotičnog odeljenja ili radne grupe da li je ta osoba još uvek zaposlena.

Treći korak: provera ovlašćenja za dobijanje informacija

Pored provere da li je zaposleni još uvek u radnom odnosu ili da li je u vezi s vašim preduzećem, još uvek se postavlja pitanje da li je podnosilac zahteva ovlašćen da pristupi željenim informacijama, odnosno da zatraži uslugu u vezi sa računarima ili pratećom opremom.

To se može učiniti na jedan od sledećih načina:

Pogledajte spisak pozicija/radnih grupa/odgovornosti. Preduzeće može objaviti spiskove zaposlenih koji imaju pravo pristupa određenim informacijama. Ti spiskovi se mogu organizovati prema pozicijama zaposlenih, odeljenjima i radnim grupama, odgovornostima, ili nekoj kombinaciji pomenutih činilaca. Takve spiskove valja postaviti na intranet da bi se ažurirali i da bi im se brzo moglo pristupiti. Obično su osobe odgovorne za informacije zadužene za nadgledanje, izradu i održavanje takvih spiskova.

napomena

Bitno je imati na umu da su spiskovi pozicija i odgovornosti mamac za obmanjivače. Razmislite o tome: ako potencijalni napadač sazna da firma ima takve spiskove, biće izuzetno motivisan da dođe do primerka. Kada ih se domogne, otvorena su mu mnoga vrata i može narušiti bezbednost firme.

Zatražite odobrenje od pretpostavljenog. Zaposleni razgovara sa svojim pretpostavljenim, ili rukovodiocem sagovornika i zatraži odobrenje da ispuni zahtev.

Zatražite odobrenje od osobe odgovorne za informacije ili njegovog zamenika. Odgovorni za informacije prosuđuje da li se nekome sme odobriti pristup podacima. Postupak podnošenja zahteva za pristup informacijama u računarskim sistemima podrazumeva da zaposleni razgovara s pretpostavljenim, koji će odluku doneti na osnovu tekućeg pravilnika firme. Ako takav pravilnik ne postoji, rukovodilac treba da pozove osobu odgovornu za informacije, i da traži dozvolu. Te se strukture valja pridržavati, da odgovori na informacije ne bi bili preopterećeni prečestim zahtevima.

Zatražite odobrenje putem specijalnog softverskog paketa. Velike kompanije u konkurentnim granama industrije mogu da razviju poseban softverski paket koji će odobravati pristup podacima. U takvu bazu podataka se pohranjuju imena zaposlenih i njihova ovlašćenja za pristup klasifikovanim informacijama. Korisnici ne bi mogli da vide tuđa ovlašćenja, već bi uneli ime podnosioca zahteva i identifikator željenih informacija. Softver bi potom ukazao na to da li osoba ima pravo da pristupi takvom podatku. Na taj način se izbegava opasnost koja pretila od krađe spiska osoblja s pravima pristupa vrednim, važnim, ili osetljivim informacijama.

PRAVILA ZA RUKOVODSTVO

Sledeća pravila se odnose na upravu firme. Podelili smo ih u oblasti klasifikacije podataka, saopštavanja informacija, administracije telefonskih poziva, i drugih pravila. Primetićete da su u svakoj od tih oblasti korišćene drugačije oznake radi lakšeg pronalaženja pojedinih pravila.

Pravila klasifikacije podataka

Klasifikacija podataka se odnosi na to kako vaša kompanija grupiše informacije prema osetljivosti, kao i na to ko bi trebalo da ima pristup njima.

1-1 Organizujte klasifikaciju podataka

Pravilo: Osoba odgovorna za informacije ili njen zamenik mora klasifikovati sve značajne, osetljive, ili važne poslovne informacije u odgovarajuće kategorije.

Objašnjenje/Napomene: Osoba odgovorna za informacije ili njen zamenik klasifikovaće svaki podatak koji se svakodnevno koristi u poslovanju. Oni takođe odobravaju pristup tim informacijama i određuju u koje svrhe se mogu koristiti. Mogu menjati klasifikaciju ili odrediti neki period za automatsku deklasifikaciju.

Svaki podatak koji ne nosi nikakvu oznaku trebalo bi klasifikovati kao „osetljivi“.

1-2 Objavite pravila za rad s klasifikovanim podacima

Pravilo: Firma mora utvrditi postupke u vezi sa saopštavanjem informacija iz svake pojedine kategorije.

Objašnjenje/Napomene: Kada se podaci klasifikuju, moraju se utvrditi i postupci saopštavanja informacija kolegama i osobama koji nisu zaposleni u preduzeću, kao što smo već naglasili u odeljku „Postupci za proveru i ovlašćivanje“ ranije u ovom poglavlju.

1-3 Označite sve podatke

Pravilo: Jasno označite odgovarajućom klasom štampani materijal i medije sa snimljenim dokumentima koji sadrže poverljive, privatne, ili interne informacije.

Objašnjenje/Napomene: Na naslovnoj i svakoj sledećoj strani štampanog dokumenta mora se jasno videti klasifikaciona oznaka.

Sve elektronske datoteke koje se ne mogu lako obeležiti klasifikacionim oznakama (na primer, baze podataka ili datoteke sa neobrađenim podacima) moraju se zaštititi kontrolisnjem pristupa da bi se sprečilo njihovo slučajno obelodanjivanje, menjanje, uništavanje, ili onemogućavanje pristupa.

Svi računarski mediji poput disketa, traka i CD-ova moraju se označiti najvišom klasom kojoj pripadaju pojedine informacije na njima.

Saopštavanje informacija

U ovu grupu ubrajamo pravila za obelodanjivanje informacija raznim osobama na osnovu njihovog identiteta i ovlašćenja.

2-1 Postupak provere zaposlenih

Pravilo: Trebalo bi utvrditi sveobuhvatne postupke koje bi radnici koristili za proveru identiteta, statusa u firmi i ovlašćenja pre nego što bilo kome daju poverljive ili osetljive informacije, ili učine bilo kakve uslugu u vezi sa računarima ili softverom.

Objašnjenja/Napomene: Za utvrđivanje identiteta mogu se primeniti napredna tehnološka rešenja, tamo gde troškove opravdavaju veličina kompanije i potrebe obezbeđenja. Najbolje je upotrebljavati identifikacione

oznake, kao i deljenu tajnu, da bi se podnosioci zahteva zasigurno identifikovali. Iako bi to značajno smanjilo rizik, troškovi bi bili isuviše veliki za neke firme. U takvim okolnostima, u firmi bi trebalo koristiti tajni podatak koji znaju svi zaposleni, kao što je dnevna lozinka ili kôd.

2-2 Saopštavanje informacija trećim licima

Pravilo: Mora se objaviti skup procedura preporučenih za saopštavanje informacija, a sve zaposlene valja obučiti da ih se pridržavaju.

Objašnjenje/Napomene: Uglavnom, postupke za saopštavanje informacija treba utvrditi za:

- Objavljivanje podataka unutar kompanije.
- Davanje informacija pojedincima i zaposlenima organizacija koje su u nekom poslovnom odnosu s preduzećem, kao što su savetnici, radnici na određeno vreme, stažisti, zaposleni u kompaniji dobavljača ili poslovnih partnera i tako dalje.
- Objavljivanje informacija van kompanije.
- Sve klasifikovane podatke kada se saopštavaju lično, telefonom, elektronskom poštom, faksimilom, glasovnom poštom, pismom, kurirskom službom i elektronskim prenosom.

2-3 Saopštavanje poverljivih informacija

Pravilo: Poverljive informacije, koje bi firmi mogle naneti znatnu štetu ako bi pale u ruke neovlašćenih osoba, mogu se obelodaniti samo osobi od poverenja ovlašćenoj da ih primi.

Objašnjenje/Napomene: Poverljivi podaci u fizičkom obliku (tj. štampani materijal ili izmenljivi medij za snimanje) mogu se davati:

- Lično.
- Internom poštom, zapečaćeni i označeni klasifikacionom oznakom „poverljivo“.
- Van firme – kurirskom službom od poverenja, pri čemu se zahteva potpis primaoca, ili preporučenom poštom.

Poverljive informacije u elektronskom obliku (računarske datoteke, baze podataka, elektronska pošta itd.) mogu se slati:

- Šifrovanim elektronskim porukama.
- Kao šifrovani prilozi elektronskih poruka.

- Elektronskim prenosom do servera u okviru interne kompanijske mreže.
- Faks programom sa računara, ako samo korisnik kome je informacija namenjena koristi faks, ili ako primalac čeka kraj faks uređaja. Druga opcija je da se faksimili šalju bez prisustva primaoca, ako se koristi šifrovana telefonska veza do faks servera zaštićenog lozinkom.

O poverljivim informacijama se može razgovarati lično, telefonom u okviru firme, telefonom van firme ako je veza šifrovana, šifrovanim satelitskim prenosom, šifrovanom vezom za videokonferencije i šifrovanim protokolom za prenos glasa preko Interneta (engl. *Voice Over Internet Protocol, VoIP*).

Za prenos faksom, preporučuje se da pošiljalac prvo pošalje naslovnu stranu. Nakon prijema, primalac pošalje jednu stranu nazad, kako bi dokazao da se nalazi kraj prijemnog faksa. Pošiljalac potom pošalje celu faks poruku.

Sledeća komunikaciona sredstva nisu prihvatljiva za prenos poverljivih informacija ili razgovor o njima: nešifrovana elektronska pošta, glasovne poruke, obična pisma, niti bilo koji oblik bežične komunikacije (mobilni telefoni, SMS poruke, bežični telefoni).

2-4 Saopštavanje privatnih informacija

Pravilo: Privatne informacije koje u slučaju obelodanjivanja mogu naškoditi zaposlenom ili kompaniji, mogu se saopštavati samo ovlašćenoj osobi od poverenja.

Objašnjenje/Napomene: Privatni podaci u fizičkom obliku (tj. štampani materijal ili izmenljivi medij za snimanje) mogu se davati:

- Lično.
- Internom poštom, zapečaćeni i označeni klasifikacionom oznakom „privatno“.
- Običnom poštom.

Privatni podaci u elektronskom obliku (računarske datoteke, baze podataka, elektronska pošta itd.) mogu se slati:

- Internom elektronskom poštom.
- Elektronskim prenosom do servera u okviru kompanijske interne mreže.

- Faksom, ako samo korisnik kome je informacija namenjena koristi određeni faks uređaj, ili ako primalac čeka kraj faks uređaja. Faksimili se mogu slati i do faks servera zaštićenih lozinkama. Druga opcija je da se faksimili šalju bez prisustva primaoca, ako se koristi šifrovana telefonska veza do faks servera zaštićenog lozinkom.

O privatnim informacijama se može razgovarati lično, telefonom, satelitskim prenosom, u okviru videokonferencije, i šifrovanim protokolom za prenos glasa preko Interneta (engl. *Voice Over Internet Protocol, VoIP*).

Sledeća komunikaciona sredstva nisu prihvatljiva za prenos privatnih informacija ili razgovor o njima: nešifrovana elektronska pošta, glasovne poruke, obična pisma, niti bilo koji oblik bežične komunikacije (mobilni telefoni, SMS poruke, bežični telefoni).

2-5 Saopštavanje internih informacija

Pravilo: Interne informacije se mogu davati u okviru firme ili drugim poverljivim osobama koje su potpisale ugovor o tajnosti. Morate utvrditi pravila za distribuciju internih informacija.

Objašnjenje/Napomene: Interne informacije se mogu saopštavati u bilo kom obliku, uključujući i internu elektronsku poštu, ali se ne smeju slati van preduzeća elektronskim porukama koje nisu šifrovane.

2-6 Razgovor o osetljivim informacijama preko telefona

Pravilo: Pre nego što se preko telefona obelodani bilo koji podatak koji nije izričito označen kao javni, osoba koja objavljuje informacije mora lično prepoznati glas podnosioca zahteva, ili kompanijski telefonski sistem mora utvrditi da je poziv upućen s internog telefonskog broja dodeljenog podnosiocu zahteva.

Objašnjenje/Napomene: Ako vam glas podnosioca zahteva nije poznat, pozovite ga na interni telefonski broj da biste uporedili njegov glas sa snimljenom glasovnom porukom, ili neka vam njegov pretpostavljeni potvrdi identitet i ovlašćenja.

2-7 Postupci za obezbeđenje na ulazu ili za službenike prijemnog odeljenja

Pravilo: Osoblje prijemnog odeljenja mora zahtevati identifikaciju s fotografijom pre nego što preda bilo koji paket osobi za koju se ne zna

zasigurno da li je trenutno zaposlena u firmi. Treba voditi dnevnik u kom bi se beležilo ime osobe, broj lične karte, datum rođenja, preuzeti predmet, i datum i vreme preuzimanja.

Objašnjenje/Napomene: Ovo pravilo se odnosi i na predaju poslatih paketa bilo kojoj kurirskoj službi. Njihovi zaposleni nose odgovarajuće identifikacije.

2-8 Slanje softvera trećim licima

Pravilo: Pre slanja ili objavljivanja bilo kog programa ili uputstva za računare, morate zasigurno utvrditi identitet podnosioca zahteva, kao i da li je zahtev u skladu s kategorijom kojoj ti podaci pripadaju. Obično se izvorni kôd softvera smatra izuzetno osetljivom materijom i klasifikuje se kao poverljiv.

Objašnjenje/Napomene: Utvrđivanje ovlašćenja se obično zasniva na tome da li je podnosiocu zahteva potreban pristup softveru za obavljanje posla.

2-9 Procena potencijalnih kupaca u komercijali i marketingu

Pravilo: Zaposleni u komercijali i marketinškom odeljenju moraju proceniti potencijalne kupce pre nego što im daju interne telefonske brojeve, planove proizvoda, telefone i adrese proizvodnog tima, ili druge osetljive informacije.

Objašnjenje/Napomene: Industrijski špijuni često u razgovoru komercijalistima i zaposlenim u marketinškom odeljenju tvrde da će možda otkupiti veliku količinu robe. Pokušavajući da iskoriste priliku za prodaju, ti zaposleni često obelodane informacije na osnovu kojih napadač može da se domogne osetljivih podataka.

2-10 Prenos datoteka ili podataka

Pravilo: Datoteke i druge elektronske podatke ne treba smeštati ni na kakav izmenljiv medij ukoliko to ne naloži osoba od poverenja čiji se identitet zasigurno zna i ko je ovlašćen da poseduje takve podatke u tom obliku.

Objašnjenje/Napomene: Obmanjivači lako mogu da prevare zaposlene, dajući im realne razloge, da im snime osetljive informacije na traku, Zip disk, ili neki drugi izmenljivi medij, i da im ih pošalju ili ostave u holu da ih neko preuzme.

Administracija telefonskih poziva

Pravilima administracije telefonskih poziva obezbeđuje se da radnici mogu utvrditi identitet sagovornika i zaštititi broj svog lokala od lica koja zovu.

3-1 Prosleđivanje poziva na faks ili modemskim vezama

Pravilo: Usluga prosleđivanja poziva do telefonskih brojeva van firme ne sme se instalirati ni na jednu faks, niti modemsku vezu u kompaniji.

Objašnjenje/Napomene: Vrsni napadači mogu pokušati da prevare osoblje telefonske kompanije ili interne radnike na telekomunikacijama da proslede interne pozive do spoljnih telefonskih linija kojima upravlja napadač. Na taj način, uljez se može domoći poslatih faksova, zahtevati da se poverljive informacije pošalju u okviru firme (osoblje smatra da je slanje podataka u okviru organizacije bezbedno), ili će na prevaru saznati lozinke korisnika modemske veze preusmeravanjem pristupne linije na svoj računar i simuliranjem postupka prijavljivanja za rad.

U zavisnosti od telefonske usluge koja se koristi u okviru firme, prosleđivanjem poziva može upravljati dobavljač telekomunikacionih usluga, a ne odeljenje za telekomunikacije u kompaniji. U tom slučaju, valja zahtevati od dobavljača telekomunikacionih usluga da isključi prosleđivanje poziva sa svih faks i modemskih veza.

3-2 Identifikacija poziva

Pravilo: U kompanijskom telefonskom sistemu mora se obezbediti identifikacija poziva na svim internim telefonskim aparatima i, ako je moguće, telefon treba podesiti tako da zvoni drugačije kada poziv stiže izvan firme.

Objašnjenje/Napomene: Mogućnost da se identifikuju telefonski pozivi upućeni izvan firme može biti korisna za sprečavanje napada, ili prijavljivanje napadača obezbeđenju.

3-3 Telefoni u javnim prostorijama

Pravilo: Da posetioци ne bi mogli da se predstavljaju kao zaposleni u firmi, pri svakom pozivu s telefona iz javne prostorije treba jasno da bude naznačena lokacija sagovornika (na primer, „Hol“) na identifikatoru poziva.

Objašnjenje/Napomene: Ako se na identifikatoru poziva prikazuje samo broj lokala, lokali u prijemnom odeljenju ili bilo kojoj drugoj javnoj prostoriji moraju biti specijalno označeni. Napadaču se ne sme omogućiti

da pozove s jednog od tih telefona i navede radnika da poveruje da je poziv uputio interno, iz druge kancelarije.

3-4 Podrazumevane lozinke na telefonskim sistemima

Pravilo: Administrator glasovnih poruka bi trebalo da promeni sve podrazumevane lozinke na telefonskom sistemu pre upotrebe.

Objašnjenje/Napomene: Obmanjivači mogu da nabave spiskove podrazumevanih lozinki od proizvođača i da pomoću njih pristupe administratorskim nalogima.

3-5 Glasovna pošta za čitavo odeljenje

Pravilo: Podesite glasovnu poštu za svako odeljenje koje obično kontaktira s javnošću.

Objašnjenje/Napomene: Prvi korak u obmanjivanju je prikupljanje informacija o ciljnoj kompaniji i njenom osoblju. Ograničavanjem pristupa imenima i telefonskim brojevima radnika, napadačima se otežava da identifikuju žrtve zaposlene u firmi, ili da saznaju imena radnika koja bi iskoristili da prevare njihove kolege.

3-6 Provera proizvođača telefonskih sistema

Pravilo: Nijednom tehničaru iz podrške proizvođača ne sme se dozvoliti da daljinski pristupi kompanijskom telefonskom sistemu, ukoliko proizvođač nije potvrdio njegov identitet i ukoliko nije ovlašćen za takav posao.

Objašnjenje/Napomene: Osobe koje na prevaru pristupe kompanijskim telefonskim sistemima mogu da naprave sebi glasovnu poštu, da se domognu poruka namenjenih drugima, ili da besplatno telefoniraju na račun firme.

3-7 Podešavanje telefonskog sistema

Pravilo: Administrator glasovne pošte mora nametnuti bezbednosna pravila podesivši odgovarajuće zaštitne parametre u telefonskom sistemu.

Objašnjenje/Napomene: Telefonski sistemi se mogu podesiti tako da glasovna pošta bude jače ili slabije obezbeđena. Administrator mora biti obavešten o problemima bezbednosti firme; mora sarađivati s obezbeđenjem tako što će podesiti telefonski sistem da se zaštite osetljivi podaci.

3-8 Pronalaženje sagovornika

Pravilo: U zavisnosti od ograničenja dobavljača telekomunikacionih usluga, funkcija pronalaženja sagovornika omogućava svim zaposlenima da otkriju lokaciju sagovornika kada posumnjaju da je napadač.

Objašnjenje/Napomene: Zaposleni se moraju obučiti da upotrebe pomenutu funkciju kada neovlašćeni sagovornik očigledno pokušava da pristupi računarskom sistemu preduzeća ili traži osetljive informacije. Kadgod neko aktivira funkciju pronalaženja sagovornika, mora odmah o tome obavestiti obezbeđenje.

3-9 Automatski telefonski sistemi

Pravilo: Ako kompanija koristi automatski telefonski sistem, njega treba programirati tako da se lokali ne objavljuju pri prebacivanju poziva zaposlenom ili odeljenju.

Objašnjenje/Napomene: Napadači mogu da iskoriste automatski telefonski sistem da bi povezali imena zaposlenih s njihovim telefonskim loklima. Potom taj podatak mogu da upotrebe da bi se žrtvama predstavili kao ovlašćene kolege.

3-10 Onemogućavanje glasovne pošte nakon određenog broja uzastopnih neuspešnih pokušaja pristupa

Pravilo: Programirajte telefonski sistem firme tako da se svaki nalog glasovne pošte isključi nakon izvesnog broja uzastopnih neuspešnih pokušaja pristupa.

Objašnjenje/Napomene: Administrator telekomunikacionog sistema mora isključiti glasovnu poštu nakon pet uzastopnih neuspešnih pokušaja prijavljivanja. Takav nalog se kasnije može uključiti samo ručno, na specijalan zahtev.

3-11 Interni telefonski lokali

Pravilo: Sve interne telefonske lokale odeljenja i radnih grupa koje obično ne primaju spoljne pozive (kao što su korisnička podrška, računarski centar, tehnička podrška i tako dalje) valja programirati tako da se ti telefoni mogu zvati samo s drugih internih lokala. Druga mogućnost je da se zaštite lozinkom koju zaposleni i druge ovlašćene osobe koje zovu izvan firme moraju uneti.

Objašnjenje/Napomene: Iako se na ovaj način sprečava većina napada obmanjivača amatera, valja imati na umu da će odlučni napadač ponekad uspeti da nagovori zaposlenog da pozove interni lokal i zamoli osobu koja se javi da pozove napadača, ili da ga spoji s takvim odeljenjem. U okviru bezbednosne obuke treba obavestiti zaposlene o ovom načinu na koji napadač na prevaru navodi radnike da mu pomognu.

Razno

4-1 Izgled propusnica zaposlenih

Pravilo: Na propusnicama zaposlenih mora se nalaziti velika slika koja se može prepoznati iz daljine.

Objašnjenje/Napomene: Standardne fotografije na kompanijskim propusnicama su gotovo beskorisne, kada je u pitanju obezbeđenje. Razdaljina između osobe koja ulazi u zgradu i čuvara ili službenika prijemnog odeljenja je obično dovoljno velika da se sa male slike ne može jasno videti da li je to upravo osoba koja ulazi. Da bi slika bila od koristi u tim situacijama, izgled propusnica se mora izmeniti, ako je neophodno.

4-2 Provera prava pristupa pri izmeni pozicija ili odgovornosti

Pravilo: Uvek kada zaposleni promeni poziciju ili mu se doda, odnosno umanjí odgovornost, njegov pretpostavljeni mora o tome da obavesti informatički tim da bi mu se dodelio odgovarajući bezbednosni profil.

Objašnjenje/Napomene: Nadgledanje prava pristupa osoblja je neophodno da bi se ograničilo odavanje zaštićenih informacija. Primenjuje se pravilo *najnižih privilegija*: korisnicima se dodeljuju minimalna prava neophodna za obavljanje posla. Ako neko zahteva veća prava, to mora biti u skladu s pravilnikom.

Rukovodilac zaposlenog ili kadrovsko odeljenje biće zaduženi za obaveštavanje informatičkog odeljenja da na odgovarajući način promene korisnikova prava pristupa.

4-3 Posebna identifikacija posetilaca firme

Pravilo: Trebalo bi da kompanija izdaje posebne oznake kuririma i posetiocima od poverenja koji iz poslovnih razloga redovno borave u firmi.

Objašnjenje/Napomene: Posetioci koji redovno dolaze u zgradu firme (na primer, da bi dostavili hranu ili pića u restoran, ili da bi popravili

mašine za fotokopiranje ili telefonske instalacije) mogu predstavljati opasnost. Osim toga što ćete izdati propusnice takvim posetiocima, obavezno obučite ljude da zapaze ako neko od njih nema oznaku i da znaju kako da postupe u toj situaciji.

4-4 Gašenje računarskih naloga privremenim radnicima

Pravilo: Kada privremeni radnik kome je bio dodeljen računarski nalog završi svoj zadatak, ili kad mu istekne ugovor, zaduženi rukovodilac mora odmah o tome da obavesti informatičko odeljenje da bi ugasili odgovarajuće računarske naloge, uključujući i naloge za pristup bazama podataka, za povezivanje na mrežu ili daljinski pristup Internetu.

Objašnjenje/Napomene: Kada radnik više nije zaposlen u firmi, postoji opasnost da će upotrebiti svoje poznavanje sistema i postupaka da bi pristupio podacima. Svi računarski nalozi koje je radnik koristio ili znao moraju se odmah ugasiti. Tu ubrajamo i naloge za pristup proizvodnim bazama podataka, za daljinsko povezivanje na mrežu, i pristup uređajima vezanim za računare.

4-5 Tim za evidentiranje incidenata

Pravilo: Valja organizovati tim za evidentiranje incidenata ili, u manjim firmama, odrediti osobu kojoj će se takvi događaji prijavljivati, i njenog zamjenika. Oni će primati i oglašavati uzbunu prilikom potencijalnih narušavanja bezbednosnog sistema.

Objašnjenje/Napomene: Centralizovanjem prijavljivanja potencijalnih bezbednosnih incidenata može se otkriti napad koji bi inače verovatno prošao neopažen. U slučaju da se otkriju i prijave sistematski napadi širom organizacije, tim za evidentiranje incidenata mogao bi da utvrdi metu napadača da bi se uložili posebni napor u zaštitu tih sredstava.

Zaposleni u timu za evidentiranje incidenata moraju se upoznati s metodama obmanjivača, jer će tako moći da procene prijave i prepoznaju eventualni napad dok je još u toku.

4-6 Posebna telefonska linija za evidentiranje incidenata

Pravilo: Treba dodeliti posebnu telefonsku liniju timu ili osobi za evidentiranje incidenata. To može biti lokal koji se lako pamti.

Objašnjenje/Napomene: Zaposlenima se mora omogućiti da odmah obaveste tim za evidentiranje incidenata kada posumnjaju na prevaru. Da bi obaveštenje bilo upućeno na vreme, svi operateri na telefonskoj centrali i službenici prijemnog odeljenja moraju držati taj broj na vidnom mestu ili tamo gde ga lako mogu pronaći.

Sistem ranog upozoravanja širom kompanije može značajno pomoći organizaciji u otkrivanju i suzbijanju tekućeg napada. Zaposleni se moraju dovoljno dobro obučiti tako da odmah pozovu telefonski broj za evidentiranje incidenata u slučaju problema. U skladu s objavljenim pravilnikom, tim za evidentiranje incidenata odmah će obavestiti ciljne grupe da je napad možda u toku i da treba da budu oprezni. Da bi svi bili obavešteni na vreme, broj posebne telefonske linije za evidentiranje incidenata mora biti poznat svima širom kompanije.

4-7 Osetljive oblasti valja zaštititi

Pravilo: Čuvar treba da štiti ulaz u osetljive ili obezbeđene oblasti. Za pristup njima valja zahtevati dva oblika identifikacije.

Objašnjenje/Napomene: Jedan prihvatljiv oblik identifikacije je primena digitalne elektronske brave kroz koju zaposleni mora da provuče propusnicu i unese šifru. Najbolja metoda obezbeđivanja osetljivih oblasti je da se postavi čuvar koji nadgleda ulaz. U organizacijama u kojima to nije isplativo, valja koristiti dve vrste identifikacije. U zavisnosti od rizika i cene, preporučujem biometričke kartice za odobrenje pristupa.

4-8 Mrežni i telefonski ormarići

Pravilo: Ormarići, kabineti, ili prostorije u kojima se nalaze mrežni kablovi, telefonske žice ili mesta za pristup mreži moraju se stalno čuvati.

Objašnjenje/Napomene: Samo se ovlašćenom osoblju može odobriti pristup telefonskim i mrežnim ostavama, prostorijama, ili ormarićima. Svi koji rade na održavanju, a nisu zaposleni, kao i osoblje dobavljača usluga, moraju se identifikovati propisanim postupcima. Napadač može iskoristiti pristup telefonskim linijama, mrežnim čvorištima, razvodnicima, mostovima, ili drugoj sličnoj opremi, da bi narušio bezbednost računarskih i mrežnih sistema.

4-9 Sandučići za internu poštu

Pravilo: Sandučići za internu poštu ne smeju se smeštati blizu javnih prostorija u firmi.

Objašnjenje/Napomene: Industrijski špijuni i hakeri koji imaju pristup mestima za prikupljanje interne pošte u firmi lako mogu da pošalju lažna pisma ovlašćenja ili interne formulare kojima ovlašćuju osoblje da im oda poverljive informacije ili da na drugi način pomogne napadaču. Uz to, napadač može poštom da pošalje diskete ili elektronske medije sa uputstvima da se instalira nova verzija softvera, ili da se otvori zlonamerna datoteka. Naravno, smatra se da je svaki zahtev koji se primi putem interne pošte odobren.

4-10 Kompanijska oglasna tabla

Pravilo: Posetioci ne smeju imati pristup prostorijama s oglasnim tablama namenjenim radnicima.

Objašnjenje/Napomene: Mnoga preduzeća koriste oglasne table za objavljivanje informacija o zaposlenima ili kompaniji koje su namenjene svim radnicima, ali ne i javnosti. Obaveštenja pretpostavljenih, spiskovi zaposlenih, interni memorandumi, kućni telefoni osoblja i drugi, slični podaci, često se objavljuju na tablama.

Takve oglasne table ponekad su smeštene blizu restorana firme, ili prostorija za pušenje i odmor, kojima posetioci imaju slobodan pristup. Posetioci ne bi trebalo da imaju pristup takvim informacijama.

4-11 Ulaz u računski centar

Pravilo: Prostorija s računarima ili računski centar trebalo bi stalno da budu zaključani, a osoblje se mora identifikovati pre ulaza.

Objašnjenje/Napomene: Obezbeđenje firme trebalo bi da razmisli o primeni elektronskih oznaka ili kartica za pristup kako bi se svi ulazi mogli elektronski nadgledati.

4-12 Korisnički nalozi za dobavljače usluga

Pravilo: Kompanijskom osoblju koje šalje narudžbine dobavljačima najvažnijih usluga mora se dodeliti lozinka kako bi se sprečilo da neovlašćene osobe šalju narudžbenice u ime firme.

Objašnjenje/Napomene: Uslužne kompanije i mnogi drugi proizvođači dozvoljavaju kupcima da po želji izaberu lozinke. Kompanija bi trebalo da koristi lozinke prilikom naručivanja od svih dobavljača najvažnijih usluga. To pravilo je posebno bitno za telekomunikacione usluge i usluge pristupa Internetu. Kad god su u pitanju najbitnije usluge, neophodna je

lozinka da bi se proverio identitet onoga ko šalje narudžbinu. Imajte na umu, takođe, da ne smete koristiti identifikatore kao što su matični broj, poreski broj, majčino devojčko ime i tome slično.

Obmanjivač bi mogao, na primer, da nazove telefonsku kompaniju i naloži im da dodaju funkcije poput prosleđivanja modemskih veza, ili da od dobavljača Internet usluga zahteva da izmeni IP adresu važnih računara.

4-13 Osoba za kontakt u odeljenju

Pravilo: Svako odeljenje ili radna grupa može da odredi jednog zaposlenog kao osobu za kontakt, koju drugi lako mogu da nazovu da bi proverili identitet nepoznatih osoba koje tvrde da su iz odgovarajućeg odeljenja. Na primer, službenik za informatičku podršku će kod te osobe proveriti identitet zaposlenog koji traži pomoć.

Objašnjenje/Napomene: Ovom metodom provere identiteta smanjuje se broj zaposlenih koji su ovlašćeni da garantuju za kolege iz svog odeljenja prilikom izmene lozinke ili rešavanja problema u vezi s računarima.

Napadi obmanjivača delom uspevaju jer osoblje za tehničku podršku nema vremena i ne proveri dobro identitet podnosioca zahteva. Osoblje za podršku uglavnom ne može lično da prepozna sve ovlašćene osobe zbog broja zaposlenih u velikim organizacijama. Kada osoba za kontakt garantuje za kolege, smanjuje se broj zaposlenih koje osoblje za tehničku podršku mora lično da poznaje da bi im pružilo uslugu.

4-14 Korisničke lozinke

Pravilo: Osoblje koje pruža usluge korisnicima ne sme biti u mogućnosti da vidi lozinke korisničkih naloga.

Objašnjenje/Napomene: Obmanjivači često pozovu odeljenje za korisničku podršku i, pod nekim izgovorom, pokušaju da dođu do identifikacionih podataka o korisniku, kao što je lozinka ili matični broj. S tim podacima obmanjivač potom može da pozove neku drugu osobu iz tehničke podrške, predstavljajući se kao korisnik, i da se domogne podataka ili dobije usluge.

Da bi se sprečili takvi napadi, softver za korisničke usluge mora se posediti tako da osoblje može isključivo da unese identifikacione podatke sagovornika, i da mu sistem odmah odgovori da li je lozinka tačna.

4-15 Pronalaženje slabih tačaka

Pravilo: Za vreme obuke o zaštiti podataka, zaposlene treba obavestiti o eventualnim probnim napadima da bi se pronašle slabe tačke u bezbednosnom sistemu.

Objašnjenje/Napomene: Ako zaposlene ne obavestite o mogućem testiranju metodama obmanjivanja, oni se mogu osramotiti, naljutiti, ili pretrpeti druge emocionalne traume jer su kolege ili privremeni radnici pokušali da ih obmanu. Ako nove zaposlene obavestite o takvim proverama, sprečićete konflikte.

4-16 Objavljivanje poverljivih informacija firme

Pravilo: Tajne kompanijske informacije ne smeju se objavljivati u proširijama firme dostupnim javnosti.

Objašnjenje/Napomene: Osim poverljivih informacija o proizvodima i postupcima, moraju se držati u tajnosti i interni podaci kao što su telefonski brojevi ili spiskovi zaposlenih, odnosno popis rukovodilaca odeljenja.

4-17 Obuka o zaštiti podataka

Pravilo: Svi zaposleni u kompaniji moraju pohađati obuku o zaštiti podataka. Štaviše, svaki radnik mora povremeno da pohađa kurs obnove znanja, u intervalima ne dužim od dvanaest meseci, prema zahtevima odeljenja zaduženog za obuku o zaštiti podataka.

Objašnjenje/Napomene: U mnogim organizacijama se ne obraća pažnja na obuku krajnjih korisnika. Prema globalnoj anketi o zaštiti informacija iz 2001. godine, samo 30 procenata anketiranih organizacija troši novac na obuku krajnjih korisnika. Obuka o zaštiti podataka je osnovni zahtev da bi se umanjila mogućnost narušavanja bezbednosnog sistema obmanjivanjem.

4-18 Obuka o zaštiti podataka pre pristupa računarima

Pravilo: Osoblje mora pohađati i uspešno okončati obuku o zaštiti informacija pre nego što im se omogući pristup bilo kom računarskom sistemu firme.

Objašnjenje/Napomene: Obmanjivači često napadaju nove zaposlene, budući da se smatra da oni najslabije poznaju bezbednosna pravila firme i odgovarajuće procedure za klasifikaciju osetljivih informacija.

U okviru obuke, zaposlenima bi trebalo omogućiti da postavljaju pitanja o pravilima obezbeđenja. Nakon obuke, svako bi trebalo da potpiše dokument kojim potvrđuje da razume bezbednosna pravila, kao i da prihvata da ih se pridržava.

4-19 Propusnice zaposlenih moraju biti odgovarajućih boja

Pravilo: Propusnice moraju biti odgovarajućih boja koje naznačavaju da li je dotična osoba zaposleni, radnik po ugovoru, privremeni radnik, dobavljač, savetnik, posetilac, ili stažista.

Objašnjenje/Napomene: Boja propusnice je odličan način da se izdela utvrdi status osobe. Drugi način je da se krupnim slovima naznači status vlasnika propusnice, ali boje teško izazivaju zabunu i uočljive su.

Uobičajena metoda obmanjivača da bi fizički ušli u zgradu firme jeste da se obuku kao kuriri ili tehničko osoblje. Kada uđe u zgradu, napadač se predstavi kao kolega da bi naivni radnici sarađivali s njim. Cilj ovog pravila jeste da spreči ljude da uđu u zgradu, a potom u oblasti kojima ne bi trebalo da imaju pristup. Na primer, osoba koja u zgradu uđe kao tehničar za telekomunikacije ne bi mogao da se predstavi kao zaposleni – boja propusnice bi ga odala.

PRAVILA ZA INFORMATIČARE

Informatičkom odeljenju svake firme potrebna su posebna pravila pomoću kojih se štite podaci kompanije. U skladu sa uobičajenom podelom informatičke službe u organizacijama, podelio sam pravila informatičkog odeljenja na opšta pravila, pravila službe za podršku korisnicima, pravila za administratore sistema i pravila za operatere.

Opšta pravila

5-1 Informacije o zaposlenima u informatičkom odeljenju

Pravilo: Telefonski brojevi i adrese elektronske pošte pojedinačnih radnika u informatičkom odeljenju ne smeju se davati neovlašćenim osobama.

Objašnjenje/Napomene: Cilj ovog pravila jeste da se obmanjivači spreče da iskoriste informacije za kontaktiranje. Ako se objavi samo telefonski broj ili adresa elektronske pošte informatičkog odeljenja, javnost

neće moći da kontaktira informatičare direktno. Adresa elektronske pošte za administrativna i tehnička pitanja trebalo bi da se sastoji isključivo od opštih imena kao što su `admin@kompanija.com`. Objavljeni telefonski brojevi trebalo bi da budu povezani samo sa glasovnom poštom čitavog odeljenja, a ne sa pojedinačnim radnicima.

Kada su javno dostupne informacije za direktno kontaktiranje, uljezi lako mogu da stupe u kontakt s pojedincima zaposlenim u informatičkom odeljenju i da ih na prevaru navedu da im otkriju korisne podatke, ili da se predstavljaju kao informatičari.

5-2 Zahtevi za tehničku podršku

Pravilo: Svi zahtevi za tehničku podršku moraju se uputiti službi za podršku.

Objašnjenje/Napomene: Obmanjivači mogu pokušati da prevare informatičko osoblje koje se obično ne bavi tehničkom podrškom, i koje možda nije upoznato sa odgovarajućim bezbednosnim postupcima pri obradi takvih zahteva. U skladu s tim, informatičari se moraju obučiti da odbiju takve zahteve i upute podnosioca na službu za pružanje podrške.

Služba za podršku korisnicima

6-1 Postupci za daljinski pristup

Pravilo: Osoblje službe za podršku korisnicima ne sme saopštavati pojedinosti, niti davati uputstva u vezi s daljinskim pristupom, uključujući i spoljna mesta za pristup mreži ili brojeve za povezivanje, ukoliko podnosilac zahteva nije:

- Ovlašćen da zna interne informacije.
- Ovlašćen da se priključi na računarsku mrežu kao spoljni korisnik. Ukoliko podnosioca zahteva ne poznaju lično, informatičari ga moraju zasigurno identifikovati u skladu s postupcima za proveru i ovlašćivanje s početka ovog poglavlja.

Objašnjenje/Napomene: Kompanijska služba za podršku korisnicima često je glavna meta obmanjivača, jer je u prirodi njihovog posla da pomažu korisnicima u rešavanju problema u vezi s računarima, kao i zbog toga što obično imaju visoka ovlašćenja za rad u sistemu. Sve osoblje iz službe za podršku korisnicima mora se obučiti da se ponaša kao ljudska zaštitna barijera koja će sprečiti otkrivanje informacija neovlašćenim licima. Jednostavno

pravilo je da se nikada ne obelodanjuju postupci za daljinski pristup dok se zasigurno ne utvrdi identitet potražioca.

6-2 Poništavanje lozinki

Pravilo: Lozinke korisničkih naloga mogu se poništiti samo na zahtev vlasnika naloga.

Objašnjenje/Napomene: Najčešća prevara koju primenjuju obmanjivači jeste da zaduže nekoga da izmeni ili poništi lozinku tuđeg naloga. Napadač se predstavi kao zaposleni koji je izgubio ili zaboravio lozinku. Kako bi se ova vrsta napada osujetila, informatičar kome se uputi zahtev za poništavanje lozinke mora uzvratiti poziv sagovorniku pre nego što išta učini, i to ne na telefonski broj koji mu je on dao, već na broj koji je pronašao u telefonskom imeniku. Pogledajte odeljak „Postupci za proveru i ovlašćivanje“ da biste saznali nešto više o tome.

6-3 Izmena ovlašćenja

Pravilo: Sve zahteve za proširenje korisničkih ovlašćenja ili prava pristupa mora pismeno odobriti pretpostavljeni vlasnika naloga. Nakon izmene, potvrda se mora poslati rukovodiocu koji je podneo zahtev putem interne pošte u kompaniji. Štaviše, takve zahteve valja proveriti u skladu s postupcima za proveru i ovlašćivanje.

Objašnjenje/Napomene: Nakon što uljez provali običan korisnički nalog, pokušaće da proširi ovlašćenja tako da ima punu kontrolu nad sistemom. Napadač koji poznaje postupak ovlašćivanja može podmetnuti falsifikovan zahtev pomoću elektronske pošte, faksa, ili telefona, može telefonirati tehničkoj podršci ili službi za podršku korisnicima i pokušati da ubedi tehničara da dodeli dodatna prava pristupa provaljenom nalogu.

6-4 Otvaranje novih naloga

Pravilo: Zahtevi za otvaranje novih naloga za zaposlene, radnike po ugovoru, ili druga ovlašćena lica, moraju se podneti ili pismeno, s potpisom pretpostavljenog, ili digitalno potpisanom elektronskom porukom. Ti se zahtevi moraju potvrditi i tako što će se internom poštom firme poslati potvrda zahteva.

Objašnjenje/Napomene: Budući da su lozinke i druge korisne informacije za upade u računarske sisteme najpoželjnije mete kradljivaca informacija, neophodne su odgovarajuće mere opreza. Cilj ovog pravila je da

spreči uljeze da se predstave kao ovlašćeno osoblje ili da podnesu lažne zahteve za otvaranje novih naloga. Stoga, takve zahteve treba proveriti postupcima za proveru i ovlašćivanje.

6-5 Slanje novih lozinki

Pravilo: Nove lozinke se moraju smatrati poverljivim informacijama, te ih valja prenositi bezbednim metodama, na primer, lično, ili kurirskim uslugama koje zahtevaju potpis primaoca, a takve su preporučena pošta, UPS, ili FedEx. Pogledajte pravila o slanju poverljivih informacija.

Objašnjenje/Napomene: Može se koristiti i interna pošta firme, ali se preporučuje da se lozinke šalju u specijalnim kovertama kroz koje se ne vidi sadržaj. Preporučuje se da se u svakom odeljenju jedna osoba zaduži za slanje podataka o novim nalogima, i potvrđivanje identiteta osoba koje izgube ili zaborave lozinke. U tim okolnostima služba za podršku će uvek biti u kontaktu s manjom grupom zaposlenih koje će lično poznavati.

6-6 Isključivanje naloga

Pravilo: Pre nego što isključite nalog nekog korisnika, morate zasigurno proveriti da je to zatražilo ovlašćeno lice.

Objašnjenje/Napomene: Cilj ovog pravila jeste da spreči napadače da na prevaru podnesu zahtev za isključenje naloga, a potom da nazovu korisnika pod izgovorom da žele da poprave problem jer korisnik ne može da pristupi računarskom sistemu. Kada obmanjivač pozove korisnika izdajući se za tehničara, znajući da korisnik ne može da se prijavi za rad, žrtva mu često kaže lozinku tokom postupka rešavanja navodnog problema.

6-7 Isključivanje mrežnih priključaka i uređaja

Pravilo: Nijedan zaposleni ne bi trebalo da isključuje nijedan mrežni uređaj, niti priključak, na molbu neproverenog lica iz tehničke podrške.

Objašnjenje/Napomene: Namera ovog pravila je da se napadač spreči da na prevaru podnese zahtev za isključivanje mrežnog priključka, a potom da nazove korisnika pod izgovorom da želi da popravi problem jer korisnik ne može da pristupi mreži. Kada obmanjivač pozove korisnika izdajući se za ljubaznog tehničara, znajući za korisnikov problem s radom u mreži, žrtva mu često kaže lozinku tokom postupka rešavanja navedenog problema.

6-8 Objavljivanje postupaka za bežični pristup

Pravilo: Osoblje ne sme da objavljuje postupke za pristupanje kompanijskim sistemima putem bežične mreže licima koja nisu ovlašćena za rad u bežičnoj mreži.

Objašnjenje/Napomene: Uvek prvo proverite da li je podnosilac zahteva ovlašćen za povezivanje na mrežu kao spoljni korisnik pre nego što mu saopštite podatke za pristup bežičnoj mreži. Pogledajte postupke za proveru i ovlašćivanje.

6-9 Problemi korisnika

Pravilo: Imena zaposlenih koji su prijavili probleme s računarima ne smeju se objavljivati izvan informatičkog odeljenja.

Objašnjenje/Napomene: Za vreme napada, obmanjivač obično pozove službu za podršku korisnicima i zatraži imena osoba koje su prijavile probleme s računarima. Ponekad se izdaje za zaposlenog, za dobavljača, ili službenika telefonske kompanije. Kada dobije imena tih osoba, obmanjivač ih pozove, navodeći kao razlog rešavanje problema, predstavivši se kao pripadnik službe za podršku korisnicima, ili lice iz tehničke podrške. Za vreme poziva napadač navede žrtvu da mu oda željene informacije, ili da mu učini uslugu koja će mu olakšati da dođe do cilja.

6-10 Pokretanje izvršnih naredaba ili pokretanje programa

Pravilo: Osoblje zaposleno u informatičkom odeljenju, koje ima privilegovane naloge, ne bi trebalo da izvršava nikakve naredbe, niti da pokreće nikakve aplikativne programe na zahtev nepoznatih osoba.

Objašnjenje/Napomene: Po uobičajenoj metodi kojom instaliraju trojanca ili neki drugi zlonamerni program, napadači izmene ime postojećeg programa, a potom pozovu službu za podršku korisnicima uz žalbu da se stalno pojavljuje poruka o grešci pri pokušaju pokretanja programa. Napadač ubedi tehničara iz službe za podršku korisnicima da sam pokrene program. Zlonamerni program se izvršava s ovlašćenjem korisnika koji ga je pokrenuo, tako da napadač dobija ovlašćenja za rad kao i pomenuti tehničar. Na taj način napadač može preuzeti kontrolu nad kompanijskim sistemom.

Pomenuta metoda predupređuje se pravilom da osoblje iz tehničke podrške proveriti status zaposlenog pre nego što na zahtev sagovornika pokrene bilo koji program.

Administracija računarskog sistema

7-1 Izmena globalnih prava pristupa

Pravilo: Zahtev za izmenu globalnih prava pristupa u elektronskom profilu zaposlenog mora odobriti tim zadužen za upravljanje pravima pristupa u kompanijskoj mreži.

Objašnjenje/Napomene: Ovlašćena lica će analizirati svaki takav zahtev i proveriti da li je izmena rizična po bezbednost informacionog sistema. U tom slučaju odgovorni moraju, zajedno sa podnosiocem zahteva, doneti odluku o izmenama.

7-2 Zahtevi za daljinski pristup

Pravilo: Daljinski pristup računarima odobrava se samo onim licima koja imaju potrebu da pristupe kompanijskim računarskim sistemima sa udaljenih lokacija. Zahtev mora podneti pretpostavljeni zaposlenog, a treba ga proveriti prema postupcima provere i ovlašćivanja.

Objašnjenje/Napomene: Ako samo ovlašćena lica dodeljuju prava daljinskog pristupa kompanijskoj mreži, i ako se takav pristup ograniči samo na korisnike kojima je to zaista neophodno, rizik od upravljanja daljinskim pristupom može se u velikoj meri umanjiti. Što manji broj ljudi ima daljinsku modemsku vezu, manji je broj potencijalnih meta napadača. Ne zaboravite da napadači mogu zloupotребiti korisnike s pravom daljinskog pristupa i oteti njihovu vezu do kompanijske mreže, koristeći njihove identifikacione podatke tokom drugog poziva.

7-3 Poništavanje lozinki privilegovanih naloga

Pravilo: Zahtev za poništavanje lozinke privilegovanog naloga mora odobriti upravnik sistema ili administrator zadužen za računar na kom se nalog nalazi. Nova lozinka se šalje internom poštom firme ili se isporučuje lično.

Objašnjenje/Napomene: Osobe koje imaju pristup nalogima s ovlašćenjima administratora mogu da pristupe svim sistemskim resursima i datotekama računarskog sistema. Naravno, te naloge treba što bolje zaštititi.

7-4 Daljinski pristup osoblja tehničke podrške

Pravilo: Nijedan član tehničke podrške (kao što je osoblje proizvođača softvera ili hardvera) ne sme da ima daljinski pristup informacijama, niti računarskim sistemima i uređajima, bez provere identiteta i specijalnih

ovlašćenja. Ukoliko proizvođač zahteva pristup sa visokim ovlašćenjima, odmah nakon pružene usluge treba izmeniti lozinku tog naloga.

Objašnjenje/Napomene: Obmanjivači se mogu predstaviti kao proizvođači softvera ili hardvera da bi pristupili računarskim ili telekomunikacionim mrežama preduzeća. Dakle, izuzetno je važno da se identitet osoblja proizvođača proveriti, kao i njihova ovlašćenja za rad na sistemu. Štaviše, kada obave posao, ne sme im se dozvoliti da i dalje koriste taj pristup sistemu. Zato treba izmeniti lozinku tog naloga.

Nijedan proizvođač ne sme sam da bira lozinku naloga, čak ni privremeno. Poznato je da neki proizvođači koriste iste ili slične lozinke u više korisničkih sistema. Na primer, jedno preduzeće za mrežnu bezbednost upotrebilo je istu lozinku na svim privilegovanim nalogima svih korisničkih sistema. Da stvar bude još gora, omogućili su daljinski pristup preko Telnet.

7-5 Stroga provera identiteta pri daljinskom pristupu sistemima preduzeća

Pravilo: Sve tačke daljinskog pristupa mreži moraju se zaštititi pouzdanim uređajima za proveru identiteta, kao što su sistemi za dinamičke lozinke ili biometrički uređaji.

Objašnjenje/Napomene: Mnoge firme se oslanjaju na stalne lozinke kao jedini način provere identiteta korisnika daljinskog pristupa. To je opasno jer nije bezbedno – prevaranti napadaju sve tačke daljinskog pristupa u kompanijskoj mreži koje bi mogle biti slabe. Upamtite da se nikad ne zna da li je neko saznao vašu lozinku.

Stoga, sve tačke daljinskog pristupa moraju se zaštititi strogom proverom identiteta. Za to se mogu koristiti uređaji na kojima se lozinke periodično smenjuju, identifikacione kartice, ili biometrički uređaji, pa lozinke kojih se napadač eventualno domogne nisu ni od kakve koristi.

Kada nije praktično primenjivati proveru identiteta zasnovanu na izmenljivim lozinkama, korisnici računara se bez izuzetka moraju pridržavati pravila za izbor lozinke koje se teško mogu pogoditi.

7-6 Podešavanje operativnog sistema

Pravilo: Administratori sistema moraju voditi računa da se operativni sistemi usklade sa svim značajnim bezbednosnim pravilima i postupcima.

Objašnjenje/Napomene: Pisanje i distribuiranje bezbednosnih pravila je osnovni korak ka smanjivanju rizika, ali se u većini slučajeva pridržavanje tih pravila ostavlja pojedincima. Međutim, postoje neka pravila u vezi s upotrebom računara koja se mogu sprovesti pomoću operativnog sistema, kao što je neophodna dužina lozinke. Automatizovanjem bezbednosnih pravila pomoću parametara operativnog sistema efikasno se zamenjuje ljudski činilac u procesu odlučivanja, čime se povećava ukupna bezbednost organizacije.

7-7 Obavezan rok trajanja

Pravilo: Svaki računarski nalog mora trajati najviše godinu dana.

Objašnjenje/Napomene: Cilj ovog pravila jeste da se eliminiše postojanje računarskih naloga koje više niko ne koristi, jer se često napadaju neaktivni nalozi. Ovim postupkom se obezbeđuje da se svi računarski nalozi bivših zaposlenih ili privremenih radnika, koji su slučajno ostali aktivni, automatski isključe.

Ako uprava tako odluči, možete od zaposlenih zahtevati da pohađaju kurs obnove znanja iz bezbednosti u vreme isteka roka trajanja naloga, ili možete tražiti da se podsete pravila zaštite podataka, te da potpišu da se s njima slažu i da će ih se pridržavati.

7-8 Opšte adrese elektronske pošte

Pravilo: Informatičko odeljenje treba da napravi opšte adrese elektronske pošte za svako odeljenje u okviru organizacije koje često komunicira s javnošću.

Objašnjenje/Napomene: Opšte adrese elektronske pošte mogu se javno davati na telefonskoj centrali ili se mogu objaviti na Web lokaciji preduzeća. Zaposleni smeju da saopšte ličnu adresu elektronske pošte samo osobama koje zaista treba da je znaju.

Tokom prve faze obmanjivanja, napadač često pokušava da se domogne telefonskih brojeva, imena i pozicija zaposlenih. U većini slučajeva, te su informacije javno dostupne na Web lokaciji preduzeća ili ih može dobiti svako ko ih zatraži. Primena opšte glasovne pošte i/ili adresa elektronske pošte otežava povezivanje imena zaposlenih s određenim odeljenjima i odgovornostima.

7-9 Informacije za kontakt u vezi s domenom

Pravilo: Pri registraciji adresa na Internetu ili imena računara, objavljene informacije administrativnog, tehničkog, i drugog osoblja ne bi trebalo da se odnose na pojedince. Umesto toga, valjalo bi objaviti spisak opštih adresa elektronske pošte i glavni telefonski broj firme.

Objašnjenje/Napomene: Cilj ovog pravila jeste da se spreči zloupotreba objavljenih informacija. Kada se obelodane imena i telefonski brojevi pojedinaca, uljez te podatke može iskoristiti za uspostavljanje veze s pojedinim licima u pokušaju da ih na prevaru navede da mu odaju sistemske informacije, ili da mu učine uslugu koja će mu olakšati da dođe do cilja. Pri pokušaju prevare drugih radnika kompanije obmanjivač se može predstaviti kao osoba navedena na spisku.

Umesto adresa elektronske pošte za svakog pojedinog zaposlenog, informacije za kontakt moraju biti u sledećem obliku: administrator@kompanija.com. Treba napraviti opšte sanduče za glasovnu poštu za administrativne ili tehničke kontakte, da bi se ograničilo obelodanjivanje informacija koje bi mogle biti korisne obmanjivačima.

7-10 Ažuriranje bezbednosnog i operativnog sistema

Pravilo: Valja instalirati sve bezbednosne zakrpe za operativni sistem i aplikativni softver čim se pojave. Ukoliko ovo pravilo narušava rad najbitnijih proizvodnih sistema, ažuriranje treba izvršiti što pre.

Objašnjenje/Napomene: Kada se pronađu propusti, treba odmah utvrditi s proizvođačem softvera da li postoji zakrpa ili privremeno rešenje problema. Računarski sistem bez zakrpa jedna je od najvećih bezbednosnih pretnji preduzeću. Kada administratori sistema odugovlače sa primenom neophodnih zakrpa, propusti su toliko očigledni da ih svaki napadač može iskoristiti kako bi se uvukao u sistem.

Desetine bezbednosnih propusta se otkrivaju i objavljuju svake nedelje na Internetu. Iako se osoblje iz informatičkog tima trudi da što pre primeni sve zakrpe i rešenja problema, uprkos tome što su ti sistemi iza zaštitne barijere firme, uvek postoji rizik od napada na kompanijsku mrežu. Izuzetno je važno da budete obavešteni o objavljenim propustima operativnog sistema ili bilo kojih aplikativnih programa koji se koriste u poslovanju.

7-11 Informacije za kontakt na Web lokacijama

Pravilo: Na javnoj Web lokaciji preduzeća ne smeju se objavljivati pojedinosti kompanijske strukture, niti se smeju pominjati pojedinci po imenu.

Objašnjenje/Napomene: Podaci o kompanijskoj strukturi, kao što su organizacioni spiskovi, hijerarhijski dijagrami, spiskovi zaposlenih i odeljenja, sistem odgovornosti, imena, pozicije, interni brojevi za kontakt, brojevi zaposlenih i slični podaci koji se koriste u internim postupcima, ne smeju se objavljivati na javnim Web lokacijama.

Napadači često dolaze do veoma korisnih informacija na Web lokaciji preduzeća. Oni ih iskoriste da bi se predstavili kao zaposleni koji te podatke znaju, pozivajući firmu pod lažnim izgovorom. Ti podaci čine obmanjivača verodostojnim. Štaviše, napadač može analizirati pomenute informacije i otkriti žrtve koje verovatno poseduju značajne podatke.

7-12 Otvaranje privilegovanih naloga

Pravilo: Ne smeju se otvarati privilegovani nalozi, niti se dodeljivati systemske privilegije nijednom nalogu, ukoliko to ne odobri administrator ili upravnik sistema.

Objašnjenje/Napomene: Obmanjivači se često izdaju za proizvođače hardvera i softvera, pokušavajući da na prevaru navedu informatičko osoblje da im neovlašćeno naprave naloge. Cilj ovog pravila je da spreči takve napade kontrolisanjem privilegovanih naloga. Administrator ili upravnik računarskog sistema moraju odobriti zahteve za izradu naloga s većim privilegijama.

7-13 Anonimni nalozi

Pravilo: Anonimni nalozi svakog računarskog sistema ili mrežnog uređaja moraju se isključiti ili ukloniti, osim na serverima za prenos datoteka (FTP) za koji je uprava odobrila anonimni pristup.

Objašnjenje/Napomene: Cilj anonimnog naloga jeste da se obezbedi privremeni pristup mreži osobama kojima nije potreban sopstveni nalog. U nekoliko operativnih sistema anonimni nalozi se uključuju automatski pri instalaciji. Njih uvek treba isključiti, inače se narušava princip odgovornosti korisnika. Informatičari bi trebalo da prate sve aktivnosti korisnika na računarima.

Obmanjivači lako mogu da iskoriste anonimne naloge da bi neovlašćeno pristupili sistemu, ili direktno, ili na prevaru – navodeći ovlašćeno osoblje da im omogući upotrebu anonimnog naloga.

7-14 Šifrovanje spoljnih rezervnih kopija podataka

Pravilo: Svi podaci koji se smeštaju van prostorija preduzeća moraju se šifrovati da bi se sprečila neovlašćena upotreba.

Objašnjenje/Napomene: Osoblje zaposleno u informatičkim odeljenjima mora obezbediti ispravnost rezervne kopije svih podataka. Za to je potrebno redovno proveravati dešifrovanje nasumičnim odabirom šifrovanih datoteka, da bi se uverilo da se podaci mogu obnoviti. Štaviše, nekom od upravnika treba dati kopiju ključeva za šifrovanje podataka, za slučaj da se originalni ključ izgubi ili ne bude dostupan.

7-15 Tačke za pristup mreži i posetioci

Pravilo: Svi javno dostupni Ethernet priključci moraju se nalaziti na odvojenoj mreži kako bi se sprečio neovlašćen pristup internoj mreži.

Objašnjenje/Napomene: Cilj ovog pravila jeste da spreči uljeze da se povežu u internu mrežu dok se nalaze u prostorijama preduzeća. Priključke za Ethernet instalirane u salama za sastanke, restoranu, centrima za obuku, i drugim prostorijama kojima posetioci imaju pristup treba filtrirati da bi se sprečio neovlašćen pristup posetilaca kompanijskim računarskim sistemima.

Administrator mreže ili bezbednosnog sistema može odlučiti da napravi virtuelnu lokalnu mrežu u skretnici, ako je to moguće, da bi upravljao pristupom s pomenutih lokacija.

7-16 Modemi za daljinski pristup

Pravilo: Modeme za daljinski pristup valja podesiti tako da se ne uključuju pre četvrtog zvučnog signala.

Objašnjenje/Napomene: Kao što je prikazano u filmu *Ratne igre*, hakeri primenjuju „automatsko pozivanje“ da bi pronašli telefonske linije na koje su priključeni modemi. Postupak započinje tako što napadač odredi početne brojeve telefona koji se koriste u oblasti u kojoj se nalazi ciljna kompanija. Potom se programom isprobava svaki telefonski broj koji počinje unesenim ciframa, da bi se pronašli oni na koje je priključen modem. Da bi se postupak ubrzao, ti programi obično čekaju jedan ili dva zvučna signala da bi se

modem oglasio, pre nego što pokušaju sledeći broj. Kada se modemi podese tako da odgovore na poziv tek posle četvrtog zvučnog signala, programi za automatsko pozivanje neće uspeti da prepoznaju modemske linije.

7-17 Antivirusni softver

Pravilo: Na svaki računarski sistem mora se instalirati i aktivirati najnovija verzija antivirusnog softvera.

Objašnjenje/Napomene: U preduzećima koja ne instaliraju automatski najnovije verzije antivirusnog softvera i ne ažuriraju datoteke s opisima virusa, svaki korisnik mora preuzeti odgovornost za instaliranje i održavanje softvera u sopstvenom sistemu, uključujući i računarske sisteme za daljinski pristup kompanijskoj mreži.

Ako je izvodljivo, softver se mora podesiti tako da se svake noći automatski ažurira. Kada se datoteke s opisima virusa ne prosleđuju do korisničkih stonih računara, sami korisnici moraju biti odgovorni za ažuriranje tih datoteka bar jednom nedeljno.

Ti uslovi se odnose na sve stone i prenosive računare koji se povezuju na kompanijske računarske sisteme, i moraju se primenjivati bez obzira na to da li je vlasnik računara firma ili pojedinac.

7-18 Prilozi elektronskih poruka (kada se zahteva visok nivo bezbednosti)

Pravilo: U organizaciji koja zahteva visok nivo bezbednosti, zaštitna barijera mora da filtrira sve datoteke priložene elektronskim porukama.

Objašnjenje/Napomene: Ovo pravilo se odnosi samo na preduzeća s visokim nivoom bezbednosti, ili na ona koja nemaju potrebe da primaju datoteke pripojene elektronskoj pošti.

7-19 Provera softvera

Pravilo: Sav novi softver, ili softverske zakrpe i nove verzije, na fizičkim medijima ili dobijeni preko Interneta, treba proveriti pre instalacije. Ovo pravilo je posebno važno za instaliranje softvera koji zahteva systemska ovlašćenja.

Objašnjenje/Napomene: U računarski softver pomenut u ovom pravilu ubrajaju se komponente operativnog sistema, aplikativni softver, zakrpe, popravke, i sve ažurirane verzije softvera. Mnogi proizvođači softvera

ugrađuju metode kojima kupci mogu da provere ispravnost paketa, obično putem digitalnog potpisa. U slučaju da se ispravnost ne može proveriti, treba konsultovati proizvođača da bi se proverilo poreklo softvera.

Zna se da hakeri šalju softver žrtvi, upakovan kao originalni proizvod. Izuzetno je važno da proverite poreklo primljenog softvera pre nego što ga instalirate na računarske sisteme, pogotovu ako je stigao nenaručen.

Imajte na umu da bi vešt napadač mogao otkriti da je vaša organizacija naručila softver od proizvođača. Služeći se tom informacijom, napadač bi mogao otkazati pravu narudžbinu kod proizvođača, i sam kupiti pomenu-ti softver. Potom bi ga izmenio tako da izvrši nešto zlonamerno, i poslao ga vašoj firmi, u originalnom pakovanju, ako treba. Kada se proizvod instalira, napadač kontroliše sistem.

7-20 Podrazumevane lozinke

Pravilo: Podrazumevanu lozinku sa svih operativnih sistema i hardver-skih uređaja treba izmeniti u skladu s kompanijskim pravilom koje se tiče lozinki.

Objašnjenje/Napomene: Nekoliko operativnih sistema i uređaja se isporučuje sa podrazumevanim lozinkama – to jest, sa lozinkama koje su iste na svakom prodatom primerku. Ukoliko ne promenite podrazume-vanu lozinku, činite ogromnu grešku koja može ugroziti preduzeće.

Podrazumevane lozinke su naširoko poznate i mogu se naći na Internetu. Prilikom napada, uljez prvo isproba podrazumevanu lozinku proizvođača.

7-21 Blokiranje naloga nakon određenog broja neuspešnih pokušaja pristupa (pri niskom i srednjem nivou bezbednosti)

Pravilo: Nakon određenog broja uzastopnih neuspešnih pokušaja pri-javljivanja za rad, nalog treba blokirati neko vreme.

Objašnjenje/Napomene: Sve kompanijske radne stanice i serveri mora-ju se podesiti tako da ograniče broj uzastopnih neuspešnih pokušaja prija-vljivanja za rad. To pravilo je neophodno da bi se sprečilo pogađanje lozinke putem pokušaja i greške, napad rečnikom, ili pogađanje lozinke na silu.

Administrator sistema mora podesiti bezbednosne parametre tako da se nalog blokira kada se dostigne određeni broj uzastopnih neuspešnih poku-šaja. Preporučuje se da se nalog blokira bar trideset minuta nakon sedam uzastopnih neuspešnih pokušaja prijavljivanja za rad.

7-22 Zaključavanje naloga nakon neuspešnih pokušaja pristupa (visok nivo bezbednosti)

Pravilo: U organizaciji koja ima velike bezbednosne zahteve, nakon određenog broja uzastopnih neuspešnih pokušaja prijavljivanja za rad nalog treba zaključati. Takav nalog može da otključa samo služba za rad s nalogima.

Objašnjenje/Napomene: Sve kompanijske radne stanice i serveri moraju se podesiti tako da ograniče broj uzastopnih neuspešnih pokušaja prijavljivanja za rad. To pravilo je neophodno da bi se sprečilo pogađanje lozinke putem pokušaja i greške, napad rečnikom, ili pogađanje lozinke na silu.

Administrator sistema mora podesiti bezbednosne parametre tako da se nalog zaključa nakon pet neuspešnih pokušaja prijavljivanja za rad. Vlasnik zaključanog naloga mora pozvati tehničku podršku ili službu za rad s nalogima da bi mu se nalog ponovo uključio. Pre nego što se nalog ponovo uključi, odgovorno odeljenje mora proveriti identitet vlasnika naloga, prema pravilima provere i ovlašćivanja.

7-23 Povremena izmena lozinki privilegovanih naloga

Pravilo: Od svih vlasnika privilegovanih naloga mora se tražiti da menjaju lozinke najmanje jednom mesečno.

Objašnjenje/Napomene: U zavisnosti od ograničenja operativnog sistema, administrator sistema mora nametnuti ovo pravilo tako što će zadati bezbednosne parametre u sistemskom softveru.

7-24 Povremena izmena korisničkih lozinki

Pravilo: Svi vlasnici naloga moraju menjati lozinke najmanje jednom u dva meseca.

Objašnjenje/Napomene: U operativnim sistemima koji imaju tu funkciju, administratori sistema moraju nametnuti ovo pravilo tako što će zadati bezbednosne parametre u softveru.

7-25 Lozinke novih naloga

Pravilo: Novi računarski nalozi moraju se otvarati sa početnom lozinkom koja je unapred istekla, čime se od vlasnika naloga zahteva da izabere novu lozinku već pri prvoj upotrebi.

Objašnjenje/Napomene: Ovim zahtevom se obezbeđuje da samo vlasnik naloga zna svoju lozinku.

7-26 Lozinka za pokretanje sistema

Pravilo: Sve računarske sisteme treba podesiti tako da se pri pokretanju mora uneti lozinka.

Objašnjenje/Napomene: Računari se moraju podesiti tako da se pri uključivanju mora uneti lozinka pre nego što se operativni sistem pokrene. Time se neovlašćene osobe sprečavaju da uključe i upotrebe tuđ računar. Ovo pravilo se odnosi na sve računare u prostorijama firme.

7-27 Pravila za lozinke privilegovanih naloga

Pravilo: Svi privilegovani nalozi moraju imati složenu lozinku koja:

- ne sme biti reč iz rečnika bilo kog jezika
- sadrži mala i velika slova, najmanje jedno slovo, jedan simbol i jedan broj
- ima bar 12 znakova
- neće nikako biti povezana s firmom, niti pojedincom.

Objašnjenje/Napomene: U mnogim slučajevima, hakeri napadaju naloge sa sistemskim ovlašćenjima. Povremeno napadač uspe da iskoristi druge propuste da bi ostvario punu kontrolu sistema. Prve lozinke koje će uneti su jednostavne, često korišćene reči iz rečnika. Biranjem složenih lozinki povećava se bezbednost zato što se otežava otkrivanje lozinke putem pokušaja i grešaka, napadom rečnikom, ili pogađanjem lozinke na silu.

7-28 Tačke bežičnog pristupa

Pravilo: Svi korisnici koji pristupaju bežičnoj mreži moraju koristiti virtuelne privatne mreže (engl. *Virtual Private Network*, VPN) da bi zaštitili kompanijsku mrežu.

Objašnjenje/Napomene: Bežične mreže se napadaju novom tehnikom koja se zove *neprijateljska vožnja* (engl. *war driving*). Napadač se vozi ili šeta, noseći prenosivi računar opremljen karticom 802.11B dok se ne otkrije bežična mreža.

Mnoge firme su pustile u rad bežične mreže i ne uključivši protokol za bežičnu ekvivalenciju (engl. *wireless equivalency protocol*, WEP), koji se koristi za šifrovanje bežične veze. Ali čak i kada se aktivira, najnovija verzija WEP-a (koja se pojavila sredinom 2002) nije efikasna. Hakeri su uspevali da prodru u bežične mreže, a nekoliko Web lokacija je posvećeno pronalazenju nezaštićenih bežičnih sistema i provaljivanju u tačke bežičnog pristupa obezbeđene WEP-om.

Stoga, neophodno je dodati još jedan nivo zaštite preko protokola 802.11B pomoću tehnologije VPN.

7-29 Ažuriranje antivirusnih datoteka

Pravilo: Svaki računarski sistem mora se programirati da automatski ažurira datoteke s opisima virusa i trojanaca.

Objašnjenje/Napomene: U najmanju ruku, takve datoteke treba ažurirati bar jednom nedeljno. U kompanijama u kojima zaposleni ostavljaju uključene računare, toplo preporučujem da se antivirusne datoteke ažuriraju svake noći.

Antivirusni softver ne može da otkrije sve nove oblike zlonamernog koda, ako se ne ažurira redovno. S obzirom na to da se pretnja od infekcija virusima, crvima i trojanskim konjima znatno povećava ako se datoteke s opisima ne ažuriraju izuzetno je važno je da imate najnoviju verziju antivirusnih datoteka.

Operateri

8-1 Unos naredaba i pokretanje programa

Pravilo: Operateri na računaru ne smeju unositi naredbe, niti pokretati programe na zahtev nepoznatih osoba. Ako dođe do situacije u kojoj se čini da neproverena osoba ima razloga za takav zahtev, on se ne sme ispuniti bez prethodnog odobrenja pretpostavljenog.

Objašnjenje/Napomene: Obmanjivači često napadaju operatere, jer uglavnom imaju naloge s visokim ovlašćenjima, a napadač očekuje da su manje iskusni i da manje poznaju kompanijska pravila od ostalih informatičara. Cilj ovog pravila jeste dodatna provera da bi se obmanjivači sprečili u iskorišćavanju operatera.

8-2 Radnici s privilegovanim nalogima

Pravilo: Zaposleni s privilegovanim nalogima ne sseju pomagati, niti davati informacije neproverenim osobama. To se posebno odnosi na uskraćivanje pomoći u vezi s računarima (na primer, obuka za rad na nekoj aplikaciji), pristup firminim bazama podataka, učitavanje softvera, ili otkrivanje imena osoba kojima je omogućen daljinski pristup.

Objašnjenje/Napomene: Obmanjivači često napadaju zaposlene s privilegovanim nalogima. Cilj ovog pravila jeste da uputi informatičare s privilegovanim nalogima kako da ispravno postupe prilikom poziva obmanjivača.

8-3 Interni sistemski podaci

Pravilo: Operateri nikada ne smeju odavati nikakve informacije računarskim sistemima preduzeća, niti o priključnim uređajima ukoliko se identitet podnosioca zahteva ne utvrdi.

Objašnjenje/Napomene: Obmanjivači često pozivaju operatere i od njih traže značajne informacije kao što su postupci za pristup sistemu, spoljne tačke daljinskog pristupa i telefonski brojevi za daljinski pristup.

U firmama koje imaju tehničku podršku ili službu za podršku korisnicima, zahteve za informacije o računarskim sistemima ili pomoćnim uređajima upućene operaterima trebalo bi smatrati neobičnim. Sve zahteve za podatke treba proceniti prema kompanijskoj klasifikaciji podataka, da bi se utvrdilo da li je podnosilac zahteva ovlašćen da poseduje datu informaciju. Kada ne možete da utvrdite klasu podataka, smatrajte ih internim.

U nekim slučajevima osoblje tehničke podrške proizvođača mora da komunicira s osobama koje imaju pristup računarskim sistemima preduzeća. Za takve kontakte se moraju zadužiti određene osobe iz informatičkog odeljenja.

8-4 Objavljivanje lozinki

Pravilo: Operateri nikada ne smeju da objavljuju svoje lozinke, niti tuđe lozinke poverene njima, bez prethodnog odobrenja upravnika informatičkog odeljenja.

Objašnjenje/Napomene: Uopšteno govoreći, strogo je zabranjeno saopštavati drugome lozinku. Razume se da operateri možda moraju da trećem licu saopšte lozinku u hitnim situacijama. Za objavljivanje lozinka pravila potrebno je odobrenje upravnika informatičkog odeljenja. Radi dodatnog opreza, za objavljivanje identifikacionih podataka treba zadužiti samo malu grupu pojedinaca posebno obučениh za proveru identiteta.

8-5 Elektronski mediji

Pravilo: Sve elektronske medije sa informacijama koje nisu namenjene javnosti treba zaključati na fizički bezbedno mesto.

Objašnjenje/Napomene: Cilj ovog pravila jeste da se spreči fizička krađa osetljivih informacija na elektronskim medijima.

8-6 Mediji za rezervne kopije podataka

Pravilo: Operateri treba da skladište medije s rezervnim kopijama podataka u sef preduzeća ili na neko drugo bezbedno mesto.

Objašnjenje/Napomene: Mediji s rezervnim kopijama podataka još su jedna omiljena meta hakera. Napadač neće trošiti vreme pokušavajući da se uključi u računarski sistem ili mrežu kad su najslabija tačka bezbednosnog sistema možda mediji s rezervnim kopijama podataka. Kada ukrade takve medije, napadač može da pristupi svim podacima, ukoliko nisu šifrovani. Stoga je fizičko obezbeđivanje medija s rezervnim kopijama podataka osnovni postupak za zaštitu poverljivih kompanijskih informacija.

PRAVILA ZA SVE ZAPOSLENE

Postoje neka pravila koja svi zaposleni moraju znati, bez obzira na to da li rade u informatici, kadrovskom odeljenju, računovodstvu, ili čiste kancelarije. Ta pravila se dele u sledeće kategorije: opšta pravila, pravila rada s računarima, pravila upotrebe elektronske pošte, pravila za radnike koji imaju daljinski pristup, pravila za korišćenje telefona, faksa, glasovne pošte i lozinki.

Opšta pravila

9-1 Prijavljivanje sumnjivih poziva

Pravilo: Zaposleni koji posumnja da je meta napada, u šta se ubrajaju i svi sumnjivi zahtevi za objavljivanje informacija i rad na računaru, odmah to moraju prijaviti odgovarajućoj službi.

Objašnjenje/Napomene: Kada obmanjivač ne uspe da ubedi žrtvu da mu ispuni zahtev, uvek će pokušati da nadmudri nekog drugog. Prijavlivanjem sumnjivog poziva ili događaja zaposleni povlači prvi potez u obaveštavanju preduzeća o mogućem napadu. Dakle, pojedinci su prva linija odbrane protiv obmanjivanja.

9-2 Dokumentovanje sumnjivih poziva

Pravilo: Prilikom sumnjivog poziva za koji se čini da je napad obmanjivača, zaposleni treba, u zavisnosti od situacije, da odugovlači s razgovorom, da bi saznao pojedinosti koje bi mogle otkriti šta napadač pokušava da postigne, i da ih zabeleži radi kasnije prijave.

Objašnjenje/Napomene: Kada se prijave timu za incidente, takve pojedinosti im mogu pomoći da uoče cilj ili tehniku napada.

9-3 Objavljivanje telefonskih brojeva za modemski pristup

Pravilo: Osoblje firme ne sme objavljivati kompanijske telefonske brojeve za modemski pristup, već bi uvek takve zahteve trebalo da prosleđuju službi za podršku korisnicima ili tehničkoj podršci.

Objašnjenje/Napomene: Telefonski brojevi za modemski pristup smatraju se internim informacijama koje se mogu davati samo zaposlenima, kojima su takvi podaci neophodni za obavljanje posla.

Obmanjivači rutinski biraju radnike i odeljenja koji često slabije čuvaju željene informacije. Na primer, napadač pozove odeljenje za naplatu predstavivši se kao radnik telefonske kompanije koji pokušava da razreši problem s računima. Potom zatraži broj faksa ili broj za modemski pristup da bi rešio problem. Uljez često bira zaposlenog koji verovatno neće shvatiti značaj takvih podataka, ili onog ko nije obučen o pravilima za čuvanje poslovnih tajni.

9-4 Kompanijske propusnice

Pravilo: Osim kad se nalazi u sopstvenoj kancelariji, sve osoblje firme, uključujući i upravu, mora stalno nositi propusnice.

Objašnjenje/Napomene: Sve radnike, uključujući i rukovodstvo firme, treba obučiti i motivisati da shvate da je nošenje propusnice obavezno u svim prostorijama firme, sem u javnim prostorijama i sopstvenoj kancelariji.

9-5 Ispitivanje osoba koje ne nose propusnice

Pravilo: Svi zaposleni moraju odmah ispitati nepoznato lice koje ne nosi propusnicu za radnike ili posetioce.

Objašnjenje/Napomene: Iako nijedna firma ne želi da stvori atmosferu u kojoj radnici stalno vrebaju kolege koji se usude da kroče u hodnik bez propusnice, svaka kompanija koja želi da zaštiti svoje informacije ipak mora ozbiljno shvatiti pretnju od obmanjivača koji neometano tumačaju njenim prostorijama. Radnici koji stalno nose propusnice mogu se motivisati na uobičajene načine, pohvalom u kompanijskim novinama ili na oglasnim tablama, sa nekoliko plaćenih slobodnih sati, ili pohvalom u ličnom dosijeju.

9-6 Provlačenje kroz obezbeđene ulaze

Pravilo: Radnici koji ulaze u zgradu ne smeju nikome nepoznatom dozvoliti da ih prati kada koriste sredstva za obezbeđenje firme, kao što su kartice za otključavanje.

Objašnjenje/Napomene: Osoblje mora shvatiti da nije nepristojno zahtevati od nepoznatih lica da se identifikuju pre nego što ih puste u zgradu ili čuvanu oblast.

Obmanjivači često koriste tehniku poznatu kao provlačenje, pri čemu čekaju da neko uđe u zgradu ili čuvanu oblast, da bi se uvukli za njima. Mnogi se osećaju nelagodno kada treba da provere nečiji identitet, smatrajući da je to verovatno kolega. Još jedan način provlačenja je kada uljez nosi nekoliko kutija, pa radnik, koji ništa ne sumnja, otvori ili pridrži vrata.

9-7 Uništavanje tajnih dokumenata

Pravilo: Nepotrebne tajne dokumente treba potpuno uništiti. Medije, u koje ubrajamo i čvrste diskove, na kojima se nalaze ili su se nalazile osetljive informacije ili materijali valja uništiti prema pravilima tima zaduženog za bezbednost informacija.

Objašnjenje/Napomene: Standardni uređaji za uništavanje dokumenata ne rade to dovoljno dobro. Uređaji za potpuno uništavanje pretvaraju papir u bezobličnu masu. Najveći konkurenti organizacije će preturati po odbačenim materijalima u potrazi za informacijama koje bi im mogle koristiti.

Industrijski špijuni i hakeri redovno dolaze do osetljivih podataka iz materijala bačenih u smeće. Zna se da su konkurentske firme pokušale da potplate čistače da bi im predali smeće. Nedavno se dogodilo da je zaposleni kompanije Goldman Sachs u smeću otkrio dokumenta korišćena u mutnim poslovima firme.

9-8 Privatni identifikacioni podaci

Pravilo: Privatni identifikacioni podaci, poput broja zaposlenog, matičnog broja, broja lične karte, datuma i mesta rođenja i majčinog devojačkog imena, nikada se ne smeju koristiti za proveru identiteta. Ti identifikacioni podaci nisu tajni i mogu se nabaviti na razne načine.

Objašnjenje/Napomene: Obmanjivač može da nabavi tuđe identifikacione podatke po određenoj ceni. Nasuprot opštem verovanju, svako ko ima kreditnu karticu i pristup Internetu može da se domogne tih privatnih identifikacionih podataka. Uprkos očiglednoj opasnosti, banke, uslužne

kompanije i kompanije za kreditne kartice obično se služe tim identifikacionim podacima. To je razlog zbog kojeg je krađa identiteta prestup koji se najbrže širio u protekloj deceniji.

9-9 Struktura organizacije

Pravilo: Nezaposlenima se ne smeju pokazivati pojedinosti strukture organizacije.

Objašnjenje/Napomene: U organizacione informacije ubrajaju se struktura firme, hijerarhijski grafikoni, spiskovi zaposlenih u pojedinim odeljenjima, struktura odgovornosti, imena zaposlenih, njihove pozicije, interni telefonski brojevi, brojevi zaposlenih, ili slični podaci.

U prvoj fazi napada cilj obmanjivača jeste da prikupi informacije o unutrašnjoj strukturi kompanije. Ti podaci se potom koriste u taktici napada. Napadači takođe analiziraju pomenute informacije da bi pronašli zaposlene koji verovatno imaju pristup željenim podacima. Ako napadač koristi pomenute informacije za vreme napada, odaje utisak radnika koji poznaje svoju firmu, usled čega će lakše navesti žrtvu da se povinuje njegovim zahtevima.

9-10 Lični podaci o zaposlenima

Pravilo: Svi zahtevi za privatnim podacima zaposlenih, mogu biti upućeni isključivo kadrovskom odeljenju.

Objašnjenje/Napomene: Izuzetak od ovog pravila može biti broj zaposlenog koji se mora pozvati zbog poslovnog problema, ili zato što je dežuran. Međutim, uvek je bolje potražiti telefonski broj podnosioca zahteva i zamoliti traženog zaposlenog da ga pozove.

Rad s računarima

10-1 Unos naredaba u računar

Pravilo: Osoblje nikada ne sme unositi naredbe u računar, niti u pomoćnu opremu na zahtev bilo koga sem proverenih radnika informatičkog odeljenja.

Objašnjenje/Napomene: Uobičajen trik obmanjivača jeste da zatraže od zaposlenog da unese naredbe za promenu parametara sistema, na osnovu čega napadač može neovlašćeno da pristupi žrtvinom računaru, ili da se domogne informacija koje mu mogu olakšati tehnički napad.

10-2 Interni dogovori o imenovanju

Pravilo: Radnici ne smeju obelodanjivati interne nazive računarskih sistema ili baza podataka bez prethodne provere da li je podnosilac zahteva zaposlen u istom preduzeću.

Objašnjenje/Napomene: Obmanjivači ponekad pokušaju da se domognu naziva računarskih sistema firme. Kada saznaju njihova imena, oni pozovu kompaniju predstavivši se kao kolega koji ima problema s radom na nekom od sistema. Njihova priča se čini verodostojnijom jer poznaju interne nazive dodeljene pojedinim sistemima.

10-3 Zahtevi za pokretanje programa

Pravilo: Osoblje nikada ne bi trebalo da pokreće računarske aplikacije niti programe na zahtev bilo koga sem proverenih radnika informatičkog odeljenja.

Objašnjenje/Napomene: Zahteve za pokretanje programa, aplikacija i bilo kakav rad na računaru morate odbiti, ukoliko niste sigurni da je podnosilac zahteva provereni radnik informatičkog odeljenja. Ako se zahteva otkrivanje poverljivih informacija iz bilo koje datoteke ili elektronske poruke, na zahtev morate odgovoriti u skladu s postupcima za davanje podataka te kategorije. Pogledajte odeljak „Saopštavanje informacija“.

Prevaranti mogu da navedu ljude da izvrše programe koji im omogućе da preuzmu kontrolu nad sistemom. Kada korisnik, koji ništa ne sumnja, pokrene program, uljez može dobiti pristup računarskom sistemu žrtve. Drugi programi snimaju rad korisnika na računaru i prenose te podatke napadaču. Kao što obmanjivač može da navede nekoga da izvrši štetne računarske naredbe, u tehničkom napadu se operativni sistem računara podešava tako da izvrši štetne naredbe.

10-4 Preuzimanje ili instaliranje softvera

Pravilo: Zaposleni nikada ne smeju preuzimati, niti instalirati softver na zahtev bilo koga sem proverenih radnika informatičkog odeljenja.

Objašnjenje/Napomene: Radnici bi trebalo da oprezno razmotre neobične zahteve u vezi s bilo kakvom računarskom opremom.

Obmanjivači često ubeđuju žrtve da preuzmu i instaliraju program koji će im pomoći da naruše bezbednost računara ili mreže. U nekim slučajevima, takav program špijunira korisnika ili omogućava napadaču da upravlja računarskim sistemom pomoću tajne aplikacije za daljinsku kontrolu.

10-5 Tekstualne lozinke i elektronske poruke

Pravilo: Lozinke nemojte slati elektronskom poštom, ukoliko ih prethodno ne šifrujete.

Objašnjenje/Napomene: Iako smatram da to nije dobro, ovo pravilo se može zanemariti na pojedinim lokacijama za elektronsku trgovinu u određenim ograničenim slučajevima, kao što su:

- slanje lozinke registrovanim korisnicima lokacije
- slanje lozinke korisnicima koji su izgubili ili zaboravili lozinku.

10-6 Zaštitni softver

Pravilo: Radnici nikada ne smeju uklanjati, niti isključivati antivirusne programe, zaštitnu barijeru, niti bilo kakav drugi bezbednosni softver bez prethodnog odobrenja informatičkog odeljenja.

Objašnjenje/Napomene: Korisnici računara povremeno isključe zaštitni softver bez posebnog razloga, misleći da će time ubrzati rad računara.

Obmanjivač može pokušati da navede zaposlenog da isključi ili izbriše softver neophodan za zaštitu firme od kradljivaca informacija.

10-7 Instaliranje modema

Pravilo: Modemi se ne smeju povezivati s računarima bez odobrenja informatičkog odeljenja.

Objašnjenje/Napomene: Važno je shvatiti da modemi povezani na radne stanice ili stane računare predstavljaju potencijalnu pretnju bezbednosnom sistemu, a pogotovo ako su računari povezani na kompanijsku mrežu. Stoga je cilj ovog pravila kontrola povezivanja modema.

Hakeri automatskim pozivanjem otkrivaju aktivne modemske linije u nekom opsegu telefonskih brojeva. Ista tehnika se može koristiti i za pronalaženje telefonskih brojeva na koje su priključeni modemi u okviru preduzeća. Napadač lako može da ugrozi kompanijsku mrežu ako pronađe računar s modemom i softverom za daljinski pristup čija se lozinka lako pogada, ili čak ne postoji.

10-8 Modemi i automatsko odgovaranje

Pravilo: Na svim stonim računarima i radnim stanicama sa modemima koje je odobrilo informatičko odeljenje trebalo bi onemogućiti automatsko odgovaranje na poziv, da bi se sprečilo neovlašćeno povezivanje na računarski sistem.

Objašnjenje/Napomene: Kad god je moguće, informatičko odeljenje bi trebalo da odredi skup brojeva za daljinsko povezivanje modemom.

10-9 Alati za zaobilaženje softverske zaštite

Pravilo: Radnici ne smeju preuzimati niti koristiti nikakve alatke za zaobilaženje zaštitnih softverskih mehanizama.

Objašnjenje/Napomene: Na Internetu se nalazi nekoliko desetina lokacija posvećenih softveru za razbijanje zaštite šervera i komercijalnih softverskih proizvoda. Upotreba tih alatki predstavlja kršenje autorskih prava vlasnika softvera, i izuzetno je opasna. Budući da ti programi dolaze iz nepoznatih izvora, mogu sadržati i tajni zlonameran kôd koji bi mogao da ošteti korisnikov računar, ili podmetne trojanca za daljinski pristup.

10-10 Objavljivanje podataka o kompaniji na mreži

Pravilo: Zaposleni ne smeju da objavljuju nikakve pojedinosti o kompanijskom hardveru ili softveru u diskusionim grupama i forumima, kao ni informacije za kontakt osim onih koje su u skladu s pravilnikom.

Objašnjenje/Napomene: Sve poruke poslate na Usenet, forume na mreži i diskusione grupe mogu se pretražiti da bi se saznalo nešto više o ciljnoj kompaniji ili pojedincima. Tokom istraživačke faze napada, obmanjivač može potražiti na Internetu sve poruke koje sadrže korisne informacije o kompaniji, njenim proizvodima ili osoblju.

U nekim javnim porukama nalaze se veoma korisne informacije koje napadač može iskoristiti kasnije. Na primer, administrator mreže bi mogao poslati pitanje o podešavanju filtera određene marke i modela zaštitne barijere. Napadač koji otkrije ovu poruku saznaće korisne podatke o vrsti i parametrima kompanijske zaštitne barijere na osnovu čega bi je mogao zaobići i pristupiti mreži preduzeća.

Taj problem se može umanjiti ili izbeći pomoću pravila kojima se zaposlenima dozvoljava da se obraćaju diskusionim grupama sa anonimnih naloga, koji ne odaju preduzeće. Naravno, pravilnikom se od radnika mora zahtevati da ne saopštavaju informacije koje bi upućivale na preduzeće.

10-11 Diskete i drugi elektronski mediji

Pravilo: Ako radnik zatekne u svojoj kancelariji ili na stolu medije za snimanje računarskih podataka, kao što su diskete ili CD-ovi, a ne zna odakle potiču, ne sme ih koristiti.

Objašnjenje/Napomene: Jedna od metoda koju napadači koriste da bi instalirali zlonameran kôd jeste da snime program na disketu ili kompakt disk i obeleže ga veoma podsticajnim nazivom (na primer, „Podaci o plata-ma zaposlenih – poverljivo“). Potom ostave nekoliko primeraka u kancelarijama zaposlenih. Ukoliko se otvori samo jedna datoteka, napadačev zlonamerni kôd se izvršava. Na taj način se može stvoriti rupa u bezbednosnom sistemu, pomoću koje se može narušiti obezbeđenje sistema, ili oštetiti mreža.

10-12 Uklanjanje izmenljivih medija

Pravilo: Pre nego što bacite elektronski medij na kom su se nekada nalazile osetljive kompanijske informacije, čak i ako su sada izbrisane, pažljivo ga razmagnetišite ili oštetite tako da se ne može ponovo upotrebiti.

Objašnjenje/Napomene: Iako je danas uobičajeno uništavanje štampanih dokumenata, radnici ponekad ne uzmu u obzir opasnost koja preti ako se bace elektronski mediji na kojima su se nekada nalazile osetljive informacije. Hakeri će pokušati da povrate sve podatke na odbačenim elektronskim medijima. Radnici obično misle da se izbrisane datoteke sigurno ne mogu ponovo upotrebiti. Ta pretpostavka je potpuno netačna, ali ako se prenebregne, poverljivi poslovni podaci mogu pasti u pogrešne ruke. Dakle, sve elektronske medije koji sadrže, ili su nekada sadržali informacije koje nisu namenjene javnosti, morate potpuno obrisati ili uništiti po propisanim postupcima.

10-13 Čuvari ekrana zaštićeni lozinkama

Pravilo: Svi korisnici računara moraju imati lozinku na čuvarima ekrana i podesiti ga tako da se blokira nakon određenog vremenskog perioda neaktivnosti.

Objašnjenje/Napomene: Svaki radnik je odgovoran za podešavanje lozinke čuvara ekrana, kao i vremena neaktivnosti od najviše deset minuta. Cilj ovog pravila je da se spreči neovlašćena upotreba tuđeg računara. Štaviše, njime se sprečava da neovlašćene osobe, koje su uspele da uđu u zgradu, lako pristupe računarskim sistemima.

10-14 Izjava o davanju ili saopštavanju lozinke

Pravilo: Pre otvaranja novog naloga, zaposleni ili radnik po ugovoru mora potpisati pismenu izjavu da neće dati niti saopštiti lozinku nekome.

Objašnjenje/Napomene: U ugovoru bi trebalo da stoji da bi kršenje tog pravila moglo dovesti do disciplinskih mera, ili čak i prekida radnog odnosa.

Upotreba elektronske pošte

11-1 Prilozi elektronskih poruka

Pravilo: Ne smete otvarati datoteke priložene elektronskim porukama ukoliko ih ne očekujete u poslovne svrhe, ili ukoliko ih nije poslala osoba od poverenja.

Objašnjenje/Napomene: Sve priloge elektronskih poruka morate pažljivo proveriti. Možete zahtevati da sve priložene datoteke moraju unapred da budu najavljene. Na taj način smanjićete rizik od toga da obmanjivači navedu osoblje da otvori zlonamerne priloge.

Jedna od metoda neovlašćenog pristupa računarskom sistemu jeste da se zaposleni na prevaru navede da pokrene zlonamerni program, koji napravi rupu u bezbednosnom sistemu. Slanjem priloga elektronskih poruka koji sadrže izvršni kôd ili makro naredbe, napadač uspostavlja kontrolu korisnikovog računara.

Obmanjivač bi mogao poslati zlonamernu datoteku zajedno s elektronskom poštom, a potom pozvati primaoca i pokušati da ga nagovori da je otvori.

11-2 Automatsko prosleđivanje na spoljne adrese

Pravilo: Automatsko prosleđivanje dobijenih poruka na spoljne adrese elektronske pošte je zabranjeno.

Objašnjenje/Napomene: Cilj ovog pravila jeste da se spreči neovlašćeno primanje elektronskih poruka poslatih na internu adresu.

Zaposleni povremeno podese prosleđivanje poruka do adrese van firme kada nisu u kancelariji. Napadač može obmanuti radnika da podesi internu adresu elektronske pošte tako da prosleđuje poruke. Napadač se potom može predstaviti kao kolega koji ima internu kompanijsku adresu elektronske pošte, i navesti ljude da mu elektronskim putem pošalju osetljive informacije na internu adresu.

11-3 Prosleđivanje elektronskih poruka

Pravilo: Pri svakom zahtevu nepoznate osobe da se elektronska poruka prosledi treba proveriti identitet podnosioca zahteva.

11-4 Provera elektronske pošte

Pravilo: Za svaku elektronsku poruku koja naizgled dolazi od poverljive osobe, a u kojoj se traže tajne informacije, ili bilo kakva usluga u vezi sa računarima ili pomoćnom opremom, potrebno je dodatno odobrenje. Pogledajte postupke za proveru i ovlašćivanje.

Objašnjenje/Napomene: Napadač lako može da falsifikuje elektronsku poruku i njeno zaglavlje, tako da izgleda kao da je poslata s druge adrese. On takođe može poslati elektronsku poruku iz računarskog sistema kome je neovlašćeno pristupio, i tako steći lažna ovlašćenja za dobijanje podataka ili rad na računaru. Čak i ako proverite zaglavlje elektronske poruke, ne možete utvrditi da li dolazi iz internog računarskog sistema kome je neko neovlašćeno pristupio.

Korišćenje telefona

12-1 Učestvovanje u telefonskim anketama

Pravilo: Zaposleni ne smeju učestvovati u anketama niti odgovarati na pitanja bilo koje organizacije ili nepoznate osobe. Takve zahteve treba uputiti odeljenju za odnose s javnošću ili drugoj za to zaduženoj osobi.

Objašnjenje/Napomene: U pokušaju da se domognu značajnih informacija, obmanjivači pozovu zaposlenog tvrdeći da sprovode anketu. Izneadajuće je koliko ljudi rado daje poslovne i lične podatke nepoznatim osobama kada su uvereni da učestvuju u legitimnom istraživanju. Napadač umetne nekoliko bitnih pitanja među druga bezazlena pitanja. Konačno, te informacije može iskoristiti za narušavanje bezbednosti kompanijske mreže.

12-2 Objavljivanje internih telefonskih brojeva

Pravilo: Ako nepoznata osoba zatraži od zaposlenog njegov broj telefona, radnik odlučuje da li je to neophodno za obavljanje posla.

Objašnjenje/Napomene: Cilj ovog pravila jeste da radnicima nametne donošenje razboritih odluka o tome da li je neophodno da nekom daju svoj broj lokala. Kada posluju s ljudima koji i ne moraju da znaju lokal, najbezbednije je zamoliti ih da pozovu glavni broj kompanije i zatraže da ih potom spoje.

12-3 Lozinke u glasovnim porukama

Pravilo: Zabranjeno je ostavljati glasovne poruke o lozinkama.

Objašnjenje/Napomene: Obmanjivač često uspe da pristupi glasovnoj pošti radnika jer se lozinka lako pogađa. U ovoj vrsti napada, obmanjivač bi mogao i da napravi lažnu glasovnu poruku i ubedi drugog zaposlenog da mu otkrije svoju lozinku. Ako se pridržavate ovog pravila, sprečićete takvu prevaru.

Korišćenje faksa

13-1 Prosleđivanje faksova

Pravilo: Faksovi se ne smeju primati i prosleđivati trećem licu bez provere identiteta podnosioca zahteva.

Objašnjenje/Napomene: Kradljivci informacija ponekad na prevaru navedu radnike da faksom pošalju osetljive informacije na faks uređaj smešten u okviru firme. Pre nego što napadač žrtvi da broj faksa, on pozove nekog radnika koji ništa ne sumnja, na primer sekretaricu ili administrativnog pomoćnika, i zamoli ga da primi dokument da bi ga kasnije neko pokupio. Nakon što radnik primi faks, napadač ga pozove telefonom i zamoli da prosledi faks na drugu lokaciju, ponekad tvrdeći da mu je potreban za hitan sastanak. Budući da osoba koju je zamolio da prosledi faks obično ne shvata značaj podataka, pristaje da ispuni zahtev.

13-2 Provera uputstava primljenih faksom

Pravilo: Pre nego što se izvrše uputstva pristigla faksom, mora se proveriti da li je pošiljalac zaista zaposleni, ili neka druga osoba od poverenja. Najčešće je dovoljno telefonom pozvati pošiljaoca da bi se proverio zahtev.

Objašnjenje/Napomene: Zaposleni moraju biti oprezni kada faksom prime neuobičajene zahteve, poput molbi da unesu naredbe u računar, ili da obelodane informacije. Podaci u zaglavlju dokumenta mogu se falsifikovati izmenom parametara faks uređaja. Zato zaglavlje faksa nije prihvatljivo kao način utvrđivanja identiteta ili provere ovlašćenja.

13-3 Slanje osetljivih informacija faksom

Pravilo: Pre nego što pošalje osetljive informacije faksom do uređaja smeštenog u javnoj prostoriji, pošiljalac mora poslati naslovnu stranu. Primatelj primi tu stranu, i uzvрати slanjem neke druge strane, čime potvrdi da se lično nalazi kraj faks uređaja. Pošiljalac tek tada treba zaista da pošalje faks.

Objašnjenje/Napomene: Ovim postupkom provere identiteta pošiljalac se uverava da je primalac fizički prisutan kraj faks uređaja. Štaviše, njime se isključuje mogućnost da je telefonski broj prijemnog faksa prosleđen na drugu lokaciju.

13-4 Zabranjeno je faksom slati lozinke

Pravilo: Lozinke ne smete slati faksom ni u kojim okolnostima.

Objašnjenje/Napomene: Slanje identifikacionih podataka faksom nije bezbedno. Više radnika ima pristup mnogim faks uređajima. Štaviše, faks se oslanja na javnu telefonsku mrežu. Na centrali se može uključiti prosleđivanje poziva upućenih telefonskom broju prijemnog faksa, tako se faks zapravo šalje napadaču na neki drugi broj.

Upotreba glasovne pošte

14-1 Lozinke glasovne pošte

Pravilo: Lozinke glasovne pošte nikada nikome ne smete saopštavati. Pored toga, morate ih menjati svakih devedeset dana ili češće.

Objašnjenje/Napomene: Ljudi ostavljaju glasovne poruke sa poverljivim kompanijskim podacima. Da bi se ti podaci zaštitili, zaposleni bi trebalo često da menjaju lozinke glasovne pošte, i nikada ih ne smeju objavljivati. Osim toga, korisnici glasovne pošte ne bi smeli da ponove, iste ili slične lozinke za glasovnu poštu u roku od dvanaest meseci.

14-2 Lozinke u različitim sistemima

Pravilo: Korisnici glasovne pošte ne smeju upotrebljavati istu lozinku na više telefonskih ili računarskih sistema, bez obzira na to da li su unutrašnji ili spoljni.

Objašnjenje/Napomene: Kada neko koristi istu ili sličnu lozinku za više uređaja, kao što su glasovna pošta i računar, obmanjivač lakše može pogoditi više lozinke nakon što odredi jednu.

14-3 Podešavanje lozinke glasovne pošte

Pravilo: Korisnici i administratori glasovne pošte moraju upotrebljavati lozinke koje se teško pogađaju. One nikako ne smeju biti u vezi sa osobom koja ih koristi, niti sa preduzećem, i ne smeju sadržati predvidljivu šemu znakova.

Objašnjenje/Napomene: U lozinkama se ne smeju nalaziti uzastopne cifre, niti one koje se ponavljaju (tj. 1111, 1234, 1010), ne smeju se podudarati s telefonskim brojem lokala, niti se zasnivati na njemu. Ne smeju biti povezane s adresom, poštanskim brojem, datumom rođenja, brojem tablica na automobilu, telefonskim brojem, težinom, koeficijentom inteligencije, niti drugim predvidljivim privatnim podacima.

14-4 Stare glasovne poruke

Pravilo: Kada u sandučetu zateknete glasovne poruke koje niste preslušali, ali nisu označene kao nove, morate obavestiti administratora glasovne pošte o mogućem narušavanju bezbednosnog sistema, i morate odmah izmeniti lozinku glasovne pošte.

Objašnjenje/Napomene: Obmanjivači bi mogli pristupiti glasovnoj pošti na razne načine. Zaposleni koji otkrije da poruke koje nikada nije preslušao nisu označene kao nove, mora smatrati da je neko drugi neovlašćeno pristupio njegovoj glasovnoj pošti i preslušao poruke.

14-5 Pozdravne poruke na glasovnoj pošti

Pravilo: Radnici bi trebalo da ograniče informacije koje objavljuju u pozdravnoj poruci glasovne pošte. Obično ne treba davati podatke o sopstvenom rasporedu u toku dana, niti sa programom putovanja.

Objašnjenje/Napomene: Pozdravna poruka (koja se oglasi kad neko pozove) ne bi trebalo da sadrži prezime, broj lokala, niti razlog odsustva (kao što je putovanje, raspored godišnjeg odmora ili dnevni program). Napadač te podatke može iskoristiti da bi osmislio uverljivu priču pri pokušaju obmane drugih lica.

14-6 Šabloni u lozinkama glasovne pošte

Pravilo: Korisnici glasovne pošte ne smeju birati lozinke čiji jedan deo ostaje stalan, dok se drugi deo menja prema predvidljivom šablonu.

Objašnjenje/Napomene: Na primer, nemojte koristiti lozinke kao što su 743501, 743502, 743503 i tako dalje, pri čemu se poslednje dve cifre odnose na tekući mesec.

14-7 Poverljivi ili privatni podaci

Pravilo: Ne smete ostavljati glasovne poruke sa poverljivim ili privatnim podacima.

Objašnjenje/Napomene: Kompanijski telefonski sistem je uglavnom slabije zaštićen od računarskog sistema. Lozinke su obično nizovi brojeva, što značajno ograničava broj mogućih kombinacija pomoću kojih bi napadač pogodio lozinku. Štaviše, u nekim organizacijama rukovodioci daju lozinke glasovne pošte sekretaricama i drugom administrativnom osoblju zaduženom za primanje poruka. Kada se sve što je prethodno pomenuto uzme u obzir, nikada ne smete ostavljati glasovne poruke sa osetljivim informacijama.

Lozinke

15-1 Zaštita preko telefona

Pravilo: Lozinke nikada ne saopštavajte preko telefona.

Objašnjenje/Napomene: Napadači mogu prisluškivati telefonske razgovore, lično ili pomoću uređaja.

15-2 Obelodanjivanje računarskih lozinki

Pravilo: Ni u kojim okolnostima nijedan korisnik računara ne sme obelodaniti svoju lozinku ukoliko mu to prethodno ne odobri odgovorni rukovodilac informatičkog odeljenja.

Objašnjenje/Napomene: Obmanjivači često pokušavaju da navedu ljude, koji ništa ne sumnjaju, da im kažu korisnička imena i lozinke. Ovo pravilo je izuzetno važan korak pri smanjivanju rizika od obmane zaposlenih. Stoga se ovog pravila moraju strogo pridržavati svi u preduzeću.

15-3 Lozinke na Internetu

Pravilo: Osoblje nikada ne sme upotrebljavati istu ili sličnu lozinku u bilo kom kompanijskom sistemu i na Internetu.

Objašnjenje/Napomene: Zlonamernici mogu napraviti Web lokaciju koja navodno nudi nešto vredno ili mogućnost osvajanja nagrade. Da bi se registrovao, posetilac lokacije mora uneti svoju adresu elektronske pošte, korisničko ime i lozinku. Budući da mnogi koriste iste ili slične podatke u više situacija, zlonamerni operater Web lokacije će pokušati da upotrebi izabranu lozinku ili njene varijacije za napad na žrtvin kućni ili poslovni

računarski sistem. Poslovni računar posetioca se ponekad može identifikovati na osnovu adrese elektronske pošte unete za vreme registracije.

15-4 Lozinke u različitim sistemima

Pravilo: Kompanijsko osoblje nikada ne sme koristiti istu ili sličnu lozinku u više sistema. Ovo pravilo se odnosi na različite tipove uređaja (računare i glasovnu poštu); različite lokacije uređaja (kućne i poslovne); i različite tipove sistema, uređaja (usmerivač ili zaštitnu barijeru), ili programa (baze podataka ili aplikacije).

Objašnjenje/Napomene: Napadači se oslanjaju na ljudsku prirodu da bi neovlašćeno pristupili računarskim sistemima i mrežama. Oni znaju da mnogi koriste istu ili sličnu lozinku na svakom sistemu kom pristupaju, da ne bi pamtili više lozinki. Stoga će napadač pokušati da sazna lozinku na jednom sistemu na kom žrtva ima nalog. Kada je dobije, verovatnoća je velika da će mu ta lozinka ili njena varijacija obezbediti pristup drugim sistemima i uređajima koje zaposleni koristi.

15-5 Ponovna upotreba lozinki

Pravilo: Nijedan korisnik računara ne sme da ponovi istu ili sličnu lozinku u periodu od osamnaest meseci.

Objašnjenje/Napomene: Ako napadač zaista otkrije korisnikovu lozinku, čestom izmenom lozinki se umanjuje potencijalna šteta. Ako je nova lozinka drugačija od prethodnih, napadaču je teže da je pogodi.

15-6 Šablonske lozinke

Pravilo: Ne smete birati lozinke čiji jedan deo ostaje stalan, a ostali elementi se menjaju prema predvidljivom šablonu.

Objašnjenje/Napomene: Na primer, ne koristite lozinke kao što su Kevin01, Kevin02, Kevin03 i tako dalje, pri čemu se poslednje dve cifre odnose na tekući mesec.

15-7 Izbor lozinki

Pravilo: Korisnici računara bi trebalo da osmišljavaju ili biraju lozinke koje odgovaraju sledećim zahtevima:

- Lozinka mora imati najmanje osam znakova za standardne korisničke naloge, i najmanje dvanaest znakova za privilegovane naloge.

- Mora sadržati najmanje jedan broj, jedan simbol (kao što su \$, _, !, &), jedno malo slovo, i jedno veliko slovo (ukoliko takve varijante podržava operativni sistem).
- Ne sme se sastojati od: reči iz rečnika bilo kog jezika, reči u vezi s porodicom, hobijima, prevoznim sredstvima, poslom, automobilskim tablicama, matičnim brojem, adresom, telefonskim brojem, imenom ljubimca, rođendanom, niti izrazima u kojima se takve reči nalaze.
- Ne sme biti varijanta prethodno korišćenih lozinki, pri čemu jedan element ostaje isti, a drugi se menja, kao što su kevin, kevin1, kevin2; ili kevinjan, kevinfeb.

Objašnjenje/Napomene: Pomoću navedenih parametara dobićete lozinku koju će obmanjivač teško pogoditi. Druga mogućnost je da se koristi metoda suglasnika i samoglasnika, kojom se dobijaju lozinke koje je lako izgovoriti i lako se pamte. Da biste osmislili takvu lozinku, naizmenično upišite suglasnike i samoglasnike. Primeri su reči MIXOCASO i CUSOJENA.

15-8 Zapisivanje lozinki

Pravilo: Zaposleni bi trebalo da zapisuju lozinke samo kada ih stavljaju na sigurno mesto udaljeno od računara ili drugog uređaja zaštićenog lozinkom.

Objašnjenje/Napomene: Ne preporučuje se zapisivanje lozinki. Međutim, pod nekim okolnostima, to je neophodno. Na primer, zaposleni koji ima više naloga na različitim računarskim sistemima, možda mora zapisati svoje lozinke. Svaku zapisanu lozinku morate staviti na bezbedno mesto, daleko od računara. Ni u kom slučaju ne smete lozinku stavljati ispod tastature, niti je kačiti za monitor.

15-9 Tekstualne lozinke u datotekama

Pravilo: Lozinke pisane običnim tekstom ne smeju se snimati u računarske datoteke, niti kao tekst koji se pojavljuje pritiskom na funkcijski taster. Kada je neophodno, lozinke možete snimiti šifrovane, ako to odobri informatičko odeljenje, da bi se sprečilo neovlašćeno objavljivanje.

Objašnjenje/Napomene: Napadač lako može doći do lozinki ako su snimljene u tekstualne datoteke, komandne datoteke, povezane s funkcijskim tasterima terminala, snimljene u datoteke za prijavljivanje za rad, makro naredbe ili skriptove, ili bilo kakve datoteke koje sadrže lozinke za FTP lokacije.

PRAVILA ZA RADNIKE KOJI IMAJU DALJINSKI PRISTUP

Osobe koje daljinski pristupaju sistemu nalaze se izvan zaštitne barijere preduzeća, pa su lakša meta napada. Ova pravila će vam pomoći da sprečite obmanjivače da preko takvih radnika dođu do vaših podataka.

16-1 Tanki klijenti

Pravilo: Svi radnici kompanije ovlašćeni da daljinski pristupe mreži treba da koriste tanak klijent (engl. *thin client*) za priključenje.

Objašnjenje/Napomene: Kada napadač analizira strategiju napada, on pokušava da identifikuje korisnike koji kompanijskoj mreži pristupaju sa spoljnih lokacija. Dakle, takvi radnici su glavne mete. Njihovi računari obično nisu pod strogom bezbednosnom kontrolom, pa mogu predstavljati slabu tačku koja će nauditi kompanijskoj mreži.

Na svaki računar povezan u internu mrežu može se tajno postaviti snimač tastature, ili se ovlašćena veza može preoteti. Da biste izbegli probleme, možete primeniti taktiku tankih klijenata. Tanak klijent je sličan radnoj stanici bez diska, ili glupom terminalu. Udaljeni računar ne može da snima podatke; umesto toga, operativni sistem, aplikativni programi i svi podaci, nalaze se na kompanijskoj mreži. Pristup mreži preko tankog klijenta značajno umanjuje rizik od nezakrpljenih sistema, zastarelih operativnih sistema, i zlonamernih programa. U skladu s tim, održavanje bezbednosti računara službenika koji imaju daljinski pristup efikasno je i olakšano centralizacijom. Umesto da se oslonite na to da će jedan neiskusni radnik ispravno rešavati bezbednosna pitanja, bolje je da te odgovornosti prepustite obučanim administratorima sistema ili mreže.

16-2 Bezbednosni softver za računarske sisteme

Pravilo: Svaki spoljni računarski sistem koji se povezuje na računarsku mrežu preduzeća mora imati antivirusni softver i ličnu zaštitnu barijeru (hardversku ili softversku). Antivirusne datoteke moraju se ažurirati bar jednom nedeljno.

Objašnjenje/Napomene: Radnici koji imaju daljinski pristup najčešće ne poznaju dovoljno pravila, pa mogu slučajno otvoriti rupu u bezbednosti računarskog sistema i kompanijske mreže. Zato oni predstavljaju ozbiljan rizik po bezbednosni sistem ako se ne obuče na odgovarajući način.

Pored instaliranja antivirusnog softvera da bi se zaštitili od zlonamernog koda, neophodna je i barijera koja će sprečiti zlonamernike da pristupe uslugama koje se nude u sistemu.

Rizik koji prei ako se ne primeni bar minimalna zaštitna tehnologija ne sme se potceniti, što dokazuje i napad na Microsoft. Na računaru jednog Microsoftovog radnika, koji je imao daljinski pristup Microsoftovoj mreži, bio je instaliran trojanac. Uljez, ili grupa njih, uspeli su da pomoću ovlašćene daljinske veze tog radnika pristupe Microsoftovoj razvojnoj mreži i ukradu razvojni izvorni kôd.

PRAVILA ZA KADROVSKO ODELJENJE

Kadrovsko odeljenje posebno je odgovorno da zaštiti radnike od prevaranata koji pokušavaju da otkriju lične podatke. Oni su takođe odgovorni da zaštite preduzeće od poteza nezadovoljnih bivših radnika.

17-1 Zaposleni koji napuštaju firmu

Pravilo: Kada neki zaposleni napušta firmu, ili je otpušten, kadrovsko odeljenje mora odmah učiniti sledeće:

- ukloniti ime osobe iz štampanog telefonskog imenika firme, odnosno onog na mreži, i isključiti ili proslediti njegovu glasovnu poštu;
- obavestiti osoblje na ulazima u zgradu i u velikim holovima;
- dodati ime zaposlenog spisku onih koji su napustili firmu; spisak će se elektronskim putem slati svim radnicima najmanje jednom nedeljno.

Objašnjenje/Napomene: Zaposleni na ulazu zgrade moraju biti obavesteni ko više ne radi u firmi da bi sprečili nekadašnjeg zaposlenog da ponovo uđe u prostorije preduzeća. Štaviše, ako o tome obavestite i ostalo osoblje, sprečićete bivšeg zaposlenog da se uspešno predstavi kao aktivni radnik i na prevaru navede bivše kolege da učine nešto što će naškoditi kompaniji.

U nekim okolnostima, neophodno je zahtevati od svakog korisnika iz odeljenja bivšeg zaposlenog da promeni lozinku. (Kada su mene otpustili iz firme GTE isključivo zbog moje reputacije kao hakera, kompanija je zahtevala od svih zaposlenih u firmi da promene lozinke.)

17-2 Obaveštavanje informatičkog odeljenja

Pravilo: Kad god neko napusti firmu ili dobije otkaz, kadrovsko odeljenje bi trebalo odmah o tome da obavesti informatičko odeljenje, kako bi isključili računarske naloge, u šta se ubrajaju i svi nalozi za pristup bazama podataka, za daljinsko povezivanje ili pristup Internetu.

Objašnjenje/Napomene: Izuzetno je značajno da se bivšem radniku onemogući pristup svim računarskim sistemima, mrežnim uređajima, bazama podataka, i svim drugim pomoćnim računarskim uređajima odmah po njegovom odlasku. U suprotnom, ogorčeni radnik može zateći širom otvorena vrata za pristup kompanijskim računarskim sistemima, i naneti znatnu štetu.

17-3 Poverljive informacije u postupku zapošljavanja

Pravilo: U oglasima i drugim oblicima javnog traženja kandidata za popunjavanje upražnjenih radnih mesta trebalo bi što više izbegavati pominjanje računarskog hardvera i softvera koji koristi kompanija.

Objašnjenje/Napomene: Uprava i kadrovsko osoblje trebalo bi da daju samo one informacije u vezi s računarskim hardverom i softverom preduzeća koje su neophodne za dobijanje biografija kvalifikovanih kandidata.

Hakeri čitaju novine i izjave za štampu, i posećuju Internet lokacije da bi pronašli ponude za posao. Kompanije često objave suviše informacija o tipu hardvera i softvera koji koriste da bi privukli buduće radnike. Kada uljez sazna koji informacioni sistem koristi žrtva, naoružan je za sledeću fazu napada. Na primer, ako zna da određena kompanija upotrebljava operativni sistem VMS, napadač će možda pozvati firmu pod nekim izgovorom da bi utvrdio postojeću verziju, a potom će na prevaru poslati hitnu bezbednosnu zakrpu koja naizgled stiže od proizvođača softvera. Kada se zakrpa instalira, napadač će imati pristup unutrašnjim sistemima.

17-4 Privatni podaci zaposlenih

Pravilo: Kadrovsko odeljenje nikada ne sme objavljivati privatne podatke bilo kog sadašnjeg ili bivšeg zaposlenog, radnika po ugovoru, savetnika, privremenog radnika, niti stažiste, ukoliko ne dobije poseban pisani pristanak zaposlenog ili upravnika kadrovskog odeljenja.

Objašnjenje/Napomene: Agencije za zapošljavanje, privatni istražitelji i kradljivci identiteta žele da se domognu privatnih podataka o zaposlenima kao što su brojevi zaposlenih, matični brojevi, datumi rođenja, istorijat plate, finansijski podaci (uključujući i informacije o stanju na računu) i podaci u vezi sa zdravstvenim osiguranjem. Obmanjivač se na osnovu tih podataka može predstaviti kao taj zaposleni. Pored toga, imena novih zaposlenih mogu biti izuzetno vredne informacije kradljivcima, jer će se novi radnici najčešće povinovati svim zahtevima pretpostavljenih osoba ili osoba na višim pozicijama, odnosno svakoga ko se predstavi da radi u obezbeđenju firme.

17-5 Provera radnika

Pravilo: Trebalo bi proveriti sve nove zaposlene, radnike po ugovoru, savetnike, privremene radnike i stažiste pre nego što im se posao ponudi ili se s njima sklopi ugovor.

Objašnjenje/Napomene: Zbog troškova koje iziskuje, provera radnika se može ograničiti samo na radna mesta za koja su potrebni poverljivi ljudi. Imajte na umu da svaka osoba koja ima fizički pristup kancelarijama firme može biti potencijalna opasnost. Na primer, čistači ulaze u kancelarije, pa samim tim imaju pristup računarskim sistemima. Napadač koji lično dođe do računara može za manje od jednog minuta instalirati hardverski snimač tastature, kako bi kasnije saznao lozinke.

Hakeri će se nekada potruditi i da dobiju posao samo da bi se domogli računarskih sistema i mreža određene firme. Napadač lako dođe do imena agencije za čišćenje koju unajmljuje dotična kompanija, tako što pozove odgovornog zaposlenog u firmi, predstavljajući se da radi u firmi za čišćenje.

PRAVILA ZA FIZIČKO OBEZBEĐENJE

Iako se obmanjivači nerado pojavljuju u preduzeću kome žele da naškode, postoje izuzeci. Ova pravila će vam pomoći da fizički obezbedite svoje prostorije.

18-1 Identifikacija nezaposlenih lica

Pravilo: Kuriri i druga lica koja nisu zaposlena, a redovno ulaze u firmu, moraju imati posebne propusnice ili neki drugi oblik dokumenta za identifikaciju u skladu s pravilnikom obezbeđenja firme.

Objašnjenje/Napomene: Licima koja nisu zaposlena, a koja redovno ulaze u zgradu (na primer, da bi restoranu dostavili hranu ili pića, ili da bi popravili aparate za fotokopiranje ili instalirali telefone) trebalo bi izdati posebne propusnice u tu svrhu. Ostali koji moraju da ulaze u firmu samo povremeno, ili u pojedinačnim slučajevima, moraju se smatrati posetioci-ma i biti pod nadzorom sve vreme.

18-2 Identifikacija posetilaca

Pravilo: Svi posetioci moraju pokazati važeću ličnu kartu, ili neki drugi dokument sa slikom, da bi ušli u prostorije firme.

Objašnjenje/Napomene: Obezbeđenje ili službenik prijemnog odeljenja trebalo bi da fotokopiraju identifikacioni dokument pre nego što posetiocu izdaju oznaku. Fotokopiju treba zadržati u dnevniku posetilaca. Čuvar ili službenik prijemnog odeljenja mogu i da unesu identifikacione podatke u dnevnik posetilaca. Posetioci ne smeju sami da upisuju svoje identifikacione podatke.

Obmanjivači koji žele da uđu u zgradu uvek upišu lažne informacije u dnevnik. Iako nije teško nabaviti lažnu ličnu kartu i saznati ime zaposlenog kog navodno posećuje, ukoliko odgovorni zaposleni unese identifikacione podatke u dnevnik nivo bezbednosti se povećava.

18-3 Nadzor posetilaca

Pravilo: Posetioce sve vreme mora pratiti čuvar, ili zaposleni.

Objašnjenje/Napomene: Popularan trik obmanjivača je da ugovori posetu nekom zaposlenom (na primer, traži da vidi inženjera proizvodnje, pod izgovorom da radi kod strateškog partnera). Nakon što ga otprate na sastanak, on uveri domaćina da može sam da se vrati do hola. Na taj način on slobodno tumara zgradom i eventualno pristupa osetljivim informacijama.

18-4 Privremene propusnice

Pravilo: Zaposleni iz drugih ogranaka firme koji nemaju propusnice uza se moraju pokazati važeću ličnu kartu ili drugi dokument sa slikom, da bi im se izdala privremena propusnica za posetioce.

Objašnjenje/Napomene: Napadači se često predstavljaju kao zaposleni iz drugih kancelarija ili ogranaka firme da bi ušli u zgradu.

18-5 Hitna evakuacija

Pravilo: U hitnim situacijama ili pri vežbama, obezbeđenje se mora uveriti da su svi evakuisani iz prostorija firme.

Objašnjenje/Napomene: Obezbeđenje mora proveriti da li je neko ostao u toaletima ili kancelarijama. Prema ovlašćenjima vatrogasaca ili drugog nadležnog tela, obezbeđenje mora obratiti pažnju na to da li neko napušta zgradu dugo nakon evakuacije.

Industrijski špijuni i vešti hakeri mogu izazvati diverzije da bi ušli u zgradu ili obezbeđenu oblast. Jedna od poznatih diverzija jeste da se u vazduh pusti butil-merkaptan bezopasna hemijska supstanca, koja miriše kao prirodni gas. Kada osoblje započne evakuaciju, odvažni napadač krađe informacije ili pristupa računarskim sistemima preduzeća. Još jedna taktika koju koriste kradljivci informacija jeste da se ostane u toaletu ili ormaru u vreme planirane vežbe evakuacije, ili nakon paljenja dimne signalne rakete ili nekog sličnog uređaja kojim se izaziva hitna evakuacija.

18-6 Posetioci u prostoriji za poštu

Pravilo: Posetiocima je zabranjen pristup prostoriji za poštu bez nadzora radnika kompanije.

Objašnjenje/Napomene: Cilj ovog pravila je da se uljez spreči u zameni, slanju ili krađi interne pošte.

18-7 Broj tablica na vozilu

Pravilo: Ako preduzeće ima čuvani parking, obezbeđenje treba da ubeleži broj tablica svakog vozila koje uđe.

18-8 Kontejneri za smeće

Pravilo: Kontejneri za smeće uvek moraju biti u okviru čuvanog prostora, nedostupni javnosti.

Objašnjenje/Napomene: Hakeri i industrijski špijuni mogu doći do vrednih informacija iz kanti za smeće u preduzeću. Sud smatra da je smeće pravno napušteno vlasništvo, pa je *kopanje po smeću* potpuno legalno, ako se kontejneri za smeće nalaze na javnom terenu. Zato je važno smestiti kontejnere u čuvan prostor firme, gde kompanija ima pravo da zaštiti njihov sadržaj.

PRAVILA ZA SLUŽBENIKE PRIJEMNOG ODELJENJA

Službenici prijemnog odeljenja se obično prvi susreću s obmanjivačima, a ipak se retko obučavaju da prepoznaju i spreče napadača. Uvedite ova pravila kako biste pomogli tim službenicima da bolje zaštite preduzeće i podatke.

19-1 Interni telefonski imenik

Pravilo: Davanje informacija iz internog kompanijskog imenika trebalo bi ograničiti samo na zaposlene.

Objašnjenje/Napomene: Sve titule, imena, telefonski brojevi i adrese zaposlenih koje se nalaze u kompanijskom telefonskom imeniku treba smatrati internim informacijama, i davati ih u skladu s klasifikacijom podataka i pravilima rada s internim informacijama.

Osim toga, lica koja pozovu firmu moraju znati ime i lokal osobe s kojom hoće da razgovaraju. Iako službenik na centrali može spojiti pozivaoca sa traženom osobom ukoliko ne zna lokal, davanje broja lokala bi trebalo da bude zabranjeno. (Radoznalci koji se radije vode nečijim primerom, mogu proveriti kako ovo pravilo funkcioniše ako pozovu neku američku državnu agenciju i zamole operatera da im kaže broj nečijeg lokala.)

19-2 Telefonski brojevi određenih odeljenja ili timova

Pravilo: Zaposleni ne smeju saopštavati direktne telefonske brojeve kompanijske službe za informatičku podršku korisnicima, odeljenja za telekomunikacije, računarskih operatera ili administratora sistema, bez prethodne provere da li je podnosilac zahteva ovlašćen da nazove pomenute timove. Kada službenik na centrali spaja nekoga sa ovim timovima, mora preneti ime pozivaoca.

Objašnjenje/Napomene: Iako je za neke organizacije ovo pravilo isuviše ograničavajuće, ono otežava obmanjivačima da se lažno predstave i navedu zaposlenog da prosledi poziv sa svog lokala (što u nekim telefonskim sistemima izgleda kao da je poziv upućen iz same firme), ili da žrtvi saopšte brojeve tih lokala i time zadobiju poverenje.

19-3 Prosleđivanje informacija

Pravilo: Radnici na telefonskoj centrali i službenici prijemnog odeljenja ne smeju primati poruke, niti prosleđivati informacije trećem licu kog lično ne poznaju kao aktivnog radnika.

Objašnjenje/Napomene: Obmanjivači vešto navode zaposlene da garantuju za njihov identitet. Jedan od trikova obmanjivanja jeste da se nabavi telefonski broj centrale, a potom da se službenik pod nekim izgovorom zamoli da primi poruke za tu osobu. Potom, kada pozove žrtvu, napadač se predstavi kao kolega, zatraži osetljive podatke ili neku uslugu, i ostavi broj centrale kao broj na koji ga ovaj može pozvati. Napadač kasnije pozove službenika na centrali, a ovaj mu izdiktira poruku koju mu je ostavila žrtva, ništa ne sumnjajući.

19-4 Preuzimanje predmeta

Pravilo: Pre nego što preda i jedan predmet kuriru ili nekoj drugoj neproverenoj osobi, službenik prijemnog odeljenja ili čuvar mora zatražiti dokument sa slikom i zapisati lične podatke kurira.

Objašnjenje/Napomene: Jedna od taktika obmanjivanja jeste da se zaposleni na prevaru navede da pošalje osetljive materijale navodno ovlašćenom kolegi ostavljajući ih u prijemnom odeljenju ili holu za isporučivanje. Naravno, čuvar ili službenik prijemnog odeljenja smatraju da se paket sme poslati. Obmanjivač se potom lično pojavi ili pošalje kurira da pokupi paket.

PRAVILA ZA TIM KOJI EVIDENTIRA INCIDENTE

Svaka kompanija bi trebalo da organizuje centralizovan tim koji se obaveštava kada se utvrdi bilo koji oblik napada na bezbednosni sistem firme. Slede neki saveti za organizovanje i strukturiranje rada ovog tima.

20-1 Tim za evidentiranje incidenata

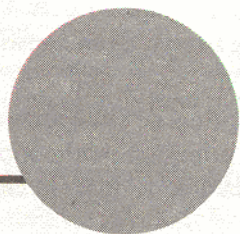
Pravilo: Treba odrediti pojedinca ili tim kojima će zaposleni prijavljivati svako narušavanje bezbednosnog sistema. Svim zaposlenima treba obezbediti podatke za kontakt s timom.

Objašnjenje/Napomene: Zaposleni moraju shvatiti kako da prepozna-ju napad, i treba ih obučiti da svaki incident prijave zaduženom timu. Važno je i da organizacija utvrdi posebna ovlašćenja tog tima, kako bi mogli da preduzmu odgovarajuće mere kada se incident prijavi.

20-2 Napad koji je u toku

Pravilo: Kada se tim za evidentiranje incidenata obavesti o napadu obmanjivača koji je u toku, oni treba odmah da upozore sve zaposlene koji pripadaju ciljnim grupama.

Objašnjenje/Napomene: Tim za evidentiranje incidenata ili odgovor-ni rukovodilac takođe moraju doneti odluku o tome da li da upozore čita-vu kompaniju. Kada odgovorna osoba ili tim imaju osnova da veruju da napad još uvek traje, moraju pokušati da umanje eventualnu štetu tako što će obavestiti zaposlene da budu na oprezu.



Pregled bezbednosnih metoda

Spiskovi i dijagrami koji slede ukratko opisuju metode obmane navedene u poglavljima od 3 do 15, i postupke provere iz poglavlja 16. Prilagodite ove podatke svojoj organizaciji i dajte ih svim radnicima da bi ih primenili kada se ukaže problem bezbednosti informacija.

PREPOZNAVANJE NAPADA

Naredne tabele i spiskovi će vam pomoći da uočite napad sistematskog obmanjivanja.

Ciklus obmane

POSTUPAK

Istraživanje

Razvijanje dobrih odnosa i poverenja

OPIS

Ispituju se i podaci iz javnih izvora kao što su godišnji izveštaji, marketinške brošure, prijave patenata, isecci iz štampe, stručni časopisi i Web lokacije. Tu spada i kopanje po smeću.

Upotreba internih informacija, lažno predstavljanje, pominjanje osoba koje žrtva poznaje, molba za pomoć, ili pozivanje na autoritet.

Zloupotreba poverenja

Traženje informacija ili usluge od žrtve. U obrnutoj žaoci, manipulisanje žrtvom da od napadača zatraži pomoć.

Upotreba informacija

Ako su dobijene informacije samo korak do konačnog cilja, napadač pribegava prethodno pomenu tim koracima ciklusa dok ne dođe do cilja.

Uobičajene metode obmanjivanja

- Izdavanje za kolegu
- Izdavanje za zaposlenog u firmi dobavljača usluga, partnerskoj firmi, ili kriminalističkoj službi
- Izdavanje za nekog ko je na višem položaju
- Izdavanje za novog zaposlenog kome treba pomoć
- Izdavanje za dobavljača usluga ili proizvođača sistema koji zove da bi ponudio sistemsku zakrpu ili najnoviju verziju
- Nuđenje pomoći ako bi nastao problem, potom izazivanje problema, čime se žrtva navede da od napadača zatraži pomoć
- Slanje žrtvi besplatnog softvera ili zakrpe da ih instalira
- Slanje virusa ili trojanskog konja u prilogu elektronske poruke
- Upotreba lažnog okvira za dijalog u kom se od korisnika traži da se ponovo prijavi za rad ili da ponovo unese lozinku
- Snimanje žrtvinih pritisaka na tastere pomoću računarskog sistema ili programa
- Ostavljanje na radnom mestu disketa ili kompakt diskova sa zlonamernim softverom
- Korišćenje interne terminologije da bi se zadobilo nečije poverenje
- Nuđenje nagrade da bi se neko registrovao na Web lokaciji pomoću korisničkog imena i lozinke
- Ostavljanje dokumenata ili datoteka u kompanijskoj prostoriji za poštu radi isporuke u kancelarije
- Prilagođavanje zaglavlja faksa tako da se čini da je poslat sa interne lokacije
- Umoljavanje službenika prijemnog odeljenja da primi i prosledi faks
- Zahtev da se datoteka prosledi do naizgled interne lokacije

- Podešavanje glasovne pošte tako da pozivaoci pomisle da im je napadač kolega
- Pretvaranje napadača da dolazi iz drugog ogranaka preduzeća, i traženje da mu se u sistemu preduzeća otvori elektronsko sanduče.

Znaci koji upozoravaju na mogući napad

- Neko odbija da vam kaže broj na koji ga možete pozvati
- Neobičan zahtev
- Naglašavanje visokog položaja
- Naglašavanje hitnosti slučaja
- Pretnja negativnim posledicama u slučaju odbijanja saradnje
- Nelagodni razgovor pri ispitivanju
- Pominjanje poznatih osoba
- Deljenje komplimenata ili laskanje
- Flertovanje

Uobičajene mete napada

TIP ŽRTVE

Neko ko nije svestan značaja informacija

Lica s posebnim ovlašćenjima

Proizvođači ili davaoci usluga

Posebna odeljenja

PRIMERI

Službenici prijemnih odeljenja, službenici na telefonskoj centrali, sekretarice i pomoćnici, čuvari.

Informatička ili tehnička podrška korisnicima, administratori računarskog sistema, računarski operateri, administratori telefonskog sistema.

Proizvođači računarskog hardvera i softvera, proizvođači sistema za glasovnu poštu.

Računovodstvo, kadrovsko odeljenje.

Faktori koji olakšavaju napad na kompanije

- Velik broj zaposlenih
- Više ogranaka
- Podaci o lokaciji zaposlenih u porukama glasovne pošte

- Objavljivanje broja lokala
- Nepostojanje bezbednosne obuke
- Nepostojanje sistema klasifikacije podataka
- Nepostojanje plana za prijavljivanje incidenata i reagovanje na njih

PROVERA I KLASIFIKACIJA PODATAKA

Ove tabele i blok-dijagrami će vam pomoći da reagujete na traženje informacija ili usluga koji mogu biti meta obmanjivača.

Postupak provere identiteta

POSTUPAK	OPIS
Identifikacija poziva	Proverite da li je poziv interni, i da li ime i broj lokala odgovaraju identitetu sagovornika.
Uzvratanje poziva	Potražite ime podnosioca zahteva u kompanijskom imeniku i pozovite ga na navedeni broj lokala.
Garantovanje	Zatražite od poverljivog radnika da garantuje za identitet podnosioca zahteva.
Deljena interna tajna	Zatražite da vam kaže tajnu koju deli čitavo preduzeće, kao što je lozinka ili dnevni kôd.
Nadzornik ili pretpostavljeni	Stupite u vezu s neposrednim pretpostavljenim tog radnika i zatražite da on potvrdi njegov identitet i status u firmi.
Bezbedna elektronska pošta	Zatražite da vam pošalju digitalno potpisanu poruku.
Lično prepoznavanje glasa	Ako neki zaposleni lično poznaje onoga za koga se sagovornik izdaje, pozovite ga da proveriti da li je to njegov glas.
Izmenljive lozinke	Koristite vremenski žeton kao što je Secure ID, ili neko drugo pouzdano sredstvo za identifikaciju.
Lično	Zatražite od podnosioca zahteva da lično dođe sa propusnicom za zaposlene ili nekim drugim dokumentom za identifikaciju.

Postupak provere statusa zaposlenog

POSTUPAK

Provera u kompanijskom imeniku

Potvrda od pretpostavljenog podnosioca zahteva

Potvrda od odeljenja ili radnog tima podnosioca zahteva

OPIS

Proverite da li se ime zaposlenog nalazi u imeniku na mreži.

Pozovite njegovog pretpostavljenog na broj naveden u kompanijskom imeniku.

Pozovite odeljenje ili radni tim podnosioca zahteva i proverite da li je još uvek zaposlen u firmi.

337

Postupak utvrđivanja ovlašćenja za posedovanje informacija

POSTUPAK

Pogledajte spisak odgovornosti radnih mesta/timova

Zatražite odobrenje od svog pretpostavljenog

Zatražite odobrenje od osobe zadužene za informacije ili njegovog zamenika

Proverite ovlašćenje pomoću automatskog alata

OPIS

Pogledajte objavljene spiskove osoba koje su ovlašćene da poseduju određene poverljive informacije.

Pozovite svog pretpostavljenog, ili pretpostavljenog podnosioca zahteva, i zatražite odobrenje da mu ispunite zahtev.

Pitajte osobu zaduženu za informacije da li je podnosilac zahteva ovlašćen da poseduje date podatke.

Proverite ovlašćenja u posebnoj bazi podataka.

Pregled bezbednosnih metoda

Kriterijumi za proveru osoba koje nisu zaposlene u firmi

KRITERIJUM POSTUPAK

Odnos

Proverite da li je firma koja podnosi zahtev davalac usluga, strateški partner, ili neka druga firma koja je u odgovarajućem odnosu s vašom.

Identitet

Proverite identitet i status zaposlenog u partnerskoj firmi.

Čuvanje tajne Proverite da li je podnosilac zahteva potpisao ugovor o čuvanju poverljivih informacija vaše firme.

Pristup Uputite zahtev pretpostavljenom kada su podaci klasifikovani kao osetljiviji od internih.

Klasifikacija podataka

KLASIFIKACIJA	OPIS	POSTUPAK
Javni	Mogu se slobodno saopštavati u javnosti.	Nema potrebe proveravati.
Interni	Za upotrebu u okviru firme.	Proverite da li je podnosilac zahteva i dalje zaposlen u vašoj firmi, a ako nije, da li je potpisao ugovor o čuvanju informacija, i da li ga je rukovodstvo ovlastilo.
Privatni	Podaci lične prirode namenjeni za upotrebu isključivo u okviru organizacije.	Proverite da li je podnosilac zahteva i dalje zaposlen u vašoj firmi, a ako nije, da li je ovlašćen da poseduje te informacije. Proverite sa kadrovskim odeljenjem da li smete da saopštite lične podatke ovlašćenim zaposlenima ili drugim podnosiocima zahteva.
Poverljivi	Znaju ih samo ona lica u okviru organizacije kojima je to neophodno za rad.	Kod osobe zadužene za informacije proverite identitet podnosioca zahteva i njegova ovlašćenja. Saopštite ih samo uz prethodno pismeno odobrenje pretpostavljenog, osobe zadužene za informacije, ili njihovog zamjenika. Proverite da li je podnosilac zahteva potpisao ugovor o čuvanju podataka. Samo uprava sme da objavljuje poverljive informacije licima koje firma ne zapošljava.

Kako reagovati kad vam neko traži informacije

Zlatna pitanja

Kako da znam da li je ova osoba ona za koju se izdaje?
Kako da znam da je ova osoba ovlašćena da zahteva tako nešto?

Osoba zahteva sledeće informacije:

PRIMERI

Struktura odgovornosti,
imena i zvanja zaposlenih

Interni telefonski brojevi
dodeljeni zaposlenima,
interni faks brojevi, interni
brojevi zgrada i spiskovi
odeljenja

Lični telefonski brojevi (kućni
ili mobilni), broj socijalnog
osiguranja, kućna adresa,
istorijat radnih mesta i plata

Tip operativnog sistema,
postupci za daljinski pristup,
telefonski brojevi za daljinski
pristup i nazivi pojedinih
računarskih sistema

Postupci proizvodnje,
strateški planovi, izvorni kôd
programa, spiskovi kupaca
i poslovne tajne

Bilo kakve lozinke

Pojedinosti
strukture
organizacije

Kompanijski
telefonski
imenik

Lične podatke

Postupke
i informacije
o računarskim
sistemima

Poverljive ili lične
informacije

NIKADA nemojte
saopštavati svoju
lozinku ni pod
kojim uslovima.

Sledite postupke
rada s internim
informacijama.

Sledite postupke
rada s internim
informacijama.

Sledite postupke
rada s internim
informacijama.

Sledite postupke
rada s internim
informacijama.

Proverite klasu
podataka; sledite
odgovarajuće
postupke za tu
klasu.

Kako reagovati kada neko zatraži da nešto uradite

Zlatna pravila

Nikome nemojte verovati dok ne proverite njegov identitet.
Poželjno je proveravati ispravnost zahteva.

Osoba od vas traži sledeću uslugu:

NAPOMENE

Izvorni kôd programa, poslovne tajne, postupak proizvodnje, formule, specifikacije proizvoda, marketinški podaci ili poslovni planovi

Nikada nemojte unositi nepoznate naredbe i nikada ne pokrećite programe na zahtev druge osobe ukoliko to posebno ne odobri informatičko odeljenje

Instalirajte samo softver iz proverenih izvora koji se može proveriti pomoću digitalnog potpisa

Ne menjajte nikakve parametre u BIOS-u, operativnom sistemu, niti bilo kojoj aplikaciji (uključujući i ličnu zaštitnu barijeru ili antivirusne programe) ukoliko to posebno ne odobri informatičko odeljenje

Da
otvorite
datoteku priloženu
uz elektronsku
poruku

Ne otvarajte priloženu datoteku ukoliko je unapred ne očekujete. Proverite sve takve datoteke pomoću antivirusnog softvera.

Ne

Da
izmenite lozinku

NIKADA ne menjajte lozinku u nešto poznato drugom licu, čak ni za trenutak!

Ne

Da
elektronski
prosledite interne
informacije

Proverite klasu podataka; sledite odgovarajuće postupke za tu klasu.

Ne

Da
unesete
naredbe u računar

Podnosilac zahteva mora biti isključivo iz informatičkog odeljenja; primenite postupke provere zaposlenog.

Ne

Da
preuzmete,
instalirate, uklonite,
ili isključite
softver

Sledite postupke rada s internim informacijama.

Ne

Da
izmenite
parametre računarskog
sistema
ili mreže

Podnosilac zahteva mora biti isključivo iz informatičkog odeljenja; primenite postupke provere zaposlenog.

Sve što preduzmete na tuđ zahtev može naškoditi vašoj firmi. Proveravajte. Proveravajte.

bibliografija

POGLAVLJE 1

BloomBecker, Buck. 1990. *Spectacular Computer Crimes: What They Are and How They Cost American Business Half a Billion Dollars a Year*. Irwin Professional Publishing.

Littman, Jonathan. 1997. *The Fugitive Game: Online with Kevin Mitnick*. Little Brown & Co.

Penenberg, Adam L. 19. april, 1999. *The Demonizing of a Hacker*. *Forbes*.

POGLAVLJE 2

Priča o Stenliju Rifkinu zasnovana je na sledećim izveštajima:

Institut za bezbednost računara. Saopštenje za štampu. Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar.

Epstein, Edward Jay. Neobjavljeno. *The Diamond Invention*.

Holwick, David, sveštenik. Neobjavljeni izveštaj.

Sam gospodin Rifkin je ljubazno potvrdio da priče o njegovom podvigu nisu potpuno tačne, jer on štiti svoju anonimnost odbijanjem da daje intervju.

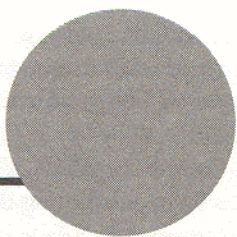
POGLAVLJE 15

Cialdini, Robert B. 2000. *Influence: Science and Practice*, četvrto izdanje. Allyn and Bacon.

Cialdini, Robert B. februar 2001. *The Science of Persuasion*. *Scientific American*. 284:2.

POGLAVLJE 16

Neka pravila u ovom poglavlju zasnovana su na idejama iz knjige *Information Security Policies Made Easy*. Wood, Charles Cresson, 1999, Baseline Software.



Zahvalnica...

...KEVINA MITNIKA

Prave prijatelje opisujemo kao dva tela koja dele jedan um. Čovek u životu nema mnogo pravih prijatelja. Džek Bjelo je bio draga i požrtvovana osoba; on se pobunio protiv užasnog maltretiranja kojem su me podvrgli novinari koji ne drže do etike, kao i suviše prilježni vladini tužioci. Vodio je pokret „Oslobodite Kevina“ i pisao izuzetno podsticajne članke u kojima je iznosio podatke koje je vlada tajila od javnosti. Džek je uvek bio tu da me bez straha brani i da mi pomaže u pripremi govora i članaka, a u jednom trenutku je bio i moj predstavnik za štampu.

Ova knjiga je, dakle, posvećena s ljubavlju mom dragom prijatelju Džeku Bjelu, čija je nedavna smrt od raka, upravo dok smo dovršavali ovu knjigu, u meni ostavila osećaj velikog gubitka i tuge.

Ove knjige ne bi bilo bez ljubavi i pomoći moje porodice. Moja majka, Šeli Džefi, i moja baka, Reba Vartanijan, pružale su mi bezuslovnu ljubav i podršku tokom čitavog života. Srećan sam što me je podizala tako nežna i požrtvovana majka, koju takođe smatram svojim najboljim prijateljem. Baka mi je bila kao druga majka, podizala me i volela majčinskom ljubavlju. Njih dve, tako požrtvovane i saosećajne, naučile su me da brinem o drugima i pomažem manje srećnima od sebe. Tako, vodeći se principom

davanja i brige, i ja na neki način idem njihovim stopama. Nadam se da će mi oprostiti što sam ih pomalo zapostavio tokom pisanja ove knjige. Propuštao sam prilike da ih vidim pod izgovorom da radim i da moram da završim do određenog roka. Ove knjige ne bi bilo bez njihove bezuslovne ljubavi i podrške koju ću uvek čuvati u srcu.

Voleo bih da su moj otac, Alan Mitnik, i moj brat, Adam Mitnik, poživali dovoljno dugo da sa mnom otvore bocu šampanjca onog dana kada se ova knjiga prvi put pojavi u knjižarama. S obzirom na to da je moj otac bio trgovački putnik i privatni preduzetnik, naučio me je mnogim stvarima koje nikada neću zaboraviti. Tokom poslednjih meseci očevoeg života, imao sam tu sreću da budem uz njega i tešim ga koliko mogu, ali bilo je to veoma bolno iskustvo od kog se još uvek nisam oporavio.

Moja tetka, Čiki Levental, uvek će za mene biti nešto posebno. Iako su je neke moje glupe greške razočarale, ipak sam uvek mogao da računam na nju, na njenu ljubav i podršku. Dok sam bio potpuno posvećen pisanju ove knjige, propustio sam mnoge prilike da s njom, mojom rođakom Mič Levental, i njenim momkom, dr Robertom Berkovicem, svake nedelje slavim Sabat.

Moram se, najtoplije zahvaliti i partneru moje majke, Stivenu Nitlu, koji ju je pazio umesto mene, pružajući joj ljubav i podršku.

Brat mog oca zasigurno zaslužuje pohvale; moglo bi se reći da sam većinu obmanjivanja nasledio od strica Mičela, koji je znao kako da manipuliše ljudima onako kako nikada neću shvatiti. Na njegovu sreću, nikada nije delio moju strast za kompjuterima. Koristio je svoj očaravajući duh da bi uticao na koga god je želeo. Uvek će nositi titulu velikog obmanjivača.

Dok pišem ovu zahvalnicu, shvatam da mnogim ljudima treba da se zahvalim za ljubav, prijateljstvo i podršku. Ne mogu ni da se prisetim imena svih dobrih i velikodušnih ljudi koje sam upoznao poslednjih godina, ali dovoljno je reći da bi mi trebao računar da ih sve popišem. Pisali su mi mnogi ljudi širom sveta, podržavali me, hvalili i hrabрили. To mi je puno značilo, pogotovo kada mi je bilo najpotrebnije.

Posebno se zahvaljujem svim ljudima koji su me podržavali i trošili svoje dragoceno vreme i energiju pronoseći glas svima koji su hteli da slušaju o neodgovarajućem postupanju prema meni i nedoličnom ponašanju onih koji su želeli da iskoriste „mit o Kevinu Mitniku“.

Imao sam izuzetnu sreću što sam sarađivao sa piscem bestselera Bilom Sajmonom. Vredno smo radili zajedno, uprkos različitim radnim navikama. Bil je veoma organizovan, budi se rano i pažljivo planira radni dan. Zahvalan sam što je bio dovoljno ljubazan da se prilagodi mom noćnom radu. Moja posvećenost ovom projektu i dug rad držali su nas do ranih jutarnjih sati, što se kosilo sa Bilovim urednim dnevnim rasporedom.

Bio sam srećan što sam sarađivao s nekim ko je uspeo da pretvori moje misli u rečenice dostojne čitaoca, ali i zato što je Bil (uglavnom) veoma strpljiv čovek koji je tolerisao moj programerski stil usredsređivanja na detalje. Na kraju smo zaista uspeali. Ovim putem bih želeo da se izvinim Bilu i da mu kažem da ću uvek žaliti što sam, zbog svoje usredsređenosti na tačnost i pojedinosti, bio uzrok nepoštovanja rokova prvi i jedini put u njegovoj dugoj karijeri pisca. On je ponosan što je pisac, a to sam konačno uspeo da razumem i podelim s njim, i nadam se da ćemo još knjiga napisati zajedno.

Smatram da je možda najbolji deo ovog projekta bio moj boravak u predivnoj kući Sajmonovih u mestu Rancho Santa Fe. Dok smo radili, pazila nas je i mazila Bilova supruga Arin. Razgovori s Arin i njena kuhinja, u mom sećanju će biti gotovo na prvom mestu. Ona je mudra i fina dama, izuzetnog smisla za humor, koja je stvorila lep i topao dom. I nikada više neću moći da pijem gazirana pića a da u glavi ne začujem Arinin glas koji mi predočava opasnosti koje prete od aspartama (veštački zaslađivač, prim. prev.).

Stejsi Kirkland mi puno znači. Posvetila je mnogo sati pomažući mi da na Mekintošu dizajniramo blok-dijagrame i grafikone kojima sam vizuelno uobličio svoje ideje. Divim se njenim izuzetnim kvalitetima; zaista je topla i saosećajna osoba koja zaslužuje sve najbolje u životu. Podržala me je kao pravi prijatelj i do nje mi je veoma stalo. Želim da joj se zahvalim na punoj podršci koju mi je pružila kad god mi je bila potrebna.

Aleks Kasper zvani Nexspace moj je najbolji prijatelj, ali i poslovni partner i kolega. Zajedno smo vodili popularni radio-program „Tamna strana Interneta“ na losandeleskoj stanici KFI AM 640 pod rukovodstvom direktora programa Dejvida G. Hola. Aleks mi je velikodušno pomagao i savetovao me u vezi sa ovom knjigom. Njegove su kritike uvek bile pozitivne, konstruktivne i dobronamerne, a naši razgovori često su se protezali do duboko u noć. Aleks i ja smo nedavno završili video koji će kompanijama pomoći da obuče ljude za sprečavanje napada obmanjivača.

Pol Drajmen iz firme Informed Decision porodični je prijatelj, i više od toga. Ovaj cenjeni i pouzdani privatni detektiv pomogao mi je da razumem sprovođenje tajnih istraga. Polovo znanje i iskustvo pomoglo mi je da se pozabavam i problemima obezbeđenja iz četvrtog dela ove knjige.

Jedna od mojih najboljih prijateljica, Kendi Lejman, stalno mi je pružala ljubav i podršku. Ona je zaista izuzetna osoba koja zaslužuje sve najbolje. U najtežim danima mog života, Kendi me je uvek podržavala i bila mi pravi prijatelj. Srećan sam što sam upoznao tako sjajnu, brižnu i saosećajnu osobu, i želim da joj se zahvalim na podršci.

Prva rata mog autorskog honorara zasigurno će otići kompaniji za mobilnu telefoniju čije usluge koristim, za sve vreme koje sam proveo razgovarajući sa Erin Fin. Bez sumnje, Erin je ista kao ja. Toliko smo slični, da je to pomalo zastrašujuće. Oboje volimo tehnologiju, istu vrstu hrane, istu muziku i filmove. Kompanija AT&T Wireless sigurno je na gubitku što mi omogućava sve te „besplatne noćne i vikend“ pozive Erin u Čikagu. Bar više ne koristim svoje stare tehnike za „besplatno“ telefoniranje. Njeno oduševljenje ovom knjigom i vera u nju dodatno su me podstakli. Srećan sam što mi je ona prijateljica.

Želim da se zahvalim neobično posvećenim osobama iz mog profesionalnog života. Razgovore i intervjuje mi ugovara Ejmi Grej (iskrena i brižna osoba kojoj se divim i koju obožavam). Agent Dejvid Fjugejt iz firme Waterside Productions umesto mene je pregovarao više puta pre i posle potpisivanja ugovora za ovu knjigu. Tu je i Gregori Vinson, advokat iz Los Anđelesa, jedan od mojih branilaca tokom višegodišnje borbe s vlastima. Siguran sam da saoseća s Bilom kada je u pitanju moje usredsređivanje na detalje; imao je isto iskustvo dok je u moje ime pisao pravna dokumenta.

Suviše sam imao posla sa advokatima, ali žarko želim da se zahvalim onima koji su, tokom godina mojih negativnih iskustava s pravosudnim sistemom, ponudili svoju pomoć kada mi je bila očajnički potrebna. Od reči utehe, do temeljnog rada na mom slučaju, upoznao sam mnoge koji se nimalo ne uklapaju u stereotip samozivog advokata. Počeo sam da poštujem ljubaznost i velikodušnost koju su mi mnogi ponudili cenim je i divim joj se. Pomenuću ih poimence, jer svako od njih zaslužuje iskrenu zahvalnost: Greg Ejklin, Bob Karmen, Džon Dusenberi, Šerman Elison, Omar Fige-roa, Karolin Hegin, Rob Hejl, Alvin Majklson, Ralf Perek, Viki Podbereski, Donald C. Rendolf, Dejv Roberts, Alan Rubin, Stiven Sadoovski, Toni Sera,

Ričard Šerman, Skip Slejts, Karen Smit, Ričard Steingard, prečasni Robert Talkot, Beri Tarlou, Džon Izurdiaga i Gregori Vinson.

Veoma cenim što mi je izdavačka kuća John Wiley & Sons pružila priliku da objavim ovu knjigu, i što su imali poverenja u pisca početnika. Želim da se zahvalim sledećim ljudima iz te izdavačke kuće koji su omogućili da ostvarim svoj san: Elen Gerstajn, Bob Ipsen, Kerol Long (moja urednica i modna savetnica) i Nensi Stivenson.

Bitno je i da pomenem i druge članove porodice, bliske prijatelje i poslovne saradnike koji su me savetovali, podržavali i pomagali mi na razne načine i odam im priznanje. To su: J. J. Abrams, Dejvid Ager, Bob Arkou, Stiven Barns, dr. Robert Berkovic, Dejl Kodington, Erik Korli, Delin Kormeni, Ed Kamings, Art Dejvis, Mišel Delio, Sem Dauning, Džon Drejper, Pol Drajman, Nik Duva, Roj Eskapa, Aleks Filding, Lisa Flores, Brok Frenk, Stiv Gibson, Džeri Grinblat, Greg Grunberg, Bil Hendl, Dejvid G. Hol, Dejv Harison, Lesli Herman, Džim Hil, Den Hauard, Stiv Hant, Rez Džohar, Stiv Nitol, Geri Kremen, Beri Krugel, Erl Krugel, Adrian Lamo, Leo Laporte, Mič Levental, Sintija Levin, C. J. Litl, Džonatan Litman, Mark Majfret, Brajan Martin, Forest Mekdonald, Keri Mekelvi, Alan Meksvejn, Eliot Mur, Majkl Moris, Edi Munjoz, Patrik Norton, Šon Nanli, Brenda Parker, Kris Pelton, Kevin Polsen, Skot Pres, Linda i Art Prior, Dženifer Rid, Izrael i Rejčel Rozenkranc, Mark Ros, Vilijam Rojer, Irv Rubin, Rajan Rasel, Nil Savedra, Vin Švartu, Pit Šipli, Džon Sif, Den Sokol, Trudi Spektor, Met Spergel, Eliza Amadea Sultan, Daglas Tomas, Roj Taker, Brajan Turbou, Ron Vecel, Don Dejvid Vilson, Darsi Vud, Kevin Vortman, Stiv Vozniak, kao i svi moji prijatelji na repertoru W6NUT (147.435 MHz) u Los Anđelesu.

I moj referent za bivše zatvorenike na uslovnoj slobodi, Leri Houli, zaslužuje da mu se posebno zahvalim što mi je dozvolio da radim kao savetnik za bezbednost i napišem ovu knjigu.

Konačno, moram pomenuti policiju. Ne uzimam im za zlo što rade svoj posao. Čvrsto verujem da je postavljanje javnih ciljeva ispred ličnih interesa i posvećivanje života služenju za opšte dobro nešto što zaslužuje poštovanje. Iako sam ponekad bio nadmen, želim da svi znate da ja volim ovu zemlju i da ću učiniti sve što je u mojoj moći da pomognem da ona postane najbezbednije mesto na svetu, što je upravo jedan od razloga zbog kojih sam napisao ovu knjigu.

...BILA SAJMONA

Smatram da za svakog negde postoji *prava* osoba; ali neki ljudi nisu te sreće da je pronađu. Drugima to uspe. Ja sam bio te sreće dovoljno rano. Dosad sam proveo velik broj godina (a nadam se i mnogim takvim godinama u budućnosti) sa blagom koje mi je Bog podario, mojom suprugom Arin. Ako ikada budem zaboravio koliko sam srećan, treba samo da obratim pažnju na to koliko ljudi uživa i želi da bude u njenom društvu. Arin, hvala ti što kroz život ideš sa mnom.

Za vreme stvaranja ove knjige, pomagala mi je grupa odanih prijatelja, koji su me uveravali da smo Kevin i ja na pravom putu da spojimo činjenice i senzacionalnost u ovoj neobičnoj knjizi. Svako od njih je iskren i zaista odan i zna da na njega mogu da računam i u sledećem projektu. Prema abecednom redu, to su: Žan-Klod Beneventi, Linda Braun, Volt Braun, general-pukovnik Don Džonson, Doroti Rajan, Guri Stark, Kris Stip, Majkl Stip i Džon Votau.

Posebne zasluge imao je Džon Lucić, predsednik Grupe za mrežnu bezbednost, koji je koristio svoje slobodno vreme da bi pomogao prijateljevom prijatelju, kao i Gordon Garb, koji je elegantno savladao moje brojne telefonske pozive u vezi sa radom informatičkih odeljenja.

Ponekad u životu jedan prijatelj postane izuzetno zaslužan zato što vas je upoznao s nekim ko vam takode postane dobar prijatelj. U književnoj agenciji Waterside Productions, u Kardifu u Kaliforniji, agent Dejvid Fjugejt je osmislio ideju za ovu knjigu i spojio me sa koautorom Kevinom koji mi je kasnije postao prijatelj. Hvala ti, Dejvide. A upravniku agencije Waterside, jedinstvenom Bilu Gledstonu, koji me stalno obasipa projektima za rad na novim knjigama poručujem: drago mi je što si mi prijatelj.

Kod kuće i u mojoj kućnoj kancelariji mojoj supruzi Arin pomaže sposobno osoblje u koje ubrajam svoju sekretaricu Džesiku Dadžeon i kućnu pomoćnicu Hozí Rodrigez.

Zahvaljujem se svojim roditeljima, Mardžori i I. B. Sajmonu. Želeo bih da su s nama na ovom svetu kako bi uživali u mom uspehu. Takode se zahvaljujem svojoj ćerki Viktoriji. Kada sam s njom, shvatam koliko joj se divim i poštujem, i koliko sam ponosan na nju.

indeks

A

- administriranje računara, pravila, 296-306
- aerodromi, obezbeđenje, 9
- agencije za zapošljavanje, obmanjivanje, 22-26
- alati za zaobilazanje softverske zaštite, 314
- ANI (automatska identifikacija broja), 84, 229
- antivirusni softver
 - ažuriranje, 104-105
 - pravila, 302, 306, 313, 324
 - špijunski softver i, 213
- ARPANet (Mreža agencije za napredne istraživačke projekte Ministarstva odbrane SAD), 8-9
- Auto-moto savez (AMS), saznavanje njihovih informacija, 144-148
- automatska identifikacija broja (ANI), 84, 229
- automobilske tablice, stare, 156

B

- banke
 - primena internog bezbednosnog koda, 136-139, 141-143
 - pristupanje njihovim informacijama, 5-7, 16-22
- bezbedan HTTP, 103
- bezbednost
 - kodovi, 136-139, 141-143, 149
 - poput bombone, 80

- putem tajnovitosti, 81-82
- uz lozinku, 80, 118-119
- zasnovana na terminalu, 187
- blokirani broj, telefonska usluga, 178-180
- blokiranje dolaznih poziva, 218
- brave, obijanje, 187-188
- brisanje datoteka, 173
- brisanje dnevnika događaja, program, 122
- broj socijalnog osiguranja, 51, 115
- brojevi kreditnih kartica, 43-46, 52-53, 98-99

C

- Centar za memorisanje i ovlašćivanje nedavno izmenjenih brojeva (RCMAC), 180
- centrala, telefonska, 145-146, 148, 217-218
- Cleaner, program, 105
- CreditChex, opis slučaja, 16-22
- crvi, 94-96

Č

- čekovi, nevažeći, 44
- čistači, bezbednosna obuka, 196-197
- čuvanje podataka na mreži, 247
- čuvari
 - obmanjivanje, 199-203
 - obuka, 211, 257
 - predvidljivost, 169

D

daljinski pristup, 163-166, 222, 292, 296-298

daljinsko komandno okruženje, 60

datoteke, prenos, 242-248, 281

davaoci usluga, nalozi, 288-289

digitalni sertifikat, Web lokacija, 102-103

direktna veza, telefonska usluga, 178-179

diskusione grupe, 88, 314

dosije o prestupima, 33

doslednost, 254

društvena potvrda, 254-255

država, informacije dostupne na Internetu, 50-51

dvostepena identifikacija, 85

E

eBay, 97, 101

elektronska pošta

digitalni potpis, 274

lokacije u stranim zemljama, 209-210, 223

objavljivanje adrese, 69

opšte adrese, 298

pravila upotrebe, 261, 316-317

prilozi, 94-96, 302, 316

tajna lokacija, 222-223

veze u porukama, 96-97, 100-102

elektronska trgovina, 98-99

F

faks

elektronski, 127

pravila za upotrebu, 318-319

proseleđivanje, 221-222, 318

fakultetska dokumentacija kao meta, 127-130, 133

Federalni istražni biro (FBI), 33-34, 50-51, 237

filmska industrija, opis slučaja, 107-109

finansijska industrija, podložnost napadima, 16-22

fizičko obezbeđenje, pravila, 327-329

G

garantovanje, 271, 273

glasovna pošta

dobijanje privremene glasovne pošte, 221

isključivanje, 284

ostavljanje telefonskog broja, 156

pravila, 261, 317-321

sanduče za celo odeljenje, 271, 283

gledanje preko ramena, 227

glupi terminal, 129

grupna tužba, opis slučaja, 231-234

gzip, 243

H

hakeri, 83-84, 93-94

I

identifikacija

dvostepena, 85

neophodni uređaji, 7

pozivaoca, 215-220, 229-230, 273, 282

provera, 273-274, 310, 327-328, 336

radi daljinskog pristupa, 297

softvera, 302-303

identifikacioni broj, 16-21

zaposlenog, otkrivanje, 27-28, 30, 78-79, 91

igranje uloga u obuci, 252, 257-258

ikonica katanca na Web strani, 102

imena

pominjanje poznatih, 112, 169

upisivanje u bazu podataka preduzeća, 76

imenik

na mreži, 149

preduzeća kao meta obmanjivača, 25-26

probnih brojeva, 34-35

informacije

kao žetoni za poker, 25

mešetarenje, 116, 246

o neobjavljenim brojevima, 32

objavljivanje, 278-281

osoba zadužena za, 269, 276
 postupanje kada neko traži, 75-76,
 90-91, 339
 pristupanje naizgled bezopasnim, 15,
 21-22, 28-30
 skriveni značaj, 15
 informatičko odeljenje, pravila, 291-308
 informativni program, 28, 255-264,
 267. *Videti i* obuka
 instalacija, tajna, 208
 Internet
 alati za hakerisanje, 190, 192-193
 državne informacije dostupne na,
 50-51
 lažne lokacije, 97-102
 spisak podrazumevanih lozinki na, 73
 tajna lokacija, 71
 interni podaci, klasifikacija, 270-271,
 280, 338
 intranet, sadržaj, 53-54
 istražni zatvor, opis slučaja, 177-183
 izgled, zaključivanje na osnovu njega,
 169
 izmenljivi mediji, 314-315
 izvor, gašenje, 20
 izvorni kôd, saznavanje, 202-203,
 242-245

J
 javni podaci, klasifikacija, 271, 338

K
 kabl i parica, broj, 111
 kadrovsko odeljenje, pravila, 325-327
 kartica s potpisom, bankovna, 138, 141
 kazna za saobraćajni prekršaj,
 izbegavanje, 223-226
 klasifikacija podataka
 interni, 270-271, 280, 338
 javni, 271, 338
 lični, 269-270, 279-280, 338
 poverljivi, 269-270, 278-279, 338
 pravila, 28, 269-271, 276
 terminologija, 271
 kodovi, bezbednost, 136-139, 141-143,
 149

komandno okruženje, daljinski pristup,
 60
 kompanija za čuvanje podataka, napad,
 232-234, 247-248
 konto, broj, 24-26
 konzola, 188
 kopanje po smeću, 160-163
 korisnici
 dobijanje informacija o, 36-38, 43
 zaštita, 52-53
 krađa identiteta, 147-148, 220, 229
 kriminalističke službe
 osećaj zadovoljstva pri obmani, 146
 prisluškivanje, 83
 upoznavanje po postupaka, 32-34
 uputstvo za NCIC, 51-52
 kutije za internu poštu preduzeća,
 287-288

L
 L0phtcrack3, uslužni program, 193
 lažna adresa, 26
 lažno osećanje bezbednosti, 5
 lažno predstavljanje
 kao policajac, 147-148
 kao zaposleni u preduzeću, 153-160,
 167-170
 lični podaci, klasifikacija, 269-270,
 279-280
 LOCK-11, 185-186
 lozinka
 biranje, 322-323
 čuvar ekrana, 302, 315
 daljinski pristup, 222
 davanje, 315-316
 gledanje preko ramena da bi se
 saznala, 227
 napad rečnikom, 191-194
 nepostojeća, 201-202
 objavljivanje, 64, 67, 74-75, 307, 321
 obuka o bezbednosti lozinki, 131-132
 otkrivanje pomoću simulatora strane
 za prijavljivanje, 129
 podrazumevana, 73, 283, 303
 pogađanje na silu, 193
 poništanje, 293, 296

pravila, 197-198, 303-305, 313,
316-323
privremeni nalog za posetioce, 70
program za pogađanje, 168
promenljiva, 274, 336
saopštavanje, 74, 79, 91, 315-316
saopštavanje novih, 294
saznavanje pomoću špijuskog
softvera, 207-208
šifrovanje, 70, 192-194, 201
telefonska centrala, 145-146, 148
u obliku običnog teksta, 323

LJ

ljuska priroda, tendencije, 252-255

M

mala vrata, 102, 111
marketinška kompanija, opis slučaja,
119-122
mediji
bacanje, 173
za rezervne kopije podataka, 232-234,
247, 308
mito, 162
mobilni telefoni, opis slučaja, 48-50
modemska veza, 301-302, 309, 313

N

Nacionalni centar za informacije o
kriminalu (NCIC), 33, 51-52
nadgledanje, računarski program, 170
nadgledanje događaja
brisanje tragova, 122, 171-172, 202,
245
dnevnik događaja, 30, 202
nagradivanje zaposlenih, 264, 267
najniže privilegije, pravilo, 285
nalog
isključivanje, 294
isticanje roka trajanja, 298
ovlašćenje za nov, 293
privilegovan, 271, 300, 304-306
privremeni, 88-89

privremeni za posetioce, 70, 300
zaključavanje, 304
napad. *Videti i* obmanjivanje
direktni, 31-39
krađa identiteta, 147-148, 220, 229
pogađanjem lozinke na silu, 193
rečnikom, 71, 191-194
statistički podaci, 7
negiranje, verovatnoća, 231
neiskvarenost u okviru organizacije, 8-9
neproverena osoba, 271
nezaposleni, kriterijumi za proveru,
337-338
neznanac, saradnja, 46-47, 74-75
novajlija, opis slučaja, 77-79

O

obmanjivači, 7-8
iskorišćavanje položaja, 52
ophođenje s ljudima, 8, 27, 135
pol, 42
samouvereni, 238, 240-241
značaj poznavanja terminologije, 32
obmanjivanje. *Videti i* napad
agencija za zapošljavanje, 22-26
ciklus, 333
finansijskih institucija, 5-7, 16-22
zaposlenih prijemnih odeljenja,
199-213
nabavljanje brojeva kreditnih kartica,
43-46
nabavljanje podataka o korisnicima,
36-38
novi zaposleni kao mete, 62-64
obrnuto, 61
od strane zaposlenih, 112
podložnost, 335-336
postotak uspešnih, 251
prepoznavanje, 333
primena od strane terorista, 9-10
procenat uspešnih napada, 251
roditeljsko, 10
saznavanje neobjavljenih telefonskih
brojeva, 31-32

- saznavanje procedura u
 kriminalističkoj službi, 32-34
 opis slučajeva prevare preko Interneta,
 97-102
 u sprezi s tehnologijom, 177-183
 uobičajene metode, 334-335
 uobičajene žrtve, 335
 znaci upozorenja, 335
 obuka, 91, 210-211, 251-264, 290-291.
Videti i informativni program
 ciljevi, 255-256
 čistača, 196-197
 čuvara, 211, 257
 igranje uloga, 252, 257-258
 motivisanje zaposlenih, 255-256
 neophodnost, 251-252
 novih zaposlenih, 64, 258
 o bezbednosti lozinki, 131-132
 planiranje programa, 257-258
 podrška za programe, 256
 prema radnom mestu, 74, 257, 259
 primena bezbednosnih podsetnika,
 133
 sadržaj programa, 259-261
 stalna, 259, 262-263
 struktura, 258-259
 testiranje, 262
 za proveravanje autoriteta, 114
 zaposleni koje valja uključiti, 35, 39,
 74
 odbrana, višeslojan sistem, 260
 oglasna tabla preduzeća, 288
 operateri na računarima, pravila,
 306-308
 operativni sistem, podešavanje, 297-298
 Oracle Corporation, 162
 osetljivi podaci, klasifikacija, 270
 osveta, 110-112, 227-228
 ovlašćenja
 administratora sistema, 187-188
 za posedovanje informacija, provera,
 131, 275-276, 337
 za pristup, 272, 300, 304-306
 ovlašćivanje, postupci, 272-276
 označavanje podataka, 277
- P**
 pad mreže, opis slučaja, 55-61
 PayPal, 97, 100-101
 pitanja
 očekivana, 41
 skrivanje ključnih, 20-21
 test, 79
 plate, saznavanje iznosa, 171-172
 podložnost napadu
 faktori koji utiču, 335-336
 procena, 196-197, 268
 provera, 290
 podsetnici, bezbednosni, 133
 pokerski žeton, informacije, 25
 pol obmanjivača, 42
 položaj
 poštovanje, 52
 provera, 114
 tendencija da se podlegne uticaju, 253
 upotreba radi zastrašivanja, 112-114
 popisivanje, 190-191
 posao na crno, 231
 posetioci, 109, 175, 301, 327-329
 posetnice, lažne, 241
 poverenje
 i uverljivost, 51
 izgradnja, 41-54
 mudro odlučivanje, 53
 u nepoznate osobe, 46-47
 zloupotreba, 8
 poverljiva osoba, 272
 poverljivi podaci, klasifikacija, 269-270,
 278-279, 290, 321, 338
 pozivaoci, provera, 21-22, 29-30, 336
 praćenje poziva, 284
 pravila, bezbednosna, 28, 195
 analiza i ažuriranje, 268
 definicija, 266
 fizičko obezbeđenje, 327-39
 informatičko odeljenje, 291-308
 administracija računara, 296-306
 operateri na računarima, 306-308
 tehnička podrška, 292-295
 kadrovsko odeljenje, 325-327
 klasifikacija podataka, 28-29,
 269-271, 338

- koraci u pisanju, 265-268
 - posledice nepridržavanja, 267
 - postupci provere i ovlašćivanja, 272-276
 - rukovodstvo, 276-291
 - klasifikacija podataka, 276
 - objavljivanje informacija, 278-281
 - propisi o telefoniranju, 282-285
 - službenici prijemnog odeljenja, 330-331
 - tim za prijavljivanje incidenata, 331-332
 - zaposleni, 308-323
 - lozinke, 197-198, 321-323
 - opšta, 308-311
 - upotreba elektronske pošte, 316-317
 - upotreba faksa, 318-319
 - upotreba glasovne pošte, 319-321
 - upotreba računara, 311-315
 - upotreba telefona, 317-318
 - zaposleni koji rade pomoću daljinskog pristupa, 324-325
 - preduzeće za snabdevanje električnom energijom, opis slučaja, 36-39
 - prepoznavanje glasa, 274
 - prevara
 - i teroristi, 9-10
 - obmanjivanje, 8
 - policije, opis slučaja, 123-127
 - poverenje kao ključ, 41-44
 - PRI ISDN, 217
 - prijavljivanje
 - bezbednosnih incidenata, 76, 132, 308-309
 - incidenata, 286-287, 331-332
 - prisluškivanje radio-frekvencija, 83
 - pristup
 - blokiranje, 303-304
 - ispraćanje zaposlenih, 173-175
 - izmena globalnih prava, 296
 - neophodnost upravljanja, 7
 - tačke bežičnog pristupa, 305
 - pritisci tastera, praćenje, 207-209, 212
 - privatni istražitelji, 18-22, 116
 - privatni podaci, klasifikacija, 321, 338
 - probni upadi, 197, 251, 261, 268
 - procena rizika, 265-266
 - propusnica
 - bezbednost, 154, 169
 - elektronska, 174
 - izgled, 285, 291
 - pravila, 172, 309
 - privremena, 172, 328
 - uzimanje od bivšeg zaposlenog, 174
 - za posetioce, 109
 - prosedivanje poziva, 145-147, 282
 - protokol za prenos datoteka (FTP), 244
 - provera
 - biografije radnika, 327
 - elektronske pošte, 317
 - garantovanje trećeg lica, 271
 - ideje, 90-91
 - identiteta, 273-274, 336
 - kriterijumi za lica koja nisu zaposlena u kompaniji, 337-338
 - linije, 111
 - metode, 149
 - neophodnost, 39
 - obuka, 259, 260
 - postupci, 272-276
 - proizvođača, 283
 - statusa zaposlenog, 274-275, 337
 - telefonskim pozivom, 21-22, 90, 215, 336
 - provlačenje neovlašćenih osoba kroz
 - kapiju, 197, 310
 - psihološki faktori, 107
 - pwdump3, alatka, 192
- R**
- računar s dve mrežne adrese, 189
 - radio-sistem, opis slučaja, 82-89
 - radnik po ugovoru, nalog, 286
 - RAT (trojanski konj za daljinski pristup), 95
 - rečnik, napadi pomoću, 71, 191-194
 - Rifkin, Stenli Mark (obmanjivač), 5-7
 - roditelji, kao obmanjivači, 10

S

- sažaljenje, iskorišćavanje, 77, 109, 117-118, 126, 242, 245
- Secure ID, 86-87
- server
 - broj za daljinski pristup, 70, 72
 - pronalaženje, 168, 190
 - saopštavanje, 88, 128, 132
 - zastupnički, 54
- simulator strane za prijavljivanje, 128-129
- skriptasi, 7
- sloj bezbedne veze (SSL), 104-105
- službenik prijemnog odeljenja
 - obmanjivanje, 166-168, 175, 234, 239
 - pravila, 330-331
- smeće
 - najbitnije što treba znati, 173
 - pravilo, 329
 - pretraživanje, 160-163
- snimci ekrana, krađa, 213
- socijalno osiguranje, opis slučaja, 114-119
- softver
 - antivirusni, 104-105, 213, 302, 306, 313, 324
 - nadgledanje, 203
 - popisivanje, 190-191
 - prenošenje trećim licima, 281
 - preuzimanje ili instaliranje, 312
 - provera, 302-303
 - saznavanje izvornog koda, 83-89
 - špijunski, 207-209, 212
 - tajna instalacija, 208
 - trojanski konj, 60
 - zaštitni 313
 - zlonamerni, 95, 213
- spiskovi reči, primena, 191-192
- SpyCop, 213
- SSL (sloj bezbedne veze), 104-105
- status zaposlenog, provera, 274-275, 337
- strana zemlja, lokacije za elektronsku poštu, 209-210, 223
- struktura organizacije, 311

Š

- šifrovane lozinke, 70, 192-194
- šifrovanje
 - glasovne pošte, 82
 - ključevi za, 247-248
 - lozinke, 70, 192-193, 201
 - podataka na Web lokaciji, 103
 - rezervnih kopija dokumenata i čuvanih datoteka, 233-234, 247-248, 301
- špijunaža, industrijska, 65-73, 161, 184-185, 231-248
- špijunski softver, 207-209, 212
- štetan kôd, 94
- štetan softver, 95

T

- tačke bežičnog pristupa, 305
- tajna instalacija, 208
- tajna lokacija, 71, 222
- tajnovitost, bezbednost zasnovana na, 81-82
- tanki klijenti, 324
- tehnička podrška
 - pravila, 292-295
 - zahtevi, 292
- telefoni u javnim prostorijama, 282-283
- telefoniranje, pravila kompanije, 282-285
- telefonski brojevi
 - ANI (automatska identifikacija broja), 84, 229
 - Biroa za imena i adrese klijenata (IAK), 81-82
 - centrala, 145, 148
 - identifikacija pozivaoca, 215-220, 229-230
 - imenik probnih, 34-35
 - informacije o neobjavljenim, 31-32
 - nabavljanje neobjavljenih, 31
 - objavljivanje internih, 22-30, 317, 330
 - poverljivi brojevi lokala, 284
 - pronalaženje pomoću broja kabla i parice, 111
 - provera veze, 111

reprogramiranje, 217-219
 saopštavanje broja za daljinski pristup,
 70, 72, 78, 309
 u osnovnim porukama glasovne pošte,
 156
 zaobilazni, 34
 telefonski sistem, automatski, 284
 terminal, 129, 187-188
 terminologija, 32, 50, 81, 138
 teroristi i obmana, 9-10
 Trojan Defense Sweep, 105
 trojanski konj, 60
 za daljinski pristup (RAT), 95

U

ubedjivanje, umetnost prijateljskog, 135
 uljezi, 158-159, 166, 169-170, 184-185
 uništavanje dokumenata, uređaji, 173,
 310
 upad, nezakonit, 153-160
 usluge, vraćanje, 61
 uverljivost, postizanje, 51
 uzvraćanje ljubaznosti, 253-254
 uzvraćanje poziva, 273

V

vandali, računarski, 93-94
 varalice, 177-178, 234
 videoteka, opis slučaja, 42-46
 virus, 93-94, 103-104. *Videti i*
 antivirusni softver
 vozačka dozvola, 143, 159, 233

W

Web lokacije
 bezbedne veze, 102-103
 lažne, 97-102
 spiskovi reči, 191-192
 za elektronsku trgovinu, 98-99

Z

zahtevi
 proizvođača, 204-205, 211
 reagovanje na molbu za uslugu, 340
 za informacijama, 75-76, 90-91, 272,
 339
 zahvalnost, iskorišćavanje, 55, 122-123
 zakrpa, 202-203, 299
 zamena uloga, opis slučaja, 127-130
 zaobilazni telefonski broj, 34
 zaposleni. *Videti i* obuka
 kao pretnja, 165
 koji rade putem daljinskog pristupa,
 pravila, 324-325
 lični podaci o, 311
 napadi na službenike prijemnih
 odeljenja, 199-213
 napadi sadašnjih ili bivših, 112
 nezadovoljni, 163-166, 228
 novi kao meta napada, 62-64
 ovlašćivanje zaposlenog iz drugog
 ogranka, 175
 postupci pri odlasku, 173-175,
 325-326
 provera, 277-278
 provera biografije, 327
 zastrašivanje
 na osnovu položaja u preduzeću,
 112-114
 primena, 113-114, 123, 205
 zastupnički server, 54
 zaštitna barijera, 105, 167, 176, 200
 zlonameran softver, 213
 zloupotreba telefona, 34-35, 82, 145,
 215

Ž

žaoaka, obrnuta, 135, 144
 žeton, vremenski, 85, 90
 žrtva, 20

LEGENDARNI HAKER OTKRIVA KAKO DA SE ZAŠTITITE OD NAJVEĆE OPASNOSTI PO BEZBEDNOST – OD LJUDSKE PRIRODE

„...niz priča o tome kako se – pomoću staromodnog laskanja i odličnog poznavanja savremenih tehnologija – mogu izvući informacije od bilo koga. Uz ovo zabavno štivo uživaćete kao da čitate najzanimljivije delove desetak uzbudljivih trilera, jedan za drugim“.

– *Publishers Weekly*

ISBN 86-7555-220-3



9 788675 552208