predgovor

Neki hakeri uništavaju ljudima datoteke ili celokupan sadržaj diskova – 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 sredstvo za krađu novca, dobara i usluga.

Uprkos mitu koji su o Kevinu Mitniku ispleli mediji, ja nisam zlonameran haker.

Ali, sad vam sve pričam unapred.

POČECI

Svoj put sam verovatno odabrao rano. Bio sam bezbrižno dete, ali sam se dosađivao. 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 istražujem čitav Los Anđeles, 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 neobičnog rasporeda izbušenih rupica kojima su vozači označavali dan, vreme i trasu. Jedan ljubazan vozač odgovorio je na moje pažljivo formulisano pitanje. 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. Kante 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 Anđelesu. 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 učenikom 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 „zlonamernog 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 Anđelesu. 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 izmamljuje 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 uvežbavao iluzionističke trikove – vežbao sam laganje preko telefona. Uskoro sam otkrio da mogu da dođem 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 najozloglašenijeg 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.

deo 1

Iza kulisa

poglavlje 1

Najslabija tačka bezbednosnog sistema

Preduzeće može da kupi najbolje dostupne bezbednosne tehnologije, obuči ljude tako dobro da zaključavaju sve tajne informacije pre nego što uveče pođu kući, i zaposli najbolje čuvare 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

mnogo 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, uljuljkuju 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 negove male avanture sa sada nepostojećom bankom Security Pacific National Bank u Los Anđelesu. 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 Švajcarskoj, 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 dijamanata 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 krade 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 „skriptaši". Ti klinci 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 motiviše 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 zaobiđe 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 zaštiti 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 uspeli 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 napori 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 uvežbavamo 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 proveri 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. Sprovodimo 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 proćaskali, 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 potrudi 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 sreli 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 gospođica, 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 oglasio 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 smera“.

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 proveri 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 proveri

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 spro vode 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 Lejkvjuu 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 skraćenice 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 zaštiti, 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 sandučiće 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 Francisko su spremne. Hoćete li da vam ih dostavimo, ili ćete sami doći po njih?“

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

„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 Francisko?“

„Ako mislite da možete nagovoriti mog šefa...“ odvraća 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.

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	OPIS
Istraživanje	Ispituju se i podaci iz javnih izvora kao što su godišnji izveštaji, marketinške brošure, prijave patenata, isečci iz štampe, stručni časopisi i Web lokacije. Tu spada i kopanje po smeću.
Razvijanje dobrih odnosa i poverenja	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 pomenutim 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 ogranka 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	PRIMERI
Neko ko nije svestan značaja informacija	Službenici prijemnih odeljenja, službenici na telefonskoj centrali, sekretarice i pomoćnici, čuvari.
Lica s posebnim ovlašćenjima	Informatička ili tehnička podrška korisnicima, administratori računarskog sistema, računarski operateri, administratori telefonskog sistema.
Proizvođači ili davaoci usluga	Proizvođači računarskog hardvera i softvera, proizvođači sistema za glasovnu poštu.
Posebna odeljenja	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.
Uzvraćanje 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 sagovonik izdaje, pozovite ga da proveri 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	OPIS
Provera u kompanijskom imeniku	Proverite da li se ime zaposlenog nalazi u imeniku na mreži.
Potvrda od pretpostavljenog podnosioca zahteva	Pozovite njegovog pretpostavljenog na broj naveden u kompanijskom imeniku.
Potvrda od odeljenja ili radnog tima podnosioca zahteva	Pozovite odeljenje ili radni tim podnosioca zahteva i proverite da li je još uvek zaposlen u firmi.

Postupak utvrđivanja ovlašćenja za posedovanje informacija

POSTUPAK	OPIS
Pogledajte spisak odgovornosti radnih mesta/timova	Pogledajte objavljene spiskove osoba koje su ovlašćene da poseduju određene poverljive informacije.
Zatražite odobrenje od svog pretpostavljenog	Pozovite svog pretpostavljenog, ili pretpostavljenog podnosioca zahteva, i zatražite odobrenje da mu ispunite zahtev.
Zatražite odobrenje od osobe zadužene za informacije ili njegovog zamenika	Pitajte osobu zaduženu za informacije da li je podnosilac zahteva ovlašćen da poseduje date podatke.
Proverite ovlašćenje pomoću automatskog alata	Proverite ovlašćenja u posebnoj bazi podataka.

Kriterijumi za proveru osoba koje nisu zaposlene u firmi

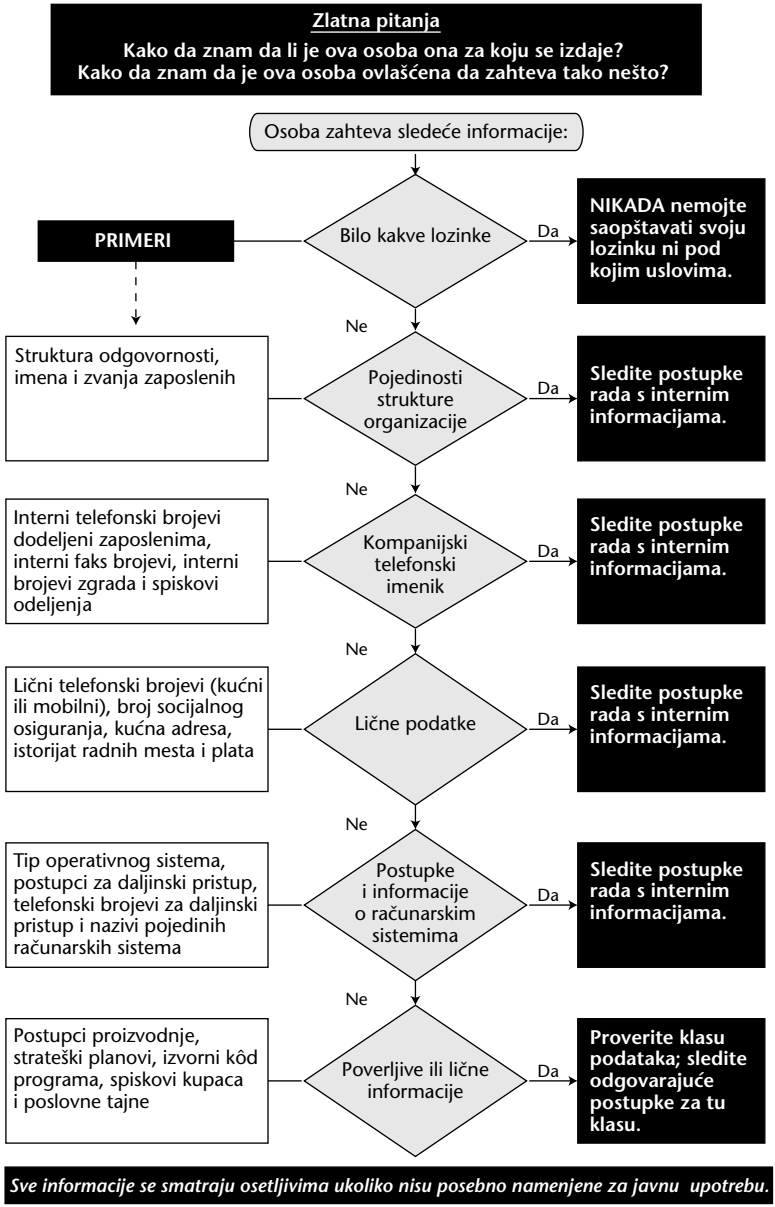
KRITERIJUM	POSTUPAK
Odnos	Proverite da li je firma koja podnosi zahtev davalac usluga, strateški partner, ili neka druga firma koja je u odgovarajućem odnosu s vašom.
Identitet	Proverite identitet i status zaposlenog u partnerskoj firmi.

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 zamenika. 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



Kako reagovati kada neko zatraži da nešto uradite