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.