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.