

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, iseći 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 pomenu-tim koracima ciklusa dok ne dođe do cilja.

Uobičajene metode obmanjivanja

- Izdavanje za kolegu
- Izdavanje za zaposlenog u firmi dobavljača usluga, partnerskoj firmi, ili kriminalističkoj službi
- Izdavanje za nekog ko je na višem položaju
- Izdavanje za novog zaposlenog kome treba pomoć
- Izdavanje za dobavljača usluga ili proizvođača sistema koji zove da bi ponudio sistemsku zakrpu ili najnoviju verziju
- Nuđenje pomoći ako bi nastao problem, potom izazivanje problema, čime se žrtva navede da od napadača zatraži pomoć
- Slanje žrtvi besplatnog softvera ili zakrpe da ih instalira
- Slanje virusa ili trojanskog konja u prilogu elektronske poruke
- Upotreba lažnog okvira za dijalog u kom se od korisnika traži da se ponovo prijavi za rad ili da ponovo unese lozinku
- Snimanje žrtvinih pritisaka na tastere pomoću računarskog sistema ili programa
- Ostavljanje na radnom mestu disketa ili kompakt diskova sa zlo-namernim softverom
- Korišćenje interne terminologije da bi se zadobilo nečije poverenje
- Nuđenje nagrade da bi se neko registrovao na Web lokaciji pomoću korisničkog imena i lozinke
- Ostavljanje dokumenata ili datoteka u kompanijskoj prostoriji za poštu radi isporuke u kancelarije
- Prilagođavanje zaglavlja faksa tako da se čini da je poslat sa interne lokacije
- Umoljavanje službenika prijemnog odeljenja da primi i prosledi faks
- Zahtev da se datoteka prosledi do naizgled interne lokacije

- Podešavanje glasovne pošte tako da pozivaoci pomisle da im je napadač kolega
- Pretvaranje napadača da dolazi iz drugog ogranaka preduzeća, i traženje da mu se u sistemu preduzeća otvori elektronsko sanduče.

Znaci koji upozoravaju na mogući napad

- Neko odbija da vam kaže broj na koji ga možete pozvati
- Neobičan zahtev
- Naglašavanje visokog položaja
- Naglašavanje hitnosti slučaja
- Pretnja negativnim posledicama u slučaju odbijanja saradnje
- Nelagodni razgovor pri ispitivanju
- Pominjanje poznatih osoba
- Deljenje komplimenata ili laskanje
- Flertovanje

Uobičajene mete napada

TIP ŽRTVE

Neko ko nije svestan značaja informacija

Lica s posebnim ovlašćenjima

Proizvođači ili davaoci usluga

Posebna odeljenja

PRIMERI

Službenici prijemnih odeljenja, službenici na telefonskoj centrali, sekretarice i pomoćnici, čuvari.

Informatička ili tehnička podrška korisnicima, administratori računarskog sistema, računarski operateri, administratori telefonskog sistema.

Proizvođači računarskog hardvera i softvera, proizvođači sistema za glasovnu poštu.

Računovodstvo, kadrovsko odeljenje.

Faktori koji olakšavaju napad na kompanije

- Velik broj zaposlenih
- Više ogranaka
- Podaci o lokaciji zaposlenih u porukama glasovne pošte

- Objavljivanje broja lokala
- Nepostojanje bezbednosne obuke
- Nepostojanje sistema klasifikacije podataka
- Nepostojanje plana za prijavljivanje incidenata i reagovanje na njih

PROVERA I KLASIFIKACIJA PODATAKA

Ove tabele i blok-dijagrami će vam pomoći da reagujete na traženje informacija ili usluga koji mogu biti meta obmanjivača.

336

Postupak provere identiteta

POSTUPAK	OPIS
Identifikacija poziva	Proverite da li je poziv interni, i da li ime i broj lokala odgovaraju identitetu sagovornika.
Uzvratanje poziva	Potražite ime podnosioca zahteva u kompanijskom imeniku i pozovite ga na navedeni broj lokala.
Garantovanje	Zatražite od poverljivog radnika da garantuje za identitet podnosioca zahteva.
Deljena interna tajna	Zatražite da vam kaže tajnu koju deli čitavo preduzeće, kao što je lozinka ili dnevni kôd.
Nadzornik ili pretpostavljeni	Stupite u vezu s neposrednim pretpostavljenim tog radnika i zatražite da on potvrdi njegov identitet i status u firmi.
Bezbedna elektronska pošta	Zatražite da vam pošalju digitalno potpisanu poruku.
Lično prepoznavanje glasa	Ako neki zaposleni lično poznaje onoga za koga se sagovornik izdaje, pozovite ga da proveru da li je to njegov glas.
Izmenljive lozinke	Koristite vremenski žeton kao što je Secure ID, ili neko drugo pouzdano sredstvo za identifikaciju.
Lično	Zatražite od podnosioca zahteva da lično dođe sa propusnicom za zaposlene ili nekim drugim dokumentom za identifikaciju.

Postupak provere statusa zaposlenog

POSTUPAK

Provera u kompanijskom imeniku

Potvrda od pretpostavljenog podnosioca zahteva

Potvrda od odeljenja ili radnog tima podnosioca zahteva

OPIS

Proverite da li se ime zaposlenog nalazi u imeniku na mreži.

Pozovite njegovog pretpostavljenog na broj naveden u kompanijskom imeniku.

Pozovite odeljenje ili radni tim podnosioca zahteva i proverite da li je još uvek zaposlen u firmi.

Postupak utvrđivanja ovlašćenja za posedovanje informacija

POSTUPAK

Pogledajte spisak odgovornosti radnih mesta/timova

Zatražite odobrenje od svog pretpostavljenog

Zatražite odobrenje od osobe zadužene za informacije ili njegovog zamenika

Proverite ovlašćenje pomoću automatskog alata

OPIS

Pogledajte objavljene spiskove osoba koje su ovlašćene da poseduju određene poverljive informacije.

Pozovite svog pretpostavljenog, ili pretpostavljenog podnosioca zahteva, i zatražite odobrenje da mu ispunite zahtev.

Pitajte osobu zaduženu za informacije da li je podnosilac zahteva ovlašćen da poseduje date podatke.

Proverite ovlašćenja u posebnoj bazi podataka.

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.

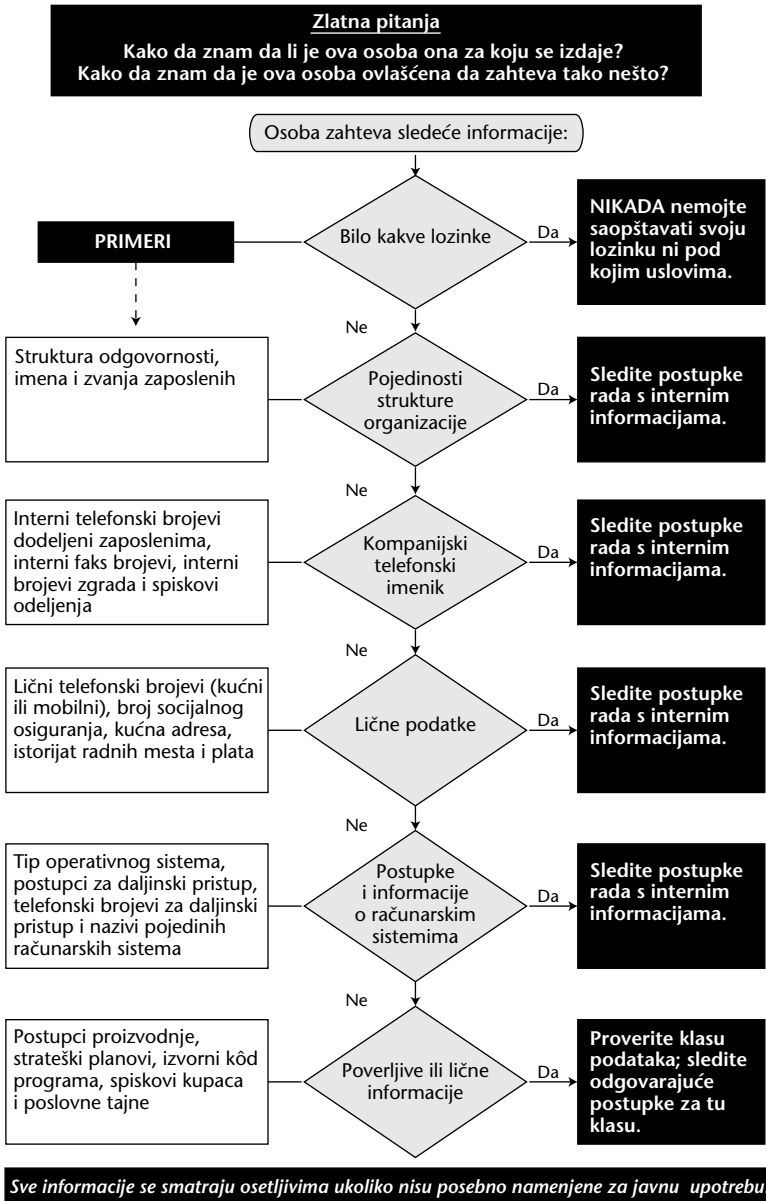
Identitet Proverite identitet i status zaposlenog u partnerskoj firmi.

- 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



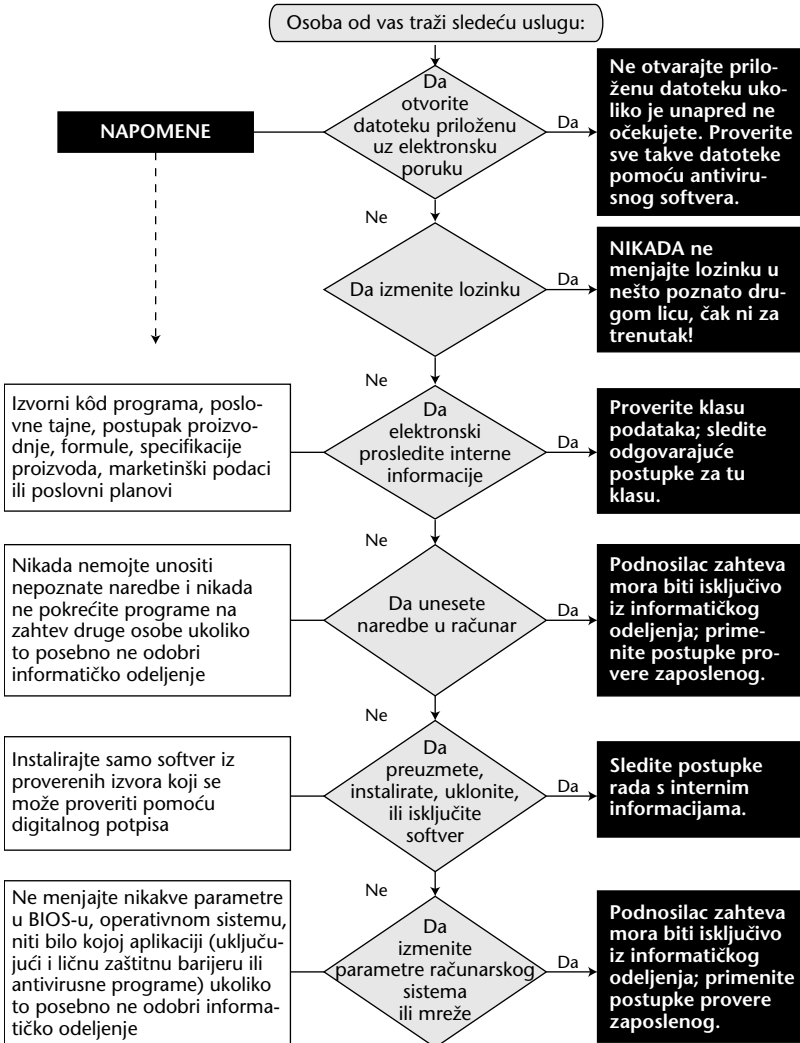
Kako reagovati kada neko zatraži da nešto uradite

Zlatna pravila

Nikome nemojte verovati dok ne proverite njegov identitet.
Poželjno je proveravati ispravnost zahteva.

340

Pregled bezbednosnih metoda



Sve što preduzmete na tud zahtev može naškoditi vašoj firmi. Proveravajte. Proveravajte.