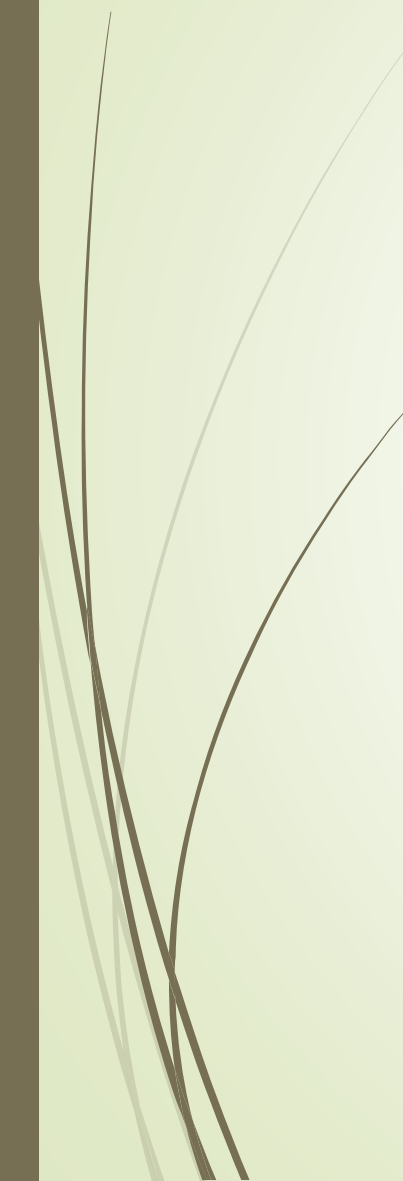


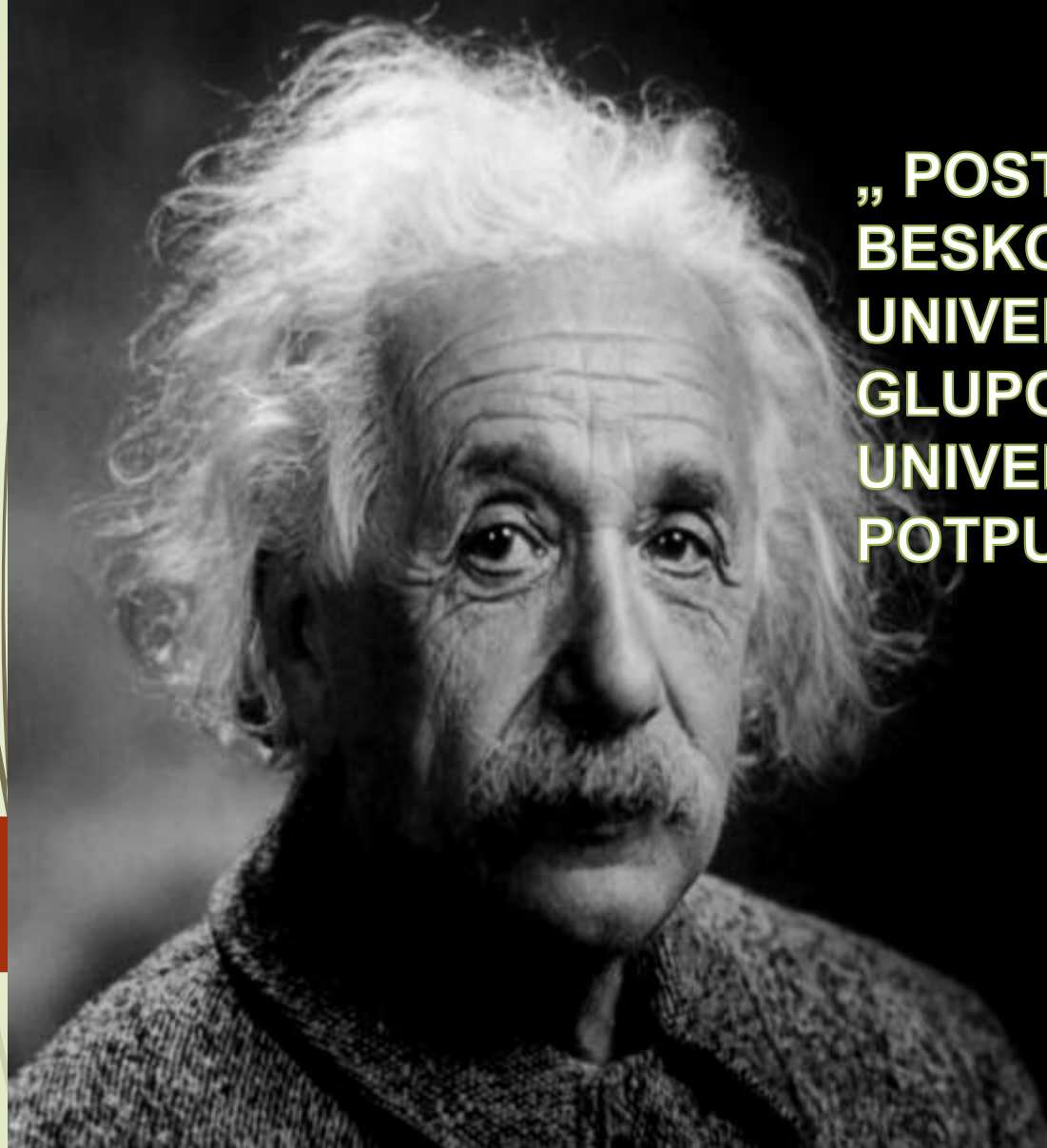
Socijalni inženjering

Specijalista menadžmenta bezbednosti
Mladen Raonić



Šta je to Socijalni Inženjering?

- ▶ Akt manipulacije ljudima u cilju stjecanja informacija i podataka do kojih napadač legitimnim putem ne bi mogao doći. Suština je da napad usmeren na najslabiju kariku celokupnog lanca – ČOVEKA.
- 

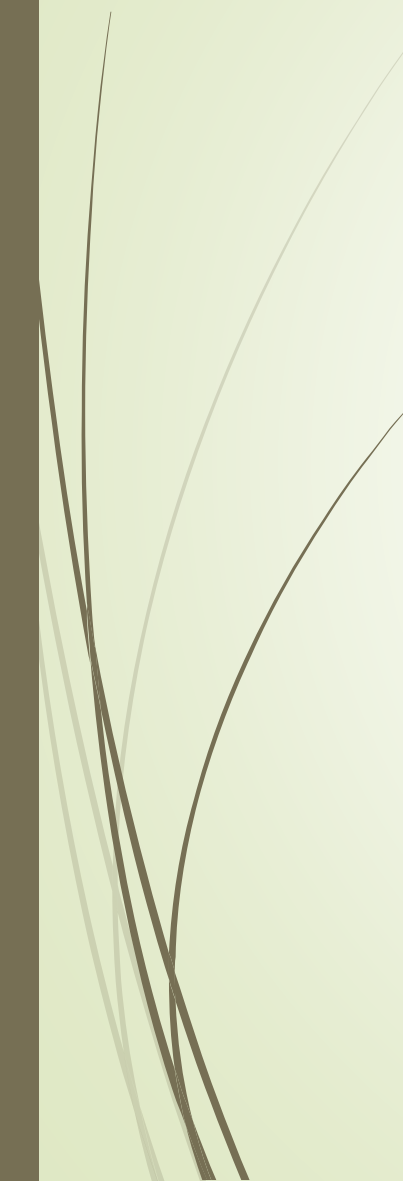


**„ POSTOJE SAMO DVE
BESKONAČNE STVARI,
UNIVERZUM I LJUDSKA
GLUPOST, MADA ZA
UNIVERZUM NISAM
POTPUNO SIGURAN “**

Albert Einstein




Ko su sve socijalni inženjeri ?

- Hakeri
 - Proverivači standarda
 - Špijuni
 - Nezadovoljni zaposleni
 - Kandidati za posao i potencijalni saradnici
 - Informatički provajderi
 - Prodavači
 - Zvanični službenici
 - Obični ljudi
- 



Filozofija socijalnog inženjeringa

- **SI = UMETNOST OBMANE**
 - **Prikupljanje informacija**
 - **Razvijanje veze sa žrtvom**
 - **Iskorištavanje veze sa žrtvom**
 - **Postizanje krajnjeg cilja**
- 



Ljudske osobine koje su meta napada

- povjerenje,
- Želju da se pomogne,
- Želju za sticanjem besplatnih stvari i nagrada,
- Znatiželja,
- Strah od nepoznatog,
- Strah od gubitka,
- Nemarnost i Nepažnja,
- Ignorisanje pravila.

7

DOBILI STE NAGRADU 😊



Uveravanje

- Nagovaranje ili uveravanje je akcija preduzeta od strane napadača kojoj je konačan cilj podstaknuti žrtvu na izvršavanje željenih postupaka.
- Primeri iz svakodnevnog života su propagandne poruke koje Vas uvlače u neku nagradnu igru ili Vas obavestavaju da ste dobili nagradu i „teraju“ da upišete lične podatke radi slanja iste.
- Sposobnost uveravanja jedna je od najvažnijih karakteristika koju socijalni inženjer mora posedovati ili razviti.

Lažno predstavljanje

- Ovo je najčešće korištena metoda napada. Predstavljanje u svojstvu nadređene osobe najučestaliji je odabir lažnog predstavljenog socijalnog inženjera. Napadač poziva djelatnika i nadređenim mu tonom zapovijeda što treba činiti.
- Napadač se može predstavljati i kao službenik pa na taj način doći do informacija od, primjerice, službenika na istoj razini u nekoj drugoj poslovnicu tvrtke. Poznato je da je ljudi, pogotovo kada su u istom položaju, najčešće žele pomoći jedan drugome. Međutim, solidarnost u ovom slučaju može značiti i obznanu tajnih informacija napadačima.

Lažno predstavljanje (2)

➔ Jedan od često korištenih načina lažnog predstavljanja je izigravanje novog zaposlenog. Ljudi su skloni pomoći početnicima, što socijalni inženjeri često koriste za saznavanje detalja o radu organizacije koju žele napasti. Nije moguće, a ni dobro, zaposlenim zabraniti međusobnu pomoć, ali je zato preko potrebno kvalitetno edukovati zaposlene u domenu bezbednosne kulture.

STVARANJE SCENARIJA

- Osnova socijalnog inženjeringa je stvaranje situacije u kojoj je žrtva ima utisak da je primorana donositi brze i važne odluke pod velikim psihološkim pritiskom s jedne strane, i brojnim zahtevima napadača s druge.
- Najčešće su žrtve same krive za nastalu situaciju pa je donošenje pogrešnih zaključaka nužan ishod pokušaja ispravljanja postojećeg stanja, odnosno otklanjanja zastoja. Jedan od najboljih načina napadanja je zblžavanje s ljudima koji su dio sustava na koga se želi izvršiti napad.
- Najčešći načini sticanja poverenja su postupno stvaranje odnosa između napadača i žrtve i navođenje žrtve na verovanje u buduću korist od napadača.

Da li crvenkapa veruje vuku ?



Nigerijska šema (šema 419)

- Gospodin iz Njujorka je dobio pismo u kome stoji da je knjigovođa iz Nigerije svojim dugim i umešnim poslovanje sakupio 20.000.000 miliona Dolara i sad traži osobu koja ima račun u drugoj zemlji da novac prebaci jer se firma u kojoj je radio zatvara, zbog političke situacije u zemlji....
- **KLJUČNI MOMENAT JE KADA ŽRTVA POVERUJE....**



Iskorišćavanje starih veza

- ▶ U ovom načinu socijalnog napada, napadač obnavlja stare ili stvara nove veze sa žrtvama. Napadač će stvoriti odnos koji je dovoljan za stjecanje poverenja.
- ▶ Ovakav pristup kod socijalnog inženjeringa ima vrlo veliki stepen uspešnosti, što je posebno izraženo ukoliko je žrtva spremna za ostvarivanje saradnje sa napadačem.
- ▶ Na taj način je pređena početna barijera i prikupljanje željenih informacija kreće lakšim tokom.

Načini izvršavanja napada

- Postoje brojne metode izvođenja navedenog napada, a poznatije su:
- 1. Shema brzog bogaćenja (eng. Get-rich-quick scheme)
- 2. Prevare vezane uz romantiku – napadač iskorištava osobe kako bi došao do njihovih sredstava.
- Prevare „gold brick“ – pokušaj prodaje proizvoda za puno veću vrednost od stvarne.
- 4. Prevare s lažnim nagradama – navođenje žrtve da veruje kako će dobiti nagradu nakon što je slučajno odabrana.
- „Online“ prevare – temeljene na uporabi Internet-a.

Zaštita od socijalnog inženjeringa...

- Edukacija zaposlenih sa naglaskom na personal koji ima kontakte sa eksternim faktorima.
- Kreiranje i unapređenje bezbednosnih protokola i procedura.
- Česte revizije bezbednosnih sistema
- Zamena IT pristupnih parametara
- Bezbednosne provere novih zaposlenih
- Praćenje konkurencije i poslovno obaveštajna delatnost

Sigurnosna politika

- ▶ U svakoj od organizacija je jedan od najvažnijih koraka postizanja bezbednosti jeste stvaranje sigurnosnih pravila (eng. Security policy). Nažalost, organizacije troše mnogo novca u sigurnost hardver-a i programske podrške, ali ne obraćaju u dovoljnoj meri pažnju na ljudski faktor.
- ▶ Kako bi problem bezbednosti bio adekvatno tretiran, odgovorna osoba mora razumeti važnost razvijanja i primene kvalitetnih sigurnosnih pravila, smernica i procedura. Efikasnost bezbednosnih procedura podrazumeva potpunu podršku svih članova organizacije.

ZAKLJUČAK

- Napadi temeljeni na socijalnom inženjeringu prisutni su u svim sferama ljudskog života, a u poslednjoj eri se multiplikuju zbog porasta mogućnosti i načina komunikacije.
- Bitna odrednica korporativne bezbednosti i uloga funkcije HR-a u poslovnim sistemima upravo jeste pojačan nadzor na rizicima koji dolaze iz kuhinje socijalnih inženjera.