Ofenzivna sigurnost

Psihološki temelji društvenog inženjeringa

Noa Oreški, 08.12.2025.

Pregled predavanja

- Motivacija
- Pitanja za ispit
- Općenito o društvenom inženjeringu
- Psihološki pogled na društveni inženjering
- Kognitivne pristranosti
- Primjeri kognitivnih pristranosti
- Detekcija i zaštita od društvenog inženjeringa
- Zaključak

Motivacija

- Društveni inženjering iskorištava ljudsku psihologiju — najveću slabost sigurnosti
- Tehničke zaštite ne mogu spriječiti manipulaciju ljudi
- Razumijevanje psihologije pomaže prepoznati i spriječiti napade ➡ bolja edukacija i sigurnosni protokoli

Pitanja za ispite

- Definirajte društveni inženjering.
- Što su mentalni prečaci?
- Kada nastaju kognitivne pristranosti?
- Navedite 3 karakteristike kognitivnih pristranosti.
- Što je pristranost hitnosti i kako ona utječe na žrtvu?

Što je društveni inženjering?

- Umjetnost iskorištavanja najslabije karike u sustavima informacijske sigurnosti – korisnici sustava
- Cilj: iskoristiti ljudske pogreške i slabosti kako bi se žrtvu navelo da učini nešto što nije u njezinom interesu
- Napadač cilja **ljudsku psihologiju**, a ne tehnologiju

Psihološki pogled na društveni inženjering (1/2)

- Društveni inženjering dio je procesa donošenja odluka
- Nemogućnost detaljnog analiziranja svih informacija ➡ proces donošenja odluka koristi mentalne prečace (heuristike)
- Heuristike - rezultat kombinacije genetike i iskustva

Psihološki pogled na društveni inženjering (2/2)

- Mentalni prečaci dobro funkcioniraju u većini situacija
- Ukoliko mentalni prečaci zakažu (dovedu do pogrešnog zaključka), tada nastaju **kognitivne pristranosti**

Kognitivne pristranosti

- Sustavne, predvidljive greške u razmišljanju koje ljude udaljavaju od logičnog i racionalnog načina razmišljanja i ponašanja
- Nastaju zato što naš mozak koristi mentalne prečace kako bi brzo donio odluke
- Utječu na odluke i prosudbe
- Čine ljude ranjivima na manipulaciju društvenim inženjeringom

Karakteristike kognitivnih pristranosti

- **Nesvjesne** - ne shvaćamo da utječu na našu odluku
- **Brze** i **automatske** - rezultat su brzog razmišljanja
- **Ugrađene** - dio su načina na koji mozak funkcionira
- **Predvidljive** - ponavljaju se u sličnim situacijama

Pristranost prema autoritetu

- Sklonost poslušati ili vjerovati osobi koju smatramo autoritetom
- Automatska reakcija na autoritet bez kritičke provjere
- Česta taktika u društvenom inženjeringu:
  - Napadač se predstavlja kao IT administrator, šef ili službenik neke institucije
  - Žrtva često daje podatke ili pristup bez provjere
- Primjer:
  - e-mail od ”šefa” koji zahtjeva dostavu neke povjerljive datoteke

Pristranost oskudice

- Stvari koje su “rijetke” ili “ograničene” djeluju vrijednije i poželjnije
- Potiče se impulzivna odluka
- Primjer:
  - Lažne ponude: “SAMO DANAS 80% POPUSTA!”
  - Phishing poruke s “ekskluzivnim pristupom”

Pristranost uzajamnosti

- Osjećaj obveze da uzvratimo uslugu
- Napadači koriste osjećaj zahvalnosti ili pomoći
- Primjer:
  - Napadač se predstavlja kao kolega i daje korisnu informaciju, ali ima i neki zahtjev
  - Žrtva poslušno izvršava njegov zahtjev jer osjeća obavezu uzvratiti uslugu

Društveni dokaz

- Radimo ono što drugi navodno rade
- Pritisak konformnosti smanjuje kritičko razmišljanje
- Primjer:
  - Napadač tvrdi: “Svi su u vašem odjelu već ažurirali korisničke podatke uporabom ove poveznice”

Pristranost hitnosti

- Brze odluke pod pritiskom vremena
- Smanjuje kritičko razmišljanje i provjeru legitimnosti informacija
- Primjer:
  - Napadač šalje poruku: “Vaš račun će biti blokiran za 5 minuta! Prijavite se pomoću poveznice kako biste sačuvali korisnički račun!”
  - Žrtva ishitreno klikne na zlonamjernu poveznicu i unese vjerodajnice svog korisničkog računa

Pristranost sviđanja

- Lakše vjerujemo ljudima koji su simpatični, prijateljski ili slični nama
- Izgradnja povjerenja čini nas ranjivima
- Primjer:
  - Napadač hvali žrtvu i odmah nakon toga traži uslugu ili informaciju
  - Žrtva vjeruje napadaču jer je “prijateljski nastrojen”

Psihološki signali koji upućuju na društveni inženjering

- Osjećaj pritiska ili žurnosti
- Neočekivan i nelogičan kontekst
  - Zahtjev koji ne odgovara proceduri ili ranijoj komunikaciji
- Previše prijateljska ili premalo formalna komunikacija
  - Pretjerana bliskost u startu
- Nagla emocija
  - Osjećaj snažne i iznenadne promjene emocije nakon interakcije

Psihološke tehnike obrane

- Praksa kognitivnog usporavanja
  - Namjerna pauza od nekoliko sekundi prije donošenja odluke
  - Smanjuje utjecaj emocija

- “STOP – THINK – VERIFY” metoda
  - STOP - ne reagiraj odmah
  - THINK – analiziraj emociju i kontekst
  - VERIFY – provjeri identitet i legitimitet

Zaključak

- Društveni inženjering cilja ljudske slabosti, ne tehnologiju
- Postoje brojne kognitivne pristranosti koje olakšavaju manipulaciju
- Razumijevanje psiholoških mehanizama pomaže u razvoju prikladnih zaštitnih mehanizama
- Edukacija i sigurnosne mjere jačaju otpornost pojedinaca, a time i organizacije

Literatura

- Todorović, Anastasia. 2025. *Kognitivne pristranosti i duhovni rad*. Završni rad, Sveučilište Jurja Dobrile u Puli, Fakultet ekonomije i turizma "Dr. Mijo Mirković". https://repozitorij.unipu.hr/object/unipu:10682
- Bullée, Jan-Willem Hendrik, Lorena Montoya, Wolter Pieters, Marianne Junger, and Pieter Hartel. 2017. *On the Anatomy of Social Engineering Attacks—A Literature-Based Dissection of Successful Attacks.* Journal of Investigative Psychology and Offender Profiling. https://doi.org/10.1002/jip.1482
- Legaspi, Pocholo. 2025. *Don't Get Hooked: 10 Social Engineering Indicators.* Admin By Request, 2025. https://www.adminbyrequest.com/en/blogs/dont-get-hooked-10-social-engineering-indicators
- Portsmouth Police Department. 2025. *Stop. Think. Verify.* Portsmouth, RI. https://www.portsmouthri.gov/1785/Stop-Think-Verify

Dodatna literatura

- RSA Conference. 7. lipnja 2023. *Protecting the Organization: The Psychology of Social Engineering.* YouTube video. https://www.youtube.com/watch?v=XEJRIhAwHoY

Hvala!