Ofenzivna sigurnost

Metodologija provođenja društvenog inženjeringa

Lucija Petkoviček, 8.12.2025.

Pregled predavanja

- Motivacija
- Pitanja
- Uvod u društveni inženjering
- Kill Chain okvir društvenog inženjeringa
  - Razrada faza okvira
- Primjer
- Obrana od napada društvenim inženjeringom
- Zaključak

Motivacija (1)

- Softverski napadi iziskuju puno znanja, alata i vremena za pronalaženje slabosti mete
- Ljudski faktor je najslabiji dio obrane jer je podložan emocijama i društvenim normama
- Za ljudske slabosti nema "zakrpe" koje će biti efektivne kao kod softvera

Motivacija (2)

- Potreba za jasnim metodološkim okvirom zbog boljeg razumijevanja napada i obrane

Pitanja za ispite

- Što je društveni inženjering?
- Nabroji faze Kill Chain-a društvenog inženjeringa i za svaku fazu navedi po barem jednu taktiku.
- Objasni taktiku izrade scenarija i nabroji tehnike koje se koriste.
- Nabroji i objasni 3 tehnike interakcije sa žrtvom.
- Objasni i daj primjer održavanja stanja (*Maintenence*).

Uvod u društveni inženjering (1)

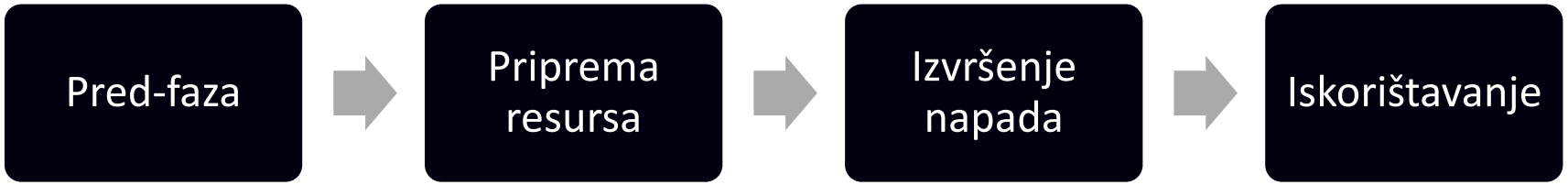
- Društveni inženjering je metoda iskorištavanja ljudskog faktora kao najslabije sigurnosne karike u svrhu postizanja određene akcije ili cilja
- Napadač se lažno predstavlja, ima izmišljen narativ, izgleda bezopasno i vjerodostojno
- Žrtva nije svjesna da je napadnuta

Uvod u društveni inženjering (2)

- Ontološki model: cilj, medij, društveni inženjer, meta, principi društvenog utjecaja, tehnike
- Principi društvenog utjecaja
  - Obvezivanje (*Commitment or consistency*)
  - Oskudica (*Scarcity*)
  - Recipročnost (*Reciprocity*)
  - Društvena validacija (*Social validation*)
  - Autoritet (*Authority*)
  - Prijateljski odnos (*Friendship or liking*)

Kill Chain okvir

- Velik broj tehnika možemo složiti u Cyber Social Engineering Kill Chain okvir (inspiracija Cyber Kill Chain)
- Faze
  - Taktike
    - Tehnike



Pred-faza (1)

- Definiranje cilja napada
- Izviđanje
  - Sakupi informacije te identificiraj slabosti i prilike
  - Tehnike:
    - Pasivno promatranje
    - Dumpster-diving
    - Izviđanje iz otvorenih izvora

Pred-faza (2)

- Odabir mete
  - Prema tome koliko je iskoristiva i koliko to doprinosi postizanju cilja
  - Tehnike:
    - Analiza slabosti
    - Identifikacija dostupnih resursa mete
    - Identifikacija ograničenja okoline
    - Utjecaj mete
    - Iskoristivost mete

Priprema resursa (1)

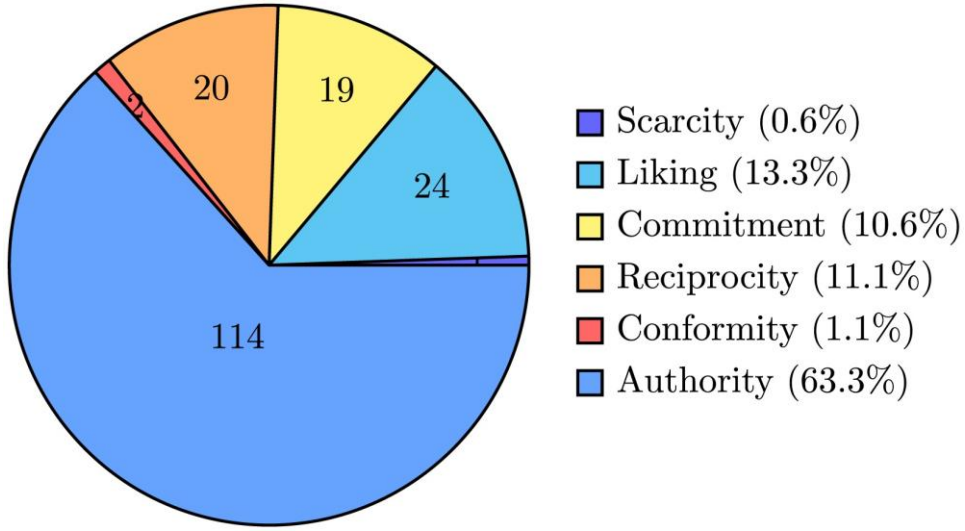
- Izrada scenarija
  - Opravdanje zašto stupamo u kontakt s metom
  - Scenarij i persona
  - Tehnike:
    - Kontekstualizacija
    - Prerušavanje

Priprema resursa (2)

- Izrada infrastrukture i artefakta
  - Dokazi koji čine scenarij vjerodostojnijim
  - Profili, web-stranice, domene, dokumenti…
  - Mogu se izgraditi ili uzeti od treće osobe
  - Tehnike:
    - Kompromitiranje infrastrukture
    - Razvoj sposobnosti
    - Vizualna obmana
    - Spoofing (krivotvorenje)

Priprema resursa (3)

- Izrada poruke
  - Cilj poruke je uvjeriti žrtvu da izvrši radnju koju napadač želi
  - Smanjiti i odgoditi žrtvinu percepciju rizika
  - Tehnike:
    - Signali hitnosti
    - Okidači pažnje
    - Uvjeravanje - autoritet u 63% slučajeva
    - Poticaji i motivatori
    - Individualizacija



Udio korištenja različitih implementacija uvjeravanja, [1]

Izvršenje napada (1)

- Inicijalni kontakt
  - Tehnike:
    - Phishing
    - Drive-by kompromitacija
    - Širenje putem prenosivih medija
    - Pouzdani odnos
    - Obrnuti društveni inženjering

Izvršenje napada (2)

- Interakcija s žrtvom
  - Kontinurirana komunikacija sa žrtvom i poticanje suradnje
  - Tehnike:
    - Pretexting
    - Scamming
    - Emocionalno povjerenje kroz kontinuirani odnos
    - Foot-in-the-door
    - Quid-pro-quo

Iskorištavanje (1)

- Ispostava uporišta
  - Kada žrtva omogući prodor napadača u sustav
  - Otvaranje mogućnosti za daljnje kompromitacije
  - Tehnike:
    - Eksploatacija ranjivosti na klijentskoj strani
    - Zakazane radnje/zadaci
    - Zlouporaba sustavskih servisa

Iskorištavanje (2)

- Okončanje
  - Završetak napada
  - Tehnike:
    - Financijski transfer
    - Informacijski transfer
- Održavanje stanja (*Maintenence*) (nije taktika Kill Chain-a nego se koristi u predlošcima [3])
  - Nastavak prijateljske i neformalne komunikacije i nakon napada
  - Normalizira prethodnu interakciju kako bi se umanjila percepciju rizika

Primjer - prevara pri zapošljavanju (1)

1. Pred-faza

- Definiranje cilja: krađa osobnih podataka i novca
- Izviđanje: istraživanje platformi za zapošljavanje i njihovih pogodnosti za organizacije -> LinkedIn (**pasivno promatranje**)
- Odabir mete: LinkedIn sam preporučuje žrtve, napadač cilja ‘white-collar’ profesionalce (projektne menadžere s dobrim financijskim primanjima)

2. Priprema resursa

- Izrada scenarija: fiktivna tvrtka i persona voditelja zapošljavanja
- Infrastruktura i artefakti: izrađuje se identična kopija web stranice legitimne građevinske tvrtke uz korištenje njihovih službenih logotipa i grafika (**spoofing**)
- Izrada poruke: nudi se visoka plaća ($105k - $160k) kako bi se privukla pažnja (**motivatori**), uz **autoritet** voditelja zapošljavanja koji zahtijeva intervju uživo (**uvjeravanje** - **društvena validacija**)

Primjer – prevara pri zapošljavanju (2)

3. Izvršenje napada

- Inicijalni kontakt: **obrnuti društveni inženjering** (žrtva se javlja napadaču)
- Interakcija sa žrtvom:
  - **Pretexting**: poziv na intervju služi kao izgovor za traženje putnih informacija i dokumenata
  - **Foot-in-the-door**: zahtjevi se povećavaju postupno , prvo životopis, zatim osobni podaci, a na kraju novac za troškove puta
  - **Scamming**: žrtva je toliko fokusirana na obećanu visoku plaću da ne uočava nelogičnost plaćanja putnih troškova unaprijed

4. Iskorištavanje

- Okončanje: žrtva vrši financijski i informacijski transfer

Obrane od napada društvenim inženjeringom (1)

- Ne rješava se temeljni uzrok – ljudsko prosuđivanje
- Većina postojećih obrana se temelji na detekciji i filtriranju poruka društvenog inženjeringa
- Mali broj psiholoških faktora je zapravo adresiran metodama obrane

Obrane od napada društvenim inženjeringom (2)

- Primjeri obrana:
  - Uvođenje procedura i **predložaka**
  - Podizanje svijesti

Zaključak

- Bitno je formirati jasnu metodologiju i Kill Chain okvir kako bi se jasnije razumjele sve tehnike društvenog inženjeringa i mane ljudskog faktora
- Bolje razumijevanje tehnika i psihičkih faktora kod društvenog inženjerstva dovest će i do unaprjeđenja obrane od takvog napada

Literatura

1. Bullée, Jan-Willem Hendrik, et al. „On the anatomy of social engineering attacks—A literature-based dissection of successful attacks.” Journal of Investigative Psychology and Offender Profiling. 15.1 (2018): 20-45
2. Montanez, Rosana & Xu, Shouhuai. „Cyber Social Engineering Kill Chain”. International Conference on Science of Cyber Security. Cham: Springer International Publishing, 2022.
3. Mouton, Francois, Louise Leenen, and Hein S. Venter. „Social engineering attack examples, templates and scenarios.” Computers & Security 59 (2016): 186-209. **(nudi puno primjera predložaka)**

Hvala!