Bezbedan ljudski element

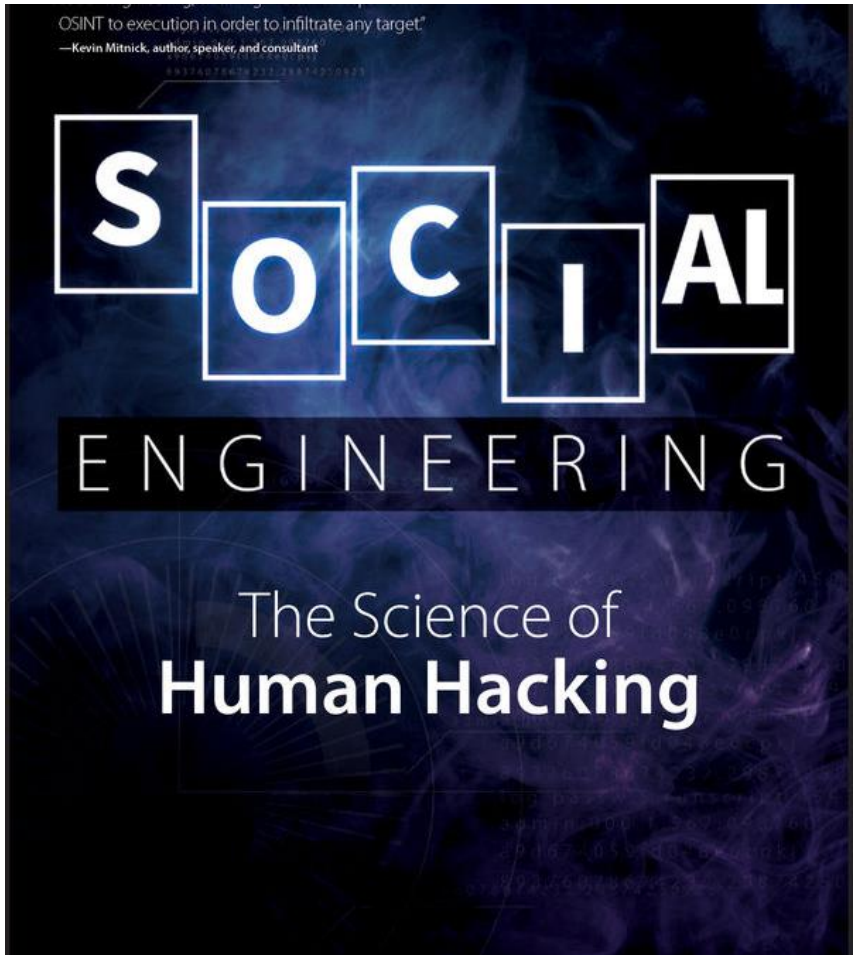
Informaciona bezbednost

Fakultet tehničkih Nauka, Univerzitet u Novom Sadu

Imre Lendak, 2020

Sadržaj današnjeg predavanja

- Slabosti i pretnje u domenu ljudskog elementa
- Zaštitne mere
- Primeri primene mera
- **Napomena:** mere bezbednosti u domenu ljudi, procesa i tehnologija → ovde pričamo o aspektu bezbednosti ljudskih resursa, tj. ljudima (eng. people)



Bezbedan ljudski element

SOCIJALNI INŽENJERING

Socijalni inženjering

- Cilj **socijalnog inženjeringa** je nalaženje slabosti u ljudskom elementu distribuiranih informacionih sistema (tj. zaposlenima i saradnicima) i zloupotreba tih slabosti u cilju postizanja nekog cilja, npr. dobijanje pristupa sistemu
- **Aktivne mere** socijalnog inženjeringa podrazumevaju (verbalnu ili elektronsku) interakciju sa zaposlenim. U ovu grupu spada(ju):
  - Impersonacija
  - Phishing i njegove podvrste
- **Pasivne mere** socijalnog inženjeringa ne zahtevaju interakciju sa zaposlenim, već se slabost ljudskog elementa zloupotrebljava posredno. U ovo grupu spada(ju):
  - Prisluškivanje i njegove varijante

Prisluškivanje

- Pretnja tipa presretanje (*interception*)
- Metodologija:
  - Lično prisustvo
  - Postavljanje uređaja za snimanje zvuka i/ili videa
  - Keylogger u digitalnom domenu

Shoulder surfing

- Shoulder surfing je pretnja tipa presretanje (*interception*) i podrazumeva lično prisustvo napadača
- Prilazak žrtvi i prikupljanje informacija gledanjem preko ramena

Impersonacija

- Impersonacija je čin predstavljanja kao neko ko ima legitiman pristup sistemu ili podacima
  - Tehnička podrška, tj. administrator
  - Predstavnik banke ili druge finansijske institucije
  - Član rukovodstva
  - Kolega kome treba pomoć
  - Predstavnik partnerske organizacije (u poslovnom svetu)
  - Eksterna služba za popravke
- Impersonacija se često kombinuje sa požurivanjem i pozivanjem na nečiji autoritet, npr. predstavljanje kao direktor ili pretnja disciplinskom merom
- Impersonacija je moguća u fizičkom ili u elektronskom prostoru

Phishing

- Phishing je jedan vid računarske impersonacije u kom napadač pribavlja osetljive informacije preko lažiranih poruka
- Komunikacioni kanal može biti email, socijalna mreža, *instant messaging* (IM) sistem, fiksna/mobilna telefonija, lično
- Napadač se predstavlja kao
  - Poruka od administratora sistema
  - Poruka od banke
  - Poruka od ožalošćene porodice (ili advokata) bogate osobe
- Termin „phishing“ potiče iz 1995

Spear phishing

- „Kampanja“ koja ciljano gađa određeni tip ljudi ili radnike određene kompanije
  - Najčešći komunikacioni medijum je email
  - Npr. radnici u poslovnim podsistemima kritičnih infrastruktura
  - Jedan od najuspešnijih tehnika na Internetu danas
- Napadači koriste razne metode ubeđivanja kroz elektronske sadržaje
  - Često se „igra“ na pohlepu i/ili strah od nadređenih
- Spear phishing je korišćen u prvoj fazi napada na energetski sektor u Ukrajini u decembru 2015. godine
- *Whaling* je podvrsta spear phising-a u kojem se kontaktiraju direktori i viši menadžeri

Bezbedan ljudski element

MERE BEZBEDNOSTI PROTIV SOCIJALNOG INŽENJERINGA

Bezbednosna politika

- Jedinstvena bezbednosna politika u borbi protiv socijalnog inženjeringa → definiše proces u kontekstu ljudi, procesa i tehnologija
- Odabir i kreiranje lojalne radne snage
  - Jasna prava i pravila za sve zaposlene
  - Edukacija zaposlenih sa ciljem jačanja svesti o socijalnom inženjeringu.
  - Jasne procedure za odlazak zaposlenih
- Unutrašnja služba bezbednosti

Mere bezbednosti

- Komunikacioni kanali: telefon, email, IM, socijalne, mreže, lično
- Znaci koji ih odaju: tehnička podrška/služba, šef, kolega na terenu, požurivanje
- Telefon:
  - Proveriti izvor telefonskih poziva
  - Tražiti broj na kojem vratiti poziv
- Socijalne mreže:
  - Selektivno zabraniti IM i socijalne mreže
- Elektronska pošta:
  - Filtriranje i skeniranje poruka na email serverima
- Fizički prostor:
  - Identifikovati drugu stranu
  - Dokaz o zakazanom sastanku

Bezbedan ljudski element

IZGRADNJA BEZBEDNE RADNE SNAGE

Mere pre zaposlenja

- Proveriti svaku prethodnu (radnu) poziciju
  - Obratiti pažnju na neobjašnjene “rupe” → zatvorska kazna, rad u službama bezbednosti i sl.
- Provera ključnih tvrdnji iz CV-a (tj. biografije):
  - diplome, sertifikati
  - znanje jezika
  - uverenje o nekažnjavanju
  - kreditna sposobnost – ovo je često zakonski zabranjeno, jer je izvor diskriminacije (npr. siromašan Afro-Amerikanac)
- Provera svih izdavaoca referenci
- Provera fizičke i psihičke sposobnosti

Mere tokom zaposlenja

- Definisati osobu kome prijavljuju bezbednosne probleme
  - Lanac prijave po zonama, npr. spratovima
- Redovne obuke i informisanje o politici bezbednosti
  - Dopisi o najnovijim Internet baziranim prevarama, npr. elektronska poruka administratora dvaput mesečno
- Nagrade za one koji prate pravila bezbednosti
- Posebno osetljivi momenti tokom zaposlenja
  - Smanjenje plate
  - Promena titule
  - Planirana otpuštanja

Odlazak zaposlenih

- Izvršiti detaljnu kontrolu hardvera, softvera i podataka (bivšeg) zaposlenog
- Sinhronizovano izvršiti sledeće akcije u fizičkom domenu
  - Zabraniti pristup radnoj stanici, npr. oduzeti službeni laptop
  - Uzeti ključeve, magnetne kartice, i sl.
  - Ispratiti zaposlenog (npr. do izlaza iz poslovne zgrade)
- Izvršiti sledeće akcije u elektronskom domenu:
  - Zabraniti i odinstalirati VPN pristup
  - Obrisati ili deaktivirati sve naloge – nekad brisanje nije moguće
  - Obrisati javno dostupne podatke o zaposlenom (npr. website)
- Po potrebi kreirati bekape i proveravati logove svih sistema kojima je zaposleni imao pristup

Posebne mere za programere

- Kompanije koje zapošljavaju veći broj programera, treba da razviju posebne planove obuke za zaposlene
  - Očekivano viši nivo znanja na polju informacionih tehnologija
  - Trening ekipa (uglavnom) ima manje posla vezano za socijalni inženjering, jer programeri imaju potrebna saznanja iz oblasti
  - Administratori treba da se dodatno potrude u onemogućavanju pristupa nedozvoljenim servisima na Internetu
  - Pažljivo deljenje administrativnih naloga, npr. samo lokalni admin
- Mogući posebni treninzi za programere:
  - Primenjena kriptografija
  - Tehnike za izbegavanje nenamernih softverskih grešaka
  - Modeliranje pretnji (engl. threat modelling)

Rezime

- Socijalni inženjering
- Primeri mera u zaštiti od socijalnog inženjeringa
- Prijem i odlazak zaposlenih
- Posebne mere za programere

Hvala na pažnji!