Social Engineering

Petr Medonos, Anna Janáčková

O nás

Petr Medonos

- 6 let v ETN
- dohled nad přiváděním projektů k životu, konzultace
- DBA, performance, security
- EWA (ewa.etnetera.cz)
- CEH, RHCE, M102, M202

@PetrMedonos

[in] PetrMedonos

Anna Janáčková

- 5 let v ETN
- nahrazení sebe sama strojem (Puppet, ... ;)
- zalohování, automatizace
- M202

@AJanackova

[in]AnnaJanackova

Co je SE?

Co je SE?

motivace

Sociální inženýrství je způsob ~~manipulace~~ lidí za účelem provedení určité akce nebo získání určité informace. (wikipedia)

Proč se zabývat SE?

- slušné zabezpečení OS
- aplikace se automaticky aktualizují
- spousta peněz investovaných do bezpečnostních prvků
- spousta lidí věnující se defenzivní bezpečnosti

Proč se zabývat SE?

- slušné zabezpečení OS
- aplikace se automaticky aktualizují
- spousta peněz investovaných do bezpečnostních prvků
- spousta lidí věnující se defenzivní bezpečnosti
- co uživatelé?

Proč se zabývat SE?

make.believe

Vlastnosti člověka

- důvěřivost
- zdvořilost a laskavost
- zvědavost
- potřeba pomáhat
- strach
- hloupost
- ego
- ...

Čeho využívá SE?

- důvěřivost
- zdvořilost a laskavost
- zvědavost
- potřeba pomáhat
- strach
- hloupost
- ego
- ...

Techniky a cíle SE

- **unesení amygdaly**
- sbírání informací (information gathering)
- vylákání (elicitation)
- převlek (pretext)
- převědčování (persuasion)
- mind tricks
  - NLP
  - budování vztahu
  - …

Neverbální komunikace

- 50% komunikace
- dokresleni převleku
- emoce
  - obličej
    - mikro výrazy
    - makro výrazy
  - tělo

Techniky získání vlivu

- reciprocita a povinnost
- ústupek
- vzácnost
- závazek a konzistence
- autorita
- oblíbenost
- sociálni schválení

Vektory útoku

- phishing
  - spear phishing
- telefon
- sociální sítě
- osobní setkání
  - usb zařízení
  - teensy
- ...

Triky :)

- můžete mi prosím pomoc?
- dotek
- protože
- využití davu

Obrana

- školit zaměstnance
  - skripty
  - důležitost informací
- definice politik pro práci s daty
- SE audity
- striktní konfigurace FW, AV :), IPS/IDS, aktualizace SW, ...

QA?