SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Testování organizací technikou sociálního inženýrství

Barbora Netolická, ESET, spol. s. r. o.

Obsah prezentace

- Sociální inženýrství (SE) obecně
- SE a firemní bezpečnost
- Důvody pro testování technikou SE
- Způsoby testování technikou SE
- Postup při testování technikou SE
- Výstupy z testování technikou SE

Sociální inženýrství

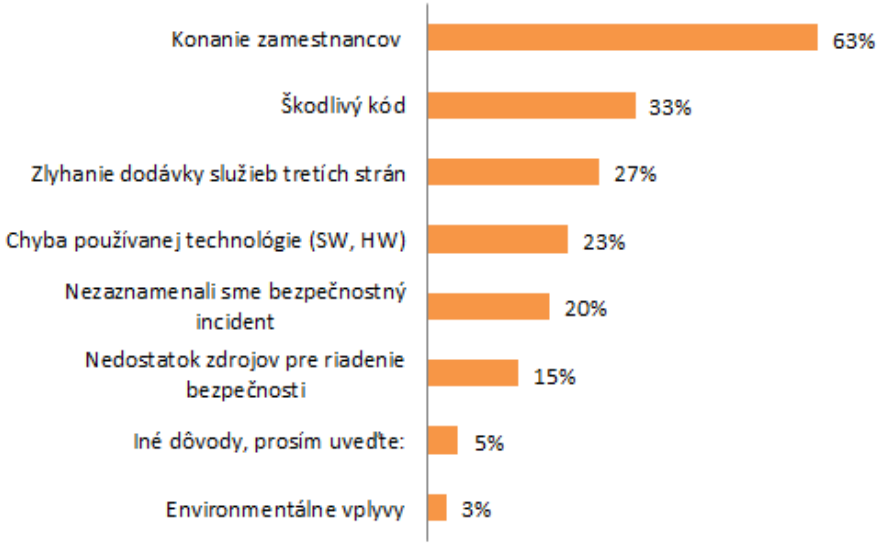
Způsob manipulace lidí za účelem provedení nějaké akce, získání informací nebo finančních prostředků…..

Proč to funguje…

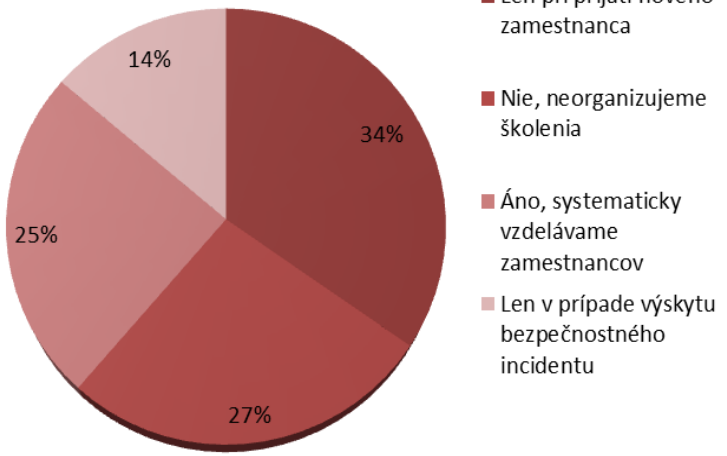
- Důvěra
- Stres
- Strach
- Vidina získání výhody
- Respektování autorit
- Ochota napomáhat
- Potřeba „mít klid“
- Sympatie

SE a firemní bezpečnost

Důvody výskytu bezpečnostních incidentů



Zvyšování bezpečnostního povědomí a školení



Zdroj: „Prieskum stavu informačnej bezpečnosti v organizáciách na Slovensku v roku 2011“ [ESET]

Slabiny v organizacích ve vztahu k SE

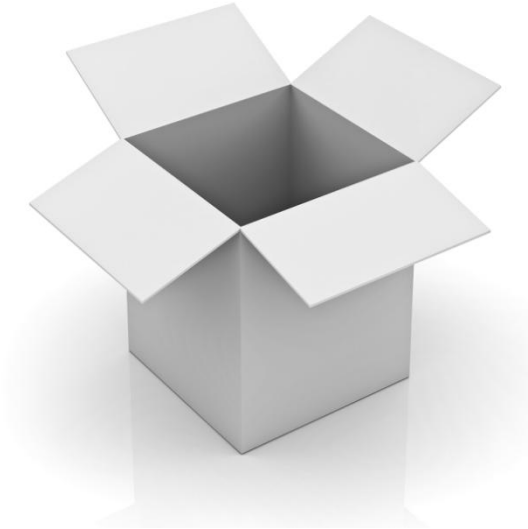
- pravidla na ochranu informací a jejich prosazení:
  - klasifikace informací
  - zacházení s jednotlivými typy informací
  - pravidla fyzické bezpečnosti
  - pravidla na ochranu proti škodlivým programům
  - pravidla na ochranu hesel
  - pravidla hlášení bezpečnostních incidentů
- školení zaměstnanců
- povědomí o SE a jeho formách

Důvody pro testování

- reálná zkušenost s tím, co se může stát
- reálná představa o dopadech
- přímá identifikace slabých míst
- představa o zacílení bezpečnostních opatření
- zvýšení bezpečnostního povědomí u zaměstnanců

Způsoby testování

- phishing test
- telefonický test
- test s přenosnými médii
- fyzický průnik do prostor
- prohledávání odpadků



Postup při testování

Nejčastější zjištění

- neuvědomují si, jaké informace jsou z pohledu organizace chráněné:
  - zveřejňování interních informací
    - firemní emailové adresy v diskusních fórech
    - informace o interním fungování organizace
  - sdělení/zaslání chráněné informace na vyžádání
- neověřují si zdroj požadavku
- reagují na emaily z nedůvěryhodných zdrojů
- nechávají „návštěvy“ pohybovat se po prostorách společnosti
- nevšímají si neznámých osob
- nehlásí podezření na bezpečnostní incident

Jak s výsledky testů pracovat

- zaměření se na selhání v systému řízení jako celku (ne jednotlivců)
- využití reálné zkušenosti zaměstnanců při zvyšování bezpečnostního povědomí
- zavedení identifikovaných zjištění do systému řízení rizik a implementace vhodných opatření

SECURITY 2013

21. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Barbora Netolická

ESET, spol. s. r. o.

netolicka@eset.cz