Uvod v informacijsko varnost

Uvod

MURPHY-jev zakon varnosti

- Vsiljivec bo uporabil vsa možna sredstva in poti za vlom.
- Poti in sredstva, ki smo jih predvideli, ne bo uporabil.
- Vedno se najdejo poti in sredstva, ki jih nismo predvideli.

Napadalec je zmeraj v prednosti

OBRAMBA	NAPADALEC
braniti vse točke	izbira najšibkejšega člena
obramba pred znanimi napadi	možnost preizkušnje novih načinov, napadov…
neprestano na preži	napad lahko izvede kadarkoli
upoštevanje pravil	ni pravil – "umazana igra"

Slabo implementirana varnost ☺

Pretnje varnosti

- človek (človeški faktor)
- tehnologija (tehnološki faktor)
- okolje (okoljski faktor)

Dejstva o varnosti

- varovanje informacijskega sistema je le tako dobro, kolikor dober je najšibkejši člen
- varovanje je povezano z omejevanjem dostopa do informacijska sistema
- varovanje upočasnjuje organizacijo
- varovanje zahteva sodelovanje človeških virov
- varovanje povzroča dodatne stroške

Posledice incidenta

- izguba
- prekinitev nudenja storitev
- razkritje informacij
- neuporabnost
- neučinkovitost
- celovitost

Verjetnost

STOPNJA	OPIS	PRIČAKOVANA POGOSTOST
skoraj gotovo	tovrstni dogodki so se zgodili v organizaciji v preteklem letu ali se stalno dogajajo (npr. zlonamerna koda)	enkrat letno ali pogosteje
verjetno	dogodki te vrste se v Sloveniji pojavijo vsako leto (npr. "website defacement")	enkrat na tri leta
možno	dogodek te vrste se je v organizaciji že pojavil; dogodek se je že večkrat pojavil v sloveniji	enkrat na deset let
redko	takšni dogodki so občasni (npr. rušilni potres)	enkrat na trideset let
izredno redko	podobni dogodki so se že pojavili in so teoretično možni (izbruh vulkana)	enkrat na sto ali več let

Obvladovanje tveganj

- izogibanje
  - s spremembo odločilnih faktorjev
- zmanjšanje
  - zmanjšamo verjetnost ali pa posledice (oz. učinek)
- prenos tveganja
  - zavarovanje, pogodbe, partnerji
- sprejemanje tveganja

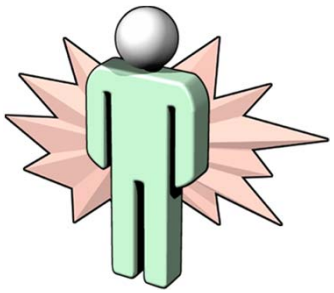
Pretnje

Pretnje

- zaposleni, ki se povezujejo v omrežje podjetja
  - omreženo, brezžično, klicno, VPN
  - PC-ji podjetja, osebni sistemi
- zaposleni, ki se povezujejo v druga omrežja
  - internetne vstopne točke, omrežja partnerjev, širokopasovno
- partnerji, ki se povezujejo v omrežje podjetja
  - lokalno/ federalno overjanje (authentication)
  - anonimni gosti
- novi scenariji in grožnje

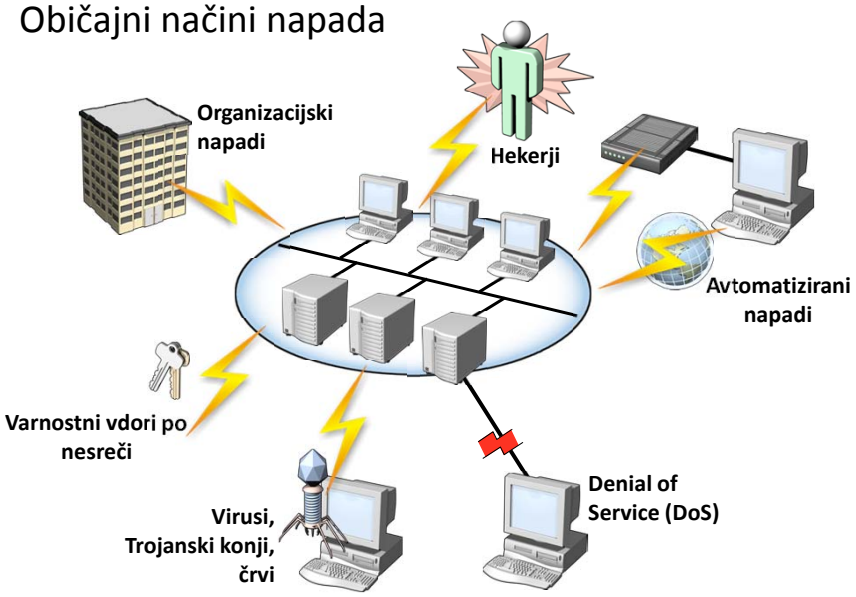
Potencialni napadalci

- Tatovi
- Ogroževalci zaupanja
- Vandali
- Kriminalci
- Hekerji



Ni čudno, da se pojavljajo napadi!

Običajni načini napada



Običajni načini napada

- organizacijski napadi
- zaščiteni podatki
- varnostni vdori po nesreči
- avtomatizirani napadi
- hekerji
- virusi, trojanski konji, črvi
- Denial of Service (DoS)

Cilji in naloge varnosti IKT

Cilji zaščite

- Zaupnost (confidentiality)
  - samo pooblaščene osebe smejo videti zaščitene podatke
- Celovitost (integrity)
  - celovitost pomeni natančnost, točnost, nespremenjenost (spremenjeno s strani pooblaščenega uporabnika s pooblaščenimi procesi in po sprejemljivih poteh), pomenski in pravilni rezultati
    - celovitost podatkov (Data integrity)
    - celovitost vira (Origin integrity)
- Razpoložljivost (availability)
  - pomeni prisotnost objektov ali storitev v uporabni obliki, zadovoljive kapacitete za opravljanje storitve, omejen čas čakanja, zadovoljiv odzivni čas

Naloge varnosti IKT

- Identifikacija (identification):
  kdo smo?
- overjanje (authentication):
  kako vemo, da ste res tisti, za katerega se izdajate?
- avtorizacija (authorization):
  kaj smemo narediti?
- celovitost (integrity):
  smo dobili take podatke, kot ste jih poslali, ali smo prejeli spremenjene?

Naloge varnosti IKT

- zaupnost (confidentiality):
  zagotovo ni nihče prebral podatkov, ki ste jih poslali?
- beleženje (auditing):
  zapisovanje vseh dogodkov za kasnejšo analizo
- zanikanje dejanj (repudiation):
  - pošiljatelj lahko dokaže, da je poslal sporočilo sprejemniku
  - sprejemnik ne more zanikati, da je prejel sporočilo
- Nadzor dostopa:
  Do ima do česa dostop?