

# Slabé miesta v IT systémoch a úloha súkromného sektora

(načrtnutie najpálčivejších problémov)

Rozdelím to

I. slabé miesta v IT systémoch

II. úloha súkromného sektora

## I.

**Slabé miesta sú (resp. môžu byť) všade... potenciál pre ich vznik je pri**

- návrhu systému
  - bezpečnosti sa nevenuje primeraná pozornosť
  - bezpečnosť sa chápe len veľmi zúžene - iba niektoré najviditeľnejšie hrozby
  - bezpečnosť sa chápe ako čosi, čo sa k systému dodatočne "prilepí"
- implementácii systému
  - nevhodne zrealizovaný styk používateľa so systémom (potenciál pre chyby či nedorozumenia pri používaní systému)
  - programátori neovládajú princípy tzv. bezpečného programovania
  - ignorovanie princípov ochrany osobných údajov
- nasadení systému
  - prioritu má funkčnosť systému, nie bezpečnosť (v prípade riešenia nejakého problému bezpečnosť ide do úzadia)
  - existujúce bezpečnostné mechanizmy sa nevhodne nakonfigurujú
- používaní (prevádzke) systému
  - ľudský faktor (chyby, bezstarostnosť obsluhy, druhý extrém - v mene bezpečnosti obmedzovanie možností používateľov, až títo nájdu spôsob ako obísť bezpečnostné opatrenia)
  - úmyselné útoky
  - nedostatočná pripravenosť riešiť mimoriadne situácie

## Prit'azujúce okolnosti

- jeden subjekt (organizácia) si môže zabezpečiť svoje systémy, v súčasnom zosieťovanom svete však potenciálne hrozby môžu prísť zo strany nedostatočne zabezpečených systémov iných subjektov (DDoS útoky, ale hoci aj neúmyselné

vnesenie škodlivého softvéru prostredníctvom cudzieho pamäťového média či notebooku host'a)

- nedostatočná "zrelosť" manažmentu, ale aj zamestnancov (vnímanie bezpečnosti ako čisto technického problému, slabá predstavivosť, resp. znalosť možných hrozieb, hľadanie "alibi" namiesto proaktívneho riešenia, príkazový ("command-based") manažment ľudí, zraniteľnosť voči sociálnemu inžinierstvu)
- niektoré prístupy k riešeniu bezpečnosti môžu byť v konflikte s princípmi ochrany ľudských práv (ochrana súkromia)
- absencia motivácie (bezpečnosť (prípadne ochrana osobných údajov klientov) zatiaľ nieje vnímaná ako konkurenčná výhoda či marketingový prvok, existujúca legislatíva nedostatočná, resp. dá sa plniť iba formálne)
- unifikácia IKT prostredia plus dostupnosť informácií a prostriedkov potrebných pre úspešný útok (Google a vyhľadávani bezpečnostných slabín, cieľov útokov)
- bezpečnosť je pohyblivý cieľ (stále prudký vývoj v IKT i technikách útokov, rastie počet systémov - potenciálnych cieľov útokov)

## II.

- bezpečnostné prostriedky (hardvér i softvér) vďaka globalizácii dostupné
- základné know-how na Internete (avšak problém odfiltrovať relevantné a aktuálne informácie)
- len lokálny prínos (ale chýbajú nám "evanjelisti", čosi ako Matej Hrebenda)
- v niektorých oblastiach ťažko nahrádzať štát - príklad: absencia vhodného vzdelávania pre laikov (spam, podvody nigérijského typu ("advance payment schemes"), orientácia v možných hrozbách, ochrana osobných údajov, nakladanie s heslami,..)
- existuje odborná komunita?
- posúdenie kvality?