IT Security:
Az ember, mint a leggyengébb láncszem

Tanka László tű. ezredes, CIO
BM Országos Katasztrófavédelmi Főigazgatóság

Tapolca, 2016. október 14.

Információs forradalom

Az emberek korlátozott adat befogadóképessége és a hatalmas mennyiségű adat közötti rést az informatikai eszközök és megoldások töltik be, amelyek az adatokból értékelhető információkat kreálnak és tudássá szerveződhetnek.

Informatikai szakterület

Informatikai Biztonság

A **biztonság** alanya:

- **INFORMÁCIÓ**
- **Információs tevékenységet támogató, megvalósító rendszer**
- **Információs szolgáltatás és ezeket biztosító informatikai rendszer**

Adminisztráció

Minősített és nyílt adathordozók kezelése

IBSZ

Emberi tényezők

A biztonsági kockázatok jelentős részét az *emberi tényezők* és a *felhasználói szokások* jelentik.

Gyakori magatartásbeli problémák:

- **Megfelelően tájékozottnak tartja magát a veszélyforrásokkal kapcsolatban (pl.: vírusok)**
- **Megfelelően védettnek érzi magát a vállalati hálózatban (pl.: tűzfalak és szerverek mögött)**
- **Hamis biztonságtudat jellemzi (pl.: ismeretlen tárgyú levél csatolmányának megtekintése, hiszen a kolléga postafiókjából érkezett)**

Gyakori technikai problémák:

- **Munkaállomás operációs rendszerének bejelentkezett állapotban hagyása felügyelet nélkül**
- **Vállalati mobil eszköz külső használata (pl.: eszköz családtagok által történő használata, nem megbízható WiFi használat)**

További problémák

- A felhasználó a vállalati infrastruktúra eszközeire úgy tekint, mint neki járó szolgáltatásra, nehezen fogad el bármilyen korlátozást
- A felhasználó kényelme, ismerethiánya, gondatlansága sok esetben ellentétes az informatikai biztonsággal
- A nem megfelelő jelszavak megkönnyítik a számítógépekbe, rendszerekbe történő illetéktelen bejutást
- A biztonsági események jelentős része belső eredetű, azaz cégen belülről származó információ vagy tudás felhasználásával történik

A naprakész védelmi rendszer sem ér semmit abban az esetben,
ha ***rosszul használják vagy megkerülik***.

További problémák

- **Vállalat mérete -> biztonság**
- **Mentalitás -> bank**
- **Mentalitás -> sárga szalag**
- **A „támadó” -> jelszavak, közösségi oldalak, keresők**

A naprakész védelmi rendszer sem ér semmit abban az esetben, ha *rosszul használják vagy megkerülik*.

Biztonsági rések csökkentése

Biztonsági kockázatok csökkentése felhasználói oldalon:

- **Képzések, oktatások és bemutatók tartása.**
- **Hozzáállás és mentalitás megváltoztatása.**
- **Vállalati kultúra részévé tenni a leginkább beváló, használható biztonsági gyakorlatokat.**

Biztonsági kockázatok csökkentése üzemeltetői oldalon:

- **Házirendek alkalmazása (pl.: jelszóbiztonság).**
- **Alkalmazások meglétének ellenőrzése (pl.: vírusvédelem)**
- **Üzemeltetői képzések.**
- **Védelmi rendszerek beszerzése és azok naprakészen tartása.**

Célpont: a leggyengébb láncszem

Tanácsok:

- **Jelszavainkat jegyezzük meg**
- **Használjunk más-más jelszót a különböző felületeken**
- **Rendszeresen változtassuk jelszavainkat**
- **Figyeljünk, mit adunk meg egy regisztrációnál**
- **Ne nyissunk meg olyan tartalmakat, melyek már ránézésre nem megbízhatóak (pl.: ismeretlen feladótól levél, nem megszokott kinézetű honlap)**

Köszönöm a figyelmet!

„Ne hagyjuk a pénztárcánkat az autó tetején, mert a végén valaki elviszi…”