Hálózati és végponti biztonság

Siket Csaba

IT Biztonság - CISO

Budapest, 2018. március 7.

Helping people achieve a lifetime of financial security

AEGON
Transform Tomorrow

2018. május 25.

1 Miért fontos számunkra a GDPR?

Nem ismeretlenek az adatvédelmi előírások, de új szempontok, és szigorúbb definíciók, nagyobb büntetési tételek! (maximum **20 millió euró vagy az előző év árbevételének 4 %-a.)**

Új szerződéses feltételek az adatkezelők, adatfeldolgozók számára! (ügynökségek, ügynökök, alkuszok – biztosítók)

2 Mit kell megtennünk a megfeleléshez?

A GDPR előírja **az informatikai rendszer önvédelmét**, az adatok biztonságos környezetének biztosítását.

Mit is jelent ez? Hogyan érhető ez el?

AEGON
Transform Tomorrow

Biztonságos informatikai környezet

Hogyan védjük meg ügyfeleink adatait ?

- Hálózati és végpont biztonság
- Biztonságos adattovábbítás
- Sérülékenység menedzsment

Adatokat érintő incidens esetén az biztosító haladéktalan értesítése!

Incidens: az adatok jogosulatlan vagy jogellenes kezelése, véletlen elvesztése, megsemmisítése vagy károsodása.

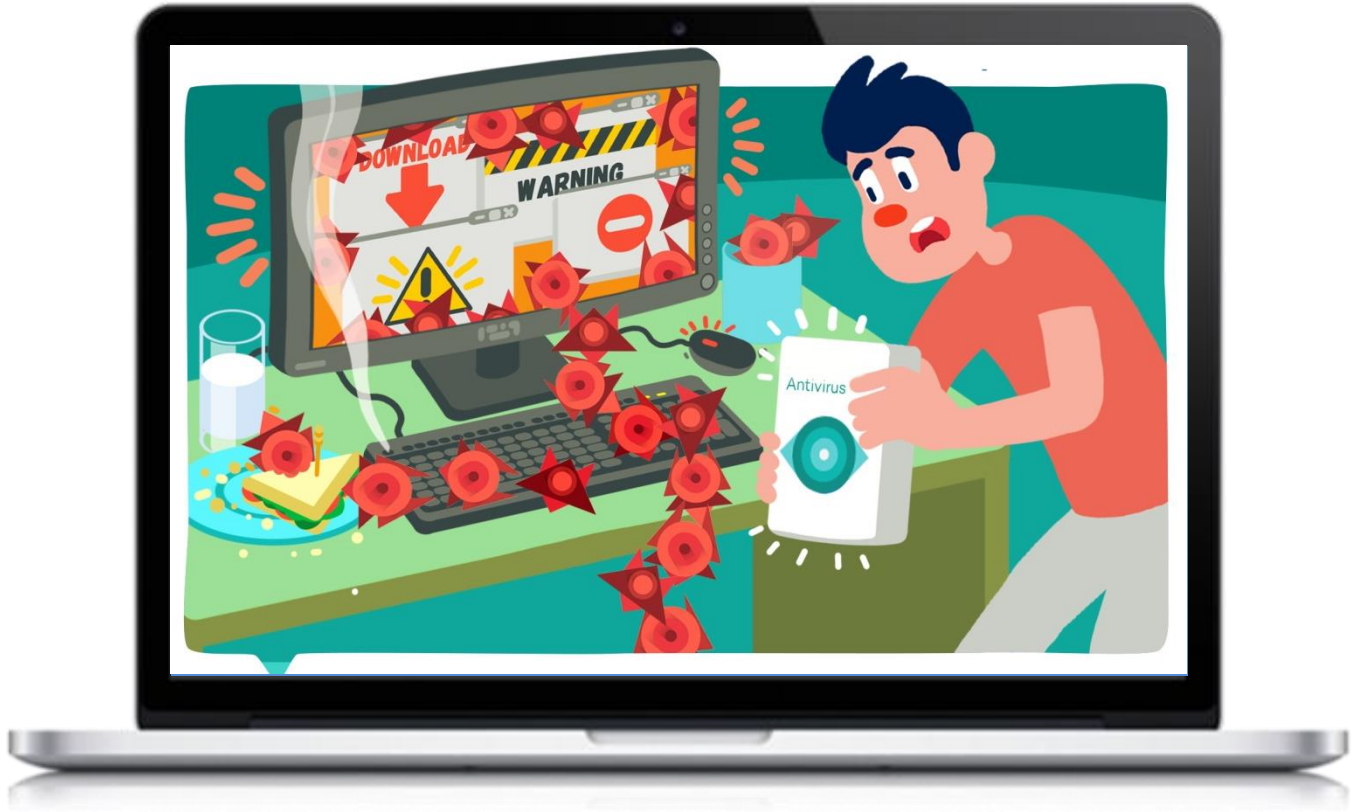
AEGON
Transform Tomorrow

I . Hálózati és végponti biztonság

Feladat:

- Hozzáférés védelem
- Tűzfal, IDS használata
- Vírus védelem és
- Merevlemez titkosítás használata

Fontos a jogtiszta szoftverek használata!



AEGON
Transform Tomorrow

Hozzáférés- vírusvédelem, titkosítás

Megoldás:

Felhasználói fiók – komplex jelszó használata

Vírusirtók által szolgáltatott végpontvédelem, önálló merevlemez titkosítással.

- Ajánlott vírusirtó szoftverek:
  - Windows Security Essential Win7
  - Későbbi Windows verziók – Defender
  - Symantec Endpoint Protection
- Ajánlott merevlemez titkosító szoftver:
  - Bitlocker
  - Pl. Symantec Encryption

Merevlemez titkosítása notebooknál

- Kínos és fájó elhagyni egy USB kulcsot a buszon, de az sem kellemes, amikor a védelem nélküli notebookunkat lopják el. Az adatok innentől bárkinél landolhatnak.
- A levédetlen Windowst nem olyan nehéz feltörni és máris megkapja a tolvaj a jelszavainkat, belépőkódjainkat - egyszerűen MINDENT.
- A meghajtó-titkosítás lényege, hogy a teljes meghajtót titkosítja egyes fájlok helyett. A kódolást használva a fájlok már eleve titkosított állapotban tárolódnak, ezekből csak azon a számítógépen tudjuk visszafejteni a tartalmakat, amelyen a védelmet aktiváltuk.
- A tárolt adat gépek számára csupán egy használhatatlan adathalmazt mutat.

II. Biztonságos (titkosított) adat továbbítás

Az email nem titkos! Hozzáértő emberek képesek elfogni, akár módosítani és úgy továbbítani az e-mail-eket.

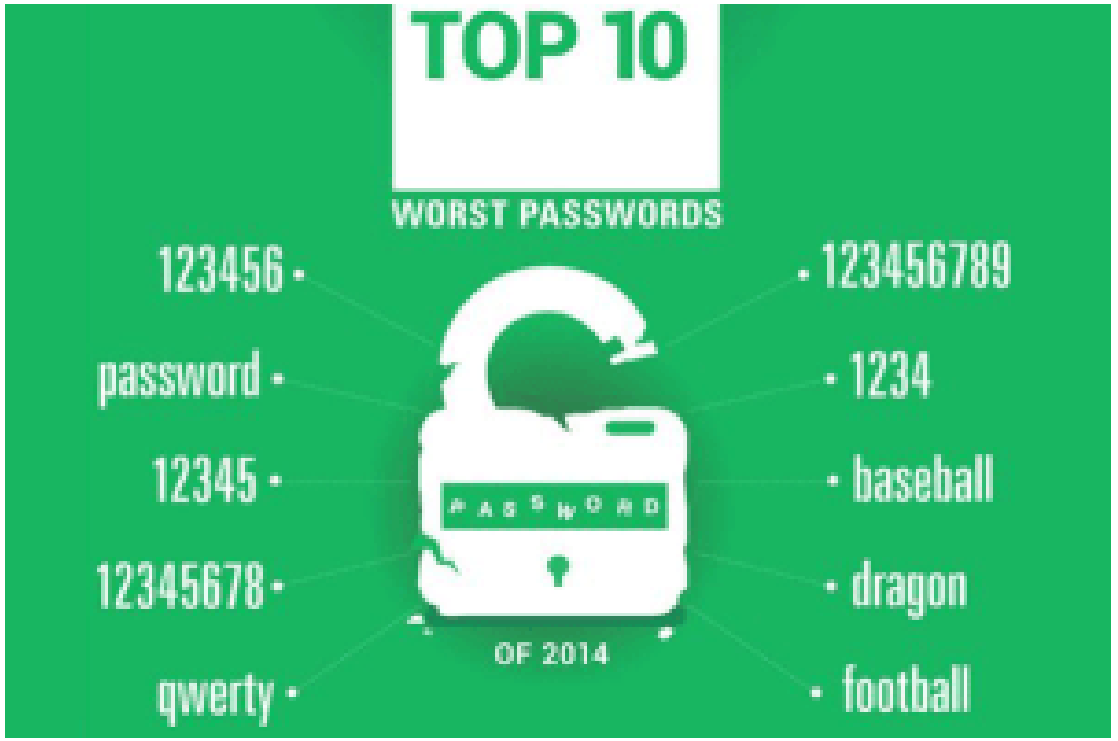
- Az érzékeny adatok titkosítása továbbküldés esetén.
- Amennyiben szenzitív, személyes információkat, (ügyfél-, szerződésadat stb.) adatokat tartalmazó (excel, word pdf. stb.) dokumentumot szeretnél küldeni email-en keresztül, azt jelszóval ellátva, titkosítva kell megtenni!

II. Biztonságos (titkosított) adat továbbítás

Megoldás

- Az excel, word képes jelszavas védelmet biztosítani, egyéb dokumentum esetén javasolt tömöríteni és ott jelszót beállítani.
- **Fontos!** A jelszót ne írjuk bele az emailbe!
- Ajánlott tömörítő szoftver: 7Zip

A 7Zip program és a felhasználói útmutató megtalálható a **download.aegon.hu** letöltő oldalon.



III. Sérülékenység menedzsment

Feladat

- Szoftvergyártók által publikált biztonsági javítócsomagok telepítése az asztali gépen/notebookon (legalább havonta).
- A vírus adatbázisok frissítése naponta, valamint vírus és kártékony program keresés futtatása (legalább hetente).

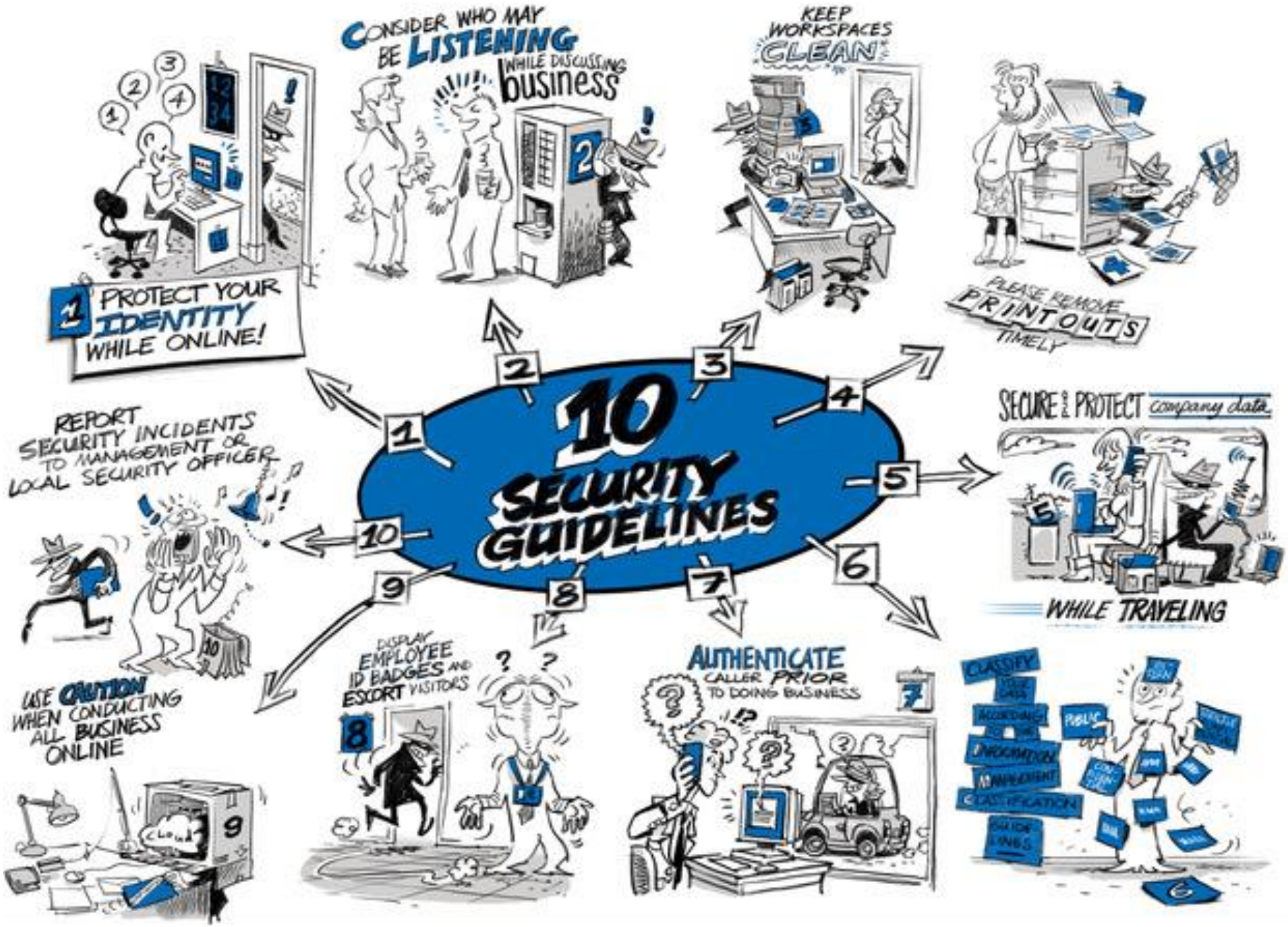
III. Sérülékenység menedzsment

Megoldás

A Windows operációs rendszerek esetén, a Microsoft minden hónap második keddjén adja ki a letölthető frissítéseket.

A frissítéseket (Windows 7 esetén) a Vezérlőpult – Windows update menüpont alatt lehet ellenőrizni, szükség esetén letölteni.

A vírusirtó alkalmazással, ütemezni lehet a gyanús, kártékony programok, fájlok heti keresését, ellenőrzését.



AEGON
Transform Tomorrow

Köszönöm a figyelmet !