Ügyviteli (információ)védelem

Andrikó Imre

Nyíregyházi Egyetem – Gazdasági Igazgatóság – Informatikai Szolgáltató Iroda

- Otthoni számítógépeket is óvjuk a veszélyforrásoktól
- Kis szervezeteknél szabályok szóbeli ismertetése
- Nagy vállalatoknál írásba foglalva a szabályok
- Az ügyviteli védelem az informatikai rendszert üzemeltető szervezet ügymenetébe épített védelmi intézkedések, biztonsági szabályok, tevékenységi formák együttese.
- Szintjei: a stratégiai, tervezési szintet (IBK: Informatikai Biztonsági Koncepció) és a mindennapi gyakorlatot érintő és szabályozó szintet (IBSZ: Informatikai Biztonsági Szabályzat)
- Néha kényelmetlen a szabályozás, de biztonságot nyújt
- A legkörültekintőbb szabályozás sem lehet eredményes

  a dolgozók együttműködése nélkül.

Védelmi intézkedések: mindenre kiterjedően

1. Infrastruktúra
2. Felhasználói jogok kezelése
3. Szoftver
4. Adathordozó
5. Dokumentum
6. Adatok
7. Hálózati védelem

1. Infrastruktúra

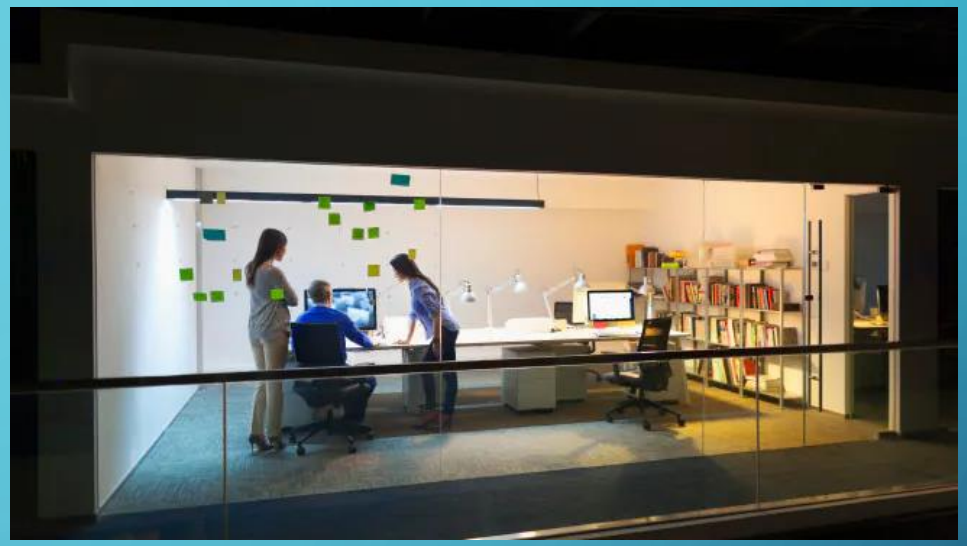
- Elhelyezése, fizikai veszélyforrásokkal szembeni védelem
- Az eszközök be és ki vitele
- Nem a vállalat tulajdonában lévő eszk.
- Hibaelhárítás felelősei és módja
- Selejtezések módja

Adatok törlése: Azokat az adathordozókat, amelyeken érzékeny adatokat tároltak nem ajánlatos törlés után tovább adni, hanem ellenőrzött módon meg kell semmisíteni.

2. Felhasználói jogok kezelése

Ajánlatos különválasztani a jogok kiosztásáért felelős és azt technikailag végrehajtó személyeket.

(adatgazda, rendszergazda)



- *<u>Felhasználó felvétele</u>*

  Az illetékes szervezet vezetője kezdeményezi az informatikai szolgáltatásért felelős egység felé, amely végrehajtja a szükséges lépéseket.

  A felhasználót tájékoztatni kell az informatikai rendszer használatának szabályairól.

- *Felhasználói jogok módosítása*

  Ezt általában a felhasználási jogot biztosító eljárási szabályok megtartása mellett, az érdekelt adatgazda igényelheti az informatikai szervezettől.

  (szabadság, helyettesítés, elfelejtett jelszó, elvesztett vagy megsemmisült azonosítók)

- *Felhasználó törlése*

  Az adott szervezet munkaügyi és személyi ügyeit intéző, nyilvántartásokat vezető szervezetének értesítése mellett az adatgazda kezdeményezheti.

  Tilos a felhasználó törlése addig, míg kezelésében adatok vannak.

- *Hozzáférési rendszer naplózási követelményei*

  A felhasználói akciókat (bejelentkezéseket, kijelentkezéseket és szerepkör váltást; a felhasználói azonosító és jogosultság módosításával, cseréjével kapcsolatos tevékenységeket) naplózni kell.

  Tilos a felhasználói jelszavak naplózása.

3. Szoftver

- A vállalatok által használt szoftverek beszerzéséről és telepítéséről általában az informatikáért felelős egység gondoskodik.
- A számítógépre történő szoftvertelepítést csak az adott alkalmazás rendszergazdája, vezetői utasításra végezheti el.
- Felhasználó a munkahelyi számítógépére más szoftvert sose tegyen fel.
- A vállalatnál használatos minden programról biztonsági másolatot, illetve munkamásolatot kell készíteni.
- Aki munkavégzése során számítógépet használ vagy üzemeltet, felelős azért, valamint köteles meggyőződni arról, hogy a számítógépen csak jogtiszta szoftver legyen.
- Internetről letöltött, szabad szoftver használata, a műveletet elvégző dolgozó felelőssége.

4. Adathordozók

- A vállalat tulajdonában lévő adathordozókat nem szabad személyes célokra használni, és saját adathordozót sem ajánlatos a munkahelyi számítógéppel kapcsolatba hozni.
- A dolgozók felelőssége a gondjaikra bízott adathordozók fizikai védelme.
- Minősített adatokat csak nyilvántartott adathordozóra szabad felvinni. Az adathordozót tilos felügyelet nélkül nyílt helyen tárolni, vagy akár rövidebb időre ott hagyni.
- Sérült vagy hibás adathordozókat újra felhasználni szigorúan tilos.
- Használaton kívül minden esetben zárjuk el egy biztonságos szekrénybe
- A leselejtezett adathordozókat fizikailag meg kell semmisíteni.

5. Dokumentum

- A számítógépen lévő dokumentumok védelmére a hardver és szoftver eszközökre vonatkozó eljárások vonatkoznak.
- A dokumentumok adatok is, melyekre adatként is kell vigyázni.

- Az informatikai rendszer biztonságának meghatározó tényezője az események visszakövethetősége. Minden olyan eseményt, amelyik eltér a megszokott üzemviteltől, pontosan naplózni kell. A naplónak tartalmaznia kell az esemény pontos leírását.

6. Adatok

- *Hozzáférés-védelem*: A számítógépeken levő adatok védelme érdekében, a számítógépes védelmi rendszerek megfelelő alkalmazása minden felhasználó alapvető kötelessége.
- Az adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal - legalább felhasználói névvel és jelszóval - lehet hozzáférni.
- Hálózati erőforrásokhoz csak érvényes felhasználói névvel és jelszóval lehet hozzáférni.
- Fokozott, illetve kiemelt védelmi kategóriába sorolt munkahelyeken speciális azonosító-, jogosultságigazoló eszközöket alkalmazzunk.

  pl: elektronikus személyi igazolvány

7. Hálózati védelem

- A szervezet belső hálózatának és központi levelező szerverének üzemeltetése valamint a világhálóra való csatlakoztatás a központi informatikai egység feladata.
- Az interneten keresztül érkező káros programok és kéretlen levelek szűrése
- A belső elektronikus levelezés szabályai

  A szabályozás során abból kell kiindulni, hogy az elektronikus levelezési cím és a hozzá tartozó elektronikus levelesláda a vállalat tulajdona

Felelősség és ellenőrzés

- Nem elegendő leírni a védelmi intézkedéseket, hanem a végrehajtásukhoz felelősöket is meg kell nevezni.
- A felelős joga és kötelessége, hogy rendszeresen ellenőrizze az előírások betartását. Figyelmeztesse a felhasználókat a védelmi intézkedések betartására, szükség esetén pedig fegyelmi felelősségre vonást is kezdeményezhet.
- Az általa észlelt vagy tudomására jutott veszélyhelyzetnek a méretétől, várható következményeitől függően a megfelelő ideiglenes védekező lépéseket meghozza.
- Minden felhasználónak kötelessége, hogy ha betörésgyanús esetet észlel, ezt azonnal jelentse a vállalat biztonsági csoportjának

Köszönöm a figyelmet!

Andrikó Imre

andriko.imre@nye.hu