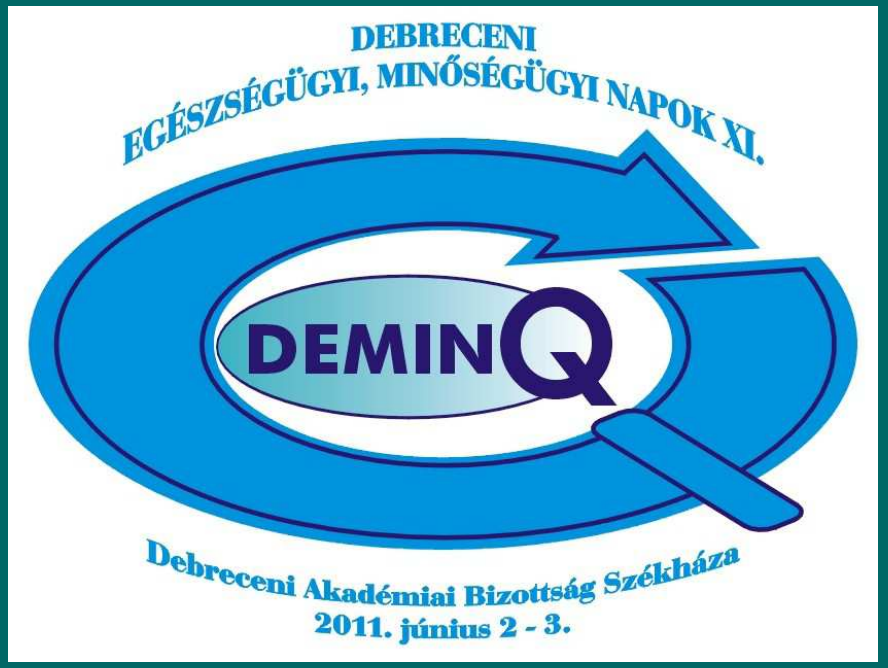
Az információbiztonság megjelenése az egészségügyi szolgáltató szervezetek minőségirányítási rendszerében



INFOBIZ

Működési kérdések az információbiztonság szemszögéből

- Tisztában vagyunk az információbiztonság kapcsán felmerülő működési kockázatokkal és megfelelően foglalkoztunk velük?
- A betegek által rendelkezésre bocsátott adatokat / információkat megfelelően kezeljük és védjük a szervezetünkön belül?
- Valóban bizalmasan kezeljük / kezelik az alkalmazottak az információkat az intézményen belül ÉS kívül?
- Biztosítva vagyunk az információink sértetlenségéről?
- Pontos és ellenőrzött információkkal dolgozunk?
- Tényleg csak azok és csak akkor férhetnek hozzá az információkhoz, akik erre jogosultsággal rendelkeznek?
- Nyugodtak vagyunk az információk folyamatos rendelkezésre állását illetően?
- Felkészültünk az esetleges adatvesztések esetén a megfelelő visszaállításukra?

Jogszabályi háttér

- 1992. évi LXIII. **törvény a személyes adatok védelméről** és a közérdekű adatok nyilvánosságáról
- 1997. CLIV **törvény az egészségügyről**
- 1997. XLVII **törvény az egészségügyi és hozzájuk kapcsolódó személyes adatok** kezeléséről és védelméről
- 2001. évi CVIII. **törvény** az elektronikus kereskedelmi szolgáltatások, valamint **az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről**
- 2080/2008. (VI. 30.) **kormányhatározat a Kritikus Infrastruktúra Védelem** Nemzeti Programjáról

Adatvédelem – miről is beszélünk?

- **Milyen adatokat kell védeni?**
  - **betegek** egészségügyi és személyes adatait
  - **egészségügyi dolgozók**, beszállítók, stb. adatait
  - **gyógyszerek, vizsgálati eszközök és eljárások**, stb. adatait
  - **minőségirányítási dokumentációt** és gyűjtött indikátorokat
  - **kórházi gazdasági / finanszírozási / ügyviteli** adatokat
- **Kitől – mitől?**
  - **Adatszivárgástól** – jogosulatlanok hozzáférése az adatokhoz
  - **Adatok hibás felhasználásától** – hibás információk a gyógyításban, menedzsmentben
  - **„Nem az előírt célnak megfelelő" adatkezeléstől** – adatok illetéktelen célú felhasználása (gyógyszercégek piaci versenyelőnyéhez)
  - **Adatok rendelkezésre állásának hiányától** – üzemszünet az informatikai rendszerben

Példák, veszélyek - betegadatokra

- **Adatszivárgás**:
  - illetékteleneknek (szándékosan vagy véletlenül) kiadott betegadatok, majd azokkal való visszaélés
- **Hibás felhasználás**:
  - „elnézett, vagy elcserélt vizsgálati eredmények (vagy kórlapok) alapján döntés a kezelésről
  - gondatlanul rögzített adatok alapján készült betegdokumentáció
  - gondatlanul rögzített vagy szándékosan „kozmetikázott” adatok alapján készült finanszírozási adatszolgáltatás
- **„Nem az előírt célú” felhasználás**:
  - Szakdolgozatokban, tudományos munkákban nem megfelelően kezelt adatok közzététele
- **Adatok rendelkezésre állásának hiánya**:
  - Diagnosztikához, beavatkozáshoz, gyógyításhoz nem, vagy késve (vagy hibásan) állnak rendelkezésre a szükséges információk

Információvédelem egyes témakörei a minőségirányításban

- *4.2.3. A dokumentumok kezelése*
- *4.2.4. A feljegyzések kezelése*
- *5.5.3. Belső kommunikáció*
- *6.3. Infrastruktúra*
- *7. A termék előállítása*
- *7.2. Ügyféllel kapcsolatos folyamatok*
- *7.5.1 A termék-előállítás és a szolgáltatás-nyújtás szabályozása; c) a megfelelő berendezések használata*
- *7.5.4 A vevő tulajdona*
- *8.4. Az adatok elemzése*
- *MEES értelmezhető standardjai, pl.:*

  MEES 1.0 - BTA.7. standard. A betegek egészségügyi és hozzájuk kapcsolódó személyes adatait a hatályos jogszabályi előírásoknak megfelelően bizalmasan kezelik és elvesztés vagy illetéktelen használat ellen védenek.

Az információ biztonsága

Információ = *(számomra értelmes)* **tartalommal bíró adat**

Információhordozó – ezen keresztül létezik az információ, és ezen keresztül sérülhet a biztonsága is!

Információ biztonsága =

- Az információ rendelkezésre állása
- Az információ sértetlensége
- Az információ bizalmassága

Adathordozók, információhordozók fajtái

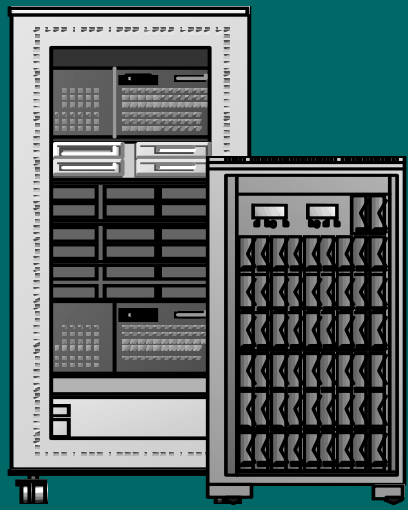
Adatok – adathordozók

Adatok védelme / biztonsága
→ az adathordozókon keresztül

- **IT alapú adathordozók biztonsága**
  (informatikai rendszer biztonsága – üzemeltetésben, felhasználók kezelésében, …)
- **Papír (és hagyományos) adathordozók biztonsága**
  (adminisztrációs folyamatok, iratkezelés és tárolás, TÜK, …)
- **Személyek, mint adathordozók biztonsága**
  (social engineering, emberi tényező, szándékos és szándékolatlan esetek, …)

Informatika: Hol is van adat?

- **Szervereken** – adatbázisban
- **Szervereken** – önálló fájlok könyvtár-struktúrákban
- **PC-ken / Notebookokon** (akár hálózathoz kapcsolt munkaállomás, akár önálló gép)
- **Diagnosztikai berendezések, műszerek** memóriájában / adathordozóin
- Kimentve (egyénileg) **külső elektronikus adathordozókon** (CD / DVD / DAT / Floppy / USB Flash / …)
- **Központi mentésekben, archív állományokban**, … (backup site-ok, stb…)



Informatika: Adatszivárgás – hol lehet?

- **Hogyan lehet hozzáférni az adatokhoz?**

  Illetéktelen …

  - … bejutás a szerverterembe
  - … hozzáférés a számítógépekhez / notebookokhoz
  - … hozzáférés a mentésekhez
  - … hozzáférés a külső / mobil adathordozókhoz
  - … bejutás az interneten / külső hálózaton át (hacking, virus, spyware, maleware, trojan, spam, hoax, …)
  - … hozzáférés a WiFi-hez

Adatszivárgás – hol lehet … még?

- **Hogyan lehet hozzáférni az adatokhoz?**

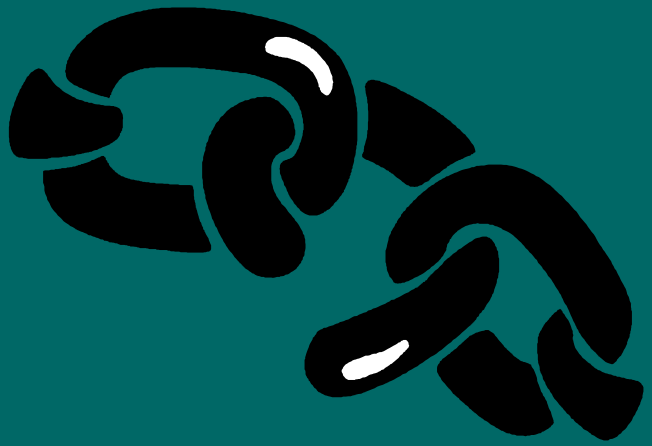
  Illetéktelen … hozzáférés / felhasználás „illetékes” által!

Belső ember (kórházi dolgozó) kiadja:

- … mert nem tudja, hogy nem lehet
- … mert megtévesztették, azt hitte ki kell adnia
- … mert megfenyegették / megzsarolták
- … bosszúból (mert sértettnek érzi magát!)
- … csak hogy megmutassa, hogy milyen rossz a rendszer … stb …

Védekezés kiépítése

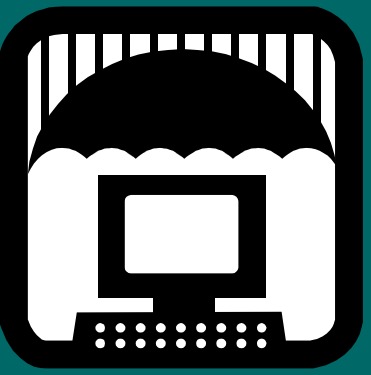
Mindenütt testre szabottan!



Minden biztonsági rendszer olyan „erős”, mint a leggyengébb eleme!

- Egyenszilárdságú védelem
- Kockázattal arányos védelem

Az információvédelmi eljárások szakmai területei



- **objektum, terület védelem,**
- **személy védelem** (rendszerben a személy védelme, vagy a rendszer védelme személyektől),
- **Hagyományos adatok** (pl. papíralapú), **módszerek, eszközök védelme,**
- **informatikai védelem,** (fizikai, logikai és szervezési)
- **elemi károk, természeti csapások elleni védelem** (az információbiztonság szemszögéből).

Az INFOBIZ Kft. programja lépésről-lépésre

- **1. lépés: Önértékelő kérdőíves felmérés** *… és a kapcsolódó intézkedési javaslatok a statisztikailag feltárt problémák pótlására*
- **2. lépés: Szakértői informatikai és információbiztonsági kezdeti állapotfelmérés** *… és a kapcsolódó intézkedési javaslatok a feltárt gyenge pontok, problémák javítására*
- **3. lépés: Adatvagyon, információs vagyon és fenyegetettségeinek, kockázatainak felmérése** *… és a kapcsolódó intézkedési javaslatok az el nem fogadható kockázatok kezelésére*
- **4. lépés: Folyamatos kockázatkezelésen alapuló biztonsági intézkedések beemelése az irányítási rendszerbe**
  *(→ integrált irányítási rendszer ezzel tartalmazza az **információbiztonsági irányítási rendszer**t is)*

Köszönöm megtisztelő figyelmüket!

Dr. Horváth Zsolt
horvathzs@infobiz.hu
http://www.infobiz.hu

Dr. Tóth Zoltán
tothz@infobiz.hu
http://www.infobiz.hu