Belügyminisztérium
Nemzeti Biztonsági Felügyelet

Minősített adatot elektronikusan kezelő rendszerek biztonsági aspektusai

Pintér Diána
elektronikus biztonsági főreferens

Tartalom

- Jogszabályi háttér
- Kialakítás előtt tisztázandó kérdések
- Mit kell biztosítani?
- Módszer
- Komplex terület
- Fizikai védelem
- Személyi feltételek
- Adminisztratív biztonsági eljárások
- Számítástechnikai (elektronikus) védelem
- TEMPEST
- Rejtjelzés
- Rendszerengedély

Jogszabályi háttér

- **2009. évi CLV. törvény** a minősített adat védelméről **(Mavtv.)**
- **2004. évi CXL. tv.** A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól **(Ket.)**
- **2013. évi L. tv.** az állami és önkormányzati szervek elektronikus információbiztonságáról **(Ibtv.)**
- **NATO: CM(2002)49 -** új Primary Directives
- **EU Tanács 264/2001/EC** és kapcsolódó dokumentumok

Jogszabályi háttér

A Mavtv. végrehajtási rendeletei:

- **90/2010. (III. 26.) Korm. rendelet** az NBF működésének, valamint a minősített adat kezelésének rendjéről
- **92/2010. (III. 31.) Korm. rendelet** az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól
- **161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól**

A kialakítás előtt tisztázandó

- ✓ már meglévő helyszínen folyik majd az adatkezelés, vagy az objektum újonnan kerül kialakításra (megépítésre)
- ✓ papír alapon kívánnak minősített adatot kezelni vagy elektronikus úton is
- ✓ kezelni kívánt **adatkör(ök**) - nemzeti, NATO, EU -
  - ✓ és minősítési **szintek** - KT, B, T, SZT
- ✓ beérkező/keletkező minősített adat várható mennyisége
- ✓ a helyszín és a szervezet veszélyeztetettségi szintje
- ✓ Elektronikus adatkezelés esetén:
  - csak **önálló** munkaállomás(ok) **vagy hálózat**ot építenek,
  - ha a minősítési szint meghaladja a KT-t, akkor a **TEMPEST** követelmények betartása is szükséges.

Mit kell biztosítani?

- Bizalmasság
  - Illetéktelen hozzáférés megakadályozása(zárt körben marad)
  - Jogosulatlan használat megakadályozása (nincs visszaélés)
- Sértetlenség
  - Illetéktelen módosítás (hiteles marad)
  - Jogosulatlan törlés megakadályozása (adat nem vész el)
- Rendelkezésre állás
  - A követelményeknek megfelelően (7/24, 99%...)
  - Jogosult számára az elérhetőség biztosítása (neki viszont legyen elérhető, mert kell a munkához)
- Azonosíthatóság (személy, eszköz, szolgáltatás)

Módszer

- Megelőzés, elrettentés (admin. eszközök)
  - Feliratok, figyelmeztetés, fenyegetés
  - Szabályzatok, nyilatkozatok, tudomásul vétel
  - Felhasználói tudatosság
- Védelem (HW-, SW-biztonság, hozzáférés, stb.)
  - Fizikai korlátok, jelszó, jogosultság, elkülönítés, naplózás
- Helyreállítás (mentések)
  - Adatok, rendszerfájlok, naplók máshol tárolása
  - Visszakereshetőség, személyhez kötés

Komplex terület

Az informatikai rendszerek biztonsága – a Mavtv. értelmében – az érintett rendszereken az alábbi biztonsági területek összességét jelenti:

- Fizikai-
- Személyi-
- Adminisztratív- és
- Számítástechnikai (hardver-szoftver) biztonság
- Kisugárzás-védelem (TEMPEST)
- Rejtjelzés

Fizikai biztonság

A fizikai védelem az alábbi biztonsági elemek együttesét foglalja magában:

- falazat, biztonsági ajtó, zárak, rácsozatok
- biztonsági tárolók (páncélszekrény)
- elektronikus jelző-, riasztó-, és beléptető rendszerek, távfelügyeleti megoldások
- megfigyelő rendszerek (zártláncú videó)
- élőerős őrzés (személyi felügyelet, biztonsági őrség, fegyveres őrség)

A kockázati besorolástól függően vannak kötelezően létesítendő és választható fizikai biztonsági elemek. A megfelelés - a 90/2010. (III. 26.) Korm. rend. mellékletét képező - pontozási tábla alapján dönthető el.

Fizikai biztonság

„Korlátozott terjesztésű!” nemzeti, külföldi minősítéssel és jelöléssel ellátott adatot kezelő rendszert ADMINISZTRATÍV ZÓNÁBAN is lehet telepíteni.

„Bizalmas” vagy magasabb minősítési szintű adatot kezelő rendszert I. vagy II. osztályú BIZTONSÁGI TERÜLETEN kell telepíteni. Ekkor a **rendszerengedély kiadásának feltétele** a - legalább az elektronikusan kezelni kívánt adat minősítési szintjének megfelelő szintű - **adatkezelési engedély** megléte.

Személyi biztonság

A szervezet állományába tartozó munkatársak közül ki kell nevezni:

- Biztonsági vezető
- Rendszerbiztonsági felügyelő (RBF)
- Rendszeradminisztrátor (RA - esetében ajánlott az informatikus képzettség)

RBF és RA kijelölése hivatalosan: munkaköri leírásban/ÜBSZ-ben

+

Felhasználók kijelölése, felkészítése, nyilatkozat az ÜBSZ-ben foglaltak tudomásulvételéről.

A biztonsági személyeknek és a felhasználóknak is rendelkezniük kell:

- kockázatmentes nemzetbiztonsági ellenőrzéssel,
- személyi biztonsági tanúsítvánnyal,
- felhasználói engedéllyel,
- titoktartási nyilatkozattal.

Adminisztratív biztonsági eljárások

- nyilvántartások vezetése (főnyilvántartó-, iktatókönyv, belső átadóokmány)
- üzemeltetés-biztonsági szabályzat (ÜBSZ) és rendszerbiztonsági követelmények (RBK) kidolgozása
- Rendszerdokumentáció (pl. nyomtatási, ellenőrzési napló, stb.) és nyomtatványok (hozzáférés jogosultság igénylő lap, biztonsági esemény jelentés, stb.) elkészítése
- rendszerszintű jelszavak, biztonsági másolatok, op. rendszer lemezek, naplófájlok elkülönített tárolása
- hardver- és szoftverlista
- ellenőrzött, követhető nyomtatás
- adathordozók nyilvántartása, kísérőlap
- jogosulatlan belépők nyilvántartása

Számítástechnikai (elektronikus) biztonság

A számítástechnikai védelem az alábbi biztonsági elemek együttesét jelenti:

- Hardveres védelmi megoldások
- Szoftveres védelmi megoldások
- Minősített adatot továbbító hálózat védett kialakítása
- Kompromittáló kisugárzás elleni védelem kiépítése
- Rejtjelző eszközök alkalmazása a minősített adatok megbízható védelmére

Hardver, szoftver

Hardver:

- kivehető merevlemez, amely munkaidőn kívül, illetve személyes felügyelet végeztével elzárandó (vagy laptop, amely elzárható),
- eszközök felbontás elleni védelme, minősítés szerinti felcímkézése
- naprakész hardverlista

Szoftver:

- engedélyezett, jogtiszta, gyártói támogatással rendelkező op. rendszer és felhasználói programok
- alkalmazások korlátozása: munkához szükséges, tanúsított, ajánlott (konzultáció NBF-el)
- az NBF által megkövetelt BIOS beállítások (jelszóvédelem, a jóváhagyott konfigurációban nem engedélyezett kimeneti portok letiltása, primary HDD boot, stb)
- biztonsági házirend (figyelmeztető üzenet, lomtár kikapcsolása, vendég letiltása, stb.)

Hardver, szoftver

- felhasználók elkülönített kezelése
- naprakész szoftverlista
- op. rendszer naplózási követelmények (pl. felhasználói belépések, belépési kísérletek, a rendszer dátum és idő módosítása, rendszer erőforrásokhoz történő sikertelen hozzáférési kísérletek, stb.)
- jelszóházirend
- aktív, jogtiszta vírusvédelem, vírusdefiníciós adatbázis rendszeres frissítése

A biztonsági beállításokat minden részletre kiterjedően tartalmazza egy beállító csomag, amelyet az akkreditációra való felkészülés során az NBF E-biztonsági Osztály munkatársai rendelkezésre bocsájtanak.

Kompromittáló kisugárzás elleni védelem

- „Bizalmas” és azt meghaladó min. adatok kezelése esetén követelmény
- A **kompromittáló kisugárzás elleni védelem** az elektromágneses kisugárzás és fémes vezetés útján előforduló adatszivárgást előzi meg
- Intézkedések pl.: elektromos kábelek (védett/nyílt) vonalvezetése, rádiófrekvenciás szűrők alkalmazása, rendszer környezetében alkalmazható berendezések korlátozása, telepítési távolságok tartása, elektromágneses árnyékolástechnikai megoldások, csökkentett kisugárzású hardver eszközök alkalmazása (TEMPEST), a rendszerhez tartozó fém berendezések földelése, stb.

A TEMPEST minősítés a hardver elemek különleges árnyékolási jellemzőit jelenti (Level A, B, C), ezt tanúsítvánnyal igazolják.

- Ha a helyszín kialakítása még nem történt meg, azt ajánlott a TEMPEST követelmények teljesülése érdekében körültekintően megválasztani.
- TEMPEST-zóna mérés kérhető az NBF-től.

Rejtjelzés

Rejtjelzés alkalmazására nincs szükség, ha *önálló munkaállomásokon* történik a minősített adat feldolgozása, és az adatot elektronikusan *nem továbbítják*.

Minősített adat elektronikusan továbbítható a nyílt informatikai átviteli utakon (pl. internet vagy szervezetek saját hálózatai) **HA azt rejtjelző eszközzel rejtjelezték.**

A címzettnek hasonló képességre van szüksége a küldemények visszafejtésére.

A minősített adat védelmére **csak az NBF által, a megfelelő szintű védelemre rendszeresített** rejtjelző eszköz használható.

A védett rendszer felhasználója nem végez rejtjelzést, a feladatra **rejtjelzőt kell kinevezni** és az adott eszköz kezelésére tanfolyamon kiképezni.

Rendszerengedély

- A Felügyelet a minősített adatot kezelő informatikai rendszer üzemeltetését **rendszerengedély kiadásával** hagyja jóvá.
- Az engedély kiadásának eljárását az adatkezelő szerv kezdeményezi, ha az üzemeltetés valamennyi feltételét megvalósították, a dokumentáció hiánytalan, a rendszer üzemkész, de minősített adat ekkor még nem lehet rajta.
- Az engedély kérelem, kérdőív és a csatolt útmutató a www.nbf.hu honlapról letölthetők.

- A rendszeren az elektronikus biztonsági jellemzőket érintő változtatásokhoz az NBF előzetes jóváhagyása szükséges. A dokumentációban a változtatásokat át kell vezetni.
- Az adatbiztonság veszélyeztetése esetén a Felügyelet jogosult felhívni a biztonsági vezetőt intézkedések megtételére, vagy intézkedhet a kiadott engedély korlátozására, felfüggesztésére, visszavonására.

Eljárásrend

- Ket. - hatósági eljárás
- **KÉRDŐÍV** kitöltése, aláírása, beküldés --> **ELJÁRÁS indul** (a szükséges feltételek teljesülését az NBF ellenőrizheti, SZT adatkezelés esetén kötelezően ellenőrzi)
- **Végzést kapnak** (8 nap)
  - Érdemi vizsgálat nélküli elutasítás
  - Hiánypótlás elrendelése határidő megszabásával
  - Eljárási határidő meghosszabbítása
  - Eljárás megszüntetése
- **Határozatot kapnak** (21 nap)
  - Kérelem elutasítása
  - Rendszerengedély kiadása (max. 3 év), visszavonása
  - Módosítás, korlátozások

Köszönöm a figyelmet!