

ÜGYVITELI VÉDELEM

Emberi veszélyforrások, IBK, IBSZ

Emberi beavatkozás elleni védelem

- Felhasználó/ügyintéző
 - ▣ **szűk jogkör**
 - ▣ adatbevitelt végez
 - ▣ a hozzárendelt, korlátozott erőforrásokat használhatja
 - ▣ ha gyakorlatlan, akkor például nem érzi a hiteles azonosítás fontosságát (egyszerű jelszó, stb)
- Üzemeltető
 - ▣ **széleskörű ismerete és jogosítványa van a rendszer felhasználásával kapcsolatban**
 - ▣ titoktartási kötelezettsége van (fontos információk)
 - ▣ beállítások végrehajtása, módosítása
 - ▣ felhasználók nyilvántartása, jogosultságok beállítása, jogosultságok életciklusának nyomonkövetése
 - ▣ utasítások alapján dolgozik

Emberi beavatkozás elleni védelem

- Mérnök
 - ▣ magas szintű informatikai végzettsége van
 - ▣ bizalmas információk – titoktartási kötelezettsége van
 - ▣ **rendszer beállítása, módosítása, javítása**
 - ▣ széles hatáskör
- Programozó
 - ▣ **rendszer készítése**
 - ▣ teljes hatáskör
 - ▣ komoly minőségbiztosítási rendszerrel felügyelik a programot

Emberi tényezőre visszavezethető veszélyek

□ Szándékos károkozás:

- ▣ behatolás az informatikai rendszerek környezetébe,
- ▣ illetéktelen hozzáférés (adat, eszköz),
- ▣ adatok- eszközök eltulajdonítása,
- ▣ rongálás (gép, adathordozó),
- ▣ megtévesztő adatok bevitele és képzése,

□ Nem szándékos, illetve gondatlan károkozás:

- ▣ figyelmetlenség (ellenőrzés hiánya),
- ▣ szakmai hozzá nem értés,
- ▣ a megváltozott körülmények figyelmen kívül hagyása,
- ▣ vírusfertőzött adathordozó behozatala,
- ▣ pszichológiai támadásokban való részvétel,
- ▣ biztonsági követelmények és gyári előírások be nem tartása,
- ▣ adathordozók megrongálása (rossz tárolás, kezelés),
- ▣ a karbantartási műveletek elmulasztása.

- In today's economic climate, the threats to your vital information are greater than ever before.
In 2008 there were 277 data breaches reported in the UK - and it's not just information that is lost.
- The costs to an organization have dramatically increased:
 - >> **£1.73 million is the average cost of a data breach***
 - >> **Lost business now accounts for more than 50% of the cost****
- One major cause of the rise of breaches has to do with the rise of the insider threat.
 - >> **67% of organizations do nothing to prevent confidential data leaving the premises on USB sticks and other removable devices.****
 - >> **53% of employees would take sensitive information with them if they were laid off.*****

Ügyviteli védelem

- Az informatikai rendszert üzemeltető szervezet ügymenetébe épített
 - ▣ védelmi intézkedések,
 - ▣ biztonsági szabályok és
 - ▣ tevékenységi formák együttese.
- más néven ez az **adminisztratív védelem**
- a szabályozás alapját a törvények és jogszabályok jelentik, ezeket pontosítják

Ügyviteli védelem

- Két szintje van:
 - ▣ stratégiai, tervezési szint:
 - *Informatikai Biztonsági Konceptió (IBK)*
 - ▣ mindennapi gyakorlatot érintő és szabályozó szint:
 - *Informatikai Biztonsági Szabályzat (IBSZ)*
- ez a két szint szorosan összefügg egymással és a szervezet más szabályaival
- a szabályozás uniformizál, csökkenti a kreativitást, kényelmetlenségeket okoz

Ügyviteli védelem

- ▣ például előírhatjuk, hogy ki jogosult a hardver- vagy szoftverhibák elhárítására, s az ügyintézőnek meg kell várnia az illetékest, hiába tudná esetleg ő is elvégezni a javítást
- ▣ *biztonságot* is nyújt a szabályozás a dolgozóknak: a szabályok betartása esetén **nem lehet őket felelősségre vonni**
- ▣ ha a szabályozás nem megfelelő, akkor a rendszergazdákra hárul a felelősség
- ▣ a szabályozás eredményességéhez hozzájárul a dolgozók együttműködése
- ▣ nemcsak betanulási időszakban, hanem **rendszeresen képezni kell a munkatársakat**

Informatikai Biztonsági Konceptió - IBK

- *A szervezet felső vezetésének informatikai biztonsággal kapcsolatos **stratégiai elképzeléseit** foglalja össze.*
- A koncepció tartalmazza a szervezet informatikai biztonságának **követelményeit**, az informatikai biztonság megteremtése érdekében szükséges **hosszú távú intézkedéseket**, ezek **kölcsönhatásait** és **következményeit**.

Informatikai Biztonsági Konceptió – IBK

Fontosabb tartalmi összetevői

- **a védelmi igény leírása:** jelenlegi állapot, fenyegetettségek, fennálló kockázatok, fenyegetések
- **az intézkedések fő irányai:** a kockázatok menedzselése,
- **a feladatok és felelősségek meghatározása és felosztása** a védelmi intézkedésekben,
- **idő- és költségterv** a megvalósításra és időterv az IBK felülvizsgálatára.

Informatikai Biztonsági Konceptió – IBK

A koncepció elkészítésének főbb szakaszai

1. Védelmi igény feltárása:

- ▣ lényeges informatikai rendszerek és alkalmazások kiválasztása (**amiket védenénk**)
- ▣ vállalat szerverei, tárolóegységei, lokális hálózata
- ▣ a vállalat tágabb környezete: világhálón való megjelenés, beszállítókkal, alvállalkozókkal szembeni követelmények
- ▣ az aktuális, a közép, esetleg a hosszú távú technológiai és **szervezeti fejlesztéseket** és változtatásokat is át kell gondolni

Informatikai Biztonsági Konceptió – IBK

A koncepció elkészítésének főbb szakaszai

2. **Fenyegetettség elemzés:**

- ▣ veszélyforrások feltárása
- ▣ a rendszerek gyenge pontjai
 - belső munkatársak...
 - az eszközökhöz és az adatokhoz való hozzáférés irányelveit is meg kell határozni
 - hozzáférések naplózásának módja

Informatikai Biztonsági Konceptió – IBK

A koncepció elkészítésének főbb szakaszai

3. **Kockázatelemzés:**

- ▣ a fenyegető tényezők, károk hatása az informatikai rendszerekre és a szervezetre
- ▣ lehetséges károk várható bekövetkezési gyakorisága
- ▣ kárérték
- ▣ ezeknek függvényében a szükséges védelem technológiáját és mértékét

Informatikai Biztonsági Konceptió – IBK

A koncepció elkészítésének főbb szakaszai

4. **Kockázat menedzselés:**

- ▣ veszélyforrások elleni védekezés módjainak kiválasztása (preventív védelem)
- ▣ intézkedési tervek, illetve ezek hasznossága, költsége
- ▣ váratlan helyzetekre adott lépések meghatározása
- ▣ felelősök kijelölése, felelősségi körök definiálása
- ▣ időterv az intézkedések bevezetésére
- ▣ intézkedések hatása felülvizsgálatának ütemezése
- ▣ IBK felülvizsgálatának ütemezése

Informatikai Biztonsági Szabályzat - IBSZ

- **Célja:** az informatikai rendszer alkalmazása során biztosítsa az **adatvédelem elveinek**, az **adatbiztonság követelményeinek érvényesülését**, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.
- Az informatikai vezető és az informatikai biztonsági ellenőr készíti el, a vállalat vezetője **adja ki**.
- Az általános élethelyzetekre vonatkozik.
- A szervezet többi szabályzatát is figyelembe kell venni.
- Rendszeresen felül kell vizsgálni.

IBSZ személyi hatálya

- **Személyi hatálya** kiterjed a vállalat informatikai szolgáltatásaiban részt vevő munkatársaira (szolgáltató, felhasználó).
- Különösen fontosak a rendszer-, valamint az adatgazdák jogait és kötelességeit meghatározó fejezetei.

IBSZ tárgyi hatálya

□ **Tárgyi hatálya** alá tartoznak a

- ▣ vállalat tulajdonában lévő, illetve általa használt számítástechnikai berendezések, szoftverek, adatok, adathordozók, dokumentációk.
- ▣ passzív adatátviteli vonalak (Ethernet, Token Ring, FDDI, ATM szegmensek, optikai és hagyományos összeköttetések), csatlakozók
- ▣ hálózati aktív elemek (repeaterk, bridge-k, switchek, routerek, transceiverek, modemek, terminálszerverek)
- ▣ minden hálózatra kötött számítógépes munkahely (PC, workstation, terminál, hálózati nyomtató) és szerver

IBSz biztonsági fokozata

- Biztonsági osztályba sorolás részleg szinten is (informatikai berendezések és adatok).
 - ▣ **Alapbiztonság:** általános informatikai feldolgozás (nyilvános és személyes adatok)
 - ▣ **Fokozott biztonság:** szolgálati titok, átlagos mennyiségű különleges adat (bizalmas adatok)
 - ▣ **Kiemelt biztonság:** államtitok, nagy mennyiségű különleges adat. (titkos adatok)

IBSZ: Felelősségi rendszer megadása

- Adatvédelmi felelősök megadása: pl. informatikai vezető, rendszergazda
- **Adatvédelmi felelősök** feladatainak megadása
Példák:
 - ▣ IBSZ alkalmazásának módja: oktatás, munkaköri leírások stb.
 - ▣ IBSZ karbantartása
 - ▣ Védelmi rendszer ellenőrzése
- **Rendszergazda** feladatainak megadása
Példák:
 - ▣ Gondoskodik a folyamatos vírusvédelemről
 - ▣ Felelős a vállalkozás informatikai rendszer hardver eszközeinek karbantartásáért
- **Felhasználók** feladatai
 - ▣ Pl. : Ismerniük és be kell tartaniuk a szabályzatot, részt kell venniük adatvédelmi oktatáson

IBSZ: Felelősségi rendszer megadása

▣ A felelős joga és kötelessége:

- Az előírások betartásának ellenőrzése
- Figyelmeztessen a betartásra
- Fegyelmi felelősségre vonást kezdeményezhet
- Az általa észlelt, tudomására jutott veszélyhelyzetnek megfelelően védekező lépéseket meghozza
 - Az adott gépek külső elérhetőségének letiltása
 - Az adott gépek hálózatról való eltávolítása
 - Egyebek
 - Az incidensekről beszámolót készíteni, azt az illetékes vezetőknek eljuttatni

▣ Minden felhasználónak kötelessége

- Betörésgyanús esetek jelentése a biztonsági csoport felé
- Együttműködés a károk elhárításában

IBSz : Védelmi intézkedések

□ **Infrastruktúra védelme**

- ▣ Eszközök megközelítése az épület belseje felől
- ▣ Kulcs, naplózott belépés
- ▣ Rács, biztonsági üveg a földszinti ablakokon
- ▣ Ki- és beviteli engedélyek az eszközökre
- ▣ Hibaelhárítás felelősei, módjai
- ▣ Selejtezés módja (adatok végleges törlése)
- ▣ **Azokat az adathordozókat, amelyeken érzékeny adatokat tároltak nem ajánlatos törlés után tovább adni, hanem ellenőrzött módon meg kell semmisíteni!**

IBSz: Védelmi intézkedések

- **Hozzáférési jogosultságok meghatározása/Felhasználói jogok kezelése**
 - ▣ Jogok kiosztásáért felelős \neq Végrehajtásért felelős
 - ▣ Naplózni és visszakereshetővé tenni minden akciót
 - ▣ Felhasználói életciklus
 - ▣ Intézkedési terv az illetéktelen hozzáférés illetve a jogosultságokkal való visszaélés eseteire
 - ▣ Biztonsági eseménynapló
 - ▣ Automatikus naplózás

IBSz: Védelmi intézkedések

- **Hozzáférési jogosultságok meghatározása/Felhasználói jogok kezelése**
 - ▣ A rendszert csak illetékes vezető engedélyével szabad megváltoztatni
 - ▣ Külső személy a kezelt adatokhoz nem férhet hozzá
 - ▣ Jelszómenedzsment
 - ▣ Felhasználók listájának rendszeres aktualizálása
 - ▣ Ideiglenesen v. tartósan távol levő munkatárs helyettesítése
 - ▣ Külső partnerek hozzáférési jogosultsága (federation)

IBSz: Védelmi intézkedések

□ Szoftver

- ▣ Informatikáért felelős egység szerzi be, telepíti
- ▣ Az egység rendszergazdája végzi, vezetői utasításra
- ▣ Szoftverek jogvédelmét figyelembe kell venni
- ▣ Munkamásolatokat kell készíteni (elkülönített helyen kell tárolni)
- ▣ Jogtisztta szoftver
- ▣ A vállalat tulajdonát tilos eltulajdonítani
- ▣ Szabad szoftver használata esetén kártékony programokat kerülni kell

IBSz: Védelmi intézkedések

□ **Adathordozó**

- ▣ Nem használható személyes célokra a vállalati adathordozó
- ▣ Sajátot sem ajánlatos munkacélra használni
- ▣ Fizikai védelemre ügyelni kell
- ▣ Minősített adatot csak nyilvántartott adathordozóra szabad felvinni
 - melyeknek külön azonosítója van
 - tilos felügyelet nélkül nyílt helyen tárolni
 - másolat készítése engedéllyel

IBSz: Védelmi intézkedések

□ **Adathordozó**

- ▣ Sérült, hibás – tilos használni
- ▣ Ha csak olvassuk, akkor legyen írásvédett
- ▣ Használaton kívül elzárni, esetleg raktárban tárolni, archiválni
- ▣ Selejtezéskor megsemmisíteni
 - Minősített adatot tartalmazókat **zúzással**

IBSz: Védelmi intézkedések

□ Dokumentumok, adatok

- ▣ Védelmére a hardver és szoftver védelmi eljárások vonatkoznak
- ▣ Papíron -> levéltárban (biztonsági rendszerrel őrzött szobában)
- ▣ A visszakövethetőség miatt: folyamatosan dokumentálni kell, naplóállományokat megfelelően kezelni kell
- ▣ Minden olyan eseményt, amely eltér a megszokott üzemviteltől naplózni kell (tartalmaznia kell az esemény pontos leírását)

IBSz: Védelmi intézkedések

□ Adatok

- hozzáférés védelem,
- rendszeres mentés,
 - tükrözés,
 - biztonsági mentés,
- adatállományok védelme
- Az input adatok helyességének biztosítása
- A feldolgozás helyességének védelme
- Archiválás

IBSz: Védelmi intézkedések

□ Hálózati védelem

- A szervezet belső hálózatának és központi levelező szerverének üzemeltetése, valamint a világhálóra való csatlakozás a **központi informatikai egység** feladata
 - Ők szűrik a kártékony programokat, leveleket
- **Hálózati rendszeradminisztrátor:** az informatikai egység vezetője által megbízott személy
 - A hálózat mindenkor kiépítettségét és
 - A hálózatra kötött minden eszköz naprakész nyilvántartását vezeti
 - Csak a hozzájárulásával lehet a hálózatra eszközt kötni, továbbá több egységet érintő szerverszolgáltatást indítani
 - Jogkörét részben átadhatja valamely egység rendszeradminisztrátorának (az átadott jogok és kötelezettségek pontos leírásával)

□ **A belső elektronikus levelezés**

- ▣ Leghasznosabb és leggyakrabban használt szolgáltatás
- ▣ Növeli a vállalat belső és külső információ forgalmának sebességét és hatékonyságát
- ▣ Dolgozók együttműködését is egyszerűbbé teszi
- ▣ Negatív hatások is vannak (pl. kéretlen levelek)
- ▣ Tilos olyan adatok továbbítása (küldése, letöltése), amely alkalmas kártékony kódnak a vállalat informatikai rendszerébe juttatására

IBSz: Védelmi intézkedések

- **A belső elektronikus levelezés**
 - ▣ A dolgozók milyen célra használhatják
 - ▣ Az elektronikus levelezési cím és a hozzátartozó elektronikus láda a vállalat tulajdona
 - Iktatni kell és ellenőrizhetik
 - Ha a dolgozó kiesik, beteg, más is hozzáférhessen
 - Projekttel kapcsolatos leveleket külön mappában tárolni, lezárás után archiválni
 - Az informatikáért felelős egységnek rendszeres mentést kell végeznie a dolgozók e-postaládájáról