Muha Lajos–Bodlaki Ákos

Az informatikai biztonság

PRO SEC

Muha Lajos–Bodlaki Ákos

Az informatikai biztonság

PRO SEC

Budapest, 2005

Muha Lajos–Bodlaki Ákos
Az informatikai biztonság

Szakmai lektor:
Dr. Papp György

Copyright © 2003
Muha Lajos, Bodlaki Ákos

Copyright © 2003
PRO-SEC Kft.

Minden jog fenntartva. A jelen – szerzői jogvédelem alatt álló – tankönyv bármely részének másolása vagy reprodukálása csak a szerzői jog tulajdonosának engedélyével lehetséges. Az engedélyeket az alábbi címen lehet beszerezni:

PRO-SEC Kft.
1024 Budapest, Keleti K. u. 13.
Peterdiné Árva Ilona ügyvezető igazgató
Telefon: 212-5723

ISBN 963 86022 6 0

JELMAGYARÁZAT 11

ELŐSZÓ 13

1. AZ INFORMATIKAI BIZTONSÁG MEGHATÁROZÁSA 15
   1.1. Az informatikai biztonság kialakulása 15
   1.2. A védelem és a biztonság 15
   1.3. Az informatikai biztonság 17
   1.4. Az informatikai biztonság és más tudományok, szakterületek kapcsolata 20

2. AZ INFORMATIKAI BIZTONSÁG JOGI SZABÁLYOZÁSA 23
   2.1. Az államtitok és a szolgálati titok védelme 23
   2.2. Az üzleti titok védelme 25
   2.3. A banktitok és az értékpapírtitok védelme 26
   2.4. A köziratok, közlevéltárak és a magánlevéltári anyag védelme 27
   2.5. A személyes adatok védelme 27
   2.6. Az elektronikus aláírás 29

3. HAZAI ÉS NEMZETKÖZI SZABVÁNYOK ÉS AJÁNLÁSOK 31
   3.1. TCSEC 33
   3.2. ITSEC 36
   3.3. X/Open 36
   3.4. ISO/IEC 15408 szabvány (Common Criteria) 37
   3.5. ISO/IEC 17799 és BS 7799 szabványok 40
   3.6. INFOSEC – Informatikai biztonság a NATO-ban 44
   3.7. MeH ITB 8. sz. ajánlás 45
   3.8. MeH ITB 12. sz. ajánlás 46
   3.9. MeH ITB 16. sz. ajánlás 47
   3.10. Az egyes ajánlások biztonsági osztályai közötti megfelelés 49

4. INFORMATIKAI BIZTONSÁGI KÖVETELMÉNYEK 49
   4.1. Bevezetés 55
   4.2. Követelmények az információvédelem területén 55
      4.2.1. Információbiztonsági osztályok az információvédelem területén 55
      4.2.2. Alapbiztonsági osztály 55
      4.2.3. Fokozott biztonsági osztály 62
      4.2.4. Kiemelt biztonsági osztály 67

4.3. Követelmények a megbízható működés területén 71
4.3.3. Fokozott biztonsági osztály 71
4.3.4. Kiemelt biztonsági osztály 74
4.3.2. Alapbiztonsági osztály 82
4.3.1. Információbiztonsági osztályok a megbízható működés területén 85

5. A VÉDELEM MEGVALÓSÍTÁSA 89

6. AZ INFORMATIKAI BIZTONSÁG TERVEZÉSE 90

7. A SZABÁLYOZÁS 95
7.1. Az informatikai biztonságpolitika 95
7.2. Informatikai Biztonsági Szabályzat 97
7.3. Az informatikai biztonsági stratégia 99
7.4. Titokvédelmi és Ügyviteli Szabályzat 100
7.4.1. Titokvédelmi Szabályzat 100
7.4.2. Ügyviteli Szabályzat 100
7.5. Üzletmenetfolytonosság-tervezés 101
7.5.1. Az üzletmenet-folytonosság fogalma 101
7.5.2. Az üzletmenetfolytonosság-tervezés célja 103
7.5.3. Üzletmenetfolytonosság-tervezés, költségek, kockázatarányosság 103
7.5.4. Az üzletmenet-folytonosság tervezési folyamata 104

8. AZ EMBERI TÉNYEZŐ 109
8.1. Információvédelem a belépéstől a szervezet elhagyásáig 111
8.2. Felvétel 111
8.3. Megtartás – a lojalítás biztosítása 112
8.4. Oktatás és képzés 113
8.5. Munkaszervezés 113

9. AZ INFORMATIKAI HELYISÉGEK FIZIKAI VÉDELME 115
9.1. Az épületek mechanikai védelme 115
9.2. Az elektronikai jelzőrendszer 116
9.3. Az informatikai helyiségek tűzvédelme 117
9.4. Informatikai helyiségek villámvédelme 118
9.5. Kisugárzás- és zavarvédelem 119

10. DOKUMENTUMKEZELÉS, ÜGYVITEL 121
10.1. Dokumentumkezelés az informatikai rendszerekben 122
11. LOGIKAI VÉDELEM AZ OPERÁCIÓS RENDSZEREKBEN, HÁLÓZATOKBAN ÉS ALKALMAZÁSOKBAN 124
11.1. Operációs rendszerek 124
11.1.1. MS Windows 95, MS Windows 98 124
11.1.2. Windows NT 125
11.1.3. UNIX 126
11.1.4. Novell hálózati operációs rendszer 128
11.2. Hálózatok 130
11.3. Alkalmazások 133
11.4. A rejtjelezés, a digitális aláírás és az elektronikus bizonyítványok 137
11.4.1. Szimmetrikus rejtjelező algoritmusok 138
11.4.2. Nyilvános kulcsú rejtjelezés 139
11.4.3. Elektronikus aláírás 140
11.4.4. Kulcskezelés, PKI, CA 141
11.4.5. Kriptográfiai Protokollok 142
11.5. Vírusvédelem 144
11.5.1. Vírusok, férgek, trójai programok 144
11.5.2. A vírusvédelem megvalósítása 145
11.6. Biztonsági kiegészítések 148
12. ELLENŐRZÉS, AUDITÁLÁS, KOCKÁZATELEMZÉS 150
12.1. Az informatikai rendszerek biztonsági ellenőrzése 150
12.1.1. Az informatikai biztonsági ellenőrzés célja 150
12.1.2. Az informatikai biztonsági ellenőrzések formái 150
12.1.3. Kötelező ellenőrzések 151
12.1.4. A szankcionálás 152
12.2. Az informatikai biztonság ellenőrzési folyamata 153
12.2.1. Informatikai biztonsági vizsgálat – kockázatelemzés 153
12.2.2. Az informatikai biztonság auditálása 166
12.2.3. Informatikai biztonsági tanúsítás és minősítés 168
13. IRODALOM 169

Ábrák, táblázatok, egyenletek

1.1. ábra 19
1.2. ábra 21
3.1. ábra 43
5.1. ábra 89
6.1. ábra 91
6.2. ábra 92
7.1. ábra 104
7.2. ábra 107
11.1. ábra 129
11.2. ábra 132
11.3. ábra 138
11.4. ábra 142
12.1. ábra 156
12.2. ábra 166

3.1. táblázat 33
3.2. táblázat 35
3.3. táblázat 46
3.4. táblázat 47
4.1. táblázat 72
4.2. táblázat 79
8.1. táblázat 110
10.1. táblázat 122
11.1. táblázat 127

1.1. egyenlet 18
4.1. egyenlet 72

Jelmagyarázat

§	Definíció, törvényszerűség
 Tudni kell!	Alapvető követelmény, ismeret
 Tanuld meg!	Kiemelkedően fontos ismeret
 Figyelj jól!	Elmélyülést igénylő anyagrész
 Jó, ha tudod	Kiegészítő ismeret

Előszó

A legkülönbözőbb szervezetek tevékenységét és működését támogatja mind intenzívebben az informatika. Ezzel együtt mind bonyolultabb, mind nagyobb kiterjedésű informatikai rendszerek alakulnak ki. Mindennapos jelenségként figyelhetjük meg a számítógépes bűnözés elleni erőfeszítéseket és az adatvédelem kezelését. Ez felértékeli az informatikai biztonság szerepét és jelentőségét, mert alapvető elvárássá vált, hogy ezek a rendszerek biztonságosan legyenek használhatóak és az általuk kezelt adatok védve legyenek.

Jegyzetünk célja, hogy a felsőoktatásban, az informatikai vagy biztonsági szakirányon tanulók részére az informatikai biztonság alapjaitól, az informatikai rendszerek teljes életciklusát felölelve, a hazai és európai ajánlásokhoz igazodva ismertessük az informatikai biztonsággal kapcsolatos követelményeket és teendőket, kitérve napjaink aktuális kérdéseire is.

A jegyzet jelentős részben a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság 8. és 12. számú ajánlásainak, illetve „Az informatikai biztonság kézikönyve" (Verlag Dashöfer, 2000–2001) felhasználásával készült.

1. Az informatikai biztonság meghatározása

1.1. Az informatikai biztonság kialakulása

Az információk megszerzésére való törekvés és ezzel együtt az információk védelme az emberi társadalmak kialakulásával egyidős tevékenység. Már az ősközösségi társadalmakban is „lopták" az információkat, amikor megpróbálták kifürkészni a másik közösség vadászási szokásait vagy túlélési praktikáit. A társadalmi és tudományos fejlődéssel együtt az információk megvédésének – és ezzel együtt természetesen megszerzésének – technikája mind tökéletesebb lett. Csak kisszámú, megbízható és védett személy ismerhette meg a legbizalmasabb adatokat, védett helyekre zárták gyakran nemcsak a védendő adatokat, hanem az azokat ismerő személyeket is. Kialakultak a „titkosítás" – és ezzel párhuzamosan a megfejtésük – módszerei, megszületett a kriptográfia, ami a huszadik századra a matematikai tudományok önálló ágává nőtte ki magát. Biztonsági „szolgálatok" szerveződtek, amelyek őrizték az információkat, az információt ismerő személyeket, felderítették és elhárították az információt fenyegető támadásokat – és természetesen ezzel együtt fejlődtek az információszerzés módszerei is.

Azonban nemcsak az információ védelme fejlődött, hanem a védendő információ, illetve annak feldolgozási, kezelési, tárolási eszközei is óriási változásokon mentek keresztül. Az elmúlt évtizedekben robbanásszerűen fejlődött az információ- és kommunikációtechnika. A számítógépek megjelenése, a személyi számítógépek tömeges elterjedése és különösen a számítógépes hálózatok összekapcsolása forradalmasította az információ gyűjtését, feldolgozását, kezelését, tárolását, és ezzel együtt a számítógépeken tárolt, továbbított adatok védelme is új értelmezést nyert.

A különböző szervezetek rájöttek, hogy nem elegendő az információkat hagyományos módszerekkel védeni, hanem magukat a számítástechnikai eszközöket is úgy kell kialakítani, hogy megfelelő védelmet biztosítsanak.

1.2. A védelem és a biztonság

A védelem egy olyan tevékenység, illetve tevékenységek sorozata, amely arra irányul, hogy megteremtse, szinten tartsa, fejlessze azt az állapot, amit biztonságnak nevezünk. Tehát **a védelem tevékenység,** amíg **a biztonság állapot.**

A védelmet mint tevékenységet modellezve egy egyszerűsített helyzetet képzeljünk el, amelyben a támadókat és a védőket egyszerűsítéssel egy-egy személy, a *védő* és a *támadó* testesíti meg. **A támadó az egyik oldalról támad**[1], és ez a támadás mindig valamilyen, a támadás végső célját képező értékre, ***a védett értékre*** irányul. A támadás legtöbbször nem közvetlenül éri a védett értéket, hanem a körülményektől függő *támadási útvonalon* zajlik le, amelyen különböző természetes vagy művi védelmi akadályokat kell legyőzni. **A másik oldalon a védő a védett értéket védi**, vagyis a támadásokat igyekszik megakadályozni, elhárítani. Mivel a védő és a támadó egymás szándékairól, módszereiről semmilyen információval nem rendelkezik, ezért elmondhatjuk, hogy mindkét fél egymástól független és egymás számára ismeretlen stratégiával igyekszik megvalósítani támadási, illetve védelmi szándékait. Ilyen és hasonló szituációkkal foglalkozik a játékelmélet, amelynek nyelvén ezt *„kétszemélyes, nullától különböző összegű játék"*-nak nevezik. A „kétszemélyes játék" kifejezés nem szorul különösebb magyarázatra, a „nullától különböző összegű játék" pedig azt jelenti, hogy a játék eredménye szempontjából a támadó nyeresége[2] és a védő vesztesége[3] sohasem egyenlítik ki egymást. A védő vesztesége a védelemre fordított költség, és ehhez adódik a támadások során a védendő értékben, illetve a védelmi rendszerben okozott károk összege, nyeresége pedig nincs. A támadó kára a támadás költsége, beleértve ebbe a védő által a támadás során és utólagosan okozott károkat, nyeresége pedig legfeljebb a védett értékig terjed. A védő olyan védelmi intézkedéseket foganatosít, hogy a sikeres támadás valószínűségét minimálisra csökkentse. A védelem kiépítése a védőnél költséget emészt fel, ugyanakkor a támadó költségeit is növeli.

Az **informatikai biztonság** két alapterületet foglal magában:

- **információvédelem,** amely az adatok által hordozott információk *sértetlenségének, hitelességének és bizalmasságának elvesztését* hivatott megakadályozni;
- **megbízható működés,** amely az adatok és erőforrások *rendelkezésre állását* és a hozzájuk kapcsolódó alkalmazói rendszerek *funkcionalitását* hivatott biztosítani.

Az információvédelem helyett talán helyesebb lenne az **adatvédelem** kifejezést használni, de ezt a fogalmat a mai magyar általános és jogi szóhasználat a szemé-

[1] Támadás alatt nemcsak a személyek, szervezetek által elkövetett támadásokat értjük, de áttételesen a gondatlanságból, nem szándékosan kiváltott veszélyeztetéseket és a környezeti, természeti fenyegetéseket is.

[2] Nyereség alatt nemcsak közvetlen, pénzben kifejezhető értéket, bevételt értünk, hanem például az erkölcsi hasznot is.

[3] Veszteség (költség) alatt nemcsak közvetlen, pénzben kifejezhető értéket értünk, hanem általános jelleggel bármilyen jellegű ráfordítást, például idő, és ideértjük az anyagi és nem anyagi jellegű károkat is.

lyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény szellemében az adatok egy szűkebb körének, a személyes adatok védelmére értelmezi. Ugyanakkor él egy tágabb értelmezés is, amely szerint minden fajta és a legkülönbözőbb formában megjelenő adat védelmét is értik alatta, vagyis azt, amit mi informatikai biztonságnak nevezünk.

Létezik az információvédelemnek egy szélesebb értelmezése, amely szerint mind a hagyományos eszközökkel (papír, telefon, szóbeli közlés stb.), mind az informatikai eszközökkel kezelt adatok halmaza beletartozik.

Gyakran hallani az **adatbiztonság** kifejezést is. Ezzel a megbízható működéshez hasonló fogalmat szoktak jelölni, bár pontosan senki sem definiálta még tartalmát.

1.3. Az informatikai biztonság

A biztonság általános értelmezéséből levezethetjük az informatikai biztonság fogalmát, **ahol a védelem, illetve a támadás alapvető tárgya az *adat***, amely az információ hordozója. Az informatikai rendszerben működő alkalmazások és a hozzájuk kapcsolódó adatok fenyegetettségét a legszélesebb körben a következőkkel lehet jellemezni:

- a **bizalmasság** elvesztése,
- a **sértetlenség** elvesztése,
- a **hitelesség** elvesztése,
- a **rendelkezésre állás** elvesztése,
- a **funkcionalitás** elvesztése.

A továbbiakban a fenti fogalmakat **alapfenyegetettségek**nek nevezzük. Az adatok bizalmassága, sértetlensége és hitelessége logikailag erősen kapcsolódik az informatikai rendszerben kezelt (feldolgozott, tárolt és továbbított) információk (adatok) védelmének fogalomköréhez és sok esetben egymáshoz is, ezért az *információvédelem* fogalmát mint a bizalmasság, a sértetlenség és a hitelesség elvesztése elleni védelmet értelmezzük.

A rendelkezésre állási és a funkcionalitási igények között szoros összefüggés mutatható ki, mert az alkalmazások funkcionalitási hiányai általában kihatnak az adott alkalmazás vagy adatállomány rendelkezésre állására is, ezért a *megbízható működés* fogalmát mint a rendelkezésre állás és a funkcionalitás biztosítását használjuk.

A támadások, a fenyegetések az *adatok bizalmasságát, sértetlenségét, hitelességét, rendelkezésre állását* és a felhasználói funkciókban betöltött *funkcionalitásukat* veszélyeztetik. Ennek figyelembevételével, a biztonság általános definíciója alapján az informatikai biztonságot a következőképpen határozzuk meg:

§ **Az informatikai biztonság a védelmi rendszer olyan, a védő számára kielégítő mértékű állapota, amely az informatikai rendszerben kezelt adatok bizalmassága, hitelessége, sértetlensége és rendelkezésre állása, illetve a rendszerelemek rendelkezésre állása és funkcionalitása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.**

- **Zárt védelemről** *az összes releváns fenyegetést figyelembe vevő védelem* esetén beszélünk.
- **Teljes körű védelem** alatt azt értjük, hogy a ***védelmi intézkedések a rendszer összes elemére*** kiterjednek.
- A **folytonos védelem** az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul.
- A **kockázattal arányos védelem** esetén egy ***kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel***, azaz a védelemre akkora összeget és oly módon fordítanak, hogy ezzel a kockázat a védő számára még elviselhető, vagy annál kisebb. (A nem nullaösszegű játék eredménye a nullához közelít a támadó egyenlegét állandónak feltételezve.) Ezt az arányt a biztonságpolitika határozza meg, és mint a védelem erősségét is értékelhetjük.

  A kockázatot mint elvont fogalmat szokták alkalmazni, ám az formálisan is definiálható az 1.1. egyenlet szerint:

$$r = \sum_{t \in T} \left(p_t \times d_t \right),$$

1.1. egyenlet

ahol: r: a kockázat (Ft/év),
T: a releváns fenyegetések halmaza,
$\mathbf{p_t}$**:** egy adott kockázat bekövetkezésének gyakorisága (valószínűsége) (1/év),
$\mathbf{d_t}$**:** egy adott kockázat bekövetkezéséből származó kár (Ft).

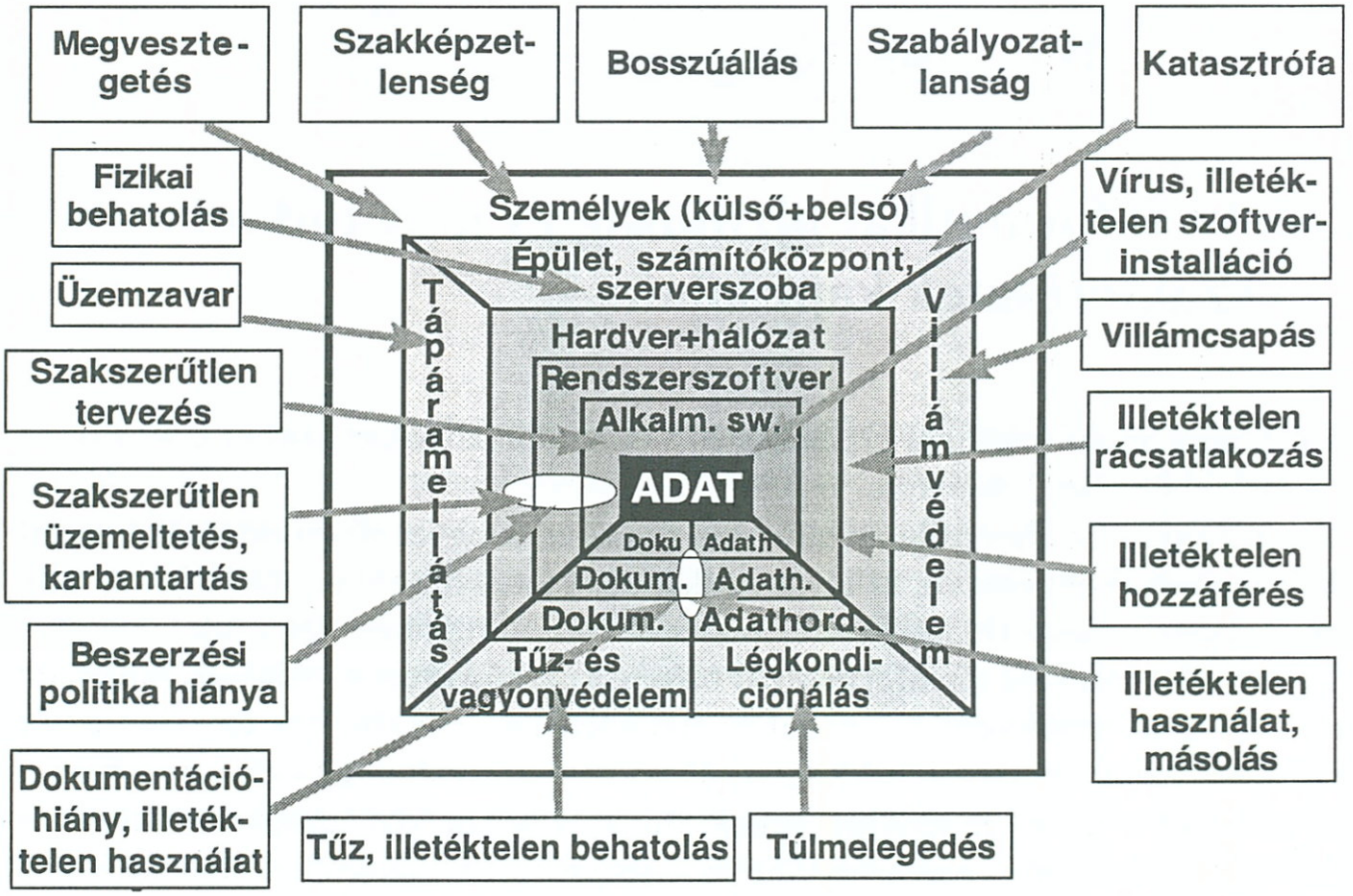

Tanuld meg!

A kockázat mértékegységekkel is kifejezhető, de nem mindig mint pontos időarányos összeg kerül meghatározásra, hanem gyakran valamilyen osztályzatként, amely a kockázat nagyságrendjét, elviselhető vagy nem elviselhető nagyságát mutatja.

A gyakorlatban, sok esetben egy védelmi intézkedésnek a megcélzott rendszerelemen kívül más rendszerelem vonatkozásában is van erősítő vagy gyengítő hatása (például egy erős fizikai védelmi intézkedés mellett az adott biztonsági tartományban nem szükséges olyan szintű azonosítási és hitelesítési eljárás a számítógéprendszerben, mint anélkül, vagy a biztonsági naplózás alkalmazásánál mindig figyelembe kell venni, hogy az hogyan hat a felhasználói funkciók hatékonyságára). **Egy rendszerelemre vonatkozóan el-**

sődlegesen alkalmazott védelmi intézkedéseknek a rendszer más elemeire ható járulékos hatását szinergikus hatásként vesszük számításba. Ha a védelmi intézkedések szinergikus hatását figyelmen kívül hagyjuk, akkor egy teljes körű, zárt, folyamatos és kockázatokkal arányos védelmi rendszert ***egyenszilárdnak*** tekinthetünk, mert az intézkedések minden rendszerelemre nézve pontosan a kockázatokkal arányosak lesznek úgy, hogy közben minden releváns fenyegetés figyelembevételre került. Ha azonban az intézkedések szinergikus hatását figyelembe vesszük, akkor egy adott rendszerelemre az elsődleges intézkedés és a többi intézkedés szinergikus hatásának eredője pozitív vagy negatív irányban a kockázatarányostól el fog térni.

A fentiek alapján egy olyan védelmi modellt állíthatunk fel, amelyben a támadás alapvető tárgya az adat. A támadások azonban nem közvetlenül érik az adatokat, hanem az azokat „körülvevő" *rendszerelemeken* (például a hardver és/vagy szoftver elemeken, a környezeti infrastruktúrán) keresztül. A támadás alatt nemcsak az adatok bizalmasságát, sértetlenségét, hitelességét veszélyeztető számítógépes bűnözési akciókat kell érteni, hanem minden olyan fenyegetést is, amely a rendszer megbízható működését, ezáltal az adatok rendelkezésre állását és a funkcionális követelményeknek megfelelő felhasználásukat veszélyezteti.



1.1. ábra

Az adatot mint a támadások alapvető célját a következő rendszerelemek veszik körül:

- az informatikai rendszer fizikai környezete és infrastruktúrája,
- hardverrendszer,
- szoftverrendszer,
- kommunikációs, hálózati rendszerek,
- adathordozók,
- dokumentumok és dokumentáció,
- személyi környezet (külső és belső).

E rendszerelemekre különböző fenyegetések hatnak, amelyek a rendszerelemek meghatározott láncán keresztül az adatokat veszélyeztetik. Az **1.1.** ábra ezt a gyakorlati szintű modellt ábrázolja, amelyen – rajztechnikai okok miatt – csak néhány jellemző fenyegetést tüntettünk fel.

Mint látható, egy informatikai rendszer számtalan pontján és sokféle módon támadható, így – különösen ha az nagyméretű és összetett – a védekezés helye és módja egyáltalán nem kézenfekvő feladat.

A fentiekből egyértelműen látható, hogy az informatikai biztonság témaköre szerteágazó, összetett kérdéskörökkel foglalkozó szakterület, illetve az is nyilvánvaló, hogy nem csupán informatikai és nem is csak védelmi kérdés, hanem több tudomány területeit felölelő – (ma még) nem önálló tudományágként kezelt – szakterület.

1.4. Az informatikai biztonság és más tudományok, szakterületek kapcsolata

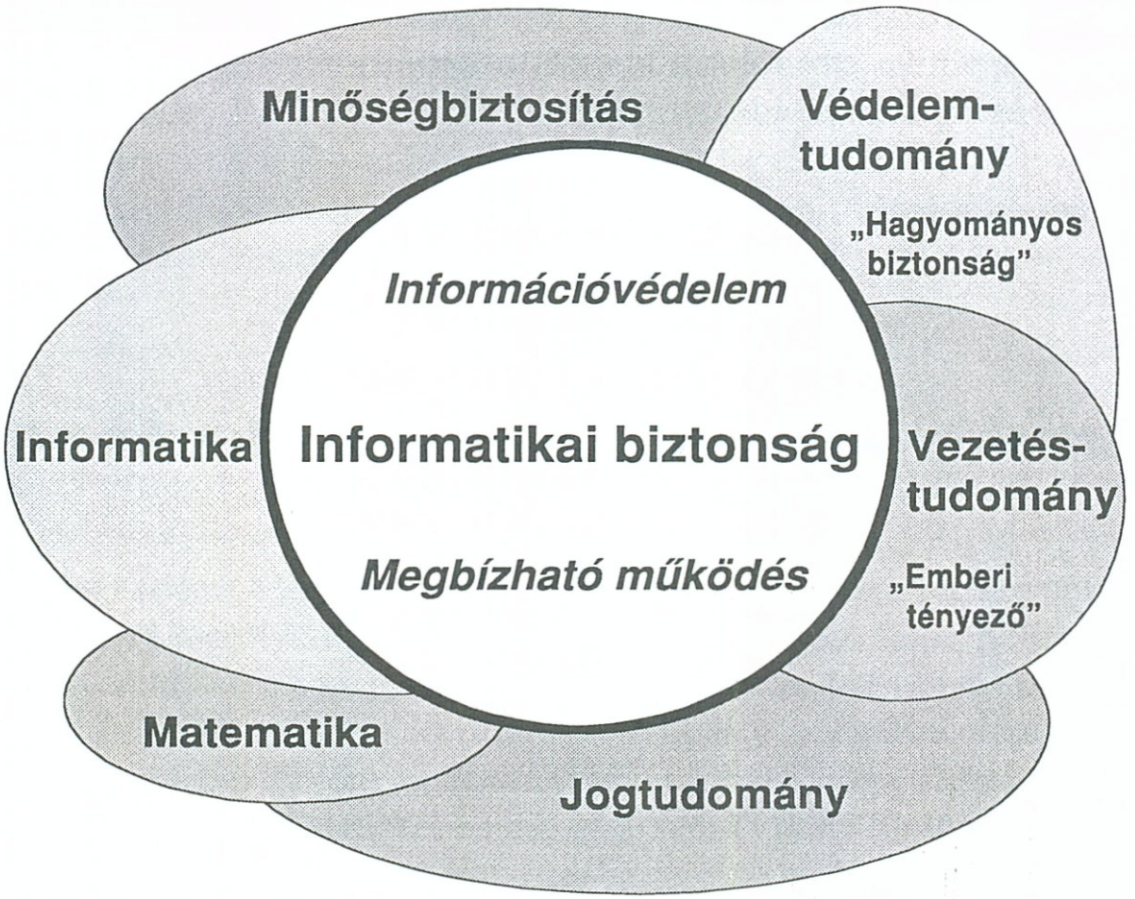
Az **1.2.** ábra az informatikai biztonság és a társtudományok egymáshoz képest való „elhelyezkedését" ábrázolja.

Az informatikai biztonság az informatikának csak egyes részterületeivel foglalkozik, ugyanakkor nemcsak az informatikához, hanem más szakterületekhez, tudományágakhoz is kapcsolódik, azaz tipikus interdiszciplináris szakterület.

A **jogtudomány**hoz az informatikai biztonság elsősorban az adat- és titokvédelem, illetve az adminisztratív védelem területén kapcsolódik. Ez egyrészt az érvényben levő jogszabályok – főleg az állam- és a szolgálati, az üzleti és a banktitok, az egyéb magán- és szakmai titkok, illetve a személyes adatok védelme – tekintetében, másrészt a szervezetek helyi szabályozási rendszerének kialakításában még szélesebb jogi területeket ölel fel.

A **védelemtudomány** elemei az informatikai rendszerek védelmében részben mint a „hagyományos biztonság" jelennek meg, de azt a biztonsági modellt is ez a

tudományág adja, amely alapján teljes körűen és logikusan tárgyalható az informatikai biztonság. A biztonságpolitika és a védelmi stratégiák kialakításában is jelentős szerepe van a védelemtudománynak.



1.2. ábra

A **minőségbiztosítás** elsősorban az adatminőség biztosítása az adatok sértetlenségének, hitelességének, rendelkezésre állásának és funkcionalitásának biztosítása területén jelentkezik, de az informatikai rendszer megbízhatósági jellemzőinek teljes életciklusában, a koncepciótól az üzemeltetésig szoros kapcsolatban van az informatikai biztonsággal. Az informatikai biztonság tanúsítási és minősítési eljárása is sok tekintetben hasonlít az ISO 9000 szabványsorozat szerinti minőségtanúsítási eljáráshoz. Az ISO 9000 szabványsorozat abban is összefüggést mutat az informatikai biztonsággal, hogy például az ügyviteli rend mindkét helyen alapvető követelmény. Kimutatható egy a gyakorlatban is megmutatkozó kölcsönhatás, miszerint ott, ahol a minőségbiztosítás – megfelelő szinten, a szabványok figyelembevételével – megvalósult, az informatikai biztonság helyzete is jó, és fordítva, ahol az informatikai biztonságot a szabványok és ajánlások szerint megvalósították, ott a minőségbiztosítási rendszer is működőképes.

A **matematika** sok kérdésben felhasználandó az informatikai biztonság területén. Gondoljunk csak az előzőekben megismert játékelméleti modellre, de például a rejtjelzés (kriptológia), az egyedi, illetve kölcsönös hitelesítési vagy integritási eljárások mint a matematikai tudományok ágai kerülnek felhasználásra az informatikai biztonság megvalósításában.

Az informatikai rendszerek tervezési és fejlesztési módszerei, a projektmenedzsment, a humánpolitika stb. mint a **vezetéstudomány** területei szintén szorosan kapcsolódnak az informatikai biztonsághoz.

2. Az informatikai biztonság jogi szabályozása

Az élet különböző területein a jogi szabályozás alapfokú ismerete elengedhetetlen feltétele a hatékony tevékenységnek. Az informatikai biztonság területén ez különösen igaz, mert itt sok jogszabályi[4] előírást kell figyelembe venni a védelem tárgyának, módszereinek és erősségének kialakítása során. A legfontosabbnak tekintett jogszabályokat ismertetjük ebben a fejezetben.

2.1. Az államtitok és a szolgálati titok védelme

Az adataival történő önrendelkezés joga nemcsak a természetes személyeket, hanem azok közösségeit is, így az államot is megilleti. Az állam biztonságának, a nemzet szuverenitásának megőrzése közérdek, ezért azokat védeni kell.

Az **1995. évi LXV. törvény az államtitokról és a szolgálati titokról** (a továbbiakban: titokvédelmi törvény) minősített adatnak nyilvánítja a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló törvényben meghatározott köziratban szereplő, államtitkot vagy szolgálati titkot tartalmazó adatokat, a szóban közölt államtitkot vagy szolgálati titkot képező információkat, az államtitkot vagy szolgálati titkot képező információt hordozó objektumokat, technikai eszközöket és a nem tárgyiasult formában megjelenő államtitkot vagy szolgálati titkot képező információkat, eljárási módokat vagy más ismeretanyagokat. **A titokvédelmi törvény a minősített adatok adminisztratív védelmének egyik legfontosabb részeként a kezelés rendjének az általános iratokénál szigorúbb meghatározását – függetlenül attól, hogy a minősített adat állami vagy gazdálkodószervezet birtokában van – tekinti elsődlegesnek,** mivel a minősített adathordozók kezelése csak az egyéb adatoknál, iratoknál szigorúbb eljárási rendben és mindenkire egyaránt vonatkozó, egységes rendszerben képzelhető el.

Államtitok a törvény alapján az az adat, amely az úgynevezett államtitokkörben meghatározott adatfajta körébe tartozik, és a minősítési eljárás alapján a minősítő kétséget kizáróan megállapította, hogy az érvényességi idő lejárta előtti nyilvánosságra hozatala, jogosulatlan megszerzése vagy felhasználása, illetéktelen személy

[4] Jogszabály a törvény, a Kormány rendelete, a miniszterelnök és a Kormány tagjának rendelete, az önkormányzat rendelete (1987. évi XI. törvény a jogalkotásról).

tudomására hozása, továbbá az arra jogosult részére hozzáférhetetlenné tétele sérti vagy veszélyezteti a Magyar Köztársaság honvédelmi, nemzetbiztonsági, bűnüldözési vagy bűnmegelőzési, központi pénzügyi vagy devizapolitikai, külügyi vagy nemzetközi kapcsolataival összefüggő, valamint igazságszolgáltatási érdekeit. Az államtitokkör a törvény mellékletét képezi.

Szolgálati titok a törvény alapján azon adatfajták körébe tartozó adat, amelynek az érvényességi idő lejárta előtti nyilvánosságra hozatala, jogosulatlan megszerzése és felhasználása, illetéktelen személy részére hozzáférhetővé tétele sérti az állami vagy közfeladatot ellátó szerv működésének rendjét, akadályozza a feladat- és hatáskörének illetéktelen befolyástól mentes gyakorlását. A szolgálati titokköröket a törvény szerint minősítésre felhatalmazottak határozzák meg.

Az államtitkot, illetve a szolgálati titkot képező adatot minősíteni kell, a minősítést annak kell kezdeményezni, akinél a feladata végrehajtása során az adat keletkezik.

A minősítésre jogosult, a titokbirtokos, továbbá a titokvédelmi felügyelő a feladat- és hatáskörében engedély nélkül hozzáférhet a minősített adathoz, más személy (kivéve, aki a minősített adatot törvényi felhatalmazás alapján ismerheti meg), ideértve az érintettet is, kizárólag az e törvényben meghatározott engedély alapján jogosult minősített adat megismerésére. A szolgálati titokká minősített adatot – ha törvény másként nem rendelkezik – az érintett korlátozás nélkül megismerheti.

Ha állami szerv a feladatának végrehajtásához más közreműködését veszi igénybe, és ehhez a közreműködőnek a minősített adatba való betekintése szükséges, erre a minősítő ad engedélyt. Az engedély megadása előtt a minősítő köteles meggyőződni arról, hogy a közreműködőnél megteremtették-e a minősített adat védelméhez szükséges, jogszabályban előírt feltételeket. Ezek hiánya esetén a minősített adat nem adható át, nem továbbítható.

A fontos és bizalmas munkakört betöltő személyeknek **a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény** szerint, amennyiben államtitkot vagy külföldi minősítésű és jelölésű iratot kell megismerniük, „A", „B" vagy „C" típusú kérdőívet kell kitölteni. A kérdőív végén található biztonsági nyilatkozat tartalmazza azt a hozzájárulást, amelynek értelmében a nemzetbiztonsági szolgálatok a kérdőívet kitöltő személyről – amennyiben az adatok másként nem szerezhetők be – titkos eszközökkel is adatokat gyűjthetnek. Az illetékes nemzetbiztonsági szolgálat kockázatmentességről kiadott biztonsági szakvéleménye alapján adja ki az illetékes vezető a betekintési engedélyt. Az **1998. évi LXXXV. törvény a Nemzeti Biztonsági Felügyeletről** szabályozza – többek között – a NATO és a NYEU (Nyugat-európai Unió) minősített adatainak megismeréséhez szükséges eljárást. Eszerint a Nemzetbiztonsági Felügyelet „a NATO- vagy NYEU-minősített adatok megismerésére, illetve kezelésére felhatalmazott személyekről, illetve gazdálkodószervezetekről biztonsági tanúsítványt ad ki, illetve a szükséges biztonsági feltételek hiánya (megszűnése) esetén a biztonsági tanúsítványt megtagadja (visszavonja)".

2.2. Az üzleti titok védelme

A gazdasági hatékonyságot és a társadalmi felemelkedést szolgáló piaci verseny fenntartásához fűződő közérdek, továbbá az üzleti tisztesség követelményeit betartó vállalkozások és a fogyasztók érdeke megköveteli, hogy az állam szabályozza a gazdasági verseny tisztaságát és szabadságát. Ehhez olyan versenyjogi rendelkezések elfogadása szükséges, amelyek tiltják a tisztességes verseny követelményeibe ütköző piaci magatartást.

E tárgyban európai közösségi szintű szabályozás még nem alakult ki, ezért jogharmonizációs kötelezettségekkel sem kell számolnunk.

Az **1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról** tiltja az üzleti titok tisztességtelen módon való megszerzését vagy felhasználását, jogosulatlanul mással való közlését vagy nyilvánosságra hozatalát. Ilyennek minősül az is, ha az üzleti titkot a jogosult hozzájárulása nélkül, a vele fennálló vagy korábban fennállt bizalmi viszony vagy üzleti kapcsolat felhasználásával szerzik meg. Az érintett személyek titoktartási kötelezettsége tehát a bizalmi viszony, üzleti kapcsolat megszűnése után is fennáll, ha a tudomásukra jutott információ üzleti titoknak minősül.

Ez teljesen összhangban van **a Büntető Törvénykönyvről szóló 1978. évi IV. törvénnyel** (Btk. 300. §), illetve **a Polgári Törvénykönyvről szóló 1959. évi IV. törvénnyel** (Ptk. 81. §).

A tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szóló törvény eligazítást ad a használt fogalmak tartalmának megállapításához is, így alkalmazásában **üzleti titok a gazdasági tevékenységhez kapcsolódó minden olyan tény, információ, megoldás vagy adat, amelynek titokban maradásához a jogosultnak méltányolható érdeke fűződik, és amelynek titokban tartása érdekében a jogosult a szükséges intézkedéseket megtette.** A tény, információ, megoldás, illetőleg adat kifejezéseket tágan kell értelmezni. Ilyenek lehetnek például a tevékenységi feltételek, a pénzügyi helyzet, a vevőkör, a műszaki dokumentáció, a recept, a modell, a minta. A titoksértés tehát akkor is megvalósulhat, ha a megszerzett vagy felhasznált, illetőleg nyilvánosságra hozott tény, információ, megoldás vagy adat nem áll iparjogvédelmi oltalom alatt.

A tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szóló törvény a versenyjogi védelemre érdemes titok fogalmi elemei közé sorolja azt is, hogy az információ titokban tartása érdekében a jogosult tegye meg az adott körülmények között ésszerűnek mutatkozó intézkedéseket. A jogosultnak kell tehát az adott körülmények között az ésszerű intézkedéseket megtennie a titokban tartás érdekében (például szabályzatban meghatározza üzleti titkainak körét, és ezt alkalmazottainak tudomására hozza; esetleg a munkaszerződésekben rögzíti az üzleti titok megőrzésének kötelezettségét; vagy nyilatkozatot írattat alá az információ közlésekor stb.). Jogvita esetén pedig a bíróság döntheti majd el, hogy a megtett intéz-

kedések a szükséges mértéket elérték-e annak ellenére, hogy elégtelennek bizonyultak a titokban maradáshoz.

A törvény felsorolja a bizalmi viszony néhány esetét, így a fennálló vagy korábban fennállt munkaviszonyt, a tagsági viszonyt (például gazdasági társaság, szövetkezet esetén), továbbá a munkavégzésre irányuló egyéb jogviszonyt. Üzleti kapcsolat alatt nemcsak a szerződéskötést, hanem az azt megelőző tájékoztatást, tárgyalást, ajánlattételt is érti, függetlenül attól, hogy a szerződés létrejött-e vagy sem.

„Az érintett személyek titoktartási kötelezettsége tehát a bizalmi viszony, az üzleti kapcsolat megszűnése után is fennáll, ha a tudomásukra jutott információ üzleti titoknak minősül" – írja a versenytörvény indokolása, vagyis az érintett személyek titoktartási kötelezettsége a munkaviszony után is korlátozás nélkül fennáll. Ezt alátámasztja a Magyar Köztársaság Kormánya és az Amerikai Egyesült Államok Kormánya között a szellemi tulajdonról kötött megállapodás (1993/26. sz. Nemzetközi Szerződés) VI. Cikk 2. bekezdése, mely szerint *„A Felek egyike sem korlátozza az üzleti titkok védelmének időtartamát..."*.

Az **1992. évi XXII. törvény a Munka Törvénykönyvéről** (a továbbiakban: munka törvénykönyve) az üzleti titokra külön is kitér. Sajnálatos módon ez utóbbi nem teljesen egyértelműen fogalmaz a betartási kötelezettségek tekintetében és különösen annak időbeli hatályát illetően, így egyedi és eseti értelmezést tesz lehetővé, jogviták alapjául szolgálhat.

2.3. A banktitok és az értékpapírtitok védelme

Az **1996. évi CXII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról** kétfajta titokfogalmat rögzít, melyek jól megkülönböztethetők egymástól. Az egyik titokfogalom a már korábban tárgyalt üzleti titok, a másik pedig a banktitok. **Banktitok minden olyan, az egyes ügyfelekről a pénzügyi intézmény rendelkezésére álló tény, információ, megoldás vagy adat, amely az ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a pénzügyi intézmény által vezetett számlájának egyenlegére, forgalmára, továbbá a pénzügyi intézménnyel kötött szerződéseire vonatkozik.**

Az üzleti és a banktitok közötti különbség az, hogy míg az üzleti titok – megfogalmazásában teljesen azonos a korábban idézett üzleti titokkal – a pénzügyi intézmény saját titka, addig a banktitok a pénzügyi intézménynél az ügyfélről rendelkezésre álló adatokat tartalmazza, tehát ebben az esetben az ügyfél titkáról van szó.

Ezzel szinte betűre azonosak **az értékpapírok forgalomba hozataláról, a befektetési szolgáltatásokról és az értékpapírtőzsdéről szóló 1996. évi CXI. törvény** 114–117. §-ai.

A törvény szigorúan meghatározza tehát a banktitok, az értékpapírtitok fogalmát és azt is, hogy kik juthatnak hozzá, illetve milyen esetekben teszi lehetővé a banktitoknak harmadik személy részére történő kiszolgáltatását.

Mind az üzleti, mind pedig a banktitok, az értékpapírtitok birtokosa köteles a feladatkörében vagy megbízásának teljesítése során birtokába került üzleti és banktitkot megtartani időbeli korlátozás nélkül, azt feladatkörén kívül nem használhatja fel, és törvényi felhatalmazás nélkül harmadik személynek nem adhatja ki. A törvény tiltja az üzleti titok külső személy részére való kiszolgáltatását, illetve annak saját célú felhasználását annak érdekében, hogy az illető személy azzal gazdasági előnyt szerezzen, vagy a pénzügyi intézménynek, illetve az intézmény ügyfeleinek hátrányt okozzon.

Egy kivételes lehetőség azonban fennáll. A pénzintézetek hitel-nyilvántartási rendszere lehetővé teszi az adósokról szóló adatcserét a hitelintézetek és a befektetési társaságok között az úgynevezett rossz adósok nyilvántartása érdekében. Érdekesség az, hogy mint garanciális szabály beépült, hogy a nyilvántartás a természetes személyekre nem terjedhet ki és az adatátadás is szabályozott.

2.4. A köziratok, közlevéltárak és a magánlevéltári anyag védelme

A maradandó értékű iratokat a világon szinte mindenütt a kulturális örökség részeként kezelik, megőrzésüket legelterjedtebben levéltári intézmények működtetésével, illetve ezek tevékenységének szabályozásával biztosítja.

Az 1995. évi LXVI. törvény az iratokat két nagy csoportra, köziratokra és magániratokra osztja és meghatározza a köziratok kezelésének, védelmének, archiválásra történő előkészítésének és közlevéltárba adásának rendjét, továbbá a közlevéltárak feladatait, fajtáit, s ezek illetékességi körét, valamint az alapításukkal és fenntartásukkal kapcsolatos követelményeket; rendelkezik a közlevéltárakban őrzött anyag kutathatóságáról, illetőleg használatának egyéb módjairól, és megállapítja a magánlevéltári anyag védelmének legfontosabb szabályait.

2.5. A személyes adatok védelme

Az állam és a gazdaság működéséhez szükséges nagy tömegű információt a hagyományos módszerekkel már nem lehet kezelni. Az informatikai eszközök alkalmazása viszont veszélyekkel is jár az állampolgárok személyi jogaira nézve, ugyanis

az egyedi információkat, az önálló informatikai rendszereket egymással össze lehet kapcsolni, és ez a kapcsolat olyan elemzésekre, következtetések levonására – vagyis új információk létrehozására – ad lehetőséget, amelyek sérthetik azok érdekeit, akikre az eredeti információk vonatkoznak. Ebben az esetben (is) az állam érdekeivel ellentétben áll az adatalanyoknak az az érdeke, hogy a magánélet bizonyos adatai ne kerülhessenek be a különböző nyilvántartásokba, de legalább e nyilvántartások kezelése során biztosítsák, hogy érzékeny adatok nem jutnak illetéktelenek tudomására, illetve, hogy csak jól meghatározott és az adatalany által is ismert célra használhassák fel azokat.

Az **1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról** (a továbbiakban: adatvédelmi törvény) rendelkezéseiben, a társadalmi indokoltság, a személyes részvétel, az érintettek és az adatfajták korlátozása, a célhoz kötöttség, a továbbadás korlátozása, az adathelyesség, az időbeli korlátozás, a nyíltság, a biztonsági intézkedések és a felelősség elveiről és szabályozásáról szól, tükrözve az Európa Tanács Adatvédelmi Egyezményét és a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) irányelveit.

A személyes adatok körébe minden olyan adat beletartozik, ami tetszőleges élő személlyel, az érintettel kapcsolatos bármilyen információt hordoz, függetlenül attól, hogy az érintett ezeket mennyire kívánja védeni. **Személyes adat az érintettre vonatkozó tény, vélemény, minősítés, továbbá az adatból levonható következtetés** is, sőt azok az adatok is személyes adatnak minősülnek, amelyek önmagukban nem, de más személyes adatokkal összekapcsolva az érintettel kapcsolatba hozhatók.

Az adatvédelmi törvény abból indul ki, hogy a **személyes adataival mindenki maga rendelkezik,** vagyis információs önrendelkezési jogot deklarál, de nem hagyja figyelmen kívül azt sem, hogy e jog nem korlátlan, így lehetővé kell tenni és teszi is a törvény, hogy a személyes adatok kezelését jogszabály elrendelhesse, vagy személyes adatok átadását – bizonyos keretek között – megengedje. A személyes adatok az érintett hozzájárulása nélküli kezelésének, és ehhez átadásának, átvételének igénye elsősorban az államigazgatás, a bűnüldözés területein merül fel, azonban nem hagyható figyelmen kívül az, hogy ez az igény mások jogainak biztosítása érdekében vagy például a gazdasági élet egyes területein is indokolt lehet.

A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény kizárólag a személyes adatok védelmére alkalmazható, és sem betűje, sem „szelleme" nem terjeszthető ki más adattípusok védelmére.

A tudományos kutatás, a közvélemény-kutatás, a piackutatás és direkt marketing tevékenység név- és lakcímadatok nélkül gyakorlatilag működésképtelen, ezért külön törvény, **a kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvény** szabályozza az e tevékenységek végzéséhez szükséges adatok megszerzésének, továbbadásának és hasznosításának módját és lehetőségét.

Az adatvédelmi törvény nemcsak a személyes adatok védelméről, hanem a közérdekű adatok nyilvánosságáról is rendelkezik, amely rendelkezésnek egyik legfontosabb alappillére, hogy csak törvény alapján államtitokká vagy szolgálati titokká minősített adatok tekintetében engedi meg a nyilvánosság korlátozását.

2.6. Az elektronikus aláírás

A **2001. évi XXXV. törvény az elektronikus aláírásról** az elektronikus kommunikációhoz, így különösen az e-bussineshez, de sok más internetes alkalmazáshoz a forgalom biztonsága érdekében az információközlések valódiságának és hitelességének bizonyíthatóságához elengedhetetlenül szükséges jogszabályi feltételeket teremti meg.

A törvény figyelembe veszi az európai jogharmonizációból eredő követelményeket, így különösen az Európai Parlament és Tanács 1999/93/EK Irányelvét az elektronikus aláírás Közösségi keretéről és „A bizottság javaslata az Európai Parlamentnek és Tanácsnak egy irányelvére a belső piacon alkalmazott elektronikus kereskedelem bizonyos jogi vonatkozásairól" című tervezetet.

Az elektronikus aláírásról szóló törvény fontosabb alapelvei a következők:

1) Az elektronikus aláírás előállítására felhasznált technológiától függetlenül alkalmazható a törvény (technológia-semleges szabályozás).
2) Az elektronikus aláírás joghatálya nem tagadható meg amiatt, hogy kizárólag elektronikus formában létezik.
3) Az elektronikus aláírás használatát csak a törvény zárhatja ki olyan jogviszonyokkal kapcsolatos jogügyletekben, melyekben az elektronikus aláírás használata a felek érdekét, illetve a jogbiztonságot sértené.
4) Az elektronikus aláírás alkalmazását – az ügyfelet érintően – nem lehet kötelezővé tenni.
5) Elektronikusaláírás-hitelesítési szolgáltatást a jogszabályi feltételeknek megfelelő gazdálkodó szervezet nyújthat.
6) A minősített elektronikus aláírással ellátott elektronikus irathoz teljes bizonyító erejű magánokirati vagy közokirati minőséget kell rendelni.
7) A törvényben meghatározott általános elveket és eljárásokat az állami/közszféra területén is alkalmazni kell – a szükséges és megfelelő eltérésekkel.

A törvény a következő három fontos területet szabályozza:

1) az elektronikus aláírás felhasználási lehetőségeit;
   A törvény az elektronikus aláírás három fajtáját különbözteti meg: az „egyszerű", a fokozott biztonságú és a minősített elektronikus aláírást. Meghatá-

rozásra került az elektronikus dokumentum, az elektronikus irat, az elektronikus okirat törvényi fogalma is. A törvény a Polgári Törvénykönyv (1959. évi IV. törvény) hatályba lépéséről és végrehajtásáról szóló 1960. évi 11. törvényerejű rendelet módosításával írásbeli alakban létrejött szerződésnek tekinti a fokozott biztonságú elektronikus aláírással aláírt okirat útján létrejött megegyezést is.

2) az elektronikus aláírással kapcsolatos szolgáltatások szabályait;
Az elektronikus aláírással kapcsolatos szolgáltatások a hitelesítésszolgáltatás, az időbélyegző-szolgáltatás és az aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezése. A hitelesítésszolgáltatási tevékenység – az Európai Parlament és a Tanács az elektronikus aláírásról szóló irányelve alapján – nem köthető engedélyezéshez, ezért a fokozott biztonságú elektronikus aláírást hitelesítő szolgáltatót a Hírközlési Felügyelet „csak" nyilvántartásba veszi. Ha a hitelesítés-szolgáltató minősített tanúsítványt kíván kibocsátani, a Hírközlési Felügyelet megvizsgálja az előírások betartását, és ennek alapján minősíti a szolgáltatót. Mindezek a szabályok vonatkoznak az időbélyegzésszolgáltatóra és az aláírás-létrehozó eszközön aláírás-létrehozó adat elhelyezésével foglalkozó szolgáltatóra is.

3) a szolgáltatókat felügyelő és a szolgáltatókat nyilvántartó, illetve minősítő Hírközlési Főfelügyelet tevékenységére vonatkozó szabályokat.
A Hírközlési Felügyelet nyilvántartásokat vezet a szolgáltatókról, a tanúsított aláírás-létrehozó eszközökről, illetve aláírás-ellenőrző eszközökről, valamint a fokozott biztonságú, illetve minősített elektronikus aláírás-létrehozó és aláírás-ellenőrző eszközök, illetve szolgáltatók minősítésére jogosult tanúsító szervezetekről. A Hírközlési Felügyelet minősítési tevékenységet is végez, továbbá jogosult a hitelesítésszolgáltatókat ellenőrizni, az előírásoknak megfelelő működést kikényszeríteni.

3. Hazai és nemzetközi szabványok és ajánlások

Nemzetközi téren már az 1970-es évek végén megindult (elsősorban az Egyesült Államokban) az informatikai biztonsági értékelés követelményrendszere kidolgozására vonatkozó tevékenység. Első kézzelfogható eredménye a **Trusted Computer System Evaluation Criteria** (magyarul: Biztonságos Számítógépes Rendszerek Értékelési Kritériumai, röviden: TCSEC) dokumentum vagy más néven a „Narancs Könyv" megjelenése volt, amelyben az USA Védelmi Minisztériumának informatikai biztonsági követelményeit hozták nyilvánosságra – elsősorban – a beszállítók részére. E dokumentum 1983-ban kiadott verziója az USA-ban a mai napig érvényes, és kötelező a kormányzati, katonai rendszerek tekintetében!

Ezt követően több országban, például Ausztráliában, Kanadában, Angliában, Németországban, Franciaországban is elindult hasonló dokumentum kidolgozása. A '80-as évek vége felé a személyi számítógépek, a helyi és a nagy területeket átfogó hálózatok elterjedésével mind jobban erősödött az Európai Közösségben az a törekvés, hogy a Közösség is rendelkezzen egy egységes az informatikai biztonságra vonatkozó dokumentummal. Ennek eredménye lett az **Information Technology Security Evaluation Criteria** (magyarul: Információtechnológia Biztonsági Értékelési Kritériumok, röviden: ITSEC) dokumentum 1. változata, amelyet Anglia, Franciaország, Hollandia és Németország közösen dolgozott ki. Az ITSEC 1.2 ideiglenes változatát az Európai Közösség számára 1991-ben adták ki.

A fenti és más dokumentumok figyelembevételével a jelentős számítógép-szállítók által támogatott független szervezet, az *X/Open Company Ltd.* az *ISO 7498, Nyílt Rendszerek Összekapcsolása* (angolul: Open Systems Interconnection, röviden: OSI) szabványt megvalósító rendszerekre (röviden: nyílt rendszerek) kidolgozta az **Open Systems Directive** (magyarul: Nyílt Rendszerek Direktívái) 5. kötetét, amelyben az ITSEC-ben definiált biztonsági alapfunkciókra vonatkozó követelményeket írják le a nyílt és osztott (hálózatokon alapuló) informatikai rendszerekre.

Az időközben Európai Unióvá lett tagállamok, valamint az Amerikai Egyesült Államok és Kanada kormányainak támogatásával kidolgozásra került a **Common Criteria** (magyarul: Közös Követelmények, röviden: CC) dokumentum, amely megpróbálta a korábbi ajánlások tartalmi és technikai eltéréseit összhangba hozni, a különböző alkalmazási területekre pedig egyedi követelményeket meghatározni. A CC követelményrendszerének első három fejezetét kitevő „CC 2.0" dokumentumot – azonos tartalommal – az International Standard Organization ISO/IEC 15408 számon, „*Common Criteria for Information Technology Security Evaluation, version 2.0*" címmel kiadta. Az CC feldolgozására és honosítására irányuló

munka hazánkban, 1997-ben kezdődött meg, majd 1998-ban az Informatikai Tárcaközi Bizottság 16. sz. ajánlásaként kiadásra is került.

Áttörő szemléletváltást hozott a Brit Szabványügyi Hivatal által kiadott **BS 7799** szabvány, amely kifejezetten a felhasználók számára nyújt segítséget egy, a teljes szervezetet és a minden rendszerelemet átfogó informatikai biztonságmenedzsment rendszerének megvalósítására és annak ellenőrzésére a vonatkozó követelményrendszer kidolgozásán keresztül. Ez a szabvány már alkalmas arra, hogy a megfelelő akkreditálás és tanúsítási eljárások alkalmazásával lehetővé váljon a felhasználói rendszer – akár egyenkénti, akár szervezeti szintű – minősítése, tanúsítása a szabványnak megfelelően. A BS 7799 1. részét 2000 augusztusában **ISO/IEC 17799** néven nemzetközi szabványként fogadták el.

Magyarországon a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottságának (MeH ITB) kezdeményezésére 1995-ben kezdődött meg egy hazai ajánlás kidolgozása, amelyet 1996 decemberére véglegesítettek, és az *Informatikai Rendszerek Biztonsági Követelményei* címmel, mint a *MeH ITB 12. sz. ajánlása* kiadták.

A MeH ITB 12. sz. ajánlás készítői – a BS 7799 széles körű, nemzetközi elismertségét megelőzően – igyekeztek ötvözni a két szemléletet. Az informatikai rendszerek elemei (hardver, szoftver, hálózatok) esetében az ITSEC lett adaptálva, ugyanakkor részletes követelményeket és védelmi intézkedéseket tartalmaz az informatikai biztonság adminisztratív és a fizikai védelem területeire, a szervezeti, személyi és fizikai biztonság kérdéseire is. Sajnos hazánkban eddig az ISO/IEC 17799 nemzetközi szabvánnyal való harmonizáció irányába történő lépések nem történtek meg. A továbbfejlesztés szükséges és sürgős lenne, tekintve, hogy Magyarországnak feltett szándéka az Európai Unióhoz való csatlakozás.

Az Informatikai Rendszerek Biztonsági Követelményei kidolgozásánál elsődleges szempont volt, hogy ne csak a logikai védelem előírásait tartalmazza, hanem jelenjenek meg benne az adminisztratív és a fizikai védelem követelményei is. A logikai védelem területén elsősorban az ITSEC-re épült, de igyekezett figyelembe venni egyéb szabványokat, ajánlásokat is.

A gazdasági élet más területén tevékenykedő számos hazai nagyvállalat a saját biztonsági politikája kialakításakor figyelembe vette a 12. sz ajánlást, több esetben is belső szabályzóként, követelményrendszerként használják a biztonsági követelmények meghatározására. A nagy nyilvánosság számára könyvformájában a mai napig nem került kiadásra, de a teljes szöveganyag elérhető az interneten.

Hazánk NATO-csatlakozása óta a védelmi intézkedések, a biztonság fokozása területén nemcsak a Magyar Honvédség, de a civil szervezetek is odafigyelnek a NATO elvárásaira. Az informatikai biztonság NATO-n belüli értelmezése INFOSEC (*infor*mation *sec*urity) néven vált ismerté.

A következőkben áttekintjük a fenti dokumentumok lényegi elemeit, a dokumentumok által meghatározott biztonsági osztályokat és azokat a biztonsági alapfunkciókat, amelyekre nézve egységesen értelmezték az egyes osztályokra vonatkozó biztonsági követelményeket.

3.1. TCSEC

A TCSEC a következő 4 csoportra bontja a biztonsági osztályokat, egyre szigorúbb követelményekkel :

- **D csoport:** minimális védelem
- **C csoport:** szelektív és ellenőrzött védelem
- **B csoport:** kötelező és ellenőrzött védelem
- **A csoport:** bizonyított védelem

A TCSEC a D csoportot „érdemtelennek" tekinti az informatikai biztonság szempontjából, az A csoport esetében pedig *matematikailag (formálisan) bizonyítható* előírásokat, specifikációkat követel meg, amelyeket a gyakorlatban csak nagyon nagy ráfordításokkal lehet megvalósítani. Ezért a továbbiakban a B és C csoportokat elemezzük. A csoportokon belül a **3.1.** táblázat szerinti osztályokat különbözteti meg a TCSEC.

Osztály	Alapjellemző
C csoport	
C1 osztály	– korlátozott hozzáférés-védelem, a hozzáférési jogokat megvonással lehet szűkíteni;
C2 osztály	– nem szabályozott, de ellenőrzött hozzáférés-védelem, a hozzáférési jogok odaítélése egyedre/csoportra szabott;
B csoport	
B1 osztály	– címkézett és kötelező hozzáférés-védelem, a hozzáférő alanyokat (felhasználók, programok) és a hozzáférés tárgyait (adatállományok, erőforrások) a hozzáférési mechanizmust szabályozó *címkével kell kötelezően* ellátni;
B2 osztály	– strukturált hozzáférés-védelem, – az alanyok azonosítása és a hozzáférés ellenőrzése elkülönített referencia-monitor segítségével történik;
B3 osztály	– elkülönített védelmi területek, – a biztonsági felügyelő, operátor és a felhasználó biztonsági funkciói és jogai elkülönítve, – már a rendszer tervezése során el kell választani a biztonsági szempontból kritikus részeket.

3.1. táblázat

A TCSEC dokumentum a következő biztonsági alapfunkciókat definiálva az információvédelem és a megbízható működés területén (az eredeti angol kifejezéseket és rövidítéseket zárójelben tüntettük fel):

Információvédelem

- Az azonosítás és a hitelesítés folyamatának kialakítása *(Identification and Authentication, I+A)*.
- A hozzáférés-jogosultság rendszerének felépítése – *jogosultság kiosztás* (alanyok-eszközök meghatározása, attribútumok rögzítése, hozzárendelések – megengedő, illetve tiltó módszer a szigorodó követelményekre) *(Access Control)*.

  A hozzáférés-jogosultság rendszerének legmarkánsabb jellemzője a hozzáférés-vezérlési tábla (*Access Control List, ACL*) bevezetése, amely két módszerrel kerülhet alkalmazásra:
  - A C1 és C2 osztályokban a hozzáférés-jogosultság kiosztása nem előre meghatározott módon, hanem személyenként vagy felhasználói csoportonként, esetenként kerül meghatározásra, ez a vezérlési mód a *Discretionary Access Control* (magyarul: szabad belátás szerint kialakított hozzáférés-vezérlés, röviden: DAC).
  - A B1 és B2 osztályokban a hozzáférés-jogosultság kiosztása előre meghatározott módon, személyenként vagy felhasználói csoportonként kerül meghatározásra, ez a vezérlési mód a *Mandatory Access Control* (magyarul: előre meghatározott hozzáférés-vezérlés, röviden: MAC).
- A hozzáférés-ellenőrzés rendszerének megvalósítása – jogosultság-ellenőrzés *(Accountability, ACC)*.
- A bizonyítékok rendszerének és folyamatának kialakítása *(Audit, AUD)*.
- Az adatok sértetlenségének és konzisztenciájának biztosítása *(Accuracy)*.
- A biztonságos kezelési funkciók – biztonsági felügyelő, a rendszeradminisztrátor és a felhasználók szerepkörének szétválasztásával – *(Trusted Facilities Management, TFM)*.

Megbízható működés

- A megbízható működésre vonatkozó alapfunkció a megbízható szolgáltatások biztosítása *(Reliability of Service)*.

  Ez az alapfunkció a következő fontosabb részfunkciókra bontható:
  - A rendelkezésre állás biztosítása *(Availability, AV)*.
  - A biztonságos rendszer-visszaállítás biztosítása *(Trusted Recovery, TRE)*.
  - A rendszer funkcionalitásának biztosítása *(Functionality, FUN)*.
  - A funkcionalitást széles értelemben véve a további részfunkciók biztosítják:
    - rendszertervezési és fejlesztési módszertan alkalmazása, beleértve ebbe a biztonsági rendszert is,
    - megfelelő dokumentációs rendszer kialakítása,

– tesztrendszer és dokumentáció biztosítása, mind a felhasználói, mind a biztonsági rendszer területén,
– Biztonsági Kézikönyv (IBSZ, Információvédelmi Tájékoztató) kialakítása.

Alapfunkcióként szerepel a biztonságos adatcsere *(Data Exchange, DAT)* funkció is. Ez a funkció is az X/Open leírásában található meg részletesebben, itt csak a rejtett csatornákra vonatkozó követelményeket vettük figyelembe.

A **3.2.** táblázat a fenti biztonsági alapfunkciók osztályonkénti megjelenését és eloszlását mutatja.

		Biztonsági alapfunkciók								
Osztály		Információvédelem						Megbízható működés		
	I+A	DAC	MAC	ACC	AUD	DAT	TFM	AV	TRE	FUN
B3										
B2										
B1										
C2										
C1										

Jelmagyarázat:

	nincs követelmény az adott osztályban,
	nincs újabb követelmény az adott osztályban,
	új vagy bővített követelmény jelenik meg az adott osztályban.

3.2. táblázat

3.2. ITSEC


Tanuld meg!

Az Európai Közösség által kiadott ITSEC kiindulási dokumentumként a TCSEC-et tekintette, így a biztonsági alapfunkciók és a biztonsági osztályok értelmezése azzal analóg. Az egyes biztonsági osztályok a következők: *F-C1, F-C2, F-B1, F-B2, F-B3.*

Az ITSEC a TCSEC-kel azonos módon értelmezett biztonsági osztályain túlmenően, az egyes releváns informatikai rendszertípusokra is definiál biztonsági osztályokat, amelyekre megadja a TCSEC biztonsági alapfunkcióit, de az adott rendszertípusra jellemző követelményeket emeli ki.


Jó, ha tudod

Ezek a rendszertípusok és biztonsági osztályaik a következők:

- **F-IN:** Nagy integritású rendszerek osztálya *(Integrity)*
  Ebbe a típusba az adatbázis alapú rendszerek tartoznak, amelyeknél a tárolt adatok és programok integritása döntő jelentőségű.
- **F-AV:** Magas rendelkezésre állású, vagy kritikus működés biztonságú rendszerek osztálya *(Availability)*
  Ide tartoznak az on-line folyamat- és termelésirányítási, helyfoglalási és banki tranzakciós rendszerek.
- **F-DI:** Adatmozgatásnál magas adatintegritást biztosító rendszerek (*Data Integrity*)
  Ide tartoznak a magas szintű hibafelismerési és hibajavítási algoritmusokkal üzemelő rendszerek.
- **F-DC:** Bizalmas adatokat feldolgozó rendszerek *(Data Confidentiality)*
  Jellemző példái ennek az osztálynak a rejtjelzést felölelő rendszerek.
- **F-DX:** Magas adatintegritást és bizalmasságot biztosító osztott rendszerek *(Data Exchange)*
  Tipikus esete ennek, amikor nem védett nyilvános hálózaton keresztül történik nagy integritási és bizalmassági igényű adatok forgalmazása.

3.3. X/Open


Jó, ha tudod

Az X-OPEN biztonsági osztályokban a TCSEC-ben és az ITSEC-ben is elfogadott biztonsági funkciók szerepelnek. Az egyes biztonsági osztályokat röviden a következőkben jellemezhetjük:

- **X-BASE**: Alap biztonsági osztály
  Azonosítás, hitelesítési funkciók, hozzáférés-vezérlés, elszámoltathatóság biztosítása,
- **X-DAC**: Szabad belátás szerint kialakított hozzáférés-vezérlés
  Szabad belátás szerint kialakított hozzáférés-vezérlés (DAC), és Hozzáférés vezérlő tábla (Access Control List – ACL)

- **X-AUDIT**: Biztonsági auditálás biztonsági osztálya
  Az X-BASE funkciói kibővülnek a biztonsági vonatkozású események rögzítésével
- **X-MAC**: Előre meghatározott hozzáférés-vezérlés biztonsági osztálya
  Minden objektumhoz és szubjektumhoz biztonsági címke van hozzárendelve, minden szubjektum csak a biztonsági címkéjének megfelelő szintű objektumhoz (adathoz, erőforráshoz) férhet hozzá.
  A rendszert elhagyó adatok (nyomtatón, képernyőn) magukkal viszik a biztonsági címkéjüket.
- **X-PRIV**: Privilegizált jogokat biztosító biztonsági osztály
  A rendszeradminisztrátorok privilegizált szerepköre a felhasználóktól és egymástól is elválasztottan kezelt. Így a támadók által okozott kár korlátok közé szorítható.

3.4. ISO/IEC 15408 szabvány (Common Criteria)

A Common Criteria (röviden CC) létrehozásának célja egy olyan biztonsági követelményrendszer létrehozása volt, amely a – forrásul használt – ITSEC, TCSEC és CTCPEC technikai különbségeit feloldja, és ezzel egy nemzetközileg elfogadott szabvány alapjává válik. A CC fő jellemzői:

- egységes követelményeket határoz meg, függetlenül a megvalósítás módjától;
- egységes kiértékelési módszert ad az informatikai rendszerek, termékek informatikai biztonsági értékeléséhez, tanúsításához;
- meghatározza az informatikai rendszerek biztonsági követelményeinek katalógusát, a katalógus többszintű kategóriákból áll: osztály, család, komponens és elem;
- egyaránt felhasználható szoftver- és a hardverelemek vizsgálatához is;
- a termékek rugalmasan megválaszthatóak, mert a követelmények nem hardver- vagy szoftverspecifikusak;
- a CC alapján kiértékelt informatikai rendszerek kiértékelésének eredménye egy dokumentum, amely kijelenti:
  - a rendszer egy adott védelmi profilnak való megfelelőségét,
  - adott biztonsági cél követelményeinek való megfelelést,
  - a definiált 7 biztonsági osztály (EAL1-7) valamelyikének való megfelelést;
- definiálható a biztonsági funkcionalitás, azaz a CC terminológiája szerint a védelmi profil (*protection profiles*: **PP**), amely függetlenül besorolható a meghatározott 7 biztonsági szint (*Evaluation Assurance Level*: **EAL**) valamelyikébe.

A védelmi profil egy implementációfüggetlen funkcionális biztonsági követelményrendszert és objektumhalmazt határoz meg egy-egy terméktípusra vagy kategóriára, kielégítve a felhasználók informatikai biztonsági követelményeit. A **PP** újrafelhasználható, a kifejlesztése során cél volt a funkcionális szabványok támogatása és a megvalósítás, kifejlesztés támogatása a fejlesztési specifikációkkal. A CC tartalmaz néhány védelmi profilt (nagyrészt a tűzfalakra), de koránt sem minden területre, vagyis **a védelmi profilok még nem teljesek!** A hiányzó területekre vonatkozó védelmi profilok elkészítése még várat magára. A védelmi profilokat meghatározhatják a fejlesztők, amikor a biztonsági specifikációt létrehozzák, illetve a nagyobb felhasználói szervezetek is definiálhatnak a számukra fontos területre vonatkozó védelmi profilt a CC-ben meghatározott követelményeket betartva.

Példák védelmi profilokra:

- Üzleti rendszerek biztonsága 1.:
  Kisebb termelői rendszerek alapszintű, ellenőrzött hozzáférés-védelme.
- Üzleti rendszerek biztonsága 3.:

Adatbázis-kezelő rendszerek, többfelhasználós operációs rendszer környezetben. A felhasználóazonosítás egyedi, a hozzáférési jogosultság rendszer szerepkörökön alapul.

- Különböző tűzfalak védelmi profiljai:
  - Hálózati/szállítási szinten működtetett csomagszűrő tűzfal
  - Application Gateway tűzfal
  - USA Kormányzati tűzfal

A védelmi profil tartalmazza többek között:

- a vizsgált rendszer környezete, ezen belül:
  - a rendszerre jellemző releváns fenyegetések felsorolását,
  - a belső szabályzatok, eljárások felsorolását, amelynek a vizsgált rendszer meg kell hogy feleljen,
  - a rendszer fizikai és személyi környezetével szemben támasztott követelményeket határozza meg, amelyek biztosítása elengedhetetlen a biztonságos működéshez.
- A biztonsági követelményeket:
  - A vizsgált rendszer funkcionális biztonsági követelményei, valamint a megcélzott biztonsági osztály meghatározása (EAL1-7).
  - Az IT környezet biztonsági követelményeinek meghatározása.

A CC funkcionális követelményrendszere gyakorlatilag egy funkcionális komponenskatalógus, amelyből összeállítható a vizsgált rendszerre *(Target of Evaluation, TOE)* vonatkozó funkcionális biztonsági követelményrendszer. A követelmények *Osztályokra,* azon belül *családokra* oszlanak. A családokon belül a komponensek már egyedi, konkrét követelményeket fogalmaznak meg. A gyakorlati megvalósításban egyes komponensek egy-egy csoportját, amelyek akár különböző osztályokból származhatnak, „összecsomagolnak".

Az alapvető funkcionális biztonsági követelményosztályok a következők:

- **FAU:** Audit *(Security Audit)*
- **FCO:** Kommunikáció *(Communication)*
- **FCS:** Kriptográfiai funkciók *(Cryptographic support)*
- **FDP:** Adatvédelem *(User data protection)*
- **FIA:** Azonosítás, hitelesítés *(Identification and Authentication)*
- **FMT:** Biztonságmenedzsment *(Security management)*
- **FPR:** Személyes adatok védelme *(Privacy)*
- **FPT:** Biztonsági funkciók védelme *(Protection of then TOE Security functions)*
- **FRU:** Erőforrás-gazdálkodás (*Resource utilization)*
- **FTA:** Hozzáférés-védelem *(TOE Access)*
- **FTP:** Megbízható kommunikációs csatornák *(Trusted path/Channels)*

A biztonsági követelmények biztonsági osztályokba (security assurance) vannak sorolva, elsősorban a forrásként használt követelményrendszerekkel való kompatibilitás, összehasonlíthatóság miatt. A definiált hét osztály **EAL1 – EAL7** (ang.: *Evaluation Assurance Level*) rövid jellemzése az alábbiakban foglalható össze.

- **EAL1:** Funkcionálisan tesztelt:
  Minimális – gazdaságossági megfontolásokkal indokolható – védelmi szint, csak a legnyilvánvalóbb hibákat detektálja a lehető legkisebb költséggel. Kicsi az esélye annak, hogy a rejtett gyengeségek kiderüljenek.
- **EAL2:** Strukturálisan tesztelt:
  A létező szabványok megfelelő alkalmazásával, kellő odafigyeléssel minimálisan növelt fejlesztőiráfordítás-költséggel megvalósítható védelmi szint. Olyan esetben használható, ha a TOE (védett objektum) alacsony vagy közepes védelmi szintet igényel, ugyanakkor a fejlesztés teljes folyamata nem elérhető, nem befolyásolható.
- **EAL3:** Módszertanilag tesztelt és ellenőrzött:
  Közepes szintű, de alaposan ellenőrzött védelmi igények esetén megkövetelt védelmi szint. Jellemzője a „Szürke doboz" tesztelés.
- **EAL4:** Módszertanilag tervezett, tesztelt és auditált:
  Gazdaságossági szempontból valószínűleg ez a még elérhető legmagasabb védelmi szint. Szigorú, biztonsági szempontokat figyelembe vevő, de nem túlságosan specializált tervezési folyamat jellemzi.
- **EAL5:** Félformális módszerrel tervezett és tesztelt:
  Már a rendszer tervezése is az EAL5 szintű biztonsági követelmények kielégítése céljából történik.
- **EAL6:** Félformális módon ellenőrzött tervezés és tesztelés:
  Csak speciális biztonsági tervezési, fejlesztési technikákkal megvalósítható biztonsági szint, ami célszerűen biztonsági termékek tervezésénél és magas kockázatú rendszereknél alkalmazható.

- **EAL7:** Formálisan ellenőrzött tervezés és tesztelés:
  Az elméletileg még megvalósítható lehető legmagasabb védelmi szint. Gyakorlatilag csak kísérleti jellegű, jól definiálható funkcionalitással rendelkező rendszerek esetén valósítható meg.

A CC (az ITSEC-hez és TCSEC-hez viszonyított) előnyei közé sorolandó, hogy:

- precízebb, nem annyira általános a benne megfogalmazott követelményrendszer;
- jobban testre szabható;
- szükség esetén a felhasználó is képes védelmi profilt létrehozni.

A CC kiterjeszthető, bővíthető, a jelenleg még benne nem szereplő funkcionalitásokat be lehet építeni a kiterjesztési kritériumok betartásával.

Ugyanakkor még mindig kevés a létező, felhasználható védelmi profil. A CC precízebben megfogalmazott követelményei ellenére nagyobb szaktudást követel meg a szakemberektől. Amint az összes jelentős termékcsoportra elérhető lesz a védelmi profil, várhatóan a CC jelentősége is felértékelődik.

3.5. ISO/IEC 17799 és BS 7799 szabványok

A Nemzetközi Szabványügyi Szervezet 2000 augusztusában a BS 7799 1. részét az **„A Code of Practice for Information Security Management"** (magyarul: Az informatikai biztonság[5] menedzsmentjének gyakorlati kódexe) változatlan szerkezetben és gyakorlatilag változatlan tartalommal nemzetközi szabványnak fogadta el ISO/IEC 17799 néven. Az ISO/IEC 17799 alapvetően abban különbözik a korábbi informatikai biztonsági ajánlásoktól, hogy a biztonsági követelményeket, intézkedéseket a szervezet üzleti céljaiból és stratégiájából vezeti le. Az eddig többségében termékorientált szemléletet egy szervezeti szintű informatikai biztonságmenedzsment központú szemlélet váltja fel. Ezt tükrözi vissza a dokumentum szerkezete is, amely négy alapszempontra épül:

- szervezet;
- IT termék és rendszer, valamint annak fizikai és személyi környezete; szolgáltatási partner;
- üzleti partner

orientált biztonsági követelmények és intézkedések.

[5] Mivel az informatikai rendszerben kezelt információk biztonságáról van szó, ezért az *„Information Security"* kifejezést az *„informatikai biztonság"* kifejezéssel azonos értelműnek vesszük, és úgy is fordítjuk.

Az ISO/IEC 17799 a következő főbb fejezetekre oszlik:

1. Terjedelem
2. Fogalmak és meghatározások
   - 2.1. Informatikai biztonság
   - 2.2. Kockázatelemzés
   - 2.3. Kockázatmenedzsment
3. Biztonságpolitika
   - 3.1. Informatikai biztonságpolitika
4. Biztonsági szervezet
   - 4.1. Az informatikai biztonság szervezeti struktúrája
   - 4.2. Előírások a külső személyek általi hozzáférésekkel kapcsolatban
   - 4.3. Informatikai biztonság outsourcing esetén
5. Az eszközök biztonsági besorolása és ellenőrzése
   - 5.1. Számadási kötelezettségek az eszközökkel kapcsolatban
   - 5.2. Az információk biztonsági osztályozása
6. Személyi biztonság
   - 6.1. Informatikai biztonság a felvételnél és a munkaköri leírásokban
   - 6.2. Felhasználói képzés
   - 6.3. Biztonsági és üzemzavarok kezelése
7. Fizikai és környezeti biztonság
   - 7.1. Biztonsági szegmensek
   - 7.2. A berendezések fizikai védelme
   - 7.3. Általános védelmi intézkedések
8. Számítógépes és hálózati szolgáltatások és üzemeltetés menedzsmentje
   - 8.1. Üzemeltetési eljárások és feladatok
   - 8.2. IT rendszerek tervezése és átvétele
   - 8.3. Védelem rosszindulatú programok ellen
   - 8.4. Operátori tevékenységek
   - 8.5. Hálózatmenedzsment
   - 8.6. Az adathordozók biztonságos kezelése
   - 8.7. Adatok és programok cseréje
9. Hozzáférés-menedzsment
   - 9.1. A hozzáférés-ellenőrzés üzleti követelményei
   - 9.2. A felhasználói hozzáférés menedzsmentje
   - 9.3. A felhasználó feladatai
   - 9.4. A hálózati szintű hozzáférések menedzsmentje
   - 9.5. Az operációs rendszer szintű hozzáférések ellenőrzése
   - 9.6. Alkalmazás szintű hozzáférések vezérlése
   - 9.7. Hozzáférés a biztonsági monitoring rendszerhez és használata
   - 9.8. Mobil IT tevékenység, távmunka


Figyelj jól!

10. Az IT rendszerek fejlesztése és karbantartása
    10.1. Az IT rendszerek informatikai biztonsági követelményei
    10.2. Biztonság a felhasználói rendszerekben
    10.3. Rejtjelzés alapú ellenőrző eszközök
    10.4. Rendszerszintű adatállományok védelme
    10.5. Informatikai biztonság a fejlesztési és a karbantartási folyamatokban
11. Üzletmenet-folytonosság menedzsment
    11.1. Üzletmenet-folytonosság menedzsment területei
12. Megfelelés a jogszabályoknak és a belső biztonsági szabályzatoknak
    12.1. A jogszabályi előírások betartása
    12.2. Az informatikai biztonságpolitikának és a műszaki követelményeknek való megfelelés
    12.3. Megfontolások a rendszer biztonsági ellenőrzésére


Tanuld meg!

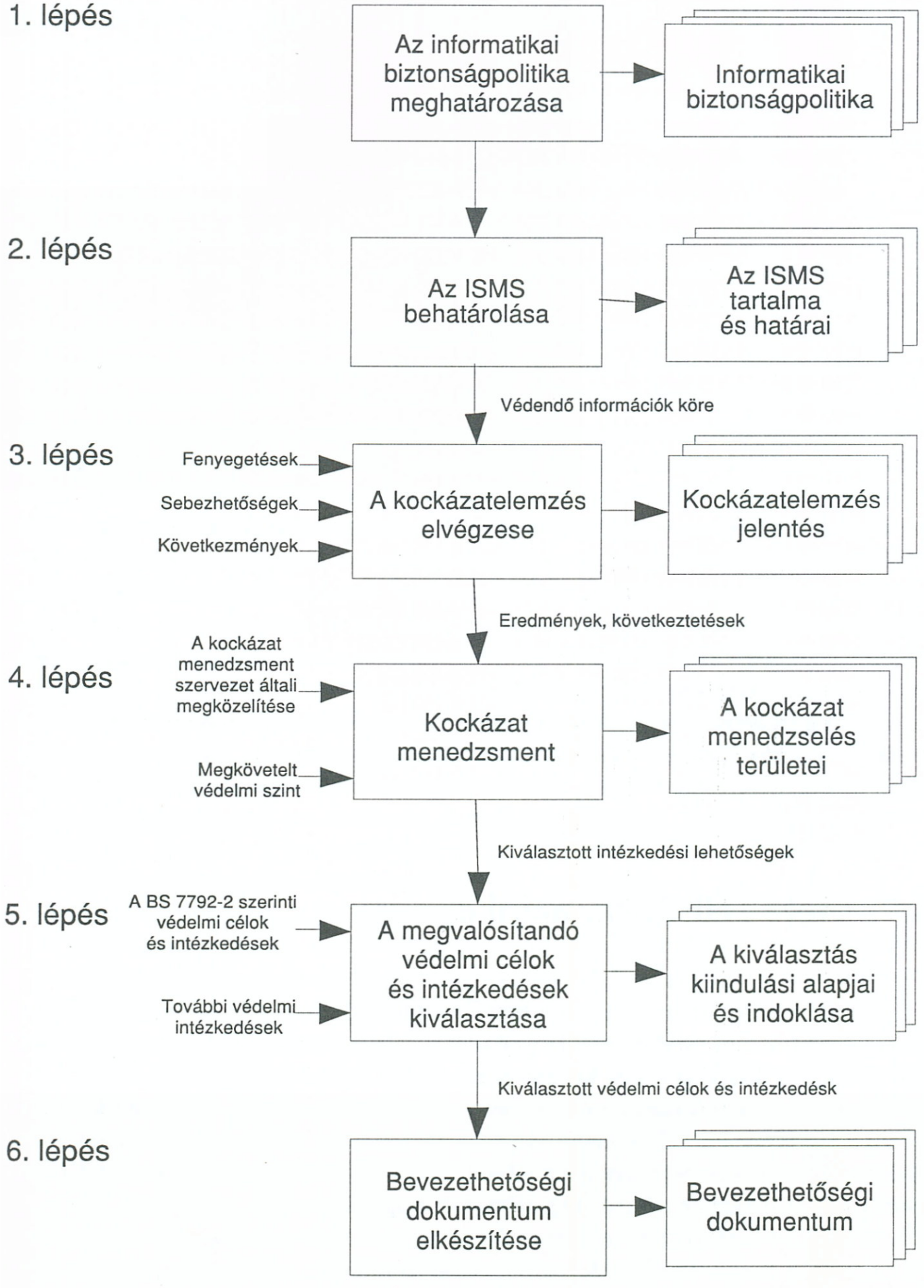
A szabvány szerkezete jól tükrözi azt a sokrétű szempontrendszert, amely a szervezeti szintű informatikai biztonságtól az informatikai rendszeren keresztül, annak személyi és fizikai környezetéig terjed. A szabvány a főbb fejezeteket még további pontokra bontja, és minden ponton tartalmazza az adott pontban megjelölt területen megvalósítandó biztonsági intézkedések célját és a területen figyelembe veendő, illetve megvalósítandó védelmi követelményeket, intézkedéseket.

Ellentmondásos, hogy az ISO/IEC 17799 csak a figyelembe veendő biztonsági követelményeket és a megvalósítandó védelmi intézkedéseket írja le, de nem foglalkozik a megfelelőségi és ellenőrzési követelményekkel. Ezt a BS 7799 *„Specification for Information Security Management Systems"* (Az informatikai biztonsági menedzsment rendszerének specifikációja) című dokumentum 2. része tartalmazza, amely brit szabvány (de még nem ISO szabvány), és amelyet néhány európai ország is, például Norvégia és Svájc egyes pénzintézetei is alkalmaznak.

A BS 7799 2. rész 3. fejezete leírja a szervezeti szintű Informatikai Biztonsági Menedzsment Rendszer (Information Security Management System, ISMS) kialakítási folyamatát, amelyet a **3.1.** ábra ábrázol. A jobb oldalon az Informatikai Biztonság Menedzsment Rendszer létrehozása közben készítendő dokumentumok láthatók. Ebben a fejezetben e dokumentumok tartalma és kezelési módja is meghatározásra kerül.

A BS 7799 2. rész 4. fejezete a szervezet menedzsmentje szempontjából megfogalmazva – az 1. rész szerkezetét követve – meghatározza azokat a követelményeket, amelyek az 1. részben leírt védelmi intézkedések megvalósítása és fenntartása ellenőrzésének a viszonyítási alapját képezik.

A nemzetközi gyakorlatban egyre jobban terjed, hogy egy szervezet menedzsmentje és belső ellenőrző szervei által végrehajtott ellenőrzések mellett megfelelő felkészülés után az ISO/IEC 17799 (BS 7799) szabványnak való megfelelést bizonyító független auditot kérnek a nemzeti akkreditációs testülettől, amely megfelelő eljárás során egy akkreditált, független tanúsító céget választ ki az audit elvégzésére. Ez az eljárás emlékeztet az ISO 9000 szabványsorozat szerinti auditálásra.


1. lépés
Az informatikai biztonságpolitika meghatározása
Informatikai biztonságpolitika
2. lépés
Az ISMS behatárolása
Az ISMS tartalma és határai
Védendő információk köre
3. lépés
Fenyegetések
Sebezhetőségek
Következmények
A kockázatelemzés elvégzese
Kockázatelemzés jelentés
Eredmények, következtetések
4. lépés
A kockázat menedzsment szervezet általi megközelítése
Megkövetelt védelmi szint
Kockázat menedzsment
A kockázat menedzselés területei
Kiválasztott intézkedési lehetőségek
5. lépés
A BS 7792-2 szerinti védelmi célok és intézkedések
További védelmi intézkedések
A megvalósítandó védelmi célok és intézkedések kiválasztása
A kiválasztás kiindulási alapjai és indoklása
Kiválasztott védelmi célok és intézkedésk
6. lépés
Bevezethetőségi dokumentum elkészítése
Bevezethetőségi dokumentum

3.1. ábra

3.6. INFOSEC – Informatikai biztonság a NATO-ban

Az INFOSEC *(information security)* az informatikai biztonság NATO-n belüli értelmezése, amely szerint:

„Az informatikai biztonság biztonsági intézkedések alkalmazása annak érdekében, hogy a kommunikációs, információs és más elektronikus rendszerekben tárolt, feldolgozott és átvitt adatok védelme biztosítva legyen a ***bizalmasság, sértetlenség és rendelkezésre állás*** *elvesztésével szemben, függetlenül az események szándékos vagy véletlen voltától."*

Az INFOSEC két nagy területet foglal magában: a *kommunikációs biztonságot (Communication Security, COMSEC)* és a *számítógépes rendszerek biztonságát (Computer Security, COMPUSEC).*

Kommunikációs biztonság az az állapot, amelyben a (tele)kommunikációs eszközök a *bizalmasság, hitelesség, sértetlenség, rendelkezésre állás* elvesztésével szemben védettek. A (tele)kommunikációs rendszereken továbbított adatok védelme a gyakorlatban a kriptográfiai eszközök felhasználásával valósul meg. A rejtjelző eszközök biztosítják, hogy az adatok illetéktelen kezekbe kerülve ne kompromittálódjanak. Az elektromágneses kisugárzással szembeni védelem (TEMPEST) is a kommunikációs biztonság területéhez tartozik, melynek során meg kell tudnunk akadályozni, hogy akár aktív, akár passzív eszközök alkalmazásával minősített adatok illetéktelen kezekbe kerüljenek.

Számítógép-biztonság az az állapot, amelyben az informatikai rendszerek a *bizalmasság, sértetlenség, rendelkezésre állás* elvesztésével szemben védettek. A számítógépes biztonság a hardver, szoftver és firmware biztonságot foglalja magában.

3.7. MeH ITB 8. sz. ajánlás

A Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) **„Informatikai biztonsági módszertani kézikönyv"** címet viselő, 1994-ben kiadott MeH ITB 8. számú ajánlása a brit kormány Központi Számítógép és Távközlési Ügynökség (Central Computer and Telecommunications Agency) „CCTA Risk Analysis and Management Method" *(CRAMM)* és az észak-rajna-vesztfáliai kormány „Informationtechnik Sicherheitshandbuch" felhasználásával, valamint az EU informatikai ajánlásai és a hazai jogszabályok alapján készült.

A kézikönyv tájékoztatja az intézmény-szervezetének vezetőségét az informatikai biztonság megteremtésének legfontosabb elemeiről, és célja felkészíteni a szervezetet az informatikai biztonsági koncepciójának kialakítására. A biztonsággal kapcsolatos legfontosabb tudnivalók, valamint az informatikai biztonság és a szer-

vezet összbiztonsága közötti összefüggések meghatározó elemei a kézikönyvhöz csatolt mellékletekben találhatók meg.

A MeH ITB 8. számú ajánlását mint az informatikai biztonság – CRAMM alapú – kockázatelemzési módszertanát a közigazgatás területén kívül is elterjedten használják.

3.8. MeH ITB 12. sz. ajánlás

A Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága 1996-ban adta ki 12. számú ajánlását az *„Informatikai Rendszerek Biztonsági Követelményei"* címen.

Ez a dokumentum lefedi az informatikai biztonság egészét, azaz az *adminisztratív,* a *fizikai* és a *logikai védelem* területeit. Az ajánlás komplex szemléletéből adódóan kiterjed mind az informatikai rendszer környezetére, mind magára az informatikai rendszerre. A 12. sz. ajánlás az érvényes hazai jogszabályok, szabványok, valamint a hazai és nemzetközi ajánlások – elsősorban az ITSEC – figyelembevételével *reális és megbízható alapot* nyújt egyrészt a működő, másrészt a megvalósítás előtt álló informatikai rendszerek és környezetük fizikai, logikai és adminisztratív védelmi követelményeinek konkrét megfogalmazásához, a védelmi rendszerek továbbfejlesztéséhez, illetve megvalósításához. Ez a jegyzet sok tekintetben ezt az ajánlást veszi alapul.

Az ajánlás az informatikai biztonság két területére (az *információvédelem* és a *megbízható működés*), területenként 3 biztonsági osztályt határoz meg, az osztályba sorolás alapja az adott osztályban tárolandó adatok érzékenysége, azaz a sérülésükből eredő károk nagysága. A biztonsági követelmények az osztályok szerint egyre emelkedő szintű biztonságot nyújtanak. A definiált biztonsági osztályok és azon adatok köre, amelyeket az adott osztálynak megfelelő szintű védelemmel kell ellátni:

- információvédelmi **alapbiztonsági** (**IV-A**) osztály:
  Személyes adatok, üzleti titkok, pénzügyi adatok, illetve az intézmény belső szabályozásában hozzáférés-korlátozás alá eső (például egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.
- információvédelmi **fokozott** biztonsági (**IV-F**) osztály:
  A szolgálati titok, valamint a nem minősített adatok közül a különleges személyes adatok, nagy tömegű személyes adatok, banktitkok, közepes értékű üzleti titkok feldolgozására, tárolására is alkalmas rendszer biztonsági osztálya.
- információvédelmi **kiemelt** biztonsági (**IV-K**) osztály:
  Az államtitok, a katonai szolgálati titok, valamint a nem minősített adatok közül a nagy tömegű különleges személyes adatok és nagy értékű üzleti titkok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.
- megbízható működési **alapbiztonsági** (**MM-A**) osztály:
  A 95,5%-nál alacsonyabb rendelkezésre állású rendszerek biztonsági osztálya.

- megbízható működési **fokozott** biztonsági (**MM-F**) osztály:
  A 99,5%-nál alacsonyabb rendelkezésre állású rendszerek biztonsági osztálya.
- megbízható működési **kiemelt** biztonsági (**MM-K**) osztály:
  A 99,95%-os vagy magasabb rendelkezésre állású rendszerek biztonsági osztálya.

Az *Informatikai Rendszerek Biztonsági Követelményei* biztonsági osztályonként, a védelmi területek szerinti csoportosításban intézkedési lista formájában került kiadásra. Az intézkedések az informatikai rendszer elemei szerinti bontásban kerültek meghatározásra, a következő sorrendben:

- Általános intézkedések;
- Infrastruktúra;
- Hardver, szoftver;
- Adathordozók;
- Dokumentációk;
- Adatok;
- Kommunikáció, osztott rendszerek;
- Személyek.

3.9. MeH ITB 16. sz. ajánlás

Common Criteria	MeH ITB 16. számú ajánlása	Az informatikai biztonság – jegyzet
TOE *Target of Evaluation*	**ÉT** Értékelés tárgya	**TOE** Vizsgált rendszer
PP *Protection Profile*	**VP** Védelmi profil	**PP** Védelmi profil
ST *Security target*	**BRT** Biztonsági RendszerTerv	**ST** Védelmi cél
TSF *TOE Security functions*	**ÉTBF** Az Értékelés Tárgyának Biztonsági funkciói	**TSF** Biztonsági funkciók
TSP *TOE Security Policy*	**ÉTBP** Az Értékelés Tárgyának Biztonsági politikája	**TSP** Biztonsági politika
EAL *Assurance Class*	**ÉGSZ** Értékelési Garancia Szint	Biztonsági osztály

3.3. táblázat

A Common Criteria 1.0 változatának hazai feldolgozása. 1998-ban a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) 16. számú ajánlásaként, „Common Criteria (CC), az informatikai termékek és rendszerek biztonsági értékelésének módszertana" címmel adta ki. Az ajánlás tartalma sok tekintetben megfelel a CC 2.0 verziónak is, de tulajdonképpen a CC 1.0 verzió adaptálásának tekinthető. Felhasználása esetén ezt mindenképpen figyelembe kell venni. Fontos szempont a terminológiai eltérések tisztázása.

A **3.3.** táblázatban összefoglalásképpen felsoroljuk a legfontosabb kifejezéseknek a CC-ben, a MeH ITB 16. sz. ajánlásában írt, illetve a jelen jegyzetben használt megfelelőjét az alkalmazott rövidítésekkel együtt.

3.10. Az egyes ajánlások biztonsági osztályai közötti megfelelés

Az előbbiekben leírt biztonsági követelmények által definiált biztonsági szintek többékevésbé megfeleltethetők egymásnak a bennük meghatározott követelmények alapján. Az **3.4.** táblázat összefoglalóan ábrázolja az egyes ajánlások biztonsági szintjei közötti összefüggést. Az ISO/IEC 17799 (BS 7799) szabvány nem szerepel a megfeleltetésben, mert explicit biztonsági osztály meghatározásokat nem tartalmaz, csupán követelményként szerepel ebben a szabványban a biztonsági osztályok meghatározása.

TCSEC	ITSEC	X/OPEN	CC	12. sz. ajánlás
B3	F-B3		EAL6	
B2	F-B2	X-PRIV	EAL5	
B1	F-B1	X-MAC	EAL4	
C2	F-C2	X-DAC, X-AUDIT	EAL3	A F K
C1	F-C1	X-BASE	EAL2	

3.4. táblázat

A 12. sz. ajánlás biztonsági osztályainak rövidítései:

A = alapbiztonsági osztály; **F** = fokozott biztonsági osztály; **K** = kiemelt biztonsági osztály.

A különböző ajánlások biztonsági osztályainak összehasonlítása akkor válik a gyakorlatban is hasznossá, amikor például egy konkrét rendszerhez kell védelmi tervet készíteni. Ehhez a védelmi rendszertervhez ki kell választani az operációs rendszert, az adatbázis-kezelőt, a tűzfal megoldást stb. Ilyenkor könnyen beleütközhetünk abba a problémába, hogy a piacon kapható termékek nem mindegyike rendelkezik biztonsági minősítéssel, de ha igen, akkor is eltérő szabványok alapján. Ebben nyújt segítséget a **3.4.** táblázat.

4. Informatikai biztonsági követelmények

4.1. Bevezetés

Minden rendszer létrehozásakor pontosan meg kell határozni, hogy létrehozásának mik a céljai, milyen feladatokat lásson el, röviden milyen követelményeknek feleljen meg. Ha ezt a lépést elhagyjuk, könnyen jutunk olyan helyzetbe – amely a gyakorlatban gyakran előfordul –, hogy a létre hozott rendszer nem olyan, mint amit vártunk.

Mit jelent ez az általános megállapítás az informatikai biztonsági rendszerekkel kapcsolatban? Azt, hogy olyan védelmi rendszert kell létrehozni, amely az informatikai rendszer által kezelt adatok összes alapfenyegetettsége szempontjából megfelelő (azaz teljes körű, zárt és kockázatarányos) védelmet nyújt. Ebben a kijelentésben van egy nehezen értelmezhető kijelentés? A „megfelelő". Mikor megfelelő a védelmi rendszer? A teljes körűség viszonylag kisebb problémát okoz, mert arra kell törekednünk, hogy a védelem kialakításakor minden rendszerelemet figyelembe vegyünk.

A zártság esetében minden potenciális fenyegetést számba kell venni, amely már nem valósítható meg mindig maradéktalanul, de az esetek többségében ez a probléma is kezelhető.

A kockázatarányossággal azonban már több a gond. Először is meg kell ismerni a kockázatokat. Ha ez már megtörtént, akkor észrevesszük, hogy azok nagyságuk függvényében egy bizonyos nagyságú tartományban oszlanak el. Hogyan értékeljük őket, és milyen kockázati szintre méretezzük a biztonsági rendszert. Milyen legyen a biztonsági funkciók választéka, mechanizmusa és erőssége? Ha túl alacsony, akkor ugyan olcsóbb lesz a védelmi rendszer, de nem lesz megfelelő, mert a védelmi szintje a kelleténél alacsonyabb lesz. Ha túl magas lesz, akkor viszont a költségekkel gyűlik meg a bajunk, viszont jobb lesz a biztonság. Hogyan mérjük a kockázatok, a szükséges védelem, a biztonság szintjét, például, hogy egy banki objektum egyes területeit az ott becsült biztonsági kockázatok szintjének megfelelően melyik biztonsági osztályba sorolják. A besorolás alapja a kockázat, illetve ennek egyik összetevője a kár szintje, amelyekre bizonyos határokat „ültetve" osztályokat lehet definiálni. A MeH ITB 12. sz. ajánlás készítői is hasonlóan jártak el, amikor a kárszintek alapján informatikai biztonsági osztályokat definiáltak.

Ez a biztonsági osztály definíció teljes összhangban van az amerikai TCSEC és az európai ITSEC ajánlások biztonsági osztály szerkezetével, azonban a MeH ITB 12. ajánlása az említett ajánlások osztályai közül csak a hazai gyakorlatban

releváns, „középen" elhelyezkedő alap, fokozott és kiemelt biztonsági osztályokat definiálta a **3.8.** fejezet szerint, és csak ezekhez illeszkedő követelményeket adott meg. A TCSEC szerinti D biztonsági osztály csoportnak (minimális védelem) megfelelő szintű informatikai rendszerekkel ugyan gyakran lehet találkozni, azonban a MeH ITB 12. sz. ajánlásban nem látszott célszerűnek erre a szintre követelményeket megadni, mert az esetek többségében e rendszerek védelmi szintjét alapbiztonsági szintre kell emelni. Az A biztonsági osztály csoport követelményei olyan magas szintet képviselnek, amelyek kielégítése csak néhány speciális rendszer esetében jön szóba. Ezek a rendszerek amúgy is teljesen zárt körben kezeltek.

A MeH ITB 12. sz. ajánlás viszont szélesebb követelménykört ölel fel, mint az ITSEC és a TCSEC, mert azok szinte kizárólag csak a logikai védelemre vonatkozó követelményekkel foglalkoznak, míg a MeH ITB 12. sz. ajánlás az összes rendszerelem csoportra, így az infrastruktúra és a különösen fontos személyek csoportjára is követelményeket szab.

Az informatikai biztonság területén figyelembe vett kár egy összetett fogalom, amely a következő kárfajtákat foglalja magában:

- dologi károk, amelyeknek közvetlen vagy közvetett költségvonzatuk van, például:
  - károsodás az infrastruktúrában (épület, vízellátás, áramellátás, klímaberendezés stb.),
  - károsodás az informatikai rendszerben (hardver, hálózat sérülése stb.),
  - a dologi károk bekövetkezése utáni helyreállítás költségei;
- károk a politika és a társadalom területén, például:
  - állam- vagy szolgálati titok megsértése,
  - személyiséghez fűződő jogok megsértése, személyek vagy csoportok jó hírének károsodása,
  - bizalmas adatok nyilvánosságra hozatala,
  - hamis adatok nyilvánosságra hozatala,
  - közérdekű adatok titokban tartása,
  - bizalomvesztés hatóságokkal, felügyeleti szervekkel szemben;
- gazdasági károk
  - pénzügyi károk,
  - lopáskárok,
  - az intézmény vagy cég arculatának (image) romlása,
  - rossz üzleti döntések hiányos vagy hamis információk alapján;
- károk az informatikai személyzet, illetve a felhasználók személyi biztonsága területén, például: személyek megsérülése, megrokkanása (például áramütés következtében);
- károk a hatályos jogszabályok és utasítások megsértéséből adódóan;
- károk a tudomány területén
  - kutatások elhalasztódása,

- eredmények idő előtti, illetve hamis név alatti nyilvánosságra kerülése,
- tudományos eredmények meghamisítása.

Az informatikai biztonsági osztályok meghatározásához a fenti kártípusokat bizonyos mértékben összevontan a következők szerint vesszük figyelembe:

- *közvetlen anyagi* (például a mindenkori amortizált értékkel vagy az elmaradt haszonnal arányos) kár,
- *közvetett anyagi* (például a helyreállítási költségekkel, perköltségekkel arányos) kár,
- *társadalmi-politikai, erkölcsi* károk,
- *személyi sérülés, haláleset,*
- jogszabály által védett adatokkal történő visszaélés vagy azok sérülése (jogsértés).

A fontosabb kártípusokhoz kvantitatív jellemzők tartományait rendelve kialakítható egy kárérték-osztályozás, amely segítségével a fenyegetett objektumok – esetünkben az informatikai rendszerek – biztonsági osztályokba sorolhatók. A biztonság értékeléséhez a következő kárérték szinteket definiálta MeH ITB 12. sz. ajánlás:

- ***„0": jelentéktelen kár***
  - közvetlen anyagi kár: – 10 000 Ft,
  - közvetett anyagi kár 1 embernappal állítható helyre,
  - nincs bizalomvesztés, a probléma a szervezeti egységen belül marad,
  - testi épség jelentéktelen sérülése egy-két személynél,
  - nem védett adat bizalmassága vagy hitelessége sérül.
- ***„1": csekély kár***
  - közvetlen anyagi kár: – 100 000 Ft-ig,
  - közvetett anyagi kár 1 emberhónappal állítható helyre,
  - társadalmi-politikai hatás: kínos helyzet a szervezeten belül,
  - könnyű személyi sérülés egy-két személynél,
  - hivatali, belső (intézményi) szabályozóval védett adat bizalmassága vagy hitelessége sérül.
- ***„2": közepes kár***
  - közvetlen anyagi kár: – 1 000 000 Ft-ig,
  - közvetett anyagi kár 1 emberévvel állítható helyre,
  - társadalmi-politikai hatás: bizalomvesztés a szervezet középvezetésében, bocsánatkérést és/vagy fegyelmi intézkedést igényel, a káreseménnyel kapcsolatos információk, hírek, cikkek jelennek meg nyilvános fórumokon, médiában, a szervezet jó hírneve sérül,
  - több könnyű vagy egy-két súlyos személyi sérülés,
  - személyes adatok bizalmassága vagy hitelessége sérül,
  - egyéb jogszabállyal védett (például üzleti, orvosi) titok bizalmassága vagy hitelessége sérül.

➠ *„3": nagy kár*
- közvetlen anyagi kár: – 10 000 000 Ft-ig,
- közvetett anyagi kár 1-10 emberévvel állítható helyre,
- társadalmi-politikai hatás: bizalomvesztés a szervezet felső vezetésében, a középvezetésen belül személyi konzekvenciák, a káresemény súlyosan veszélyezteti a szervezet jó hírnevét,
- több súlyos személyi sérülés vagy tömeges könnyű sérülés,
- szolgálati titok bizalmassága vagy hitelessége sérül,
- szenzitív személyes adatok, nagy tömegű személyes adat bizalmassága vagy hitelessége sérül,
- banktitok, közepes értékű üzleti titok bizalmassága vagy hitelessége sérül.

➠ *„4": kiemelkedően nagy kár*
- katonai, szolgálati titok bizalmassága vagy hitelessége sérül,
- közvetlen anyagi kár: – 100 000 000 Ft-ig,
- közvetett anyagi kár 10-100 emberévvel állítható helyre,
- társadalmi-politikai hatás: súlyos bizalomvesztés a szervezet felső vezetésén belül személyi konzekvenciával, a káresemény következményei súlyosan veszélyeztetik a szervezet működésbeli és/vagy gazdasági helyzetét,
- egy-két személy halála vagy tömeges sérülések,
- államtitok bizalmassága vagy hitelessége sérül,
- nagy tömegű szenzitív személyes adat bizalmassága vagy hitelessége sérül,
- nagy értékű üzleti titok bizalmassága vagy hitelessége sérül.

➠ *„4+": katasztrofális kár*
- közvetlen anyagi kár: 100 000 000 Ft felett,
- közvetett anyagi kár több mint 100 emberévvel állítható helyre,
- társadalmi-politikai hatás: súlyos bizalomvesztés a szervezet felső vezetésén belül és kormányszinten, személyi konzekvenciával,
- tömeges halálesetek,
- különösen fontos (nagy jelentőségű) államtitok bizalmassága vagy hitelessége sérül.

A fenti definíciókban szereplő közvetlen anyagi kárszintek számszerűsített értékei a tapasztalatok szerint egy 2-3000 munkatárssal, 1500-2000 munkaállomással rendelkező vállalat esetében jó becslést adnak. Minden konkrét kockázatelemzéses vizsgálat vagy adatérzékenység-elemzés esetén az első lépés az adott vállalat gazdasági jellemzőit figyelembe véve ellenőrizni a kárértékszint definíciókban levő számértékek realitását. **Szükség szerint ezeket korrigálni kell, mert a kockázatok szintje és a biztonsági osztályba sorolás csak így lesz a realitásoknak megfelelő.**

§ Az informatikai rendszerek biztonsági osztályaira vonatkozó, a kárszint fogalmán alapuló általános definíció a következő:

➠ ***alapbiztonsági** követelményeket kielégítő informatikai rendszert kell létrehozni akkor, ha a rendszerben maximum „2", azaz legfeljebb **közepes kárértékű** esemény bekövetkezése fenyeget;*

- ***fokozott biztonsági** követelményeket kielégítő informatikai rendszert kell létrehozni akkor, ha a rendszerben maximum „3", azaz legfeljebb **nagy kárértékű** esemény bekövetkezése fenyeget;*
- ***kiemelt biztonsági** követelményeket kielégítő informatikai rendszert kell létrehozni akkor, ha a rendszerben a „4+", azaz a **katasztrofális kárértékig** terjedő esemény bekövetkezése fenyeget.*

A biztonsági osztályba sorolás birtokában osztályonként megadhatók azok a követelmények, amelyek teljesítésével a védelmi rendszer az osztályba sorolásnak megfelelő kockázatcsökkentő hatással fog bírni.

A következőkben a teljes körűség elvének megfelelően a követelmények az informatikai rendszerre, valamint annak környezetére terjednek ki a következő csoportosításban:

- *infrastruktúra,*
- *hardverrendszer,*
- *a szoftver- (alap + alkalmazói) rendszer,*
- *kommunikáció, számítógépes hálózatok,*
- *adathordozók,*
- *I/O dokumentumok, dokumentáció,*
- *adatok,*
- *személyek.*

Az informatikai és a kommunikációs rendszer biztonsági funkcióra vonatkozó követelményeknél az ITSEC-ben definiált biztonságifunkció-palettát vesszük figyelembe a következők szerint:

Információvédelem

- Az azonosítás és a hitelesítés folyamatának kialakítása. *(Identification and Authentication).*
- A hozzáférés-jogosultság rendszerének felépítése – jogosultságkiosztás (alanyok/személyek, programok/ – elérési objektumok meghatározása, attribútumok rögzítése, hozzárendelések – megengedő, illetve tiltó módszer a szigorodó követelményekre) *(Access Control).*

A hozzáférés-jogosultság rendszerének két elve szerint kerülhet kialakításra:

- A C1 és C2 osztályokban a hozzáférés-jogosultság kiosztása nem előre meghatározott módon, hanem személyenként vagy felhasználói csoportonként, esetenként kerül meghatározásra. A TCSEC terminológia erre a vezérlési módra a *Discretionary Access Control (DAC)* kifejezést használja.
- A B1 és B2 osztályokban a hozzáférés-jogosultság kiosztása előre meghatározott módon, személyenként vagy felhasználói csoportonként kerül meghatározásra. A TCSEC terminológia erre a vezérlési módra a *Mandatory Access Control (MAC)* kifejezést használja.

- A hozzáférés-ellenőrzés rendszerének megvalósítása – jogosultság-ellenőrzés *(Accountability).*

- A bizonyítékok rendszerének és folyamatának kialakítása *(Audit)*.
- Az adatok sértetlenségének és konzisztenciájának biztosítása *(Accuracy)*.

Megbízható működés

- A megbízható működésre vonatkozó alapfunkció a TCSEC-ben a megbízható szolgáltatások biztosítása *(Reliability of Service)*.
- Ez az alapfunkció a következő fontosabb részfunkciókra bontható:
  - A hibaáthidalás folyamatának kialakítása *(Redundancy)*.
  - Az újraindítási képesség megvalósítása *(Recovery)*.
- A rendszer funkcionalitásának biztosítása *(Functionality)*.

  A funkcionalitást széles értelemben véve a további részfunkciók biztosítják:
  - rendszertervezési és fejlesztési módszertan alkalmazása, beleértve ebbe a biztonsági rendszert is,
  - megfelelő dokumentációs rendszer kialakítása,
  - tesztrendszer és dokumentáció biztosítása, mind a felhasználói, mind a biztonsági rendszer területén.

A védelmi rendszer tervezésekor a fizikai, a logikai és az adminisztratív biztonsági funkciókat, azok mechanizmusát és erősségét úgy kell megválasztani, hogy azok együttes hatása alkalmas legyen az adott fenyegetés által okozott kockázat elviselhető szintre való mérséklésére, a lehető legalacsonyabb költségszinten, azaz törekedni kell a biztonságtervezési *mini-max elv* alkalmazására, amely szerint olyan védelmi rendszert kell tervezni, amellyel minimális költséggel maximális védelem biztosítható.

A MeH ITB 12. sz. ajánlás részletesen tartalmazza az információvédelmi és a megbízható működésbeli osztályokra a biztonsági követelményeket. Ennek megfelelően a 1.2. és 1.3. fejezetekben a követelmények *informatikai biztonsági osztályok* és *rendszerelemek* szerint csoportosítva kerülnek meghatározásra. Tekintve, hogy a MeH ITB 12. sz. ajánlás részletesen tartalmazza a biztonsági követelményeket és a védelmi intézkedéseket, itt csak azokat a legfontosabb követelményeket adjuk meg, amelyeket alkalmazási területtől függetlenül általánosan és minimálisan érvényesíteni javasolt.

A MeH ITB 12. sz. ajánlás használatával az informatikai rendszer információvédelem és megbízható működés szerinti biztonsági osztályba sorolása után már kialakíthatók az adott rendszerre jellemző *védelmi intézkedések,* amelyeket az informatikai rendszerre és annak környezetére a védelmi rendszertervben konkrétan kell meghatározni. Az így kialakított intézkedések alapján már megtervezhető és kialakítható az adott védelmi szint biztosításához szükséges biztonsági rendszer.

A védelemnek egyenszilárdságúnak kell lennie, azaz a követelményrendszert komplexitásban, az összes védelmi területet lefedve és az összes releváns fenyegetést figyelembe véve kell meghatározni, mert csak az így kialakított védelmi rendszer lesz „hézagmentes", vagyis nem rendelkezik olyan nem védett „biztonsági résekkel", amelyeken keresztül megtörténhet a védelmi rendszer megkerülése, a potenciális fenyegetések aktivizálódása és a káresemények bekövetkezése.

4.2. Követelmények az információvédelem területén

4.2.1. Információbiztonsági osztályok az információvédelem területén

Az információvédelem területén a biztonsági osztályokat a következőképpen határoztuk meg a **3.8.** fejezetben:

- Információvédelmi alapbiztonsági osztály:
  Személyes adatok, üzleti titkok, pénzügyi adatok, illetve a szervezet belső szabályozásában hozzáférés-korlátozás alá eső (például egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.
- Információvédelmi fokozott biztonsági osztály:
  A szolgálati titok, valamint a nem minősített adatok közül a különleges személyes adatok, nagy tömegű személyes adatok, banktitkok, közepes értékű üzleti titkok feldolgozására, tárolására is alkalmas rendszer biztonsági osztálya.
- Információvédelmi kiemelt biztonsági osztály:
  Az államtitok, a katonai szolgálati titok, valamint a nem minősített adatok közül a nagy tömegű különleges személyes adatok és nagy értékű üzleti titkok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya.

Az információvédelem fenti biztonsági osztály definíciói úgy függenek össze a 4.1. fejezetben megadott általános biztonsági osztály definíciókkal, hogy az egyes információvédelmi osztályokra jellemző adatkörtípusok bizalmassága, hitelessége vagy sértetlensége sérülésének vagy elvesztésének az általános definíció szerinti osztályra meghatározott szintű kárvonzata lesz.

4.2.2. Alapbiztonsági osztály

4.2.2.1. Az alapbiztonsági osztály minimális követelményei

- Az azonosítás és hitelesítés keretében a hozzáférést jelszavakkal kell ellenőrizni. A jelszómenedzselést úgy kell biztosítani, hogy a jelszó ne juthasson illetéktelenek tudomására, ne legyen könnyen megfejthető, megkerülhető.
- A felhasználók azonosítása egyedi, jellemző, ellenőrizhető és hitelesítésre alkalmas legyen.
- Biztosítani kell a felhasználói azonosítók időszakos vagy végleges tiltását.
- A felhasználók közé sorolandók a természetes személyek, folyamatok vagy egyéb eszközök egyaránt.

- A hitelesítés legáltalánosabb módja a jelszó megadása. Kezelésére az alábbi szabályokat kell alkalmazni:
  - A munkaállomásokon a hitelesítési folyamatban a beírt jelszó összefüggő szövegként ne legyen olvasható.
  - A jelszó és a felhasználó azonosító soha nem kerülhet egy postai küldeménybe, még elektronikus levelezésben sem.
  - A jelszónak minden felhasználó számára szabadon, bármikor megváltoztathatónak kell lennie.
- A felhasználói jelszavakkal kapcsolatban biztosítani kell az alábbi követelményeket:
  - minimális jelszóhossz megadása,
  - a jelszó egyediségét (történeti tárolás),
  - a központi jelszómegadás utáni első bejelentkezéskor a kötelező jelszócserét,
  - a jelszó maximális élettartamát,
  - a jelszó minimális élettartamát,
  - a jelszó zárolását,
  - a jelszóképzés szabályainak meghatározását.
- A rendszer hozzáférés szempontjából érdekes erőforrásaihoz (processzek, fájlok, tároló területek, berendezések) olyan egyedi azonosítót kell rendelni, amely a hozzáférési jogosultság meghatározásának alapjául szolgál.
- Ki kell dolgozni az informatikai rendszerhez történő hozzáférések illetékességi, jogosultsági rendszerét.
- A rendszer felhasználóihoz hozzáférési jogokat kell rendelni. A jogokat minimálisan egyedi, illetve csoporttulajdonosi szinten kell tudni megadni. Az egyértelmű jogosultságszabályozás kialakítása céljából célszerű a felhasználók és a rendszer által nyújtott szolgáltatások biztonsági követelmény-mátrixát felállítani.
- A hozzáférés jogosultság menedzselésénél a szabad belátás szerint esetenként (legtöbbször a rendszer tervezésekor) kialakított *hozzáférés-vezérlés* (Discretionary Access Control, röv.: DAC) elvét kell alkalmazni a következő hozzáférési jogokkal:
  - olvasási jog (betekintés),
  - írási jog (létrehozás, módosítás),
  - törlési jog.
- A rendszernek alkalmasnak kell lennie a hozzáférési jogok egyedi vagy csoportszinten történő megkülönböztetésére és szabályozására.
- A rendszer objektumaihoz (fájlok, eszközök, processzek közötti kommunikációs csatornák) egyedi, illetve csoporttulajdonosokat kell rendelni az objektum létesítésekor. A hozzáférés vezérlése esetén az adott objektumhoz (például fájl) esetenként (például létesítéskor) rendelődnek hozzá a tulajdonosok jogai is.

- A hozzáférési események esetén jogosultság-ellenőrzést kell végrehajtani. A hozzáférés-vezérlés a szubjektumokhoz (felhasználók, processzek) rendelt jogok és az objektumokhoz rendelt tulajdonosok és jogaik összevetése alapján történik.
- A jogosultsági rendszernek támogatnia kell a jogosultságok módosítását, átadását másik személynek, törlését és időleges korlátozását. Új jogosultság kiosztását, a jogosultság törlését vagy átmeneti felfüggesztését csak erre felhatalmazott rendszeradminisztrátor végezheti el.
- A jogosulatlan hozzáférési kísérleteket rögzíteni kell a biztonsági naplóban, amelynek értékelését rendszeresen el kell végezni.
- On-line adatmozgás (tranzakció) kezdeményezésének jogosultságát minden esetben ellenőrizni kell.
- A rendszeradminisztrátorok jogosultsági rendszerének kialakításakor speciális figyelmet kell fordítani a rendszerparancsok és adatállományok használatának szigorú és egyértelműen körülhatárolt szabályozására.
- Az elszámoltathatóság és auditálhatóság biztosítása érdekében olyan regisztrálási és naplózási rendszert (biztonsági napló) kell kialakítani, hogy utólag meg lehessen állapítani az informatikai rendszerben bekövetkezett fontosabb eseményeket, különös tekintettel azokra, amelyek a rendszer biztonságát érintik. Ezáltal ellenőrizni lehessen a hozzáférések jogosultságát, meg lehessen állapítani a felelősséget, valamint illetéktelen hozzáférés megtörténtét.
- A rendszernek képesnek kell lennie minden egyes felhasználó vagy felhasználó csoport által végzett művelet szelektív regisztrálására.

A minimálisan regisztrálandó események a következők:

- rendszerindítások, leállások, leállítások
- rendszeróra-állítások,
- be/kijelentkezések,
- programleállások,
- az azonosítási és hitelesítési mechanizmus használata,
- hozzáférési jog érvényesítése azonosítóval ellátott erőforráshoz,
- azonosítóval ellátott erőforrás létrehozása vagy törlése,
- felhatalmazott személyek műveletei, amelyek a rendszer biztonságát érintik.

A biztonsági naplóban az eseményekhez kapcsolódóan a következő paramétereket kell rögzíteni:

A felhasználó azonosítása és hitelesítése esetén:

– dátum,
– időpont,
– a kezdeményező azonosítója,
– az eszköz (például terminál) azonosítója, amelyről az azonosítás és hitelesítés művelet kezdeményezése történt,
– a művelet eredményessége vagy eredménytelensége.

Olyan *erőforráson kezdeményezett hozzáférési művelet* esetén, amelynél a hozzáférési jogok ellenőrzése kötelező:

– dátum,
– időpont,
– az erőforrás azonosítója,
– a hozzáférési kezdeményezés típusa,
– a művelet eredményessége vagy eredménytelensége.

Olyan *erőforrás létrehozása vagy törlése* esetén, amelynél az ehhez fűződő jogok ellenőrzése kötelező:

– dátum,
– időpont,
– a kezdeményező azonosítója,
– az erőforrás azonosítója,
– a kezdeményezés típusa.

Felhatalmazott felhasználók (például rendszer-adminisztrátorok) olyan *műveletei* esetén, amelyek a rendszer biztonságát érintik:

– dátum,
– időpont,
– a műveletet végző azonosítója,
– az erőforrás azonosítója, amelyre a művelet vonatkozik, például hozzáférési jog megadása, felfüggesztése, elvétele, tároló erőforrás logikai kijelölése vagy megszüntetése, rendszerindítás vagy leállítás.

- A biztonsági napló adatait legalább havonta egy alkalommal ellenőrizni és archiválni kell.
- Meg kell határozni, hogy a biztonsági napló értékelése során mely eseményeket kell jegyzőkönyvezni, melyek azok az események (például illetéktelen hozzáférések, jogosultságokkal való visszaélések), amelyek szankciókat vonnak maguk után, és melyek ezek a szankciók.
- A biztonsági naplók és a jegyzőkönyvek archiválandók, és meghatározandók a megőrzési határidők.
- A biztonsági eseménynapló és a jegyzőkönyvek adatait védeni kell az illetéktelen hozzáféréstől, ezekhez az adatokhoz csak erre felhatalmazott személy férhet hozzá.
- A biztonsági eseménynapló fájlok vizsgálatához és karbantartásához a rendszernek megfelelő eszközökkel és ezek dokumentációjával kell rendelkeznie, ezen eszközök állapotának regisztrálhatónak és dokumentálhatónak kell lennie.
- A rendszerben a biztonsági eseménynapló fájlok auditálásához szükséges eszközöknek lehetővé kell tenniük egy vagy több felhasználó tevékenységének szelektív vizsgálatát.
- Az informatikai rendszer üzemeltetéséről a biztonsági napló mellett üzemeltetési naplót kell vezetni, amelyet az informatikai szervezeti egység felelős

vezetőjének és az informatikai biztonsági felügyelőnek rendszeresen ellenőriznie kell.

- Intézkedési tervet kell kidolgozni arra vonatkozóan, mi történjék illetéktelen hozzáférések, illetve jogosultságokkal való visszaélések esetén, amely során a lehető legnagyobb mértékben meg kell tudni határozni a felelősséget.
- Egy rendszeren belül a különböző adattípusokat olyan mértékben kell elkülönítetten kezelni, hogy megállapítható legyen a hozzáférések jogossága.
- Ki kell alakítani a biztonság belső ellenőrzésének rendszerét, amely során meg kell határozni a felügyeleti és megelőzési tevékenységek eljárásrendjét.
- Az informatikai rendszer üzemeltetéséről nyilvántartást kell vezetni, amelyet az arra illetékes személynek rendszeresen ellenőriznie kell.

4.2.2.2. Infrastruktúra

A fizikai védelmi intézkedések jó részére jellemző, hogy mind az információvédelem, mind a megbízható működés szempontjából védőhatást fejtenek ki. Az ilyen jellegű funkciók követelményeit ebben a pontban foglaltuk össze, a tisztán megbízható működést támogató követelményeket az 4.3. fejezetben az egyes biztonsági osztályok fizikai védelemre vonatkozó pontjaiban adtuk meg.

- A védendő helyiséget minden oldalról legalább a 6 cm vastagságú tömör téglafal szilárdsági mutatóival egyenértékű falszerkezet határolja.
- Az ajtószerkezetek reteszhúzás ellen védettek, az ajtók zárását olyan zár végzi, amely megfelel a prEN 1303 szabvány 3. biztonsági osztály (szabványos) követelményeinek. Az ajtók, ablakok ráccsal nem védett üvegezése összességében min. 6 mm vastagságú.
- Elektronikai jelzőrendszert nem kell kiépíteni (hacsak jogszabály erre nem kötelez). A helyiségen belül személyi felügyeletet csak munkaidőben kell biztosítani. A felügyelet hiányában az ajtókat folyamatosan kulcsra kell zárni, a belépés csak kulccsal vagy munkaidőben beléptető rendszer működtetésével lehetséges.
- A kisugárzás elleni védelmi intézkedések foganatosítása nem indokolt.

4.2.2.3. Hardver/szoftver rendszer

- A számítástechnikai eszközökre a vagyonvédelem szempontjából a MABISZ ajánlásait kell alkalmazni.
- A PC-s munkaállomásokat a felhasználói igények figyelembevételével úgy kell konfigurálni, hogy a felhasználóhoz kötött jelszóhasználat biztosított, illetve az illetéktelen flopihasználat megakadályozható legyen.
- A flopiról történő rendszerindítást megfelelő technikai megoldásokkal meg kell akadályozni.

- Biztosítani kell a szervezet egészére kiterjedő, rendszeres és folyamatos vírusvédelmet.
- A szoftverben megvalósított védelmeket az operációs rendszer és a felhasználói rendszer védelmi tulajdonságai kölcsönös gyengítése nélkül kell kialakítani. Követelmény, hogy az alkalmazások szintjén megvalósított védelmi funkciók az operációs rendszer megfelelő védelmi eszközeire – ha ilyenek léteznek – épüljenek.
- Össze kell állítani, és elérhető helyen kell tartani a számítástechnikai eszközök használatára felhatalmazott személyek névsorát, és feladataikat körül kell határolni.
- A programok, alkalmazások és eszközök tervezése, fejlesztése, tesztelése és üzemeltetése során a biztonsági funkciókat kiemelten és elkülönítetten kell kezelni.

4.2.2.4. Adathordozók

Adathordozóként értelmezzük a szoftver, adat vagy dokumentáció és azok biztonsági másolatainak papíron, mikrofilmen és a mágneses vagy egyéb számítástechnikai adathordozón tárolt változatait.

- Az adathordozó eszközök elhelyezésére szolgáló helyiségeket úgy kell kialakítani, hogy elegendő biztonságot nyújtsanak illetéktelen vagy erőszakos behatolás, tűz vagy természeti csapás ellen.
- Adatátvitelre, valamint mentésre, archiválásra használt adathordozók tárolása csak megbízhatóan zárt helyen történhet.
- Az adathordozók beszerzését, tárolását, felhasználását és hozzáférését szabályozni, nyilvántartani, rendszeresen és dokumentáltan ellenőrizni kell.
- Biztosítani kell, hogy az adathordozók kezelése a vonatkozó iratkezelési szabályok szellemében, a tartalmazott adatok szempontjából egyenértékű papír dokumentumokkal azonos módon történjék. A mentésre, archiválásra szolgáló adathordozók tartalmáról nyilvántartást kell vezetni.
- A szervezetnél csak leltár szerint kiadott, azonosítóval ellátott adathordozót szabad használni. Idegen adathordozó használata nem megengedhető.
- A szervezeten kívüli adatforgalomban használt adathordozók előállítása, kiadása és fogadása csak kijelölt helyeken, írásban szabályozott, dokumentált és ellenőrzött módon történhet. Az adathordozókat használatba venni csak az előírt ellenőrző eljárások (például vírusellenőrzés) után szabad.
- Minden adathordozót újra alkalmazása előtt, felszabadítás, selejtezés után az adatok megsemmisítését eredményező megfelelő eljárással törölni kell.

4.2.2.5. Dokumentumok, dokumentáció

- A nyomtatott anyagok kezelését az iratkezelési szabályzat szerint kell elvégezni.

- Az informatikai rendszer biztonságával kapcsolatos dokumentációt az informatikai rendszer biztonsági fokozatának megfelelően kell kezelni.
- Az informatikai rendszer vagy annak bármely elemének dokumentációját változás-menedzsment keretében kell aktuális szinten tartani.

4.2.2.6. Adatok

- Az információs rendszer hozzáférési kulcsait (azonosító kártya, jelszó), a jogosultságokat és más, a biztonsággal kapcsolatos paramétereket titkosítva kell továbbítani.
- A rendszer biztonságát érintő adatok (például jelszavak, jogosultságok, naplók) védelméről a hozzáférési jogosultságok kiosztásánál kell gondoskodni.
- Külső személy – például karbantartás, javítás, fejlesztés céljából – a számítástechnikai eszközökhöz úgy férhet hozzá, hogy a kezelt adatokat ne ismerhesse meg.
- Az adatbevitel során a bevitt adatok helyességét az alkalmazási követelményeknek megfelelően ellenőrizni kell.
- Programfejlesztés vagy próba céljára valódi adatok felhasználását – különösen akkor, ha a próbát külső szerv vagy személy végzi vagy annak eredményeit megismerheti – el kell kerülni. Ha ez nem valósítható meg, akkor az adatok bizalmasságát más módszerekkel kell megőrizni.
- Gondoskodni kell arról, hogy a számítógépen feldolgozott minden adatállomány az adattípust jelölő biztonsági címkével legyen ellátva.

4.2.2.7. Kommunikáció, számítógépes hálózatok

- Az elektronikus úton továbbított üzenetek, állományok tekintetében az iratkezelési szabályzatnak megfelelően kell eljárni.
- Az alanyokra a szolgáltatások indítása vagy az azokkal történő kommunikáció megkezdése előtt megvalósítandó a hitelesítési eljárás.
- Az adott hálózati alrendszer hitelesítési mechanizmusa nem érintheti a hálózat többi alrendszerének hitelesítési rendszerét.
- Egy adott alhálózatban azonosítani kell a más alhálózatból importált adatok feladóját. Ha ilyen nincs, ezeket az adatok el kell különíteni.
- A hálózati erőforrások használata a felhasználók számára szabályozandó, korlátozandó.
- A hálózat elosztott és diszkrét elemeit rendszeresen ellenőrizni kell annak érdekében, hogy a hálózatban a hálózati forgalom monitorozására és rögzítésére alkalmas erőforrást illetéktelenül ne használjanak.
- Egy alhálózatban definiált azonosító hozzáférési joga delegálható egy másik alhálózatba, és ez alapján kell érvényesíteni az eredeti azonosítóhoz rendelt jogokat.


Figyelj jól!

- A szabad belátás szerint kialakított hozzáférés-vezérlést (DAC) ki kell terjeszteni a teljes osztott rendszerre.
- Központi hozzáférés-menedzsment esetén az alanyoknak egy privilegizált hálózati szolgáltatás (például egy biztonsági szerver) által kezelt hozzáférési jogai biztonságos úton eljutnak az osztott rendszer többi feldolgozó egységéhez a hozzáférés-vezérlés végrehajtása céljából. Ehhez elosztott hozzáférés-vezérlési táblakezelés szükséges. Az ilyen információk titkosítva kerüljenek továbbításra.
- A biztonságos adatcsere követelményének teljesítéséhez biztosítani kell az adatintegritást mind a protokollvezérlő, mind a felhasználói adatokra.
- Az adatvesztés és sérülés elkerülése céljából hibadetektáló és javító eljárásokat kell alkalmazni.
- Az osztott rendszerben a jelszavak, a jogosultságok és a biztonsággal kapcsolatos egyéb paraméterek, adatok csak titkosítva továbbíthatók.

4.2.2.8. Személyek


Figyelj jól!

- A szervezet területén ki kell alakítani a kitűzők viselésével kapcsolatos szabályozást.
- A belépés rendjét a hozzáférési jogosultságokkal összhangban kell szabályozni.
- A magasabb jogosultságú személyeknél el kell kerülni a jogok túlzott koncentrációját.
- Munkába álláskor minden munkatárs számára biztosítani kell az informatikai biztonsággal kapcsolatos oktatást, valamint az összes munkatárs számára a rendszeres továbbképzést.
- Az informatikai rendszer biztonságát meghatározó munkakörökben dolgozó munkatársak helyettesítési rendjét ki kell alakítani.
- A fontosabb alkalmazásokhoz rendszergazdákat kell kinevezni, akiknek feladatkörét pontosan meg kell határozni.
- A fejlesztői környezetet el kell választani az alkalmazói környezettől, szét kell választani a fejlesztői, működtetői és adminisztrációs hozzáférési jogköröket.
- Külső partnerekkel kötött fejlesztési, karbantartási szerződések biztonsággal kapcsolatos részeinek kialakítására pontos szabályozást kell adni.

4.2.3. Fokozott biztonsági osztály


Figyelj jól!

A következőkben megadott követelmények alkalmazásánál az alap biztonsági osztály követelményeit is meg kell valósítani, mert *a fokozott biztonsági osztály magában foglalja az alap biztonsági osztály követelményeit is*. A dőlt betűvel szedett részekkel lettek jelezve azok a részek, amelyek alapbiztonsági követelményt foko-

zott biztonsági szintre emelnek. A fokozott biztonsági osztálynál jelentkező új követelmények normál betűtípussal lettek szedve.

4.2.3.1. A fokozott biztonsági osztály minimális követelményei

- Az interaktív kommunikáció (egyedi munkaállomások és hálózatok esetében egyaránt) létrejötte előtt *egyedi szinten* azonosítani és hitelesíteni kell a felhasználó személyazonosságát, az interaktív kommunikációra csak a sikeres azonosítás és hitelesítés után kerülhet sor.
- Az azonosítás hardver eszközeinél (például chipkártyák) gondoskodni kell a jogosulatlan továbbadás és az illetéktelen használat megelőzéséről.
- *Az informatikai rendszer alanyaihoz (felhasználók, programok) és tárgyaihoz (fájlok, eszközök, programok, illetve processzek közötti logikai vagy fizikai csatornák) biztonsági címkéket kell rendelni, amelyek tartalmát (hozzáférési jogok, adatvédelmi szintek, adatcsoportok) előre meghatározott módon kell kialakítani. Ezt – a nemzetközi ajánlásokat is figyelembe véve – előre meghatározott szabályokon alapuló hozzáférési jogosultság vezérlésnek (Mandatory Access Control, röv.: MAC) nevezzük, és használata ebben az osztályban kötelező.*

Ennek megfelelően:

- az alanyokhoz olyan biztonsági címke van rendelve, amely meghatározza, hogy az adott felhasználó vagy program milyen biztonsági szintű adatokhoz és mely adatcsoportokhoz férhet hozzá,
- a tárgy címkéje az általa tárolt vagy kezelt adat biztonsági kategóriáját és a hozzáférés módját tartalmazza,
- az olvasási jogosultság esetében a személy azonosítója a meghatározó (magasabb vagy azonos értékű) az erőforráséhoz (például fájl) képest,
- az írási jogosultság esetében az erőforrás azonosítója a meghatározó (magasabb vagy azonos értékű) a személyéhez képest,
- új objektumok létesítésekor a biztonsági címke automatikusan hozzárendelődik.

- A hozzáférési jogok a fokozott biztonsági osztályban a következők:
  - olvasási jog (betekintés),
  - létrehozási jog,
  - módosítási jog,
  - törlési jog (selejtezés),
  - *másolási jog*.
- A MAC hozzáférési jogosultság-vezérlés elvének megfelelően az adatokat minősítési jellemzőkkel kell ellátni (például nyílt adatok, kis, közepes tömegű személyes adatok, a szervezet belső szabályozása alapján védendő adatok, nagy tömegű bank- és üzleti titok, szolgálati titok, államtitok stb.),

valamint a felhasználási területnek megfelelően be kell sorolni őket (például bérszámfejtési, pénzügy-számviteli, műszaki fejlesztési, döntés-előkészítési stb. adatok).

- Új adat-objektumok létesítésekor a biztonsági címke automatikus hozzárendelését biztosítani kell.
- A minősítést és az adatérzékenységet magasabb, illetve alacsonyabb biztonsági szinttel kell jellemezni.
- Az adatok minősítési jellemzőinek megállapításánál a törvényekben meghatározott előírásokat kell figyelembe venni.
- A minősítést csak a törvényekben meghatározott személyek engedélyezhetik.
- A feljogosítás műveletét engedélyhez kell kötni, az engedélyezés eljárásrendjét a törvényekben meghatározott módon kell kidolgozni.
- Egy rendszeren belül a különbözőképpen minősített adatok kezelését csak abban az esetben szabad együtt kezelni, ha megakadályozhatók az engedéllyel nem rendelkező hozzáférések. Ez érvényes az osztott rendszerek esetében a teljes rendszerre nézve is.
- Az egy rendszeren belül kezelt, különbözőképpen minősített adatokat olyan mértékben kell elkülönítetten kezelni, hogy egyértelműen ellenőrizhető legyen a hozzáférések jogossága.
- Ha ez utóbbi feltétel nem biztosítható, a különbözőképpen minősített adatokat csak fizikailag teljesen elkülönített rendszeren szabad kezelni. Ez érvényes az osztott rendszerek esetében a teljes rendszerre nézve is.
- Az elszámoltathatóság és auditálhatóság biztosítása érdekében a biztonsági naplóban az eseményekhez kapcsolódóan az alapbiztonsági osztálynál meghatározott műveletekre a megadott paramétereket kell rögzíteni.

Ezen túlmenően rögzíteni szükséges:

- A felhasználó azonosítása és hitelesítése műveletnél a *felhasználó jogosultsági paramétereit.*
- Erőforrás létrehozása vagy törlése, illetve erőforráson kezdeményezett hozzáférési művelet esetén az erőforrás biztonsági címkéjét.
- Felhatalmazott felhasználók (például rendszeradminisztrátorok) olyan műveletei esetén az erőforrás azonosítóját és *biztonsági címkéjét,* amelyre a művelet vonatkozik, például hozzáférésijog-megadás, felfüggesztés, elvétel, tároló erőforrás logikai kijelölése vagy megszüntetése, rendszerindítás vagy leállítás, *új biztonságicímke-kijelölés, biztonságicímke-változtatás, átviteli csatorna biztonsági jelölés vagy osztályba sorolás.*

- A napló adatait havonta legalább *két* alkalommal ellenőrizni és archiválni kell.

4.2.3.2. Infrastruktúra

- A védendő helyiséget minden oldalról legalább a *15 cm* vastagságú tömör téglafal szilárdsági mutatóival egyenértékű falszerkezet határolja.
- A *nyílászárók* feleljenek meg a magyar vagy európai szabványok által előírt minimális követelményeknek.
- A területen legalább 12 órás áthidalást biztosító szünetmentességgel ellátott olyan *elektronikai jelzőrendszert* kell kiépíteni, amellyel biztosítható a teljes felület és a részleges térvédelem.
- A személyzet és a külső *személyek belépési és azonosítási rendjét* szabályozott formában kell megvalósítani.
- Az *őr- és a biztonsági személyzet* létszámát úgy kell kialakítani és olyan eszközzel kell ellátni, hogy esemény esetén az érintett személy jelezni tudjon.
- A kisugárzás elleni védelmi intézkedések foganatosítása a *kockázatokkal arányosan indokolt.*

4.2.3.3. Hardver/szoftver rendszer

- A beépített adathordozókon tárolt adatokkal azonos szinten védendő minden számítástechnikai eszköz.
- A minősített (az 1995. évi LXV. törvény hatálya alá tartozó) adatot előállító, feldolgozó, tároló és lekérdező programok, valamint ezek dokumentációi (adatfüggetlen elemek) minősítéséről az adatot minősítőnek kell gondoskodnia.

4.2.3.4. Adathordozók

- Az adathordozók tárolása csak megbízhatóan *zárt helyiségben, minimum 30 perces tűzállóságú tárolószekrényben* történhet.
- A fokozott biztonsági osztályba tartozó minősített adatokat tároló adathordozók kezelését az *1995. évi LXV. törvény* szellemében kell végezni.
- Az adattípus (minősítés) felismerhető jelölését a számítástechnikai berendezéssel előállított adattároló és megjelenítő eszközökön biztosítani kell.
- Az adatok sértetlen és hiteles állapotának megőrzését biztosítani kell.

4.2.3.5. Dokumentáció

- A felhasználók részére Biztonsági Kézikönyv (Információvédelmi Tájékoztató) biztosítandó.
- Gondoskodni kell a változásmenedzsmentről és a *biztonságot érintő változások naplózásáról.*

- A rendszerben feldolgozásra kerülő, a fokozott biztonsági osztályba sorolt adatok és a hozzájuk kapcsolódó jogosultságok nyilvántartását elkülönítetten kell kezelni.

4.2.3.6. Adatok


Figyelj jól!

- Minősített és nem minősített adatok párhuzamos feldolgozása az 1995. évi LXV. törvény szellemében végezhető.

4.2.3.7. Kommunikáció, osztott rendszerek


Figyelj jól!

- A kisugárzással, illetve a zavartatással kapcsolatos EN 55022 és EN 55024 szabványok a mérvadók.
- Minden kommunikációs csatorna egy- vagy többszintű biztonsági azonosítással legyen ellátva.
  - egyszintű csatorna esetében a csatorna csak egy azonosítóval (címke) rendelkezik, és csak olyan adatállomány vihető át rajta, hogy az ahhoz rendelt biztonsági azonosító megfelel a csatorna azonosítójának,
  - többszintű csatorna esetében egy protokoll kezeli a csatorna és az adatazonosítók megfeleltetését, és biztosítja, hogy a fogadó fél teljesen és egyértelműen helyreállíthassa, valamint párosíthassa a fogadott adatokat azok azonosítóival,
  - csak erre felhatalmazott személyek változtathatják meg a védelem szempontjából fontos azonosítókat.
- A *kötelező hozzáférés-vezérlést (MAC)* ki kell terjeszteni a teljes rendszerre.
- Központi hozzáférés menedzsment esetén az *alanyok biztonsági paramétereit* biztonságos úton kell az osztott rendszer többi feldolgozó egységéhez eljuttatni.
- A fokozott biztonsági osztályba sorolt adatok forgalmazásával kapcsolatba kerülő valamennyi hálózati elemre ki kell terjeszteni a fokozott biztonsági szintnek megfelelő védelmet.
- A hálózaton megvalósítandó a végpont-végpont szintű jogosultság-ellenőrzés, az elszámoltathatóság és auditálhatóság biztosítása védelmi funkciók.
- Központi auditálás esetén védetten kell továbbítani az auditálási információkat a többi alhálózatból.
- Az adattovábbításra használt hálózat esetében a biztonsági osztálynak megfelelő szinten biztosítani kell az illegális rácsatlakozás és a lehallgatás akadályozását.
- A minősített adatok rejtjelzése során a 43/1994. (III. 29.) Korm. Rendelet előírásai kötelezőek.

4.2.3.8. Személyek

- A felhasználók tevékenységének szelektív szétválasztását az ellenőrzés céljából biztosítani kell.
- A minősített adatok kezelésében a titokbirtokos és az informatikai rendszert üzemeltető közötti feladat- és felelősségmegosztást szabályozni kell.

4.2.4. Kiemelt biztonsági osztály

A következőkben megadott követelmények alkalmazásánál az alap és a fokozott biztonsági osztályok követelményeit is meg kell valósítani, mert *a kiemelt biztonsági osztály magában foglalja ezen osztályok követelményeit is.* A dőlt betűvel szedett részekkel lettek jelezve azok a részek, amelyek fokozott biztonsági követelményt kiemelt biztonsági szintre emelnek. A kiemelt biztonsági osztálynál jelentkező új követelmények normál betűtípussal lettek szedve.

4.2.4.1 A kiemelt biztonsági osztály minimális követelményei

- Az azonosítást és hitelesítést a felhasználó és a rendszer között egy, a felhasználó által megnyitott, védett csatornán keresztül kell biztosítani.
- Az informatikai rendszer minden alanyára és objektumára ki kell terjeszteni a hozzáférés jogosultságvezérlési mechanizmusát. *A szervezet informatikai biztonsági politikája határozza meg, hogy mikor kerül alkalmazásra az esetenként meghatározott hozzáférés-vezérlés (DAC) és mikor az előre meghatározott hozzáférés-vezérlési rendszer (MAC).*
- Az informatikai rendszer tárgyaihoz legalább az alábbi hozzáférési módokat kell hozzárendelni:
  - olvasási jog (betekintés),
  - létrehozási jog,
  - módosítási jog,
  - *selejtezési jog,*
  - törlési jog,
  - másolási jog.
- *A rendszerrel kapcsolatba kerülő személyekhez az alábbi hozzáférési módokat kell hozzárendelni:*
  - engedélyezési jog,
  - visszavonási jog,
  - olvasási jog (betekintés),
  - létrehozási jog,
  - módosítási jog,


Figyelj jól!

- selejtezési jog,
- törlési jog,
- másolási jog.

➠ A hozzáférés-védelmet mező (lásd adatbázisban) szinten kell megvalósítani.

➠ A hozzáférési műveletek megkezdése előtt jogosultság-ellenőrzést kell végrehajtani.

➠ A rendszernek alkalmasnak kell lennie a hozzáférési jogok egyedi vagy csoportszinten történő megkülönböztetésére és szabályozására, a hasonló szerepkörű személyek csoportos munkájának támogatására azonos hozzáférési jogú csoportokat kell tudni kialakítani, és el kell határolni a rendszeradminisztrátor, az operátor és a biztonsági felügyelő szerepkörét.

➠ A jogosultság hozzárendelésének végrehajtását (felhatalmazás) csak engedélyezési joggal rendelkező személy(ek) végezheti(k).

➠ A jogosultság hozzárendelésének megszüntetését (visszavonás) csak visszavonási joggal rendelkező személy(ek) végezheti(k).

➠ Az adatok minősítését és a feljogosítás műveletét a vonatkozó hatályos jogszabályok és utasítások szerint kell elvégezni, illetve engedélyezni.

➠ Biztosítani kell a biztonsági monitor rendszerben végbement, a biztonságot érintő vagy a fellépési gyakoriságuk miatt biztonsági szempontból kritikus veszélyt jelentő események figyelését biztosító mechanizmust. E mechanizmusnak késedelem nélkül értesítenie kell az ilyen események bekövetkezéséről egy ezzel megbízott adminisztrátort, akinek haladéktalanul értesítenie kell az informatikai biztonsági felügyelőt.

➠ A biztonsági napló adatait *hetente legalább két alkalommal* ellenőrizni és archiválni kell.

4.2.4.2. Infrastruktúra


Figyelj jól!

➠ A *mechanikai védelem* közforgalmú területről történő betekintés ellen is védjen.

➠ Az *elektronikai védelem* terjedjen ki a számítástechnikai eszközökre, a felügyelet nélküli helyiségekre.

➠ A személyzet és a külső személyek *belépési és azonosítási rendjét* szabályozott formában, intelligens beléptető-rendszerrel kell megvalósítani, amely a mindkét irányú áthaladásokat naplózza, és biztosítja az azonosító eszköz azonos irányban történő többszöri felhasználásának tilalmát.

➠ A helyiségbe (épületbe) belépni szándékozókat hitelesíteni és azokról nyilvántartást vezetni kell.

➠ A *kisugárzás elleni védelmi intézkedések* foganatosítása szükséges.

4.2.4.3. Hardver/szoftver

- Kiemelt biztonsággal védett adathordozókkal azonos szinten védendő fizikailag minden számítástechnikai eszköz, amellyel az ebbe az osztályba tartozó adatokat kezelnek.
- Az informatikai biztonsági rendszer külön architektúrával rendelkezzék és tartalmazzon egy referencia felügyelet (monitor) elvén működő modult, amely magát a biztonsági rendszert is védi külső támadások (például programmódosítás, biztonsági adatok módosítása, kinyerése) ellen. Alapvetően moduláris felépítésű legyen. A biztonsági monitor rendszernek sérthetetlennek kell lennie, állandó működését biztosítani kell, és méretét tekintve elég kicsinek (vagy felépítését és összetettségét tekintve elég egyszerűnek) kell lennie ahhoz, hogy elemzése és ellenőrzése könnyen megoldható legyen, illetve, hogy teljességét, sérthetetlenségét biztosítani lehessen.
- Tegye lehetővé az informatikai rendszer biztonsági szempontból érzékeny hardver és szoftver elemeinek szegmentálhatóságát. Rendelkezzék egy speciálisan a biztonsági műveleteket támogató képernyős felhasználó felülettel.
- A biztonságos kezelési funkciókat az X/Open privilegizált jogokat biztosító osztály követelményeinek megfelelően kell kialakítani.
- Biztosítani kell a biztonsági monitor rendszerben végbement, a biztonságot érintő vagy a fellépési gyakoriságuk miatt biztonsági szempontból kritikus veszélyt jelentő események figyelését biztosító mechanizmust. E mechanizmusnak késedelem nélkül értesítenie kell az ilyen események bekövetkezéséről egy ezzel megbízott adminisztrátort, akinek haladéktalanul értesítenie kell az informatikai biztonsági felügyelőt.

4.2.4.4. Adathordozók

- Az alap- és a fokozott biztonsági osztályok követelményei érvényesek az 1995. évi LXV. törvénynek *a kiemelt osztálynak megfelelő értelmezésével.*

4.2.4.5. Dokumentáció

- Dokumentációt kell készíteni a referencia hitelesítési mechanizmus megvalósítási módjáról. Ennek tartalmaznia kell a biztonsági és az informatikai rendszerek közötti interfészek leírását, a referencia rendszer védelmi tulajdonságait, amelyekkel bemutatható, hogy az nem megkerülhető és a potenciális támadások ellen jól véd. Tartalmaznia kell az informatikai rendszer tesztelési eljárásainak dokumentációját, így például azoknak a tesztmódszereknek az eredményeit, amelyek célja a rejtett csatornák sávszélessége hatékony csökkentésének vizsgálata.

- Ki kell alakítani a változásmenedzsmentet, amely biztosítja az informatikai rendszer fejlesztése és üzemeltetése során beállt változások, módosítások és a vonatkozó dokumentációk közötti összhangot. A *változás-menedzsmentet számítástechnikai úton kell megvalósítani.*
- Az informatikai biztonsági rendszer dokumentációjában (kézikönyv) meg kell adni a referencia monitor ellenőrzési mechanizmusának működését és a szoftverek módosítás utáni, forráskódból történő újra generálásának biztonságos eljárását. A referenciahitelesítési mechanizmus dokumentáció struktúrájának és szintjének meg kell felelnie az ITSEC E3 értékelési követelményeknek.
- Az informatikai biztonsági rendszer dokumentációjának (kézikönyv) tartalmaznia kell a referencia monitor működésével kapcsolatos ellenőrzési és üzemeltetési eljárások leírását.

4.2.4.6. Kommunikáció, számítógépes hálózatok

- Többszintű csatorna esetén a védendő adat csak rejtjelezve vihető át.
- Nem alkalmazható olyan (elfogadhatatlanul magas, közvetlen mérés vagy műszaki becslés útján meghatározott maximális sávszélességű ismeretlen) tároló jellegű csatorna, amely adatokat vihet át processzek között a hozzáférési jogok ellenőrzése nélkül.
- Az adatáramlás bizalmasságának megőrzése céljából ajánlott szelektív útvezérlés (selective routing) alkalmazása.
- A kábelezésre vonatkozóan az EIA/TIA-568 Kereskedelmi Épületkábelezési Szabvány, valamint a kisugárzással, illetve a zavartatással kapcsolatos EN 55022 és EN 55024 szabványok a mérvadók.

4.2.4.7. Személyzet

- A rendszer-adminisztrátorok többszintű, úgynevezett privilegizált szerepkörét a felhasználóktól és egymástól is elválasztottan kell kezelni.
  A privilegizált rendszer-adminisztrátorok a következő műveleteket hajthatják végre:
  - processzekhez valódi egyedi vagy csoportfelhasználói azonosítókat (User ID) rendelhetnek, ezáltal védett alrendszereket alakíthatnak ki,
  - az esetenként meghatározott hozzáférés-vezérlés paramétereit felülírhatják,
  - a rendszert elindíthatják és leállíthatják,
  - a processzek határait, a fájlok paramétereit módosíthatják,
  - speciális eszközfájlokat létesíthetnek,
  - fájlrendszereket magukhoz csatolhatnak (mounting),
  - felhasználói azonosító beállító programokat indíthatnak,
  - adatokat importálhatnak/exportálhatnak.

- Új jogosultság kiosztását, a jogosultság törlését, átmeneti felfüggesztését csak az erre felhatalmazott személy végezheti el. Minden jogosultsági azonosítóval ellátott erőforrás esetében a hozzáférésre jogosult felhasználók vagy felhasználói csoportok listáját, azok hozzáférési jogosultságaival együtt ki kell tudni nyomtatni. A biztonsági szintben a használat (például tranzakció, interaktív kommunikáció) közben beállt változásokat a felhasználónak azonnal és közvetlenül jelezni kell, és le kell tudnia kérdezni a többi alannyal kapcsolatos védelmi attribútumokat.
- A Biztonsági Kézikönyv (IBSZ, Információvédelmi Tájékoztató) felhasználásával rendszeres oktatást és vizsgáztatást kell rendszeresíteni.
- A biztonsági személyzet feladatát „vállalkozás keretében" nem láthatja el.

4.3. Követelmények a megbízható működés területén

4.3.1. Információbiztonsági osztályok a megbízható működés területén

Az informatikai rendszerek *megbízható működését* úgy értelmezzük, hogy az alkalmazói rendszernek (felhasználói programok és adatok) a tervezés és megvalósítás során kialakított *funkcionalitását* egy megbízható informatikai alaprendszer (hardver és alapszoftver) az adott biztonsági osztálynak megfelelő követelményeknek megfelelő szintű rendelkezésre állásával biztosítja a felhasználó részére. Másképp kifejezve ez azt jelenti, hogy egy nem megfelelően tervezett és megvalósított alkalmazói rendszerrel egy magas rendelkezésre állást biztosító alaprendszer esetén sem tudjuk a felhasználói követelményeknek megfelelő működést biztosítani (gyakori programhibák, „lefagyások", adatvesztések, bonyolult kezelés, felhasználóidegen kezelési felületek stb.). Ennek a fordítottja is igaz, nevezetesen, hogy egy funkcionálisan jól megtervezett és megvalósított alkalmazói rendszer szintén nem tud megbízhatóan működni, nem tudja megfelelő rendelkezésre állással biztosítani a funkciók használatát a felhasználó részére, ha az alaprendszer nem éri el az adott biztonsági osztály követelményeinek megfelelő megbízhatósági szintet.

Rendelkezésre álláson azt a valószínűséget értjük, amellyel egy definiált időintervallumon belül az alkalmazás a tervezéskor meghatározott funkcionalitási szintnek megfelelően a felhasználó által használható. Gyakorlati megközelítéssel a **rendelkezésre állást** az **4.1.** egyenlet szerinti formulával lehet meghatározni:

Tudni kell!

$$R = \frac{T_{üz} - \sum_{üz} T_{ki}}{T_{üz}} \times 100(\%)$$

4.1. egyenlet

ahol $T_{üz}$ az üzemidő periódus, amelyre a rendelkezésre állást értelmezzük és T_{ki} a kiesési idő egy alkalomra.

A megbízható működés szempontjából értelmezett biztonsági osztályokra jellemző paraméterként a *rendelkezésre állást,* a *kiesési időt* és az ezen belül *egy alkalomra megengedett maximális kiesési időt* adjuk meg a **4.1.** táblázatban. A paraméterek számításánál napi 24 órás üzemet és 1 hónapos üzemidőt tételeztünk fel.

Az itt definiált paraméterek és a biztonsági osztályokra a károsztályokon alapuló definíció közötti összhangot a következőképpen lehet megteremteni, ha például a kiesési idő paramétert vesszük alapul. Ha egy adott biztonsági osztályba sorolt alkalmazás kiesése meghaladja a megengedett kiesési időt, akkor a fellépő kárfajták közül a legnagyobb érték a biztonsági osztályra jellemző kárnagyságot eléri.

$T_{üz}$ = 1 hónap	Rendelkezésre állás (R)	Megengedett kiesési idő (ST_{ki})	Megengedett legnagyobb kiesési idő egy alkalomra ($maxT_{ki}$)
Megbízható működési alapbiztonsági osztály	95,5%	23,8 óra	–
Megbízható működési fokozott biztonsági osztály	99,5%	2,6 óra	30 perc
Megbízható működési kiemelt biztonsági osztály	99,95%	16 perc	1 perc

4.1. táblázat

A hiba bekövetkezésétől számított kiesési időt a rendszeren belüli megoldásokkal és a rendszeren kívül foganatosított intézkedésekkel állíthatjuk be az adott biztonsági osztály követelményeinek megfelelő értékre.

A kiesési időt befolyásolják:

- az újraindítási képesség megvalósítása,
- a hibaáthidalás folyamatának kialakítása,
- a rendszerkonfiguráció hatékony menedzselése.

A fenti tulajdonságokat a megbízható működés biztonsági osztályának megfelelő követelményekkel arányosan kell megvalósítani. Amennyiben ez sikerül, akkor a rendszeren üzemeltetett felhasználói funkciók a tervezéskor specifikált és a megvalósításuk során realizált funkcionalitással használhatók a biztonsági osztályra jellemző rendelkezésre állási szinten.

Az alapbiztonsági osztályban a rendszer – néhány rendszerelem (például lemezegység) kivételével – általában nem tartalmaz redundanciát, így az újraindításig eltelt időt a hiba természetén túlmenően a hibaleírás és behatárolás pontossága, a szerviz háttér reakcióideje, valamint hatékony munkája határozza meg. A rendszerben általában nem alkalmaznak hibaáthidalási és az ehhez szükséges visszaállítás-menedzselési (recovery management) megoldásokat. Menedzselést a tartalék alkatrész és szervizbiztosítás igényel.

A fokozott biztonsági osztálynál már megjelenik egy bizonyos szintű redundancia, amely a legfontosabb rendszerelemeknek egy lazán csatolt (például hálózaton keresztül történő meleg vagy hideg) tartalék biztosításával oldható meg. A konkrét rendszer és a fellépő költségek ismeretében dönthető el, hogy melyik tartalékolási módot célszerű alkalmazni. A meleg tartalékra történő átkapcsolás már igényel áttérés-menedzsmentet, amely alapvetően automatikusan vagy manuálisan vezérelt áttérést jelent. A melegtartalék megoldásvezérlési és adatállomány-aktualizálási eljárásait már a rendszertervezés idején ki kell alakítani, a konfiguráció erőforrásait is ennek megfelelően kell méretezni. A fokozott biztonsági osztályban még mindig komoly szerepe van a megfelelő – szerződésben rögzített – reakcióidejű szerviz háttérnek, azonban a saját üzemeltető személyzettel szemben már komolyabb szakmai követelményeket támaszt a tartalékolási folyamat irányítása.

A kiemelt biztonsági osztályban kizárólag a szorosan csatolt melegtartalékkal megvalósított hibaáthidalás jöhet szóba[6], amely komoly áttérés-menedzsmentet (reconfiguration management) igényel. A kiesési idő itt gyakorlatilag az átkapcsolási idővel azonos. A szó eredeti értelmében vett rendszerindításra nincs szükség. Ebben az osztályban a legmagasabb az üzemeltető személyzettel szembeni szakmai követelmény, mert az esetlegesen szükséges beavatkozás reakcióideje olyan rövid, hogy azt külső szervizzel biztosítani nagyon drága megoldás lenne. A szerviz feladata elsősorban a meghibásodott egység kijavítása.

A fentiekből látszik, hogy a rendelkezésre állásra, azaz az alkalmazói rendszer üzem közbeni funkcionalitásának megőrzésére vonatkozó követelmények növekedésével arányosan szigorodnak a rendszer-újraindítással, a hibaáthidalással és az ezekhez szükséges menedzselési funkciókkal kapcsolatos eljárások, és nem lineárisan nőnek az ezekkel járó költségek. Más szóval ez azt jelenti, hogy már a rendszertervezés idején ki kell elemezni az adott biztonsági követelményszintet kielégítő legolcsóbb megoldást. Az alkalmazói rendszer funkcionalitását a felhasználói

[6] A legtöbb szakirodalom ezt a rendszerműködési jellemzőt „mission critical" funkciónak nevezi.

követelményrendszer, a funkció specifikáció, a szoftver rendszerterv kidolgozása és a megvalósítás specifikációhű kivitelezése határozza meg, valamint az ezeket a folyamatokat kísérő dokumentációs rendszer kialakítása és a dokumentációk megvalósítása. Az alkalmazói rendszer tervezési lépéseivel és a dokumentációs rendszerrel kapcsolatos követelményeket az egyes biztonsági osztályok tárgyalásánál részletesen kifejtjük.

4.3.2. Alapbiztonsági osztály

A követelmények megfogalmazásánál mindazon közvetlen vagy közvetett feltételekre kitérünk, amelyek biztosítása szükséges ahhoz, hogy az adott biztonsági osztályra jellemző megbízható működési mutató tartható, más szóval a megengedett kiesési idő túllépése elkerülhető legyen.

A közvetett feltételek közé soroljuk például a beszerzéssel, a rendszer fejlesztésével, a dokumentáció rendszerével stb., kapcsolatos követelményeket, amelyeket teljesítve az informatikai rendszer magasabb funkcionalitási szinten alakítható ki, megbízhatóbban lesz üzemeltethető, és így hatással lesznek az alkalmazások jobb, megbízhatóbb működésére.

4.3.2.1. Az alapbiztonsági osztály minimális követelményei

- Az informatikai rendszer megbízhatóságát a megbízható működés alapbiztonsági osztály szintjén jó minőségű és megfelelő számú referenciával rendelkező hardver- és szoftvertermékek beszerzésével kell biztosítani.
- A szállítóval és a szervizcégekkel olyan garanciális, illetve garancián túli szervizszerződést kell kötni, amely garantálja a megbízható működés alapbiztonsági osztályra definiált rendelkezésreállási szint betarthatóságát. A szervizszerződésben legalább a 12 órás reakcióidő kikötése ajánlott.
- Az informatikai rendszer tervezésénél betartandók a funkcionalitás biztosítását meghatározó lépések.
- Az informatikai rendszer beszerzéssel és/vagy fejlesztéssel történő kialakítása folyamatának dokumentációs rendszerét ki kell alakítani és ennek megfelelően a dokumentációkat el kell készíteni, illetve be kell szerezni.
- A fontosabb számítástechnikai eszközöket tartalmazó helyiségeket (például szerverszoba, hálózati központi elosztó helyiség) a MABISZ és a Rendőrség által jóváhagyott biztonsági zárral zárni kell, a kulcskezelést szabályozottan kell végezni.
- A számítástechnikai eszközöket tartalmazó helyiségekben az országos és a szervezeti szintű tűz- és munkavédelmi rendszabályokat be kell tartani és tartatni.

- A fontosabb számítástechnikai erőforrások (például szerverek) legyenek ellátva szünetmentes tápegységgel.
- A rendszerbe kívülről bekerülő adathordozókat felhasználás előtt vírusellenőrzésnek kell alávetni. A vírusdetektálás és eltávolítás is biztonsági eseménynek számít, ezért a biztonsági naplózásnál (lásd 4.2.2.1 pontnál!) leírtaknak megfelelően kell eljárni
- A megbízható működéssel kapcsolatos eseményekre (rendszerindítás/leállás, nagyobb üzemzavarok, alap- és felhasználói szoftverekkel kapcsolatos, a megbízható működést érintő események) gépi, illetve manuális biztonsági naplózásokat kell végezni.
- A rendszer- és adatmentéseket az üzemviteli előírásoknak megfelelő rendszerességgel el kell végezni, a mentésekről biztonsági másolatot kell készíteni. A primer és a biztonsági mentések adathordozóit külön-külön, tűzbiztos helyen kell tárolni.
- 100-nál nagyobb számú felhasználót kezelő hálózatnál az egyszerűsített SNMP szintű hálózatmenedzsment alkalmazása szükséges.
- A hálózati elemek rongálás és tűz elleni védelmét biztosítani kell.
- Az informatikai rendszer üzemeltetéséhez és karbantartásához biztosítani kell a megbízható működés alapbiztonsági osztály követelményeinek megfelelő szaktudású és tapasztalatú személyzetet.

4.3.2.2. Fizikai védelem

A fizikai védelmi intézkedések túlnyomó többségéről elmondható, hogy egyaránt szolgálja az informatikai rendszerben az információvédelem és a megbízható működés biztosítását. Az ilyen jellegű követelményeket a 4.2.2.2 fejezetben már megadtuk, ezért ebben a pontban csak megbízható működést támogató védelmi funkciókra vonatkozó követelményeket adtuk meg, amelyek jellemzően a tűzvédelemre, a tápáramellátási rendszerre, a villámvédelemre, stb. vonatkoznak.

- A tűz elleni védelmet elsődlegesen a személyi felügyelet, valamint a jelenlévő személyzet biztosítja a helyiségen belül készenlétben tartott, az MSZ 1040/1-5, vagy az MSZ EN 3 szabványoknak megfelelő kézi tűzoltó készülékekkel. A védelmet a tűzvédelem adminisztratív szabályozásával (Tűzvédelmi Szabályzat) kell erősíteni. A készenléti helyeken elsődlegesen gáz halmazállapotú oltóanyaggal feltöltött tűzoltó készülékek legyenek. A készülékek típusát és darabszámát, illetve elhelyezését a helyi tűzvédelmi utasításnak kell tartalmaznia. A készülékeket a helyiségeken belül a bejárat mellett, valamint a helyiség erre alkalmas, jól megközelíthető pontjain kell elhelyezni. A helyiségben a vonatkozó szabványok előírásainak megfelelő tűzjelző rendszert kell kiépíteni és üzemeltetni.
- Az elektromos hálózat elégítse ki az MSZ 1600 sorozatú szabványok előírásait, az érintésvédelem feleljen meg az MSZ 172 sorozatú szabványok előírásainak.

A megbízható működés szempontjából lényeges követelmény, hogy az elektromos hálózatot a szünetmenetességre, az áthidalási és újratöltési időre vonatkozó követelményeknek megfelelően kell kialakítani és külön leágazásról kell a táplálásról gondoskodni. Ha egy nem szerverszobának kijelölt hivatali helyiségben szerver üzemel, gondoskodni kell lokális szünetmentes tápáramellátásról.

- A villámvédelem elégítse ki a kommunális és lakóépületekre vonatkozó előírásokat.
- Az átlagostól eltérő klimatikus viszonyú (például a hőmérséklet, illetve a páratartalom értéke túllépi a számítástechnikai eszközökre vonatkozó megengedett tartományt) helyiségekben lokális klimatizálásról kell gondoskodni.
- Besugárzás ellen az alapbiztonsági osztály rendelkezésre állási követelményével arányos védelem indokolt.

4.3.2.3. Hardver/szoftver rendszer, adatok


Figyelj jól!

Az informatikai rendszer megbízható működését közvetlenül a kritikus hardver és szoftver elemek megbízhatósága határozza meg. Kritikus elemeknek tekintjük általában a központi egységet, a mágneslemez rendszert, az operációs rendszert, a hálózati szoftvereket és hardver elemeket, valamint az alkalmazói szoftvert.

Az alapbiztonság szintjén az informatikai rendszer kritikus elemeit nem szükséges tartalékolni. A kritikus hardverelemek megbízhatósága a mai technológiai színvonalon eléri azt a szintet, hogy megfelelő szervizhátteret feltételezve, tartalékolás nélkül biztosítani lehessen az alapbiztonságra meghatározott megbízható működést.

A szervizcégekkel olyan szerződést kell kötni, amely biztosítja a hibás elemek javításának megkezdését a bejelentéstől számított 12 órán belül. Ha ez nem sikerül, akkor cserekészüléket kell biztosítani. A javítási idő lerövidítése céljából az üzemeltető személyzetnek a hibát olyan szinten kell tudnia behatárolni, hogy a szerviz munkatársai felkészülten szálljanak ki a hibaelhárításra. E követelmény biztosításához az üzemeltető személyzetet megfelelő szintű oktatásban kell részesíteni. A helyszíni tartalékalkatrész-biztosítás szintjét alacsonyan lehet tartani, inkább az üzemeltetés során sűrűn pótlandó elemekből (például festék-szalag) célszerű tartalékot képezni.

A hardverrendszerre a szállítónak minimum 1 éves garanciát kell biztosítania. A rendszer értékétől függően 5-10 évig kell biztosítania a tartalékalkatrész-ellátást.

A hardveelemeknél a megelőző karbantartást az adott elemre vonatkozó karbantartási előírásoknak megfelelően el kell végezni.

Törekedni kell olyan beszerzési politika kialakítására, amely biztosítja egy független minősítő cég által kiállított minőségi bizonyítvánnyal rendelkező, helyszíni referencialátogatásokkal leellenőrzött számítástechnikai termékek beszerzését.

A szoftvertermékek esetében beszerezni, illetve installálni csak jogtiszta, megfelelő dokumentációval ellátott, vírus- és hibamentességre tesztelt szoftvert sza-

bad. Szabályozni kell az újonnan beszerzett szoftverek nyilvántartásba vételének és installációs feltételeinek módját, és a szoftverek másolásának, kivitelének módját.

Biztosítani kell a rendszer felfelé való kompatibilitását mind hardver, mind szoftver szempontból úgy, hogy a rendszer bővíthetősége, az alkalmazói rendszerek hordozhatósága hosszú távon biztosítható legyen. A szállítónak legalább 3 éves távon biztosítania kell a nagy értékű szoftverrel kapcsolatos szavatosságot és támogatást. A kritikus, különösen az egyedileg fejlesztett szoftverek forráskódját megfelelő letéti megbízásban szabályozott feltételek mellett közjegyzőnél vagy más hiteles letétben el kell helyezni. Ha a szállító részéről megszűnik a szoftvertámogatás, a felhasználónak a forráskód birtokába kell jutnia, hogy a támogatást akár saját erővel, akár külső kapacitással biztosítani tudja.

Az informatikai rendszerek funkcionalitásának biztosításában – mind a hardver, mind a szoftver területen – a rendszer tervezésében és megvalósításában alkalmazott módszertan által megkövetelt lépések maradéktalan végrehajtása a meghatározó. (Az ITSEC idevonatkozó követelményei teljes összhangban vannak a nemzetközileg elterjedt módszertanokkal, így a továbbiakban a funkcionalitás biztosításával kapcsolatos követelmények kifejtésében is az ITSEC-et követjük.)

A fejlesztést a következő fázisokra kell bontani:

- követelményrendszer megfogalmazása,
- globális rendszerterv, architektúraszintű tervezés,
- részletes megvalósítási terv,
- megvalósítás,
- tesztelés,
- átadás.

Már az alapbiztonság szintjén meg kell határozni:

- az egyes fázisokban elvégzendő tevékenységet, a formalizált eljárásokat,
- a fázisok dokumentációs előírásait és rendszerét,
- a minőségi követelményeket,
- a biztonsági követelményeknek és mechanizmusoknak az egyes fázisokra jellemző elkülönített kezelését.

4.3.2.4. Adathordozók

A 4.2.2 fejezetben az adathordozókra az információvédelmi alapbiztonsági osztályban meghatározott követelmények itt is érvényesek.

Ezeken túlmenően az adathordozók kezelésével, használatával és tárolásával kapcsolatban meg kell határozni:

- Az adathordozó-adminisztrációt, ezen belül:
  - a beszerzési szabályokat, a minőségi követelményeket, az ellenőrzési és engedélyezési eljárásokat a használatbavétel előtt,
  - a nyilvántartási rend kialakítását,

- a megsemmisítési, illetve újrafelhasználási eljárásokat,
- a készlet- és használat-nyilvántartást.

➠ Az adathordozók tárolására vonatkozó fizikai védelem követelményeit.

➠ A tárolók (helyiség, szekrény stb.) környezeti paramétereire (hőmérséklet, nedvesség, elektromos/mágneses zavarok) vonatkozó előírásokat és a paraméterek normál értékeinek biztosítására, valamint ellenőrzésére vonatkozó intézkedéseket.

➠ A megelőző intézkedéseket az elöregedésből fakadó adatvesztés ellen.

➠ Az adathordozók másodpéldányai (biztonsági másolatok) biztonságos tárolásának előírásait.

➠ Az adathordozók kölcsönzésével kapcsolatos előírásokat.

➠ A rendszer- és a felhasználói szoftver törzspéldányok biztonságos tárolására, valamint a használati másodpéldányok készítésére vonatkozó előírásokat.

4.3.2.5. Dokumentumok, dokumentáció

A 4.2.2.5 pontban az I/O dokumentumokra és a dokumentációra az információvédelem alapbiztonsági osztályban meghatározott követelmények itt is érvényesek.

Az informatikai rendszer késztermékek és fejlesztett elemek integrálása során alakul ki. Az informatikai rendszer beszerzéssel és/vagy fejlesztéssel történő kialakításához és az üzemeltetéshez, rendszer funkcionalitásának és megbízható üzemeltetésének biztosításához az **4.2.** táblázatban meghatározott dokumentációk beszerzése, illetve megvalósítása szükséges.

A biztonsági rendszer dokumentációjának tartalmaznia kell a biztonsági funkciók leírását, azok installációját, aktiválását, leállítását és használatát a fejlesztés, valamint az üzemeltetés során. A biztonsági rendszer dokumentációját csak az informatikai biztonsági felügyelő kezelheti.

A fenti dokumentumok alapján szabályozni kell:

➠ a szállítások fogadásával, az installációval és a rendszerindítással kapcsolatos követelményeket, feladatokat, procedúrákat és felelősöket,

➠ az üzemeltetési, karbantartási biztonsági előírásokat, valamint a karbantartási munkálatok előtti, illetve utáni intézkedéseket,

➠ a számítástechnikai eszközöket szállítókkal szemben a dokumentáció biztosításával kapcsolatos követelményeket,

➠ a dokumentumok nyilvántartási rendjét,

➠ a dokumentumok tárolására vonatkozó fizikai védelem követelményeit,

➠ a tárolók (helyiség, szekrény stb.) környezeti paramétereire (hőmérséklet, nedvesség, elektromos/mágneses zavarok) vonatkozó előírásokat és a paraméterek normál értékeinek biztosítására, valamint ellenőrzésére vonatkozó intézkedéseket,

➠ a számítástechnikai dokumentációkkal kapcsolatos változások követésére vonatkozó előírásokat,

Késztermék	Fejlesztett termék
Szállítási dokumentáció, minőségi bizonyítványok	Architektúra és konfiguráció szintű dokumentáció
Rendszerelemek egységek dokumentációi (Reference Manuals)	Modul szintű dokumentáció
Teljes rendszerdokumentáció	Teljes rendszerdokumentáció
Rendszerteszt dokumentáció	Tesztkövetelmények és eljárások dokumentációja modul szinten
Üzemeltetési dokumentáció (normál üzemeltetés, hibaelhárítás, újraindítás)	Tesztkövetelmények és eljárások dokumentációja rendszer szinten
Felhasználói dokumentáció (User's Guide)	Átadás/átvételi dokumentáció
Biztonsági rendszer dokumentációja	Üzemeltetési dokumentáció (normál üzemeltetés, hibaelhárítás, újraindítás)
	Biztonsági rendszer dokumentációja

4.2. táblázat

- a számítástechnikai dokumentációk másolására, kölcsönzésére vonatkozó előírásokat.

A biztonsági rendszer dokumentációjának tartalmaznia kell a biztonsági funkciók leírását, azok installációját, aktiválását, leállítását és használatát a fejlesztés, valamint az üzemeltetés során. A biztonsági rendszer dokumentációját csak az informatikai biztonsági felügyelő kezelheti.

A megbízható működéssel kapcsolatos eseményekről (rendszer indítás/leállás, nagyobb üzemzavarok, alap- és felhasználói szoftverekkel kapcsolatos, a megbízható működést érintő események) gépi, illetve manuális biztonsági naplózásokat kell végezni. Meghatározandók azok tartalmi követelményei, a naplók kezelési, értékelési és tárolási módja. A biztonsági napló tartalmi és formai követelményei legyenek összhangban az információvédelmi biztonsági naplózásnál ismertetett követelményekkel (lásd 4.2.2.1 pont!).

4.3.2.6. Adatok

Az adatok kezelésével kapcsolatban a következőket kell szabályozni:

- a biztonságos adatbevitellel kapcsolatos előírások kialakítása,
- az adatvesztés pótlására vonatkozó szabályok kialakítása,
- adatszolgáltatási előírások kialakítása.

4.3.2.7. Kommunikáció, osztott rendszerek

- A helyi hálózatok, a kommunikációs kábelek műanyag védőburkolattal ellátott kábelcsatornában legyenek vezetve a helyi lehetőségek által megszabott lehető legnagyobb magasságban.
- 100-nál nagyobb felhasználószámú hálózat esetén javasolt a strukturált kábelezési rendszer alkalmazása. Ez lényegesen növeli a hálózat üzembiztos működtetését, a kábelezés struktúrájában bekövetkező változások (például költözés) rugalmas kezelését.
- A hálózat diszkrét elemeit (elosztó szekrények, bridge-ek, router-ek, modemek stb.) olyan zárható helyiségben kell elhelyezni, ahol biztosíthatók az üzembiztos működéshez szükséges hőmérsékleti feltételek is.
- Az átvitel biztonsága érdekében az adatátvitelben a CRC-CCITT szerinti hibafelismerési és- javítási szintet vagy ezzel azonos hatékonyságú védelmet kell biztosítani az átviteli eljárásokban, amely a kettős bithibák felismerésére alkalmas. Ezt a manapság elterjedt szinkron adatátviteli eljárások biztosítják.
- Már az alapbiztonsági osztályban szükséges valamilyen szintű hálózatmenedzsment alkalmazása. Általában két szinten valósul meg:
  - fizikai szintű menedzsment, amely alapvetően a hálózat összefüggőségét (connectivity) a kábelezés és a hálózat diszkrét eszközeinek fizikai szintjén vizsgálja, és lehetővé teszi a hálózat legkisebb egybefüggő szakaszára a fizikai kapcsolat megszűnésének detektálását,
  - logikai szintű menedzsment, amely a hálózat felsőbb rétegei szintjén ellenőrzi az összefüggőséget.

  Ma a logikai hálózati menedzsmentre de facto standardként az SNMP szintű menedzsmentet használják, amelynek egyszerűsített és bővített változata ismert.

  Alapbiztonsági osztályban 100 user-nél nagyobb hálózatokon az egyszerűsített SNMP szintű menedzsment használatát biztosítani kell, a bővített használata javasolt.

Adminisztratív úton *szabályozni* kell:

- a hálózati elemek fizikai és környezeti veszélyek (tűz, elektromos/mágneses zavarok stb.) elleni védelmére vonatkozó előírásokat,
- a biztonságot befolyásoló események naplózására vonatkozó követelményeket,
- a hálózati szoftverek védelmére vonatkozó előírásokat.

➠ A rendelkezésre állás és a biztonságos rendszer-visszaállítás biztosításához a következő követelményeket kell kielégíteni:
- ha az osztott rendszer a felhasználónak megtagadja a kért szolgáltatást (Denial of Service, röv.: DoS), megfelelő mechanizmust kell biztosítani a szolgáltatások degradációjának detektálására és közlésére (például nem megfelelő az átviteli áteresztőképesség, a megcímzett hálózati rész nem érhető el, a kért erőforrás nem áll rendelkezésre stb.),
- biztosítani kell a néhány perces kiesés áthidalását.

4.3.2.8. Személyek

Minden szervezetnél ki kell alakítani azt a személyzeti struktúrát, amelynek feladata és felelőssége az informatikai rendszer megbízható üzemeltetése, és ezáltal az alkalmazások megbízható működésének biztosítása. Az informatikai biztonság területén a következő jól elhatárolható feladatokat kell meghatározni, és az elvégzésükért felelős személyeket kijelölni, illetve alkalmazni.

- Őrző/védő feladatok ellátását biztosító személyzet, amely elsősorban a szervezet egészének és ezen belül az informatikai rendszernek a fizikai védelmét biztosítja. Feladataik kijelölése és alkalmazásuk a szervezet vezetésének feladata. Erre a feladatra csak olyan személyek alkalmazhatók, akik erkölcsileg feddhetetlenek és megbízhatók, valamint rendelkeznek az őrző/védő feladatok ellátásához szükséges vizsgákkal, minősítésekkel.

➠ Az informatikai szervezeti egység vezetőjének ki kell jelölnie a legfontosabb részrendszerek (rendszerszoftver, hálózatiadatbázis-kezelők, levelező rendszerek stb.) rendszer-adminisztrátorait, feladataikat és felelősségüket meg kell határoznia.

➠ Az informatikai szervezeti egység vezetőjének, valamint a nagyobb és fontos alkalmazási területek vezetőinek egymással egyeztetve ki kell jelölniük a fontos alkalmazások rendszergazdáit, feladataikat és felelősségüket meg kell határozniuk.

➠ Az informatikai szervezeti egység vezetőjének gondoskodnia kell az üzemeltető és karbantartó személyzet olyan szintű kiképzéséről, hogy az egyszerűbb hibákat mind a hardver-, mind a szoftverterületen elhárítsák, illetve az összetettebbeket a szervizszemélyzet részére körülhatárolják.

➠ A szervezet általános biztonságáért felelős vezetőnek és az informatikai szervezeti egység vezetőjének szabályoznia kell:
- külső személyek belépési és tartózkodási rendjét az informatikai biztonság szempontjából kritikus területeken,
- a kilépőkkel kapcsolatos informatikai biztonsági intézkedéseket,
- rendszeres oktatás rendjét a felhasználók, az adminisztrátorok, a rendszergazdák, az üzemeltető és karbantartó személyzet részére az informatikai

rendszer megbízható üzemeltetésével és biztonságos használatával kapcsolatban,
- az informatikai biztonság megsértése esetén a személyekre vonatkozó intézkedéseket.

4.3.3. Fokozott biztonsági osztály

4.3.3.1. A fokozott biztonsági osztály minimális követelményei

- A szerverszobában ki kell építeni a technikai védelmi rendszert. A riasztásoknak az épület biztonsági szolgálatánál meg kell jelenniük.
- Az informatikai rendszer legyen ellátva másodlagos villámvédelemmel.
- A központi egység rendelkezzen egy laza csatolású (például hálózaton keresztül biztosított) melegtartalékkal vagy egy hidegtartalék-egységgel. A mágneslemezegységek és kritikus hálózati elemek, illetve kapcsolatok tartalékolása szintén biztosított legyen. Az adatbázis-kezelő szoftver rendelkezzen automatikus adatállomány-mentési és -visszaállítási funkciókkal.
- A szállítóval és a szervizcégekkel olyan garanciális, illetve garancián túli szervizszerződést kell kötni, amely garantálja a megbízható működés fokozott biztonsági osztályra definiált *rendelkezésre állási* szint betarthatóságát. A szervizszerződésben minimálisan 8 órás reakcióidő kikötése ajánlott.
- A kritikus hardver- és hálózati elemekről olyan szintű dokumentációval kell rendelkezni, hogy az üzemeltető személyzet az egység- vagy kártyaszintű hibaelhárítást el tudja végezni.

4.3.3.2. Infrastruktúra

Fizikailag az informatikai rendszer megbízható, működési szempontból kritikus részeit kell elsősorban védeni. A mai rendszertechnikai megoldásokból kiindulva elsősorban ez a számítóközpontok, a szerverszobák és az egyéb „központi" jellegű informatikai helyiségek (de nem az irodák!) védelmét jelenti.

- A helyiségbe csak annak üzemeltetéséhez elengedhetetlenül szükséges közműhálózat csatlakozhat, tehát a helyiségen belül nem mehet át víz-, gáz-, csatorna- és egyéb közművezeték. Felette és a határoló falfelületeken vizes blokkot tartalmazó helyiségrész ne legyen, nyomó- és ejtőcsövek ne haladjanak át, gázvezetéket telepíteni tilos.
- Az alapbiztonsági osztály tűzvédelmi követelményein túl a számítógépes helyiség ajtaja rendelkezzen legalább 30 perces (műbizonylatolt) tűzgátlással, továbbá a helyiségen belül automatikus és kézi jelzésadók kerüljenek telepítésre. A jelzésadók jelzéseit mind a helyiségen belül, mind az épület biz-

tonsági szolgálatánál meg kell jeleníteni. A jelzésadó eszközök, valamint a jeleket feldolgozó központ feleljen meg az MSZ 9785, valamint az EN 54 szabványsorozatok előírásainak, rendelkezzenek a hazai minősítő intézetek forgalomba hozatali engedélyével.

- Az elektromos hálózat legalább a szerver és a szükségvilágítás vonatkozásában 30 perces áthidalási idejű megszakításmentes átkapcsolással rendelkező szünetmentes tápegységgel legyen ellátva. A tápegység akkumulátorai a maximális igénybevételt követő töltés hatására teljes kapacitásukat 24 órán belül nyerjék vissza.
- A villámvédelem elégítse ki a kommunális és lakóépületekre vonatkozó előírásokat, és az MSZ IEC 1312-1 (Az elektromágneses villámimpulzus elleni védelem) szabvány szerint az LPZ 0_B – LPZ 1 zónahatáron túlfeszültség elleni védelembe kell bevonni az árnyékolást megtestesítő, az épületbe belépő minden fémszerkezetet (az elektromos hálózatot, víz-, gáz-, távfűtés-, csatornahálózatokat, antennabevezetéseket, adatátviteli és távbeszélő hálózatokat stb.).
- A padlóburkolatok, berendezési tárgyak antisztatikus kivitelűek legyenek.
- A túlmelegedés elleni védelmet a helyiség klimatizálásával kell biztosítani. A légellátásnak a klimatizáló berendezések által átlagos szinten biztosított porkoncentrációt kell elérnie.
- Besugárzás ellen a fokozott biztonsági osztály rendelkezésre állási követelményével arányos védelem indokolt.

4.3.3.3. Hardver/szoftver rendszer

A fokozott biztonsági osztályban az előírt megbízható működési mutatóval, illetve a megengedett kiesési idővel arányos tartalékolási intézkedéseket kell megvalósítani. Ez elsősorban a kritikus hardverelemekre vonatkozik. A központi egység hálózaton keresztül történő tartalékolása és/vagy a megfelelő tartalék alkatrész biztosítása elegendő ezen a biztonsági szinten.

A lemezegységeknek redundáns (tükrözés, Raid technika) kiépítésűeknek kell lenni.

Biztosítani kell az állandó jellegű on-line backup file készítést az operációs rendszer vagy az adatbázis-kezelő szoftverrendszer szintjén, hogy fájlművelet megszakadás esetén rövid idő alatt megtörténhessen az eredeti fájlok visszaállítása (recovery).

A hálózatok megbízhatóságának növelésére azok túlterhelését, hálózatrészek kiesését megelőző, a helyi adottságoknak megfelelően kiválasztott rendszertechnikai megoldásokat (redundáns átviteli utak, illetve aktív elemek, dinamikus átkonfigurálás, osztott hálózatvezérlés stb.) kell kialakítani.

A szerviz háttérhez – amelynél indokolt a 8 órás *rendelkezésre állás* – csak indokolt esetben kelljen fordulni. A szerviz megjelenéséig az üzemeltető személyzetnek olyan átmeneti megoldást kell találnia, hogy a rendszer üzeme a megengedett kiesési idő lejárta előtt biztosítható legyen.

A fejlesztett szoftverek esetében rendelkezni kell a forrásnyelvi kóddal, és biztosítani kell a forráskód szintű hibajavítás feltételeit. A fejlesztett szoftverek tesztelési eljárásait részletesen le kell dokumentálni, a szoftverüzemeltetőknek a tesztelésben részt kell venniük.

A szállítónak legalább 5 éves távon biztosítania kell a nagy értékű szoftverrel kapcsolatos szavatosságot és támogatást.

4.3.3.4. Adathordozók

A biztonsági másolatokat az elsődleges tároló helyiségtől elkülönített helyen, a fokozott biztonság követelményei szerint kialakított helyiségben, másodlagos adathordozón kell tárolni.

A DOS alapú rendszerekben idegen adathordozó használatának megakadályozására olyan logikai védelmet kell használni, amely a PC védelmi rendszerében csak a már előzetesen regisztrált és valamilyen formában engedélyezett programok indítását teszi lehetővé. Az ilyen szintű rendszer az adatfájlok idegen adathordozóról történő beolvasása ellen nem nyújt védelmet, de minden, az adathordozóról indított vagy onnan beolvasott program aktivizálását megakadályozza. Ezt a védelmi funkciót a vírusvédelmi programok némelyike biztosítja.

4.3.3.5. Dokumentáció

A kritikus hardver- és hálózati elemekről rendelkezni kell olyan szintű dokumentációval, hogy az üzemeltető személyzet a tartalék egységek vagy alkatrészek segítségével az egység vagy *kártya szintű hibaelhárítást* el tudja végezni.

A rendszer hibajavítási és újraindítási dokumentációja olyan szintű legyen, hogy az erre az osztályra jellemző megbízható működés elérését támogassa.

4.3.3.6. Kommunikáció, osztott rendszerek

A kábelezésre vonatkozóan az EIA/TIA-568 Kereskedelmi Épületkábelezési Szabvány, valamint a kisugárzással, illetve a zavartatással kapcsolatos EN 55022 és EN 5024 szabványok a mérvadók. Egyéb tekintetben a csavart érpáros *árnyékolatlan* kábeltípus követelményei megfelelőek. 50-nél nagyobb felhasználószámú hálózat esetén javasolt a strukturált kábelezési rendszer alkalmazása.

50 felhasználónál nagyobb hálózaton a bővített SNMP szintű menedzsmentet használni kell, a fizikai hálózat menedzsment használata javasolt.

A szolgáltatásokat hálózati elemek, számítástechnikai erőforrások kiesése esetén degradált szinten kell biztosítani.

A szolgáltatás megszűnésének okát a hálózatmenedzsment szoftvernek detektálnia, regisztrálnia és jeleznie kell.

4.3.4. Kiemelt biztonsági osztály

4.3.4.1. A kiemelt biztonsági osztály minimális követelményei

- A számítóközpontok, a szerverszobák és az egyéb „központi" jellegű informatikai helyiségek legyenek ellátva intelligens beléptető rendszerrel, amely a mozgásokat két irányban regisztrálja, és legalább 4 000 eseményt képes naplózni egy időben.
- A szerverszobában vízhűtéses klíma nem üzemeltethető.
- A számítóközpontok, a szerverszobák és az egyéb „központi" jellegű informatikai helyiségek legyenek ellátva automatikus működtetésű oltórendszerrel.
- A központi egység rendelkezzen egy szoros csatolású melegtartalékkal és megfelelő automatikus áttérés menedzsment megoldással. A mágneslemezegységek és kritikus hálózati elemek, illetve kapcsolatok tartalékolása a megbízható működés kiemelt biztonsági osztály *rendelkezésre állási* követelményeinek megfelelő szinten legyen biztosítva.
- A szállítóval és a szervizcégekkel olyan garanciális, illetve garancián túli szervizszerződést kell kötni, amely garantálja a megbízható működés kiemelt biztonsági osztályra definiált *rendelkezésre állási* szint betarthatóságát. A szervizszerződésben minimálisan 4 órás reakcióidő kikötése ajánlott.
- A teljes hardver/szoftver rendszerről és a hálózati elemekről olyan szintű dokumentációval kell rendelkezni, hogy az üzemeltető személyzet az egység- *vagy a kártya*szintű hibaelhárítást el tudja végezni.
- A személyzet összetétele és kiképzettsége olyan legyen, hogy erre a biztonsági osztályra meghatározott 16 perces kiesési időt tartani tudja a kiemelt fontosságú alkalmazások, illetve a teljes rendszer kiesése esetén.

4.3.4.2. Infrastruktúra

- A fűtést a klímarendszeren keresztül meleglevegő-befújással kell megoldani, a helyiségben vizes fűtés nem létesíthető. A klímarendszer kültéri és beltéri egységből épüljön fel, vízhűtéses klíma nem telepíthető. Központi klímagép telepítése esetén a befújó és az elszívó légcsatornába légmentesen záró, tűzgátló tűzcsappantyúkat kell telepíteni.
- A szerverszobába csak az annak üzemeltetéséhez elengedhetetlenül szükséges közműhálózat csatlakozhat.
- A helyiség automatikus működtetésű oltórendszerrel egészítendő ki, az oltórendszer működését tekintve helyi vagy teljes elárasztásos legyen, működése előtt biztosítson elegendő időt a személyzet evakuálására, vezérlő kimeneteinek egyikén adjon jelzést a szerver felé az automatikus mentésre, majd azt követően a lekapcsolásra.

- Az energiaellátás biztonsága érdekében a szünetmentes tápegység mellett szükség-áramellátó dízel-elektromos gépcsoport is telepítendő, amely automatikus indítású és szabályozású, teljesítménye képes kiszolgálni a számítástechnikai eszközökön túl azok működéséhez szükséges segédüzemi (például klíma) berendezéseket is.
- A villámvédelem a fokozott biztonsági osztály követelményein túl a központi erőforrások (szerverek) és a munkaállomások részére egyaránt biztosítsa az MSZ IEC 1312-1 (Az elektromágneses villámimpulzus elleni védelem) szabvány szerint az LPZ 1–LPZ 2 zónahatáron a túlfeszültség elleni védelmet úgy az energiaellátó, mint az adatvonalak részére egyaránt.
- Besugárzás ellen a kiemelt biztonsági osztály rendelkezésre állási követelményével arányos védelem indokolt.

4.3.4.3. Hardver/szoftver

Ebben a biztonsági osztályban a központi egység esetében a kívánt megbízható működési szint *nagy sebességű kapcsolaton* keresztül, szoros csatolással megvalósított tartalékolással érhető el. A központi egységek normál üzemmódban végezhetnek különböző funkciókat (master-slave üzemmód), ez esetben az áttérési idő hosszabb, de még elegendően rövid a megengedett kiesési időhöz képest. Rövidebb áttérést lehet biztosítani, ha a tartalék gép ugyanazt a feladatot végzi, mint a biztosított, és a szükséges adatfrissítések is párhuzamosan megtörténnek (hot stand by üzemmód). Ez a megoldás általában drágább. A választott tartalékolási módot a kitűzött megbízható működési célok, a tartalékolási módok költségei és a rendszer konfigurációjának elemzése alapján lehet kiválasztani.

A lemezegységek tartalékolása ebben az osztályban is tükrözéssel vagy Raid eljárással történjék.

A szerviz háttérhez – amelynél a 4 órás *rendelkezésre állás* szükséges – csak indokolt esetben kelljen fordulni. A szerviz megjelenéséig az üzemeltető személyzetnek olyan átmeneti megoldást kell találnia, hogy a rendszer üzeme a megengedett kiesési idő lejárta előtt biztosítható legyen.

A szállítónak legalább 8 éves távon biztosítania kell a nagy értékű szoftverrel kapcsolatos szavatosságot és támogatást.

4.3.4.4. Adathordozók

A biztonsági másolatokat az elsődleges tároló helyiségtől *földrajzilag* elkülönített helyen, a fokozott biztonság követelményei szerint kialakított helyiségben, másodlagos adathordozón kell tárolni.

4.3.4.5. Dokumentáció

Dokumentációt kell készíteni a referenciahitelesítési mechanizmus (monitor) megvalósítási módjáról. Ennek tartalmaznia kell a logikai védelem rendszertervének, a biztonsági és az informatikai rendszerek közötti interfészek szemiformális leírását, a referenciarendszer védelmi tulajdonságait, a védelmi funkciók szemiformális specifikációját, amelyekkel bemutatható, hogy az nem megkerülhető és a potenciális támadások ellen jól véd. Tartalmaznia kell az informatikai rendszer tesztelési eljárásainak dokumentációját, így például azoknak a tesztmódszereknek az eredményeit, amelyeknek a rejtett csatornák sávszélessége hatékony csökkentésének vizsgálata a céljuk.

Biztosítani kell a *számítástechnikai eszközökkel támogatott változásmenedzsmentet,* amely gépi úton biztosítja az informatikai rendszer fejlesztése és üzemeltetése során beállt változások, módosítások és a vonatkozó dokumentációk közötti összhangot.

A *teljes hardver/szoftver rendszerről és a hálózati elemekről* rendelkezni kell olyan szintű dokumentációval, hogy az üzemeltető személyzet a tartalék egységek vagy alkatrészek segítségével az egység- vagy kártyaszintű hibaelhárítást el tudja végezni.

A fejlesztett szoftverek esetében rendelkezni kell a forrásnyelvi kóddal, *a futási idejű (run time) programok könyvtáraival,* és biztosítani kell a forráskód szintű hibajavítás feltételeit. A fejlesztett szoftverek tesztelési eljárásait részletesen le kell dokumentálni, a szoftverüzemeltetőknek a tesztelésben rész kell venniük.

4.3.4.6. Kommunikáció, osztott rendszerek

A kábelezésre vonatkozóan az EIA/TIA-568 Kereskedelmi Épületkábelezési Szabvány, valamint a kisugárzással, illetve a zavartatással kapcsolatos EN 55022 és EN 5024 szabványok a mérvadók, a csavart érpáros *árnyékolt* kábeltípus alkalmazandó. 50-nél nagyobb user-számú hálózatok esetében strukturált kábelezési rendszer használandó.

A szolgáltatásokat az eredetivel azonos szinten kell biztosítani hálózati elemek, számítástechnikai erőforrások kiesése esetén, automatikus tartalékolással. Például az adatátviteli kapcsolatokat kettőzni vagy hálózaton keresztül útvonalvezérléssel olyan rövid (csatornák közötti) átkapcsolási idővel kell tartalékolni, hogy az átvitelre kerülő adatoknál az adatvesztés (hibajavítással, ismétléssel) elkerülhető legyen.

4.3.4.7. Személyzet

A személyzet összetétele és kiképzettsége olyan legyen, hogy erre a biztonsági osztályra meghatározott 16 perces kiesési időt tartani tudja a kiemelt fontosságú alkal-

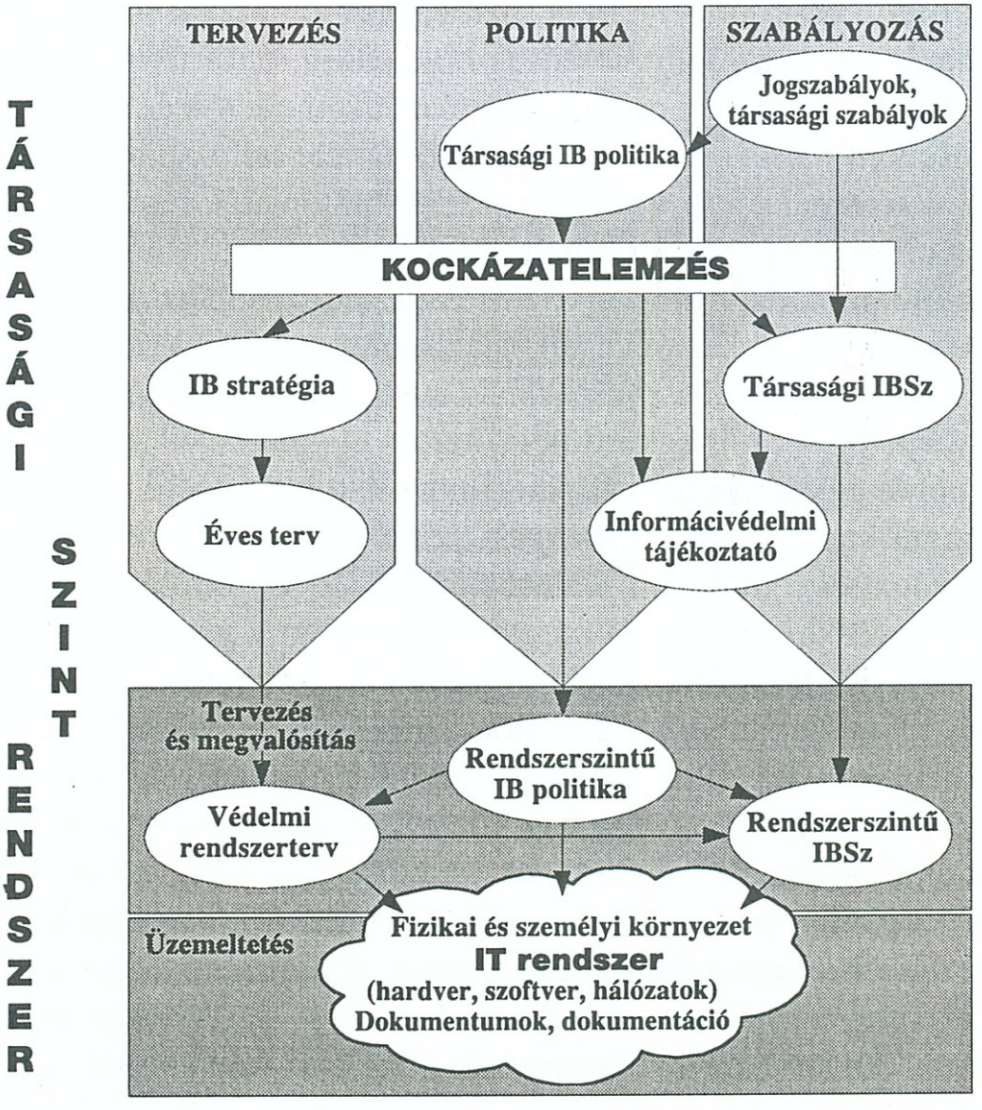
mazások, illetve a teljes rendszer kiesése esetén. Ehhez feltétlenül szükséges, hogy az üzemeltető, karbantartó személyzet rendszeres oktatással és gyakorlattal szinten tartsa az ismereteit a rendszerrel és azokkal az egységekkel kapcsolatban, amelyek üzemeltetéséért és karbantartásáért felelős.

Fontos szempont a rendszer üzemeltetésében és karbantartásában kulcsszerepet betöltő személyek erkölcsi és anyagi érdekeltségének megfelelő szintű biztosítása a fluktuáció elkerülése céljából. A kulcsszakértők kiesése a rendszer kiemelt megbízható működési szintű üzemeltetésében komoly gondot tud okozni, pótlásuk külső forrásból általában nehezen megoldható. Ezért gondoskodni kell arról, hogy a szakértők tudása „átlapolt" legyen, azaz egy hardver-, illetve szoftverterülethez a kulcsember mellett más is értsen.

5. A védelem megvalósítása

A védelem megvalósítása ebben a fejezetben nem csupán egy eszközrendszer megvalósítását, hanem egy szervezet teljes, azaz a fizikai, a logikai és az adminisztratív védelmi rendszerére vonatkozóan, a tervezéstől a megvalósításig terjedő folyamatát jelenti. Ennek a folyamatnak a vázlatát az **5.1.** ábra mutatja.

Egy nagyobb szervezetnél, ahol kiterjedt az IT infrastruktúra, nagy az alkalmazások száma, az adminisztratív szabályozási háttér nem valósítható meg egy politikával és egy szabályzattal, mert ha azok a részletekre is kiterjednek, akkor a politikai és a szabályzati dokumentumok egyszerűen kezelhetetlenek lesznek. Ezért nagy szervezeteknél az adminisztratív védelemnek társasági és rendszerszintekre tagolt hierarchikus szerkezetét kell kialakítani.



5.1. ábra

6. Az informatikai biztonság tervezése


Tanuld meg!

Egy informatikai rendszer számtalan pontján és sokféle módon támadható, így – különösen, ha az nagyméretű és összetett – a védekezés helye és módja egyáltalán nem kézenfekvő feladat. A teljes körű, zárt és kockázatarányos védelem létrehozása csak egy átgondolt tervezési folyamat után valósítható meg, amelynek új vagy rekonstruálandó informatikai rendszer esetén az adott feladat teljesítésére indított informatikai projekt keretében kell megvalósulnia.

Sajnos ennek a megfontolásnak ellentmond a jelenlegi gyakorlat. Tapasztalati tény, hogy az informatikai rendszerek és az általuk kezelt adatok fizikai és logikai védelmi rendszere minden rendszerelemre kiterjedő, és a potenciális fenyegetéseket figyelembe vevő tervezésére ritkán kerül sor. Gyakran „ad hoc" módon kialakul a jelszóhasználat, és valamilyen hozzáférési gyakorlat, amelyek nem sok összefüggést mutatnak a szervezet informatikai biztonságpolitikájával – már, ha van ilyen. A biztonsági naplózás és az auditálhatóság biztosítása rendszerint elmarad, így sok esetben a megtörtént biztonsági eseményekről az üzemeltetők és a vezetők nem tudnak, illetve ha tudnak, az események bizonyító háttere nem áll a rendelkezésükre.

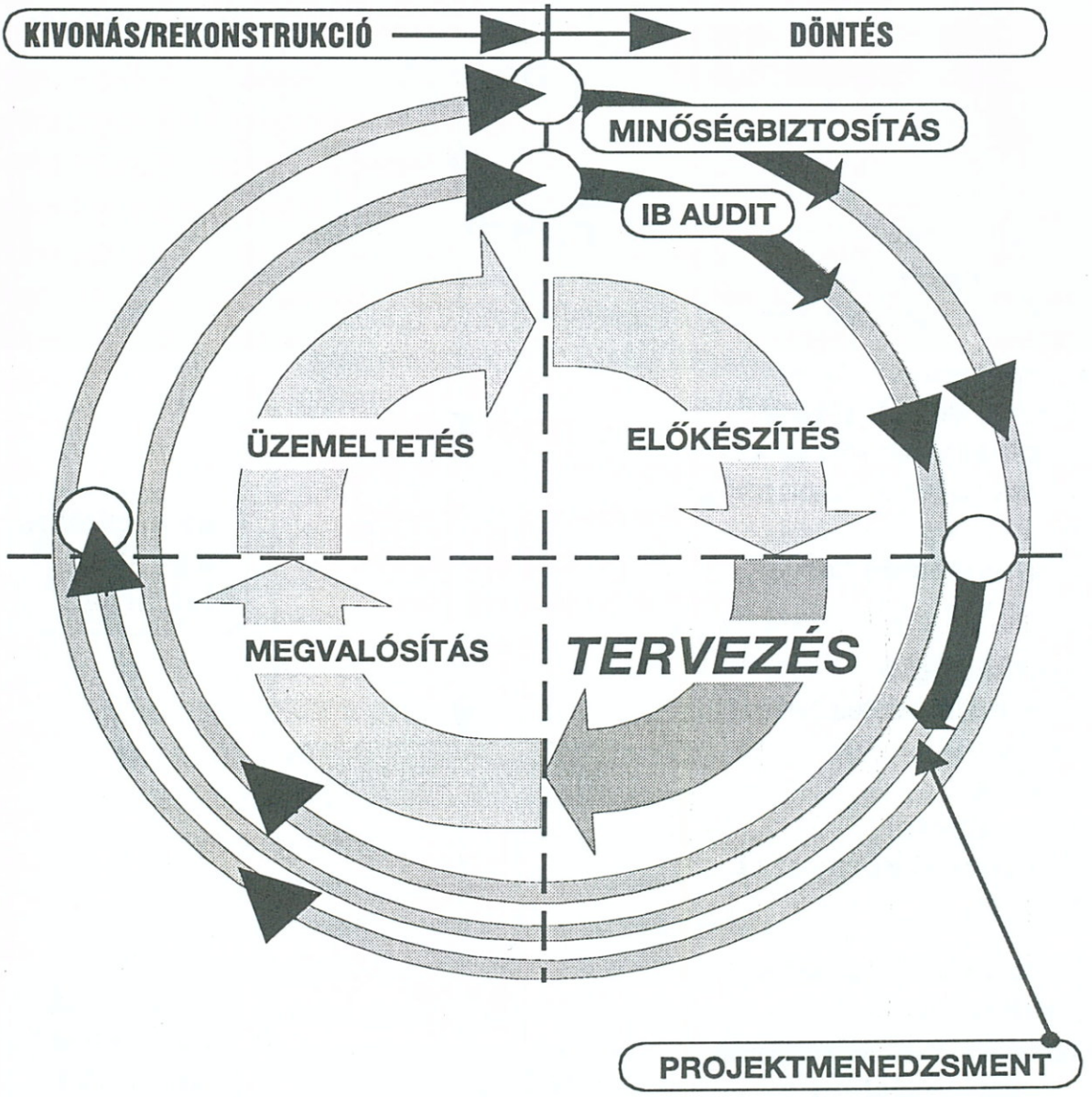
Az informatikai rendszerek és környezetük biztonsági rendszere legtöbbször nem a fejlesztési, megvalósítási projekt szerves részeként valósul meg, hanem a projekt befejezése után, akár több éves késéssel, leginkább az első biztonsági esemény bekövetkezése után. Ez azért jelent gondot, mert így a biztonsági megoldások többnyire a kényszerszülte improvizált megoldások szintjén maradnak, amelyek hatékonysága gyakran megkérdőjelezhető.

Jellegzetes példa egy lényeges védelmi funkció, a biztonsági naplózás megoldása. A biztonsággal kapcsolatos események (be/ki lépés, hozzáférések, tranzakciók követése stb.) rögzítése általában jelentős erőforrás- és tárolásikapacitás-igényű. Amennyiben a biztonsági naplózás megtervezése nem a projekt során történik és az informatikai rendszer erőforrásai, konfigurációs paraméterei nem ennek megfelelően kerülnek kialakításra, akkor a naplók legtöbbször egyáltalán nem, vagy csak nagyon korlátozottan valósulhatnak meg, mert a menedzsment nem vállalja be a rendszer funkcionalitásának és/vagy hatékonyságának csökkenését. Másik példa – amely sajnálatos módon szinte valamennyi társaságnál, vállalatnál megfigyelhető – a biztonság felügyeletének, illetve menedzsmentjének (események figyelése, értékelése, szükséges beavatkozások meghozatala stb.) elmaradása. Ennek a biztonsági funkciónak nem tulajdonítanak jelentőséget. Ugyanakkor könnyen belátható, hogy a vállalat a funkció bevezetése esetén idejében felismerheti a közelgő veszélyt, megelőzhet például egy támadást, így jelentősen csökkentheti az esemény bekövetkezése során fellépő üzleti veszteségeit.

Az *informatikai biztonsági rendszer,* azaz a *fizikai* és a *logikai védelmi rendszer* megtervezésének, valamint az *adminisztratív védelem* koncepciója felállításának minden informatikai projekt részének kell lennie.

Az informatikai biztonsági rendszerre is éppúgy vonatkozik az életciklus-szemlélet, mint magára az informatikai rendszerre. Ezt az elvet fejezi ki az **6.1.** ábra.

Tanuld meg!

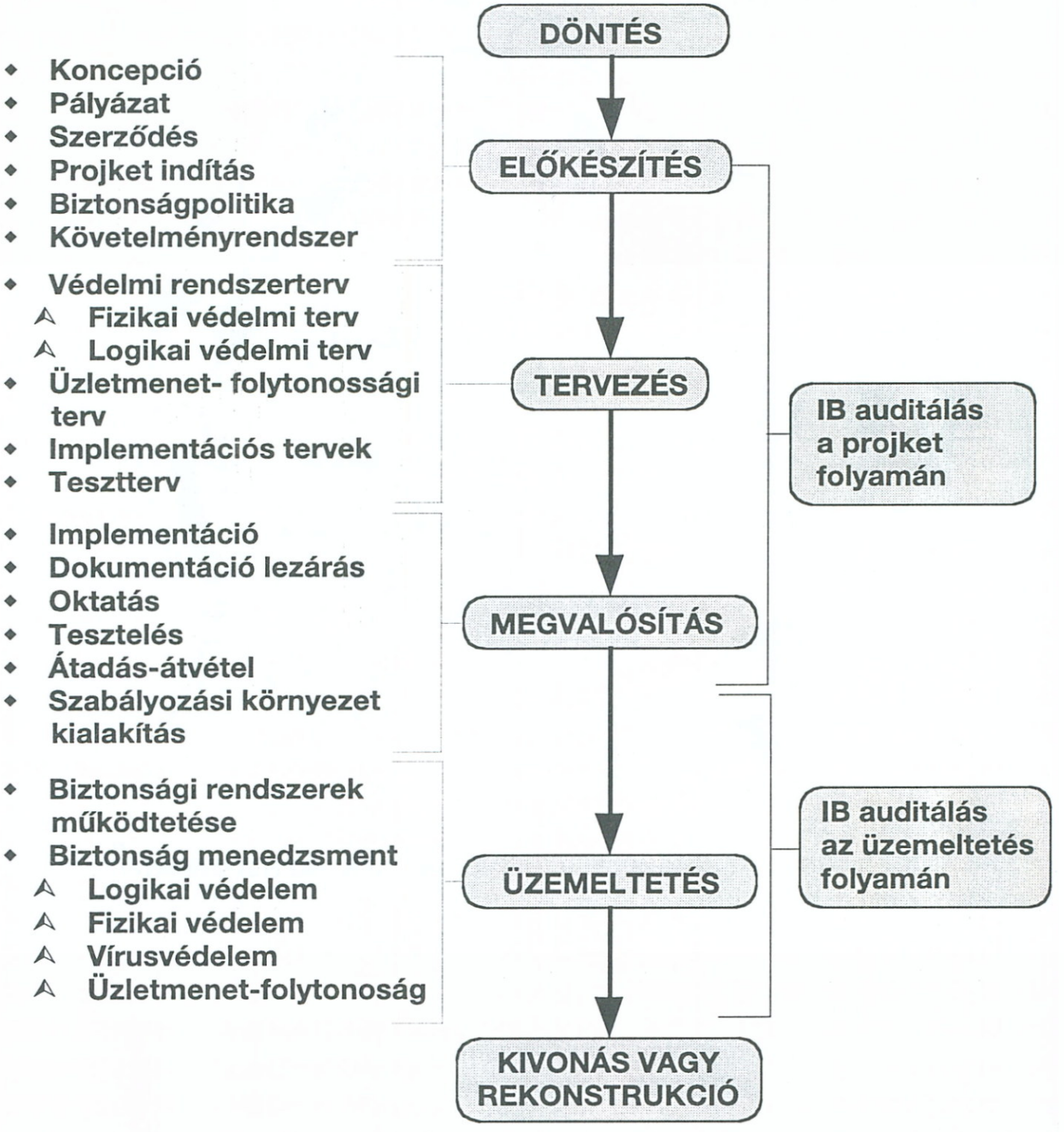


6.1. ábra

Minden informatikai rendszer „léte" a létrehozásáról szóló döntéstől kezdve négy szakaszra oszlik (előkészítés, tervezés, megvalósítás, üzemeltetés) egészen a rendszer kivonásáig, illetve rekonstruálásáig. Ezt az életciklus-szemléletet az informatikai biztonsági rendszerekre is érvényesíteni kell, azaz a megvalósítást elő kell készíteni, meg kell tervezni, majd a megvalósítás után üzemeltetni, fenntartani és továbbfejleszteni kell.

Tanuld meg!

Jelen fejezet az életciklus négy fázisa közül a tervezéssel foglalkozik részletesen, azonban a következőkben az előkészítési fázissal kapcsolatban felsoroljuk a legszükségesebb tudnivalókat és teendőket. Az **6.2.** ábra összefoglalva mutatja be az informatikai rendszerek életciklusa során az informatikai biztonsági rendszerekkel kapcsolatos főbb ciklusszakaszokat és lépéseket.



6.2. ábra

Az informatikai biztonsági rendszer „élete" az informatikai rendszerről szóló döntéssel kezdődik. A döntésről szóló dokumentumnak tartalmaznia kell a biztonsági rendszer megvalósításának szükségességét (indokolását) és a finanszírozási feltételeket.

Az informatikai rendszerekre vonatkozó ajánlatkérések, pályázatok kiadása előtt meg kell határozni a *minimális informatikai biztonsági követelményeket.*

Az informatikai rendszerre vonatkozó ajánlatkiírásban és ennek megfelelően a pályázatban és annak értékelésében is szerepelnie kell az informatikai biztonsági fejezetnek.

Az informatikai projekt kifejezést a következőkben széles értelemben használjuk, mert a tervezés és megvalósítás tárgya lehet számítógépes infrastruktúra (hálózat, hardver, alapszoftver rendszerek) vagy alkalmazásszintű. Az alkalmazás is lehet „zöld mezős" fejlesztés vagy standard, csomag alapú. A tervezési lépések különbözhetnek, mert például egy csomag alapú alkalmazás már eleve magában hordozza (hordozhatja) a biztonsági lehetőségeket, míg egy alkalmazás fejlesztésénél a biztonsági funkciókat „testre szabottan" kialakítására.

Biztonsági rendszert természetesen lehet informatikai projekten kívül is tervezni, ebben a fejezetben azonban a fejlesztési lépéseket a projektmenedzsment szokásos lépéseivel szinkronban adjuk meg. A biztonságtervezést szervezetnek célszerű a saját fejlesztési módszertanához illesztenie az informatikai rendszer funkcionális fejlesztésével való összhang megtartása érdekében.

A **6.1.** ábra szerintieknek megfelelően a teljes projektet minőségbiztosítás és informatikai biztonsági auditálás kíséri, amelyekre vonatkozó ellenőrző pontokat és ellenőrző tevékenységeket a projekt minőségbiztosítási tervnek kell tartalmaznia.

Az implementáció során a részletes rendszertervekben meghatározott védelmi funkciók és intézkedések kerülnek megvalósításra az informatikai rendszer hardver- és szoftvereszközein, valamint a fizikai környezetben. Az implementáció során a teljes projektre alkalmazott változásmenedzsmentet a biztonságtervezés és megvalósítás területére is alkalmazni kell annak érdekében, hogy a végső dokumentáció és az implementált, letesztelt rendszer egymással összhangban legyen.

A védelmi rendszer tesztelése a tervezési fázisban elkészült tesztelési tervek alapján történik, amelyben a korábban meghatározott gyenge pontok és potenciális fenyegetések figyelembevételével tesztelni kell a biztonsági funkciókat és azok védelmi mechanizmusának erősségét a biztonsági funkciók közötti kapcsolatokat, azok esetleges erősítő vagy gyengítő kölcsönhatásait.

A tesztelési fázist rendszerszintű teszt zárja le, amelynél több biztonsági funkció együttes működése kerül tesztelésre. A tesztelési eredmények dokumentálásra kerülnek.

Az informatikai rendszer éles üzemre történő átadásáig elkészítendő a rendszerszintű Informatikai Biztonsági Szabályzat, amelyet az üzemeltetésvezető véleményez és véglegesít. A jóváhagyás a szervezet informatikai biztonsági menedzserének feladata.

A védelmi rendszer funkció és rendszerszintű tesztje után előre meghatározott ideig üzemi jellegű tesztelést kell megvalósítani, amely már valós üzemi környezetben és feltételek mellett történik. Az üzemi teszt során észlelt rendellenességeket dokumentálni és értékelni kell. Az indokolt módosításokat a védelmi rendszerben meg kell valósítani. Az összes módosítás elvégzése után az informatikai rendszer átadás-átvételi eljárása keretében átadásra kerülhet a teljes védelmi rendszer.

Az üzemi teszt megkezdése előtt a vezetők, a végfelhasználók és az üzemeltetők részére külön csoportokban és az egyes szerepköröknek megfelelő tematikával oktatást kell biztosítani.

7. A szabályozás

A bármilyen gondosan is megtervezett és bevezetett fizikai és logikai védelem nem valósítja meg maradéktalanul a teljes védelmi rendszert, ha – a tervezést megelőzően – hiányoznak, vagy nem lettek hatályba léptetve azok a politikai elkötelezettségek, amelyek érvényre juttatják a szervezet tulajdonosainak és menedzsmentjének akaratát az informatikai biztonság vonatkozásában, ha hiányoznak azok a szabályok, amelyek gyakorlati szinten érvényesítik a politikában kifejtett vezetői akaratot. A politikák és a szabályzatok optimális esetben egyértelművé teszik, hogy mit szabad tenni és mit nem, valamint azt is, hogy a szabályok megsértése milyen következményekkel jár. Az **5.1.** ábra szerint a fizikai és logikai védelmen túl szükséges a politikák és a szabályzatok hierarchikus rendszerét mint az *adminisztratív védelem* egyik fontos területét is kialakítani a védelmi rendszer teljessége és menedzselhetősége érdekében.

7.1. Az informatikai biztonságpolitika

Ha az információ védelme és/vagy az informatikai rendszer megbízható működése sérül, az a szervezetnek közvetlen vagy közvetett károkat okoz. Ez a károkozás azért rendkívül veszélyes, mert általában nem néhány drámai következményekkel járó esemény keretében valósul meg – bár ilyen is előfordul –, hanem a károk lappangó, a vezetés számára egy ideig észrevétlen módon, sok kis esemény formájában realizálódnak. Amikor a problémák már észrevehető szinten jelentkeznek, azok megszüntetése már sokkal nagyobb nehézségekbe ütközik – sőt, némelykor már nem is lehetséges – és jóval nagyobb anyagi ráfordítást igényel. Az előzőekből következik, hogy az informatikai biztonság biztosítása állandó folyamat, amelynek fenntartása megfelelő viszonyulást, magatartást feltételez. Ennek kialakításában jelent vezérfonalat az informatikai biztonságpolitika.

Az informatikai biztonságpolitika (irányelv) szerepe az, hogy a szervezet teljes egészére, egységes szemlélettel megfogalmazza azt a vezetői akaratot, amely meghatározza minden munkatárs viszonyát az informatikai rendszerek által kezelt adatok bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának megőrzéséhez, annak érdekében, hogy a sokszor nehezen kiszámítható politikai és gazdasági környezeti változások közben is a szervezet védelmi és túlélő képességei stabilak maradjanak. Az informatikai biztonságpolitiká-

nak meg kell fogalmaznia egy olyan tájékoztatási politikát is, amely biztosítja a megfelelő külső és belső tájékoztatást.

Ahhoz, hogy bármilyen biztonságpolitikát meg lehessen határozni, néhány alapkérdést kell tisztázni. Ezek a következők:

- Azonosítani kell, hogy milyen védendő tárgyaink, értékeink vannak. Minél több az értékünk, ez annál nagyobb vonzerőt gyakorol a támadókra. Az informatikai biztonság esetében fel kell mérnünk az informatikai rendszerekben kezelt adatokat. Azokat az adatköröket, amelyek bizalmasság, hitelesség, sértetlenség, rendelkezésre állás vagy a funkcionalitásban betöltött szerep vonatkozásában érzékenyek, a követelményrendszerben meghatározott érzékenységi szintekre kell besorolni.
- Meg kell határozni, hogy milyen szintű védelmet kell biztosítani a feltérképezett adatkörökre. Ehhez ismerni kell a releváns fenyegetéseket, az azok által okozott kockázatok szintjét. Ez csak kockázatelemzésen alapuló biztonsági vizsgálattal érhető el, amelyet vagy a teljes társaság, vagy egy adott informatikai rendszer szintjén kell elvégezni. A kockázatok szintjétől függ az alkalmazandó védelmi funkciók erőssége. Annak érdekében, hogy ezek a szintek elfogadhatók legyenek, a kezelt adatok érzékenységi szintje alapján a szervezet minden lényeges informatikai rendszerét biztonsági osztályba kell sorolni. A politikának tehát definiálni kell a biztonsági osztályokat, és mint politikai elvet ki kell jelenteni, hogy a biztonsági osztályba sorolást minden fontos rendszerre el kell végezni. Ennek természetes és logikus időpontja az informatikai projektek előkészítési szakasza (l. **6.** fejezet). Az adott rendszerre vonatkozó konkrét biztonsági osztálybasorolást a rendszerszintű biztonságpolitikának kell tartalmaznia.

Fontos, hogy a társasági informatikai biztonságpolitikának legyen olyan rövid, az informatikai, illetve a biztonsági területen nem jártas munkatársak számára is érthető változata, amelyet minden munkatársnak el kell olvasnia, és aláírásával ezt igazolnia kell. Ez az információvédelmi tájékoztató (l. **5.1.** ábra). Sok külföldi cégnél ezt (is) társasági szintű informatikai biztonságpolitikának nevezik (Company Level IT Security Policy).

Mint azt a **5.1.** ábra mutatja, a társasági és a rendszerszintű informatikai biztonságpolitikának alapvető jelentősége van az adminisztratív védelmi rendszer többi alkotóeleme vonatkozásában. A társasági informatikai biztonságpolitikát figyelembe kell venni az információvédelmi tájékoztató, a rendszerszintű politikák és a társasági szintű Informatikai Biztonsági Szabályzat kidolgozásánál.

A társasági szintű informatikai biztonságpolitika – szerkezetét és a főleg a biztonsági funkciókat érintő politikák vonatkozásában – meghatározó jelleggel bír a rendszerszintű politikákra nézve, amelyek konkrét politikái (például jelszókezelési, a hozzáférési politikák) viszont a védelmi rendszerterv kidolgozásához szükségesek.

7.2. Informatikai Biztonsági Szabályzat

A politika érvényesítésének első szakasza a szabályozás, amely nem más, mint a politikában elfogadott célok és elvek alapján történő működési rend és mód meghatározása.

Ahhoz, hogy a szabályozási folyamat működjön a következő feltételek szükségesek:

- a realitásokat figyelembe vevő, „működőképes" szabályzatot kell kidolgozni, és hatályba léptetni (például vezetői utasítással);
- egyértelmű vezetői akarat kell a szabályzat érvényesítéséhez, a szabályzat működéséhez szükséges emberi és egyéb erőforrás-feltételek biztosításához;
- az érvényesítésben szerepet játszó személyekre pontosan meg kell határozni a szabályzathoz kapcsolódó feladat-, felelősség- és hatáskört;
- ki kell alakítani az ellenőrzés rendszerét, és azt működtetni kell;
- az intézkedések, a szankcionálás következményeit az azért felelős személynek fel kell vállalnia.

Az előzőekben elmondottak minden szabályozásra – így az informatikai biztonság szabályozására is – érvényesek.

Az Informatikai Biztonsági Szabályzat felépítésének a korábban megfogalmazott védelmi alapelveket kell figyelembe venni, azok közül is elsősorban a *teljes körűségre* és a *folytonosságra* törekedve.

A teljeskörűség követelménye azt jelenti, hogy az Informatikai Biztonsági Szabályzatnak minden rendszerelemhez, így

- a fizikai környezethez,
- a hardver- és szoftverrendszerhez,
- a kommunikációhoz, számítógépes hálózatokhoz,
- az adathordozókhoz,
- az input/output dokumentumokhoz és a dokumentációhoz,
- a külső és belső személyi környezethez

kapcsolódó biztonsági szabályokra kell kiterjednie.

A folytonosság követelménye azt jelenti, hogy az Informatikai Biztonsági Szabályzatnak át kell fognia az informatikai rendszer teljes életciklusát, azaz az előkészítés, a tervezés, a megvalósítás, az üzemeltetés fázisait egészen a kivonásig/rekonstrukcióig.

Nagyobb szervezeteknél az informatikai biztonság szabályozását két szinten javasolt megvalósítani (l. **5.1.** ábra). A társasági szintű Informatikai Biztonsági Szabályzat a társaság minden szervezeti egységére általános érvénnyel meghatározza az informatikai rendszerrel és környezetével kapcsolatos biztonsági szabályokat és intézkedéseket, szervesen illeszkedve a szervezet egyéb működési, ügyrendi és biztonsági előírásaihoz, továbbá meghatározza az eljárások rendjét, a felelősöket, az ellenőrzés rendjét és a szankcionálás módját.

A társasági Informatikai Biztonsági Szabályzat térjen ki a fejlesztés, beszerzés, karbantartás és üzemeltetés általános biztonsági szabályaira. Rögzítse az informatikai rendszerek fejlesztése területén a biztonsági rendszerek tervezésére, fejlesztésére, megvalósítására, tesztelésére és bevezetésére vonatkozó szabályokat.

Foglalkozzon a vírusvédelem, a hálózatok, a külső hozzáférések, az üzletmenetfolytonosság-tervezés és menedzsment, a változásmenedzsment, a biztonságmenedzsment általános szabályaival.

A rendszerszintű Informatikai Biztonsági Szabályzat a társasági Informatikai Biztonsági Szabályzat struktúráját követve, az abban szereplő előírásokat bontja le az adott rendszerhez kapcsolódó, konkrét, a szabályozás hatálya alá tartozó területre érvényes és értelmezhető szabályokra, nevezze meg az egyes feladatok végrehajtásában kompetens beosztásokat, szervezeteket (felelős, irányító, végrehajtó, ellenőrző stb.). Rendszerszintű Informatikai Biztonsági Szabályzatot minden nagyobb alkalmazásra, a számítóközpontokra és a számítástechnikai infrastruktúrára ki kell alakítani.

A rendszerszintű Informatikai Biztonsági Szabályzatokban az általános szabályokat az adott rendszerre nézve konkréttá kell tenni. A részletes szabályok kialakítása függ az informatikai rendszer jellegétől (alkalmazás, hálózat, számítóközpont stb.). A nem értelmezhető fejezeteket el lehet hagyni, és ha szükséges, újakat kell kidolgozni.

A szabályozás lényeges eleme az érvényesítés. A legtöbbször ez a tevékenység marad el, mert nem világosak az érvényesítés szempontjai, területei, és nem biztosítottak a személyi és anyagi feltételek.

A társasági szintű Informatikai Biztonsági Szabályzatot minden olyan területen érvényesíteni kell, ahol informatikai rendszerben adatokat kezelnek. Ha az érvényesítés nem teljes körű, azaz nem egyenszilárdságúan érvényesül minden szervezeti egységnél, akkor a politika és a szabályzatok különböző értelmezése, megvalósítása, valamint az ellenőrzés részleges kiterjedése miatt gyenge pontok alakulnak ki. Ezért nagyon fontos, hogy a politika és a szabályzatok érvényesítését, valamint az ezeknek való megfelelés ellenőrzését olyan szervezeti egységek végezzék, amelyeknek a teljes társaságra nézve megvan a hatáskörük e tevékenységek elvégzésére, és függetlenek az ellenőrzött szervezeti egységektől.

Az informatikai biztonságpolitikában megfogalmazott védelmi alapelvek alapján pontosan meghatározhatók azok a dimenziók, amelyek megszabják az érvényesítés irányait.

Érvényesítés az informatikai rendszer teljes életciklusában

- Minden informatikairendszer-beruházás előkészítésében az informatikai biztonsági rendszerrel kapcsolatos követelményeket, valamint a megvalósításhoz szükséges anyagi és humán erőforrásokat fel kell mérni, be kell állítani a beruházási tervbe, és megfelelő elemzés után jóvá kell hagyatni.
- Vezetői szinten biztosítani kell, hogy az informatikai rendszerek megvalósítási projektjének szerves része legyen a biztonsági rendszer tervezése és

megvalósítása. Informatikai rendszer ne legyen átvehető éles üzemre a biztonsági rendszer megfelelő tesztelése és elfogadása nélkül!

- Az üzemeltetés szakaszában az érvényesítés eszköze a biztonság menedzselési és adminisztrációs funkciók kialakítása és ezek működtetéséhez a megfelelő IT és informatikai biztonságmenedzsment eszközrendszer és humán feltételek biztosítása.
- Az informatikairendszer-üzemeltetésből történő kivonása keretében a biztonsági rendszer megszüntetését (jelszavak, jogosultságok megszüntetése, biztonsági adatállományok, adathordozók biztonságos törlése és üzemen kívül helyezése stb.) szabályozottan kell végrehajtani.

7.3. Az informatikai biztonsági stratégia

Tanuld meg!

Miért van szükség informatikai biztonsági stratégiára? Stratégiára azért van szükség, hogy kialakítható legyen – egy hosszú, akár több éves fejlődési, fejlesztési folyamaton keresztül – egy előre meghatározott, egy távlati céllal összhangban levő összetett rendszer.

Az informatikai biztonsági stratégia kidolgozásánál az első lépés egy *jövőkép* (hova *akarunk eljutni*) kialakítása, amelynek teljes összhangban kell lennie a szervezet IT stratégiájával és az üzletpolitikájából fakadó biztonsági célkitűzésekkel. A jövőképnek tartalmaznia kell elképzeléseket az informatikai biztonságpolitika várható változására. Nagyon aktuális példa, hogy például az e-business fejlesztése a szervezetnél biztosan nagyban befolyásolni fogja a szervezet informatikai biztonságpolitikáját. A stratégiának fel kell tudnia vázolni, hogy ez a hatás várhatóan a politika mely területén milyen hatást fog kifejteni. Tartalmaznia kell az eszközrendszerre, az informatikai biztonságmenedzsmentre, a szabályozási rendszerre és az informatikai biztonsági szervezetre vonatkozó jövőképet.

A következő lépés a *jelenlegi helyzet értékelése* (honnan *indulunk*). A jelenlegi helyzet és a jövőkép ismeretében az informatikai biztonsági stratégiai tervezői már látják a kettő közötti „távolságot", amelyet be kell járni ahhoz, hogy a jövőkép megvalósuljon. Az anyagi és más erőforrás-feltételek, a vállalati célkitűzések függvényében többféle út elképzelhető a jövőkép elérésére. A feltételrendszerek, a megvalósíthatóság és sikertényezők elemzésével javasolni kell a lehetséges „útvonalak" közül egyet, amelyet a stratégiai tervezők a felállított üzleti, informatikai és biztonsági elvárásoknak megfelelően a legkedvezőbbnek ítélnek. Ki kell jelölni a preferált útvonalat „kifeszítő" azon *kulcs projekteket,* amelyek sikeres megvalósításával a jövőkép elérhető.

Az éves tervezés a stratégiai terv birtokában következik. Lényege az, hogy a stratégiai terv megfelelő része éves szintre le legyen bontva, költségtényezőként be legyen állítva és jóvá legyen hagyva. Ezután már a megvalósítás következhet.

7.4. Titokvédelmi és Ügyviteli Szabályzat

7.4.1. Titokvédelmi Szabályzat

Az információvédelem szabályozása céljából elkészítendő Titokvédelmi Szabályzatról írunk. Ezekben az összefüggésekben – mintaszerűen – az üzleti titkot tekintjük védendőnek, és minősített adat alatt az üzleti titokként kezelt adatot értjük.

A Titokvédelmi Szabályzat kiterjed minden, a szervezetnél – akár belföldön, akár külföldön – keletkezett, kezelt, birtokában levő, tulajdonát képező, illetve mások által rábízott tényre, információra, megoldásra vagy adatra, valamint ezek bármely megjelenési módjára, például iratra, informatikai adathordozóra, írásbeli vagy szóbeli közlésre, melyek tartalmát nem minősítették nyilvános információnak.

A Titokvédelmi Szabályzat célja, hogy a teljes szervezetre vonatkozóan egységesen meghatározza:

- az üzleti titok és az „egyéb" (bank-, értékpapír-, biztosítási stb.) titok fogalmát és tartalmát, továbbá kezelésük, felhasználásuk és védelmük szabályait;
- a megkülönböztetett védelem elrendelésére és az információ minősítésére kötelezettek és jogosultak körét;
- a minősítési eljárás és a minősített adatok megismerésének rendjét;
- a védelmi feladatok végrehajtásának szervezeti rendjét;
- a szervezet alkalmazottainak vonatkozó feladatait, kötelezettségeit és jogait

annak érdekében, hogy mindazok, akik a szervezet tevékenységében közreműködnek, megismerhessék és felhasználhassák a feladatuk ellátásához szükséges minősített információkat, de egyúttal ilyen információk illetéktelenek tudomására ne juthassanak.

Az államtitok és szolgálati titok körébe tartozó iratok, információk esetében az 1995. évi LXV. törvény, és az arra vonatkozó rendeletek, utasítások szerint kell eljárni!

7.4.2. Ügyviteli Szabályzat

A különböző minősítésű iratok kezelésének szabályozása érdekében Ügyviteli (Iratkezelési) Szabályzatot kell kiadni, amelyben a Titokvédelmi Szabályzat figyelembevételével kell meghatározni az egyes iratfajták – minősítési szintjüktől függő – kezelésének (készítésének, iktatásának, továbbításának, tárolásának stb.) részletes szabályait.

Az Ügyviteli Szabályzat térjen ki:

- Az ügyvitel szervezeti rendjére;
- Az ügyvitel alapelveire;
- Az ügyvitelben részt vevők feladataira;

- Az ügyviteli munka ellenőrzésére;
- Az általános ügyviteli eljárásokra, különösen: az iratok nyilvántartására
- Az iratkezelési feladatokra az ügyintézés folyamatában;
- Az irattározás és levéltárba adás rendjére.

7.5. Üzletmenetfolytonosság-tervezés

7.5.1. Az üzletmenet-folytonosság fogalma

Az informatikai rendszerek megbízható működése területén meghatározó tényező az üzletmenet-folytonosság (Business Continuity Planning, röviden: BCP) biztosítása. Alapvető célja az, hogy a szervezetnek az üzleti folyamatait támogató informatikai erőforrásai a rendelkezésre álló üzemidőben a lehető legjobb időkihasználással és a legmagasabb funkcionalitási szinten működjenek – figyelembe véve az üzemzavari és katasztrófaesemények széles skáláját – annak érdekében, hogy az üzleti folyamatok zavara által okozott közvetlen és közvetett károk minimálisak legyenek.

Az üzletmenet-folytonosság ideális esetben azt jelenti, hogy az üzleti folyamatokat támogató informatikai rendszerek egy hosszabb időszakon át megszakítás nélkül, folyamatosan és a kívánt funkcionalitási szinten működnek.

Ez az állapot azonban csak elméletileg létezik. A valóságban – az informatikai rendszer hardver- és szoftverösszetevőinek korlátos megbízhatósága, illetve a környezeti fenyegetések bekövetkezése miatt – az informatikai rendszerek üzemi működése kisebb-nagyobb megszakításokat szenved el, amelyek következtében előálló kiesések közvetlen és/vagy közvetett károkat okoznak a szervezetnek.

Megfelelő üzletmenet-folytonosságnak tekintjük az informatikai rendszer üzemi működése folyamatosságának azt a szintjét, amely során a kiesési kockázati szint a szervezet számára elviselhető. Másként kifejezve egy meghatározott időszakokra vetítve a működéskiesésekből származó károk összessége a szervezet számára elviselhető.

Az üzletmenet-folytonosság kívánt szintjét megfelelő megelőző, illetve a kiesés bekövetkezése után visszaállító intézkedésekkel kell biztosítani, amelyek megvalósítását előzetesen meg kell tervezni. A továbbiakban az *üzletmenet-folytonosság-tervezés* alatt a vészhelyzeti (katasztrófa[7]) és a nem katasztrofális jellegű üzemza-

[7] A katasztrófa olyan helyzet, amikor az informatikai rendszert vagy a környezetét olyan természeti csapás, erőszakos beavatkozás vagy műszaki zavar éri el, amely a teljes rendszer funkcionális működésének kiesésével, szélsőséges esetben a rendszer vagy környezete fizikai megsemmisülésével jár.

vari események által előidézett üzemiműködés-kiesések megelőzését, minimalizálását, illetve a kiesési időben helyettesítő részfolyamat-beiktatást és visszavonást célzó tervezési lépéseket értjük. A fő cél az, hogy a tartalék informatikai és a humán erőforrások megfelelő szintű rendelkezésre állását, mobilizálását *tervezett* műszaki és szervezési megoldásokkal és intézkedésekkel úgy biztosítsuk a kiesés idejére, hogy az informatikai szolgáltatások visszaállítása a szervezet által meghatározott sebezhetőségi résen belül megvalósuljon.

Az üzletmenetfolytonosság-tervezés terméke az *üzletmenet-folytonossági terv*, amely részletesen meghatározza a kívánt üzletmenet-folytonosság fenntartásához szükséges megelőző, helyettesítő, illetve visszaállító intézkedések megvalósításához szükséges feltételeket, szervezeti és szervezési lépéseket és a megvalósítás módját.

A hagyományos értelemben vett *katasztrófaelhárítás-tervezés* (Disaster Recovery Planning, DRP) és az üzletmenetfolytonosság-tervezés között az alapvető különbség az, hogy az üzletmenetfolytonosság-tervezés a szervezet üzleti folyamatainak előre meghatározott minimális kiesési idejű és kívánt funkcionalitású működésének biztosítását célozza meg *a kiesést előidéző események széles spektrumában.*

A katasztrófaelhárítás-tervezés – hagyományos értelmezésben – csak a katasztrófaeseményeknek az informatikai rendszerek kritikus elemeire vonatkozó hatásait elemzi, és tervet ad olyan globális helyettesítő megoldásokra, valamint megelőző és elhárító intézkedésekre, amelyekkel a bekövetkezett katasztrófaesemény után az informatikai rendszer funkcionalitása degradált vagy eredeti állapotában visszaállítható. Tehát figyelmen kívül hagyja az, ugyan nem katasztrófa szintű, de az üzemi működés folytonosságát lényegesen befolyásoló üzemzavari események halmazát. Ezzel a tervezés látószögéből egy olyan eseményhalmaz kerül ki, amely – figyelembe véve a megengedett sebezhetőségi rést – lényeges szerepet játszik a károkozásban, a megkívánt üzletmenet-folytonosság veszélyeztetésében.

A nemzetközi irodalomban és egyre inkább a gyakorlatban is a katasztrófaelhárítás-tervezést az üzleti működésfolytonosság-tervezés részeként fogják fel abban az értelemben, hogy az informatikával támogatott üzleti folyamatokat zavaró események halmazába a katasztrófaesemények is beletartoznak. Ilyen értelemben a katasztrófaelhárítás-tervezés az üzletmenetfolytonosság-tervezés integráns részét képezi, azaz az üzletmenetfolytonosság-tervezés során az üzleti folyamatok folytonos működését zavaró teljes eseményhalmazt – beleértve a katasztrófaeseményeket is – vesszük figyelembe és azok hatása megítélésében az üzleti folyamatok zavara vagy kiesése által, a szervezet belső működésében és szolgáltatásaiban okozott károk játsszák a főszerepet.

A továbbiakban tehát az üzletmenetfolytonosság-tervezés alatt a vészhelyzeti (katasztrófa) és a nem katasztrofális jellegű üzemzavari események által előidézett szolgáltatáskiesések megelőzését, illetve minimalizálását célzó tervezési lépéseket értjük.

7.5.2. Az üzletmenetfolytonosság-tervezés célja

A teljes körű üzletmenet-folytonosság terv kialakítása a következő előnyöket hozza magával:

- a gazdasági veszteségek minimalizálása,
- az üzletmenet-folytonosságot veszélyeztető fenyegetések csökkentése,
- az üzletmenet-folytonosságot megszakító események számának, illetve időtartamának csökkentése,
- az üzemeltető szervezetek stabilitásának növelése,
- a visszaállítási folyamat hatékonyságának és szervezettségének növelése,
- az informatikai rendszerre vonatkozó biztosítási feltételek javítása,
- a kulcsszemélyektől való függőség csökkentése,
- a szervezet informatikai rendszerét és a környezetét alkotó vagyontárgyak, valamint az adatvagyon épsége védelmi szintjének növelése,
- a személyzet és az ügyfél szolgáltatások biztonságának növelése,
- a döntéshozatali kényszerek csökkentése az üzemzavar- és katasztrófaelhárítás folyamatában,
- a jogszabályoknak és a belső szabályzatoknak való megfelelés erősítése.

7.5.3. Üzletmenetfolytonosság-tervezés, költségek, kockázatarányosság

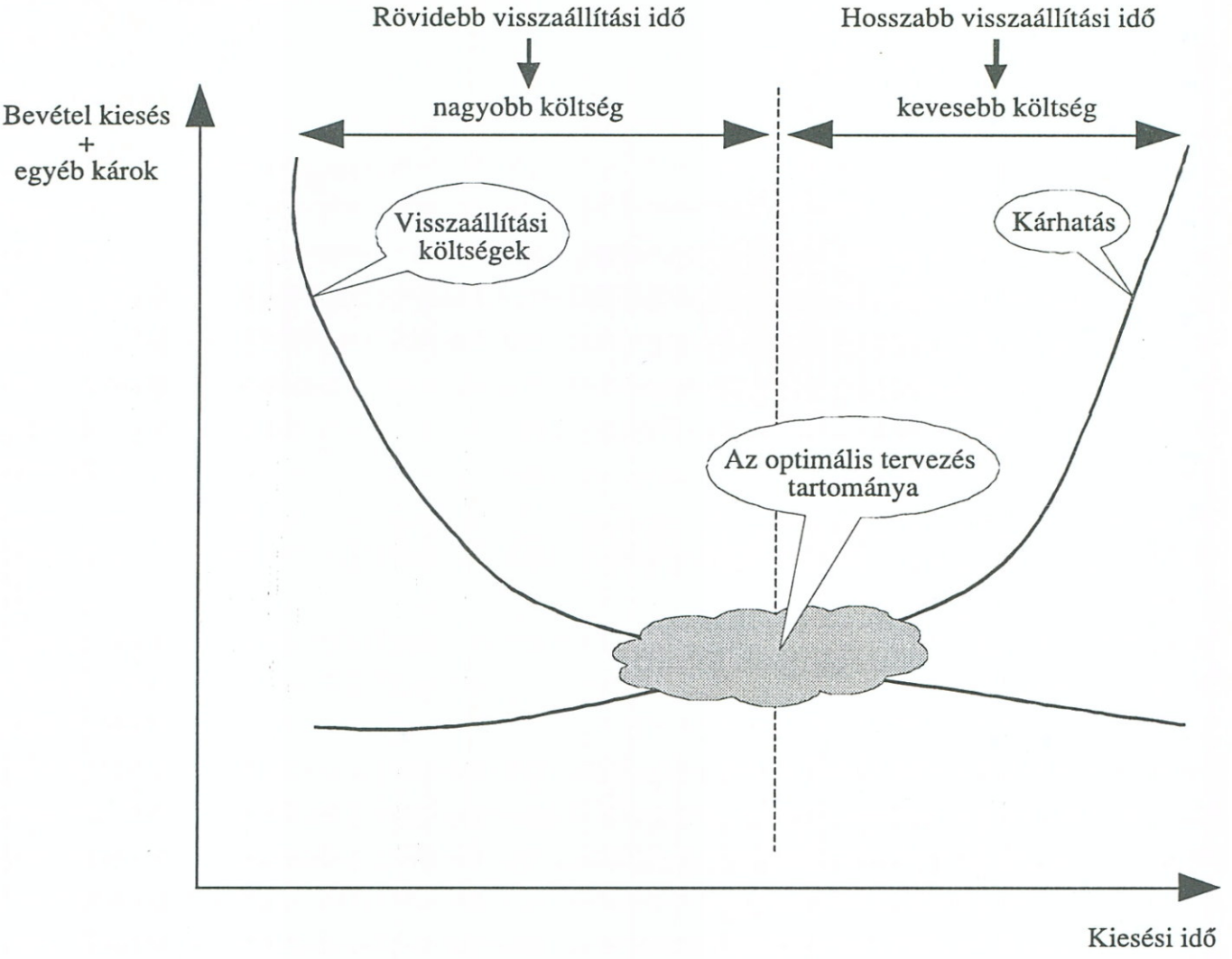
Mint minden biztonsági intézkedés, az üzletmenetfolytonosság-tervezés és a katasztrófaelhárítás-tervezés által javasolt intézkedések költségvonzatát sem lehet figyelmen kívül hagyni. A tervezés egyik lényeges eleme a kiesési kockázatok elemzése, amelynek során mérlegelni kell az okozott kár nagyságát és az üzemzavari események, a veszélyhelyzetek bekövetkezésének gyakoriságát. A kár nagyságát magának az informatikai és környezeti rendszerelemnek az értéke, a kiesés következtében előálló közvetlen és közvetett működésbeli és üzleti károk határozzák meg. Az üzemzavarból eredő vészhelyzetek bekövetkezési gyakoriságát a berendezések minősége, megbízhatósága, az üzemeltető személyzet képzettsége, tapasztalata és többek között a földrajzi elhelyezkedés befolyásolja, például természeti katasztrófák (földrengés, hurrikán stb.) által gyakrabban sújtott területen más fajsúlyú és költségű erőforrás-biztosítás és intézkedési rendszer szükséges, mint egy kevésbé veszélyeztetett területen.

A katasztrófaelhárítás-tervezés célja a kiesési idő, a rendszer normál állapotának lehető legrövidebb időn belül történő visszaállításán túl az, hogy ezt a *kockázatokkal arányosan* lehessen megvalósítani. Más szóval a normál állapot visszaállítását nem „mindenáron", hanem a valószínűsíthető kárnagyság és bekövetkezési gyako-

Tanuld meg!

riséggal arányos költségszinten kell biztosítani, azaz *minimális költségráfordítással maximális kockázatcsökkenést* kell elérni.

Ezt az elvet szemléletesen a **7.1.** ábra mutatja be.



7.1. ábra

7.5.4. Az üzletmenet-folytonosság tervezési folyamata

Tanuld meg!

Az üzletmenetfolytonosság-tervezés összetett és költséges folyamat, ezért célszerű, ha azt projektszerűen, azaz projektmenedzsmenttel kísérve valósítjuk meg. A következőkben az üzletmenetfolytonosság-tervezés folyamatát egy feltételezett projekttervbe ágyazott formában mutatjuk be.

Az üzletmenetfolytonosság-tervezés folyamata a következő fő fázisokra tagozódik:

1. Helyzetfelmérés és értékelés

2. Az üzletmenet-folytonossági terv elkészítése

3. Oktatás, tréning és tesztelés

Helyzetfelmérés és értékelés

- Projekt-előkészítő megbeszélés, amelyen megtörténik:
- A részletes projektterv elkészítése.
- Projektindító megbeszélés, amelyen:
- Előzetes helyzetfelmérő interjúterv elkészítése és véglegesítése (területek, személyek, előzetes ütemezés).
- Az interjúk megszervezése (személyek és időpontok egyeztetése), az interjúterv véglegesítésre kerül.
- Az interjútematikák elkészítése.
- A projektvezetőnek átadásra kerülnek a projekttervben maghatározott dokumentumok, az interjútematikák továbbításra kerülnek az interjúalanyokhoz.
- Az interjúk elvégzése az interjúterv szerint, amelyekről emlékeztetők készülnek.
- Az interjúk és a feldolgozott dokumentumok alapján meghatározásra kerülnek:
  - a szervezet üzletmenet-folytonossága szempontjából kritikus üzleti folyamatok és az ezeket támogató alkalmazások,
  - a kritikus informatikai rendszerek kiesésének következményei, kockázatai és rangsorolása a szervezet hatékony és eredményes működése szempontjából (üzletihatás-elemzés – Business Impact Analysis),
  - a kritikus alkalmazások rendelkezésre állási követelményeire vonatkozó javaslatok, amelyeket a szervezet megfelelő működési területein kompetens vezetői jóváhagynak,
  - a kritikus alkalmazások, az informatikai infrastruktúra elemei és az informatikai személyzet közötti kapcsolatrendszer, valamint a kritikus rendszerelemek kiesésének következményei, kockázatai és rangsorolása az alkalmazások szempontjából – IT Security and Risk Analysis,
  - az üzletmenetfolytonosság-tervezés kiindulási alapját képző, potenciális üzemzavari és katasztrófaesemények palettája – Event Definition,
  - a rendelkezésre állási követelményeket kielégítő tartalékolási és visszaállítási stratégiák, a felmért kockázatok és üzleti folyamat-prioritások, figyelembe véve az üzemzavari és a katasztrófaeseményeket – Back-up and Recovery Analysis,
  - a stratégiák alapján a tartalékolási és visszaállítási megoldások.
- A meghatározott tartalékolási és visszaállítási megoldások megvalósíthatósági feltételeinek tesztelése és ez alapján előzetes intézkedési tervjavaslat kidolgozása a feltételek kielégítésére.
- Helyzetfelmérő és értékelő jelentés elkészítése.

Az üzletmenet-folytonossági terv elkészítése

Az üzletmenetfolytonosság-tervezési projekt ezen fázisában történik meg az üzletmenet-folytonossági terv kidolgozása, amely a következő fő fejezetekből áll:

Megelőzési terv és intézkedések

A megelőzési terv tartalmazza mindazon szabályzatokat, dokumentumokat és intézkedéseket, amelyek az informatikai rendszer folytonos üzemét valamilyen módon veszélyeztető tényezőkkel kapcsolatosak. Az üzletmenet-folytonosság biztosításában alapvető szerepe van a megelőzésnek, mivel a mai korszerű informatikai rendszereknél nem a nagyobb üzemzavarok vagy katasztrófaesemények, hanem sokkal inkább a nagyszámú, de kisebb üzemeltetési és felhasználási problémák miatt sérül az alkalmazások rendelkezésre állása. E problémák nagy része megfelelő odafigyeléssel és szabályozottsággal, és annak következetes érvényesítésével és ellenőrzésével megelőzhető.

A megelőzési terv fontos fejezetét képezi a *tesztelési és tréningterv*, amely meghatározza a tesztelés formáit. Az üzletmenetfolytonosság-tervezés tesztelésének két formája javasolt:

1. *Auditálás jellegű check-listás teszt,* amelyet egy előre elkészített ellenőrzési lista alapján független belső vagy külső auditorok végeznek el legalább félévenként.
2. *Valós üzemzavari vagy katasztrófaesemény szimulációja,* amelynek keretében az Eseménykezelő Team (Incident Management Team), az üzemeltetők és a felhasználók *gyakorlati üzletmenetfolytonosság-tervezés tréningje* is megvalósul. Ezt évente egyszer javasolt megismételni.

Visszaállítási terv

A visszaállítási terv alapvető célja az, hogy az üzemzavari vagy katasztrófaesemények bekövetkezése esetén az esemény azonosítása, a szükséges emberi és eszköz erőforrások haladéktalan mozgósítása és a visszaállítás a lehető leggyorsabban és szervezetten történjen meg a tervben meghatározott utasítások szerint.

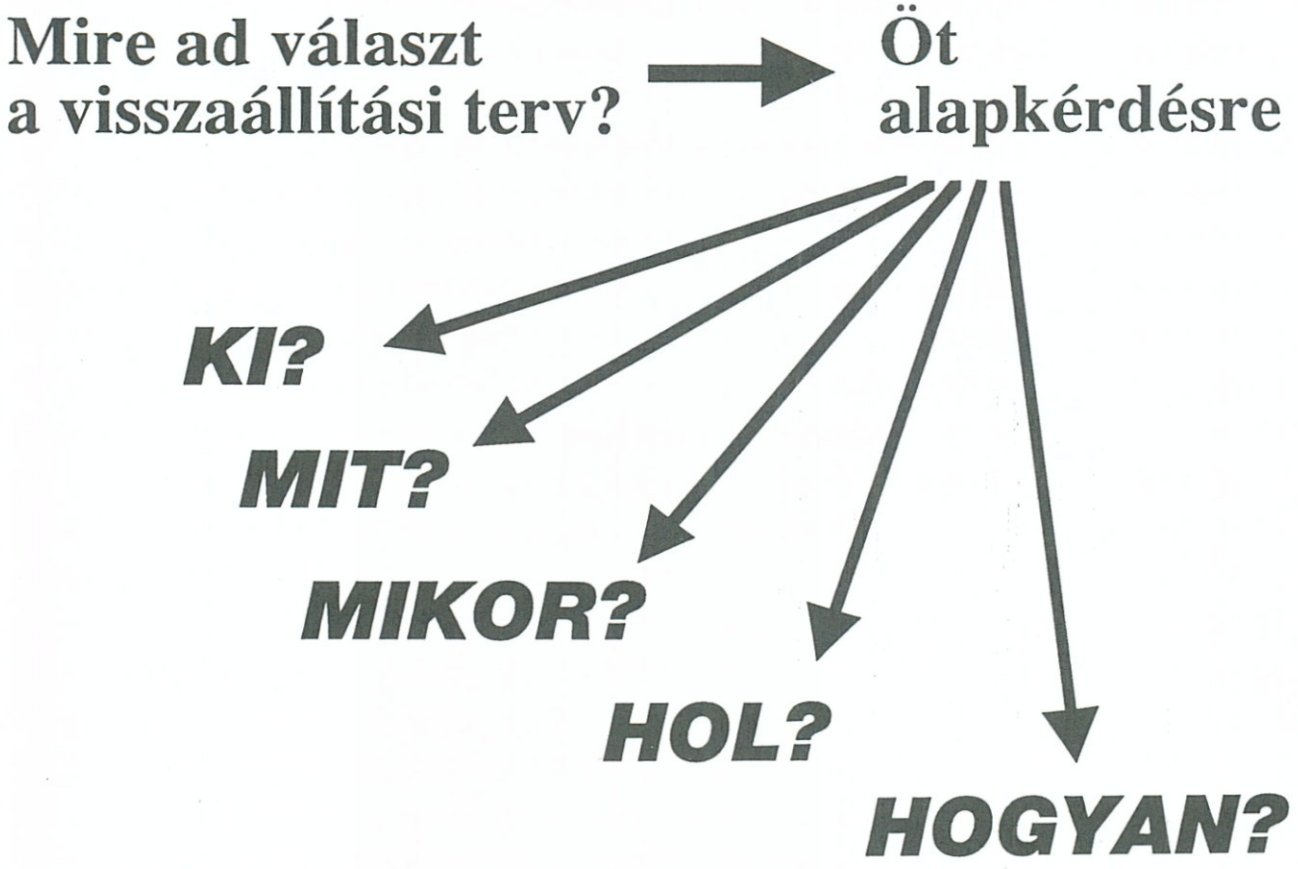
A visszaállítási terv a következőket tartalmazza:

- a visszaállítási terv célja és használata,
- az üzemzavari és a katasztrófaesemények meghatározása,
- az események bekövetkezési és kezelési időszakai (munkaidőben, munkaidőn kívül, hétvégén, többnapos ünnepen)
- visszaállítási forgatókönyvek az esemény kategóriájától és a bekövetkezési időszaktól függően,
- az Eseménykezelő Team összetétele, faladatai és hatásköre,
- Visszaállítási intézkedések forgatókönyvek szerint a következő lépésekre:

- azonnali válasz (riadóterv),
- futtatókörnyezet-helyreállítás,
- funkcionális helyreállítás,
- üzemeltetési szintű helyreállítás,
- áttelepülés (katasztrófa esetén),
- normalizáció az áttelepülés után.

Az intézkedések átfogják a központi erőforrások, azok fizikai és személyi környezete, a végponti munkaállomások és a kommunikációs rendszer területeit.

Röviden összefoglalva a visszaállítási terv alapvető célját a **7.2.** ábra fogalmazza meg.



7.2. ábra

Az üzletmenet-folytonossági terv elkészítése után véglegesítésre kerül a *helyzetfelmérés és értékelés* projekt fázisban elkészített előzetes intézkedései terv, amely tartalmazza mindazon feltételek biztosítására vonatkozó intézkedéseket, amelyek megléte nélkül az üzletmenet-folytonossági terv nem működőképes, és a következő projektfázisban elvégzendő üzletmenet-folytonossági terv teszt és tréning nem valósítható meg.

Oktatás, tréning és tesztelés

Az üzletmenet-folytonossági terv oktatását vezetői, üzemeltetői és végfelhasználói szinten célszerű megvalósítani.

Az oktatás célja:

- az üzletmenet-folytonosság jelentőségének tudatosítása,
- az üzletmenetfolytonosság-tervezés alapismeretek átadása,
- a megelőzési és a visszaállítási tervben foglaltak megismerése és elsajátítása.

Az oktatási tematikák az oktatást megelőzően a projektterv szerinti határidőre lesznek elkészítve az oktatás céljainak és szintjeinek megfelelő tematikával.

Az üzletmenet-folytonossági terv tesztelése és tréningje akkor lesz elindítható, ha a szervezet által az üzletmenet-folytonossági terv készítési fázisa végén elfogadott intézkedési tervben foglaltak olyan szinten megvalósultak, hogy az üzletmenet-folytonossági terv tesztje és tréningje a szervezet és a vállalkozó cég által közösen meghatározott üzemzavari/katasztrófa eseményre kivitelezhető.

Az üzletmenet-folytonossági terv tesztje szimulált esemény bekövetkezésével és a terv szerint visszaállítással lesz megvalósítva, amelynek keretében az Eseménykezelő Team, az üzemeltető személyzet és a felhasználók a valós körülményeknek megfelelően gyakorolják a visszaállítási terv utasításainak végrehajtását.

Az első teszt után megtörténik annak kiértékelése és az üzletmenet-folytonossági terv ennek megfelelő korrekciója. Sikeres teszteléssel lezárásra kerül az üzletmenetfolytonosság-tervezés.

8. Az emberi tényező

Az informatikai rendszerekben kezelt adatok biztonsága a különböző rendszerelemeken megvalósított védelemtől függ, ezért a védelmi rendszer kialakításánál mindenkor számításba kell venni az embert, amely az egész védelmi rendszerben a legnagyobb bizonytalansági tényezőt jelenti. Felvetődik a kérdés: miért?

A válasz a többi rendszerelem és az ember közötti lényeges különbségekben rejtőzik:

- Az ember *kreatív intelligenciával* rendelkezik, amit a legerőteljesebben azzal jellemezhetünk, hogy az ember a meglévő információs bázisára támaszkodva minőségileg új ismereteket, új összefüggéseket tud alkotni. Intelligenciája révén képes új információk, új összefüggések alkotására, illetve ha az általa ismert információk megosztását alapvetően saját belső – sokszor *nehezen kiszámítható és ellenőrizhető* – motivációi alapján végzi, akkor azonnal belátható, hogy az információk bizalmasságának védelmében a személyek szerepe az információvédelem teljes tárgykörében a legösszetettebb, legnehezebben kezelhető probléma.
- Az ember *szabad akarattal* rendelkezik. Csupán az adminisztratív szabályozás kényszerével nehezen orientálható egy cél, adott esetben egy szervezet üzleti céljai felé anélkül, hogy igénybe ne vennénk az emberi természetet, a szabad akaratát figyelembe vevő úgynevezett humán menedzsment eszközöket, amelyekkel elő lehet segíteni meghatározott célok teljesítésére vonatkozó *motiváltságát*, az erre vonatkozó saját belső meggyőződését, valamint a szervezet iránti *lojalitását*. Végső soron azonban mindig ő dönt arról, hogy ezeket a környezeti befolyásokat magáévá teszi vagy sem. Ez fogja alapvetően meghatározni a *célokkal való azonosulását* és a *normakövetési hajlandóságát*.
- Az ember *érzelmi lény*. Cselekedeteit és így a normakövetési hajlandóságát sok esetben alapvetően befolyásolják pillanatnyi érzelmei, ennél fogva – ellentétben a műszaki rendszerekkel – várható cselekedetei nem jósolhatók meg minden esetben logikusan és racionálisan.

A szabályozás területén mindig vannak pozitív, előre vivő és hátráltató tényezők. Ezek eredőjeként minden szervezetnél kialakul egy, a szervezetre jellemző szabályozási, érvényesítési, ellenőrzési és intézkedési gyakorlat. A kívánatos célt úgy fogalmazhatjuk meg, hogy a **8.1.** táblázatban szereplő hatásokat a szervezetnek a szabályozás és a humán menedzsment eszközeivel úgy kell befolyásolnia, hogy a mérleg nyelve mindig pozitív tartományban legyen.

Az előzőekből következik, hogy egy szervezet munkatársainak a lojalitását és a biztonság növelésével kapcsolatos motiváltságát csupán szabályokkal nem lehet erősíteni. Ehhez más eszközök, módszerek is szükségesek, nevezetesen a humán vagy emberi erőforrás (Human Resource, HR) menedzsment módszerei. Az emberi erőforrás stra-

Negatív folyamatok, jelenségek	Pozitív folyamatok, jelenségek
Nehezen realizálható szabályok, amelyeket mindenki kikerül	Pontos, jól végrehajtható, megfelelő visszatartó erejű szabályozás
Nincs vagy nem hatásos érvényesítő mechanizmus	A szabályozás hatásos mechanizmussal érvényesül
Ellenőrzés nincs vagy rendszertelen	A szabályok betartása rendszeresen ellenőrzött
Az intézkedések elmaradnak vagy nem hatásosak	A hiányosságok felderítését intézkedések követik
A szankciók elmaradnak (szabályozatlanság, konfliktus kikerülés miatt)	A visszaélések felderítését szankciók követik
Feszült munkahelyi légkör (nem megfelelő vezető, átszervezések miatti egzisztenciális bizonytalanság stb.)	Jó munkahelyi légkör
Alulfizetettség	Teljesítményarányos jövedelem
Rendezetlen családi háttér	Kiegyensúlyozott családi háttér
Problémákkal terhes gyermekkor	Megfelelő gyerekkori szocializáció
Szakmai kilátástalanság	Kedvező szakmai perspektíva
A szakmai továbbképzést a vezetők nem nézik jó szemmel	A szakmai továbbképzés támogatott
Fásultság, érdektelenség, rutinszerű hozzáállás, az intelligenciaszint a munkakörhöz szükségesnél alacsonyabb	A munkakörnek megfelelő kreativitás és intelligenciaszint
A szervezetnek nem alakultak ki hagyományai	A szervezet doktrínával (íratlan szabályokkal, hagyományokkal) rendelkezik, és ennek jól kialakult, hatásos közvetítő mechanizmusa van

8.1. táblázat

tégia (megszerzés, fejlesztés, mozgatás, leépítés) vezetői és szervezeti szintű feladatai részben meglevő ismereteken alapulnak, részben további kutatásokat igényelnek.

Az emberi biztonsághoz kapcsolódó fontosabb vezetői, felsővezetői feladatokra és általánosan használt eszközökre térünk ki. A vállalati menedzsment számára megfogalmazható elvek, tevékenységek és eszközök ágazat, és szervezetspecifikus tulajdonságokkal is rendelkeznek, ezek konkrét meghatározása csak egy **informatikai biztonsági átvilágítás** után lehetséges, így erre a jelenlegi keretek között csak utalásszerűen tudunk kitérni.

8.1. Információvédelem a belépéstől a szervezet elhagyásáig

Valamennyi szervezeten belül a biztonság az ott dolgozó munkatársaktól függ. Ebből kiindulva a személyzeti politikát úgy kell kialakítani, hogy:

- biztosítsa a megfelelő személyi állomány kiválasztását, foglalkoztatását,
- biztosítsa a meglévő személyi állomány megtartását,
- annak folyamatos képzését, fejlesztését,
- a szakmai alkalmasság folyamatos ellenőrzését,
- a biztonsági előírásoknak történő megfelelést,
- a munkaerő utánpótlását.

A fentiek közül a következő fejezetekben néhányat önkényesen kiemelve ismertetünk.

Az informatikai biztonsághoz is kapcsolódó HR feladatok:

- személyek kiválasztása és felvétele,
- optimális képzési, továbbképzési lehetőségek biztosítása,
- jó munkahelyi környezet kialakítása,
- megfelelő fizikai és szervezeti biztonsági intézkedések kialakítása és érvényesítése,
- megfelelő megelőző és katasztrófaelhárítási intézkedések.

8.2. Felvétel

Egy szervezet csak abban az esetben lehet versenyképes, ha a potenciális munkaerő piacán a legjobbakat tudja megkeresni, felvenni és megtartani.

A jelentkezőtől normál, illetve szakmai önéletrajzot szükséges beszerezni, amelyben a betöltendő munkakörnek megfelelő sajátosságokra ki kell térni, melyhez a


Jó, ha tudod

szakmai szempontokat előzetesen ki kell dolgozni. Új dolgozó felvétele előtt – lehetőség szerint – a korábbi munkahelytől írásos (dokumentált) véleményt kell beszerezni. Szükséges továbbá minden olyan referencia beszerzése, amely a kiválasztást segíti elő. A felvételi folyamat előtt a munkavállalót tájékoztatni kell a munkaköréhez kapcsolódó valamennyi biztonsági követelményről. Alkalmazásra csak akkor kerülhet sor, ha a munkavállaló tudomásul veszi a biztonsági követelményeket, hozzájárul az életmódvizsgálathoz, és vállalja a biztonságból fakadó előírásokat.

A gazdasági szférában történő személyellenőrzést életmódvizsgálatnak nevezzük. Az életmódvizsgálat lényege, hogy az informatikai biztonság területén foglalkoztatni kívánt munkavállaló magatartásáról, életviteléről, pozitív és negatív tulajdonságairól, az úgynevezett kockázati tényezőkről megfelelő képet kapjon a későbbi munkáltató. Legyen lehetősége a döntés meghozatala előtt mérlegelni, hogy az esetlegesen büntetett előélet, a káros szenvedélyek, a pénzügyi bizonytalanság, a fecsegésre való hajlam, a magánélet rendezetlenség stb. alapján alkalmazza-e a jelentkezőt, vagy eltekint attól. Az életmódvizsgálatról szóló anyag alapkritériuma az objektivitás.

A bizalmi munkakörben alkalmazásra kerülő személy életvitele átlátható és társadalmilag elfogadott, káros szenvedélyektől mentes, anyagi helyzete rendezett, nincs olyan adat, amely későbbi zsarolásra lehetőségét biztosítana.

Mindezeket figyelembe véve a leendő munkavállalót tájékoztatni kell, hogy az adatszolgáltatás önkéntes vagy kötelező jellegű. Ismertetni kell az adatkezelés célját és az adatkezelőket. Az életmódvizsgálat a jogszabályi megfogalmazások alapján csak a vizsgált személy hozzájárulásával hajtható végre.

8.3. Megtartás – a lojalitás biztosítása

A munkavállalót nemcsak megfelelően kell kiválasztani, majd alkalmazni, hanem kiemelkedően fontos a jó munkaerő megtartása, hosszú időre szóló foglalkoztatása is.


Jó, ha tudod

Az emberek lojalitásának biztosítása sokrétű feladat. Beletartozik a külső, belső motiváció, a pénzbeli és nem pénzbeli ösztönzés valamennyi formája. Az általános cél, hogy a különböző csoportokat és az egyéneket nagyobb teljesítményre késztesse és biztosítsa a dolgozók lojalitását a vállalat irányába, szolgálva ezzel az általános biztonság növelésének igényét is.

Ennek érdekében az ösztönző rendszer:

- motiválja a dolgozókat,
- növeli elkötelezettségüket,
- építi a teljesítményorientált szervezeti kultúrát,
- segíti a kultúraváltást,
- a teljesítmények alapján differenciál,
- segíti a megfelelő munkaerő kiválasztását és a lojális munkaerő megtartását.

A menedzsment feladatok között szerepeltetni szükséges az információvédelmi vonatkozású változásokkal szembeni ellenállás kezelését. Ennek részeként fel kell mérni az ellenállások mértékét, fel kell tárni annak okait, ki kell munkálni a szükséges stratégiai és operatív lépéseket, majd ezután, a hozott döntés függvényében a fokozatosság vagy a radikális váltás stratégiájának megfelelően el kell érni, hogy az intézkedések bevezethetők és fenntarthatók legyenek.

A lojalitás kialakításához tartozik, hogy a szervezet minden szintjén tudatosuljon:

- **Az információ,** az adat a vállalat rendkívüli **értékkel bíró vagyona.**
- Az alkalmazotti, a menedzsment és tulajdonosi érdekek egyik közös eredője, ha tetszik az **egyének személyes érdeke az információ védelmének reális szinten tartása.**
- A versenyhelyzetben az információkezelés hiányosságai olyan mértékű hátrányt jelenthetnek, amelynek hatására **veszélybe kerülhet a munkahely, az elért egzisztencia.**

8.4. Oktatás és képzés

Az emberi viselkedést számtalan összetevő vezérli. Az eddigiekben érintettük az informatikai biztonsággal kapcsolatos attitűdöket, a vállalathoz kapcsolódó lojalitást stb., de a magatartás szintű megvalósulás első lépése az információk eljuttatása az egyénekhez, a szervezeti csoportokhoz, vagyis szervezett információbevitel, aminek egyik hagyományosan használatos módja az oktatás. Az informatikai biztonság megvalósítása szempontjából is nélkülözhetetlen a munkavállalók folyamatos képzése.

A képzéskor elsősorban a problémamegoldásra, konfliktuskezelésre kell a hangsúlyt helyezni. A munkavállalók vonatkozásában a feladatok hatékony végrehajtása, a kommunikációs készség javítása, a biztonsági szabályok betartása a cél.

Az ismert modellek és képzési irányzatok mindegyike alkalmas az információbiztonsággal összefüggő oktatási feladatok egy rendszerbe foglalására. Természetesen lehetséges a témának a cég meglevő rendszeréhez illesztése, illetve az integráció mellett speciális képzési forma kimunkálása is.

8.5. Munkaszervezés

A munkaszervezés biztonsági, informatikai biztonsági „aranyszabályai”:

1) Valamennyi munkaterületre részletes munkaköri leírást kell készíteni. A munkaköri leírásnak tartalmaznia kell az adott munkaterületre vonatkozó, biztonsággal kapcsolatos követelményeket.

2) Nem szabad megengedni, hogy a munkavállaló a törvény által biztosított szabadságát az adott időszakban ne vegye igénybe.
3) A munkavállalókat munkájuk ellátásához szükséges információkkal el kell látni, s ugyanakkor tudatosítani kell, hogy jogosulatlan személy részére információt átadni kockázatos, s ezért tilos.
4) A munkakörök élesen határolódjanak el, hogy ily módon minden munkavállaló csak a szigorúan rá vonatkozó feladatot hajthassa végre.
5) A szervezet támadhatóságának csökkentése érdekében a bizalmi munkaköröket betöltő munkavállalókra a vezetésnek kiemelt figyelmet kell fordítania.
6) Bizalmi munkakörökben foglalkoztatott dolgozók helyettesítését megfelelő képzettségű és gyakorlatú háttérszemélyzettel kell biztosítani.
7) Minden munkaterületen az adott vezető kötelezettsége, hogy mind az alkalmi, mind az időleges munkavégzőkkel a biztonsági előírásokat betartassa.
8) A biztonsági szabályzatban foglaltak alapján minden munkaterületre ki kell dolgozni a konkrét tennivalókat.
9) A biztonsági szempontból kiemelt bizalmi munkakörök betöltésénél lehetőleg belső személyzetet kell foglalkoztatni.
10) A biztonság érdekében az üzemeltetés területén bizonyos munkakörökben fontos a munkakörök időszakos váltása, ezzel elkerülhető az a helyzet, hogy egy személy mindig ugyanazt a feladatot hajtsa végre.
11) A vállalaton belül nem engedhető meg, hogy egymással rokonságban álló személyek kulcsfontosságú munkaköröket betölthessenek.

9. Az informatikai helyiségek fizikai védelme

Az informatikai biztonság megteremtése során alapvető a fizikai védelem kialakítása. A fizikai védelem alatt

- a mechanikai vagy fizikai védelem,
- az elektronikai védelem és
- az élőerővel történő őrzés értendő.

Ebben a fejezetben az informatikai helyiségek mechanikai és elektronikai védelmével foglalkozunk. Nem térünk ki az élőerővel történő őrzés kérdéseire. Az élőerővel történő őrzés a mechanikai és elektronikai védelemmel egységes egészet kell hogy alkosson úgy, hogy az élőerő részben kiegészíti, részben megerősíti a mechanikai és elektronikai védelmeket, ezen eszközrendszereket mindig komplexen kell alkalmazni. Az élőerővel történő őrzés esetében az őrző-védő személyzet emberi erőforrásként jelentkező problémáiról, a megbízhatóság kérdéseiről itt sem szabad megfeledkezni.

9.1. Az épületek mechanikai védelme

A mechanikai védelem feladata, hogy akadályozza, lassítsa a védendő objektumba való illetéktelen behatolást és a védendő értékekhez történő illetéktelen hozzáférést. Az optimális helyzet az lenne, ha nem csupán akadályozásról, hanem megakadályozásról beszélhetnénk, de a kérdés ilyen módon történő felvetése csupán utópia lehet. Vizsgáljuk meg a mechanikai védelem összetevő elemeit:

1. kerítések: meghatározza a védett terület határait, akadályozza az illetéktelen behatolást, anyagától függően korlátozhatja a belátást.
2. héjvédelem: a védett objektum külső felülete (falak)
3. nyílászárók: a különböző ajtók és ablakok
4. zárak, zárrendszerek
5. rácsok, rácsszerkezetek: a nyílászárók védelmének alapvető eszközei
6. biztonsági fóliák
7. speciális értéktárolók, mint a trezorhelyiség és a páncélszekrények
8. biztonsági táskák és borítékok

Az épületek mechanikai védelmével szembeni elvárás, hogy nyújtsanak kellő felületvédelmet az épületen belül kialakított különféle rendeltetésű helyiségekben

folytatott tevékenység számára. Általánosságban elmondhatjuk, hogy az épületek statikai méretezése – a tartószerkezetek, falazatok, padozatok, födémek – megfelelő mechanikai védelmet biztosítanak a külső környezetből történő gondatlan (véletlen) vagy szándékos behatásokkal szemben. Az épületen belüli helyiségek falazata eltérő mechanikai védelmi értékű lehet. Kialakításukat az építészeti (statikai) szempontokon túl befolyásolja a bennük folyó tevékenység és a tűzvédelem szempontjai.

Az építmény egyes helyiségeire vonatkozó biztonsági előírás eltérhet – szigorúbb lehet – az építmény egészére megfogalmazott biztonság mértékétől. Ilyen helyiségek lehetnek a távbeszélő hálózat hozzáférési pontjai, a szerverszobák, a számítógéptermek, a pénztárak, a titkos ügykezelés helyiségei.

Külön kell foglalkozni a bejáratokkal, ugyanis a statisztikák tanúságai szerint az illetéktelen behatolások döntő többsége azokon keresztül valósul meg.

9.2. Az elektronikai jelzőrendszer

Feladata, hogy a védett területre történt illetéktelen behatolásról már a behatolás kezdeti időszakában jelzést adjon és továbbítson, növelve a mechanikai védelem és az élőerős őrzés hatékonyságát.

Az elektronikai védelem alkotórészei:

1. Felületvédelem: a védett objektum határoló felületeinek elektronikus védelme
2. Területvédelem: az építészetileg zárt területek jelzőrendszere
3. Tárgyvédelem: egy adott, konkrét tárgy védelmét biztosító jelzőrendszer
4. Személyvédelem: a személyek védelmét biztosító elektronikai eszközök

Az elektronikai jelzőrendszer feleljen meg az MSZ IEC 839 „Riasztórendszerek" című szabványsorozat előírásainak.

Az elektronikai jelzőrendszer elektronikus eszközökkel érzékeli és értékeli a felügyelt védelmi rendszer állapotát, kijelzi annak változásait. Kiépítésében lehet teljes körű, vagy részleges. Teljes körű a rendszer, ha minden alkalmazott alkotóeleme teljes körű.

Teljes körű a felületvédelem, ha az elektronikai jelzőrendszer éles üzemmódban figyeli az összes nyílászáró-szerkezetet, portált és a mechanikailag nem megfelelő (38 cm-es tömör téglafal szilárdsági tulajdonságainál gyengébb értékű) falazatokat, födémeket, padozatokat, jelzi az át- és behatolási kísérleteket.

Teljes körű a térvédelem, ha az elektronikai jelzőrendszer éles üzemmódban a felügyelt terek, tárgyak környezetében mindennemű illetéktelen emberi mozgást jelez, valamint a megközelítési útvonalat (útvonalakat) legalább csapdaszerűen figyeli.

Teljes körű a tárgyvédelem, ha az elektronikai jelzőrendszer éles üzemmódban az összes védendő tárgyat felügyeli, páncélszekrények és páncéltermek (stb.) esetében a felügyelet nyitásra, zárásra és áttörésre is kiterjed.

Teljes körű a személyvédelem, ha az elektronikai jelzőrendszer folyamatos üzemmódban az összes védendő, támadásnak kitett személyt „felügyeli".

A rendszerrel szemben támasztott követelmények: Az elektronikai jelzőrendszer minden részegysége rendelkezzen szabotázsvédelemmel, melynek jelzései az érzékelők riasztásjelzésétől elkülönítve jussanak a központi egységbe. A szabotázsvédelemnek – az elektronikai jelzőrendszer élesítésétől függetlenül – 24 órás, folyamatos üzemmódban kell működnie.

Az elektronikai jelzőrendszer csak az érzékelők nyugalmi állapotában legyen élesíthető. Ezt az állapotot a központi egység jelezze ki. A központi egység működése olyan legyen, hogy a rendszer kezelése az arra jogosult felhasználón kívül más személy részére ne legyen hozzáférhető.

A nyílászárók védelmét úgy kell kialakítani, hogy azok süllyesztettek legyenek, és a felszerelésre kerülő eszközök az 1-2 cm-es mozgást érzékeljék.

Az üvegfelületek védelmét úgy kell kialakítani, hogy az érzékelők már az üveg repedésére is jelzést adjanak. Az érzékelő kiválasztása a védeni kívánt üvegfelület típusának figyelembevételével történjen. Az érzékelőnek a teljes üvegfelületet védeni kell.

Falazatok védelméhez úgy kell kiválasztani az érzékelő eszközt, hogy az érzékenységi karakterisztikája alapján az egész védeni kívánt felületet lefedje. Túl nagy felület esetén több érzékelő elhelyezése szükséges.

Térvédelmet úgy kell kialakítani, hogy a felszerelésre kerülő érzékelő eszközök az illetéktelen behatolást a lehető legrövidebb idő alatt jelezzék a központ felé.

Tárgyvédelem kialakítása csak különleges esetekben indokolt (banki alkalmazások, különösen nagy értékű tárgyak, kiemelt fontosságú információhordozók).

Személyvédelmet a védett objektumban dolgozók védelme érdekében szükség esetén kell kialakítani. A támadásjelző eszközök rögzített változatai csak védett helyen telepíthetők, szabotázsvédett kivitelben, 24 órás üzemmódban működtetve. Telepítésük úgy történjen, hogy jelzésük esetén egyenként is azonosíthatók legyenek (címazonosítás, jelzőhurok-azonosítás).

A riasztás jelzése céljából szabotázsvédett dobozban felszerelt hang-fény jelző és hangjelző készülékeket az épületen kívül úgy kell felszerelni, hogy azok egyszerű (például a környezetben fellelhető) eszközökkel ne lehessenek elérhetők. Állandó biztonsági ügyeletre való átjelzés esetén „néma riasztás" is megengedett.

Az elektronikai jelzőrendszert indokolt esetben beléptető rendszer, és helyi biztonsági szolgálat jelenléte esetén videomegfigyelés egészítheti ki.

9.3. Az informatikai helyiségek tűzvédelme

Az informatikai helyiségek tűzvédelmével kiemelten kell foglalkozni az esetlegesen bekövetkező káresemények megelőzése érdekében!

Az informatikai helyiségeket a bennük folytatott tevékenység jellegének megfelelő tűzvédelemmel kell ellátni. A tűzvédelem tárgyi oldalát aktív és passzív eszközök együttes alkalmazásával, személyi oldalát szabályozással, oktatással, gyakoroltatással lehet biztosítani.

A passzív tűzvédelem eszközei a megfelelő tűzgátló tulajdonsággal rendelkező falazatok, bejárati ajtók, a menekülő útvonalak, füstmentes lépcsőházak, vészkijáratok és szakszerűen tömített kábelátvezetések. Az aktív tűzvédelem eszközei a különféle tűzoltó eszközök, a beépített tűzjelző és automatikus oltórendszerek. Kialakításukra az építési és tűzvédelmi jogszabályok, szabványok adnak iránymutatást.

Egy szervezeten belül gyakran okoz dilemmát a szerverhelyiségek tűzvédelme, legyen-e telepítve automatikus működésű oltórendszer, vagy nem. Erre egyértelmű állásfoglalást az Országos Tűzvédelmi Szabályzat tartalmaz, ami a számítástechnikai helyiség alapterületéhez köti a telepítés szükségességét. 150 m^2 alapterület fölött annak létesítését kötelezően előírja. Az ennél kisebb alapterület esetén csak jelzőrendszer telepítése kötelező. Az alapterület szerinti kötelezés nem biztos, hogy a legszerencsésebb. A szervezetnek az ennél kisebb alapterületű szerverhelyiségek esetében is mérlegelni kell az informatikai rendszerében tárolt és feldolgozott adatok alapján az oltórendszer telepítésének szükségességét. Egyéni mérlegelés alapján kisebb alapterület esetén is szükséges lehet az automatikus beavatkozás.

9.4. Az informatikai helyiségek villámvédelme

A villámcsapások okozta közvetlen károkat valamennyien jól ismerjük. A létesítmények az elsődleges villámkárok ellen általában védettek, létesítésükkor villámhárító, villámvédelmi levezető a környezetnek megfelelő besorolással telepítésre kerül – erről az építmények tervezői, kivitelezői gondoskodnak. A villámvédelmi rendszerek felülvizsgálatát az előírt gyakorisággal végre kell hajtani. Az épületek elsődleges, közvetlen villámcsapás elleni védelmét jogszabályok, szabványok határozzák meg, ezért ennek részletezésére nem térünk ki.

A villámcsapás másodlagos hatásaival kapcsolatos védelem csak az utóbbi évtizedben került előtérbe. Számtalan villámkár igazolta, hogy az elektronikus rendszerek (és az ott tárolt, feldolgozott adatok) a közeli villámcsapások hatására „egy pillanat" alatt megsemmisülhetnek, ha nincs megfelelően kialakított belső, másodlagos villám- és túlfeszültség védelem kialakítva. Az esetek zömében az eszköz kieséséből származó közvetlen károkon túl nagyságrendekkel nagyobb értéket képviselnek a szolgáltatás kieséséből, adatvesztésből bekövetkező eszmei és üzleti károk.

Az épületekben a villamosenergia-elosztó hálózatok, az árnyékoló- és földelő rendszerek, valamint a különböző mérő-, szabályozó-, (épületfelügyeleti, vagyon-

védelmi) rendszerek és adatátviteli hálózatok fémes vezetékei különböző pontokon lépik át a külső és belső villámvédelmi zónahatárt és eltérő nyomvonalon érik el a berendezéseket. Ebből adódik, hogy ezek a vezetékek szinte minden esetben nyitott vezetőhurkot képeznek. A hurok felülete már egy kisebb épületen belül is eléri, vagy elérheti, illetve meghaladja a 10 m^2-t. A jelvezetékek méretei még az előző méreteknél is sokkal nagyobbra adódhatnak. Az ilyen nyitott vezetőhurok szakaszát képezhetik a villámvédelembe tartozó, vagy attól különálló, földtől független fémszerkezetek egyes részei, vagy bármilyen szigetelt villamos jelvezeték egy-egy szakasza is.

Közeli villámcsapáskor a villámáram időben változó mágneses tere, a fentiekben leírt különböző méretű és elrendezésű nyitott vezetőhurkokban 10^4–10^6 V nagyságrendű túlfeszültséget indukál. Ez a feszültség jelentősen meghaladja a berendezések üzemi szigeteléseire előírt 1 perces szabványos vizsgálófeszültség értékeit. Ez a magyarázata annak, hogy a villámcsapás által indukált másodlagos induktív hatása „túlfeszültségként" egyszerre több ponton is átüti az áramkörök szigetelését.

Ha a létesítmény csak elsődleges villámvédelmi rendszerrel rendelkezik, de túlfeszültség-levezető rendszerrel nem, a villámáramok hatása (10 km-s körzeten belüli becsapási talpponttal) teljes adatvesztéssel, illetve meghibásodással járhat minden bekapcsolt elektronikus rendszer – számítóközpontok, távbeszélő alközpontok, vezetői információs hálózatok, telefaxok stb. – vonatkozásában.

9.5. Kisugárzás- és zavarvédelem

A számítástechnikai eszközök, így például a monitorok, a hálózati és nyomtatókábelek, de még a tápfeszültséget biztosító vezetékrendszer is sugároz – mérhető és kiértékelhető – jeleket. Az ehhez szükséges lehallgató eszközök laboratóriumi körülmények között egyszerűek és olcsók, de a valós helyzetben, ahol több tucat vagy akár több száz sugárforrás közül kell szelektíven kiválasztani, mérni és értékelni a jeleket. Ezek az eszközök már nagyon bonyolultak és „méregdrágák". Általában csak a kiemelt biztonsági osztályban szükséges a kisugárzás elleni védelemről gondoskodni, de tekintettel ennek magas költségeire, mindig egyedileg, a kockázatokkal arányosan, az adott környezetre szabva érdemes csak megvalósítani.

Hasonló jellegű, de gyakoribb és nagyobb veszélyeket hordoznak magukban a külső, elektromos zavarójelek, ezek igen gyakran különböző villamos gépektől származnak, például trolibusz, klímagépház. A zavarvédelem megoldásai hasonlóak, mint a kisugárzásvédelemé, és az ezzel kapcsolatos költségek is hasonlóak. Ha ilyen probléma gyanúja felmerül, érdemes ellenőrző méréseket végeztetni, és az eredmények ismeretében megoldani a problémát.

A kisugárzás- és zavarvédelem esetében az EN 55022 és EN 5024 szabványokat kell figyelembe venni. A kábelezésre vonatkozóan az EIA/TIA-568 Kereskedelmi Épületkábelezési Szabvány a mérvadó. A kiemelt biztonsági osztályban a csavart érpáros *árnyékolt*, egyéb tekintetben a csavart érpáros *árnyékolatlan* kábeltípus követelményei megfelelőek.

A kisugárzás- és zavarvédelemben szükség esetén az úgynevezett Faraday-ketrec elvét kell alkalmazni, ez kiegészíthető a kisugárzásvédelemben az úgynevezett „zaj-generátor" alkalmazásával.

10. Dokumentumkezelés, ügyvitel

A dokumentumkezelés, az ügyvitel nemcsak az informatikai biztonság, de a szervezet biztonságos és megbízható működése, és így például a minőségbiztosítás szempontjából is fontos terület. Az **7.4.** fejezetben már foglalkoztunk az ügyviteli szabályzat szükségességével és tartalmi elemeivel, amelyekben előírják a dokumentumkezelés feladatait, sajátosságait a szervezeten belül. Az ügyviteli szabályzat rendelkezései biztosítják, hogy az irat útja pontosan követhető, ellenőrizhető és visszakereshető legyen, amely támogatja a szervezet tevékenységének hatékonyságát, ellenőrizhetőségét és a dokumentumok, iratok épségben, illetve használható állapotban való megőrzését.

Az ügyviteli tevékenység egyik alapvető eleme az iktatás. A szervezethez beérkező vagy ott keletkező valamennyi iratot iktatással kell nyilvántartani. Az iktatás történhet hagyományosan, papíralapon vagy számítógépes eljárással.

Az iratokat úgy kell iktatni, hogy abból az irat beérkezésének pontos ideje, az intézkedésre jogosult ügyintéző neve, az irat tárgya, az elintézés módja, a kezelési feljegyzések, valamint az irat fellelhetősége megállapítható legyen. Számítógépes iktatás esetén is szerepelni kell az ügyiraton mindazon kezelési feljegyzéseknek, melyeket a „hagyományos" iratkezelés szabályai rögzítenek. A számítógépes nyilvántartás mellett – ma még – használni kell azokat az átadókönyveket, kézbesítőkönyvek, melyekben az átadás-átvétel tényét az érintett felek saját kezű aláírása bizonyítja.

A számítógépes iktatási rendszerben az iktatási adatok bevitelét, módosítását vagy törlését úgy kell naplózni, hogy az időpont és az ügyintéző felhasználóazonosítója is rögzítésre kerüljön. Javítás vagy törlés esetén az eredeti adattartalmat is meg kell őrizni. A naplózást a számítógépes iktatási rendszer emberi beavatkozás nélkül, kikapcsolhatatlanul kell hogy elvégezze.

Hazánkban az elektronikus okiratokról szóló jogi szabályozás még előkészítési állapotban van, ezért az elektronikus formában megjelenő adatok okiratokként csak korlátozottan használhatók. Ez azonban nem jelenti azt, hogy az elektronikus adathordozók (például CD-ROM, hajlékonylemez, magnetofonszalag stb.) ügyviteli kezelése elhanyagolható lenne. Az elektronikus adathordozók a jelenleg hatályos szabályok szerint a hagyományos iratokkal azonos módon kezelendők az alábbi eltérésekkel.

Az elektronikus adathordozón keletkezett vagy érkezett iratok mellé kísérőlapot kell csatolni. A kísérőlapon fel kell tüntetni az adathordozó iktatószámát, az adathordozó típusát, tartalmi ismérveit, az adathordozón található adatok megnevezését és annak „elektronikus nevét" (például a könyvtár- és állománynevet), a készítő és

a nyilvántartásba vevő aláírását. Az iktatószámot magára az adathordozóra vagy annak külső borítójára (tokjára) maradandó módon ugyancsak rá kell vezetni.

Az elektronikus adathordozókon az állományokat úgy kell elhelyezni, hogy – lehetőleg – az egy ügyhöz tartozó adatok, de mindenképpen azonos minősítésű adatok kerüljenek egy adathordozóra.

10.1. Dokumentumkezelés az informatikai rendszerekben


Tanuld meg!

Gyakorlati tapasztalat, hogy – még azoknál a szervezeteknél is, ahol a hagyományos, papír alapú iratkezelés jól szervezett – az informatikai rendszerbe be- és kikerülő dokumentumok, az ott feldolgozott, tárolt adatok iratkezelési szempontból elhanyagoltak, minősítésüknek megfelelő kezelésre, iktatásra nem kerülnek. Jellemző példa volt erre, amikor az egyik informatikai biztonsági vizsgálat során egy hálózatba nem kötött (stand alone) számítógépen a szervezet számára nagy értékű információkat dolgoztak fel. A feldolgozásra kerülő iratok, dokumentumok szabályosan iktatva, kezelve voltak, és ugyanez volt elmondható a feldolgozás eredményeképpen kinyomtatott anyagokról is. Amikor azt kezdtük el feszegetni, hogy ki férhet hozzá a számítógéphez, ki másolhatja hajlékonylemezre az adatokat, ezek a lemezek hová kerül(het)nek, mi történik az outputként megjelenő „rontott" példányokkal – döbbent hallgatás volt a válasz.

A titkos iratokat kezelő ügyintézők kiválasztása során természetes, hogy mind szakmai felkészültségüket, mind megbízhatóságukat ellenőrizni kell. Ugyanez érvényes az adatokat feldolgozó, tároló és továbbító informatikai rendszerekre is.

az adat (irat) minősítése	biztonsági osztály
nem minősített személyes adat üzleti titok	ALAP
szolgálati titok kiemelt üzleti titok különleges személyes adat	FOKOZOTT
államtitok katonai szolgálati titok	KIEMELT

10.1. táblázat

Az informatikai rendszerekbe bekerülő adatoknak már a bekerülés előtt van valamilyen minősítésük (államtitok, üzleti titok, személyes adat stb.). Ez alapján **a minősítés alapján be kell sorolni a feldolgozást, a tárolást végző informatikai rendszereket** valamilyen biztonsági osztályba (alap, fokozott, kiemelt), és a besorolásnak megfelelő követelményeket érvényre kell juttatni.

A dokumentumok minősítése és a követelmények szerinti biztonsági osztályok szintjei közötti összefüggéseket a **10.1.** táblázat mutatja.

Az informatikai rendszerekben az ott kezelt iratokra – bekerülésüktől a törlésükig – ugyanúgy be kell tartani a dokumentumkezelés szabályait. A bevitelre kerülő adat kerüljön az informatikai rendszerben iktatásra, és ebben az iktatási rendszerben ugyanúgy legyen végigkísérve az adat „életútja", mintha az hagyományos adathordozón lenne kezelve, tárolva vagy továbbítva. Nem a számítógéphez, hanem az ott fellelhető adatokhoz kell igazítani a hozzáférési jogosultságokat. A hazai tapasztalok alapján különösen fontos, hogy a nyomtatások, a kinyomtatott „selejt" útja, sorsa nyomon követhető legyen.

11. Logikai védelem az operációs rendszerekben, hálózatokban és alkalmazásokban

11.1. Operációs rendszerek


Tanuld meg!

A közhiedelem szerint a tűzfalak, titkosító és egyéb biztonsági eszközök játsszák a legfontosabb szerepet az informatikai rendszerek biztonságában, ez nemcsak hogy az informatikai rendszerek biztonsága szempontjából, de még azon belül, a logikai védelem területén sem igaz. Itt az egyik legkritikusabb választás az operációs rendszer. A központi erőforrások és a végponti munkaállomások operációs rendszere ugyanis döntően meghatározza a rendszer potenciális biztonsági követelményeit.

Az operációs rendszert egyrészt virtuális gépként, másrészt erőforrás-menedzserként határozhatjuk meg. Mint virtuális gép magasabb absztrakciós szintet biztosít a felhasználó számára, az eszközöket és állományokat szimbolikus neveken engedi kezelni, ezekben magasabb szintű műveleteket biztosít. Mint erőforrás, menedzser az operációs rendszer feladata, hogy a rendszer erőforrásait elossza a számítógépen futó különböző, az erőforrások birtoklásáért vetélkedő programok, alkalmazások számára.

A legelterjedtebben használt operációs rendszerek közül a közismert és széles körben népszerű operációs rendszereket mutatjuk be biztonsági szempontok figyelembevételével.

11.1.1. MS Windows 95, MS Windows 98


Figyelj jól!

Ezekben az operációs rendszerekben definiálhatunk felhasználókat, a felhasználók bejelentkezése jelszóhoz köthető, azonban ez a folyamat egyszerű eszközökkel (jelszóbekéréskor az ESC billentyű lenyomása) kikerülhető. A felhasználódefiniálásnak a környezet beállításában jut szerep, biztonsági szempontból gyakorlatilag nem használható. Az erőforrásokhoz való hozzáférés nem korlátozható, minden felhasználó minden erőforráshoz korlátlanul hozzáfér. A biztonsági naplózás nem lehetséges. A Windows 95 elsősorban otthoni felhasználásra, szórakozásra, tanulásra alkalmas, vállalati alkalmazásokban, ahol a biztonság igénye felmerül, már komoly kockázati tényezőt jelent.

11.1.2. Windows NT

A Microsoft 1988-ban létrehozott egy (Windows New Technology) fejlesztői csoportot azzal a szándékkal, hogy egy modern, teljesen 32 bites, megbízható több célú operációs rendszert hozzon létre. Az első verzió (Windows NT 3.1 és Windows NT 3.1 Advanced Server) 1993 júliusában került piacra, melyet 1994 szeptemberében követett a Windows NT 3.5. A Windows 95 kompatibilis felhasználások Windows NT-n való futtathatóságát az 1995 májusában bevezetésre került Windows NT 3.51 verzió biztosította. A Windows NT 3.5 1995 júliusában – erős korlátozásokkal – megszerezte a TCSEC C2, a Windows NT 3.51, 1996 októberében az ITSEC E2 minősítést.

Ennek a változatnak a továbbfejlesztésével és a Windows 95-nél bevezetett felhasználói grafikus felület alkalmazásával került piacra 1996 júliusában a Windows NT 4.0 család, mely négy tagból áll:

- Windows NT Workstation 4.0, munkaállomások operációs rendszere;
- Windows NT 4.0 Server, többcélú hálózati operációs rendszer;
- Windows NT 4.0 Server, Enterprise Edition, többcélú, fürtözhető hálózati operációs rendszer;
- Windows NT 4.0 Terminal Server Edition, Windows alapú terminál támogatás.

Az eredeti változat időközben sokat változott a szervizcsomagok (Service Pack) kiadásával. (2000 októberében az SP6a a legfrissebb). A Windows NT 4.0 munkaállomás és szerverváltozat 1999 novemberében a TCSEC szerinti C2, valamint 1999 márciusában az ITSEC szerinti E2 minősítést kapta meg. (Mindkét minősítés a legújabb SP6a szervizcsomaggal érvényes.)

A Windows NT új fejlesztésének neve 1998-ban NT 5-ről Windows 2000-re változott. A Windows 2000, mely 2000 februárjában került piacra, alapvetően a Windows NT alapokon épült, azonban nemcsak egy továbbfejlesztett változat, hanem több új, eddig Microsoft rendszereknél még nem használt funkcióval is rendelkezik.

A Windows 2000 család négy tagból áll: – Windows 2000 Professional, az üzleti munkaállomások és laptop számítógépek operációs rendszere; Windows 2000 Server, többcélú vállalati hálózati operációs rendszer; Windows 2000 Advanced Server, elektronikus kereskedelmi és üzleti alkalmazásokhoz; végül a Windows 2000 Datacenter Server, mely a vállalatok nagy teljesítményű és hatékony kiszolgáló operációs rendszere lehet.

A Windows NT biztonsági architektúrája alapvetően az alábbi rendszerelemekre épül:

- Local Security Authority (LSA):
  Ez az elem alkotja a Windows NT központi biztonsági modulját. Feladata a felhasználóazonosítás, helyi biztonsági intézkedések alkalmazása, valamint a naplózás végrehajtása.
- Security Account Manager (SAM):
  Ez az elem végzi a felhasználók és csoportfiókok kezelését.
- Security Reference Monitor (SRM):


Figyelj jól!

A rendszer objektumaihoz való hozzáférések ellenőrzését végzi, illesztési felületet biztosít a központ biztonsági modul (LSA) számára.

A Windows 2000 a biztonsági követelmények kielégítése szempontjából a következő újdonságokat vezette be:

- Megosztott erőforrások kezelése;
- Active Directory;
- Új NTFS fájlrendszer, lényegesen több attribútummal (ezt már az NT Service Pack 4 is tartalmazta, de a beállításokat csak az Option Pack telepítése után lehet használni);
- Lemezkvóták bevezetése;
- EFS (Encrypted File System), a merevlemezen lévő állományok titkosítása. Ez megakadályozza a fájlokhoz való illetéktelen hozzáférést. Ez például hordozható számítógépeken kiválóan alkalmazható;
- DFS (Distributed File System), összefogja a megosztott mappákat, és leegyszerűsíti a navigációt közöttük.

11.1.3. UNIX


Figyelj jól!

UNIX név alatt operációs rendszerek egy egész sorát szokták érteni. A UNIX operációs rendszer kialakulása 1969-ben kezdődött az AT&T Bell Laboratóriumának Computing Science Research Department-jén, ahol ez időpontban egy korai többfelhasználós interaktív rendszert, az úgynevezett MULTICS operációs rendszert használták. Az alapelvek lefektetésénél nem az akkori technikai színvonal volt a meghatározó, így sikerült elérni, hogy a UNIX ugyan eleinte meglehetősen lassan terjedt, ugyanakkor időtálló operációs rendszerré vált, a különböző biztonsági és védelmi funkciók a kezdetektől fogva integráns részét képezték.

A 70-es években elsősorban kutatóintézetekben és egyetemeken terjedt, amelyek számára az AT&T a kezdeti időkben ingyenesen adta. Ezen kívül a telefontársaságok is kiterjedten alkalmazták és alkalmazzák a mai napig, mind programfejlesztési, mind pedig hálózati tranzakciós feladatok ellátására.

A 80-as években a UNIX új szolgáltatásokat integrált magába. Kiegészült grafikus kezelői felületekkel, a rendszerek egy része az X-WINDOW/OPEN LOOK, más rendszerek az X-WINDOW/MOTIF grafikus felhasználói felületet tartalmazták. Később a CDE (Common Desktop Environment) felülettel próbálták a különböző gyártótól származó termékek kezelői felületét egységesíteni, de mindegyik rendszerben meghagyták az eredeti ablakkezelő felületet is. Különböző hálózati szolgáltatások is elérhetővé váltak a TCP/IP protokollra alapozva, NFS, FTP stb. felhasználásával. A UNIXnak az internetben és általában a hálózatos üzemben kiemelkedő szerepe volt és van. A Berkeley egyetemen kidolgozott BSD UNIX volt az, amely gyakorlatilag máig referencia implementációnak szolgál a TCP/IP protokollhoz, és szinte minden UNIX és jópár nem UNIX rendszer is az ott írt kódot

használja máig a hálózatkezeléshez. Általános vélemény, hogy internetkörnyezetben szerverfeladatokra a UNIX rendszerek a legmegfelelőbbek. Mindezek lehetővé tették, hogy a UNIX ezen időszakban kilépjen az egyetemi-kutatóintézeti szférából és önálló piaci termékké váljon.

A UNIX-ot magas szintű programozási nyelven, C-ben írták, ezért egyszerűen lehet más számítógép-architektúrákon is implementálni. Ennek következtében szinte minden gyártó elkészítette a saját UNIX változatát. Szigorúan véve ezek közül keveset lehet UNIX-nak hívni, hiszen ez az elnevezés védjegy, de ennek ellenére a rendszerek nagyfokú hasonlóságot mutatnak, sőt gyakran közös kódra épülnek. Ezeket a rendszereket is szokás azonban UNIX vagy UNIX-szerű rendszereknek hívni. A **11.1.** táblázat az ismertebb rendszereket sorolja fel. Az utolsó négy rendszer különös figyelmet érdemel, mert nemcsak ingyenesen hozzáférhetőek, de forráskódban terjesztik őket, amelynek biztonsági szempontból nagy jelentősége van.

A kezdeti időszak ingyenes terjesztési politikája és a mindenki által szabadon módosítható forráskód egyúttal komoly hátrányokat is jelentett: viszonylag rövid idő alatt számtalan egymástól lényegesen eltérő implementáció jött létre, amelyek egymással csak többé-kevésbé voltak kompatibilisek.

Gyártó	Platform	Operációs rendszer
Compaq (volt DEC)	Alpha	Tru64 UNIX
Hewlett Packard (HP)	HPPA	HPux
IBM	RS6000	AIX
Santa Cruz Operation	Intel	SCO UNIX
SGI (Silicon Graphics)	Mips	Irix
Sun Microsystems	Sparc és Intel	Solaris
Internet közössége	Intel és több más	Linux
Internet közössége és FreeBSD Inc.	Intel, Alpha	FreeBSD
Internet közössége	Intel és több mint 35 másik	NetBSD
Internet közössége	Intel és sok más	OpenBSD

11.1. táblázat

Az egységes UNIX szabvány létrejöttének érdekében gyártói és felhasználói szervezetek jöttek létre. Így az USA-ban POSIX (Portable Operating System Interface (X)), Európában pedig X/OPEN néven hoztak létre ajánlásokat kidolgozó csoportokat. A POSIX-ot az Egyesült Államokban kormányzati ajánlásként is elfogadták, az X/OPEN Európában mint európai uniós ajánlás szerepel. Kormányzati beszerzések esetén az X/OPEN ajánlásait kell figyelembe venni Magyarországon is.

A UNIX rendkívül sok implementációval rendelkezik, konstrukciója lehetővé teszi, hogy a TCSEC C2 szintű követelményeknek megfeleljen, azonban mindig célszerű ellenőrizni, hogy a konkrét implementáció és verzió milyen minősítést szerzett. Szükség esetén, ha az adott verzió nem rendelkezik a követelményeinket kielégítő minősítéssel, akkor nekünk magunknak kell egy tanácsadóval minősíttetni, vagy legalább véleményeztetni.

Tisztában kell lenni azzal is, hogy nagy popularitása, nyitott, akár forrásnyelvi szintű hozzáférhetősége miatt nagyobb külső fenyegetésekre kell számítani, mint mondjuk egy egyedi operációs rendszerrel rendelkező nagygépes rendszer esetén. Figyelemmel kell kísérni a biztonsági tanácsadók által feltárt biztonsági réseket, és ha a gyártó javítása megbízható forrásból rendelkezésre áll, lehetőleg azonnal telepíteni kell, betömendő a keletkezett biztonsági rést. A CERT[8] már 1999. év végén jelezte a DDoS (Distributed Denial of Service) támadást lehetővé tevő eszközök létrejöttét, 2000. február elején mégis megtörténtek az AOL és más nagy portálokat megbénító támadások.

11.1.4. Novell hálózati operációs rendszer

A Novell hálózat logikai topológiáját tekintve alapvetően csillagpontos hálózat, melynek központjában egy Novell Netware szerver található, ehhez kapcsolódnak a hálózati munkaállomások. A szervergép alapvetően fájl, és nyomtató szerver, szemben például a UNIX rendszerekkel ahol a felhasználó belépve kap egy saját shell-t is.

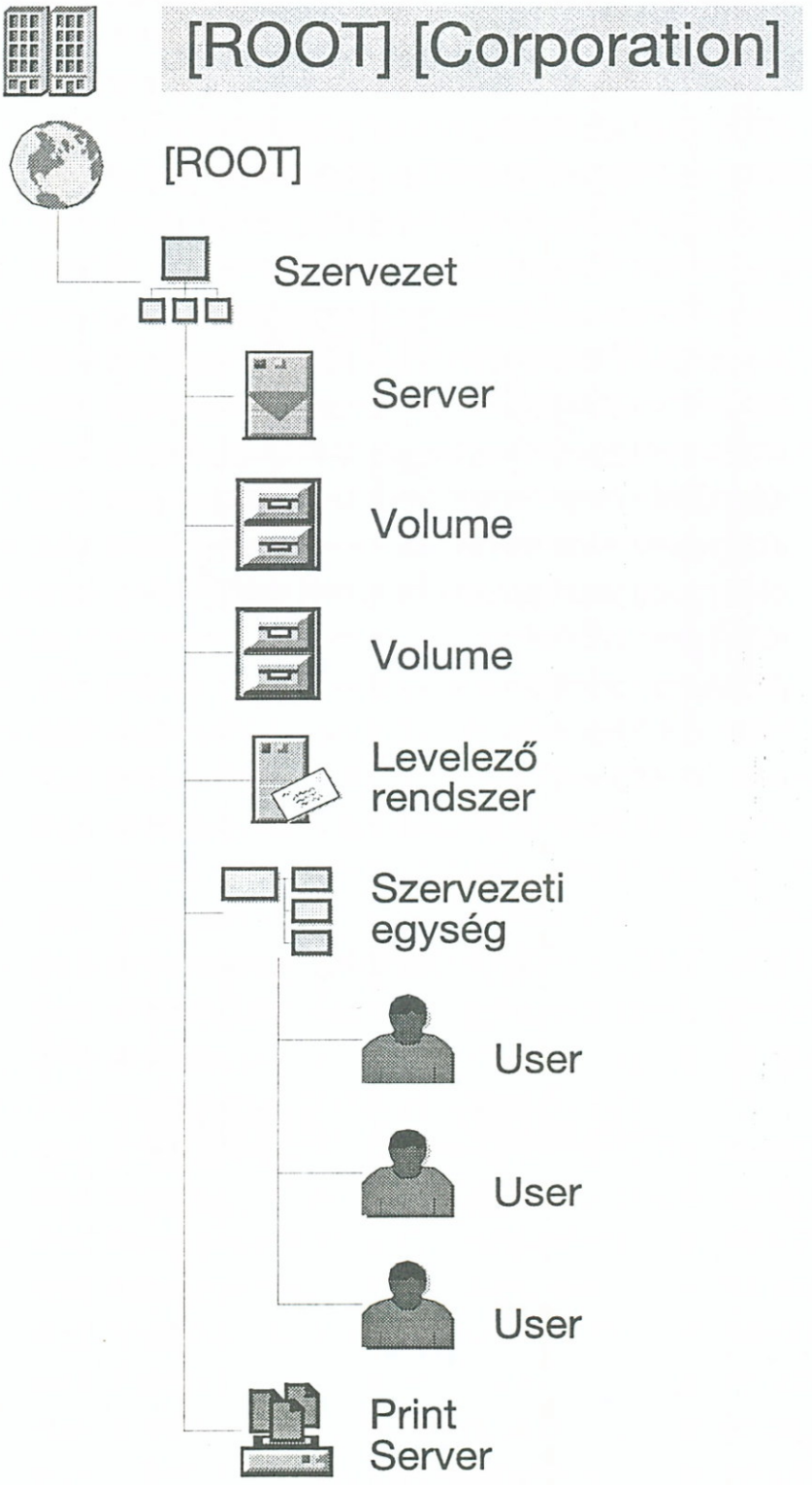
A Novell szerverhez számos különböző operációs rendszert használó kliens kapcsolódhat (DOS, OS2, Windows, Windows NT, UNIX, Macintosh), így egy adott fájlhoz számos operációs rendszer környezetet kell biztosítani.

A Novell szerveren az állományokat nem meghajtókra bontva tárolják, hanem a fájlrendszer egységes fastruktúrát alkot, ahova volume-okat (köteteket) lehet beilleszteni. A 4.1x-es változattól kezdődően egy kötet több partíción helyezkedhet el, vala-

[8] CERT = Computer Emergency Response Team (Számítógép Veszélyekre Reagáló Csoport) – nemzetközi szakmai-társadalmi szervezet, amely a számítógépes rendszereket fenyegető veszélyekre történő figyelmeztetéssel, az elkerülés, a megoldás lehetőségeinek közreadásával foglalkozik.

mint egy partíción több kötetet lehet definiálni. A definiált köteteket be lehet illeszteni (mount), illetve ki lehet venni (unmount) az állományokat tartalmazó „fából".

A Novell 3. verzióval bezáróan a bindery elv szerint minden szerver kizárólag a saját erőforrásait és az azokhoz tartozó hozzáférési jogokat tartja nyilván. Ez komoly adminisztrációs nehézségeket jelentett nagyobb hálózatok esetén.



11.1. ábra


Figyelj jól!

A Novell 4.x-es verziótól kezdődően a bindery elvet felváltotta az NDS (Novell Directory Service). Az NDS hálózati szinten egységes, osztottan tárolt, hierarchikus felépítésű adatbázis (**11.1.** ábra), amely tartalmazza a hálózat összes erőforrását és az azokhoz való hozzáférési jogokat. Az NDS fa alapvetően a következő elemeket tartalmazhatja:

- Tároló (Container) objektumok: Olyan tároló objektumokat szimbolizálnak, amelyek az NDS fa egyes elágazásait jelentik. Tartalmazhatnak más tároló, ill. levél objektumokat.
- Levél (Leaf) objektumok: A hálózaton megtalálható erőforrásokat reprezentálják. A fa struktúra legvégén helyezkednek el.

Az NDS-ben a hálózat összes erőforrásához tartozó jogosultság tárolásra kerül (beleértve a nyomtatókra és a fájlrendszerre vonatkozó jogokat is). Az NDS-ben található objektumokhoz alapvetően kétféle jogosultsági rendszert lehet megadni, egyik magára az objektumokra vonatkozik, a másik az objektumokhoz tartozó tulajdonságokra (properties) vonatkozik.

A hálózatba való bejelentkezés sikeres azonosítás és hitelesítés után történhet meg. A belépés nem azt jelenti, hogy egy adott Novell szerverre lép be a felhasználó, hanem azt, hogy belép a hálózatba az NDS fa egy adott pontján.

Novell NetWare szerverként IBM PC kategóriájú számítógépek jöhetnek szóba. A Novell kifejlesztett egy specifikációt a különböző hardvereszközökhöz tartozó „driver"-ek megírására, és létrehozott egy azok tesztelését szolgáló eljárást is (Yes Tested and Approved). A Novell NetWare 4.11 verzió TCSEC szerinti C2 minősítéssel rendelkezik, mely minden olyan szervergépre érvényes, amelyik a Novell által bevizsgált eszközökből épül fel („Yes" logó). A kliensek esetében is igazak a fent említettek, amennyiben a kliens számítógép operációs rendszere is rendelkezik minősítéssel. A leggyakrabban használt kliens operációs rendszerek közül a Windows NT 4.0 rendelkezik csak TCSEC szerinti C2-es minősítéssel, az MS-DOS, Windows 95, Windows 98 rendszerek nem.

11.2. Hálózatok


Tanuld meg!

A gyors adatátvitel, ill. a nagyobb teljesítmény elérése érdekében a számítógépeket egy közös kommunikációs rendszerben kapcsolják össze. Az összekapcsolt gépeket munkaállomásoknak (workstation) nevezik. Ezeket a hálózatba kötött számítógépeket egy speciális, úgynevezett hálózati operációs rendszer működteti. A számítógép-hálózat számítógépei a rendszerben egymással adatokat, információkat cserélhetnek, ill. erőforrásaikat megosztva használhatják. Ilyen erőforrások lehetnek a fájlok, nyomtatók stb. ... A megosztás azt jelenti, hogy az adott munkaállomás tulajdonosa, hozzáférési jogosultságot ad a saját gépén elérhető erőforrások-

hoz való hozzáféréshez. Az információcserét úgynevezett hálózati vezérlőkártyák és adatkábel-rendszer biztosítja.

A számítógép-hálózatok – mivel több számítógépből állnak – általában nem azonos típusú és konfigurációjú számítógépekből állnak, ezt a hálózat tervezésekor, a megfelelő szabványok és protokollok használatának alkalmazásával figyelembe kell venni.

A korszerű hálózatokban egy vagy több számítógép kitüntetett szerepet kap (szerver), ezek a gépek kezelik az erőforrásokat, tárolják az adatokat, garantálják a biztonsági követelmények betartását.

A számítógépes hálózatok lehetnek központi vagy osztott erőforrást használók.

- Központi erőforrás-használat esetén a hálózati összeköttetés révén a munkaállomások a szerver számítógép gépének erőforrását használják. A munkaállomásokkal szemben támasztott hardver- és szoftverigények lényegesen egyszerűsödnek. Biztonsági szempontból kedvező, hogy a központi erőforrásokat tartalmazó szerver számítógép(ek) jól védhetők mind a fizikai, mind a logikai támadások ellen.
- Osztott erőforrás-használat esetén nincs kitüntetett szerepű számítógép, a hálózat valamennyi tagja megosztja saját erőforrását úgy, hogy azok a többiek számára elérhetők legyenek. Ezt az eljárást csak kis, pár számítógépből álló hálózat esetén célszerű használni. Az erőforrásokhoz való hozzáférést minden számítógépen külön-külön be kell állítani, ezért biztonsági szempontból lényegesen nagyobb a kockázat.

A hálózatokat általában három nagy csoportba szokták sorolni:

- Helyi hálózatok (LAN – Local Area Network)
  A helyi hálózatok olyan rendszerek, amelyekben a számítógépek fizikailag viszonylag egymáshoz közel helyezkednek el, például egy épületen belül. Ezek a hálózatok kapcsolódhatnak más hálózatokhoz, így rákapcsolódhatnak a nagy kiterjedésű hálózatokra is.
- Nagy kiterjedésű hálózatok (WAN – Wide Area Network)
  A nagy kiterjedésű hálózatok olyan rendszerek, melyeknek egyes szegmensei (elemei) földrajzilag is távol lehetnek egymástól. Ebben az esetben a kapcsolattartás más speciális módszerekkel valósítható meg.
- Globális hálózatok
  A globális hálózatok olyan világméretű hálózati rendszerek, melyek nagyszámú elemet tartalmaznak, eléggé heterogén felépítésűek, nagyon sok számítógépet, ill. részhálózatot foglalnak magukban. Globális hálózat például az Internet.

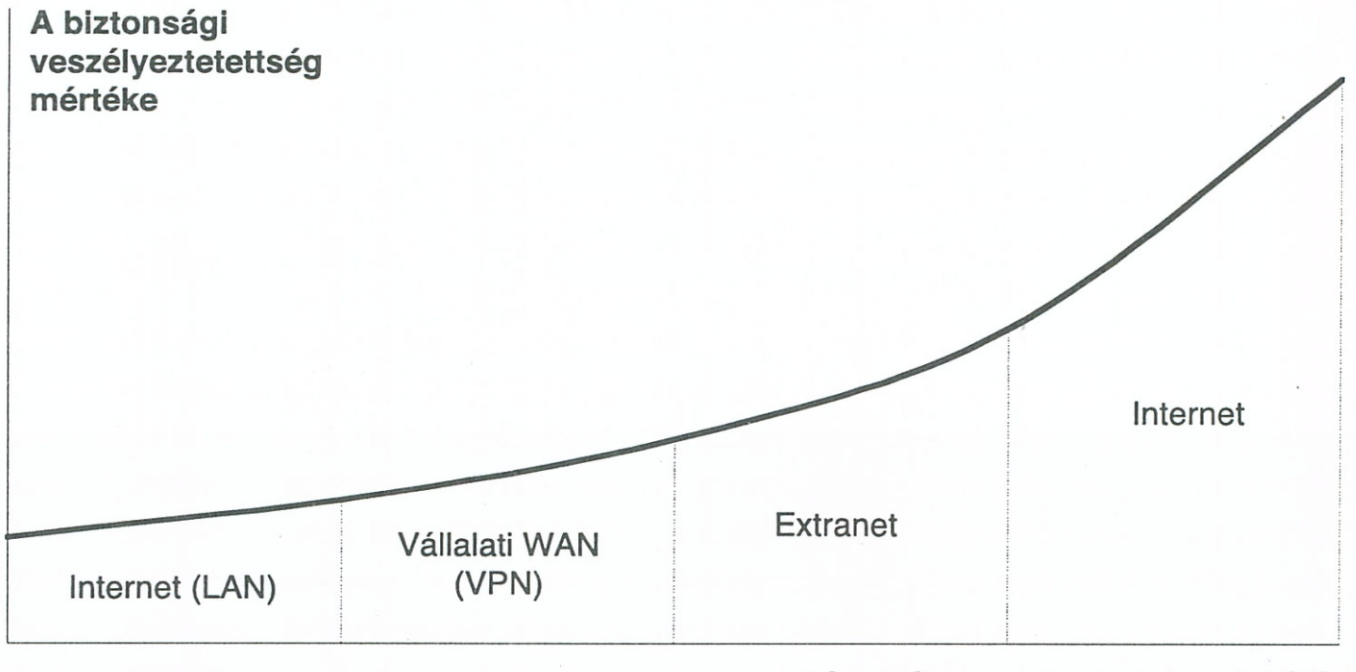
Közép- és hosszabb távra mutató elemzések szerint visszaszorulóban van az egyedi számítógépekre szabott informatika. Egyes előrejelzések szerint a 2000-es évek elejére a jelenlegi PC alapú szoftvermegoldások mintegy fele web alapú szoftverré válik. Az interneten külső támadásoktól vagy e-mailben elküldött vírusoktól kell tartanunk, az intraneteken leginkább az a veszély fenyeget, hogy az érzékeny adatokhoz az arra feljogosított felhasználókon kívül más is hozzáférhet, az

extraneteken pedig attól, hogy nem csak az arra feljogosított és ellenőrzött stratégiai partnerek férnek majd hozzá a hálózathoz. Mivel a cégek egyre több és jelentősebb információt tárolnak számítógépes hálózataikon, ezért egy-egy biztonsági résen történő behatolással egyre nagyobb károkat lehet okozni. Ilyen környezetben a védekezési lehetőségek pontos ismerete kulcsfontosságú tényező, sőt egy szervezet stratégiája nem képzelhető el megfelelő biztonsági stratégia kialakítása nélkül.

A vállalati, ill. a pénzintézeti számítástechnikai hálózatok legtöbbször stratégiai fontosságú adatokat tárolnak. Ezek bizalmasságát még akkor is meg kell őrizni, ha egyébként igény van az internet széles körű használatára. Ahhoz, hogy egy cég hatékony és biztonságos eszközként alkalmazza az internetet az üzleti vagy szervezeti működéséhez, átgondolt fejlesztési stratégia kidolgozására van szüksége. A kapcsolódás műszaki feltételei mellett biztosítani kell az informatikai rendszer magas szintű védelmét is. A kialakított biztonsági rendszert célszerű rendszeresen (például félévenként) átvilágítani, a gyenge pontokat és a konfigurációs hibákat feltárni.

Mint a **11.2.** ábra mutatja, egy informatikai rendszer biztonságát bármilyen kommunikációs kapcsolat csökkenti. A biztonsági veszélyforrások az adminisztrációtól való távolság függvényében egyre jelentősebbek.

Az internet bevezetésével a csatlakozó hálózat egésze (minden egyes hálózati csomópont, ill. azokon minden egyes szolgáltatás, például FTP, WWW, Telnet) támadási felületet nyújt megfelelő védelem hiányában. A hálózat biztonságos üzemeltetése megfelelő rendszabályok és intézkedések bevezetésével biztosítható.



11.2. ábra

A teljesség igénye nélkül a következőkben bemutatunk egy pár ilyen intézkedést:

1. Csak azonosított és hitelesített felhasználó jelentkezhet be a hálózat bármely erőforrására.
2. A hálózati adatátvitel a hitelesség és hitelesítés biztosítása érdekében harmadik fél számára értékelhetetlen legyen (például titkosított adatátvitel).
3. Minden biztonsági szempontból fontos eseményt naplózni kell, a naplózott adatokat rendszeresen ki kell értékelni.
4. A hálózatok biztonságos leválasztására, ahol ez szükséges tűzfalakat kell alkalmazni.
5. Virtuális magánhálózatok kialakítása.

11.3. Alkalmazások

Mit értünk alkalmazáson?

Az alkalmazáson értünk minden olyan, a felhasználó által betölthető és futtatható programot, ami nem tartozik az operációs rendszerrel szállított szolgáltatások közé.

Felhasználási területük szerint több csoportba sorolhatjuk az alkalmazásokat, itt most a felhasználási kör alapján csak a legjellemzőbb típusokat vizsgáljuk:

- Hálózattal kapcsolatos eszközök: Internet-böngésző, levelező rendszerek, FTP kliens stb.
- Irodai programcsomagok (szövegszerkesztők, táblázatkezelők, „asztali" adatbázis-kezelők, bemutató készítők)
- Adatbázis-kezelők
- „Nagy" alkalmazások (például integrált vállalatirányítási rendszerek, mint az SAP, Peoplesoft, MFG/Pro stb.)
- Egyéb kiegészítő és segédprogramok

Irodai rendszerek

Az irodai programcsomagok említésekor mindenkinek a piacot uraló Microsoft Office jut eszébe, de ide sorolhatóak a régebben nagyobb jelentőséggel bíró Wordperfect, a Lotus SmartSuite, vagy az ingyenessége és a Linux megerősödése folytán terjedő StarOffice is. Ezen alkalmazásokra általánoson elmondható, hogy a fejlesztésük során biztonsági szempontokat csak nagyon kis mértékben vettek figyelembe, de nem is ez volt az alapvető cél. Szinte mindegyik programban létezik jelszavas hozzáférés-védelem, de ez nem jelent igazán komoly akadályt a dokumentumokban tárolt információkat megszerezni igyekvő hozzáértő személyeknek,

mivel a programok és az általuk használt fájlformátumok publikusak, a jelentősebb formátumokhoz készített jelszófeltörő programok szabadon letölthetők az internetről. Nem is feltétlenül rossz szándékkal készültek ezek a jelszófeltörő programok, hanem csak a feledékeny felhasználók megsegítésére. Azonban, ha ez az eszköz már létezik, mindig akad annak rosszindulatú felhasználója is.

Ha az a célunk, hogy elektronikus formában hozzunk nyilvánosságra egy dokumentumot, de úgy, hogy azt ne lehessen módosítani, kinyomtatni, vagy az a cél, hogy csak a címzett olvashassa el, akkor bizonyos korlátok között jó megoldás lehet az Adobe PDF (Portable Document Format) formátuma. A dokumentumokat a megszokott szövegszerkesztőnkkel szerkeszthetjük, csak a nyomtatást kell az úgynevezett „PDF Writer" nevű virtuális nyomtatóra küldeni, amely egy olyan dokumentumot hoz létre, amelyet a szabadon hozzáférhető Acrobat Reader programmal elolvashatunk. Ha korlátozni akarjuk a hozzáférést, akkor nem elég a PDF formátumot előállítani, hanem az Acrobat Exchange programba betöltve be kell állítani a kívánt biztonsági jellemzőket, nem elfeledkezve a „Change Security" (védelem megváltoztatása) opció jelszóhoz kötéséről sem, különben bárki, aki rendelkezik az Acrobat Exchange programmal, szabadon módosíthat minden védelmi beállítást.

A fenti kitérő egyúttal arra is példa volt, hogy nem elég olyan terméket vennünk, amelyik kielégíti a biztonsági követelményünket, azzal is tisztában kell lennünk, hogy a gyártók általában – a telepítés megkönnyítése és az egyszerűbb kezelhetőség érdekében – a termék biztonsági beállításait a legalacsonyabb szintre állítják be. Erre a másik, ennél jóval szemléletesebb példa az Operációs rendszerekről szóló fejezetben található, ahol azt látjuk, hogy egy alapértelmezés szerint telepített Windows NT rendszeren még mennyi beállítást kell ahhoz elvégezni, hogy a rendszer, amely a TCSEC C2 szintű biztonsági követelményeknek eleget tud tenni, ténylegesen is a C2 szinten működjön.

Adatbázis-kezelők

Az adatbázis-kezelőkön itt most az SQL felületű relációs adatbázis motorokat értjük, mint például Oracle, Ingres, Informix, DB2, Rdb, stb. Ezek a robusztus rendszerek általában egy nagy teljesítményű szerveren futnak a bekapcsolástól a tervezett vagy hibából következő leállásáig. Egyidejűleg több adatbázist képes kezelni és párhuzamosan bejelentkezett több felhasználót kiszolgálni. A nagy adatmennyiséggel, tranzakciókkal jellemezhető felhasználói programok az adatbáziskezelők beépített szabványos szolgáltatásait használják az adatok elérésére, módosítására, lekérdezésére ellentétben a számítástechnika hajnalára jellemző egyedi fejlesztésű, célorientált fájlformátummal, és fájlkezelő eljárásokkal jellemezhető programokkal. Biztonsági szempontból e régi programoknak ugyan megvolt az az előnye, hogy az egyedi adatformátum miatt, a benne lévő információ csak a formátumot ismerők számára volt értelmezhető, de rengeteg más praktikus szem-

pontból az adatbázis-kezelők idővel teret nyertek, és ma már az egy felhasználós videokazetta-nyilvántartó programocskák is az adatbázis-kezelők szolgáltatásait veszik igénybe.

A minősítéssel rendelkező operációs rendszerekhez hasonlóan a jelentősebb adatbázis-kezelők is rendelkeznek minősítéssel. A minősített termékek táblázatában több standard verziójú terméket is találhatunk a C2 osztályban, illetve bizonyos speciális kiegészítésekkel némelyikük a B1-es minősítést is eléri. Itt ismét meg kell jegyezni a korábban hangoztatott intelmet, hogy a termékkel elérhető legmagasabb szintű biztonság nem az alapértelmezett beállításokkal érhető el. Sőt kimondottan erre a termékkörre jellemző tapasztalat, hogy a termék alapváltozatával elérhető biztonsági szint az opcióként kínált kiegészítőkkel együtt érhető el. Ez elsősorban nem azért kellemetlen, mert az opciók plusz költséget jelentenek, hanem azért, mert amikor ez kiderül – optimális esetben már a rendszerterv biztonsági auditálásakor –, régen túl vagyunk a projekt költségtervezési fázisán, az utólagos költségmódosítások pedig általában rendkívüli egyeztetéseket, vitákat jelent.

Ez a helyzet azonban még mindig kezelhető, mert a biztonsági tervezés a projekt szerves részét képezi, időben kiderülnek a problémák. Ennél jóval súlyosabb a helyzet, ha az informatikai biztonság tervezése nem képezi a projekt részét, és a fent említett hiányosság ki sem derül, az elkészült rendszer pedig biztonsági lyukakkal lesz tele. Egy utólagos biztonsági auditálás kideritheti a hiányosságokat, de azok megszüntetése utólag mindig jóval bonyolultabb és költségesebb.

„Nagy" alkalmazások

Ebbe a körbe itt most olyan termékeket értünk, függetlenül a felépítésétől, az általa ellátott feladattól, amelyek – esetleg egy kis kiegészítéssel – komplett informatikai rendszert alkotnak. Ezeket a rendszereket általában egyidejű hozzáféréssel nagy felhasználószámra, maximált válaszidőre és nagyméretű adatbázisok felhasználására tervezték. Az ilyen követelmények óhatatlanul felvetik a rendelkezésre állás jól meghatározott szintű biztosítását és a felhasználók egyedi azonosítását, ezért fejlesztés során már biztonsági szempontokat is figyelembe vettek. Az integrált vállalatirányítási rendszerek jellemzője az adatokhoz való szelektív hozzáférés biztosítása is. A cél itt elsősorban nem a külső, rosszindulatú betörések elleni védelem, hanem a belső, szervezeti hierarchiaszinttől függő kompetencia alapján definiált hozzáférések szabályozása. Míg a hálózat és az operációs rendszer szintjén az adatfájlokhoz történő hozzáférést szabályozhatjuk, az adatbázis-kezelő vagy az alkalmazás már a felhasználói jogosultság kezelésével az adatbázison belüli adattáblákhoz, illetve akár mezőkhöz, rekordokhoz való hozzáférést is szabályozhatja. A bérszámfejtő például elkészítheti a havi bérjegyzéket, de nem kérdezheti le a dolgozó egyéb, más szempontból nyilvántartott személyes adatait, vagy fordítva, egy speciális ügykezelő dolgozhat ezen adatokkal, de nem tudhatja, kinek mennyi a bé-

re. A differenciált, szerepkörökhöz kötött hozzáférés mind az adatbázis-kezelőben, mind az alkalmazásban megoldható, de ezt általában mégis inkább az alkalmazások szintjén építik be a rendszerbe. Általában azért történik ez így, mert ha nem használjuk ki az adatbázis-kezelő speciális lehetőségeit, hanem csak a szabványosakat, amelyek a konkurens termékekben is rendelkezésre állnak, akkor az alkalmazás jóval könnyebben áttehető más adatbázis-kezelőre, ezzel kevésbé függünk a gyártótól, és a technikai fejlődést is könnyebb követni.

Fentebb említésre került, hogy a nagy alkalmazások fejlett jogosultságkezeléssel rendelkeznek. Ugyanakkor meg kell említeni, hogy ehhez nagyon szorosan kapcsolódik a felhasználók korrekt, hasonló szintű azonosítása és hitelesítése. Az alkalmazások ezen modulja viszont általában elég felületes módon készült. Több rendszerben tapasztaltuk, hogy a jelszavakat sima, kódolatlan szöveges adattáblában tárolják, vagy nincs kötelező jelszóváltás, a jelszó hosszára nincs minimális megkötés, esetleg a korábban használt jelszavakat újra fel lehet használni. Egy korrekt jelszókezelő mechanizmus beépítése természetesen rendkívül munkaigényes feladat, ezért talán nem is ez a célszerű megoldás, hanem az alkalmazást úgy kell elkészíteni, hogy az operációs rendszer megbízható felhasználóazonosító rendszerét vagy a szervezetnél alkalmazott biztonsági szerver hasonló szolgáltatásait vegye igénybe. Ez utóbbi biztonsági szerverek általában a heterogén számítástechnikai rendszerrel rendelkező, nagy szervezetek egységes felhasználóazonosító rendszerének (SSO[9]) biztonsági szerverei, amelyek szabványos protokollon (LDAP[10]) keresztül biztonságos, megbízható módon azonosítják a felhasználót.

Egyéb kiegészítő és segédprogramok

A kiegészítő programok körébe rendkívül sok programtípus beleérthető. Ide tartoznak a mindenféle formátumú szövegfájlok, képek, mozgóképek megtekintésére, szerkesztésére szolgáló programok, bináris fájl-editorok, adatbázis lekérdező/módosító eszközök, fájlkezelők, tömörítő, szótár-, rajzoló programok és egyebek. Ezekre még inkább igaz, mint az irodai programokra, hogy tervezésük során biztonsági szempontokat nem vettek figyelembe.

E programok – minden praktikus hasznuk mellett – sajnos biztonsági kockázatot jelentenek, mert ellenőrizetlen hozzáférésre adnak alkalmat. Miért? A különböző DBview (adatbázis nézegető) programok például az alkalmazói rendszer hozzáférési rendszerét megkerülve közvetlenül olvashatóvá tesznek minden adatot, esetleg annyi kényelmetlenséget okoznak, hogy a kódok mögötti tartalmat egy másik adattáblában kell keresni. A SQL nyelvű lekérdező eszközök hasonló veszélyeket

[9] SSO: Single Sign On – Egyszeri bejelentkezés

[10] LDAP: Lightweight Directory Access Protocol

rejtenek, itt annyival csökken a veszély, hogy az adatbázis-kezelő felhasználó azonosító rendszere csak a jogosult – vagy a jelszót megszerző – személyeknek enged teljes hozzáférést, de a korábban említett alkalmazásszintű finomított hozzáférés szabályozás így mégis megkerülhető.

Következő példa: Képlopó programok – Roppant hasznos jószág, például nagyon könnyű a segítségükkel felhasználói kézikönyvet készíteni, stb. Ha semmi más program nem lenne a PC-n, csak az alkalmazói rendszer és egy képlopó program, már ez is azt jelenti, hogy nem lehet *fokozott biztonsági osztályú* rendszert készíteni. Miért?

Csak egyetlen indok a sok közül: A MeH ITB 12. sz. ajánlás szerint a kiemelt üzleti titkot, szolgálati titkot tartalmazó adatokat kell ilyen szintű védelemmel ellátni, ami a TCSEC szerinti B1-es osztály követelményeinek kielégítését jelenti. Az ilyen rendszerben minden nyomtatott kimeneten biztosítani kell, hogy a kezelési jelzés, ami a dokumentum minősítésére utal, megjelenjen. Az ilyen biztonsági címkék meglétét csak a megfelelő alkalmazói rendszer tudja biztosítani, de van mellette egy képlopó, amivel tetszőleges képernyőkivágatot kinyomtathatunk, minden gond és nyom nélkül.

11.4. A rejtjelezés, a digitális aláírás és az elektronikus bizonyítványok

A *kriptológia* az adatok, üzenetek *rejtjelezés*ével (kódolás, sifrírozás) és *megoldás*ával (rejtjelfejtés, dekódolás, desifrírozás) foglalkozó tudományág, a matematikai tudományok egyik részterülete.

A kriptológia egyik fő területe a *kriptográfia,* magyarul a rejtjelezés, amelynek alapvető feladata matematikai módszereket alkalmazó ***algoritmusokkal*** és azok használatának pontos leírását tartalmazó – szigorúan betartandó – ***kriptográfiai protokollok*** segítségével biztosítani az üzenetek, illetve tárolt információk bizalmasságát, védettségét, hitelességét. A kriptológia másik tudományága a *kriptoanalízis* (*kriptográfiai* bevizsgálás), amely a rejtjeles üzenet birtokában, de az eljárás teljes ismerete nélküli megfejtéssel (feltörésére) irányuló eljárásokkal foglalkozik. A kriptoanalízis főként matematikai módszereket használ.

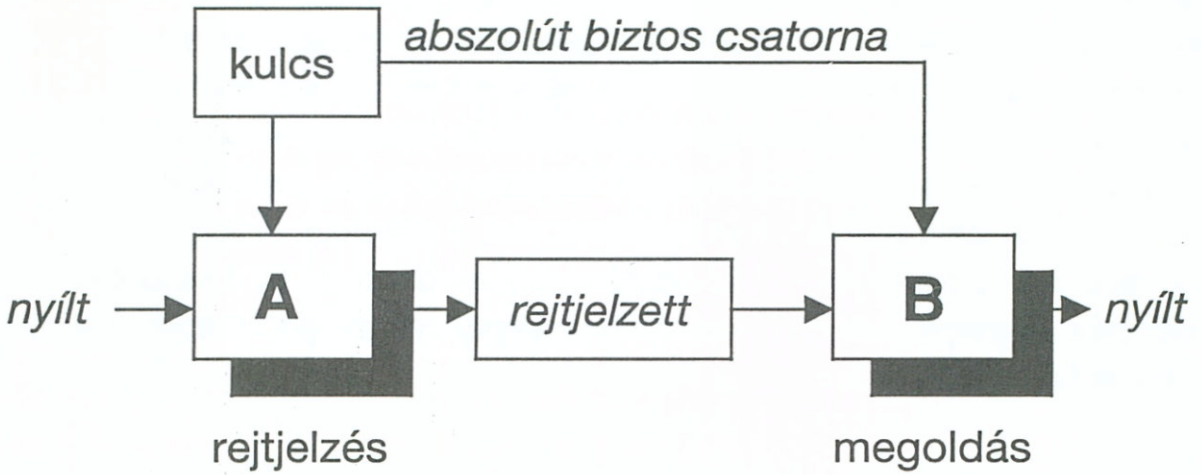
Maga az adatok rejtjelezése egyfajta védekezési eszköz, amely komoly védelmet jelent, de önmagában meglehetősen „sérülékeny", ha nem párosul egyéb, többek között az informatikai biztonságot is érintő védelmi intézkedésekkel.

A rejtjelzett kommunikáció folyamatában a *küldő* és a *fogadó* üzenetváltása történik meg. A küldő a *nyílt szövegből rejtjelezés* segítségével *rejtjelzett szöveget* állít elő, majd elküldi a vevőnek, aki azt *visszafejtve* megkapja az eredeti nyílt szöveget. A rejtjelezési folyamat – kódolás – során a rejtjelezett szöveg előállításához

Tudni kell!

az algoritmuson kívül általában szükséges egy *kulcs* is, amelynek ismerete elengedhetetlen a rejtjelezésnél és a visszafejtésnél is.

A rejtjelezés C. E. Shanon által – II. világháborús rejtjelfejtői tevékenységének tapasztalatait felhasználva – megfogalmazott „klasszikus" matematikai modellje szerint a rejtjelezés által védett kommunikációs csatornát kiegészíti egy „abszolút biztos csatorna", amelyen a kulcstovábbítás történik (**11.3.** ábra).



11.3. ábra

11.4.1. Szimmetrikus rejtjelező algoritmusok

Tudni kell!

A klasszikus rejtjelező eljárások egyetlen kulcsot használnak rejtjelezésre és megoldásra, miközben a megoldó algoritmus nem feltétlenül egy fordított sorrendben végrehajtott rejtjelezés. A legismertebb a *DES (Data Encryption Standard, Adat Rejtjelező Szabvány)*. A DES használata nem kizárólagos. Több helyen használják a svájci IDEA eljárást, vagy a Blue-Fish algoritmust.

1976 decemberében a *National Bureau of Standards*, USA, bejelentett egy új „Nemzeti Adatfeldolgozási Szabványt" (FIPS No. 46), amelyben a Data Encryption Standard, DES, rejtjelező gépet szabványosították. A DES 64 bites nyílt üzenet-blokkokat képez le ugyancsak 64 bites rejtjeles üzenetblokkokba, 56 bit nagyságú kulcsméret mellett. Az IBM által kifejlesztett algoritmus biztosítja, hogy a blokkon belül a kimenet minden bitje függ a bemenet minden bitjétől. A szabvány tartalmazza azt a kikötést is, hogy csak hardware implementált változata használható az USA-n belül, és az USA-kormányzat megtiltotta, hogy ezt a hardware kivitelezést exportálják.

Figyelj jól!

A DES javításként elterjedt a „Triple Des, 3-DES" használata. Ez vagy kettő, vagy három 58 bites kulccsal dolgozik. Az üzenetet először az első kulccsal rejtjelzik normál DES módban, majd a második kulccsal a megoldó algoritmust alkalmazzák. Az így nyert közbülső szövegre alkalmazzák ismét az első, háromkulcsos rendszerben a harmadik kulcsot.

Az exporttilalom miatt számos konkrét chipmegvalósítás található a piacon, és a pénzügyi szféra több nemzetközi szabványában található 3-DES elem. *Elsőrendű alkalmazási területe maga a kulcsterítés.*

Magát az algoritmust 5 évenként biztonsági vizsgálatnak vetették alá. Ez utoljára 1994-ben történt meg, amikor 1998-at jelölték meg a felhasználhatóság utolsó határának.

Ennek megfelelően a National Institute of Standards and Technology (NIST) olyan döntést hozott, hogy ki kell fejleszteni a DES utódját, amely az *Advanced Encryption Standard (AES, Fejlett Rejtjelező Szabvány)* nevet kapta. A pályázatot 1997 szeptemberében írták ki, közzétéve azon elvárásoknak a listáját, amelynek az AES algoritmusnak meg kell felelni. Ugyanakkor deklarálták, hogy a benyújtott rejtjelezési algoritmusok nyilvánosak, szabadon felhasználhatók lesznek. A kiírás szerinti elvárások:

- Legyen blokkos algoritmus 128 bites blokkmérettel
- A 128, 196 és 256 bites kulcsméret opcionálisan egyaránt megválasztható legyen
- Az algoritmus nyilvános, jogdíj nélkül használható
- Álljon ellen valamennyi ismert rejtjelfejtési módszernek
- Legyen világos, logikus szerkezetű, áttekinthető
- Mind a kódolás, mind a dekódolás gyors legyen
- Kevés memóriát foglaljon el
- Többféle processzoron is hatékonyan implementálható legyen

A versenyt a RIJNDAEL algoritmus nyerte meg, melynek szerzői *Daemen és Rijmen*, belga kriptográfusok. A Rijndael algoritmus teljes mértékben megfelel a fent leírt feltételeknek. A Rijndael algoritmus *egyszerű, világos, bármely programozási nyelven gyorsan programozható.* Ez is számos iterációs lépésben valósul meg.

A győztes algoritmust 2000. október másodikán jelentették be, de ez még nem jelenti azt, hogy ez automatikusan új USA-szabvány lesz. Át kell mennie egy sor formalizmuson, ami egy teljes évet is igénybe vehet.

11.4.2. Nyilvános kulcsú rejtjelezés

Olyan kriptográfiai rendszerben használják, amelybe bárki beléphet résztvevőként. A rejtjelező és a megoldó algoritmus azonos, és a rejtjelezéshez, illetve a visszafejtéshez kulcspárt használ. Az egyik kulcs a *nyilvános kulcs*, amivel a rejtjelezést végezzük, a másik pedig a *titkos (privát) kulcs,* amivel a visszafejtés végezhető el. A nyilvános kulcsot a felhasználó nevével együtt nyilvánosságra hozzák, a titkos kulcsot pedig titokban tartják.

A rejtjelezést a nyilvános kulcs birtokában könnyű elvégezni, de pusztán ezzel a kulccsal a dekódolás gyakorlatilag nem kivitelezhető. A titkos kulcs segítségével azonban a dekódolás is gyors művelet. Ezt a filozófiát megvalósító rendszerek gyűjtőneve: *Nyilvános kulcsú rendszerek* (public key cryptosystems).

A széleskörben használt RSA algoritmus a *modulo aritmetikában* az ismeretlent hatványban tartalmazó egyenletek megoldásának nagyfokú bonyolultságát használja ki, így megfelelő nagyságú modulus esetén a megoldás technikai kivitelezhetetlensége szolgáltatja a biztonságot. A „megfelelő nagyság" igen lényeges és a technika fejlődésével változik. A kezdetben biztonságosnak ítélt 40 bit hosszú kulcsok helyett ma már nem nevezhető biztonságosnak egy 1024 bitnél rövidebb kulcs.

A nyilvánosságra hozott kulcs egy (E,M) egészekből álló számpár. A titkosítás ezek segítségével történik. Először a dokumentum adott hosszúságú blokkjait az M modulusnál kisebb egész számmá alakítják, majd ezt a számot M modulusban felemelik az E-edik hatványra. Ez a szám, illetve ennek az átviteli csatornára elfogadható sorozattá kódolt változata lesz a titkosított üzenet.

A titkos kulcs a nyilvánoshoz hasonlóan egy (D,M) számpár, ahol M azonos az előzővel, míg a D dekódoló exponens úgy van megválasztva, hogy a titkosított üzenetnek megfelelő modulo-M számot D-edik hatványra emelve az eredeti üzenet adódik.

Megbízható algoritmushoz M-et két nagyon nagy prímszám szorzatának, E-t véletlenszerűen választják. Megjegyezzük, hogy a rejtjelezést a (D,M) titkos kulccsal is el lehet végezni. Ekkor a megoldó kulcs a nyilvános (E,M) kulcs lesz.

11.4.3. Elektronikus aláírás

A hagyományos aláíráshoz hasonlóan az elektronikus, vagy ahogy a mindennapi életben használjuk, a digitális aláírás biztosítja az elektronikus iratok hitelességét és sértetlenségét. A digitális aláírás fizikai megvalósításához általában az aszimmetrikus rejtjelezésen alapuló protokollt használják.

Digitális aláírásnak olyan elektronikus karaktersorozatot neveznek, amely igen nagy valószínűséggel csak az aláírótól származhat. A digitális aláírás tartalmazza az üzenet egyirányú képét (lenyomatát) s egyéb adatokat, például keltezést (dátumot, pontos időpontot), sorszámot, a küldött üzenetből képezett ellenőrző számot. Az aláírás jellemző a létrehozójára és az üzenetre egyaránt. Az elektronikus aláírást bárki ellenőrizni tudja, aki a megfelelő infrastruktúrához hozzáfér. A digitális aláírás két részből áll: a személyhez kötött aláírást generáló részből, s az ellenőrzést bárki számára lehetővé tevő részből.

A digitális aláírás elkészítéséhez először kiegészítjük a dokumentumot a megfelelő azonosítókkal, majd ennek a kiegészített dokumentumnak egy alkalmas sűrítményét készítjük el. Ez lesz a digitális aláírás. Az alkalmas sűrítmények elkészítésére szolgálnak az úgynevezett Hash eljárások.

A *Hash algoritmus* egy olyan transzformáció, amely egy tetszőleges hosszú szöveg fix hosszúságú digitális sűrítményét készíti el, amely kizárólag az adott szövegre jellemző. Angolul *message digestnek* is nevezik.

A nyilvános kulcsú kriptográfiában leggyakrabban alkalmazott a *Standard Hash Algoritmus, SHA*, amely USA-szabvány. Az algoritmus inputja egy tetszőleges, de

maximum 2^64 bit hosszúságú dokumentum, az outputja pedig egy 160 bit hosszúságú string. Az algoritmus számítástechnikailag sokféle módon valósítható meg, amelyeknek azonban ugyanazon bemeneti sorozat esetén ugyanazt a lenyomatot kell eredményezni.

11.4.4. Kulcskezelés, PKI, CA

A nyilvános kulcsú rendszerben fontos tudni, hogy a nyilvános kulcs tulajdonosa valóban az a személy, akinek a levelet szánjuk. A digitális aláírást bárki létrehozhatja, ezért valakinek tanúsítani kell, hogy valóban az az aláíró, akinek vallja magát. Ennek valódiságát egyrészt az alkalmazott digitális aláírások biztosítják, másrészt különféle, úgynevezett biztonsági modellek. A legbiztosabb megoldás a direkt biztonsági modell, amelyben mint a neve is mutatja a vevő személyesen adja át nyilvános kulcsát az adónak. Ez a valóságban – a fizikailag nagy távolságok miatt – a legtöbbször kivihetetlen, ezért széles körben a *hierarchikus biztonsági modell* alapján kiépített *Hitelesítés Szolgáltatón,* vagy közismert nevén a Certificate Authorityn (CA) alapuló rendszer terjedt el a gyakorlatban. A résztvevők által megbízhatónak tekintett harmadik fél egy digitális közjegyző szerepét játssza. Olyan szakosodott szervezet vagy cég, amely tanúsítványokat adhat ki kliensek és szerverek számára. A CA igazolja, hogy egy adott azonosítóval rendelkező felhasználó az, akinek vallja magát.

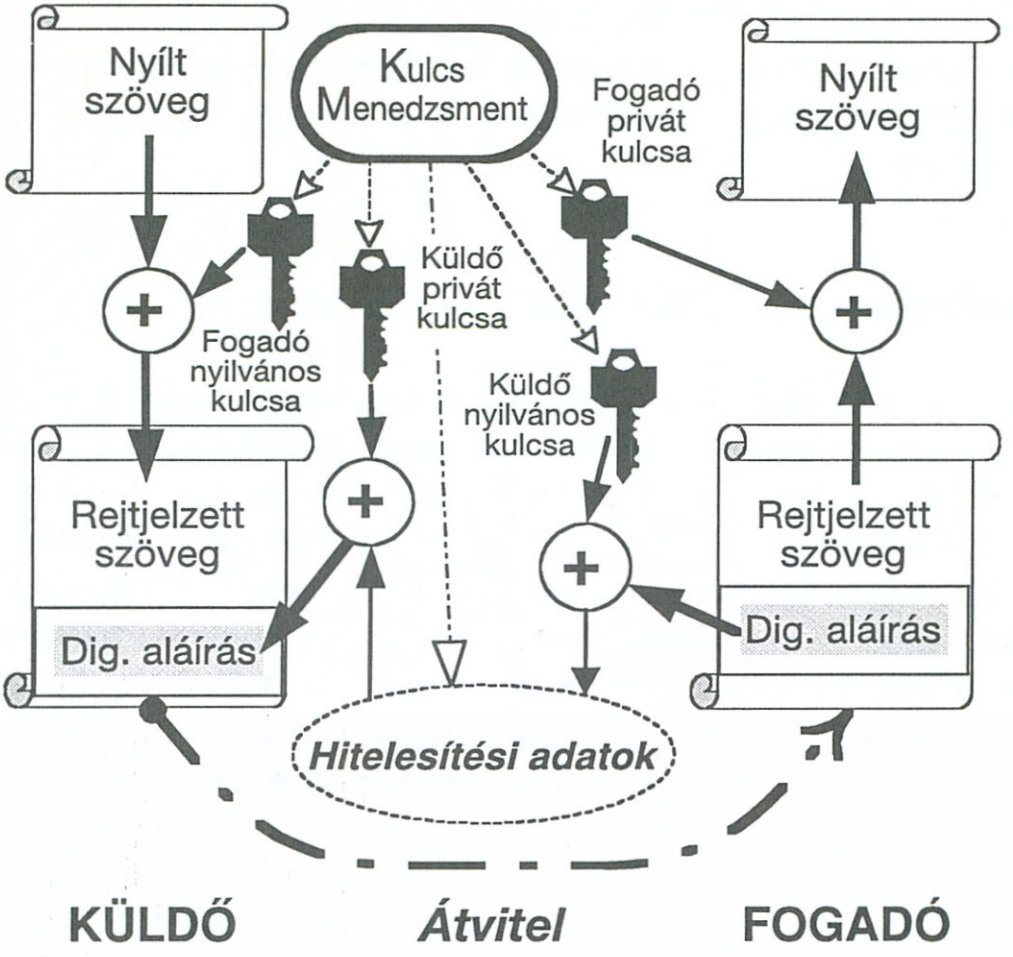
A rendszer legfontosabb eleme a fa struktúra gyökerében elhelyezkedő CA, aki direkt módon bizonyítja egy kulcs valódiságát, amennyiben ő adta ki. A fa szerkezet többi szereplője a CA-tól vagy egymástól kaphat igazolást egy objektum valódiságáról.

A CA-nak is van nyilvános-titkos kulcspárja, amit az elektronikus igazolás kiadására alkalmaz. A kibocsátott tanúsítvány tartalmazza az adott entitáshoz tartozó nyilvános kulcsot, az entitás nevét (személyazonosítóját), az érvényesség (lejárat) idejét. Ezt írja alá titkos kulcsával a CA, s ezzel az adott entitás és a nyilvános kulcs összetartozását mindenki számára ellenőrizhető módon hitelesíti.

Az elektronikus iratok (informatikai rendszerben tárolt adatok) hitelessége, bizalmassága és sértetlenségének védelme tehát az aszimmetrikus rejtjelezés, a digitális aláírások és a CA alapú kulcskezeléssel elméletileg magas biztonsággal oldható meg.

Egy küldő és egy fogadó közötti kapcsolatban megjelenő elektronikus dokumentum bizalmasságának és hitelességének a biztosítását a fenti elemek felhasználásával az **11.4.** ábra vázolja.

A Hitelesítés Szolgáltatónak feladata ellátásához rendkívül szigorú biztonsági feltételeket kielégítő infrastruktúrával kell rendelkezni. Ezek a biztonságos titkosítási módszerek mellett magukban foglalnak számítástechnikai követelményeket, mint például megbízható tűzfalak alkalmazása, de kiterjednek a személyzetre



11.4. ábra

és a fizikai környezetre is. A nemzetközi feltételeket, szabványokat kielégítő infrastruktúrát magyarul is az angol Public Key Infrastructure (Nyilvános Kulcsú Infrastruktúra) kifejezésből származó PKI rövidítés jelöli.

A hozzáférést leginkább jelszóval szabályozzák. Elterjedőben vannak biometriás azonosítók is. A maradék követelmények kielégítésére elsősorban a nyilvános kulcsú kriptográfia módszereit használják. Nem elhanyagolható szempont a kulcskezelés kérdésköre. Megnyugtató módon kell gondoskodni a kulcsok generálásáról, tárolásáról, visszavonásáról, a korrumpálódott kulcsok kezeléséről stb.

11.4.5. Kriptográfiai Protokollok

Figyelj jól!

Az elektronikus hírközlésben egymást nem feltétlenül ismerő felek lépnek egymással kapcsolatba, miközben biztonságosan akarnak üzeneteket váltani. Ehhez egy sor szabványosított eljárást használhatnak, ha tudják, hogy ezeket a szabványokat társuk is tudja használni. Ennek megállapításához a kapcsolat felvételének idején kérdéseket intéznek egymáshoz, információt cserélnek ki. A kérdéseket is lehet szabványosítani annak érdekében, hogy ezeket emberi beavatkozás nélkül,

automatikusan fel lehessen tenni, és meg lehessen válaszolni. Ilyen *szabványgyűjteményeket* protokollnak neveznek. Pontosabban egy protokoll különböző gépeken azonos hálózati rétegben futó társfolyamatok kommunikációját leíró szabályok gyűjteménye.

A kriptográfiai protokoll kriptográfiai algoritmusokból, alapelemekből épül föl, és egy összetett feladatot hajt végre két vagy több résztvevő között. Leggyakrabban hitelesítő és kulcs-csere protokollokat használunk. A gyakorlatban legismertebb komplex protokoll az interneten két gép közötti bizalmasság és hitelesség biztosítására használt *SSL* (az újabb változat neve TLS) *protokoll*. Manapság egyre több helyen alkalmaznak különböző digitális pénzt kezelő protokollokat is (E-cash, Digicash, Micromint), bár ezek némelyike annyira összetett, hogy több részprotokollra bontható. Ezekre a sémaelnevezés is használatos.

Egy szimmetrikus kulcsot használó esetben a protokoll rendkívül egyszerű lehet, míg nyilvános rendszerben – éppen annak nyilvános volta miatt – a protokoll nagyon bonyolulttá válhat.

A protokollok működési elveik alapján, három módon csoportosíthatók:

- *Döntőbírós:*
  Ebben a protokollban három szereplő működik közre, a küldő és a fogadó közötti információcserét egy mindkettőjük által elfogadott döntőbíró hitelesíti. E protokoll hátránya, hogy a gyakorlatban nehezen találni mindkét fél számára elfogadható döntőbírót. A döntőbírós protokoll elektronikus megvalósításának hátrányai a szintén fennálló bizalmi hiány mellett a késleltetés és a nem mérhető költségek.
  A valós életben a döntőbírós protokoll alkalmazására példa a közjegyző igénybevétele.
- *Ítélkező:*
  Ebben a protokollformában a felek közötti kommunikáció döntőbíró nélkül zajlik mindaddig, míg vitás eset nem merül fel. Ekkor a döntőbíró ítélkezik, ítéletét a felek pedig feltétel nélkül elfogadják. A hátrányok hasonlóak, mint az előző esetben, de a problémamentes működés gyorsabb, késleltetés nélkül zajlik.
  A valós életben az ítélkező protokoll alkalmazására példa a bíróságok működése.
- *Önműködő:*
  Ebben a protokollban a protokoll garantálja, hogy ha egyik fél sem csal, akkor nem fordulhat elő vita, illetve ha valamelyik fél csal, akkor a másik azt azonnal észleli és leállíthatja a protokollt. A döntőbíró szerepét egy biztonságos kriptográfiai rendszer látja el.

A kriptográfiai gyakorlatban három jelentős protokollt említhetünk meg:

- Kommunikáció *szimmetrikus* kriptorendszerrel
  E protokoll gyors, egyszerű, de legnagyobb hátránya, hogy a kulcs átküldésére biztonságos csatornát kell biztosítani, valamint a résztvevők számának növekedésénél jóval nagyobb ütemben növekszik a kulcsok száma.

- Kommunikáció *nyilvános kulcsú* kriptorendszerrel
  A kulcsmenedzselés problémája ebben a protokollban megoldott. Az alkalmazott eljárások nyers erőn alapuló visszafejtési időszükséglete jóval nagyobb, viszont a használt algoritmusok jóval lassabban működnek, mint a szimmetrikus kulcsú rendszerekben. Nagyon kritikus eleme a rendszernek a nyilvános kulcsok tárolása és menedzsmentje, mert ha ez nem elég biztonságos, akkor egy megszemélyesítő támadással elfoghatók a másnak szánt üzenetek.
- *Hibrid* kommunikációs protokoll
  Ez a rendszer egyesíti a szimmetrikus rendszer gyorsaságát a nyilvános kulcsú rendszer jó menedzsmentjével és nehezebb visszafejthetőségével.

A korábban említett SSL (TSL) protokoll az ítélkező, hibrid kommunikációs protokollok közé sorolható.

Ide tartoznak még az úgynevezett *zero-knowledge protokollok* (amelyre nem létezik igazán jó magyar elnevezés) is. A résztvevők egyike be akarja bizonyítani a másik félnek, hogy ismer egy információt, és mindezt anélkül, hogy magát az információt felfedné, vagyis a bizonyításnak olyannak kell lennie, hogy abból a másik fél az információ egyetlen bitjét se ismerhesse meg.

11.5. Vírusvédelem

11.5.1. Vírusok, férgek, trójai programok

A ma már nemzetközileg elfogadott terminológiában *vírusnak* egy olyan programot nevezünk, amely képes arra, hogy önmagát reprodukálja, azaz szaporodjon, figyelembe véve mindig változó környezetét.

A *féreg* (worm) némi hasonlóságot mutat a vírusokkal, de nem fertőz meg minden hozzáférhető programot, hanem egyik programból a másikba vándorolnak, azaz nem szaporodnak, mint a vírusok, tehát belőlük mindig csak egy példány létezik. A féreg a fertőzés után eltávolítja magát abból a programból, amelyből fertőzött és az újonnan megfertőzöttben „él" tovább.

A számítógépes *„trójai faló"* egy program, amelynek külső megjelenése, elnevezése hasonlít vagy megegyezik egy közismert vagy fontos programéval, azonban a belső működése eltér, illetve teljesen más, mint az eredeti funkciója.

A vírusfertőzések terjedésében, a férgek vagy a trójai programok bejutásában, nemcsak külső eredetű, ellenőrizhetetlen források játszanak szerepet, hanem igen jelentős mértékben a belső viszonyok, a szervezettség, a szabályozottság, illetve a kezelő és üzemeltető személyzet hozzáértése is hozzájárul.

Jelen fejezetben nem térünk ki a különböző vírusvédelmi eszközökre, hanem „eszközfüggetlen" szervezeti megoldásokat mutatunk be.

11.5.2. A vírusvédelem megvalósítása

Biztonságpolitika

A központosított hálózati felhasználói adminisztráció megvalósítása lehetővé teszi biztonságpolitika, más néven házirend (system policy) alkalmazását. A biztonságpolitika segítségével a hálózatba bejelentkező felhasználók számára előre meghatározott környezet biztosítható. A felhasználó korlátozható abban, hogy milyen hálózati, illetve helyi erőforrásokhoz tud hozzáférni, és hogy milyen beállításokat tud elvégezni a saját rendszerén. A biztonságpolitika külön definiálható az egyes felhasználói csoportokra vagy akár az egyes felhasználókra is, ami lehetővé teszi, hogy rugalmasan, a felhasználók munkakörének megfelelően tudjuk szabályozni a számítógép-használatát.

Vírusvédelmi szabályzat

A vírusvédelemmel kapcsolatos folyamatokat, teendőket és kötelezettségeket írásos dokumentumban kell rögzíteni, amely egyrészt pontosan leírja, hogy kinek mi a teendője, továbbá alapját képezi az esetleges számonkérésnek. A dokumentumnak szabályzaterejűnek kell lennie, ami alapján munkajogi felelősségre vonást lehet érvényesíteni. A vírusvédelmi szabályzatot el kell juttatni minden érintett dolgozónak.

A szabályzatnak tárgyalnia kell az alábbi pontokat:

- Végfelhasználók kötelességei a vírusfertőzések elkerülése érdekében.
- Végfelhasználók kötelességei vírusfertőzés észlelése esetén.
- Vírusfelelősök feladata, hatásköre.
- Vírusfelelősök kötelességei a vírusfertőzések elkerülése érdekében.
- Vírusfelelősök kötelességei vírusfertőzés észlelése esetén.
- Rendszergazdák kötelességei a vírusfertőzések elkerülése érdekében.
- Rendszergazdák kötelességei vírusfertőzés észlelése esetén.
- Vírusellenőrző munkaállomások használati rendje.
- Naplózási rend.
- Ellenőrzések gyakorisága.

Hardvervédelem

A személyi számítógépek hardverkonfigurációjával kapcsolatos specifikációi az úgynevezett BIOS (Basic Input-Output System) beállításokkal változtathatóak. A helyes beállítások alapvetően fontosak a számítógép működése szempontjából, ezért azoknak a felhasználók által való megváltoztatása nem kívánatos. A legtöbb BIOS lehetőséget nyújt a beállítások jelszóval való levédésére, amivel megelőzhető a beállítások jogosulatlan megváltoztatása. A BIOS beállítások között vannak a vírusvédelemmel közvetlenül összefüggő paraméterek is, mint a boot-szekvencia beállítás és a boot-szektor védelem.

Biztonsági mentés

A logikai támadások vagy más okok (műszaki hiba, emberi hanyagság, természeti csapás stb.) miatt adatvesztésre kerülhet sor. Ebben az esetben csak a korábban lementett adatok visszaállításával lehet kiküszöbölni a kárt, ezért minden szervezet számára valamilyen mentési (backup) eljárást kell bevezetni.

Szoftvervédelem

Keresőeszközök:
A vírusok elleni védelem hatékonyabb módszere a vírus-szkenner szoftverek alkalmazása. A szkenner szoftver a már a gépre került vírusok után keres a boot-szektorban, a memóriában és a merevlemezen lévő fájlokban, azokat egyenként megvizsgálva. A vírust egy adatbázis alapján képes azonosítani, ami gyakorlatilag a találati teljesítményét határozza meg. Mivel az adatbázis statikus, ezért idővel elavul, és frissíteni kell, hogy újabb vírusok felismerésére legyen képes. Az ilyen típusú víruskereső szoftverek általában a vírusok eltávolítására, becsomagolására vagy valamilyen más módon való ártalmatlanná tételére is képesek. Az ilyen szoftverekkel már hatásosan lehet védekezni, feltéve, ha megfelelő módon alkalmazzák őket, azaz rendszeresen futtatják és frissítik. A módszer hátránya, hogy csak a már ismert vírusokat tudja detektálni, azokat is csak miután már valamilyen formában fertőztek. Egyes vírusokat nem képesek eltávolítani, vagy valamilyen adatvesztéssel jár az eltávolításuk. Az ellenőrzés nem folyamatos, két víruskereső futtatása közti időszakban a vírus szabadon fertőzhet.

Preventív eszközök:
Mint minden más káros dolog esetében, a vírusokkal szemben is a legjobb védekezés a megelőzés. Ilyen célt szolgálnak a rezidens (a számítógép memóriájába beköltöző) vírusvédelmi szoftverek. Ezek az eszközök a számítógép memóriájába töltődve folyamatosan figyelik, hogy mi történik az adott számítógép működése közben. Minden egyes fájlhozzáférésnél a beolvasás közben az adatbázisuk alapján ellenőrzik, hogy fertőzött-e az állomány. Minden behelyezett flopi boot-szektorát ellenőrzik. Folyamatosan figyelik a gép azon paramétereit, amelyek alapján arra lehet következtetni, hogy vírus próbálkozik bejutni a rendszerbe. A rezidens vírusfigyelő programok képesek a vírustevékenység felismerésére, pusztán bizonyos vírusok viselkedése alapján, ezért nem feltétlenül szükséges, hogy az adott vírus szerepeljen az adatbázisukban. Ugyanakkor a hasznos szoftverek ráutaló magatartása esetén téves riasztást is generálhatnak. A rezidens víruskeresők alkalmazása csak akkor hatékony, ha folyamatosan aktívak a számítógép memóriájában, ami természetesen állandó erőforrás-allokációt igényel, és esetleges teljesítménycsökkenéshez vezethet. A preventív eszközök sem nyújtanak tökéletes védelmet. Több vírus képes *kijátszani* őket, valamint az adatbázis-frissítés az új vírusok adataival ugyanolyan fontos, mint a szkenner megoldások esetében.

Biztonsági szoftverek:
A vírusok elleni védekezésre is alkalmas, de azon bizonyos szempontból túlmutató eszközök a biztonsági szoftverek. A biztonsági szoftver a számítógép egy állapotáról – ami lehet a vírusmentes állapot is – egy *pillanatfelvételt* készít a számítógép merevlemezére, amelyben a fájlok integritási adatait jegyzi fel. Ezekután a biztonsági szoftvernek a gépen rezidensen futó komponense képes letiltani minden, a pillanatfelvételen nem szereplő vagy ahhoz képest megváltozott fájl használatát. Ily módon megakadályozható a nem *hitelesített* és a megváltozott fájlokhoz való hozzáférés – függetlenül a változás okától. Az ilyen eszközökkel megakadályozható a nem megfelelő verziójú, tévedésből felülírt vagy vírusos alkalmazások futtatása. A nagyfokú biztonság elérése érdekében azonban a felhasználónak több, a számítógép használatára vonatkozó jogosultságról le kell mondania. A biztonsági szoftverek által nyújtott bizonyos funkciókat egyes operációs rendszerek (például Windows NT, Windows 2000) magukba integrálják.

Adathordozók kezelése

Egy szervezet sem tudja garantálni, hogy a kívülről érkező adathordozók is vírusmentesek legyenek. Azonban kialakítható olyan belső vírusmentes övezet, amely határvonalain csak megfelelő ellenőrzés után juthat át adathordozó. A kívülről érkező adathordozók ellenőrzésére külön munkaállomások állíthatók fel, amelyek csak erre a célra használatosak. A vírusellenőrző munkaállomásokat a hálózatról le kell választani, továbbá más, üzleti jellegű szoftvereket nem szabad rajtuk üzemeltetni, ezáltal biztosítva azt, hogy vírusos adathordozó esetén még véletlenül se tudjon a fertőzés továbbterjedni. A művelet időigényességére való tekintettel a szervezeten belül használatban lévő adathordozókra nem célszerű minden esetben alkalmazni a vírusellenőrző munkaállomást, az kifejezetten a vírusmentes övezetbe való beléptetésére szolgál.

Felhasználói oktatás

A vírusvédelmi politikában komoly figyelmet kell fordítani a dolgozók megfelelő szintű tájékoztatására. A dolgozói hozzáállás pozitív befolyásolása a megelőző vírusvédelem első frontját jelenti. Ha a dolgozók kellő odafigyelést tanúsítanak a problémával kapcsolatban, akkor nagymértékben csökkenteni lehet a műszaki megoldások hatékonyságától való függést.

A felhasználói oktatás ajánlott tematikája

- Átfogó ismertető a vírusokról
- Vírusok fajtái
- Viselkedésük
- Terjedési módjuk
- Vírusfertőzések elkerülése


Tanuld meg!

- Fertőzések forrásai
- Megelőző védekezés
- Víruskereső szoftverek
- Flopik használata
- Teendők vírus észlelésekor
- A felhasználó kötelezettségei

11.6. Biztonsági kiegészítések


Tanuld meg!

Gyakran felvetődik az informatikai rendszerek tervezése, beszerzése során, hogy a költségek csökkentése érdekében egy olcsóbb operációs rendszert szerezzünk be és egészítsük ki valamilyen biztonsági termékkel. Az ilyen választást az is indokolhatja, ha például mindenképpen minősített termékkel szeretnénk biztosítani a szükséges védelmi szintet, de az elérhető vagy már eleve rendelkezésre álló operációs rendszerek csak egy ilyen speciális kiegészítővel képesek azt biztosítani. Ilyen például a nagy megbízhatóságú Tandem Himalaya rendszeréhez társuló Guardien, ami nélkül nem lehetne elérni a C2 szintet, vagy az IBM s390 biztonsági kiegészítése, a RACF, amellyel az MVS-t kiegészítve a B1 szint is elérhető. Ezek az esetek, amikor a központi erőforrás biztonságát tudjuk növelni, racionális és ésszerű többletköltséget jelenthetnek, ha az adatok biztonsága megköveteli az adott szintű védelmet.

A másik lehetséges eset a biztonsági kiegészítések alkalmazására, amikor a végponti munkahelyek védelmét próbáljuk növelni, úgy hogy a Windows NT-re való áttérés helyett maradnak a végponti Windows 3.1, 95 vagy 98-as PC-k, csak kiegészítik valamilyen eszközzel, ami jelszóhoz köti a bekapcsolást, bejelentkezést, esetleg titkosítja az adatokat. Tekintettel arra, hogy egy nagy felhasználószámú rendszernél ez már jelentős árbeli megtakarítást jelent, első ránézésre racionálisnak tűnhet egy ilyen választás. Azonban egy összetett rendszer nehezebben (drágábban) menedzselhető a bonyolultabb konstrukció és az üzemeltetőktől megkövetelt nagyobb szaktudás miatt, tehát a rendszer teljes költségei már megközelíthetik egy nagyobb beruházási költségű, de homogén rendszerét, ugyanakkor az is kérdéses, nyújt-e legalább megközelítően olyan szintű védelmet, mint az áttérés a Windows NT-re.

Az előző Win95, kontra Windows NT példánál maradva a kiegészítő védelmi eszközöknek akkor lehet racionálisan értelme, ha elkerülhetetlen, hogy a végponti PC-kre értékes, védendő információ kerüljön. A vezetők laptopján lévő adatokat bárki megszerezheti, még akkor is, ha megfelelő azonosítási és hitelesítési mechanizmussal felvértezett Windows NT az operációs rendszere, mert elég csak kivenni a merevlemezt az ellopott laptopból és áttenni egy másik PC-be, máris hozzáférhetők az adatok. Ilyen eset elkerülésére van értelme olyan kiegészítő berendezés

vagy szoftver alkalmazásának, amely a merevlemez tartalmát kódolja, és csak a jogosult által ismert jelszóval válnak hozzáférhetővé az adatok.

Harmadik, speciális esete a „kiegészítő berendezéseknek", amikor cégünk nagy, szinte áttekinthetetlenül bonyolult informatikai rendszerének menedzselésére *központi IT menedzsment* rendszert vezetünk be, amelynek általában biztonsági szempontból is előnyei vannak, de ez egy rendkívül összetett kérdés, amellyel itt nem foglalkozunk.

12. Ellenőrzés, auditálás, kockázatelemzés

12.1. Az informatikai rendszerek biztonsági ellenőrzése

12.1.1. Az informatikai biztonsági ellenőrzés célja

Az informatikai biztonsági ellenőrzések alapvető célja, hogy **objektív információkat** biztosításon a felelős vezetők számára az informatikai biztonság helyzetéről, amelyek alapján a kockázatok csökkenthetők és a rendkívüli események elkerülhetővé válnak.

Az informatikai biztonsági ellenőrzés célja az, hogy teljes körűen, azaz minden informatikai rendszerre és azok teljes életciklusára (az előkészítéstől, a bővítéseken és módosításokon át, a rendszerből történő kivonásig) rendszeresen vizsgálja, hogy:

- az informatikai rendszerek biztonsága megfelel-e a Társaság által elfogadott biztonsági követelményeknek (például MeH ITB 12. sz. ajánlás),
- érvényesülnek-e a jogszabályokban, a társasági és a rendszer szintű biztonságpolitikákban és szabályzatokban foglaltak,
- történnek-e az informatikai rendszerek, illetve az általuk nyújtott szolgáltatások biztonságát sértő események, illetve mekkora ezek bekövetkezési valószínűsége.

Az ellenőrzések során feltárt hiányosságok (a megállapításokat mindig írásos jelentésbe kell foglalni!) képezik azon védelmi intézkedések (adott esetben szankciók) alapját, amelyek szükségesek ahhoz, hogy *minimális legyen a védelmi képességek kívánt és valós szintje közötti távolság, ezért az ellenőrzések során tapasztalt hiányosságok megszüntetésére intézkedési tervet (javaslatot) kell kidolgozni, és azt meg kell valósítani.*

12.1.2. Az informatikai biztonsági ellenőrzések formái

Az ellenőrzésekkel szemben alapvető követelmény, hogy az alkalmazott módszer biztosítsa a tárgyszerűséget, a valósághű képet és a valós helyzet feltárását, ennek megfelelően az ellenőrzések különböző formában valósulnak meg. Az ellenőrzések formáját annak típusa, jellege és szintje határozza meg.

Az informatikai biztonsági ellenőrzések típusai:

- *informatikai biztonsági vizsgálat* (fenyegetettség, védelmiképesség-elemzés kockázatelemzéssel),
- *auditálás* (meghatározott követelményeknek való megfelelés vizsgálata),
- *informatikai biztonsági tanúsítás és minősítés* (például az ITSEC F-C2 osztálya követelményeinek való tanúsított megfelelés).

Az ellenőrzés eszközei:

- személyes ellenőrzés,
- megfigyelés,
- információ bekérés,
- dokumentumok vizsgálata,
- technikai berendezések által rögzített adatok elemzése,
- feladatlap kitöltése,
- folyamatelemzés.

Az ellenőrzések munkaszakaszai:

- előkészítés,
- felkészülés, helyszíni vizsgálat,
- írásba foglalás,
- hasznosítás, javaslatok (realizálás).

Az ellenőrzések jellegük szerint feloszthatók:

- *tervezett és rendszeres ellenőrzésekre,*
- *eseti vizsgálatokra,*
- *biztonságiesemény-kivizsgálásokra.*

12.1.3. Kötelező ellenőrzések

Minden szervezetben célszerű kidolgozni egy tervet, amely a kötelező ellenőrzések gyakoriságát, módszertanát, kiterjedését (a bevonásra kerülő területeket) és az ellenőrzést végző szervezetet meghatározza. Egy ilyen tervre adunk az alábbiakban mintát:

1. Évente legalább egyszer társasági szinten **független auditálást** kell végezni, amelyet független, külső informatikai biztonsági auditor cég végez. Az auditálás terjedjen ki a Számítóközpontban üzemelő központi erőforrásokra és alkalmazásokra, a számítógépes hálózatra és a munkaállomásokra, valamint ezek fizikai és személyi környezetére.
2. Hathavonta rendszerszintű **belső auditálást** kell végezni az üzemelő rendszereknél. Az auditálás terjedjen ki a Számítóközpontban üzemelő központi erőforrásokra és alkalmazásokra, a számítógépes hálózatra, a fizikai és a személyi környezetre.
3. Ha bármely rendszernél a biztonság helyzete indokolttá teszi (például gyakori biztonságsértések, jelentős változás a rendszerben), rendszer szintű független auditálást kell elvégezni.

4. Az új rendszerek fejlesztésének indítása előtt, illetve a már korábban elvégzett vizsgálatoknál kimutatott magas kockázatok ellenőrzése céljából kockázatelemzésen alapuló vizsgálatot kell elvégez(tet)ni.
5. A fejlesztési projektekben belső, indokolt esetben külső auditálást kell végezni.

12.1.4. A szankcionálás

A jogszabályok, illetve a társasági utasítások, szabályzatok megsértése munkaügyi vagy komolyabb esetben büntető jogi felelősségre vonást kell hogy maga után vonjon.

A szabályok megsértését általában a következő események merítik ki:

- minősített adatok szóban történő közlése illetéktelenekkel,
- minősített adatok dokumentumon, adathordozón vagy informatikai rendszeren keresztül, például levelezéssel történő illegális átadása illetékteleneknek,
- minősített adatok jogosulatlan nyilvánosságra hozatala,
- gondatlan közreműködés az informatikai rendszerhez történő illetéktelen hozzáférésben,
- szándékos (bosszúból, anyagi előnyszerzés érdekében stb.) közreműködés az informatikai rendszerhez történő illetéktelen hozzáférésben.

Az informatikai biztonságot sértő események megvalósulása vagy annak alapos gyanúja esetén az illetékes (informatikai vagy biztonsági) vezető utasítása alapján az informatikai biztonsági vezetőnek (menedzsernek) a területileg illetékes vezetők bevonásával haladéktalanul ki kell vizsgálnia.

A vizsgálat során meg kell állapítani, hogy

- milyen események történtek,
- történt-e bűncselekmény,
- az események milyen és mekkora kárt okoztak, illetve okozhattak,
- milyen intézkedések szükségesek a kárelhárításhoz, illetve mérsékléshez,
- mik az események kiváltó okai, előzményei,
- az eseményért kik a közvetlenül és közvetve felelős személyek, és milyen a felelősségük mértéke.

Bűncselekményre utaló gyanú vagy körülmény esetén az arra illetékes szervezeti egységgel (általában a jogi osztály) közösen, haladéktalanul meg kell tenni az illetékes hatóságnál a feljelentést. Bűnügyi eljárás esetén a nyomozó hatósággal együttműködve kell a további vizsgálatot lefolytatni. Amennyiben ilyen esetben konkrét személlyel, mint elkövetővel szemben alapos gyanú merül fel, úgy az illetőt az ügy kivizsgálásának befejezéséig a munkavégzés alól fel kell függeszteni. Az ilyen események szankcionálásának alapját, az esemény értékelésétől függően a Munka Törvénykönyv 103. §. (3) bekezdése, illetve büntetőjogi szintű felelősségre vonásnál a Büntető Törvénykönyv a számítógépes csalásra, valamint az üzleti titok megsértésére vonatkozó részei képezik.

Az illetékes (informatikai vagy biztonsági) vezető a kivizsgálás eredményéről írásban tájékoztatja a szervezet első számú vezetőjét (esetleg – nagy szervezetnél – illetékes helyettesét). A tájékoztatásban tegyen javaslatot:

- a felelősségre vonandó személyekre,
- a felelősségre vonás mértékére,
- a további hasonló károk, biztonságsértések elkerülésére teendő intézkedésekre.

A szervezet első számú vezetője, saját hatáskörében, a szükséges intézkedéseket a tájékoztatás alapján haladéktalanul hozza meg.

A progresszív fegyelmezés egy olyan folyamat, amely fokozódó minőségi jelleget követő büntetésekre épül, amelyeket fegyelmi intézkedéseknek nevezünk. A fegyelmi intézkedések fajtái:

- szóbeli megrovásról,
- írásbeli figyelmeztetésről,
- felfüggesztésről,
- elbocsátásról.

Az informatikai biztonsági vezető (menedzser) a biztonságsértő eseményekről vezessen folyamatos nyilvántartást, amelyből megállapítható, hogy mikor milyen események történtek, arra hogyan derült fény, mekkora kárt okozott, kik voltak a felelősök, milyen intézkedések történtek az esemény kapcsán.

12.2. Az informatikai biztonság ellenőrzési folyamata

12.2.1. Informatikai biztonsági vizsgálat – kockázatelemzés

Az informatikai biztonsági vizsgálat olyan elemző és értékelő jellegű szakértői vizsgálat, amelynek fő célkitűzése a kezelt adatok és alkalmazások biztonságának elemzése. Ennek során a védelmi célokkal, a teljes rendszer biztonsága kerül feltérképezésre, mellyel – lehetőleg kockázatelemzés után – az elviselhetetlen kockázatot jelentő fenyegetések kerülnek kimutatásra. A vizsgálattal kockázatkezelési és intézkedési javaslatok is készülhetnek. A vizsgálatot végezhetik belső ellenőrök vagy külső szakértők, illetve akkreditált auditorok. Az informatikai biztonság átfogó, a szervezet egészére, ágazataira, igazgatóságaira, számító- vagy szolgáltató központjaira, az informatikai stratégiában meghatározott rendszereire és alkalmazásaira kiterjedő ellenőrzése során a szervezet által elfogadott kockázatelemzésen alapuló módszertant kell felhasználni, például a MeH ITB 8. számú ajánlását, az Informatikai Biztonsági Módszertani Kézikönyvet. (A következő részek is e szerint a módszertan szerint készültek.)

Valamely informatikai rendszer biztonságának kockázatelemzésen alapuló vizsgálata során elsőként a meglévő, potenciálisan fenyegetett értékeket kell feltérké-

pezni és újraértékelni. Ehhez meg kell határozni a felhasználó biztonsági követelményeit, amelyek teljesülése ahhoz szükséges, hogy lehetővé váljon a védelmi célkitűzéseknek megfelelő rendeltetésszerű felhasználás.

Ezután azokat a várható következményeket kell feltárni, amelyek akkor alakulhatnak ki, ha ezek a követelmények (védelmi célok) az alapfenyegetettségeket illetően nem teljesülnek.

A fenyegető tényezők, illetve veszélyek az informatikai rendszerelemekhez kapcsolódnak és azokon keresztül okozhatnak károkat mind a kezelt adatra, mind az alkalmazásra, miután az informatikaalkalmazás függ a rendszerelemektől. Éppen ezért valamennyi olyan rendszerelemet vizsgálni kell, amelyektől az informatikai rendszer működése és valamilyen módon az alkalmazásai függnek, és amelyeket valamely fenyegető tényező vagy veszélyforrás közvetett, illetve közvetlen módon érinthet.

Ehhez a következő meglévő rendszerelemcsoportokat kell áttekinteni:

Tárgyiasult elemcsoportok:

- környezeti infrastruktúra,
- hardver,
- adathordozók,
- dokumentumok, iratok.

Logikai elemcsoportok:

- szoftver,
- adatok,
- kommunikáció.

Személyi elemcsoport:

- személyzet,
- felhasználók,
- ellenőrök.

A rendszerelemekhez rendelve egyedileg meg kell határozni a fenyegető tényezőket, amelyek a vizsgált környezetben egyáltalán felléphetnek.

Miután nem védekezhetünk tökéletesen valamennyi fenyegető tényező (veszélyforrás) ellen, meg kell ismerni a legfontosabbakat. Ehhez valamennyi feltárt fenyegető tényezőt értékelni kell. Az értékelés függ a kár bekövetkezésének várható **valószínűségétől** és a bekövetkezett **kár nagyságától,** amennyiben a fenyegető tényező kifejtheti hatását. Ebből a két részből tevődik össze a ***kockázat.***

A bekövetkezés valószínűsége például olyan eseményeknél, amelyeket emberek célzottan idéznek elő, a potenciális tettesek felkutatásával és azok számának megadásával becsülhető meg, akik a megfelelő lehetőségekkel és ismeretekkel rendelkeznek. Az olyan események gyakoriságát pedig, melyek műszaki hibák vagy „vis maior" esetén lépnek fel, statisztikák, megbízható működési adatok és saját tapasztalatok összegzésével lehet megbecsülni. Ugyanez érvényes a személyek gondatlan vagy hibás tevékenysége miatt bekövetkező károk gyakoriságának becslésére.

A kárnagyság előzetes értékelésekor mérlegelni kell, hogy egy adott fenyegető tényező hatására milyen anyagi és más természetű veszteség (kár) következik be, melyek a közvetlen károk, és ennek hatására milyen későbbi következménnyel, úgynevezett következményes kárral kell még számolni.

A kockázatelemzésből biztonsági igény adódik, amennyiben minden kockázatot megvizsgálunk, *és megállapítjuk, hogy egy vagy több kockázat nem elviselhető.*

A ***biztonsági követelmények*** egyenként abból adódnak, hogy kiválasztjuk a túl magas kockázatokat, és ezek alapján meghatározzuk azokat a megfelelő intézkedéseket, amelyek ezeket a kockázatokat elfogadható szintre csökkentik, és a költségek, illetve a haszon szempontjából is igazolhatók.

Az általános biztonsági stratégiából vezethető le az ***elviselhető kockázatok*** mértéke, illetve a tervezett intézkedések elfogadhatósága.

Az informatikai rendszerekre és környezetükre ható fenyegetések által okozott kockázatok felmérése és minősítése után olyan **védelmi intézkedésekre** kell javaslatot tenni, amelyek minimális költségszint mellett maximális kockázatcsökkentést eredményeznek. Az informatikai biztonsági vizsgálat négy eljárási szakaszra, azon belül pedig 13 lépésre bontható.

Az egyes lépéseket szükség szerint meg kell ismételni.

A **5.10.** ábra az informatikai alkalmazásokra mutatja be az eljárást a szakaszok és lépések összetartozásának feltüntetésével.

12.2.1.1. I. szakasz: a védelmi igény feltárása

A szakasz áttekintése

Az **első szakaszban** kell választani és be kell határolni a további vizsgálódások tárgyát. Ehhez meg kell állapítani, hogy értékük alapján mely informatikaalkalmazások szorulnak védelemre.

Az első szakasz gyakorlatilag az informatikai stratégiai tervezés „hol vagyunk" kérdésére ad választ. Célszerű összehangolni, illetve közösen végrehajtani ezt a szakaszt az informatikai stratégiai tervezés projektjének alárendelve.

E szakaszban valamennyi adat- és informatika-alkalmazás közül ki kell választani azokat, amelyek az adott szervezet számára jelentőséggel bírnak, így védelmet igényelnek. Ehhez az alkalmazónak kell megállapítania, milyen védelmi célokat tűz maga elé az öt alapfenyegetettség vonatkozásában.

A védelmi igény megállapítása két lépésben történik:

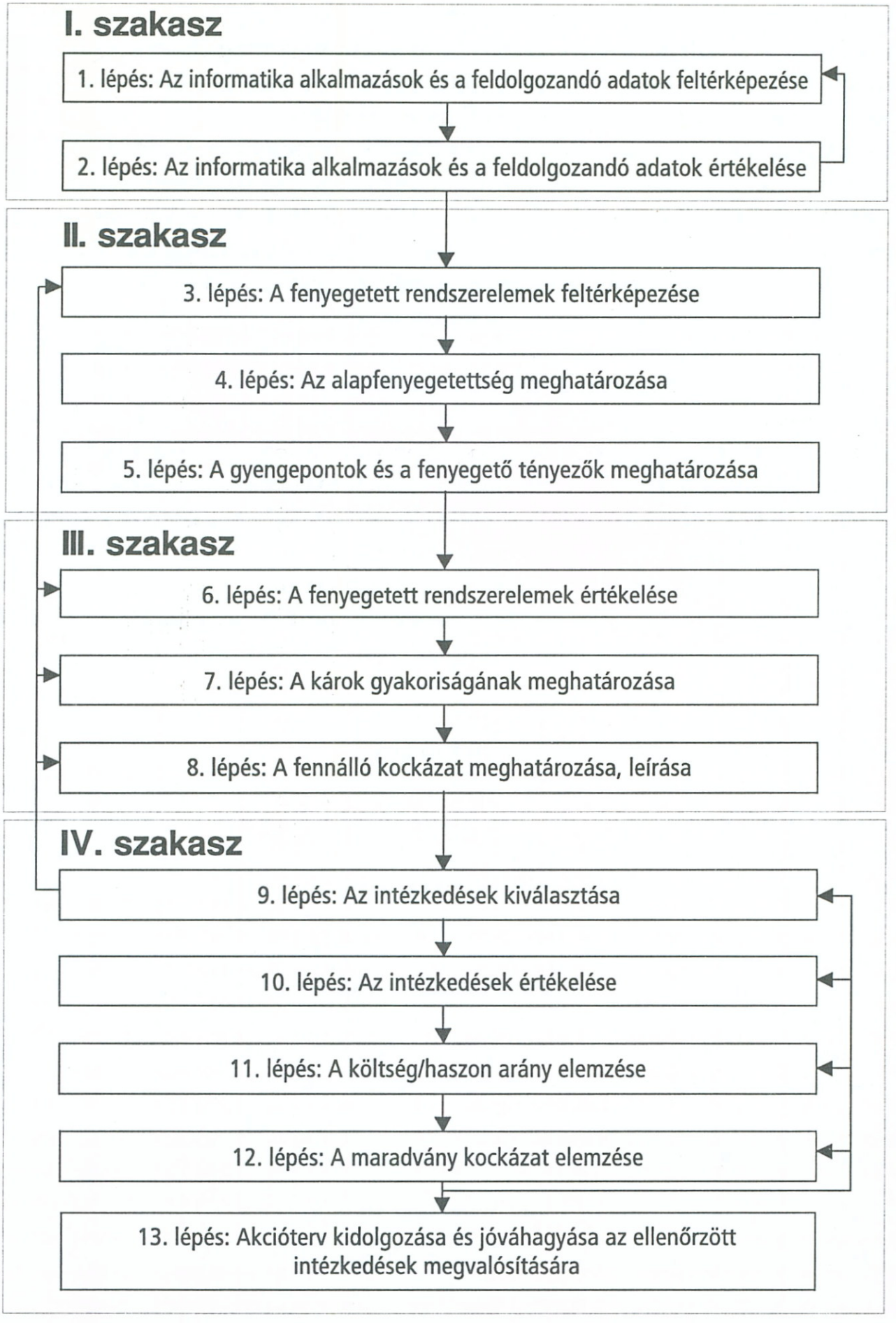
Első lépés: az informatikaalkalmazások és a feldolgozandó adatok feltérképezése:

1. feladat: Az informatikaalkalmazások feltérképezése;

2. feladat: Igény esetén a különleges szolgáltatások feltérképezése;

3. feladat: Az informatikai rendszerben feldolgozásra kerülő valamennyi adat feltérképezése.


Figyelj jól!


I. szakasz
1. lépés: Az informatika alkalmazások és a feldolgozandó adatok feltérképezése
2. lépés: Az informatika alkalmazások és a feldolgozandó adatok értékelése
II. szakasz
3. lépés: A fenyegetett rendszerelemek feltérképezése
4. lépés: Az alapfenyegetettség meghatározása
5. lépés: A gyengepontok és a fenyegető tényezők meghatározása
III. szakasz
6. lépés: A fenyegetett rendszerelemek értékelése
7. lépés: A károk gyakoriságának meghatározása
8. lépés: A fennálló kockázat meghatározása, leírása
IV. szakasz
9. lépés: Az intézkedések kiválasztása
10. lépés: Az intézkedések értékelése
11. lépés: A költség/haszon arány elemzése
12. lépés: A maradvány kockázat elemzése
13. lépés: Akcióterv kidolgozása és jóváhagyása az ellenőrzött intézkedések megvalósítására

12.1. ábra

Második lépés: az informatikaalkalmazások és a feldolgozandó adatok értékelése:

1. feladat: A felhasználó védelmi céljainak leírása;

2. feladat: Az ötrészes értékskála rögzítése;

3. feladat: Az értékek hozzárendelése az informatikaalkalmazásokhoz és az adatkörökhöz.

Előzmények:

- a szervezet informatikai stratégiája,
- a szervezet biztonsági stratégiája, szabályzata.

A szakasz eredménye:

- az alkalmazó védelmi céljainak leírása,
- a skálaértékek speciális jelentésének leírása a különböző károkra vonatkozóan,
- az informatikaalkalmazások, szolgáltatások és információk listája hozzárendelt skálaértékekkel az öt alapfenyegetettség vonatkozásában.

Kapcsolódási pontok

A feltérképezés és az értékelés e szinten tisztán üzemeltetői vagy másképpen felhasználó-specifikus célból történik, nevezetesen az informatikai szolgáltatásokat felhasználó szemszögéből. Ennek során az informatikai mérlegelések semmiféle szerepet nem játszanak. Ezek a szempontok csak a fenyegetettség- és a kockázatelemzés során lépnek be. A pótlólagos intézkedések kiválasztását nem vesszük figyelembe ennek a szakasznak a tárgyalása során.

Ez a munkafázis, részben vagy egészben, a biztonsági projektek kijelölésével együtt az informatikai stratégiai tervezés fázisában elvégezhető, a stratégiai tervezési folyamat kereteitől függő részletességgel.

A szakasz lebonyolítása

Elsőként durva megközelítésben be kell határolni és fel kell tárni valamennyi, az informatikai rendszerben kezelt adatot és valamennyi informatikaalkalmazást. A teljességre különös súlyt kell fektetni, mert az a további lépések során már nem biztosítható. Egy kezdeti durva osztályozás megkönnyíti az áttekintést.

A második lépés megvalósítása során a felosztás elvileg még finomítható, nevezetesen a különböző értékű területek egymástól elválaszthatók és elkülönítve szerepeltethetők. A kockázatelemzés befejezése, lezárása után egy további, még finomabb megkülönböztetés válhat szükségessé.

Az informatikaalkalmazások értékét egy ötrészes skálán ábrázolhatjuk, mérhetjük fel, amelyek értéktartományát a felhasználónak kell megállapítania. Ezek segítségével lehet azután a károkat durván osztályozni. Az informatikaalkalmazások és adatok értékeléséhez nincs valamiféle egyszerű, általánosan érvényes koncepció. Az értékeket csak maga az alkalmazó állapíthatja meg. Az érté-

kelés során mindenekelőtt saját biztonsági adottságait és követelményeit kell figyelembe venni.

Ha az informatikaalkalmazások és adatok értéke – a második lépésben – kimagaslóan nagy bizonytalansági tényezőkkel terhelt, meg kell ismételni az értékelést.

A feladat megoldásához szükséges döntéseket a szervezet felső-, illetve informatikai vezetése szintjén kell meghozni. A döntések előkészítésében, a szükséges elemzések elvégzésében biztonsági szakértői támogatás válhat szükségessé. Az együttműködés során az informatikai biztonsági szakértőktől származó ismeretek az alapértékek és értelmezésük, az adatok és a feldolgozási folyamatok leírásának módja, míg az informatikai szakemberektől származó ismeretek a védendő adatok és szolgáltatások, valamint azokhoz értékek rendelése.

Az értékelés során meghatározható, sőt meghatározandó, milyen célból és milyen mértékben ésszerű és szükséges egy fenyegetettség- és kockázatelemzés. Ez a CRAMM módszertana szerint szűkített elemzést jelent. Akkor van ennek jelentősége, ha az informatikaalkalmazások csekély értéket képviselnek a szervezet egyéb működéséhez viszonyítva. A nagy értékű informatikaalkalmazások és adatok pontos, mindent feltáró módon keresztülvitt fenyegetettség- és kockázatanalízist követelnek. Az első lépések eredményeitől függően határozhatók meg a további lépések végrehajtásának ráfordításai.

Az első szakasz lezárása során a szakasz eredményeit a résztvevőknek és a felelősöknek ellenőrizni kell, akiknek ítéletet (véleményt) kell alkotniuk.

A különböző informatikaalkalmazások eredményeinek összehasonlíthatósága érdekében szükséges az összműködésért felelősök (vezető munkatársak, a cégvezetés, az igazgatási szerv vezetése, hatósági vezetés, intézményigazgatók, döntőbizottság, projektvezetés) bevonása.

Csak akkor szabad elkezdeni a II. szakaszt, amennyiben a fenti eredményeket már elfogadták projektvezetési szinten.

12.2.1.2. II. szakasz: fenyegetettségelemzés

A szakasz áttekintése

*A **második szakaszban** kell feltárni mindazon fenyegető tényezőket, amelyek az első szakaszban kiválasztott informatikaalkalmazásokra veszélyesek lehetnek.*

Ennek során vizsgálni kell az informatikai rendszer úgynevezett gyenge pontjait. Itt kerül vizsgálatra a törvényeknek és más szabályozóknak való megfelelés, és értékelésre kerülnek a működésre vonatkozó jegyzőkönyvek, „audit" és „log" fájlok.

A fenyegetettségelemzés során fel kell tárni valamennyi elképzelhető fenyegető tényezőt, amelyek kárt okozhatnak az informatikai rendszerben, s ezzel az informatika-alkalmazásban vagy az adatokban. Különösen ügyelni kell arra, hogy egyetlen fontosabb fenyegető tényezőt se hagyjunk ki, miután a kockázatelemzés ennek eredményeire épül, és a teljeskörűség hiánya a biztonsági koncepció súlyos hiányához vezethet.

A fenyegetettségelemzés a következő három lépésből és annak feladataiból áll:

Harmadik lépés: A fenyegetett rendszerelemek feltérképezése:

1. feladat: A rendszerelemek feltérképezése;

2. feladat: A rendszerelemek kölcsönös függőségeinek leírása.

Negyedik lépés: Az alapfenyegetettségek meghatározása:

1. feladat: Az alapfenyegetettségek és a rendszerelemek összerendelése;

2. feladat: Az összerendelések dokumentálása.

Ötödik lépés: A fenyegető tényezők meghatározása:

1. feladat: Az informatikai rendszer gyenge pontjainak feltérképezése;

2. feladat: A fenyegető tényezők meghatározása.

Előzmény:

- a szervezet összbiztonsági stratégiája.

A szakasz eredményei:

- a rendszerelemek listája az alapfenyegetettségek megadásával,
- az informatikaalkalmazások és adatok más rendszerelemektől való függőségeinek leírása,
- rendszerelemenként a gyenge pontok leírása,
- az érvényes védelmi intézkedések leírása,
- az érvényes védelmi intézkedések kölcsönhatásainak leírása,
- a releváns fenyegető tényezők listája,
- a releváns fenyegető tényezők hozzárendelése a rendszerelemekhez és az alapfenyegetésekhez.

Kapcsolódási pontok

Az I. szakasz eredményeire építve feltérképezik azokat a rendszerelemeket, amelyektől az informatikaalkalmazások és az információfeldolgozás megvalósítása függ, és amelyekre a fenyegető tényezők hatással lehetnek. Itt csupán kiválasztják a rendszerelemeket és a fenyegető tényezőket, de még nem kerül sor a fenyegető tényezők és a rendszerelemek értékelésére (ez már a kockázatelemzés).

A szakasz lebonyolítása

A fenyegetettségelemzés során az azt végzők meghatározzák a finomságnak azt a fokát, amellyel az objektumokat és a fenyegető tényezőket vizsgálni kell. Ebből következik, hogy milyen számú rendszerelemet és fenyegető tényezőt kell értékelni, és ez utóbbiak közül melyek ellen kell intézkedéseket tenni. A feltárt, feltérképezett rendszerelemek és fenyegető tényezők száma nagymértékben befolyásolja, hogy milyen költséges a további lépések megvalósítása. Amennyiben a vizsgálatra szánt ráfordítás csekély, akkor a rendszerelemek és a fenyegető tényezők csak durva megközelítéssel térképezhetők fel. Nagyobb ráfordítást feltételez, ha a rend-

szerelemeket és a fenyegető tényezőket részletesebben kívánjuk feltérképezni. Ez a ráfordítás azonban elkerülhetetlen, ha nagy értékekről van szó vagy különleges veszélyhelyzetek is feltételezhetők.

A rendszerelemek és fenyegető tényezők standard listáját igény szerint rövidíthetjük vagy bővíthetjük, illetve finomíthatjuk.

Figyelnünk kell arra, hogy a rendszerelemek és a fenyegető tényezők listája szinkronban legyen, azaz a rendszerelemeket és a fenyegető tényezőket azonos részletezettséggel kell vizsgálnunk. Ésszerű egyes rendszerelemeket részeire felosztani, ha a fenyegető tényezők csak ezekre a pontosan meghatározható részekre hatnak. Ezért a szakasz három lépését (a harmadik, negyedik és ötödik lépést) általában többször kell elvégezni, hogy a kívánatos összhang elérhető legyen a rendszerelemek és a fenyegető tényezők részletezettségében.

A második szakasz lezárása során az eredményeket a résztvevőknek és a felelősöknek együttesen kell felülvizsgálni és megítélni. A kockázatelemzés (a harmadik szakasz) csakis akkor kezdhető el, ha a második szakasz eredményeit már minden érdekelt elfogadta.

12.2.1.3. III. szakasz: kockázatelemzés

A szakasz áttekintése

*A **harmadik szakaszban** azt kell értékelni, milyen káros hatása lehet a fenyegető tényezőknek az informatikai rendszerre, azaz mely kockázatok állnak fenn.*

A kockázatelemzés során a feltárt fenyegető tényezőket lehetséges kihatásaik szempontjából értékelik, s ebből vezetik le a fennálló kockázatokat. Ez jelenti az adott informatikai rendszer „hol vagyunk" állapotát, amelyből kiindulva kell meghatározni a „hova igyekszünk" állapotot.

A kockázatelemzés a következő három lépésből áll:

Hatodik lépés: A fenyegetett rendszerelemek értékelése:

1. feladat: Az értékek átvitele a rendszerelemekre;

2. feladat: A károk áttekintő ábrázolása.

Hetedik lépés: A károk gyakoriságának meghatározása:

1. feladat: Az ötrészes gyakorisági skála rögzítése;

2. feladat: A gyakorisági értékek hozzárendelése a fenyegető tényezőkhöz.

Nyolcadik lépés: A fennálló kockázatok meghatározása és leírása:

1. feladat: Valamennyi kárérték összeállítása egy áttekintésben;

2. feladat: Az elviselhető és az elviselhetetlen kockázatok rögzítése;

3. feladat: Az elviselhető és az elviselhetetlen kockázatok megjelölése az áttekintésben.

Előzmény:

➠ a II. szakaszban rögzített eredmények.

A szakasz eredményei:

- a gyakorisági skálaértékek jelentésének leírása,
- a rendszerelemek és a fenyegető tényezők listája
  - kárnagyságértékekkel,
  - gyakorisági értékekkel és
  - a kockázatok megjelölésével,
- kockázatáttekintés,
- kockázati mátrix.

Kapcsolódási pontok

Azokat a rendszerelemeket és fenyegető tényezőket értékelik, amelyeket a második szakaszban határoztak meg. Ezáltal kapjuk meg a „hol vagyunk" állapot leírását, amely megkönnyíti a kiegészítő ellenintézkedések kiválasztását. Ez a választás és ezen intézkedések megalapozása azután a negyedik szakasz tárgya.

A szakasz lebonyolítása

A kockázat feltárásához nem létezik valamiféle egyszerű, általánosan érvényes koncepció. A kockázat részét képező „lehetséges kárnagyságot" csak maga az alkalmazó értékelheti. A „bekövetkezési gyakoriságot" pedig megfelelő szakszemélyzet becsülheti meg. Az értékelés során döntően esnek latba a második, a harmadik és az ötödik lépés eredményei. A felhasználó szükséges gondolkodását az egyes lépéseknél megjegyzésekkel, utalásokkal és példákkal támogatja a kézikönyv.

A fenyegetett rendszerelemek értékét ötrészes skálán rögzítik, amely a második lépésben szerepel. A gyakoriságok értékeit egy másik ötrészes skálához rendelik hozzá, amelynek jelentőséget azonban csak a felhasználó, az alkalmazó adhat és kell hogy adjon.

Ha valamely kockázati rész – hatodik és hetedik lépésben szereplő – becslése kimagaslóan nagy bizonytalansági tényezővel terhelt, azt jelölni kell. Általában a „ritka" események gyakorisága, mint például az informatikarendszer külső tényezők általi megtámadásáé (például terrorcselekmények), nehezen becsülhető.

A harmadik szakasz lezárása során a szakasz eredményeit, kiemelten a kárnagyság, a kárgyakoriság értékeit és a kockázatok leírását a résztvevőkkel, a felelősökkel és a vezetőkkel felül kell vizsgáltatni, és véleményt kell mondatni velük ezekről.

Csak amennyiben már elfogadottnak tekinthetők az eredmények, lehet rátérni a munka következő szakaszára, a biztonsági koncepció elkészítésére.

12.2.1.4. IV. szakasz: kockázatmenedzselés

A szakasz áttekintése

A negyedik szakaszban kell kiválasztani a fenyegető tényezők elleni intézkedéseket, és kell értékelni azok hatásait.

Az informatikai rendszert megfelelő és elfogadható intézkedések révén úgy kell kialakítani, hogy a maradványkockázat elfogadható legyen.

Az informatikai biztonsági intézkedések összeállítását és értékelését a következő négy lépésben kell elkészíteni:

Kilencedik lépés: Az intézkedések kiválasztása:

1. feladat: Az elviselhetetlen kockázatok összeállítása;

2. feladat: Az intézkedések kiválasztása.

Tizedik lépés: Az intézkedések értékelése:

1. feladat: Az intézkedésekkel leküzdött valamennyi fenyegető tényező feltérképezése;

2. feladat: Az intézkedések kölcsönhatásának leírása;

3. feladat: Az üzemmenetre való kihatások vizsgálata;

4. feladat: Vizsgálat az előírásokkal való egyezésre vonatkozóan;

5. feladat: Az intézkedések hatékonyságának értékelése.

Tizenegyedik lépés: A költség-haszon arány elemzése:

1. feladat: Az intézkedések költségeinek megállapítása;

2. feladat: Az elfogadhatóság vizsgálata.

Tizenkettedik lépés: A maradványkockázat elemzése:

1. feladat: A hatékonysági értékek bedolgozása a kockázatáttekintésbe;

2. feladat: A maradványkockázat elemzése.

Tizenharmadik lépés: Akcióterv kidolgozása.

A szakasz eredményei:

Egy olyan informatikai biztonsági koncepció, amelyben rögzítve van:

- az informatikai biztonsági stratégia, azaz a célok, az alapelvek és a felelősségi viszonyok,
- az eddigi „hol vagyunk?" állapot (a fenyegetettség- és kockázatelemzés eredménye),
- új intézkedések kiválasztása (a kilencedik lépés eredménye),
- az intézkedések kölcsönhatásai (a tizedik lépés eredménye),
- az intézkedések kihatásai a szervezeti működésre,
- az intézkedések elfogadhatóságának alapjai (a tizenegyedik lépés eredménye),
- a kockázatok „hova igyekszünk?" állapota (a tizenkettedik lépés eredménye),
- alapkövetkeztetések, amennyiben a fenyegető tényezőket nem tudjuk intézkedésekkel lefedni,
- a maradványkockázat elviselhetőségének alapjai.

Kapcsolódási pontok

Miután a fenyegetettségelemzés és a kockázatelemzés megállapította a „hol vagyunk?" állapotot és rögzítette a „hova igyekszünk?" állapotot, a „hol vagyunk?"

állapotot a fenyegető tényezők elleni intézkedések révén átvezetjük a „hova igyekszünk?" állapotba.

A szakasz lebonyolítása

Az intézkedések kiválasztásával általában új rendszerelemek keletkeznek, amelyeket védeni kell. A rendszerelemekre vonatkozóan a fenyegetettség- és kockázatelemzést utólagosan végre kell hajtani.

A tizedik lépésben az intézkedések hatékonyságát értékeljük. Ennek során – akárcsak a második és hetedik lépésekben – nem adott egy egyszerű általános eljárás. Ez a lépés a kiválasztott intézkedések területén szerzett tudást és tapasztalatot feltételezi. Különösen vonatkozik ez annak megítélésére, hogyan hatnak egymásra az intézkedések, milyenek a kölcsönhatásaik.

A negyedik szakasz lezárása során az informatikai biztonsági koncepciót a kidolgozásában részt vevők, felelősök körében be kell mutatni, felül kell vizsgálni, arról határozni kell, és a következő pontokkal ki kell egészíteni:

- az intézkedések prioritási sorrendje,
- a személyes felelősség az intézkedések
  - kiadásáért,
  - megvalósításáért és
  - felügyeletéért,
- időrendi terv az intézkedések megvalósítására,
- utalások az intézkedések betartásának felülvizsgálatára és
- az informatikai biztonsági koncepció felülvizsgálata időpontjának meghatározása.

Csak amennyiben elértük az informatikai biztonsági koncepció elfogadását, kezdhetünk bele annak végrehajtásába. Az informatikai biztonsági koncepciónak független átvizsgálása – például külső tanácsadók által – ajánlatos az alábbi szempontok szerint:

- nem feltárt releváns fenyegető tényezők,
- hamisan értékelt fenyegető tényezők,
- hamisan értékelt intézkedések stb.

Az informatikai biztonsági vizsgálati dokumentum tartalmi felépítése

Az informatikai biztonsági vizsgálat során készülő jelentés javasolt tartalma:

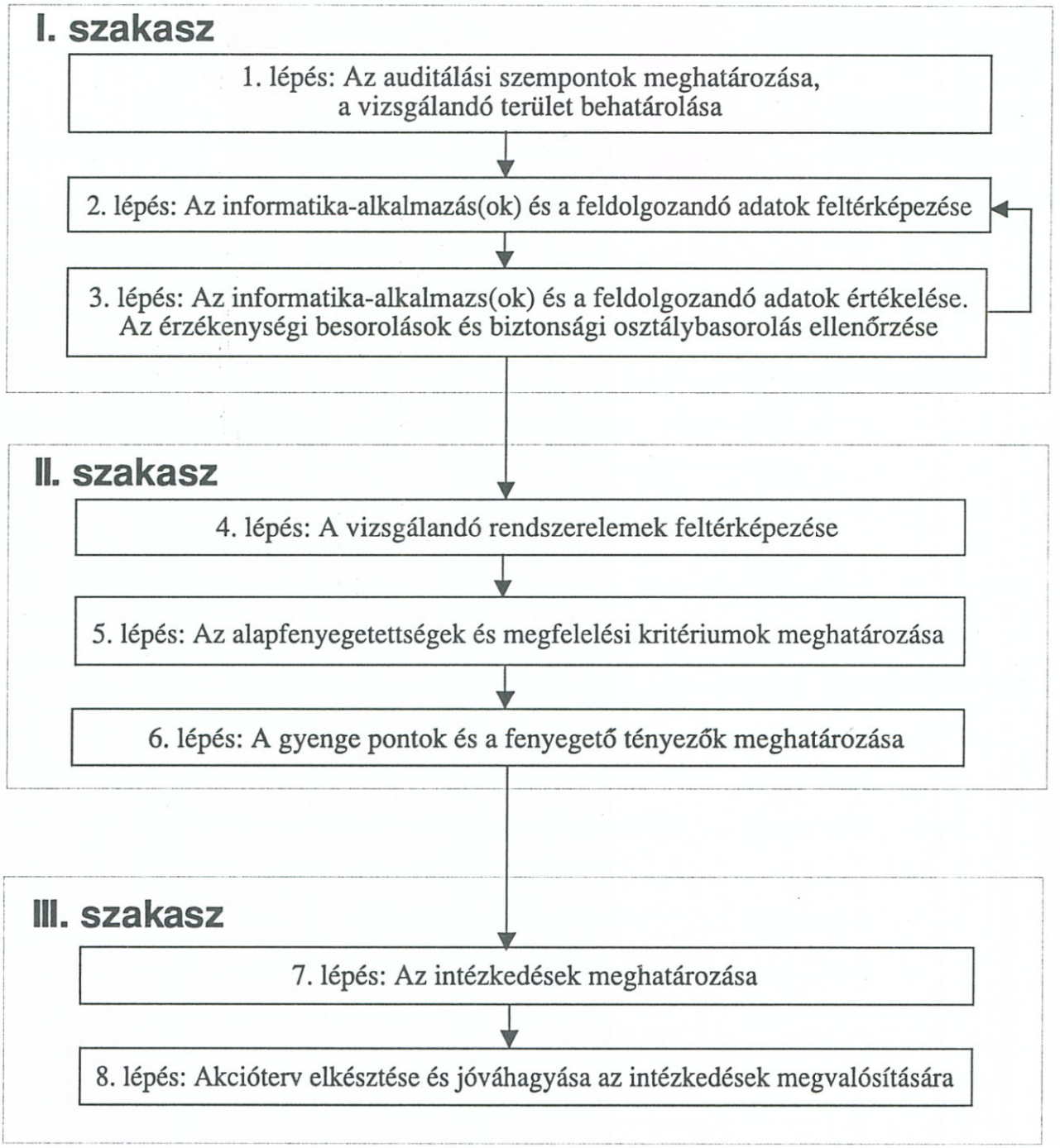
1. BEVEZETÉS
   - 1.1. A vizsgálat célja
   - 1.2. Módszertan, tartalom, a vizsgálat határai
   - 1.3. A vizsgálat ütemezése
   - 1.4. A vizsgálat körülményei
     - 1.4.1. A helyzetfeltáráshoz használt eljárások
     - 1.4.2. Az informatikai biztonsági vizsgálathoz rendelkezésre bocsátott dokumentumok
     - 1.4.3. Az informatikai biztonsági vizsgálat során figyelembe vett fontosabb jogszabályok, szabványok és ajánlások
   - 1.5. Résztvevők (vizsgált szervezeti egységek)
2. A VÉDELMI IGÉNYEK FELTÁRÁSA
   - 2.1. A szervezet bemutatása
     - 2.1.1. A szervezet rendeltetése, funkciói
     - 2.1.2. A szervezet funkcionális folyamatai és szervezete
     - 2.1.3. A szervezet kapcsolatrendszere
   - 2.2 Az informatikai rendszerekben kezelt főbb adatkörök
   - 2.3 A védelmi igények
     - 2.3.1. A védelmi célok feltérképezése, a védelmi igények meghatározása
     - 2.3.2. A károk értékskálájának rögzítése
     - 2.3.3. A kárértékek hozzárendelése az informatikai rendszerben kezelt adatokhoz
3. FENYEGETETTSÉG-ELEMZÉS
   - 3.1. A fenyegetett rendszerelemek feltárása
     - 3.1.1. A rendszerelemek feltérképezése
       - 3.1.1.1. A környezeti infrastruktúra elemcsoport
       - 3.1.1.2. A hardver elemcsoport
       - 3.1.1.3. A szoftver elemcsoport
       - 3.1.1.4. Az adathordozó elemcsoport
       - 3.1.1.5. A dokumentáció és dokumentum elemcsoport
       - 3.1.1.6. Az adatok elemcsoport
       - 3.1.1.7. A kommunikáció elemcsoport
       - 3.1.1.8. A személyek elemcsoport

3.2. A fenyegető tényezők meghatározása
3.2.1. A rendszerelemek gyenge pontjai
3.2.2. Fenyegető tényezők
4. KOCKÁZATELEMZÉS
4.1. A kárértékek átvitele a rendszerelemekre
4.2. A fenyegetések által okozott károk gyakoriságának meghatározása
4.3. A fennálló kockázatok értékelése
4.3.1. Az elviselhető és a nem elviselhető mértékű kockázatok rögzítése
4.3.2. A kockázatok meghatározása és minősítése
5. KOCKÁZAT-KEZELÉS
5.1. A nem elviselhető kockázatok
5.2. Az informatikai biztonsági intézkedések kidolgozásának szempontjai
5.3. A szervezet egészét érintő, globális intézkedési javaslatok
5.3.1. Általános helyzetkép
5.3.2. Az informatikai biztonság szabályozási hátterének értékelése
5.3.3. Hosszú- és középtávú feladatok
5.3.4. Operatív feladatok
5.3.4.1. Globális védelmi intézkedések az informatikai fejlesztés területén
5.3.4.2. Globális védelmi intézkedések az informatikai üzemeltetés területén
5.3.5. Az informatikai biztonság ellenőrzése
5.3.6. Az informatikai biztonság szervezeti vonatkozásai
5.4. Intézkedési javaslatok a kockázatok értékelése alapján
5.4.1. Általános jellegű biztonsági intézkedések
5.4.2. Biztonsági intézkedések a környezeti infrastruktúra védelmében
5.4.3. Biztonsági intézkedések a hardver védelmében
5.4.4. Biztonsági intézkedések az adathordozók védelmében
5.4.5. Biztonsági intézkedések a dokumentumok védelmében
5.4.6. Biztonsági intézkedések a szoftver védelmében
5.4.7. Biztonsági intézkedések az adatok védelmében
5.4.8. Biztonsági intézkedések a kommunikáció védelmében
5.4.9. Biztonsági intézkedések a személyek védelmében
5.5. Akcióterv és költségbecslés a javasolt intézkedésekre
6. ÖSSZEFOGLALÓ
MELLÉKLETEK

12.2.2. Az informatikai biztonság auditálása

Tanuld meg!

Az informatikai biztonság auditálása során **engedélyezett, elfogulatlan és független** külső vagy belső **auditor** a lefolytatott vizsgálat alapján nyilatkozik, hogy a vizsgált rendszer adott követelményeknek (meghatározott biztonsági szintnek, előírásoknak) megfelel (vagy nem felel meg). Az informatikai biztonsági auditálások során a hatályos jogszabályok, a biztonságpolitika, illetve az az alapján készült társasági szabályozások, követelmények, érvényre jutását kell alapul venni, és az



12.2. ábra

ezeknek való megfelelést vizsgálni. Ez adott esetekben kiegészülhet további követelményekkel, speciális feladatokkal.

Az informatikai biztonsági auditálás során (**12.2.** ábra) lényegében a vizsgálat lépéseit kell alapul venni, azzal az eltéréssel, hogy a fenyegetettségeket a szabályzatok, előírások teljesítettsége alapján vizsgáljuk (II. szakasz), vagyis a kockázatelemzés elmarad, viszont hangsúlyozottan történik az egyes szabályzóknak való megfelelés, illetve eltérés leírása.

Az előkészítés és a fejlesztés időszakában a kiválasztott fejlesztési módszertan szerint meghatározott fázisokban *tervezett auditálással* kell meggyőződni arról, hogy

- megvalósultak-e az *informatikai biztonságpolitikában* foglaltak a következő szempontok szerint:
  - megvalósult-e a megvalósítandó informatikai rendszer által kezelt adatok minősítése,
  - ezek alapján megtörtént-e a megvalósítandó informatikai rendszer biztonsági osztályba sorolása,
  - megtörtént-e az informatikai rendszer és környezete fizikai, logikai és adminisztratív védelmi rendszereinek tervezése és megvalósítása a fejlesztési projekt szerves részeként,
  - megvalósul-e a központi felhasználóazonosítás és jogosultság-nyilvántartó és az eseményfigyelő rendszerhez történő csatlakozás,
  - megtörtént-e az üzleti működés folytonossági és a katasztrófaterv kialakítása, a megvalósított rendelkezésre állási képességek megfelelnek-e az adott biztonsági osztályra vonatkozó követelményeknek.
- a megvalósított védelmi képességek megfelelnek-e a meghatározott informatikai biztonsági osztályra vonatkozó követelményeknek,
- megvalósul-e a jogszabályoknak és a szervezet belső szabályzatainak való megfelelés a fejlesztés és megvalósítás folyamán,
- megtörtént-e a projekt kezdetén az adott informatikai rendszerre vonatkozó nem elviselhető kockázatok és a projekt végén a maradvány *kockázatok felmérése*.

Az informatikai rendszerek ***üzemeltetését*** biztonsági szempontból éves szinten *tervezett auditálásnak* kell alávetni, amely kiterjed arra, hogy:

- megvalósul-e az *informatikai biztonságpolitika* folyamatos érvényesítése az *Informatikai Biztonsági Szabályzat* és a rendszer szintű informatikai biztonsági szabályzatokon keresztül,
- megvalósul-e a kialakított fizikai és logikai védelmi képességeknek az adott biztonsági osztályra vonatkozó követelmények szerinti folytonos biztosítása,
- megvalósul-e az üzleti működés folytonossági és katasztrófatervben meghatározott képességek aktivizálhatósága a tervekben lefektetett módon és követelményeknek megfelelően,
- megvalósul-e a megvalósított rendelkezésre állási képességeknek az adott biztonsági osztályra vonatkozó követelmények szerinti folytonos biztosítása,

- megvalósul-e a vonatkozó jogszabályoknak, a titokvédelmi szabályzatoknak és az egyéb belső szabályzatainak való megfelelés.

12.2.3. Informatikai biztonsági tanúsítás és minősítés

Az informatikai biztonság tanúsítása és minősítése engedélyezett, elfogulatlan és független tanúsító által lefolytatott vizsgálat után tanúsításra kerül, hogy a vizsgált rendszer vagy termék adott, a minősítő által előírt követelményrendszerben meghatározott biztonsági szintnek megfelel (vagy nem felel meg), a tanúsítási eljárás hitelességét független nemzeti minősítő vizsgálja, és ez alapján bocsátja ki a minősítést. Az Európai Közösség országaiban a tanúsítás követelményrendszerét az ITSEC, az Egyesült Államokban a TCSEC foglalja magában.

- A szervezet működését támogató informatikai rendszer tanúsíttatása – a kiemelt biztonsági osztályba sorolt informatikai rendszerek kivételével – nem kötelező.
- Biztonsági tanúsítási igény esetén a tanúsítást a megvalósítási projekt keretében kell elvégezni. A tanúsíttatásra vonatkozó javaslatot az IT projektvezető készíti el az informatikai biztonsági vezetővel (menedzser) egyeztetve, és az illetékes (informatikai) vezető hagyja jóvá.
- A tanúsítást csak a gyártótól, szállítótól, üzemeltetőtől független tanúsító végezheti el és csak nemzetközileg is elfogadott követelmények, például az ITSEC ajánlás szerint.

Irodalom

Akl, S. G.: *Digital signature: A tutorial survey.* IEEE Trans. on Computers, C-34, 1983

Ameljańczyk, Andrzej: *Teoria Gier*, WAT, Warsó, 1978

Bakacsi; Bokor; Császár; stb.: *Stratégiai emberi erőforrás menedzsment*, KJK, Budapest, 2000.

Bodlaki Ákos, Endrédi Gábor, Farmosi István, Hajnal János, Komor Levente Dr., Muha Lajos, Nagy Béla, Nemetz Tibor Dr., Nyitrai Miklós Zoltán, Sajti János, Szigeti Szabolcs, Vadász Dezső: ***Az informatikai biztonság kézikönyve*****. Verlag Dashöfer, 2000–2001.**

Bodlaki Ákos: *Az informatikai biztonság tervezési kérdései*, HISEC '96. Budapest. 1996.

Bodlaki Ákos; Muha Lajos: *Az informatikai biztonság tanúsítási és minősítési eljárásrendjének terve (tervezet).* MeH ITB. Budapest. 1996.

Braun, Christoph: *UNIX System Security Essential*, Addison-Wesley, 1994.

British Standard 7799 (http://www.istc.org.uk/bs7799.htm)

Central Computer and Telecommunications Agency: *Risk Analysis and Management Method*

Common Criteria for Information Technology Security Evaluation (*CC*) version 2.1, (ISO/IEC 15408:1999), (http://csrc.nist.gov/cc/)

Computer Emergency Response Team (CERT) (http://www.cert.org/)

Dietz Gusztávné Dr.; Pap Márta: *Adatvédelem, adatbiztonság*, Budapest, 1995.

Diffie, W.: *The first ten years of public-key cryptography.* Proc. of the IEEE, 1988.

Diffie, W. – Hellman, M. E.: *New directions in cryptography* IEEE Trans. on Info. Theory, IT-22, 1977.

Elbert, N. F.; Karoliny; Farkas; Poór: *Személyzeti/emberi erőforrás menedzsment kézikönyv*, KJK, Budapest, 2000.

Fridrichs, Günter; Schaff, Adam: *Microelektronika és társadalom*, Statisztikai Kiadó Vállalat, Budapest, 1984.

Gazdag Miklós Dr.: *Vállalati humánpolitika*, Szelektor, Budapest, 1991.

Gömbös Ervin Dr.: *Informatika és hatalom*, Statisztikai Kiadó Vállalat, Budapest, 1984.

Gönci Dr.; Gyenes; Dr. Kaló; Kuti; Dr. Margitai; Nagy; Neumann; Nyilas; Pelbárt Dr.; Szövényi Dr.; Tímár; Vörösmarti Dr.: *Biztonságvédelmi kézikönyv* (Budapest, 2000, KJK)

Gönci Dr.; Nagy: *Biztonságtechnika és információvédelem (tanulmány)*, Future Security, Budapest, 1999.

Guide. Defining and Buying Secure Open Systems. – X/Open Company Ltd., 1992 szeptember.

Guldentops, Erik, CISA: *COBIT Update.* The First Central and East European International Conference on Information Systems Audit, Control and Security. Budapest. 4–7 September,1996.

Hacker Proof: *The Ultimate Guide to Network Security*, Jamsa Press, 1997.

Information Technology Security Evaluation Criteria. (ITSEC) v.1.2 EC DG XIII. 1991. május. (http://www.itsec.gov.uk/docs/formal.htm#ITSEC)

Information Technology Security Evaluation Manual (ITSEM). Draft V0.2. 1992. április.

Inside Windows NT 4.0, Second Edition, Microsoft Press, 1998.

ISO/IEC 16164-7 Information Technology. Open Systems Interconnection. System Management: Security alarm reporting function.

ISO/IEC 16164-8 Information Technology. Open Systems Interconnection. System Management: Security audit trail function.

ISO/IEC 9796 Information Technology. Security Techniques. Digital signature scheme giving message recovery.

ISO/IEC 9797 Information Technology. Security Techniques. Data integrity mechanism using a cryptographic check function employing a block cipher algorithm.

ISO/IEC 9798-1 Information Technology. Security Techniques. Entity authentication mechanisms. Part 1: General model.

ISO/IEC 9798-3 Information Technology. Security Techniques. Entity authentication mechanisms. Part 3: Entity authentication using a public key algorithm.

IT-Grundschutzhandbuch. Massnahmenempfehlungen für den mittleren Schutzbedarf. Schriftenreihe zur IT-Sicherheit. Band 3. 1995.

IT-Grundschutzhandbuch. Schiftenreihe zur IT-Sicherheit. Band 3. – Bundesamt für Sicherheit in der Informationstechnik, 1995.

Jenkins, A. Milton: *The Problems and Opportunities Regarding Security in Client-Server Environments.* The First Central and East Europian International Conference on Information Systems Audit, Control and Security. Bp., 4–7 September, 1996.

Kahn, D.: The codebreakers, MacMillan, New York, 1967.

Lainhart, John W. IV, CISA.: *Auditing Control and Security.* The First Central and East Europian International Conference on Information Systems Audit, Control and Security. Budapest. 4–7 September,1996.

Lainhart, John W., Donahue, Michael: *Computerized Information Systems (CIS) Audit Manual.* 1992.

Landreth, Bill: *Out of the Inner Circle*, Microsoft Press, 1989.

Liderman, Krzysztof: *Bezpieczeństwo informacji w systemach komputerowych*, WAT, Warsó, 2000.

Maximum Security, Second Edition, Sams Publishing, 1998.

Merkle, R. C.: *Protocols for public-key cryptosystems.* Proc. of the IEEE Symp. on Security and Privacy. Oakland, 1980.

Microsoft Windows NT 4.0 Security, Audit, and Control, Microsoft Press, 1999.

Microsoft Windows NT Security Guidelines, Trusted Systems Services, 1998.

Microsoft Windows NT Security Handbook, Osborne McGraw-Hill, 1997.

Microsoft Windows NT Server Resource Kit, Microsoft Press, 1996.

Microsoft Windows NT Server: Security Features and Future Direction, Coopers & Lybrand L.L.P., 1998.

Microsoft Windows NT Workstation Resource Kit, Microsoft Press, 1996.

***Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság 8. számú ajánlása, Informatikai biztonsági módszertani kézikönyv*, Budapest, 1994. (http://www.itb.hu /ajanlasok/a8)**

***Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság 12. számú ajánlása, Informatikai Rendszerek Biztonsági Követelményei*, Budapest, 1996. (http://www.itb.hu /ajanlasok/a12)**

Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság 16. számú ajánlása, Common Criteria (CC), az informatikai termékek és rendszerek biztonsági értékelésének módszertana, Budapest, 1998. (http://www.itb.hu /ajanlasok/a16)

MSZ ISO 7498-1 Információfeldolgozó rendszerek. Nyílt rendszerek összekapcsolása. Referenciamodell. 1. rész: Alapmodell

MSZ ISO 7498-2 Információfeldolgozó rendszerek. Nyílt rendszerek összekapcsolása. Referenciamodell. 2. rész: Biztonsági architektúra

MSZ ISO 7498-3 Információfeldolgozó rendszerek. Nyílt rendszerek összekapcsolása. Referenciamodell. 3. rész: Névadás és címzés

MSZ ISO 7498-4 Információfeldolgozó rendszerek. Nyílt rendszerek összekapcsolása. Referenciamodell. 4. rész: Menedzselési keretrendszer

Muha Lajos: *Az informatikai biztonság auditálása.* HISEC '96. Budapest, 1996.

Muha Lajos: *Az elektronikus okirat bevezetésének kérdései az informatikus szemével.* HiSec '97. Budapest. 1997.

National Bureau of Standards: *Data Encryption Standard.* Washington, D.C., 1977.

ORACLE7 Server Administrator's Guide. Part IV. Database Security.

OS/400 TCP/IP Security Enhancement Positioning v4r3: Mark McKelvey, IBM.

Parthasarathy T.; Raghavan T.E.: *Some topies in two-person games*, P.C. New York, 1971.

Polgári Védelmi Nemzetközi Szervezetek (Organisation Internationale de Protection Civile – OIPC.) VI. Világkonferenciája, 1974. Genf

Poór J. Dr.: *Menedzsment tanácsadási kézikönyv*, KJK, Budapest, 2000.

Poór J. Dr.; Borgulya; Mohácsi: *Nemzetközi emberi erőforrás menedzsment,* KJK, Budapest, 1996.

Raymond, Eric S.: *The New Hacker's Dictionary,* MIT Press, 1996; (http://www.tuxedo.org/~esr/jargon/jargon.html)

Rivest, R.L.–Shamir, A.–Adleman, L.: *A method for obtaining digital signatures and public-key cryptosystems.* Comm ACM 21. 1978.

Securing Windows NT Installation, Microsoft Corporation, 1997.

Security. Part 5 of the Open Systems Directive. – X/Open Company Ltd., 1993. március.

Security Focus (http://www.securityfocus.com/)

Shannon, Claude E.: *Communication Theory of Secrecy Systems*, Bell Syst. Techn. J., 1949.

Shannon, Claude E.: *Prediction and Entropy of Printed English*, Bell Syst. Techn. J., 1951.

Shannon, Claude E.; Weaver, Warren: *A kommunikáció elmélete*, Budapest, 1986.

Stang; David J. Ph.D.; Moon, Sylvia: *Network Security Secrets.* 1993.

Szövényi György Dr.: *A bizalmi munkakört betöltők ellenőrzése* (előadásanyag, 1998)

Tips and Tools for Securing Your AS/400: SC41-5300-04, IBM.

Trusted Computer System Evaluation Criteria (TCSEC) Department of Defense USA. (*Orange Book of the Security of Information Systems*), 1983. augusztus

Trusted Network Interpretation Environments Guideline. – National Computer Security Center, USA, 1990. augusztus.

Trusted Product Evaluations. A Guide for Vendors. National Computer Security Center. USA. NCSC-TG-002. Version-1. 1990. június.

UK IT Security Evaluation and Certification Scheme.
UK Certified Product List. UKSP 06. 2. kiadás. 1993. április.

Várhegyi István Dr.; Makkai Imre Dr.: *Információs korszak, információs háború, biztonságkultúra*, OMIKK, Budapest, 2000.

Warren; J. Donald, Edelson Jr.; Lynn W., Parker; Xenia Ley.:
Handbook of IT Auditing. Coopers & Lybrand L.L.P. 1996 edition.

Williams, Paul: *Controlling End-User Environment*. The First Central and East European International Conference on Information Systems Audit, Control and Security. Budapest, 4–7 September, 1996.

Felelős kiadó:
Peterdiné Árva Ilona,
a PRO-SEC Kft. ügyvezető igazgatója

Tipográfia és nyomdai előkészítés:
EMU Stúdió, Budapest, 388-3236

Nyomás és kötés:
INFO Nyomdaipari Kft., Budapest
Felelős vezető: Kerekes Pál

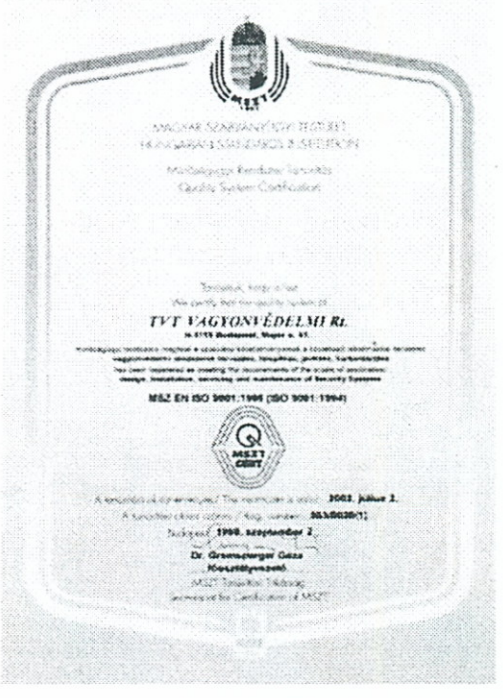
VAGYONVÉDELMI RT.

„Célunk a partnereink igényeinek teljes körű kielégítése a tervezés, fejlesztés, kivitelezés és vevőszolgálat területén, céltudatosan túlszárnyalva azt a minőségi szintet, melyet a megrendelő maga elé kitűzött. A minőség kijelöli azt az utat, amelyre cégünk vezető pozícióját megtartva elsőként tette rá lábát, ezzel is biztosítva az elégedett vevőink és munkatársaink hosszan tartó baráti, üzleti kapcsolatát."

Az ISO 9001:1996 szerinti minőségbiztosítási rendszer tanúsított alkalmazási területei:

elektronikus behatolásjelző-, videomegfigyelő-, automatikus tűzjelző-, beléptető- és épületfelügyeleti rendszerek tervezése, telepítése és karbantartása.

ISO


TVT VAGYONVÉDELMI Rt.

MSZ EN ISO 9001:1996 (ISO 9001:1994)

9001

1119 Budapest, Major u. 61. ➢ Telefon/fax: 203-1070 ➢ Levélcím: 1518 Budapest, Pf. 148.