Nemzeti
Közszolgálati Egyetem

Vezető- és Továbbképzési Központ

MUHA LAJOS – KRASZNAY CSABA

Az elektronikus információs rendszerek biztonságáról vezetőknek

Nemzeti Közszolgálati Egyetem © Budapest

A tananyag az ÁROP-2.2.21
Tudásalapú közszolgálati előmenetel című projekt
keretében készült el.

Eredeti megjelenés éve: 2014

A hatályosított tananyag a KÖFOP-2.1.1-VEKOP-15-2016-00001
„A közszolgáltatás komplex kompetencia, életpálya-program és oktatás technológiai fejlesztése"
című projekt keretében készült el és jelent meg.

A hatályosított kézirat lezárásának dátuma: 2018. április 6.

Szerzők:
© Dr. Muha Lajos
© Dr. Krasznay Csaba

Szakmai lektor:
Dr. Szádeczky Tamás

Olvasószerkesztő:
Kiss Eszter

Kiadja:
© NKE, 2018.
Felelős kiadó:
Prof. Dr. Kis Norbert
Dékán

Tartalom

Bevezetés

A nemzetközi és a hazai tapasztalatok is azt mutatják, hogy az elektronikus információs rendszerek – különösen az állami rendszerek – állandó célpontjai a szervezett bűnözésnek, a jól képzett informatikai támadóknak (az ún. hackereknek) és adott esetben akár más államok hivatalos szerveinek.

Információs rendszereinkre fenyegetést jelent a hadviselés új formája az információs hadviselés, valamint a békeidőkben is fenyegető terrorizmus számítógépes változata, a kiberterrorizmus. Ezáltal a modern hadviselés egyik legfontosabb színtere lett a kibertér.

A fentiek miatt Magyarország Országgyűlése 2013. április 23-án elfogadta az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt. Célunk, hogy e törvényhez kapcsolódóan, a hazai és európai ajánlásokhoz igazodva bemutassuk az elektronikus információs rendszerek biztonságával kapcsolatos követelményeket és teendőeket, kitérve napjaink aktuális kérdéseire is.

Budapest, 2014. május 30.

Dr. Muha Lajos és Dr. Krasznay Csaba

1. A kibertér biztonsági kihívásai

Ma már nem telik el úgy nap, hogy ne olvashatnánk vagy hallhatnánk valamilyen kiberbiztonsági incidensről. Lehet ez több millió személyes adat kiszivárgása, egy digitális „bankrablás" vagy éppen egy választás befolyásolása a közösségi média „eltérítésével", a lehetőségek tárháza végtelen. Észre kell vennünk, hogy a 2010-es években alapvetően változott meg társadalmunk és gazdaságunk működése, hiszen az ezekhez kapcsolódó folyamatok nagymértékben áttevődtek a virtuális világba. Kialakítottuk a digitális jelenlétünket, mely majdnem olyan fontos, mint a fizikai megjelenésünk. Az új élettér pedig új biztonsági kihívásokat jelent, melyekre nem vagyunk felkészülve sem magánszemélyként, sem szervezetként.

Magyarország kormánya a 2010-es évek elejétől jelentős erőfeszítéseket tesz annak érdekében, hogy a jogszabályi és szervezeti háttér készen álljon az új típusú fenyegetések kezelésére. Ennek első lépése Magyarország Nemzeti Kiberbiztonsági Stratégiájának megalkotása volt, melynek első cikke így fogalmazza meg országunk céljait: „Jelen stratégia célja, hogy az Alaptörvény elveivel összhangban, az értékek és érdekek számbavétele, valamint a kibertér biztonsági környezetének elemzése alapján meghatározza azon nemzeti célokat, stratégiai irányokat, feladatokat és átfogó kormányzati eszközöket, amelyek alapján Magyarország érvényesíteni tudja nemzeti érdekeit a globális kibertér részét képező magyar kibertérben is. A stratégia célja a szabad és biztonságos kibertér kialakítása és a nemzeti szuverenitás védelme a XXI. század meghatározóvá vált új közege, a kibertér létrejöttének következtében megváltozott nemzeti és nemzetközi környezetben. Célja továbbá a nemzetgazdaság és társadalom szabad tevékenységének védelme és biztonságának garantálása, az új technológiai innovációk biztonságos adaptálása a gazdaság növekedésének biztosítása érdekében, valamint nemzetközi együttműködések kialakítása ezen a téren a magyar nemzeti érdekek szerint. Jelen stratégia jelzi, hogy Magyarország a kibertér védelemével összefüggő feladatok ellátását felelősséggel vállalja és a magyar kiberteret, mint a gazdasági és társadalmi élet meghatározó pillérét szabad, biztonságos és innovatív környezetté kívánja alakítani. A megelőzésre épülő hatékony védelmi intézkedések útján elsődleges cél a kibertérben jelentkező és a kibertérből érkező fenyegetések és az ezzel járó kockázatok kezelése, az ehhez szükséges kormányzati koordináció és eszköztár erősítése." [12]

Ezek a stratégiai célok azonban nem teljesülhetnek az abban szerepet kapó szereplők harmonikus együttműködése nélkül. Hajlamosak vagyunk azt gondolni, hogy a kiberbiztonság elsősorban műszaki feladat, melyet az informatikusoknak kell megoldani. Ez azonban ma már nem igaz. Mi is a kibertér? A Stratégia meghatározása alapján „A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett." Az informatika tehát csak eszköz, melynek szabályok nélküli használata minden pozitív eredmény mellett számos devianciát is magával hoz, ezt pedig az informatikai szakma egymagában nem tudja megoldani.

A káros jelenségek pedig egyre nagyobb hangsúlyt kapnak. Alapvetően négy motiváció köré lehet csoportosítani azokat a kihívásokat, melyekkel szembesülnünk kell:

- Anyagi haszonszerzés: talán a leggyakoribb probléma a kibertérben, elkövetői között pedig nem csak a kiberbűnözői csoportokat, de az informatikailag képzettebb munkavállalókat is megtalálhatjuk. Mivel az anyagi javak egyre inkább digitális formában jelennek meg (gondoljunk csak arra, hogy bankunk is számítógépen tartja nyilván a bankszámlánkon levő pénzt), nem meglepő, hogy világszerte egyre többen használják a virtuális teret illegális pénzszerzésre.
- Információszerzés: adataink szinte kivétel nélkül digitálisan keletkeznek, tehát az ezekhez kapcsolt információt is a számítógépek „megcsapolásával" lehet a legegyszerűbben megszerezni. Az elkövető lehet egy állam titkosszolgálata csakúgy, mint egy féltékeny családtagunk. Ne felejtsük el, az okostelefonok tömeges elterjedésével egy folyamatosan bekapcsolt mikrofont és kamerát hordunk magunkkal, melynek jó eséllyel állandó hozzáférése van minden féltett adatunkhoz. Ez pedig csak egy eszköz a számtalan másik közül, melyen keresztül az információ kiberkémkedés útján megszerezhető.
- Személyes motivációk: előfordul, hogy a kibertér adta lehetőségeket valamilyen személyes motiváció fordítja a közösség ellen. Akár a hacktivista csoportok weboldal-feltöréseire vagy adatszivárogtatásaira, akár a terrorista csoportok közösségi oldalon folytatott propagandájára gondolunk, a háttérben személyek vagy kisebb csoportok vélt vagy valós sérelmek megtorlására használják a technológiát.
- Államok stratégiai céljai: Egyes államok évtizedek óta fejlesztik azokat a képességeket, melyek felhasználásával a kiberteret is hadrendbe állítják stratégiai céljaik elérése érdekében. Ma már minden fegyveres cselekményt

kísér valamilyen informatikai támogatóművelet is, valamint megismerhettük a hibrid hadviselés, a „se nem béke, se nem háború" fogalmát is, mely magában foglalja az online térben végzett műveleteket is. Nem véletlen, hogy a NATO 2016 óta a kiberteret a hadviselés ötödik színtereként ismeri el.

Ezen komplex kihívások kezeléséhez tehát az egyének és a szervezetek közös hozzájárulása szükséges. A szervezeti hozzájárulás pedig nem lehet hatékony a vezetői támogatás nélkül. A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról ezért szentel kiemelt figyelmet annak, hogy a közszféra vezetői is megértsék és támogassák Magyarország kibervédelmi törekvéseit. Ahogy a törvény 11. § (1)-ben olvashatjuk, „A szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről", ez a kötelesség pedig nem csak a saját szervezet belső védelmét szolgálja, hanem ezen keresztül Magyarország biztonságát is.

2. Az elektronikus információs rendszerek biztonságának fogalma és tartalma

„Alapvető elvárássá vált, hogy az informatikai rendszerek által kezelt adatok védve legyenek és biztonságosan legyenek használhatók. Az információs rendszerekben kezelt információk biztonsága a sikeres tevékenység egyik alapfeltételévé vált. Egyetlen szervezet sem tud napjainkban sikeres lenni az informatikai rendszereinek elfogadható védelme nélkül. … Az informatikai rendszerek biztonsága érdekében hozott, jól megválasztott védelmi intézkedések segítenek károk megelőzésében, csökkentésében, és a kárfelszámolás meggyorsításában – sikeressé tehetik a szervezetet." [3]

„**A védelem tevékenység, amíg a biztonság egy állapot**." [6] „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 másik oldalon a védő a védett értéket védi.**" [4]

2.1. Elektronikus információs rendszerek

Az információ- és kommunikációs technológiák[2] konvergenciája miatt mára elterjedten használják az *információ és kommunikációs technológia* kifejezést és annak IKT vagy angolosan ICT rövidítését. Összhangban az információbiztonsági törvénnyel [7] ezeket a rendszereket nevezzük **elektronikus információs rendszerek**nek.

„Elektronikus információs rendszer az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese" [3]. Az elektronikus információs rendszerekhez tartoznak:

1. a számítástechnikai rendszerek és hálózatok;
2. a helyhez kötött, mobil és egyéb rádiófrekvenciás, valamint műholdas elektronikus hírközlési hálózatok, szolgáltatások;
3. a rádiós vagy műholdas navigáció;
4. **az automatizálási, vezérlési és ellenőrzési rendszerek (vezérlő és adatgyűjtő[4], távmérő, távérzékelő és telemetriai rendszerek stb.);**
5. a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek.

A továbbiakban informatikai, infokommunikációs vagy informatikai és kommunikációs rendszer alatt is elektronikus információs rendszert értünk.

„Az elektronikus információs rendszerek biztonságát, vagy, ahogy gyakran használjuk magyarul, az *informatikai biztonság*ot és az *információbiztonság*ot – néha még a szakemberek is – gyakran összekeverik egymással, sőt időnként az adatvédelemmel is. Az adatvédelem a személyes adatok védelmére vonatkozik. Az információbiztonság a szóban, rajzban, írásban, a kommunikációs, informatikai és más elektronikus rendszerekben, vagy bármilyen más módon kezelt információk védelmére vonatkozik. Ezzel szemben például az elektronikus információs rendszerek biztonsága „csak" az elektronikus információs rendszerekben kezelt adatok és az azt kezelő rendszer védelmét jelenti. Mivel angolul általában az információvédelemre, illetve az elektronikus információs rendszerek védelemére is az *information security* kifejezést (néha a *computer security*, a *network security* kifejezéseket is) használják, így az egyes fordítások még inkább zavarossá teszik a képet. (A védelem és biztonság kifejezést egymás szinonimájaként használjuk, bár nem azonos a jelentésük.)" [5]

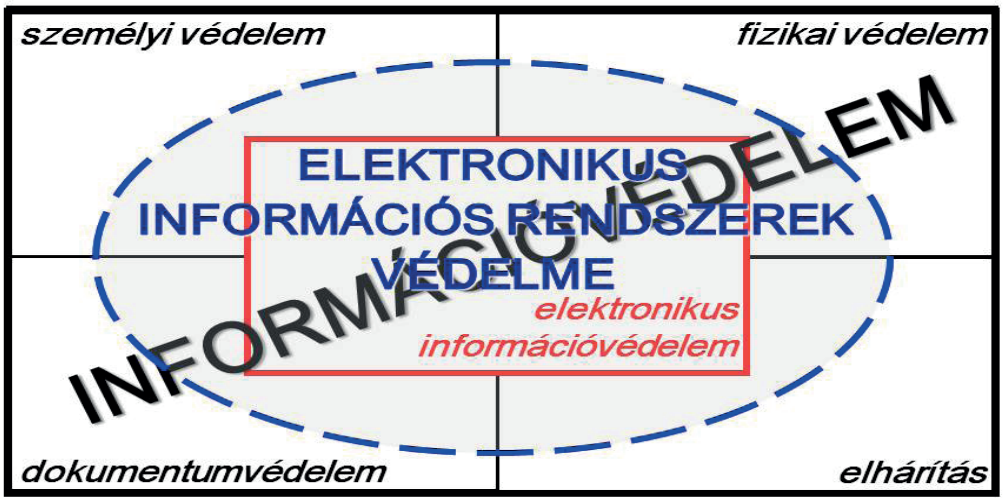
---

[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] Angolul: Information and Communications Technology (ICT), néha az Information and Related Technology kifejezést is használják.

[3] 2013. évi L. törvény 1.§ (1) bek.

[4] Ideértve a SCADA (Supervisory Control and Data Acquisition – felügyelet-irányítás és adatgyűjtés) rendszereket.



1. ábra Az információvédelem és az elektronikus információs rendszer védelme – [2] alapján

2.2. Az elektronikus információs rendszerek biztonsága

„Az elektronikus információs rendszer biztonsága az elektronikus információs rendszer olyan – az érintett[5] *számára kielégítő mértékű – állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos."*[6] *[5], [2]*

Ahol az információbiztonsági törvény szerint:

- Bizalmasság[7]: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt[8] adatot, információt csak az arra jogosultak és csak a jogosultságuk szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról. [5], [2]
- Sértetlenség[9]: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség[10]) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanság[11]) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható. [5], [2]
- Rendelkezésre állás[12]: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.[13]
- A bizalmasság, a sértetlenség és a rendelkezésre állás hármasát szokták az angol kezdőbetűik (*Confidentiality, Integrity, Availability*) alapján *CIA-elvnek* nevezni.

„Teljes körű védelem alatt azt értjük, hogy a védelmi intézkedések **a rendszer összes elemére kiterjed**nek.

Zárt védelemről **az összes releváns fenyegetést figyelembe vevő** védelem esetén beszélünk.

A **folytonos védelem** az időben változó körülmények és viszonyok ellenére is **megszakítás nélkül valósul meg**." [6]

„**A kockázattal arányos védelem** esetén egy **kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel**, azaz a védelemre akkora összeget és olymódon fordítanak, hogy ezzel a kockázat a védő

---

[5] Az érintett alatt a védelem nem kielégítő megvalósítását elszenvedő, a védelmet előíró, továbbá a védelemért felelős személyek és szervezetek együttese értendő.

[6] Az „érintett számára kielégítő mértékű" kifejezés a 2013. évi L. törvényben nem szerepel.

[7] Angolul: confidentiality

[8] Helyesebb lenne a „kezelt" kifejezés.

[9] Angolul: integrity

[10] Angolul: authenticity

[11] Angolul: non-repudiation

[12] Angolul: availability

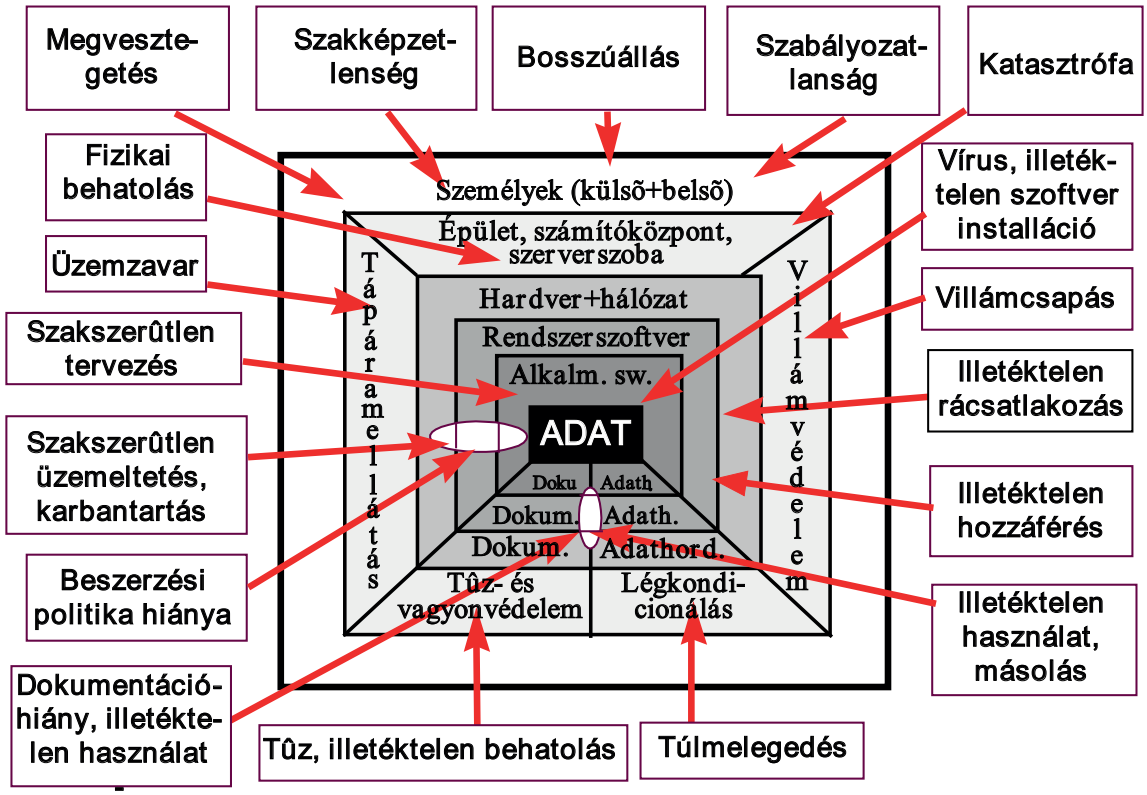
[13] Egy precízebb meghatározás szerint: „az adat, illetve az informatikai rendszer elemeinek tulajdonsága, amely arra vonatkozik, hogy az arra jogosultak által a szükséges időben és időtartamra használható." [5]

számára még elviselhető, vagy annál kisebb. […] Ezt az arányt a biztonságpolitika határozza meg, és mint a védelem erősségét is értékelhetjük.

A kockázatarányosság megértéséhez fontos, „hogy „*az elmaradt haszon az veszteség*" gazdasági bölcsesség mintájára „**az elmaradt kár az haszon**" tételt is értelmezzük, vagyis azt, hogy a kár az veszteség, és a meghatározható valószínűségű veszteség elkerülése haszonként fogható fel. Ebből egyenesen következik, hogy a potenciálisan bekövetkező károk elkerülésére tett intézkedés nem „pénzkidobás", hanem olyan beruházás, amely hasznot hoz." [2]

Az adatot mint a támadások alapvető célját az eszközök, eljárások és személyek mint rendszerelemek veszik körül.

E rendszerelemekre különböző fenyegetések hatnak, amelyek a rendszerelemek meghatározott láncán keresztül az adatokat veszélyeztetik. Az ábrán ennek a modellje látható.



2. ábra Az elektronikus információs rendszer védelmi modellje [6]

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.

2.3. A kritikus információs infrastruktúrák védelme és a kibervédelem

Hazánkban a kritikus infrastruktúrák védelmével kapcsolatos előírásokról *a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény* rendelkezik. A kritikus információs infrastruktúrák védelmét a *Magyarország Nemzeti Kiberbiztonsági Stratégiájáról* szóló 1139/2013. (III. 21.) Korm. határozat, illetve a 2013. évi L. törvény írja elő.

A kritikus információs infrastruktúrák védelme ágazatközi jelenség, védelmüket szorosan koordinálni kell magával a kritikus infrastruktúrák védelemmel.

A [2] megfogalmazásával összhangban a 2013. évi L. törvény meghatározása szerint *létfontosságú információs rendszerelem* az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény alapján kijelölt létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt rendszerelemeket vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené.

Divattá vált a *kiber* előtaggal megjelölni bármit, ami az internethez, az elektronikus információs rendszerekhez kötődik. A kiber kifejezés a *kibertér*[14] leegyszerűsítéseként került át a mindennapi szóhasználatba szerte a világon. [9]

„**Egy globális tartomány az informatikai környezeten belül, amely tartalmazza az egymással összefüggő informatikai hálózatok infrastruktúráit, beleértve az internetet, a távközlési hálózatokat, a számítógépes rendszereket, valamint beágyazott processzorokat és vezérlőket.**" [10]

Mára a kiber kifejezést önállóan használják mindenre, ami az internethez, az elektronikus információs rendszerekhez kötődik, de különösen ott, ahol valamilyen fenyegetés tárgya vagy eszköze az internet, az elektronikus információs rendszer. [9]

Ilyen a c*ybercrime*, magyarul a *kiberbűnözés*. A kiberbűnözéshez tartoznak az informatikai rendszerek és adataik ellen irányuló bűncselekmények mellett a felhasználásukkal elkövetett bűncselekmények, illetve olyan kapcsolódó bűncselekmények, mint a gyermekpornográfia, illetve a szerzői vagy szomszédos jogok megsértése.

*Kiberterrorizmus*nak a kibertérben elkövetett terrorcselekményeket nevezik. [11]

És akkor mit nevezhetünk *kiberbiztonság*nak?[15] „Kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez." [12]

[14] Angolul: cyberspace

[15] Angolul: Cybersecurity, helyesebben Cyberspace Security

3. Az elektronikus információs rendszerek biztonságához kapcsolódó jogi szabályozás

3.1. Az elektronikus információs rendszerek biztonsága

Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény [7] (a továbbiakban: Ibtv.) megalkotásával Magyarországon széles körre kiterjedően szabályozásra került az elektronikus információs rendszerek védelme. Az Ibtv. hatálya az állami és önkormányzati szerveken túl – a címével ellentétben – kiterjed a nemzeti adatvagyont és a kritikus információs infrastruktúrát (létfontosságú információs rendszerelem) kezelő szervezetekre.

Az Ibtv. a szervezetek számára alapvető feladatokat szab a biztonsággal kapcsolatosan, amelyeket a végrehajtási rendeletek részleteznek. Így a vezetés általános felelősségét írja elő az érintett szervezet által működtetett elektronikus információs rendszer biztonságáért. A szervezet köteles az elektronikus információs rendszer biztonságáért felelős személyt kijelölni, akinek alapvető feladatait is meghatározza a törvény.

A törvény nagy hangsúlyt fektet a biztonságtudatosságra, az oktatás-képzés kialakítására. A szervezet vezetője, az elektronikus információs rendszer biztonságáért felelős személy és munkatársai képzését a jogszabályi előírások szabályozzák.

Az Ibtv. létrehozta a Nemzeti Elektronikus Információbiztonsági Hatóságot. A biztonsági események kezelésére kormányzati és ágazati eseménykezelő központokat kell az Ibtv. alapján működtetni.

3.2. A minősített adatok védelme

A *2009. évi CLV. törvény a minősített adatok védelméről* (a továbbiakban: Mavtv) megteremti a minősített adatok védelmének egységes jogszabály- és intézményrendszerét. A tőrvényhez kapcsolódik a *90/2010 (III.23.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről*, és a *161/2010 (V.6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól*.

A fontos és bizalmas munkakört betöltő személyeknek *a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény* szerint nemzetbiztonsági szolgálatok által végzett nemzetbiztonsági ellenőrzésnek kell alávetniük magukat.

3.3. Az üzleti titok védelme

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.

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.

3.4. A banktitok és az értékpapírtitok védelme

A *2013. évi CCXXXVII. 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 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.**

Ezzel szinte betűre azonosak *a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló 2007. évi CXXXVIII.* törvény előírásai.

3.5. A személyes adatok védelme

A *2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról* szabályozza a személyes adatok védelmét. Az információs önrendelkezési jogról és az információszabadságról szóló 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.

3.6. Az elektronikus aláírás

A *2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól* az elektronikus ügyintézés széles körű elterjedése, az eljárások gyorsítása és az adminisztratív terhek csökkentése, a magánjogi jogviszonyok, továbbá az állam és polgár közötti jogviszonyok szélesebb körű elektronizálása, az elektronikus ügyintézést biztosító szervek együttműködésének biztosítása, valamint a lakosság számára a korszerűbb és hatékonyabb közszolgáltatások nyújtása a lakosság számára a korszerűbb és hatékonyabb közszolgáltatások nyújtása érdekében elengedhetetlenül szükséges jogszabályi feltételeket teremti meg.

Az elektronikus aláírást elsőként 2001-ben szabályozta törvény Magyarországon. Ennek fontosabb alapelvei a következők voltak [13]:

- az elektronikus aláírás előállítására felhasznált technológiától függetlenül alkalmazható a törvény (technológiasemleges szabályozás);
- az elektronikus aláírás joghatálya nem tagadható meg amiatt, hogy kizárólag elektronikus formában létezik;
- 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;
- az elektronikus aláírás alkalmazását – az ügyfelet érintően – nem lehet kötelezővé tenni;
- elektronikus aláírás hitelesítésszolgáltatást a jogszabályi feltételeknek megfelelő gazdálkodó szervezet nyújthat;
- a minősített elektronikus aláírással ellátott elektronikus irathoz teljes bizonyító erejű magánokirati vagy közokirati minőséget kell rendelni;
- a törvényben meghatározott általános elveket és eljárásokat az állami/közszféra területén is alkalmazni kell – a szükséges és megfelelő eltérésekkel.

3.7. A számítógépes bűnözés jogi kérdései

A számítógépes bűnözés a haszonszerzés vagy károkozás céljából, az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége és rendelkezésre állása, illetve a rendszerelemek rendelkezésre állása és funkcionalitása ellen irányuló vagy informatikai eszközök felhasználásával elkövetett bűncselekmények összefoglaló megnevezése. [13]

Az elektronikus információs rendszerek biztonsága szempontjaiból elsősorban a számítógépes bűncselekmények első csoportjával kell foglalkoznunk, amely mint *az információs rendszer vagy adat megsértése* ismert, de nem tekinthetünk el a másik csoportba tartozó bankkártyával, illetve a szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények figyelemmel kisérésétől sem. Itt nem tárgyaljuk, de nagyon fontos a számítógépet használó gyermekek védelme, az informatikai rendszereket használó, az interneten terjedő gyermekpornográfia elleni harc.

3.7.1. Az információs rendszerek védelme

A nemzetközi Számítástechnikai Bűnözésről szóló Egyezménnyel összhangban a Btk. 423. §-a szerint az információs rendszer vagy adat megsértése bűncselekményt az követi el, aki:

- információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve megakadályozza;

– információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz. A Btk. 424. §-ban meghatározott információs rendszer védelmét biztosító technikai intézkedés kijátszása bűncselekményt az követi el, aki a 375., a 422. § (1) bekezdés d) pontjában vagy a 423. §-ban meghatározott bűncselekmény elkövetése céljából az ehhez szükséges vagy ezt könnyítő:
    - jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez vagy forgalomba hoz, illetve
    - jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja.

3.7.2. A szerzői vagy szerzői joghoz kapcsolódó jogok megsértése

A „szoftverkalózkodás” a személyi számítógépek elterjedésével indult el, és az internet fejlődésével egyre nagyobb, riasztó méreteket ölt. Ez sérti a szerzők, a forgalmazók jogait és érdekeit. Ennek megfelelően került a Btk-ba a szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének bűncselekménye, amelyet az követ el, aki „másnak vagy másoknak a szerzői jogról szóló törvény alapján fennálló szerzői vagy ahhoz kapcsolódó jogát vagy jogait vagyoni hátrányt okozva megsérti”. A védelem megsértésére is „szakosodtak”, ezért a szerzői vagy szerzői joghoz kapcsolódó jog védelmét biztosító műszaki intézkedés kijátszása is bűncselekménynek minősül, amelyet az követ el, aki haszonszerzés végett „a szerzői jogról szóló törvényben meghatározott hatásos műszaki intézkedés megkerülése céljából az ehhez szükséges eszközt, terméket, számítástechnikai programot, berendezést vagy felszerelést készít, előállít, átad, hozzáférhetővé tesz vagy forgalomba hoz” vagy aki „az ehhez szükséges vagy ezt könnyítő gazdasági, műszaki, szervezési ismeretet másnak a rendelkezésére bocsátja”.

4. Hazai és nemzetközi szabványok és ajánlások

4.1. Common Criteria (ISO/IEC 15408 szabvány)

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.

A védelmi profil egy implementációfüggetlen funkcionális biztonsági követelményrendszert és objektumhalmazt határoz meg egy-egy terméktípusra vagy kategóriára.

A CC funkcionális követelményrendszere gyakorlatilag egy funkcionális komponenskatalógus, amelyből összeállítható a vizsgált rendszerre (*Target of Evaluation, TO*E) vonatkozó funkcionális biztonsági követelményrendszer. [14]

A biztonsági követelmények 7 **biztonsági osztályba (security assurance)** vannak sorolva.

4.2. ISO/IEC 27000 szabványsorozat

Az ISO/IEC:27001 szabvány[16] alapvető célja az Információbiztonsági Irányítási Rendszer[17] (IBIR) létrehozása és működtetése. A szabvány felhasználóinak a biztonsági követelményeket, intézkedéseket a szervezet üzleti céljaiból és stratégiájából kell levezetniük. A szabvány a megfelelőségi és ellenőrzési követelményei alapján elvégezhető az informatikai (információs) rendszer tanúsítása.

Az ISO/IEC 27002 szabvány teljes szervezetrevonatkozó, az összes rendszerelemcsoportot átölelő informatikai biztonsági követelményeket és védelmi intézkedéseket tartalmaz a teljes körű informatikai biztonság megteremtéséhez. A de facto nemzetközi szabvánnyá vált ITIL is ezt használja hivatkozási alapként.

A szabványcsaládnak sok – jelenleg 47 – tagja már kiadásra került és továbbiak is fejlesztés alatt vannak.

4.3. Az ISO/IEC TR 13335

Az informatikai biztonság területén sokáig használták az *ISO/IEC TR 13335 – Guidelines for the Management of IT Security*[18] (GMITS) műszaki jelentést, de idővel visszavonták. Az ISO/IEC TR 13335-öt például a Közigazgatási Informatikai Bizottság 25. számú ajánlásának készítéséhez is felhasználták.

4.4. Az informatikaszolgáltatás módszertana (ITIL)

Az ITIL, azaz *informatikaszolgáltatás módszertana* az informatikára, mint szolgáltatás egészére kiterjedő, nemzetközileg széles körben elfogadott dokumentum. „Az ITIL célja a jó minőségű, költséghatékony IT szolgáltatások támogatása, a minőségügyben ismert Plan-Do-Check-Act (PDCA) elv alkalmazásával. A biztonsági követelmények elsősorban IT szolgáltatás-folytonossági követelményként kerültek be a keretrendszerbe.” [14]

„Az ITIL egy jó gyakorlatokról szóló irányelv (best practice guide), addig az ISO 20000 az ezekből levezetett kötelező minimumkövetelmények, amelyek minimálisan elvárhatóak az IT szolgáltatások biztosítása terén. Céljaik és gyökerük viszont azonos, így azokat célszerű együtt kezelni.” [14] Az ITIL-t számos nemzetközi informatikai cég is elfogadta és támogatja, így például a Hewlett Packard, Microsoft, IBM stb. Ezek a cégek saját gyakorlatukba beépítették az ITIL terminológiáját és megközelítését.

---

[16] Ugyan a szabványcsalád egyes elemeit magyar szabványként is kiadták, de ezek nagyon rossz, a már kialakult informatikai és informatikai biztonsági szakmai nyelvezetet semmibe vevő fordítások. (A jegyzet kiadásakor készülők már nagy valószínűséggel jobbak lesznek!)

[17] Information Security Management System (ISMS)

[18] Segédlet az informatikai biztonság irányításához.

Az ITIL Biztonságirányítás (Security Management) kötete az ISO/IEC 1BS7799 (ISO/IEC 27002) szabványt használja hivatkozásként, valamint a létező ITIL folyamatokat bővíti a biztonságirányítással.

4.5. COBIT

Az Information Systems Audit and Control Foundation és az IT Governance Institute által kidolgozott **C**ontrol **Objectives for Information and Related Technology** az üzleti folyamatokra, valamint az ezeket támogató informatikai megoldások négy területére – tervezés és szervezés; beszerzés és üzembe állítás; informatikai szolgáltatás és támogatás, valamint felügyelet – helyezi a fő hangsúlyt.

„A COBIT nagy figyelmet fordít az informatikai irányítás elméleti hátterére, így több aspektusból elemzi az informatikai irányítás lényegét és területeit, valamint a különböző követelmények egymásra hatását és összefüggéseit." [14]

4.6. Magyar Informatikai Biztonsági Ajánlások (MIBA)

A Közigazgatási Informatikai Bizottság (KIB) 25. ajánlásaként kiadott Magyar Informatikai Biztonsági Ajánlások (**MIBA**) **három fő rész**ből áll:

1. A **Magyar Informatikai Biztonsági Keretrendszer (MIBIK)** szervezeti szempontból kezeli az informatikai biztonság kérdését. Ezért a MIBIK a biztonságos informatikai rendszerek irányításáért, menedzseléséért felelős vezetőknek, illetve a szervezet egészére vonatkozó követelmények teljesülését értékelő szakembereknek szól.
2. A **Magyar Informatikai Biztonság Értékelési és Tanúsítási Séma (MIBÉTS)** technológiai szempontból kezeli az informatikai biztonság kérdését. Ezért a MIBÉTS célközönsége az informatikai rendszer kialakításáért, fejlesztéséért felelős vezetők, valamint az informatikai termékek és rendszerek biztonsági értékelését és tanúsítását végző szakemberek köre.
3. Az **Informatikai Biztonsági Iránymutató Kis Szervezetek Számára (IBIX)** olyan szervezeteknek nyújt segítséget biztonságos informatikai rendszereik kialakításához, amelyek nem rendelkeznek jelentősebb informatikai rendszerrel, illetve ehhez elkülönült informatikai személyzettel.

4.7. Követelménytár

A Közigazgatási Informatikai Bizottság 2009-ben kiadta a 28. számú ajánlását, amely egy Követelménytár.

4.8. A NIST kiadványai

Az amerikai NIST (National Institute of Standards and Technology[19]) SP (Special Publication) 800 sorozata az USA számítógépes biztonsági politikáit, eljárásait és irányelveit írja le. A dokumentumok ingyenesen elérhetők, és nagyon hasznosak úgy a kormányzati szervek, mind a vállalkozások, az oktatási intézmények számára. Új sorozatként az SP 1800-as kiadványok a kiberbiztonsági gyakorlatokat mutatják be.

NIST SP 800 sorozat kiadványai között megtalálhatók a fenyegetések és sérülékenységek, a nemkívánatos események értékelésére és dokumentálására, a biztonsági intézkedések meghozatalához ajánlott eljárások. Jelenleg a gyűjtemény 195 tagból áll.

4.9. INFOSEC – Informatikai biztonság a NATO-ban

Az INFOSEC (information security) az elektronikus információvédelem NATO-n belüli értelmezése. Az INFOSEC két nagy területet foglal magába: a *kommunikációs biztonság*ot (*Com*munication *Sec*urity, *COMSEC*) és a *számítógépes rendszerek biztonságá*t (*Comp*uter *Sec*urity, *COMPUSEC*).

[19] Nemzeti Szabványügyi és Technológiai Intézet

4.10. Minőségirányítás

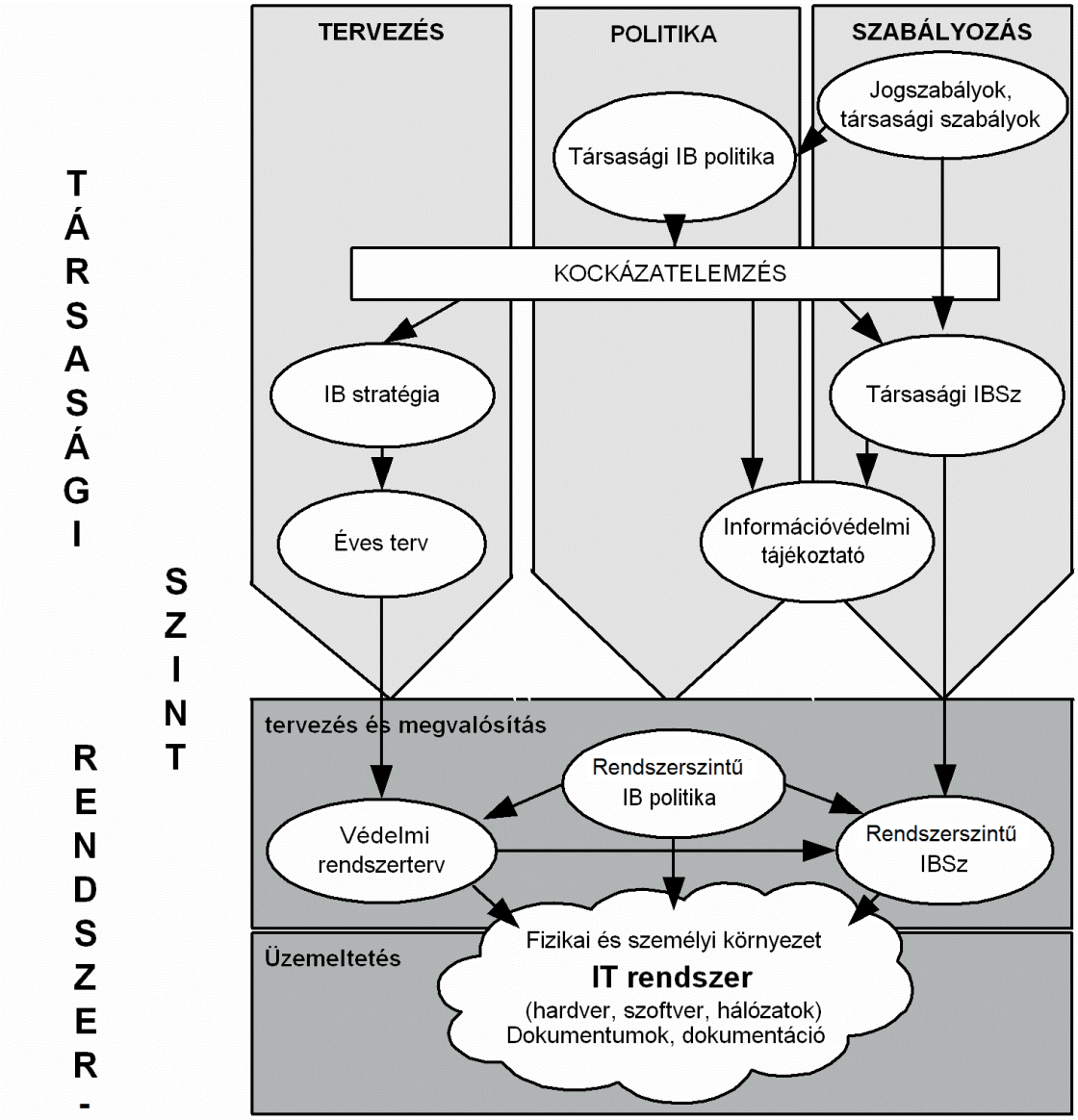
A minőségirányítással foglalkozó ISO 9001:2015 szabvány rendszerszabvány, ami azt jelenti, hogy előírásai nem a termék vagy szolgáltatás valamilyen tulajdonságait határozzák meg, hanem a szervezet működésének egészét átszövő minőségirányítás elveit. Ez a szabvány egy olyan szervezet követelményeit írja le, amely képes a vevők igényeinek kielégítésére, és felkészült e képességek független külső fél által végzett értékelésére.

4.11. Környezetirányítás

A környezetirányítási-rendszerek (KMR) nemzetközi szabványa az ISO 14001.

5. A védelem megvalósítása

A védelem megvalósítása 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 a 3. ábra mutatja.



3. ábra A védelem megvalósítása [1]

5.1. Az információbiztonsági irányítási rendszer

Az Információbiztonsági Irányítási Rendszer (IBIR)[20] egy általános irányítási rendszer, amely az üzleti kockázat elemzésén alapul, megállapítja, megvalósítja, üzemelteti, ellenőrzi, karbantartja és javítja az információbiztonságot. Az IBIR magában foglalja a szervezetet, a struktúrát, a szabályzatokat, a tervezési tevékenységeket, a felelősségeket, a gyakorlatokat, az eljárásokat, a folyamatokat és az erőforrásokat. Az IBIR akkor hatékony, ha hasznos a szervezet számára.

[20] Informatikai Biztonsági Irányítási Rendszer = Information Security Management System (ISMS) – az ISO/IEC 27001:2005 szabvány alapvető fogalma.

5.1.1. A PDCA modell

„Az IBIR létrehozása és működtetése ugyanolyan megközelítést igényel, mint sok más irányítási rendszer. Az ISO 27001-es szabvány erre a célra az OECD[21] által is támogatott PDCA, magyarul TVEB[22] folyamatmodell használatát vezette be az Informatikai Biztonság Irányítási Rendszere fejlesztésének, megvalósításának és hatékonyságának biztosítására. … A TVEB bármilyen műveletre, tevékenységre, folyamatra, rendszerre, működtetésre, koncepcióra, elgondolásra vonatkoztatható, zárt hatásláncú, folytonosan ismétlődő körfolyamat-elv. A nemzetközi szakirodalomban elterjesztőjéről, W. E. Demingről elnevezve Deming-ciklusnak (Deming's Cycle) is nevezik." [3]

A TVEB modell négy szakaszból áll [15]:

1. **Tervezés (Plan)** (Az Információbiztonsági Irányítási Rendszer létrehozása): A szervezet általános szabályainak megfelelő biztonságpolitika, célok, módszerek, folyamatok és eljárások meghatározása, amelyek relevánsak a kockázatkezelés és az informatikai biztonság fejlesztése szempontjából.
2. **Végrehajtás (Do)** (Az Információbiztonsági Irányítási Rendszer bevezetése és működtetése): A biztonsági szabályzat, intézkedések, módszerek és eljárások megvalósítása és üzemeltetése.
3. **Ellenőrzés (Check)** (Az Információbiztonsági Irányítási Rendszer ellenőrzése és felülvizsgálata): Fel kell becsülni és – ahol alkalmazható – fel kell mérni a biztonságpolitika végrehajtásának folyamatát, a célok és a gyakorlati tapasztalatok alapján az eredményeket a vezetés számára jelenteni kell.
4. **Beavatkozás (Act)** (Az Információbiztonsági Irányítási Rendszer továbbfejlesztése és karbantartása): A vezetői felülvizsgálat eredményén alapuló korrigáló és megelőző intézkedéseket kell hozni, illetve folyamatosan tovább kell fejleszteni az Informatikai Biztonsági Irányítási Rendszert.

5.2. 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. [1]

5.2.1. Az informatikai biztonságpolitika

Az informatikai biztonságpolitika (irányelv) szerepe az, hogy a szervezet teljes egészére vonatkozóan, 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 biztonságpolitikának meg kell fogalmaznia egy olyan tájékoztatási politikát is, amely biztosítja a megfelelő külső és belső tájékoztatást.

5.2.2. 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 [1]:

– a realitásokat figyelembe vevő, „működőképes" szabályzatot kell kidolgozni és hatályba léptetni (például vezetői utasítással);
– egyértelmű vezetői akarat kell a szabályzat érvényesítéséhez, valamint a működéséhez szükséges emberi és egyéb erőforrás feltételek biztosításához;

[21] Organistaion for Economic Co-Operation and Development = Gazdasági Együttműködési és Fejlesztési Szervezet
[22] Tervezés-Végrehajtás-Ellenőrzés-Beavatkozás = Plan-Do-Check-Act – **PDCA**

– 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.

Nagyobb szervezeteknél az informatikai biztonság szabályozását legalább két szinten javasolt megvalósítani (ld. 3. 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.

5.2.3. Az informatikai biztonsági stratégia

Az informatikai biztonsági stratégiának tartalmaznia kell az eszközrendszerre, az informatikai biztonságmenedzsmentre, a szabályozási rendszerre és az informatikai biztonsági szervezetre vonatkozó jövőképet. 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. Az éves tervezés a stratégiai terv birtokában következik. [1]

5.2.4. Titokvédelmi és Ügyviteli Szabályzat

5.2.4.1. Titokvédelmi Szabályzat

A Titokvédelmi Szabályzat célja, hogy a teljes szervezetre vonatkozóan egységesen meghatározza [1]:

– 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.

5.2.4.2. Ügyviteli Szabályzat

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

5.2.5. Üzletmenetfolytonosság-tervezés

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 működés kiesésekből származó károk összessége a szervezet számára elviselhető.

A nemzetközi irodalomban és egyre inkább a gyakorlatban is a katasztrófa elhárítás tervezést az üzleti működésfolytonosság tervezés részeként fogják fel.

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.

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

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

6. 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.

Egy szervezet munkatársainak a lojalitását és a biztonság növelésével kapcsolatos motiváltságát csupán szabályokkal nem lehet erősíteni. Ehhez más eszközök, módszerek is szükségesek, nevezetesen az emberierőforrás-kezelés vagy humánmenedzsment (Human Resource Management, HR Management) módszerei. Az emberierőforrásstratégia (megszerzés, fejlesztés, mozgatás, leépítés) vezetői és szervezeti szintű feladatai részben meglevő ismereteken alapulnak, részben további kutatásokat igényelnek.

6.1. 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 [16]:

- 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.

Az informatikai biztonsághoz (is) kapcsolódó emberierőforrás-kezelési feladatok [16]:

- 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 katasztrófa-elhárítási intézkedések.

Az informatikai biztonság megvalósítása szempontjából is nélkülözhetetlen a munkatársak folyamatos képzése, vagyis folyamatosan gondoskodni kell arról, hogy a munkatársak tudatában legyenek az informatikai biztonsági fenyegetéseknek, és motiválva legyenek a szervezet információvédelmi szabályzatainak és intézkedéseinek a betartására. A felhasználók legyenek kioktatva a biztonsági eljárásokról és az adatfeldolgozó eszközök helyes használatáról a lehetséges biztonsági kockázatok minimalizálása érdekében.

A biztonsági oktatás (képzés) egyik alapvető célja, hogy valós biztonságtudatot (security awareness) alakítsunk ki, vagyis a munkatársak legyenek tisztában azzal, hogy az általuk kezelt adatok milyen értéket képviselnek a szervezetük számára, és így az ő számukra is, valamint milyen értéket képviselnek a bűnözés számára. A fenyegetések, a kockázatok nem ismerete hamis biztonságtudatot eredményezhet, ami felesleges kockázatvállalást, nemtörődömséget, túlzott magabiztosságot okoz.

6.2. A Social Engineering

A social engineering[23] az emberi hiszékenységre, együttműködésre építő támadási forma. Bár ezt az élet sok más területén is kihasználják, a social engineering kimondottan az információ megszerzésére irányul.

A támadónak több olyan emberi tulajdonságot van lehetősége kihasználni, ami szinte kivétel nélkül minden potenciális áldozatban megtalálható. A legalapvetőbb ilyen tulajdonság a segítőkészség, de szóba kerülhet még a hiszékenység, a kíváncsiság és a naivság. Emellett nem szabad elfeledkezni a munkatársak figyelmetlenségéről, hanyagságáról és alulképzettségéről sem.

A **humánalapú technikák**nál a támadó csupán pszichológiai technikákat vet be. A lényeg, hogy a felvett személyiség és a kapcsolattartási megoldás illeszkedjen a social engineering támadási stratégiához. A leghatékonyabb stratégia az, hogy a támadó a szervezet egy másik munkatársának adja ki magát. A legideálisabb áldozatok ebben az esetben az új munkatársak, akik még nem teljesen ismerik a helyi viszonyokat, de fontos információkhoz van hozzáférésük.

[23] A *social engineering* vagy a *social engineer* kifejezéseknek nincs elfogadható magyar megfelelője.

Segítség kérése: A legtöbb sikerrel kecsegtető humánalapú technika, hiszen az emberek alapvetően segítőkészek, és nem feltételeznek semmi rosszat egy kétségbeesett kollégáról. Elsődleges célpontjai a különböző ügyfélszolgálati munkatársak, akiknek ráadásul elsődlegesen az a feladatuk, hogy segítsenek a hozzájuk fordulókon.

Segítség nyújtása: Az előző eljárásnak a fordítottja, amikor a támadó azt akarja elérni, hogy a célszemély rászoruljon a segítségre. Ezt úgy lehet elérni, hogy a támadó valamilyen hibát okoz, majd készségesen felajánlja az áldozatnak azt, hogy segít ezt a hibát kijavítani. .

Kölcsönösség kihasználása: A támadó ebben az esetben apró dolgokat tesz meg a célszemély érdekében, amiért egyszer majd kér egy szívességet. Ennek a nagyvállalati marketingszlengben üveggyöngy-technikának is nevezett módszernek az egyik jellegzetessége, hogy a viszontszívességet olcsó dolgokkal is el lehet érni.

Megszemélyesítés: Míg az előző esetekben a támadó feltehetően valamilyen fiktív identitást használt, a megszemélyesítés jellegéből adódóan olyan, hogy a felvett személyiség valós, a célszemély számára is ismert. A támadás jellegzetessége, hogy a támadó vagy egy fontos embernek adja ki magát, vagy azt állítja, hogy egy fontos ember nevében beszél.

Shoulder Surfing: Ennél a támadási módszernél azt lehet kihasználni, hogy a social engineer a célszemély mögött áll a számítógépes terminálnál, és a válla fölött átnézve le tudja lesni azt, amit begépel.

Piggybacking: A támadás során az egyébként legitim felhasználó jogosultságait használja ki a támadó. Ezt úgy lehet elérni, hogy otthon hagyott vagy elveszett kártyára hivatkozik, amivel általában segítőkész, megértő alanyokra lehet találni.

Tailgating: Szemben az előző megoldással, a támadó itt az áldozat tudta nélkül használja a belépési jogosultságot.

Dumpster Diving: A papírmentes irodák elterjedése ellenére (vagy ezzel együtt?) a felhasznált iratmennyiség folyamatosan növekszik, így egyre több információt lehet kinyerni a papírhulladékból. A technika lényege, hogy a támadó átkutatja a célpont hulladéktárolóit, hátha talál valamilyen értékes információt. Az erre vonatkozó esettanulmányok alátámasztják ennek a megközelítésnek a sikerességét.

Az elterjedtebb és egyszerűbb **számítógép-alapú social engineering technikák** a közvetett kapcsolattartást preferálják.

Scam: Speciális, széles körben használt technika, magyarul csalásnak fordíthatnánk. A social engineering terminológiájában olyan weboldalakat sorolunk ide, melyek valamilyen kedvező ajánlatot kínálnak a felhasználónak, akinek ezért nincs más dolga, mint regisztrálni az oldalon.

Adathalászat: Az adathalászat vagy más néven phishing célja az, hogy valamilyen üzenet formájában egy valósnak tűnő weboldalra csábítsa a felhasználókat, ahol azok kiadják azonosítójukat. Elsősorban banki weboldalak ellen indított támadásokból ismerhetjük.

Whaling: Ez a felhasználó kör – ahogy a szó is a bálnavadászatra utal – a „nagy halak", azaz a vezetők. Ezek a becsapós üzenetek elsősorban a menedzsmentre kihegyezve készülnek el, elsősorban célzott támadások során használják őket. Általában valamilyen partner vagy állami szerv nevében érkeznek. A cél sokrétű lehet, a támadási stratégiától függően lehet meghatározni.

Baiting: Magyarul szétszórást jelent. A támadás viszonylag költséges, és ötvözi a humán- és számítógép-alapú technikákat. A támadó a célpontként funkcionáló szervezet telephelyén „véletlenül" elveszít néhány DVD-t vagy pendrive-ot. Az áldozatok ezeket megtalálják, és nagy valószínűséggel saját számítógépükön megnézik ezeket. Ekkor egy kártékony kód fut le a számítógépen, ami segít megszerezni a kívánt adatokat. A támadást elősegítheti az, ha a DVD-re valamilyen közérdeklődést kiváltó cím van felírva.

A social engineering típusú támadás céltól függően más és más környezetben kerül végrehajtásra, de a forgatókönyve általában állandó, leggyakrabban négy lépésből áll. Ezek a következők:

1. Információszerzés
2. Kapcsolat kiépítése
3. Kapcsolat kihasználása
4. Támadás végrehajtása

A négy lépés általában egymásra épülve, egymás után kerül végrehajtásra, de a 2. és 3. lépés akár egyidőben is megtörténhet.

6.2.1. Információszerzés

A sikeres social engineering típusú támadás alapja az, hogy mind a célpontszervezetről, mind pedig a célpontszemélyről alapos információ álljon rendelkezésre. Ehhez az összes releváns információval rendelkezni kell. Napjaink interneten keresztül elérhető adatáradata hatalmas segítség egy támadónak abban, hogy az áldozat profilját felépítse, de emellett nem elhanyagolható az egyéb csatornák hasznossága sem.

Mind a szervezet, mind a személy számos információt oszt meg magáról, vagy osztanak meg róla mások az interneten. Kijelenthető, hogy napjainkban nagyon nehéz észrevétlen maradni, ráadásul a láthatatlanság nem csak rajtunk múlik. Egy cégre ez hatványozottan igaz, ugyanis az igazán kívánatos célpontok nagyok, sok ember dolgozik nekik, így az információszivárgás is kontrollálhatatlanul nagy.

6.2.2. Kapcsolat kiépítése

A támadási stratégia kidolgozásánál a legmegfelelőbb személyt kell kiválasztani. Ez a személy lehet „nagy hal”, elégedetlen munkatárs, olyan ember, aki nagy titkok tudója, lényegében bárki, akitől a kívánt információ megszerezhető. A kapcsolat kiépítése történhet a már korábban megismert módon, telefonon, levélben, személyesen. A támadó pedig a teljes pszichológiai fegyvertárat bevetheti, attól függően, hogy a célpont milyen személyiség. Legtöbbször a cél az, hogy az áldozat megbízzon a támadóban, ne kételkedjen annak szavahihetőségében, és segítse a kívánt információ elérésében.

7. Az informatikai helyiségek fizikai védelme

Az informatikai biztonság megteremtése során alapvető a fizikai védelem kialakítása.

A különböző funkcionális területek biztonsági zónákba sorolhatók. A különböző biztonsági zónák elhelyezkedésére a **hagymahéj-elv** a jellemző. Kívül találhatók a nyilvános területek és az alacsony biztonsági igényű ügyfélterületek. Ezeken belül az üzemviteli és műszaki területek. A középső részen az informatikai infrastruktúra és más fokozottan védendő helyiségek helyezkednek el.

A **mechanikai védelem** feladata, hogy akadályozza, lassítsa a védendő objektumba való illetéktelen behatolást és a védendő értékekhez történő illetéktelen hozzáférést. A mechanikai védelem összetevői: kerítések, héjvédelem (falak), nyílászárók: a különböző ajtók és ablakok, zárak, rácsok, biztonsági fóliák, trezorok, biztonsági táskák, borítékok.

Az élőerő feladata részben a beléptetés ellenőrzése, részben az elektronikai védelem és a videorendszer jelzései alapján reagáló (beavatkozó) erőként való fellépés, harmadrészt a mechanikai és az elektronikai védelem kiegészítése és ellenőrzése céljából járőrözés ellátása.

Ezen eszközrendszereket mindig komplexen kell alkalmazni. Az élőerő alkalmazása esetén az őrző-védő személyzet emberi erőforrásként jelentkező problémáiról, a megbízhatóság kérdéseiről sem szabad megfeledkezni, ugyanakkor nagyon fontos, hogy az emberi érzékelés, a megérzés olyan lehetőségeket biztosít, amelyekre az elektronika még nem képes.

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]:

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 informatikai helyiségek esetében a **tűzvédelem** kiemelt fontosságú 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 **villámcsapás**ok okozta közvetlen károk ellen a létesítmények általában védettek, de 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 túlfeszültségvédelem. Az esetek zömében az eszköz kieséséből származó közvetlen károkon túl nagyságrendekkel nagyobb értéket képviselnek a szolgáltatás kieséséből, adatvesztésből bekövetkező eszmei és üzleti károk.

Gyakori, és nagy veszélyeket hordoznak magukban a külső, elektromos **zavarójelek**. Ha ilyen probléma gyanúja felmerül, érdemes ellenőrző méréseket végeztetni, és az eredmények ismeretében megoldani a problémát.

A **kisugárzás** elleni védelem TEMPEST[24] néven ismert. Az adatok vezetés vagy sugárzás útján történő kijutását szűréssel és árnyékolással kell megakadályozni.

A kisugárzás- és zavarvédelem esetében az EN 55022, az EN55024 és az EIA/TIA-568 szabványokat kell figyelembe venni.

[24] A TEMPEST értelmezésére több magyarázat is van, de hivatalos vélemények szerint csak fantáziaszó.

8. 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 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 hagyományos eljárással papíralapon, vagy számítógépes eljárással.

Gyakorlati tapasztalat, hogy – még azoknál a szervezeteknél is, ahol a hagyományos, papíralapú iratkezelés jól szervezett – az informatikai rendszerbe be- és abból kikerülő dokumentumok, az ott feldolgozott, tárolt adatok iratkezelési szempontból elhanyagoltak, minősítésüknek megfelelő kezelésre, iktatásra nem kerülnek.

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 végigkisérve az adat „életútja”, mintha az hagyományos adathordozón lenne kezelve, tárolva vagy továbbítva.

A közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet meghatározza a közfeladatot ellátó szervekhez beérkező és az ott keletkezett papíralapú és elektronikus köziratok kezelésének követelményeit.

9. Logikai védelem

9.1. Hozzáférés-vezérlés

A hozzáférés-vezérlés olyan biztonsági mechanizmusok gyűjteménye, mely meghatározza, hogy a felhasználók mit tehetnek a rendszerben, azaz milyen erőforrásokhoz férhetnek hozzá és milyen műveleteket hajthatnak végre. Azok a védelmi intézkedések tartoznak ide, melyek szabályozzák, hogy egy felhasználó:

- milyen felhatalmazással férhet a rendszerhez,
- milyen alkalmazásokat futtathat,
- milyen információkat olvashat, hozhat létre, adhat hozzá és törölhet.

Általánosságban magába foglalja az **azonosítás** (identification), a **hitelesítés** (authentication), a **hozzáférés-engedélyezés** (access approval) és az **audit** (hozzáférés-ellenőrzés) lépéseit, de bizonyos esetekben a hozzáférés-vezérlés részének tekintik az elszámoltathatóságot (accountability) is.

Az azonosítás a szubjektum megnevezése, kicsit bővebben: a rendszer entitásainak egyedi azonosítóval való ellátásának folyamata. Az elszámoltathatóság alapfeltétele az, hogy minden eseményt egy egyedi entitáshoz tudjunk kötni.

A hitelesítés az a folyamat, mely arra szolgál, hogy az entitás bizonyítsa az önmagáról állítottak valódiságát. A felhasználó bemutatja a rendszernek az azonosítóját, amit a rendszer hitelesít, mielőtt engedné hozzáférni a rendszerhez. A hitelesítési eljárásnak három típusa ismert:

- Tudásalapú
- Tulajdonalapú
- Tulajdonságalapú

A kockázatokkal arányos, megbízható és erős hitelesítéshez a különböző típusú hitelesítési eljárásokat keverten, a **háromból legalább kettőt együtt** érdemes használni!

A leggyakoribb hozzáférés-vezérlési felderítő védelmi intézkedés a **behatolás detektáló rendszerek** (Intrusion Detection System – IDS) használata.

A leggyakoribb hozzáférés-vezérlési javító védelmi intézkedés a behatolástesztelés. Ekkor egy támadó képességeivel felvértezett külső vagy belső ember támadást szimulál a rendszer ellen, nulla, részleges vagy teljes rendszerismerettel. Igen hatékony megoldás a sérülékenységek felderítésére és a szervezet védelmi szintjének felmérésére. Csak megfelelő felhatalmazással és gondos tervezéssel, különböző módszertanok alapján szabad belekezdeni. Különösen vigyázni kell az éles rendszerek elleni behatolás-teszteléssel! A lehetséges módszerek:

- Biztonsági funkcionális tesztelés
- Sérülékenység-vizsgálat
- Behatolás-tesztelés
- Etikus hackelés

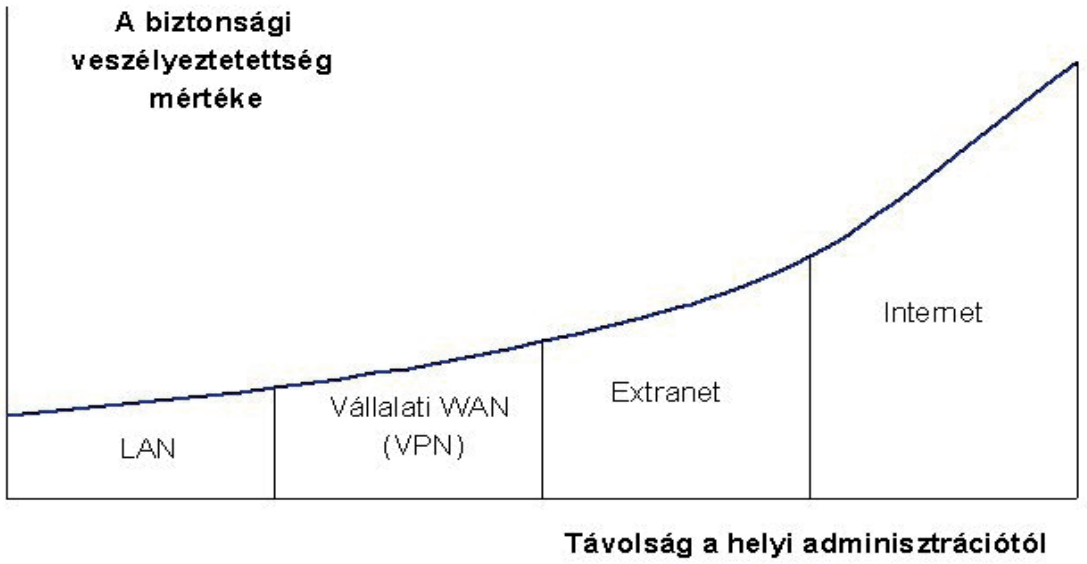
A **hozzáférés-vezérlés**ek jelentős része a közismert *kell, hogy tudja*[25] elven alapul. A *kell, hogy tudja* elv azt jelenti, hogy egy adathoz (információhoz) csak az kaphat hozzáférési engedélyt, akinek adott információhoz a feladatköre miatt szükséges hozzáférnie (szükséges és elégséges jogosultság). A hozzáférés-vezérlést engedélyező, ellenőrző eljárások úgynevezett hozzáférés-vezérlési politikák alapján működnek.

9.2. Hálózatbiztonság

A gyors adatátvitel, illetve a nagyobb teljesítmény elérése érdekében a számítógépeket egy közös kommunikációs rendszerben kapcsolják össze. A számítógép-hálózat számítógépei a rendszerben egymással adatokat, információkat cserélhetnek, illetve erőforrásaikat megosztva használhatják. Ilyen erőforrások lehetnek a fájlok, nyomtatók, stb. [18]

Az informatikai hálózatok legtöbbször stratégiai fontosságú adatokat tárolnak. Ezek bizalmasságát még akkor is meg kell őrizni, ha egyébként igény van az internet széleskörű használatára. Mint a 4. ábra mutatja, egy informatikai rendszer biztonságát bármilyen kommunikációs kapcsolat csökkenti. A biztonsági veszélyforrások az adminisztrációtól való távolság függvényében egyre jelentősebbek.

[25] Need to know



4. ábra A veszélyeztetettség mértéke [18]

Az internet használatával a csatlakozó hálózat egésze (minden egyes hálózati csomópont, illetve azokon minden egyes szolgáltatás) támadási felületet nyújt megfelelő védelem hiányában. A hálózat biztonságos üzemeltetése megfelelő rendszabályok és intézkedések bevezetésével biztosítható. [18]

A legtöbb hálózati szintű sérülékenység ellen a modern határvédelmi rendszerek kitűnő védelmet jelentenek. Az elosztott túlterheléses támadások (Distributed Denial of Service) elterjedtsége azonban jelzi, hogy korántsem sikerült még teljes egészében a hálózati támadások kezelését megoldani.

A **tűzfalak** olyan eszközök, amelyek a hálózati forgalom szűrésére szolgálnak, és mint ilyenek, a határvédelem legfontosabb építőkövei. A hálózat egy pontján kontrollálják a forgalmat, szabályok alapján. Több tűzfaltípus ismeretes, napjainkban kombinált megoldások terjednek el.

A mobilitás megjelenésével, a hordozható eszközök, okostelefonok, tabletek robbanásszerű elterjedésével fontos feladattá vált a felhasználók távoli hozzáférésének biztosítása. Ez számos problémát, kihívást jelent biztonsági szempontból, melyeket kezelni kell! A távoli hozzáférést többféleképpen meg lehet valósítani, de napjainkban szinte kizárólag az interneten keresztüli elérés dominál.

Az interneten keresztüli elérést virtuális magánhálózatok (VPN) segítségével szokás megvalósítani. Látszólag a két hálózat közvetlenül van összekötve, egy hálózatként működik. A VPN biztosítja a bizalmasságot, az adat sértetlenségét és a hitelesítést.

Szintén a mobilitás segíti elő a **vezetéknélküli hálózatok** (wireless LAN – WLAN, vagy WiFi) elterjedését. Alapvető fontosságú, hogy megfelelő csatornarejtjelzést használjunk! Ez ma a WPA2.

9.3. Alkalmazások

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. A különböző termékkel elérhető legmagasabb szintű biztonság nem az alapértelmezett beállításokkal érhető el!

Az alkalmazásokat úgy kell elkészteni, hogy az operációs rendszer megbízható felhasználó-azonosító rendszerét vagy a szervezetnél alkalmazott biztonsági szerver hasonló szolgáltatásait vegye igénybe.

Az egyéb kiegészítő és segédprogramok – minden praktikus hasznuk mellet – számos 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.

9.4. A rejtjelzés, a digitális aláírás és az elektronikus tanúsítványok

A *kriptológia* az adatok, üzenetek *rejtjelzés*ével (kódolás, sifrírozás) és *megfejtésével* (rejtjelfejtés, dekódolás, desifirozás) foglalkozó tudományág, a matematikai tudományok egyik részterülete.

9.4.1. Szimmetrikus rejtjelző algoritmusok

A klasszikus rejtjelző eljárások egyetlen kulcsot használnak rejtjelzésre és megoldásra. A szimmetrikus rejtjelző eljárások közül a 128–256 bit kulcshosszúságú AES rejtjelzőeljárás az elfogadott, ezen kívül a 128–256 bit kulcshosszúságú Twofish, a 128–256 bit kulcshosszúságú Serpent vagy a 128 bit kulcshosszúságú IDEA eljárást, algoritmusokat tartja a szakma kellően erősnek. A 168 bit kulcshosszúságú Triple DES titkosítás még megjelenhet a gyakorlatban, de használata nem ajánlott.

9.4.2. Nyilvános kulcsú rejtjelzés

„Olyan kriptográfiai rendszerben használják, amelybe bárki beléphet résztvevőként. A rejtjelző és a megoldó algoritmus azonos és a rejtjelzéshez, illetve a visszafejtéshez kulcspárt használ. Az egyik kulcs a *nyilvános kulcs*, amivel a rejtjelzést 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." [19] Az ezt a filozófiát megvalósító rendszerek gyűjtőneve: *Nyilvános kulcsú rendszerek* (public key cryptosystems).

9.4.3. 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 rejtjelzésen 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." [19]

9.4.4. 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 a *hitelesítésszolgáltatón,* vagy közismert nevén a Certificate Authority-n (CA) alapuló rendszer. A CA egy digitális közjegyző szerepét játssza. A CA igazolja, hogy egy adott azonosítóval rendelkező felhasználó az, akinek vallja magát.

A CA tanúsítvány bocsájt ki, amelyek tartalmazzák az adott entitáshoz tartozó nyilvános kulcsot, az entitás nevét (személyazonosítóját), az érvényesség (lejárat) idejét. Ezt írja alá a saját 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 rejtjelzés, a digitális aláírások és a CA-alapú kulcskezeléssel elméletileg magas biztonsággal oldható meg.

A hitelesítés-szolgáltatónak feladata ellátásához rendkívül szigorú biztonsági feltételeket kielégítő infrastruktúrával kell rendelkezni.

9.4.5. Kriptográfiai protokollok

„A gyakorlatban legismertebb komplex protokoll az interneten két gép közötti bizalmasság és hitelesség biztosítására használt *SSL-protokoll* (az újabb változat neve TLS). Manapság egyre több helyen alkalmaznak különböző digitális pénzt kezelő protokollokat is (E-cash, Digicash, Micromint).” [19]

9.5. Rosszindulatú programok

A vírusvédelemmel kapcsolatos folyamatokat, teendőket és kötelezettségeket írásos dokumentumban kell rögzíteni, ami alapján munkajogi felelősségre vonást lehet érvényesíteni.

„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.” [20]

„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.” [20]

„A vírusvédelmi politikában komoly figyelmet kell fordítani a munkatársak megfelelő szintű tájékoztatására. … Ha a munkatársak kellő odafigyelést tanúsítanak a problémával kapcsolatban, akkor nagymértékben csökkenteni lehet a műszaki megoldások hatékonyságától való függést.” [20]

9.6. Az üzemeltetés biztonsági kérdései

A biztonságot nem elég „megvenni”, azt fent is kell tartani. Az információbiztonság tehát nem egy atomi esemény, hanem egy életcikluson átívelő folyamat. A rendszer életciklusának leghosszabb része az üzemeltetés, emiatt különösen fontos az üzemeltetés biztonságával foglalkozni.

Az üzemeltetés átfogja a rendszer egészét. Tartalmazza a hardverek, a szoftverek, a kommunikációs eszközök, az adathordozók karbantartását, valamint ezen eszközök konfigurációmenedzsment-eljárásait.

Az egyik legfontosabb biztonsági üzemeltetési feladat az elektronikus információs rendszerek sérülékenységeinek kezelése, azaz a biztonsági frissítés.

A naplózás, azaz az infrastruktúrában történt események rögzítése, információt nyújt az informatikai elemek általános állapotáról csakúgy, mint a biztonságilag fontos történésekről, nélkülözhetetlen a szabálysértések azonnali érzékeléséhez és a későbbi kivizsgáláshoz.

Az információ életciklusának a végén gondoskodni kell arról, hogy az adott információk biztonságos megsemmisítésre kerüljenek.

10. Ellenőrzés, auditálás, kockázatelemzés

10.1. Az informatikai rendszerek biztonsági ellenőrzése

„Az informatikai biztonsági ellenőrzések alapvető célja, hogy **objektív** információkat biztosítsanak a felelős vezetők számára az informatikai biztonság helyzetéről, amelyek alapján a kockázatok csökkenthetők és a rendkívüli események elkerülhetővé vállnak." [21]

„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." [21]

Az informatikai biztonsági ellenőrzések típusai [21]:

- *informatikai biztonsági vizsgálat* (fenyegetettség, védelmi képesség elemzése kockázatelemzéssel),
- *auditálás* (meghatározott követelményeknek való megfelelés vizsgálata),
- *informatikai biztonsági tanúsítás és minősítés* (például a Common Criteria EAL2 osztálya követelményeinek való tanúsított megfelelés).

10.2. A kockázatelemzés

„A kockázatelemzés olyan elemző és értékelő jellegű szakértői vizsgálat, amely az informatikai rendszerekben kezelt adatok és alkalmazások értékelése, gyenge pontjainak és fenyegetettségeinek elemzése útján meghatározza a potenciális kárértékeket és azok bekövetkezési gyakoriságát.

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." [17]

Az **ISO/IEC 27005:2011** útmutatást ad a biztonsági kockázat kezeléséhez. A szabvány nem nevez meg semmilyen konkrét kockázatelemzési módszert!

A kockázatelemzés kapcsán a sokat emlegetett **ISO 31000:2009** és az ISO/IEC 31010:2009 nem a kockázatelemzésről, hanem a vállalatirányítási rendszer hatékonyabbá tételét szolgáló kockázatkezelésről szól!

A KIB 25. számú ajánlásának **Informatikai Biztonsági Irányít**ásának **Vizsgálata** kötetében [22] leírt kockázatelemzési módszertan a brit CRAMM[26] módszertan adaptációja. A kockázatelemzésen alapuló módszer egy olyan modellen nyugszik, amelynek a középpontjában a védendő alapérték, az informatikai rendszerben kezelt adatok által hordozott információk állnak.

Valamely informatikai rendszer biztonságának kockázatelemzésen alapuló vizsgálata során elsőként a meglévő, potenciálisan fenyegetett értékeket kell feltérképezni és újraértékelni. Ezután a várható következményeket kell feltárni. Valamennyi feltárt fenyegető tényezőt értékelni kell. Az értékelés függ a kár bekövetkezésének várható **valószínűség**étől és a bekövetkezett **kár nagyság**ától, amennyiben a fenyegető tényező kifejtheti hatását. Ebből a két részből tevődik össze a **kockázat**.

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 informatikai rendszerekre és környezetükre ható fenyegetések által okozott kockázatok felmérése és minősítése után olyan **védelmi intézkedések**re kell javaslatot tenni, amelyek minimális költségszint mellett maximális kockázatcsökkentést eredményeznek.

[26] CCTA Risk Analysis and Management Method

10.3. Kockázatkezelés

A kockázatkezelési intézkedések célja: azoknak a biztonsági kockázatoknak az elfogadható/méltányos költségen történő azonosítása, kézbentartása, minimalizálása vagy megszüntetése, amelyek hatással lehetnek információrendszerekre.

A kockázatkezelés olyan védelmi intézkedések kidolgozása, elemzése és meghozatala, amelyet követően a maradványkockázatok elviselhető szintűre változnak.

10.4. Az informatikai biztonság auditálása

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).

10.5. Informatikai biztonsági tanúsítás

Az Európai Közösség országaiban elfogadott informatikai biztonsági tanúsítás követelményrendszere az ISO/IEC 27001 vagy a CC.

11. Irodalom

Muha Lajos – Bodlaki Ákos (2007): Az informatikai biztonság, PRO-SEC KFT, Budapest, 176 p.

Muha Lajos (2007): A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, PhD értekezés, ZMNE, Budapest, 127 p.

Muha Lajos: Az Informatikai Biztonsági Irányítási Rendszer. In: Az Informatika Korszerű Technikái Konferencia, Dunaújváros, 2010.03.05-2010.03.06., 156–164. pp.

Muha Lajos: Az informatikai biztonság meghatározása (3.3. fejezet). In: Muha Lajos (szerk., 2004): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig. Verlag Dashöfer Szakkiadó, Budapest.

Muha Lajos (2008): Az informatikai biztonság egy lehetséges rendszertana. In: Bolyai Szemle, XVII. évfolyam, 4. szám, Budapest.

Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) 12. számú ajánlása. Bodlaki Ákos – Csernay Andor – Mátyás Péter – Muha Lajos – Papp György – Vadász Dezső (1996): Informatikai Rendszerek Biztonsági Követelményei. Budapest, 217 p.

Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.)

Zöld Könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról. Európai Bizottság, Brüsszel, 2005. http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52005DC0576&rid=20 (Utolsó letöltés: 2018.04.16.)

Muha Lajos: Kiberhadviselés – kiberbűnözés. In: IDC IT Security Konferencia, Budapest, 2012.03.22.

Joint Publication 1-02, Dictionary of Military and Associated Terms, Department of Defense, USA, 2010/2013

Szádeczky Tamás (2008): Terrorizmus a kibertérben. In: Infokommunikáció és jog, , 5. évfolyam, 6. szám, Budapest, 200–205. pp.

Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat

Muha Lajos: Az informatikai biztonság jogi szabályozása (3.4. fejezet). In: Muha Lajos (szerk., 2004): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig. Verlag Dashöfer Szakkiadó, Budapest.

Szádeczky Tamás (2014): Információbiztonsági szabványok. Egyetemi jegyzet, Nemzeti Közszolgálati Egyetem, Budapest, 50 p.

Berkes Zoltán – Déri Zoltán – Krasznay Csaba – Muha Lajos (2008): Informatikai Biztonsági Irányítási Rendszer (IBIR). Miniszterelnöki Hivatal, Budapest, 96 p. (Közigazgatási Informatikai Bizottság ajánlásai; 25./1-1.)

Komor Levente – Nagy Béla: Az emberi tényező jelentősége az informatikai biztonságban (5.5. fejezet). In: Muha Lajos (szerk., 2000): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig. Verlag Dashöfer Szakkiadó, Budapest.

Déri Zoltán – Lobogós Katalin – Muha Lajos – Sneé Péter – Váncsa Julianna (2008): Informatikai Biztonság Irányítási Követelmények (IBIK). Miniszterelnöki Hivatal, Budapest, 275 p. (Közigazgatási Informatikai Bizottság ajánlásai; 25./1-2.)

Endrédi Gábor: Hálózatok (5.8.2. fejezet). In: Muha Lajos (szerk., 2000): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig. Verlag Dashöfer Szakkiadó, Budapest.

Nemetz Tibor: A rejtjelzés, az elektronikus dokumentumok azonosítása és a digitális aláírás (6.4. fejezet). In: Muha Lajos (szerk., 2004): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig. Verlag Dashöfer Szakkiadó, Budapest.

Farmosi István: Vírusok és más logikai támadó eszközök (6.6. fejezet). In: Muha Lajos (szerk., 2000): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig. Verlag Dashöfer Szakkiadó, Budapest.

Muha Lajos: Az informatikai rendszerek biztonsági ellenőrzése (5.9.1. pont). In: Muha Lajos (szerk., 2001): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig. Verlag Dashöfer Szakkiadó, Budapest.

Balázs István – Déri Zoltán – Lobogós Katalin – Muha Lajos – Nyíry Géza – Sneé Péter – Váncsa Julianna (2008): Informatikai Biztonság Irányításának Vizsgálata (IBIV). Miniszterelnöki Hivatal, Budapest, 324 p. (Közigazgatási Informatikai Bizottság ajánlásai; 25./1-3.)

A Nemzeti Közszolgálati Egyetem kiadványa.

Nemzeti Közszolgálati Egyetem;
Államtudományi és Közigazgatási Kar
www.uni-nke.hu

Felelős Kiadó:
Prof. Dr. Kis Norbert Dékán

Címe:
1083 Budapest, Üllői út 82.

Kiadói szerkesztő:
Kiss Eszter

Tördelőszerkesztő:
Bödecs László

978-615-5870-26-2 (PDF)

A hatályosított tananyag
a KÖFOP-2.1.1-VEKOP-15-2016-00001
„A közszolgáltatás komplex kompetencia,
életpálya-program és oktatás technológiai
fejlesztése” című projekt keretében készült
el és jelent meg.

Európai Unió
Európai Szociális
Alap

BEFEKTETÉS A JÖVŐBE