Nemzeti
Közszolgálati Egyetem

Vezető- és Továbbképzési Központ

MUHA LAJOS – KRASZNAY CSABA

Az elektronikus információs rendszerek biztonságának menedzselése

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. március 26.

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

1. Tartalom

1. Bevezetés

A modern állam, annak minden szervezete és polgára szükségszerűen felhasználója a számítógépekből, kommunikációs eszközökből és automata rendszerekből álló bonyolult, többszörösen összetett elektronikus információs infrastruktúráknak, melyek az élet minden területén megjelennek. Magyarország közigazgatásának működésében ma már elengedhetetlenül fontos szerep jut az elektronikus információs rendszereknek, és ezen rendszerek biztonságos működése nemzetbiztonsági szempontból kiemelt kérdés, hiszen nélkülük az ország gazdasági és társadalmi működése jelentős akadályokba ütközne.

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 úgynevezett hackereknek) és adott esetben akár más államok hivatalos szerveinek. Tudomásul kell vennünk, hogy információs rendszereink és hálózataink egyre gyakrabban szembesülnek sokféle forrásból származó biztonsági fenyegetéssel, többek között gazdasági hírszerzéssel, ipari kémkedéssel, számítógépes csalással, szabotázzsal, vandalizmussal, tűzzel vagy árvízzel. A szándékos károkozások olyan formái, mint a számítógépvírusok, a számítógépes betörések, vagy a szolgáltatás kimaradására, megtagadására vezető támadások egyre gyakoribbá, általánosabbá válnak, ugyanakkor ezek egyre vakmerőbbek és egyre bonyolultabbak is. 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

2. Az elektronikus információs rendszerek biztonságának fogalma és tartalma

2.1. Az elektronikus információs rendszerek védelmének megjelenése, fejlődése

„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."[1]

Ugyanakkor mind bonyolultabb, mind nagyobb kiterjedésű elektronikus információs rendszerek alakulnak ki. Az állam és a társadalom működése – a gazdaság és a közigazgatás mellett számos más területen is – jelentős arányban épül az elektronikus információs rendszerekre. A modern társadalmak, így Magyarország is, nagymértékben függenek az egymással szoros kapcsolatban álló létfontosságú információs infrastruktúráktól.

Az elmúlt évtizedben bekövetkezett terrortámadások (New York WTC, Madrid, London), természeti katasztrófák (ázsiai szökőár, földrengések, Fukushima,) és egyéb technikai kihívások (kétezredik évi dátumváltás, nagykiterjedésű áramkimaradások), különösen az utóbbi időben egyre gyakrabban bekövetkező kibertámadások (például a 2007-es Észtország elleni kibertámadások) felhívták a figyelmet a létfontosságú információs rendszerek és rendszerelemek, valamint az ezekben kezelt elektronikus információk sebezhetőségére, valamint az infrastruktúrák, a társadalom és kormányzati működés kölcsönös egymásrautaltságára. E rendszerek működési zavarai, illetve egyes elemeinek, valamint a kezelt információknak az ideiglenes kiesése, megsemmisülése vagy bizalmasságának sérülése jelentős kihatással vannak mindennapi életünkre, a gazdaság, a közigazgatás hatékony működésére, a lakosság életére.

„A modern állam, annak minden szervezete és polgára kiszolgáltatottá vált a számítógépekből, kommunikációs eszközökből és automata rendszerekből álló bonyolult, többszörösen összetett információs infrastruktúrának. Napjainkban ezen eszközök nélkül életünk elképzelhetetlenné vált. Vezetékes és mobil telefonon tartjuk szeretteinkkel a kapcsolatot, ha pénzre van szükségünk, a bankjegykiadó automatához (ATM) fordulunk, amelynek a lényege egy személyi számítógép, ami vezetékes telefonvonalon keresztül a bankunk vagy az elszámoló központ számítógépére csatlakozik, és digitális kommunikációjuk dönti el, hogy kaphatunk-e készpénzt az automatából vagy sem. Munkahelyünkön a munkánkhoz szükséges adatok jelentős része a számítógépen van tárolva. A legtöbb esetben már nem is a saját asztali számítógépünkön, hanem távol, néha több száz vagy ezer kilométerre lévő központi számítógépeken. Ezek a számítógépeken tárolt adatok teszik lehetővé, hogy például a villamosenergia-szolgáltatónk átlássa, hol mennyi áramra van szükség, és honnét tudja azt beszerezni. Ha ezekben a rendszerekben bárhol, bármilyen hiba adódik, máris elindul egy dominóhatás. Villamos energia nélkül más számítógépek is leállnak, sötétség lesz, de még hideg is, mert az elektromosan vezérelt gázfűtésünk is leáll. Ha nem működnek a bankjegykiadó automaták, akkor még a vésztartalék petróleumlámpával világító üzletben sem tudjuk alapvető létszükségleti cikkeinket beszerezni. Ez olyan káoszba torkollhat, amelynek kimenetele nehezen jósolható meg.

Tudomásul kell vennünk, hogy információs rendszereink egyre gyakrabban szembesülnek az igen sokféle forrásból származó biztonsági fenyegetéssel, többek között gazdasági hírszerzéssel, ipari kémkedéssel, számítógépes csalással, szabotázzsal, vandalizmussal, tűzzel vagy árvízzel. A szándékos károkozások olyan formái, mint a számítógépvírusok, a számítógépes betörések vagy a szolgáltatás-megtagadásra vezető támadások egyre gyakoribbá, általánosabbá válnak, ugyanakkor ezek egyre vakmerőbbek és egyre bonyolultabbak is. Egyre nagyobb fenyegetést jelent sérülékeny információs rendszereinkre a hadviselés új formája, az információs hadviselés, de még inkább a békeidőkben is állandóan fenyegető terrorizmus számítógépes változata, a kiberterrorizmus." [2]

„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. A különböző szervezetek rájöttek, és mára alapvető elvárássá vált, hogy az információs rendszerek által kezelt adatok védve legyenek és biztonságosan legyenek használhatók, hogy magukat az információs rendszereket, azok információ- és kommunikációtechnológiai eszközeit is úgy kell kialakítani, hogy megfelelő védelmet biztosítsanak. Az informatikai rendszerek biztonsága érdekében hozott, jól megválasztott védelmi intézkedések segítenek károk megelőzésében, csökkentésében, és a kárfelszámolás meggyorsításában – sikeressé tehetik a szervezetet." [3]

2.2. A védelem és a biztonság

„A védelem – a magyar nyelvben – tevékenység, illetve tevékenységek sorozata, amely arra irányul, hogy megteremtse, fejlessze, vagy szinten tartsa azt az állapot, amit biztonságnak nevezünk[1]. Tehát **a védelem tevékenység, amíg a biztonság egy állapot**. Az (amerikai) angol nem tesz különbséget a biztonság és a védelem között, általában mindkettőre a security[2] szót használja[3]." [2] Ennek ellenére a mindennapos szóhasználat a védelemre, a védelmi tevékenységre is a biztonság kifejezést használja!

„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**[4], 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. Természetesen a gyakorlatban rendelkeznek egymásról több-kevesebb, valós vagy valósnak vélt információval. Az 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[5] és a védő vesztesége[6] sohasem egyenlítik ki egymást. [4] 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." [5]

„A biztonság értelmét, tartalmát sokan sokféleképpen magyarázzák. Azt hiszem, hogy *„A biztonság olyan kedvező állapot, amelynek megváltozása nem valószínű, de nem is zárható ki ..."*[7] megfogalmazás értelmetlensége magyarázatot nem igényel. A Magyar Értelmező Kéziszótár szerint *„a biztonság veszélytől vagy bántódástól mentes, zavartalan állapot"* [6]. Ezt a megfogalmazást is elég nehéz tudományos és műszaki szemlélettel elfogadni, mert zavartalan állapot – mint tudjuk – nem létezik, másrészt nem a zavar teljes hiánya, hanem valamilyen *még elviselhető* mértéke és bekövetkezésének gyakorisága az, ami már valamilyen szinten biztonságnak tekinthető. Elfogadva, hogy a biztonság egy *kedvező állapot*, amellyel szemben elvárható, hogy a fenyegetések bekövetkezésének lehetősége, valamint az esetlegesen bekövetkező fenyegetés által okozott kár a lehető legkisebb legyen. Ahhoz azonban, hogy teljes legyen ez a biztonság, az szükséges, hogy minden valós fenyegetésre valamilyen védelmet nyújtson, ugyanakkor körkörös legyen, vagyis minden támadható ponton biztosítson valamilyen akadályt a támadó számára. Mindezek mellett elvárható, hogy folyamatosan létezzen." [2].

---

1 A teljesség kedvéért megjegyezzük, hogy a magyar nyelvben az igéből képzett főneveknek, így a „védelem" kifejezésnek is két szemantikai reprezentációja lehet: jelenthet eseménytípust, tehát kategóriát vagy halmazt, mint általában a főnevek; jelentheti egy esemény eredményét, ami ebben az esetben a biztonság.

2 A biztonságra a safety szót is használja környezet-, munka- és egészségvédelmi dimenzióban.

3 A protection ugyan védelmet jelent, de azt ritkán (például data protection – a személyes adatok védelme) használja a szakirodalom.

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

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

6 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

7 Csík B. et al. (2003): Az informatikai biztonság fogalmainak gyűjteménye, BME GTK, Budapest.

„A fentiek alapján a biztonság a rendszer olyan – az érintett[8] számára kielégítő – állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg." [7]

„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**." [8]

„**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 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." [2]

A fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye. [11] A kockázatot mint elvont fogalmat szokták alkalmazni, ám az formálisan is definiálható:

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

ahol:

r: a kockázat [Ft/év],

T: a releváns fenyegetések halmaza,

$\mathbf{d_t}$: egy adott kockázat bekövetkezéséből származó kár [Ft],

$\mathbf{p_t}$: egy, a fenyegetett által okozott kár bekövetkezésének várható éves gyakorisága [1/év].

Ezt a pénzügyi kockázatkezeléseknél várható éves veszteségnek is nevezik.[9]

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 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]

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 elsődlegesen alkalmazott védelmi intézkedéseknek a rendszer más elemire 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. " [5]

---

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

[9] Angolul: Annualized Loss Expectancy (ALE).

2.3. Elektronikus információs rendszerek

„Az elektronikus információs rendszerek eszközei – a számítástechnikai, a kommunikációs és az egyéb elektronikus eszközök – közötti konvergenciát az informatikával és a távközléssel foglalkozó szakemberek már több mint egy évtizede vizsgálják. Az információs társadalomhoz és a médiához kötődő iparágak konvergenciáját már az Európai Unió által 1997-ben kiadott, *Zöld Könyv a távközlési, média és informatikai ágazatok konvergenciájáról és annak szabályozási kihatásairól* [9] leírta, később pedig – az újabb fejleményeket is figyelembe véve – az európai audiovizuális politika szabályozásának jövőjéről szóló 2003-as közlemény aktualizálta. A közlemény megállapítja, hogy *„Az információs társadalom fordulóponthoz érkezett: az elmúlt időszakban hatalmas technológiai fejlődés zajlott le, és az IKT*[10] *napjainkban lép a tömeges alkalmazás szakaszába… Műszaki szempontból a távközlési hálózatok, a médiumok, a tartalom, a szolgáltatások és az eszközök digitális konvergenciájával állunk szemben. … Az* **információs társadalom és a média területén működő szolgáltatások, hálózatok és eszközök digitális konvergenciája** *végre mindennapjaink valóságává válik… A technológiában zajló alapvető változások… a* **politikában** *is* **konvergenciát** *tesz szükségessé, és késznek kell lenni arra, hogy a szabályozási keretet a kialakulófélben lévő digitális gazdaság igényei szerint alakítsuk”.*”[10]

Sokszor csak a számítógép- és távközlési rendszereket értik ez alatt, de ténylegesen ide tartozónak kell tekintenünk minden olyan elektronikus eszközt vagy rendszert, amely adatok[11] feldolgozására szolgál. [2]

Az információ- és kommunikációs technológiák[12] fent bemutatott konvergenciája miatt mára elterjedten használják az *informá*ció *és kommunikációs technológia* kifejezést és annak IKT vagy angolosan ICT rövidítését. Összhangban az információbiztonsági törvénnyel [11] 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”[13].

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 adatgyűjtő14, 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.

2.4. Az információbiztonság

„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 kifejezés – érdekes módon az angol nyelvben (data protection) is – a személyes adatok védelmére vonatkozik, a személyiségi jogokkal összefüggő tevékenység. Az információbiztonság és az elektronikus információs rendszerek biztonsága különbözik egymástól. 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

---

[10] IKT: információs és kommunikációs technológiák

[11] Információ: Bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságot csökkent vagy szüntet meg. Adat: Az információnak olyan új formában való ábrázolása, amely alkalmas közlésre, értelmezésre, vagy feldolgozásra. Tények, fogalmak vagy utasítások formalizált ábrázolása, amely alkalmas az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra. [12]

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

[13] 2013. évi L. törvény 1.§ (1) bek.

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

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.)" [7]

„Általában a szövegkörnyezet egyértelművé teszi, hogy információvédelemről vagy elektronikus információs rendszerek védeleméről van szó. Például az ISO/IEC 27001:2005 nemzetközi szabvány [13] eredeti angol címe az *Information technology – Security techniques – Information security management systems – Requirements*, aminek a kezdetén lévő *Information Technology* kifejezés – számomra – egyértelművé teszi, hogy itt az informatikáról van szó, majd ez után következik az *Information security*, ami így informatikai biztonságot (az elektronikus információs rendszerek biztonságát) jelent magyarul. Ezt a magyar szabványban [14] szó szerint információbiztonságnak fordították. (Sajnos a vonatkozó magyar szabványokban nem ez az egyetlen, és nem is a legnagyobb fordítási hiba.)

Az információvédelem tartalmának meghatározására a NATO védelmi előírásában [28] szereplő definíció tűnik a legjobbnak. E szerint „**az információvédelem az általános védelmi rendszabályok és eljárások alkalmazása az információ megsemmisülésének vagy kompromittálódásának megelőzése, felfedése ellen és helyreállítása céljából.**"[15] Az egyértelműség (?) kedvéért a NATO bevezette az INFOSEC kifejezést, amelyet az *information security* kifejezés szavainak összevonásával (INFOrmation SECurity) képeztek. Ezt a vonatkozó magyar szakirodalmakban általában *elektronikus információvédelem* vagy néha *elektronikus dokumentumvédelem* formában használják. Az INFOSEC *„a biztonsági rendszabályok alkalmazása a kommunikációs, információs és más elektronikus rendszerekben a feldolgozott, tárolt vagy továbbított információ bizalmasságának, sértetlenségének vagy rendelkezésre állásának véletlen vagy szándékos elvesztése ellen, és e rendszerek sértetlenségének vagy rendelkezésre állásának elvesztése ellen"*[16]. Ez a meghatározás egyértelmű – az információs és kommunikációs rendszerek, illetve az azokban kezelt adatok védelmére vonatkozik." [7]

Azonban ez az elektronikus információvédelem önmagában nem kezelhető, mert egy igen széles körű információvédelem része. Az elektronikus információs rendszerek védelme (informatikai védelem) pedig az információvédelemnél szűkebb, de „önállóan" is működtethető szakterület, amely a NATO INFOSEC-ben is meghatározott elektronikus információvédelmen kívül az információvédelem többi részét is magába foglalja, de csak az elektronikus információs rendszerek vonatkozásában. Más szóval az információvédelem olyan területeit, mint a személyi védelem, a dokumentumvédelem, a fizikai védelem és a hírszerzés (felderítés), illetve elhárítás (felderítés elleni tevékenység) az elektronikus információs rendszerek védelme esetében csak az elektronikus információs rendszer és elemei vonatkozásában, azokkal kapcsolatban alkalmazzuk. Az elektronikus információs rendszer védelemének ki kell terjedni az elektronikus információs rendszer valamennyi elemére[17], de nem feltétlenül a teljes információs rendszerre. Azaz az elektronikus információs rendszer védelme az információvédelemnél szűkebb, de „önállóan" is működtethető szakterület, amely a NATO INFOSEC-ben is meghatározott elektronikus információvédelmen kívül az információvédelem többi részét is magába foglalja, de csak az elektronikus információs rendszer vonatkozásában.

Az 1. ábrán az elektronikus információs rendszer védelme és az információvédelem egymáshoz való viszonyát mutatjuk be.

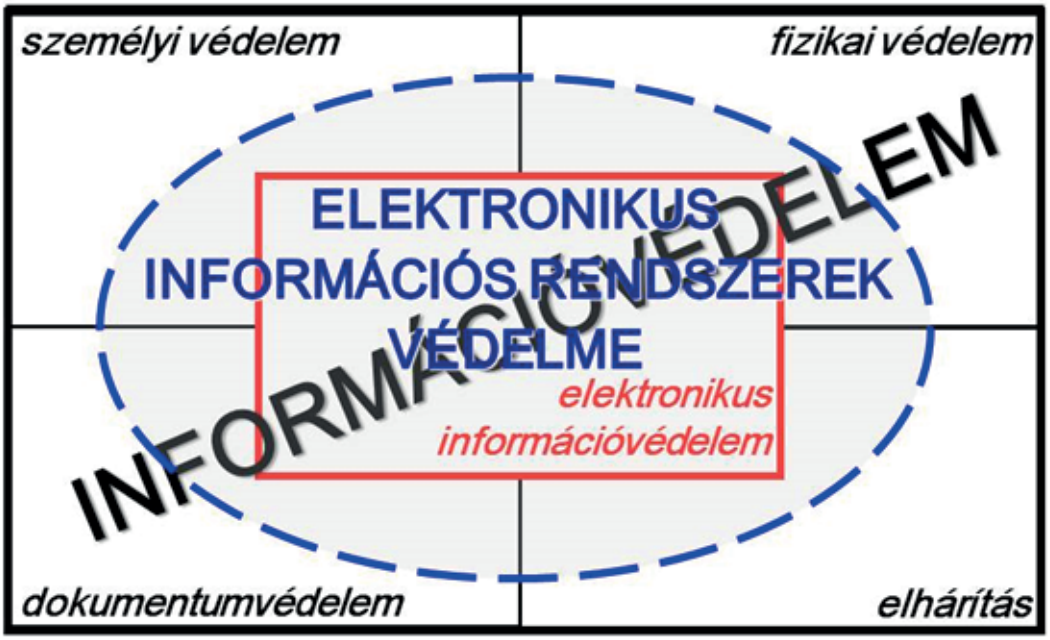
Azonban ez az elektronikus információvédelem önmagában nehezen kezelhető, mert egy igen széles körű információvédelem része.

---

[15] Angolul: „Security of information is the application of general protective measures and procedures to prevent, detect and recover from the loss or compromise of information" [28]

[16] Angolul: „INFOSEC is the application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems against loss of confidentiality, integrity or availability, whether accidental or intentional, and to prevent loss of integrity or availability of the systems themselves." [28]

[17] A rendszerelemek az informatikai rendszert és működési környezetét alkotó és működéséhez szükséges erők és eszközök (infrastruktúra, hardver, szoftver, dokumentáció és a rendszer kezelői, kiszolgálói és felhasználói stb.). A pontos definíciót lásd később.



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

2.5. Az elektronikus információs rendszerek biztonsága

Az előzőek alapján az elektronikus informatikai rendszerek védelme a rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint a rendszer elemei sértetlenségének és rendelkezésre állásának megóvása.

„A biztonság fenti meghatározását elfogadva levezethetjük az elektronikus információs rendszer biztonságának[18] fogalmát. „Ehhez kiindulópont, hogy **a védelem alapvető** tárgya az **adat,** de az adatot kezelő rendszerelemek is védendőek, hiszen ezek megfelelő állapota feltétele az adat védelmének. Mint már rögzítettük, a fenyegetések az *adatok bizalmasságát, sértetlenségét és rendelkezésre állását* veszélyeztetik, de nem közvetlenül érik az adatokat, hanem az azokat kezelő *rendszerelemeken* (például a hardver, szoftver, hálózat, személyek,…) keresztül érvényesülnek.” [7]

Ennek figyelembe vételével, a biztonság általános definíciója alapján az elektronikus információs rendszerek biztonságát a következőképpen határozhatjuk meg: „**Az elektronikus információs rendszer biztonsága az elektronikus információs rendszer olyan** – az érintett[19] számára kielégítő mértékű – **állapota, amelyben annak védelme az elektronikus inform**ációs **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**.”[20] [7], [2]

Ahol az információbiztonsági törvény szerint:

- Bizalmasság[21]: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt[22] adatot, információt csak az arra jogosultak és csak a jogosultságuk szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról. [7], [2]
- Sértetlenség[23]: 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[24]) és a származás

[18] A továbbiak informatikai biztonság alatt is az elektronikus információs rendszer biztonságát értjük.
[19] Az érintett alatt a védelem nem kielégítő megvalósítását elszenvedő, a védelmet előíró, továbbá a védelemért felelős személyek és szervezetek együttese értendő.
[20] Az „érintett számára kielégítő mértékű” kifejezés a 2013. évi L. törvényben nem szerepel.
[21] Angolul: confidentiality
[22] Helyesebb lenne a „kezelt” kifejezés.
[23] Angolul: integrity
[24] Angolul: authenticity

ellenőrizhetőségét, bizonyosságát (letagadhatatlanság[25]) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható. [7], [2]

– Rendelkezésre állás[26]: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.[27]

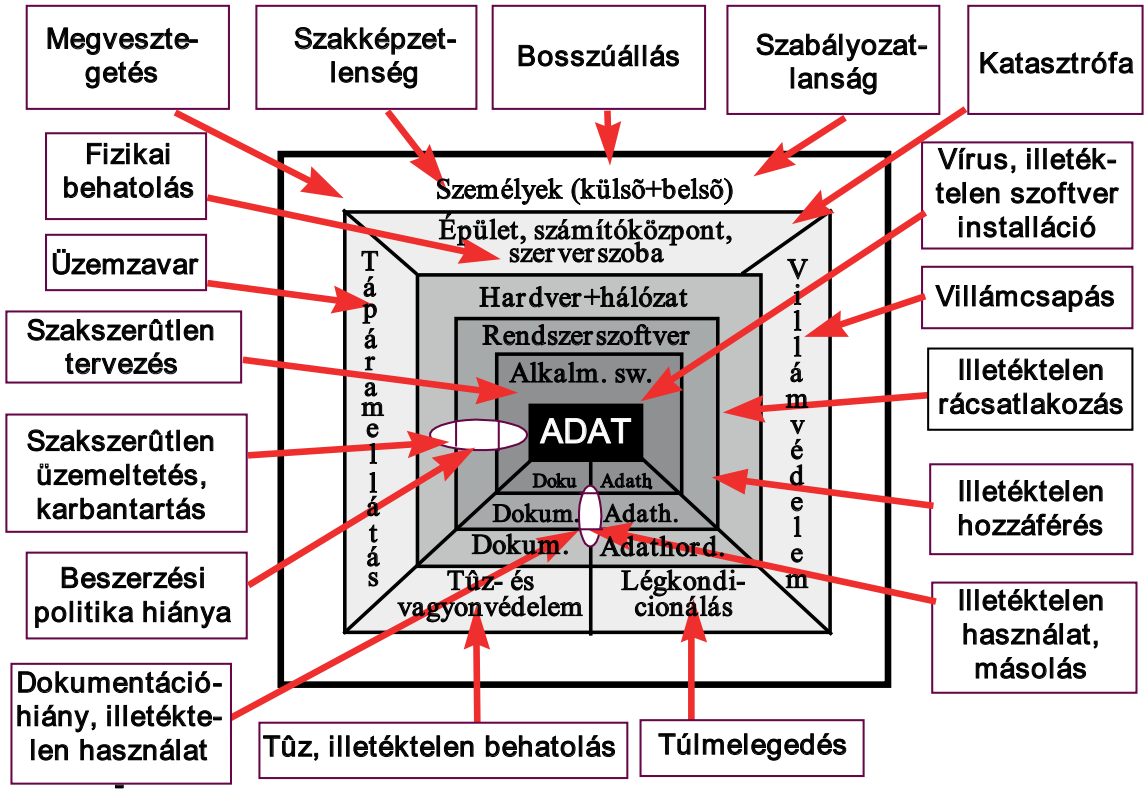
A bizalmasság, a sértetlenség és a rendelkezésre állás hármasát szokták az angol kezdőbetűik (*Confidentiality, Integrity, Availability*) alapján *CIA-elvnek* nevezni.

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

– az informatikai rendszer fizikai környezete és infrastruktúrája,
– hardver,
– kommunikáció, hálózat,
– adathordozók,
– szabályozás,
– szoftver,
– személyi környezet.

E rendszerelemekre különböző fenyegetések hatnak, amelyek a rendszerelemek meghatározott láncán keresztül az adatokat veszélyeztetik. A következő 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.

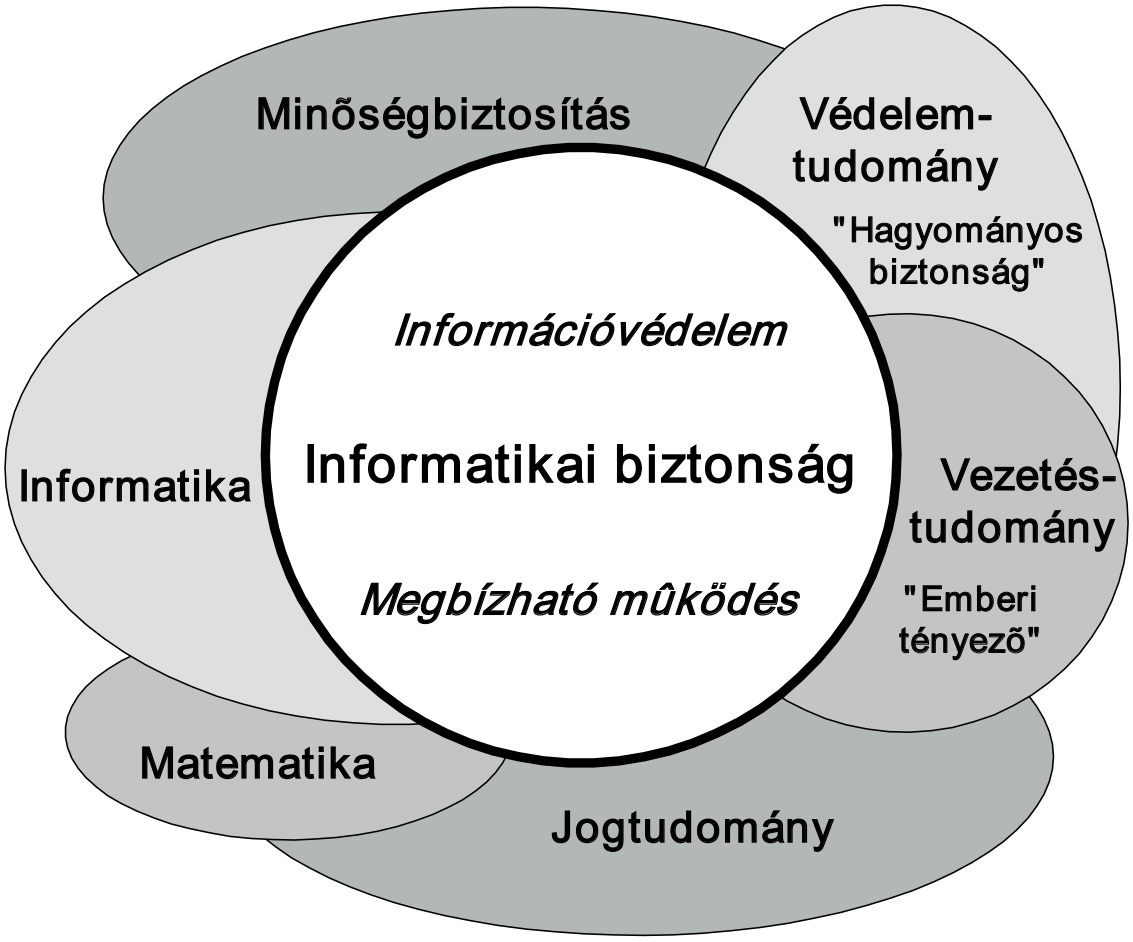


2. ábra Az elektronikus információs rendszer védelmi modellje [8]

A fentiekből egyértelműen látható, hogy az elektronikus információs rendszerek biztonságának témaköre szerteágazó, összetett kérdéskörökkel foglakozó 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.

[25] Angolul: non-repudiation
[26] Angolul: availability
[27] 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.” [7]

A következő ábra az elektronikus információs rendszerek biztonsága és a társtudományok egymáshoz képest való „elhelyezkedését” ábrázolja.



3. ábra Az elektronikus információs rendszerek biztonsága és a társtudományok viszonya [13]

Az elektronikus információs rendszerek biztonsága az informatikának csak egyes részterületeivel foglalkozik, ugyanakkor nemcsak az informatikához, hanem más szakterületekhez, tudományágakhoz is kapcsolódik, azaz tipikus multidiszciplináris szakterület.

A jogtudományhoz az elektronikus információs rendszerek biztonsága 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 (hadtudomány, rendészettudomány) 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 elektronikus információs rendszerek biztonsága. A biztonságpolitika és a védelmi stratégiák kialakításában is jelentős szerepe van a védelemtudománynak.

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 elektronikus információs rendszerek biztonságával. 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 elektronikus információs rendszerek biztonságával, 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 figyelembe vételével – megvalósult, ott az elektronikus információs rendszerek biztonságának helyzete is jó, és fordítva, ahol az elektronikus információs rendszerek biztonságát a szabványok és ajánlások szerint megvalósították, ott a minőségbiztosítási rendszer is működőképes.

A matematika sok kérdésben felhasználandó az elektronikus információs rendszerek biztonsága területén. Gondoljunk csak az előzőekben megismert játékelméleti modellre, de például a rejtjelzés (kriptográfia), az egyedi, illetve kölcsönös hitelesítési vagy integritási eljárások mint a matematikai tudományok ágai kerülnek felhasználásra az elektronikus információs rendszerek biztonságának megvalósításában.

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

2.6. A kritikus információs infrastruktúrák védelme és a kibervédelem

2.6.1. A kritikus információs infrastruktúrák védelme

A kritikus információs infrastruktúrák védelme[28] kifejezés magyarosabban a létfontosságú információs infrastruktúrák védelmét, vagy a 2013. évi L. törvény szerint a *létfontosságú információs rendszerelemek védelmé*t jelenti.

Hazánkban a kritikus infrastruktúrák[29] 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 Stratégiá*járól szóló 1139/2013. (III. 21.) Korm. határozat, illetve a 2013. évi L. törvény írja elő.

Figyelemre méltó az a tény, hogy napjainkban szinte valamennyi létfontosságúnak (kritikusnak) minősített, minősíthető infrastruktúra nemcsak használja az elektronikus információs rendszereket, hanem egyre erősebben függ ezektől. Az elektronikus információs rendszerektől függ az egyes infrastruktúra-elemek működése, és függ a létfontosságú infrastruktúra elemeinek együttműködése is, más szóval az infokommunikációs technológiáktól való függőség olyan mértékű, hogy azok összeomlása vagy megsemmisülése súlyos következményekkel járhat nemcsak az adott infrastruktúra szempontjából, hanem más létfontosságú infrastruktúrákra nézve is. A létfontosságú információs infrastruktúra egészére nézve az egyes infrastruktúraelemek infokommunikációs technológiái egy „belső" létfontosságú infrastruktúrát jelentenek.

Kijelenthetjük, hogy az infrastruktúrák között kölcsönös függőség (ez az un. *interdependencia*) áll fenn. A támogató információs infrastruktúrákon[30] keresztül az információs társadalom funkcionális információs infrastruktúráinak[31] működését károsan lehet befolyásolni (zavarni, korlátozni, megszüntetni), azon keresztül pedig:

- az információs társadalom információs és vezetési működési rendjére (minőségére, harmóniájára, dinamikus egyensúlyára);
- vezetési rendszerére (a vezetés integrációjára, annak szilárdságára és minőségére);
- a vezetés struktúrájára (szervezettségi fokára);
- a belső és külső kommunikációra és végezetül
- az adott szervezet operatív vezethetőségére lehet igen komoly, negatív hatást gyakorolni.[2]

Az Európai Bizottság által 2005 novemberében kiadta a *Zöld Könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról* [17] dokumentumot. E fontos okmány szerint a létfontosságú információs infrastruktúrák védelme a *„tulajdonosok, üzemeltetők, gyártók és használók, valamint a hatóságok programjai és tevékenységei, melyek célja fenntartani az információs infrastruktúra teljesítményét meghibásodás, támadás vagy baleset esetén a meghatározott minimális szolgáltatási szint felett, illetve minimálisra csökkenteni a helyreállításhoz szükséges időt, valamint a károkat."*

A létfontosságú információs infrastruktúrák védelme tehát ágazatközi jelenség, nem korlátozódhat egyes konkrét ágazatokra. A létfontosságú információs infrastruktúrák védelmét szorosan koordinálni kell a létfontosságú infrastruktúrák védelmével.

---

[28] Angolul: Critical Information Infrastructure Protection (CIIP).

[29] Olyan infrastruktúra (eszköz, létesítmény vagy rendszer), amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.

[30] A támogató információs infrastruktúrák biztosítják a funkcionális információs infrastruktúrák működéséhez a támogató hátteret. [16]

[31] A funkcionális információs infrastruktúrák biztosítják a társadalom működéséhez az információk megszerzését, előállítását, továbbítását, feldolgozását és felhasználását, azaz közreműködnek minden alapvető társadalmi feladat – funkció – ellátásában. [13]

„Kritikus információs infrastruktúrák *azon infokommunikációs létesítmények, eszközök vagy szolgáltatások, amelyek önmagukban is kritikus infrastruktúra elemek, továbbá a kritikus infrastruktúra elemeinek azon infokommunikációs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése a kritikus infrastruktúrák működésképességét jelentősen csökkentené.*" [15] Ez a megfogalmazás lett a 2013. évi L. törvényben tovább finomítva[32], hogy illeszkedjen a 2012. évi CLXVI. törvényhez.

2.6.2. A kiberbiztonság

Divattá vált a *kiber* előtaggal megjelölni bármit, ami az internethez, az elektronikus információs rendszerekhez kötődik, például kiberbűnözés. Ennek „magyartalan" változata, ha a magyar kifejezést az angol *cyber* előtaggal használják, például *cyberhadviselés*.

A kiber szó magyarázatát a kibernetikával kell kezdeni. A *kibernetika*[33] kifejezést Norbert Wiener (1894–1964) matematikus és filozófus a *kübernétész*, görögül *kormányos* szóból alkotta 1948-ban [18] egy komplex tudományos irányzat megjelölésére, amely a **szabályozás, vezérlés, információfeldolgozás és -továbbítás** általános törvényeit kutatja.

A kibernetika ágai: elméleti (fontosabb részei: rendszerelmélet, játékelméletet, információelméletet, automaták elmélete) és alkalmazott kibernetika. Az alkalmazott kibernetika az egyes tudományokban az elméleti kibernetika fogalomrendszerének és módszereinek felhasználása. Fontosabb területei a műszaki kibernetika (elektronikus számítógépek, szabályozókörök), a biokibernetika (élőlények mint kibernetikai rendszerek szabályozási folyamatai) és a gazdasági kibernetika (nemzetközi, nemzeti és szervezeti szintű gazdasági folyamatok). Az alkalmazott kibernetika alapvető eszköze a modellezés.

Bár Magyarországon az ötvenes években a kibernetika „burzsoá áltudománynak" számított, többen is kutatták ezt a tudományterületet. Kalmár László professzornak (1905–1976), a számítástudomány nagy úttörőjének kezdeményezésére és vezetésével 1963-ban a Szegedi Tudományegyetemen létrejött a Kibernetikai Laboratórium. Hazánkban a kibernetika kifejezést a múlt század hatvanas-hetvenes éveiben széles körben használták mindenre, aminek köze volt a számítógéphez, majd felváltotta a számítástudomány, illetve az informatika kifejezés.

Sokan – tévesen – a kibernetika rövidítéseként értelmezik, magyarázzák a kiber kifejezést, például *kibernetikai biztonság*.

A kiber kifejezés a *kibertér*[34] leegyszerűsítéseként került át a mindennapi szóhasználatba szerte a világon. [19] A kibertér kifejezést a kanadai sci-fi író, *William Gibson* használta először 1982-ben, a „Burning Chrome" című rövid elbeszélésében, majd az 1984-es Neurománc című regényével vált közismertté. Kibertér a számítógép-kommunikáció birodalma, annak virtuális világa – egy tér, amelyben a kibernetika dominál. Gibsontól származik a *hústér*[35] kifejezés is, amelyet a kibertér ellentéteként használ a fizikai világ jelölésére. És ettől kezdve a kibertér **a számítógép-rendszerek és -hálózatok** által alkotott metaforikus tér, amelyben elektronikus adatok tárolódnak és online adatforgalom, valamint kommunikáció zajlik. Olyan virtuális világot is jelent(het), amelyben a megszállott számítógép-használók és más lények, például kiborgok[36] élnek.

Számtalan definíció jelent meg a kibertérről. Számomra a legmeggyőzőbb az USA Védelmi Minisztériuma Katonai és kapcsolódó kifejezések szótárában [20] található. „**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.**"[37]

Érdekes módon ennek az amerikai katonai terminológiai szótár [20] B függelékének 6. pontjában, az általánosan használt hibás kifejezések között szerepel a kiber szó, a helyes kibertér mellett. Ez azért is érdekes, mert mára általánosan – például a NATO-ban is – a kiber kifejezést önállóan használják.

---

[32] 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.

[33] Angolul: cybernetics

[34] Angolul: cyberspace

[35] Angolul: meatspace

[36] Kibernetikus organizmus (angolul: cybernetic organism, cyborg), azaz gépi és biológiai elemek együttműködése.

[37] Angolul: „A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

Mire? Tulajdonképpen mindenre, ami az internethez, az elektronikus információs rendszerekhez kötődik, de különösen ott, ahol valamilyen fenyegetés tárgya vagy eszköze az internet, az elektronikus információs rendszer. [19]

Ilyen a c*ybercrime*, magyarul a *kiberbűnözés*. Például az Európa Tanács Budapesten, 2001. november 23-án kelt, a 2004. évi LXXIX. törvénnyel kihirdetett nemzetközi *Számítástechnikai Bűnözésről szóló Egyezmény*e [21] (angolul: *Covention of Cybercrime*) a magyar címben, és akkor még a törvény szövegében is, a „számítástechnikai bűnözés" kifejezést alkalmazta. Ezt a dokumentumot ma már magyarul is „mindenki" csak *Kiberbűnözésről szóló Egyezmény*ként emlegeti.

A kiberbűnözéshez tartoznak:

- az informatikai rendszerek és adataik ellen irányuló bűncselekmények,
- az informatikai eszközök felhasználásával elkövetett bűncselekmények,
- az informatikai rendszerekhez kapcsolódó bűncselekmények, tipikusan a gyermekpornográfiával kapcsolatos bűncselekmények (pedofília) és a szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények.

*Kiberterrorizmus*nak a kibertérben elkövetett terrorcselekményeket nevezik. [22]

És akkor mit nevezhetünk *kiberbiztonság*nak[38]? A kibervédelem mint a kibertér védelme támadások, sérülések vagy jogosulatlan hozzáférések ellen fogható fel. Vagyis magába foglalja a kibertér elektronikus információs rendszereinek védelmét, ugyanakkor annál több, jóval több. [19]

Magyarország Nemzeti Kiberbiztonsági Stratégiája[39] [23] szerint „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".

A Nemzeti Kiberbiztonsági Stratégiában [23] megfogalmazott védelmi célok:

- a magyar kiberteret érintő rossz szándékú kibertevékenység, fenyegetés, támadás, illetve vészhelyzet, valamint a vétlen információszivárgás elleni hatékony megelőzési, észlelési, kezelési (reagálási), válaszadási és helyreállítási képességek;
- a nemzeti adatvagyon megfelelő szintű védelme;
- a létfontosságú rendszerek és létesítmények (kritikus infrastruktúrák) kibertérhez kapcsolódó működésének üzembiztossága;
- a megfelelően gyors, hatékony és a veszteséget minimalizáló, különleges jogrend idején is alkalmazható helyreállítási képesség megléte;
- a magyar kibertér biztonságos működéséhez szükséges, a hazai és nemzetközi biztonsági tanúsítási szabványoknak megfelelő, a legjobb nemzetközi gyakorlatnak megfelelő színvonalú informatikai, hírközlési termékek és szolgáltatások;
- a legjobb nemzetközi gyakorlatoknak megfelelő színvonalú kiberbiztonsági oktatás, képzés, valamint kutatás és fejlesztés;
- a biztonságos kibertér a legjobb nemzetközi gyakorlatoknak megfelelő kialakítása a gyermekek és a jövő nemzedékek számára.

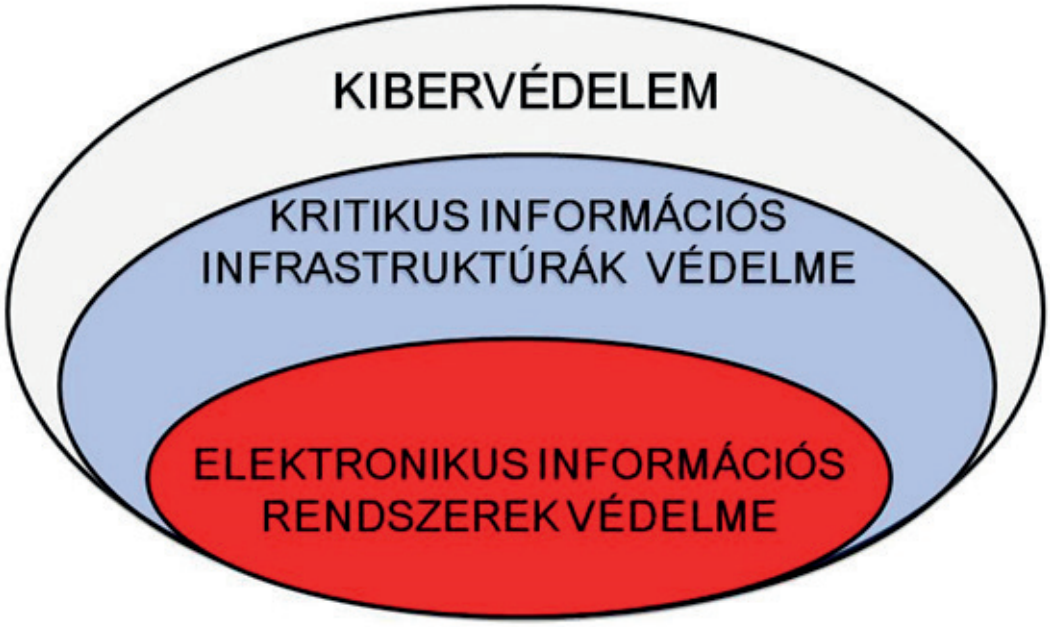
A célok eléréséhez szükséges feladatok:

- kormányzati koordináció,
- együttműködés a civil, a gazdasági és a tudományos területekkel,
- szakosított intézmények létrehozása a kiberbiztonsággal összefüggő feladatok ellátására,
- szabályozásban a jogalkotási tevékenység mellett együttműködési megállapodások a civil, a gazdasági és a tudományos terület szereplőivel,
- nemzetközi együttműködések (EU, NATO, ENSZ, EBESZ),
- tudatosság, oktatás, kutatás-fejlesztés,
- gyermekvédelem,
- gazdasági szereplők motivációja a kiberbiztonság fokozására.

A kibertér védelme, a kritikus információs infrastruktúrák védelme és az elektronikus információs rendszerek védelme közötti összefüggést a következő ábra mutatja.

[38] Angolul: Cybersecurity, helyesebben Cyberspace Security

[39] Tulajdonképpen ez nem stratégia, hanem politika (Angolul: policy), hiszen célokat, alapelveket, elkötelezettségeket határoz meg, míg a stratégia (Angolul: strategy) a politikában megfogalmazott célkitűzések megvalósításának módszerét és érvényesítési módját deklarálja.



4. ábra A kibertér, a kritikus információs infrastruktúrák és az elektronikus információs rendszerek védelme közötti összefüggés [24]

3. Az elektronikus információs rendszerek biztonságához kapcsolódó jogi szabályozás

Az élet különböző területein a jogi szabályozás alapfokú ismerete elengedhetetlen feltétele a hatékony tevékenységnek. Az elektronikus információs rendszerek biztonsága területén ez különösen igaz, mert itt sok hazai jogszabályi[40] előírást kell figyelembe venni a védelem tárgyának, módszereinek és erősségének kialakítása során.

Magyarországon a „jelenleg hatályos jogszabályokban rendkívül heterogén az informatikai biztonságra vonatkozó előírások tartalma és hatálya. Nincsen olyan jogszabály, amely az információbiztonság vagy az informatikai biztonság területén keretszabályozás jelleggel minden területre kiterjedően határozna meg előírásokat. Ezzel szemben a különböző nemzetgazdasági ágakra, adatkezelésekre, egyes szakmák gyakorlására vonatkozó szabályok között gyakran található eltérő mélységű biztonsági szabályozás" [25].

Fel kell hívnom az olvasó figyelmét, hogy itt kizárólag a magyar jogszabályi környezetről szólunk, a külföldi jogszabályokról nem. Fontos, hogy a jogalkalmazás során meggyőződjünk a jogszabályok aktuális állapotáról!

3.1. Az elektronikus információs rendszerek biztonsága

Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény [11] (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 biztonság kialakítása nem általánosan, hanem a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából 5-5 biztonsági osztályban kell, hogy megtörténjen. A biztonsági osztályba sorolás alapja a kockázatelemzés. A szervezetet a legmagasabb biztonsági osztályának megfelelően biztonsági szintbe kell sorolni, amely tulajdonképpen a szervezetnek a biztonságkezelésével kapcsolatos képességeit mutatja. Ennek részletesebb leírását *az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló41/2015. (VII. 15.) BM rendelet* tartalmazza. Fontos, hogy a rendelet a konkrét megoldásokat illetően megengedő, azaz a szervezetre bízza azt, hogy milyen kockázatelemzési módszertannal dolgozik, milyen védelmi intézkedéseket hoz. Elvárás viszont, hogy ezek feleljenek meg nemzetközi vagy hazai szabványoknak, ajánlásoknak.

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 törvényi előírásoknak megfelelően *a 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról* szabályozza.

Az Ibtv. létrehozta a Nemzeti Elektronikus Információbiztonsági Hatóságot, amely nem annyira előíró-engedélyező típusú hatóság, hanem egy olyan felügyeleti szervezet, amely nyilván tart, ellenőriz és csak szükség esetén avatkozik be. A hatósági munkát *az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet* szabályozza.

A biztonsági események kezelésére kormányzati és ágazati eseménykezelő központokat kell az Ibtv. alapján működtetni. Ennek részleteit *a 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól* írja elő.

40 „Jogszabály a törvény, a kormányrendelet, a miniszterelnöki rendelet, a miniszteri rendelet, a Magyar Nemzeti Bank elnökének rendelete, az önálló szabályozó szerv vezetőjének rendelete és az önkormányzati rendelet. Jogszabály továbbá a Honvédelmi Tanács rendkívüli állapot idején és a köztársasági elnök szükségállapot idején kiadott rendelete." Magyarország Alaptörvénye T) cikk (2) bek.

Az egyes elkülönült, önállóan szabályozott ágazati szintű szabályozásokat a *187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról*tartalmazza.

Az Ibtv. az elektronikus információs rendszerek biztonságán túl Magyarország Kiberbiztonsági Stratégiájával összhangban megteremti a kibertér biztonsága állami koordinációjának alapját és ezt *a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről szóló 484/2013. (XII. 17.) Korm. rendelet*ben szabályozza.

3.2. A minősített adatok 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.

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 Mavtv. szabályozása szerint az adat minősítéssel csak akkor védhető, ha a törvényben meghatározott minősítéssel védhető közérdek körébe tartozik. A minősítés szintjét pedig a jogosulatlan hozzáférés által okozható kár mértéke fogja meghatározni; azaz minél nagyobb kárt okozhat a Magyar Köztársaságnak a minősített adathoz történő illetéktelen hozzáférés, annál magasabb szintű biztonsági követelményeket kell érvényesíteni a védelem során.

A káralapú minősítési rendszer négyszintű – „szigorúan titkos", „titkos", „bizalmas", illetve „korlátozott terjesztésű". A minősítés lehetséges leghosszabb időtartama „szigorúan titkos" és „titkos" minősítési szintű adat esetén legfeljebb 30 év, „bizalmas" minősítési szintű adat esetén legfeljebb 20 év, „korlátozott terjesztésű" minősítésű adat esetén legfeljebb 10 év. Az érvényességi idő meghosszabbítására csak új minősítési eljárás keretében van lehetőség.

Minősített adatot kezelni kizárólag a Nemzeti Biztonsági Felügyelet által kiadott engedély alapján lehet, amennyiben az adat kezelése állami vagy közfeladat ellátásához nélkülözhetetlen. A nemzeti, illetve a külföldi minősített adatok esetében egyaránt meg kell teremteni a kezelésükhöz szükséges személyi, fizikai, adminisztratív és elektronikus biztonsági feltételeket. A személyi biztonság feltételei körében kiemelést érdemel, hogy – hasonlóan a NATO, illetve az EU követelményeihez – a nemzeti minősített adathoz való hozzáférésnek is feltétele a személyi biztonsági tanúsítvány megléte. A tanúsítvány érvényességi idejének lejártáig meghatározza, hogy valamely természetes személy milyen legmagasabb minősítési szintű adat felhasználására kaphat felhasználói engedélyt.

Az Mavtv. alapján, ha a minősített adatot kezelő szerv állami vagy közfeladat végrehajtásához gazdálkodó szervezet közreműködését veszi igénybe, akkor az érintett gazdálkodó szervezet vonatkozásában a „bizalmas" vagy annál magasabb minősítési szintű adatok átadása előtt iparbiztonsági ellenőrzést kell végrehajtani. Az ellenőrzés célja annak megállapítása, hogy a minősített adat kezelésének biztonsági feltételeit megteremtették-e az érintett gazdálkodó szervezetnél. Ennek igazolására a Nemzeti Biztonsági Felügyelet telephely biztonsági tanúsítványt ad ki.

A Mavtv. alapján a Nemzeti Biztonsági Felügyelet a nemzeti és külföldi (NATO, illetve az EU) minősített adatok védelmének hatósági felügyeletéért és kezelésének engedélyezéséért felelős. Emellett ellátja a rejtjeltevékenység hatósági engedélyezését és felügyeletét is, illetve a nemzeti iparbiztonsági hatósági feladatokat.

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. A nemzetbiztonsági ellenőrzés célja annak vizsgálata, hogy a fontos és bizalmas munkakörre jelölt, illetve az ilyen munkakört betöltő személyek megfelelnek-e az állami élet és a nemzetgazdaság jogszerű működéséhez szükséges, valamint – amennyiben szükséges – a nemzetközi kötelezettségvállalásokból fakadó biztonsági feltételeknek. A biztonsági feltételek vizsgálata azon kockázati tényezők, körülmények, információk felderítését jelenti, amelyek felhasználásával a fontos és bizalmas munkakört betöltő személyek tevékenysége jogellenes céllal befolyásolhatóvá, illetve támadhatóvá válhat, és ezáltal a nemzetbiztonságot sértő vagy veszélyeztető helyzet állhat elő. Az ellenőrzéshez a személynek a törvény mellékletében megadott kérdőívet kell kitöltenie. 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.

3.3. 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.

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 intézkedések a szükséges mértéket elérték-e annak ellenére, hogy elégtelennek bizonyultak a titokban maradáshoz. [26]

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…".

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.**

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

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. [26]

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. [26]

3.5. A személyes adatok védelme

Az állam és a gazdaság működéséhez szükséges nagytömegű 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. [26]

A *2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról* 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 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.

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény kizárólag a személyes adatok védelmére alkalmazható, és sem betűje, sem „szelleme" nem terjeszthető ki más adattípusok védelmére.

Az adatvédelmi törvény nemcsak a személyes adatok védeleméről, 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.

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.

A törvény figyelembe veszi az európai jogharmonizációból eredő követelményeket, így különösen az Európai Parlament és a Tanács 910/2014/EU rendeletét (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (eIDAS Rendelet). Tekintettel az eIDAS Rendelet jogszabályi formájára és jellegére (t.i. hogy ez, a korábbi szabályozással ellentétben nem Irányelv, hanem Rendelet), ez minden EU-s tagállamban közvetlenül (bármiféle nemzeti transzformáció nélkül) és kötelezően alkalmazandó. .

Az elektronikus aláírást elsőként 2001-ben szabályozta törvény Magyarországon. Ennek fontosabb alapelvei a következők voltak [26]:

1. az elektronikus aláírás előállítására felhasznált technológiától függetlenül alkalmazható a törvény (technológiasemleges 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. elektronikus aláírás hitelesítésszolgáltatást 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.

Az eIDAS Rendelet egyik célkitűzése, hogy „elhárítsa azokat a meglévő akadályokat, amelyek a tagállamokban az elektronikus azonosító eszközök határokon átnyúló használatának útjában állnak, legalábbis a közszolgáltatások igénybevétele céljából való hitelesítés tekintetében. (…) További célja, hogy a tagállamok által kínált, határokon átnyúló online szolgáltatások igénybevételéhez biztosítsa a biztonságos azonosítás és hitelesítés lehetőségét."[41] Szintén fontos változás, hogy az új jogszabályi előírások a korábbinál szigorúbb, EU szinten egységes követelményeket fogalmaznak meg a tanúsítványok kiadását, valamint az ezzel párhuzamosan akár időbélyegzés illetve archiválás szolgáltatást nyújtó, úgynevezett bizalmi szolgáltatókra vonatkozóan. Ennek köszönhetően a Rendelet szerint minősített tanúsítványokat, valamint az ezeken alapuló minősített aláírásokat/bélyegzőket minden tagállamban, az eIDAS rendelet által meghatározott joghatással el kell fogadni

3.7. A számítógépes bűnözés jogi kérdései

Az informatika világában is egyre jobban „tör előre" a bűnözés, amelyet számítógépes bűnözésnek, kiberbűnözésnek neveznek és az úgynevezett „fehérgalléros bűnözés" speciális formájának tekintenek. A bűnözés mintegy nyolcvan százalékát az anyagi haszonszerzés motiválja, amelynek során az eszközök és a módszerek, a potenciális áldozatok szinte kizárólag a költség és kockázat alapján kerülnek kiválasztásra. A haszonszerzés módszereit a bűnelkövetők a lehetőségekhez igazítják, ezért a számítógépek és az internet használatának mindennapossá válása az informatikai rendszerek nem kellő védelmével párosulva a számítógépes bűnözés mind nagyobb térnyerését vetítik előre, ezzel milliárdos károk bekövetkezését prognosztizálják.

Mit is jelent a számítógépes bűnözés? Köznapi használatban minden olyan bűnözési, károkozási, ügyeskedési formát, cselekedetet, ahol a számítástechnikai eszközt célként vagy a tett eszközeként veszik igénybe, számítógépes bűnözésnek szokás nevezni. Magyarországon a kilencvenes évek közepére kialakultak az „intellektuális bűnelkövető" csoportok, amelyek igen gyakran a szervezett bűnözéshez kapcsolódnak. Nemzetközi visszhangot és fenyegetéseket váltott ki az illegális szoftvermásolás és forgalmazás. Ezenkívül ezek a bűncselekmények a távközlési szolgáltatások (mobil távbeszélő szolgáltatások mások előfizetésének terhére történő igénybevétele, távbeszélő alközpontokban hívásátirányítás, távhívási jogosultság jogtalan igénybevétele, bérelt audiotext számok – számítógéppel vezérelt – hívásismétlő berendezésekkel folyamatos hívása) gyengeségeinek kihasználására irányultak, de megjelentek a hamis telefon-, sőt a hamis bankkártyák is, illetve a hamis bankkártyák felhasználására szerveződött csoportok. [26]

[41] Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (12).

A fentiek alapján kimondhatjuk, hogy 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. [26]

Könnyen beláthatjuk, hogy a számítógépes bűncselekményeket az informatikai rendszerek felhasználói (tulajdonosai, üzemeltetői) szempontjából két nagy csoportra oszthatjuk [26]:

– az informatikai rendszerekben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, illetve a rendszerelemek sértetlensége és rendelkezésre állása ellen irányuló bűncselekményekre (itt az informatikai rendszer(elem) a bűncselekmény tárgya) és
– az informatikai eszközök felhasználásával elkövetett bűncselekményekre (itt az informatikai rendszer(elem) a bűncselekmény eszköze).

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.

A magyar büntetőjogban, illetve a *Büntető Törvénykönyv*ben[42] (a továbbiakban: Btk.) összhangban a 2004. évi LXXIX. törvénnyel kihirdetett nemzetközi Számítástechnikai Bűnözésről szóló egyezménnyel az alábbi tényállásokat kezelik számítógépes bűncselekményeknek, illetve számítógépes bűnözésként:

– Információs rendszer vagy adat megsértése – 423. §;
– Információs rendszer védelmét biztosító technikai intézkedés kijátszása – 424. §;
– Készpénz-helyettesítő fizetési eszköz hamisítása – 392. §;
– Készpénz-helyettesítő fizetési eszközzel visszaélés – 393. §;
– Szerzői vagy szerzői joghoz kapcsolódó jogok megsértése – 385. §;
– Védelmet biztosító műszaki intézkedés kijátszása – 386. §;
– Jogkezelési adat meghamisítása – 387. §.

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.

Más szóval, az információs rendszer és adatok elleni bűncselekménynek, illetve az információs rendszer védelmét biztosító technikai intézkedés kijátszásának

jogi tárgya:	a vagyonvédelem és a tulajdoni viszonyok védelme,
elkövetési tárgya:	az információs rendszer és adata(i),
az elkövetési magatartás:	az információs rendszerbe történő belépés, az adatok bevitele, továbbítása, megváltoztatása, törlése, hozzáférhetetlenné tétele és egyéb meg nem engedett műveletek végzése.

E bűncselekményeknél a bizonyíthatóság érdekes kérdés. Általában a bizonyítást a nyomozóhatóság feladataként kezelik, de az információs rendszer elleni bűncselekmények esetében, ha az információs rendszerben nem állnak

[42] 2012. évi C. törvény a Büntető Törvénykönyvről

rendelkezésre azok a garanciális elemek, amelyek lehetővé teszik a felhasználók és tevékenységeik utólagos ellenőrzését, akkor a nyomozóhatóság nehéz helyzetbe kerül. A bizonyíthatósághoz [26]:

- ki kell dolgozni az informatikai rendszerhez történő hozzáférések olyan jogosultsági rendszerét, ahol a felhasználók azonosításának egyedinek, jellemzőnek, ellenőrizhetőnek és hitelesítésre alkalmasnak kell lennie;
- az informatikai rendszernek képesnek kell lennie minden egyes felhasználó vagy felhasználói csoport által végzett művelet szelektív regisztrálására;
- az elszámoltathatóság és auditálhatóság biztosítása érdekében olyan regisztrálási és naplózási rendszert (biztonsági napló) kell kialakítani, hogy utólag meg lehessen határozni az informatikai rendszerben bekövetkezett fontosabb eseményeket, különös tekintettel azokra, amelyek a rendszer biztonságát érintik, hogy ezáltal ellenőrizni lehessen a hozzáférések jogosultságát, meg lehessen állapítani a felelősséget, valamint az illetéktelen hozzáférés megtörténtét;
- a rendszerben a biztonsági napló auditálásához szükséges eszközöknek lehetővé kell tenniük egy vagy több felhasználó tevékenységének szelektív vizsgálatát;
- a biztonsági eseménynapló és a jegyzőkönyvek adatait védeni kell az illetéktelen hozzáféréstől, ezekhez az adatokhoz csak erre felhatalmazott személy férhet hozzá. A biztonsági napló adatait rendszeresen ellenőrizni és archiválni kell.

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”.

Az informatika területén jellemző elkövetési magatartások:

- munkahelyi, iskolai számítógépekről az ott – többnyire – jogszerűen használt program jogosulatlan lemásolása és használata vagy továbbadása, illetve az így szerzett program sokszorozása és kereskedelmi forgalomba hozatala;
- a legális kereskedelemből származó, eredeti programok sokszorozása és kereskedelmi forgalomba hozatala önállóan vagy számítógéppel együtt;
- a felhasználónál az engedélyezett licencszámnál nagyobb számú alkalmazás;
- a programok védelmének feltörése (például hardverkulcs kiiktatása, a regisztrációs kód feltörése);
- a programok terjesztése az interneten ellenértékért vagy anélkül (ezek a letölthető programok találhatók az úgynevezett „warez” file-okban).

A büntetőügy ezekből többnyire csak a jogosulatlanul sokszorosított programok kereskedelmi forgalomban való megjelenése esetén lesz, hiszen a hatóságoknak csak ekkor jut tudomására, ekkor kerül a látóterébe.

A szoftverkalózkodás kapcsán sok vitát és ellenszenvet váltott ki a *szoftverrendőrség* néven elhíresült BSA (Bussines Software Alliance) működése. A BSA, mint nemzetközi szövetség, a szoftvergyártók és forgalmazók érdekképviselete, amelynek semmilyen nyomozati, eljárási joga nincs. Sőt tekintettel arra, hogy a szoftvergyártók és forgalmazók érdekeit pénzért képviseli, ezért nem tekinthető függetlennek és így szakértőként sem járhat el a szerzői vagy szomszédos jogok megsértése kapcsán.

4. Hazai és nemzetközi szabványok és ajánlások

Nemzetközi téren már az 1970-as évek végén megindult (elsősorban az Egyesült Államokban) az informatikai biztonsági értékelés követelményrendszerének kidolgozására vonatkozó tevékenység. Első kézzelfogható eredménye az 1983-ban kiadott **Trusted Computer System Evaluation Criteria** (magyarul: Biztonságos Számítógépes Rendszerek Értékelési Kritériumai, röviden: TCSEC) dokumentum vagy más néven „Narancs Könyv" megjelenése volt, amelyben az USA Védelmi Minisztériumának informatikai biztonsági követelményeit hozták nyilvánosságra – elsősorban – a beszállítók részére. Ezt követően az Európai Közösség is kidolgozta az **Information Technology Security Evaluation Criteria** (magyarul: Informatikai Biztonsági Értékelési Követelmények, röviden: ITSEC) dokumentumot.

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, közismert nevén ISO 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.

Tekintettel arra, hogy a fenti dokumentumok az informatikai rendszereket általánosságban kezelték, ami megnehezítette a védelem testre szabását, az Európai Unió, 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 Bizottság16. 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 szabvány volt az ISO/IEC 27xxx szabványsorozat kiinduló anyaga. Az BS 7799, illetve az ISO 27xxx szabványsorozat egyik célja az, hogy az informatikai rendszerek biztonságát, mint irányítási, menedzsmentrendszert kezeljék, mert csak így kezelhetők megfelelően az informatikai rendszert érintő biztonsági kockázatok. A szabványok kialakítása során törekedtek a más irányítási rendszerekre vonatkozó szabványokkal való összhangra. Már a BS 7799-2:2002 szabvány, és így az ISO/IEC 27001:2005 szabvány is, az ISO 9001:2000 szabvány figyelembevételével készült. Ez, és a szabvány alkalmazásának mind szélesebb körű elterjedése, valóban abba az irányba mutat, hogy az informatikai biztonság tervezését és működtetését vezetési rendszerként kell értelmezni.

A Közigazgatási informatikai Bizottság 25. számot viselő ajánlássorozata az Informatikai Tárcaközi Bizottság 1994–1996. között kiadott 8. (Az informatikai biztonság módszertani kézikönyve), 12. (Az informatikai rendszerek biztonsági követelményei) és 16. számú (A Common Criteria (CC), az informatikai termékek és rendszerek biztonsági értékelésének módszertana) ajánlásait váltotta fel – kiegészített, átdolgozott és a korábbinál bővebb tartalommal.

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 (*info*rmation *sec*urity) néven vált ismertté.

Az informatikai biztonság kérdésével számos szabvány és ajánlás foglakozik. Gyakran hivatkoznak ezen területen az ITIL[43]-re és a COBIT[44]-ra. Az ITIL, *„Az informatikaszolgáltatás módszertana"* egy az informatika mint szolgáltatás egészére kiterjedő, nemzetközileg széles körben elfogadott dokumentum. Az ITIL-ben a biztonságirányítás bár önálló folyamat, amennyire csak lehetséges, integrálódik a többi folyamatba. Az ITIL Biztonságirányítás (Security Management) kötete az ISO/IEC 27002 szabványt használja hivatkozásként, amikor a létező ITIL-folyamatokat bővíti a biztonságirányítással. A COBIT az információrendszer-ellenőrök egy nemzetközileg is ismert és elfogadott,

[43] ITIL = Information Infrastructure Library
[44] COBIT = Control Objectives for Information and Related Technology

az informatikai rendszerek szervezéséhez és különösen az ellenőrzéséhez szükséges irányelveket tartalmazó dokumentuma. A biztonság kérdésére nagy hangsúlyt fektet, de részleteiben nem foglalkozik a kérdéssel.

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.

4.1. Common Criteria (ISO/IEC 15408 szabvány)

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 jelenlegi verziója a 3.1 Release 5 (2017. április)[45].

„A szabványban a funkcionális követelmények, bizonyossági követelmények és értékelési bizonyossági szintek (EAL) mátrixaként határozhatóak meg az alkalmazandó biztonsági követelmények. A követelmények konkretizálása céljából az általános, eszköz fajtájára jellemző védelmi profilok (Protection Profile, PP) alapján biztonsági célkitűzést (Security Target, ST) kell készíteni, amely már az eszköztípusra vonatkozó követelményeket tartalmazza, és ez alapján kerül megvalósításra maga a termék, a vizsgálat tárgya (Target of Evaluation, TOE).” [27]

A CC három részből áll:

1. Bevezetés és általános modell[46]
2. A biztonság funkcionális követelményei[47]
3. A biztonság garanciális követelményei[48]

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, mely 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 korántsem 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 felhasználó-azonosítás egyedi, a hozzáférésjogosultságrendszer szerepkörökön alapul.

---

[45] A szabványok kiadásánál nagy az „időkésés”, az ISO/IEC 15408 szabvány kötettől függően 2009-es vagy 2008-as kiadású, míg a magyar szabványé 2003-as, illetve 2002-es.

[46] Angolul: Introduction and general model

[47] Angolul: Security functional requirements

[48] Angolul: Security assurance requirements

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 környezetét, 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 követelmények meghatározását, amelyek biztosítása elengedhetetlen a biztonságos működéshez.
– A biztonsági követelményeket:
  - A vizsgált rendszer funkcionális biztonsági követelményeit, valamint a megcélzott biztonsági osztály meghatározását (EAL1-7).
  - Az IT környezet biztonsági követelményeinek meghatározását.

A CC funkcionális követelményrendszere gyakorlatilag egy funkcionális komponenskatalógus, amelyből összeállítható a vizsgált rendszerre (*Target of Evaluation, TOE*) vonatkozó funkcionális biztonsági követelményrendszer. A követelmények *osztályok*ra, azon belül *család*okra 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, „összecsomagolják".

Az alapvető funkcionális biztonsági követelmények osztályai a következők:

– **FAU:** Audit (Security Audit)
– **FCO:** Kommunikáció (*Communication*)
– **FCS:** Kriptográfiai támogatás (*Cryptographic support*)
– **FDP:** Adatvédelem (User data protection)
– **FIA:** Azonosítás, hitelesítés (Identification and Authentication)
– **FMT:** Biztonságmenedzsment (*Security management*)
– **FPR:** Személyes adatok védelme (*Privacy*)
– **FPT:** A TOE biztonságának védelme (Protection of then TOE Security functions)
– **FRU:** Erőforrás-gazdálkodás (*Resource utilization*)
– **FTA:** TOE 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** (angolul: *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 fejlesztői ráfordítási 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 előnyei közé sorolandó, hogy **testre szabható** és 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.

4.2. ISO/IEC 27000 szabványsorozat

Az ISO/IEC 27000 szabványsorozat alapját a Brit Szabványügyi Hivatal[49] által kiadott brit szabvány, a BS 7799 brit szabvány képzi. Ennek a szabványnak az elődjét a DTI/CCSC[50] dolgozta ki a brit számítógép-felhasználók támogatására 1989-ben *„A Users Code of Practice"* címen. Ezt az ipari terület felhasználóiból szervezett konzorcium bevonásával később továbbfejlesztette, és a BSI ezt adta ki 1995-ben a BS 7799 szabványként. (Itt érdemes megjegyezni, hogy a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság 12. számú ajánlása, az Informatikai Rendszerek Biztonsági Követelményei [8] ezzel egyidőben készült, hasonló elvek alapján.) Később igény támadt e szabvány olyan jellegű bővítésére, amely az informatikai biztonság menedzsmentjével foglakozik, és ez lett a BS 7799 szabvány második része, amely *Specification for Information Security Management Systems*[51] címmel került kiadásra 1998-ban. A BS 7799-2:1998 már kifejezetten a tanúsítási eljárás céljával készült.

A BS 7799 szabvány első revíziója 1999-ben történt meg, és az első részét nemzetközi szabványként történő elfogadásra javasolta a BSI. A Nemzetközi Szabványügyi Szervezet[52] 2000 augusztusában a BS 7799 1:1999 szabványt változatlan szerkezetben és gyakorlatilag változatlan tartalommal nemzetközi szabványnak fogadta el ISO/IEC 17799 néven.

A brit szabvány második része, a BS 7799-2:1999 már a megjelenése után *de facto* nemzetközi szabvánnyá vált, de több ország (például Japán, Svédország) nemzeti szabványként is bevezette. 2002-ben kiadták a BS 7799-2:2002 szabványt, amely már az ISO 9001:2000 szabvány figyelembevételével készült. 2005-ben a BS 7799-2:1999 szabványt ISO/IEC 27001:2005 számon Informatika – Biztonsági technikák – Informatikai biztonsági irányítási rendszer – Követelmények címmel nemzetközi szabványnak fogadták el. Ezzel egyidejűleg az ISO/IEC 17799:2005 szabvány átnevezésre került, és ez lett az ISO/IEC 27002:2005 szabvány, azaz az informatikai rendszerek biztonságával foglalkozó 27000-es szabványsorozat első két eleme. Ez azért is jelentős esemény a szabvány történetében, mert létrehoztak egy egész szabványcsaládot, az ISO 27000-eset is, amelyben további, a kérdéskörhöz tartozó szabványok jelentek és jelennek meg. A sorozat számozása az ISO Informatikai Munkabizottsága (JTC1) illetékes albizottságának (IT Security techniques), az SC27-nek a számából ered.

Az ISO/IEC:27001 szabvány alapvető célja az Információbiztonsági Irányítási Rendszer[53] (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.

Az ISO/IEC27002:2013 szabvány címe változatlan: Informatika – Biztonsági technikák – Kézikönyv az informatikai biztonság irányításához[54]. A szabvány fő fejezetei bővültek a 2005. évi kiadásban szereplőkhöz képest. Az ISO/IEC27001:2013 szabvány alapelvei is változtak a 2005. évi kiadáshoz képest. Így például már nem kötelező a PDCA modell alkalmazása, nagyobb hangsúlyt kaptak a célok, a mérések és az ellenőrzések. Az ISO/IEC27002:2013 szabvány szerkezete követi az ISO/IEC direktívákat, és így kompatibilis az egyéb irányítási rendszerekkel (lásd ISO 9001, ISO 14001, OHSAS 18001 stb.).

[49] Angolul: British Standard Institute, röviden: BSI

[50] Department of Trade and Industry's, Commercial Computer Security Centre (magy.: Kereskedelmi és Ipari Minisztérium, Kerekedelmi Számítógép-biztonsági Központ)

[51] Az informatikai biztonsági irányítási rendszer specifikációja

[52] ISO = International Standard Organization (Nemzetközi Szabványügyi Testület)

[53] Information Security Management System (ISMS)

[54] Information technology – Code of practice for information security management

Az ISO/IEC27002:2013 szabvány fő fejezetei:

0. Bevezetés
1. Hatály
2. Hivatkozások
3. Fogalommeghatározások
4. A szabvány felépítése
5. Biztonságpolitika
6. Az információbiztonság szervezete
7. Emberi erőforrások biztonsága
8. Vagyontárgyak kezelése
9. Hozzáférés-vezérlés
10. Kriptográfia
11. Fizikai és környezeti biztonság
12. Az üzemeltetés irányítása
15. A kommunikáció biztonsága
14. Rendszerek beszerzése, fejlesztése és karbantartása
15. Beszállítói kapcsolatok
16. Az információbiztonsági incidensek kezelése
17. Az információbiztonság üzletment-folytonossági vonatkozásai
18. Megfelelőség

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 2014-ben készülők már nagy valószínűséggel jobbak lesznek!)

A szabványcsaládnak sok tagja már kiadásra került, és továbbiak is fejlesztés alatt vannak. A már kiadott elemek:

ISO/IEC 27000:2016 – Information technology – Security techniques – Information security management systems – Overview and vocabulary

ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls

ISO/IEC 27003:2017 – Information technology – Security techniques – Information security management system implementation guidance

ISO/IEC 27004:2016 – Information technology – Security techniques – Information security management – Measurement

ISO/IEC 27005:2011 – Information technology – Security techniques – Information security risk management

ISO/IEC 27006:2015 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27007:2017 – Information technology – Security techniques – Guidelines for information security management systems auditing

ISO/IEC TR 27008:2011 – Information technology – Security techniques – Guidelines for auditors on information security controls

ISO/IEC 27009:2016 – Information technology – Security techniques – Sector-specific application of ISO/IEC 27001 – Requirements.

ISO/IEC 27010:2015 – Information technology – Security techniques – Information security management for inter – sector and inter – organizational communications

ISO/IEC 27011:2016 – Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

ISO/IEC 27013:2015 – Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000 – 1

ISO/IEC 27014:2013 – Information technology – Security techniques – Governance of information security

ISO/IEC TR 27015:2012 – Information technology – Security techniques – Information security management guidelines for financial services

ISO/IEC TR 27016:2014 – Information technology – Security techniques – Information security management – Organizational economics

ISO/IEC 27017:2015 – Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27018:2014 – Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC TR 27019:2013 – Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
ISO/IEC 27023:2015 – Information technology – Security techniques – Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002
ISO/IEC 27031:2011 – Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity
ISO/IEC 27032:2012 – Information technology – Security techniques – Guidelines for cybersecurity
ISO/IEC 27033 – 1:2015 – Information technology – Security techniques – Network security – Part 1: Overview and concepts
ISO/IEC 27033 – 2:2012 – Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security
ISO/IEC 27033 – 3:2010 – Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues
ISO/IEC 27033-4:2014 – Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways
ISO/IEC 27033 – 5:2013 – Information technology – Security techniques – Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
ISO/IEC 27033-6:2016 – Information technology – Security techniques – Network security – Part 6: Securing wireless IP network access
ISO/IEC 27034 – 1:2011 – Information technology – Security techniques – Application security – Part 1: Overview and concepts
ISO/IEC 27034-2:2015 – Information technology – Security techniques – Application security – Part 2: Organization normative framework for application security
ISO/IEC 27034-5:2017 – Information technology – Security techniques – Application security – Part 5: Protocols and application security controls data structure – XML schemas
ISO/IEC 27035:2016 – Information technology – Security techniques – Information security incident management
ISO/IEC 27035:2016-2 – Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response
ISO/IEC 27036-1:2014 – Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts.
ISO/IEC 27036-2:2014 – Information technology – Security techniques – Information security for supplier relationships – Part 2: Requirements.
ISO/IEC 27036-3:2013 – Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security.
ISO/IEC 27036-4:2016 – Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services.
ISO/IEC 27037:2012 – Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence
ISO/IEC 27038:2014 – Information technology – Security techniques – Specification for digital redaction.
ISO/IEC 27039:2015 – Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems (IDPS).
ISO/IEC 27040:2015 – Information technology – Security techniques – Storage security
ISO/IEC 27041:2015 – Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative methods.
ISO/IEC 27042:2015 – Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence
ISO/IEC 27043:2015 – Information technology – Information technology – Security techniques – Incident investigation principles and processes

ISO/IEC 27050-1:2016 – Information technology – Security techniques – Electronic discovery – Part 1: Overview and concepts.
ISO/IEC 27050-3:2017 – Information technology – Security techniques – Electronic discovery – Part 3: Code of Practice for electronic discovery.
ISO/IEC 27799:2016 – Health informatics – Information security management in health using ISO/IEC 27002

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*[55] (GMITS) műszaki jelentést. Az ISO/IEC TR 13335 úgynevezett *Technical Report*-ként került kiadásra, 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 informatikai biztonság kérdésével számos az informatikai rendszerekre vonatkozó szabvány és ajánlás foglakozik. Gyakran hivatkoznak ezen a területen az ITIL[56]-re és a COBIT[57]-ra.

Az ITIL eredetileg az Egyesült Királysági Central Computing and Telecommunications Agency (CCTA) ajánlása volt, és a közigazgatási területen általában megkövetelték az alkalmazását. Mivel a gyakorlati alkalmazás tapasztalatai kedvezőek voltak, a módszertant a piaci környezetben is egyre inkább használni kezdték. Az ITIL egyre inkább elterjedt a szigetországon kívül is. Egyre több országban alakultak helyi *Fórumok*, amelyek összefogására létrejött az *IT Service Management Forum International*. Ez a nemzeti fórumokon keresztül egyrészt segítette az ITIL terjedését, másrészt ügyelt arra, hogy az egységes maradjon. Az ITIL-hez kapcsolódó brit szabvány, a BS 15000 ISO/IEC 20000 számon mára szintén nemzetközi szabvánnyá vált, amelynek több országban működik felhasználói szervezete, meghatározó módszertanná vált az informatikai infrastruktúra és informatikaszolgáltatás irányítása területén. „Amíg 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." [27] Az ITIL-t számos nemzetközi informatikai cég is elfogadta és támogatja, így például a Hewlett Packard, a Microsoft, az IBM stb. Ezek a cégek saját gyakorlatukba beépítették az ITIL terminológiáját és megközelítését. Sok szolgáltató, amely támogató szoftver eszközöket kínál, igyekszik azokat ITIL-konformmá tenni, hogy ezzel is javítsa piaci pozícióját.

Az ITIL legutóbbi változata a 2007-es v3, a MeH ITB Infrastruktúra menedzsment címen 15. számú ajánlásaként kiadta, majd az ITIL 3.1 verzióját a Széchenyi-terv támogatásával 2002 novemberében honosították.

Összefoglalva, 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." [27]

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 Informatikai Irányítási és Ellenőrzési Módszertan[58] támogatói, az Information Systems Audit and Control Foundation (Információs Rendszerek Ellenőrzésével és Vizsgálatával foglalkozó Alapítvány) és az IT Governance Institute elsősorban azzal a céllal dolgozták ki az *Összefoglaló áttekintés,* a *Keretrendszer,* az *Ellenőrzési irányelvek,* a

[55] Segédlet az informatikai biztonság irányításához.
[56] ITIL: IT Infrastructure Library, Az informatikaszolgáltatás módszertana.
[57] COBIT: Control Objectives for Information and Related Technology (Information Systems Audit and Control Foundation és IT Governance Institute).
[58] Control Objectives for Information and Related Technology

Vezetői útmutató, az *Auditálási útmutató* és az *Alkalmazási módszerek* elnevezésű kiadványokat, hogy forrásanyagot biztosítsanak az ellenőrzési szakemberek számára. A COBIT az üzleti folyamatokra, valamint az ezeket támogató informatikai megoldások négy területére – tervezés és szervezés; beszerzés és üzembe állítás; informatikai szolgáltatás és támogatás; 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. Példa ezekre … a COBIT kocka, amely a COBIT által lefedett három dimenziót, az üzleti követelmények – informatikai folyamatok – informatikai erőforrások dimenzióit és azok elemeit mutatja be." [27]

Az Information Systems Audit and Control Association (ISACA) COBIT-ra épülő Certified Information Systems Auditor (CISA) szakmai képesítése világszerte elismert. A szintén az ISACA kezelésében lévő Certified Information Security Manager (CISM) is széles körben ismert, és az Amerikai Egyesült Államok Védelmi Minisztériuma (USA DoD) által informatikai biztonsági szakvizsgának elismert[59]. A COBIT Magyarországon a pénzügyi szektorban elsődlegesen követett szabvány.

A COBIT-nak nem célja a más szabványokkal való együttműködés, de ennek ellenére több megfeleltetés készült az ITIL, ISO/IEC 27002 és PMBOK szabványokkal.

A COBIT legújabb, ötödik kiadása magába foglalja a COBIT 4.1-et, a Val IT 2.0-t[60] és a Risk IT keretrendszereket, valamint jelentős mértékben hatással van rá a Business Model for Information Security (BMIS)[61] és az Information Technology Assurance Framework (ITAF)[62].

A COBIT 5 szemléletében és hatókörében is bővült a 4.1-hez képest, ugyanis a korábbi informatikai irányítás (IT Governance) hatókörét az érdekelt csoportok (stakeholders) igényeivel bővítve már nagyvállalati informatikai irányításról (Governance of Enterprise IT) beszélhetünk. Többek között a folyamatok és a kontroll célkitűzések is bővültek, módosultak. [28]

A COBIT 5 folyamatai:

- Értékelés, irányítás és figyelemmel kísérés (Evaluate, Direct and Monitor, EDM)
- Összehangolás, tervezés és szervezés (Align, Plan and Organise, APO)
- Építés, beszerzés és megvalósítás (Build, Acquire and Implement, BAI)
- Szállítás, szolgáltatás és támogatás (Deliver, Service and Support, DSS)
- Figyelemmel kísérés, értékelés és felmérés (Monitor, Evaluate and Assess, MEA)

A COBIT 5 magyar nyelvű fordításban is rendelkezésre áll.

4.6. Magyar Informatikai Biztonsági Ajánlások (MIBA)

A Közigazgatási Informatikai Bizottság (KIB) 25. ajánlásaként kiadott Magyar Informatikai Biztonsági Ajánlások (**MIBA**) című ajánlássorozat fő célja, hogy biztonságos informatikai rendszerek kialakítását és fenntartását segítse elő. A nemzetközi szabványokhoz és ajánlásokhoz igazodva a 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.

A **MIBIK** az ISO/IEC 27001:2005, ISO/IEC 27002:2005 és az ISO/IEC TR 13335 nemzetközi szabványokon, valamint az irányadó EU és NATO szabályozáson alapul. A MIBIK része az Informatikai Biztonsági Irányítási Rendszer (IBIR), amely a szervezet informatikai biztonságának tervezésére, üzemeltetésére, ellenőrzésére és javítására vonatkozik. A MIBIK további részei az Informatikai Biztonság Irányítási Követelmények (IBIK), amely az informatikai biztonság kezelésének hatékonyabbá tételéhez nyújt segítséget, lehetőséget teremtve a követelmények

[59] Department of Defense Directive 8570

[60] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Val-IT-Framework-2.0.aspx [utolsó letöltés: 2014. 07.01.]

[61] http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx [utolsó letöltés: 2014. 07.01.]

[62] http://www.isaca.org/itaf [utolsó letöltés: 2014. 07.01.]

és feladatok szakmailag egységes kezelésére, illetve az Informatikai Biztonsági Irányítás Vizsgálata (IBIV), amely az informatikai biztonság ellenőrzéséhez ad módszertani segítséget.

A **MIBÉTS** az ISO/IEC 15408:2005 és ISO/IEC 18045:2005 nemzetközi szabványokon, illetve a nemzetközi legjobb gyakorlatokon és nemzeti sémákon alapul. Keretet biztosít arra, hogy az informatikai termékek és rendszerek tekintetében a biztonsági funkciók teljessége és hatásossága értékelésre kerüljön. Értékelési módszertana alkalmas az operációs rendszerek, hardverek (például hálózati eszközök, tűzfalak, behatolás-észlelők, intelligens kártyák), szoftveralkalmazások (például különböző programnyelveken megírt kritikus alkalmazások) speciális biztonsági szempontjainak értékelésére. Ezzel a MIBÉTS a megbízható harmadik felek által végzett biztonsági ellenőrzés és audit egységes szempontrendszerét alkotja meg.

Az **IBIX** elsődleges célja, hogy segítséget nyújtson az informatikai biztonság megfelelő szintjének kialakításához önkormányzati és más informatikai szempontból kis méretű környezetben. Javasolt az anyag azon szervezetek számára, ahol a szervezet méreténél fogva nem áll rendelkezésre külön emberi és egyéb erőforrás az informatikai rendszerek biztonságának kialakítására és üzemeltetésére, hanem ezt „házon belül" kell megoldani.

4.7. Követelménytár

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

Ez a Követelménytár az elektronikus közigazgatás fejlesztéséhez és üzemeltetéséhez szükséges szabványokat, követelményeket és előírásokat tartalmazza. Az *IT biztonsági követelmények* és a *Termékek, szolgáltatások értékelésének, auditjának előkészítése* a 25. számú ajánlásra épülve azt kiegészítő vagy végrehajtását támogató előírásokat tartalmaz, illetve az *Egyéb követelmények, ajánlások* számos biztonsági szabványt mutat be. Az IT biztonsági követelmények részei:

- Biztonsági tervezési útmutató;
- IT biztonsági követelményrendszer – biztonsági szintek követelményei;
- IT biztonsági követelményrendszer érvényesítésének módja;
- IT biztonsági politika követelményei;
- IT biztonsági stratégia követelményei;
- IT biztonsági szabályzatok követelményei;
- IT biztonsági szintek és biztonsági kategorizálási minta;
- Közigazgatási Operatív Programok IT biztonsági környezete, követelményrendszere;
- Szabályzatmenedzsment-rendszer követelményei;
- Útmutató az IT biztonsági szintek meghatározásához.

A termékek, szolgáltatások értékelésének, auditjának előkészítése rész tartalma:

- IT biztonsági értékelő labor koncepció;
- Létező tanúsítások megfeleltetése – technikai leírás;
- Összetett termékekre vonatkozó értékelési módszertan;
- Rendszerekre vonatkozó értékelési módszertan;
- Termékekre vonatkozó értékelési módszertan;
- Útmutató akkreditorok számára;
- Útmutató rendszerértékelők számára;
- Útmutató rendszerintegrátorok számára;
- Útmutató tanúsítók számára.

4.8. A NIST kiadványai

A NIST (National Institute of Standards and Technology[63]) az Amerikai Egyesült Államok Kereskedelmi Minisztériumához tartozik. A NIST SP (Special Publication) 800 sorozata 1990-ben jött létre, mint közérdekű dokumentumok gyűjteménye, amelyek az Amerikai Egyesült Államok szövetségi kormánya számítógépes biztonsági politikáit, eljárásait és irányelveit írják le. Új sorozatként az SP 1800-as kiadványok a kiberbiztonsági gyakorlatokat mutatják be. A dokumentumok ingyenesen elérhetők, és nagyon hasznosak úgy a kormányzati szervek, mind a vállalkozások, az oktatási intézmények számára.

[63] Nemzeti Szabványügyi és Technológiai Intézet

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. A NATO védelmi előírása szerint „Az információvédelem az általános védelmi rendszabályok és eljárások alkalmazása az információ megsemmisülésének vagy kompromittálódásának megelőzése, felfedése ellen és helyreállítása céljából." Ettől megkülönbözteti az úgynevezett INFOSEC[64]-et, amely „a biztonsági rendszabályok alkalmazása a kommunikációs, információs és más elektronikus rendszerekben a feldolgozott, tárolt vagy továbbított információ bizalmasságának, sértetlenségének vagy rendelkezésre állásának véletlen vagy szándékos elvesztése ellen, és e rendszerek sértetlenségének vagy rendelkezésre állásának elvesztése ellen." [28] Ez gyakorlatilag megegyezik Európai Unió Tanácsának Biztonsági Szabályzata [29] előírásaival. Jól érzékelhető, hogy az információvédelem általában, mindenféle információ védelméről szól. Az INFOSEC része az információvédelemnek, és egyértelműen a kommunikációs, információs és más elektronikus rendszerekre vonatkozik.

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*).

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 magába.

Az INFOSEC további részterületei:

1. rejtjelbiztonság (CRYPTOSEC);
2. átviteli biztonság (TRANSEC);
3. hálózati biztonság (NETSEC);
4. kisugárzás-biztonság (EMSEC).

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, amelyek a következők:

Vevőközpontúság

A szervezetek vevőiktől függenek, ezért ismerniük kell a jelenlegi és a jövőbeli vevői szükségleteket, teljesíteniük kell a vevők követelményeit, és igyekezniük kell felülmúlni a vevők elvárásait.

Vezetés

A vezetők megteremtik a szervezet céljainak és igazgatásának egységét. Hozzanak létre és tartsanak fenn olyan belső környezetet, amelyben a munkatársak teljes mértékig részt vehetnek a szervezet céljainak elérésében.

A munkatársak bevonása

A szervezet lényegét minden szinten a munkatársak jelentik, és az ő teljes mértékű bevonásuk teszi lehetővé képességeik kihasználását a szervezet javára.

Folyamatszemléletű megközelítés

A kívánt eredményt hatékonyabban lehet elérni, ha a tevékenységeket és a velük kapcsolatos erőforrásokat folyamatként irányítják.

[64] INFOSEC: information security (angolul), az általánosabb értelmű információbiztonságtól való megkülönböztetés érdekében használt kifejezés. Magyar fordítása: elektronikus információvédelem.

Rendszerszemlélet az irányításban

Az egymással összefüggő folyamatok rendszerként való azonosítása, megértése és irányítása hozzájárul ahhoz, hogy a szervezet eredményesen és hatékonyan valósítsa meg céljait.

Folyamatos fejlesztés

A szervezet teljes működésének átfogó, folyamatos fejlesztése legyen a szervezet állandó célja.

Tényeken alapuló döntéshozatal

Az eredményes döntések az adatok és egyéb információ elemzésén alapulnak.

Kölcsönösen előnyös kapcsolatok a (be)szállítókkal

A szervezet és (be)szállítói kölcsönösen függnek egymástól, és kölcsönösen előnyös kapcsolatuk fokozza mindkettejük értékteremtő képességét.

A minőségirányítási rendszerekkel szemben támasztott követelményeket az ISO 9001:2015 (magyar megfelelője MSZ EN ISO 9001:2015) szabvány rögzíti. 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.

A vevői bizalom elnyeréséhez természetesen nem elegendő a minőségirányítási rendszer megléte, az ISO 9000 nemzetközi szabványsorozatban rögzített követelményrendszernek való megfelelés független tanúsító szervezet általi tanúsítása is szükséges.

A tanúsítás folyamata:

1. előaudit (nem kötelező, választható),
2. dokumentációvizsgálat,
3. helyszíni audit,
4. auditjelentés készítése (pozitív esetben javaslat a tanúsítvány odaítélésére).

A minőségirányítási rendszer kiépítésének időszükséglete a cég vezetési szintjeinek számától és tevékenységének összetettségétől függően mintegy 6–12 hónap.

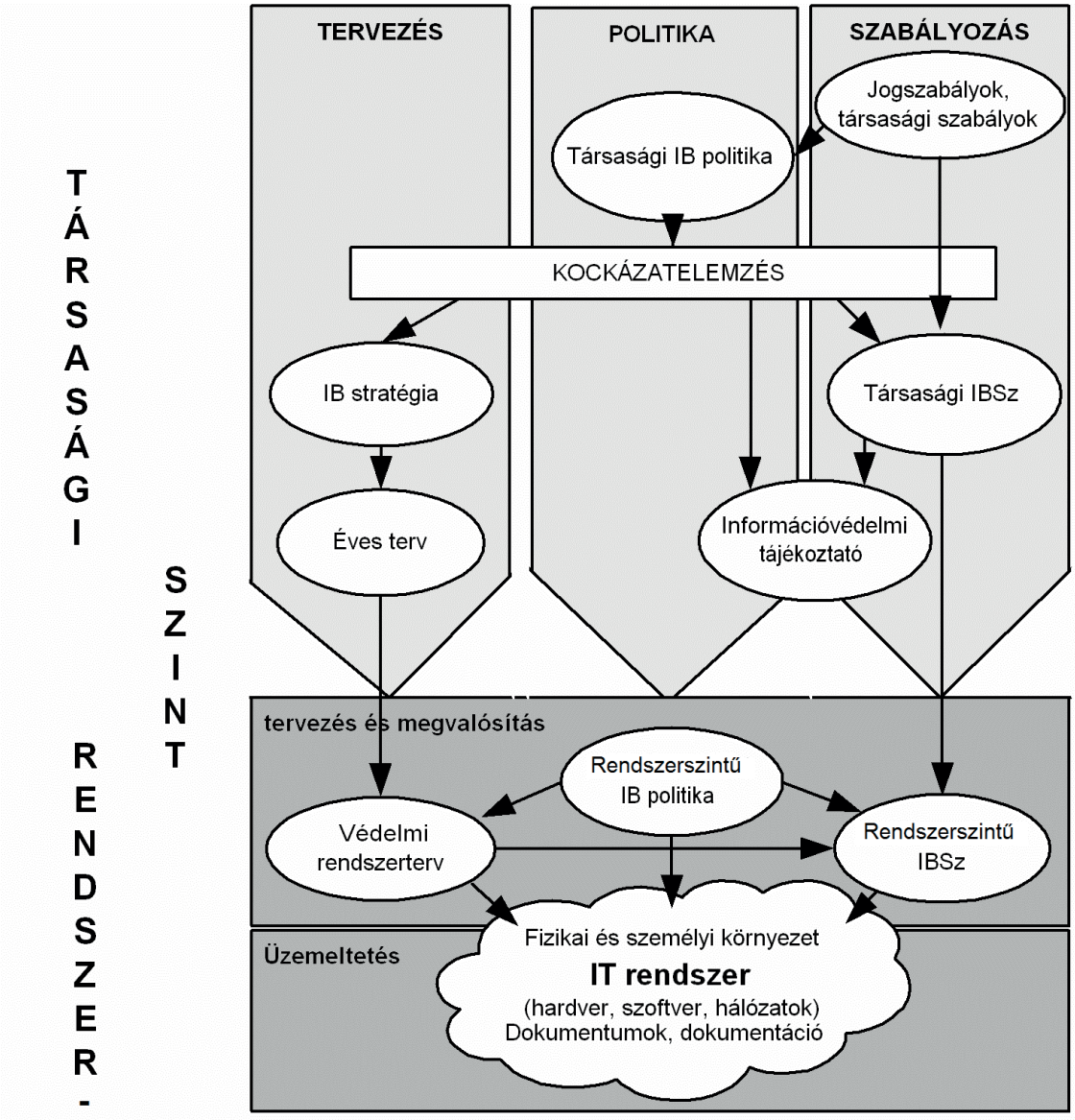
4.11. Környezetirányítás

A környezetirányítási-rendszerek (KMR) nemzetközi szabványát, az ISO 14001-et 1996 szeptemberében adták ki, legutolsó változata 2015-ben került kiadásra. A Magyar Szabványügyi Testület jelentette meg a magyar nyelvű fordítását „Környezetközpontú irányítási rendszerek. Követelmények alkalmazási útmutatóval" címmel, MSZ EN ISO 14001 jelzéssel, melyet 2015-ben frissítettek.

Az ISO 14001 a gazdaság minden szektorában alkalmazható a szervezetekre: az iparban, a mezőgazdaságban, a szolgáltatóiparban.

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 az 5. ábra mutatja.



5. ábra A védelem megvalósítása [1]

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 szintekre és rendszerszintekre tagolt hierarchikus szerkezetét kell kialakítani.

5.1. Az információbiztonsági irányítási rendszer

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.

Az Információbiztonsági Irányítási Rendszer (IBIR)[65] 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.

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[66] által is támogatott PDCA, magyarul TVEB[67] folyamatmodell használatát vezette be az Informatikai Biztonság Irányítási Rendszere fejlesztésének, megvalósításának és hatékonyságának biztosítására. Ezek a folyamatok lefedik a teljes tevékenységi ciklust, megcélozva az effektív informatikai biztonság irányítását egy folytonos fejlesztési programon keresztül.

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 [31]:

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.

5.1.2. Az Információbiztonsági Irányítási Rendszer létrehozása

Az Információbiztonsági Irányítási Rendszer létrehozása érdekében a következő **tervezés**i lépéseket kell megtenni tervezés során [32]:

a) **Az Inform**ációb**iztonsági Irányítási Rendszer területének, kiterjedésének definiálása** a szervezet üzleti jellegzetességeinek, elhelyezkedésének, aktíváinak értelmében. Az IBIR alkalmazási területét pontosan meg kell határozni. Az IBIR alkalmazási területét az elektronikus információs rendszer egészére kell meghatározni. Az alkalmazási terület meghatározása igényli a csatlakozási felületeket más rendszerekhez, szervezetekhez, külső beszállítókhoz, és szintén figyelembe kell venni olyan igényeket és függőségeket, mint például hogy a biztonsági követelmények kielégíthetőek-e az Információbiztonsági Irányítási Rendszerrel.

a) **Az informatikai biztonsági dokumentumok definiálása** az elektronikus információs rendszer üzleti jellegzetességeinek, elhelyezkedésének, aktíváinak értelmében, figyelembe véve a törvényi és szabályozási követelményeket. A vezetésnek el kell fogadnia az informatikai biztonsági dokumentumokat:

– Informatik*ai Biztonsági Stratégia*
– *Informatikai Biztonsági Szabályzat*
– *Informatikai Felhasználói Szabályzat*
– *Üzletmenet-folytonossági Terv*
– *Katasztrófa-elhárítási Terv*
– *Alsóbbrend*ű szabályozások (végrehajtási eljárásrendek)

---

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

[66] Organistaion for Economic Co-Operation and Development = Gazdasági Együttműködési és Fejlesztési Szervezet

[67] Tervezés – Végrehajtás – Ellenőrzés – Beavatkozás = Plan-Do-Check-Act – PDCA

a) **A kockázatelemzési eljárás meghatározása.** Az elfogadható kockázatok és az elfogadható kockázatok szintjének meghatározásához szüksége van egy követelményrendszerre. Minden esetben a szervezet maga dönti el, hogy melyik kockázatelemzési eljárást alkalmazza, de akármelyik módszert is kívánja használni a szervezet, az Információbiztonsági Irányítási Rendszer egészére kell kiterjeszteni.
b) **A kockázatok azonosítása** a vagyontárgyakról szóló jelentések és a vagyontárgyakkal kapcsolatos fenyegetettségek, a bizalmasság, a sértetlenség, valamint a rendelkezésre állás elvesztése figyelembevételével történik. A kockázatelemzés elengedhetetlen feltétele az adatleltár. Az Informatikai Biztonsági Szabályzatban részletezett módon az elektronikus információs rendszer egészére el kell készíteni az adatvagyonleltárt, mely minden egyes, az elektronikus információs rendszerben kezelt adatkörhöz meghatározza annak gazdáját, kezelőjét és értékét a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából, továbbá a kezelésére vonatkozó előírásokat (például személyes adat, a nemzeti adatvagyon része, nyilvános).
c) **A kockázatok elemzése** magába foglalja a gyenge pontokon (sérülékenységeken) keresztül a fenyegetések bekövetkezéséből eredő üzleti károk becslését, és az esemény bekövetkezési valószínűségének a meghatározását, majd ez alapján a kockázat szintjének becslését, és annak meghatározását, hogy vajon ezek a kockázatok még elfogadhatóak, vagy szervezetileg meghatározott eljárást igényelnek.
d) **A kockázatok kezelési módjának megállapítása és kiértékelése.** A már megállapított, felbecsült és ismert kockázatok kihatásának (arányának) megfelelő intézkedéseket kell hozni.
e) **A kockázatkezelési intézkedések tárgyának és céljának a kiválasztása**. Ha biztonsági intézkedések alkalmazhatóságáról születik döntés, akkor ki kell választania azt az intézkedési rendszert, amely megfelel kockázat kezelésére.

5.1.3. Az Információbiztonsági Irányítási Rendszer bevezetése és működtetése

A **végrehajtási** szakaszban biztosítania kell a tervezési szakaszban létrehozott IBIR eljárások használatát. Ezek magukba foglalnak egy jól működő kockázatkezelési rendszert, melyet az informatikai biztonsági fenyegetések azonosítására és kezelésére terveztek. A tervnek meg kell határoznia a biztonságot érintő események és a biztonsági fenyegetettségek esetén használatos vezetői és felhasználói tevékenységeket, valamint a vezetői és a felhasználói felelősségi köröket az Információbiztonsági Irányítási Rendszer alapján. [3]

El kell készítenie egy kockázatkezelési tervet, egy eljárásgyűjteményt, amely a kiválasztott biztonsági intézkedéseket, a szabályokat, a felelősségek meghatározását, a felhasználói tréningek leírását, az erőforrás-kezelést és a biztonsági események (incidensek) kezelését tartalmazza. A kiválasztott intézkedések megvalósításakor a legfontosabb szempont azok hatékonysága. [31]

5.1.4. Az Információbiztonsági Irányítási Rendszer ellenőrzése és felülvizsgálata

Az ellenőrzési szakaszban biztosítania kell a végrehajtási szakaszban létrehozott IBIR eljárások használatát. Ezek egy jól működő kockázatkezelési rendszert kell, hogy tartalmazzanak, amelyet az informatikai biztonsági fenyegetések azonosítására és kezelésére terveztek. Ahhoz, hogy az Információbiztonsági Irányítási Rendszer hatékonyan kezelje a biztonsági kockázatokat, folyamatosan ellenőrizni és nyomon követni kell az Informatikai Biztonsági Irányítási Rendszert érintő összes változást. [3]

Az ellenőrzési szakaszban újra kell vizsgálniuk az Informatikai Biztonsági Irányítási Rendszert: megfelel-e a hatóköre, az intézkedési rendszere kellően hatékony-e és megfelelő-e, az eljárások használata megfelel-e a követelményeknek, a létrehozott szabályzatok használhatók-e, a felelősségek kezelése megfelel-e a követelményeknek, a biztonsági tevékenységek elfogadottak-e, a biztonsági események alapján vannak-e kifejlesztve az eseménykezelő eljárások, továbbra is megfelelő-e az üzletfolytonossági terv. [32]

5.1.5. Az Információbiztonsági Irányítási Rendszer továbbfejlesztése és karbantartása

A beavatkozási szakaszban biztosítania kell a végrehajtási szakaszban létrehozott IBIR eljárások karbantartását, javítását, valamint az ellenőrzési szakaszban meghatározott további eljárások felülvizsgálatát. Az ellenőrző szakasz vizsgálatai által az Információbiztonsági Irányítási Rendszer folyamatait érintő azonosított változások miatt szükség van a biztonsági folyamatok javítására, csak így kezelhetők megfelelően az informatikai biztonsági rendszert érintő kockázatok. [3]

Fontos szempont, hogy minden javító és megelőző intézkedés rögzítve legyen, és ezen intézkedések eredménye megfelelő kommunikációs csatornákon jusson el a munkatársak és a felhasználók részére. Ez a kommunikáció a tevékenységek implementációjához elengedhetetlen. A szervezetnek biztosítania kell, hogy az Informatikai Biztonsági Irányítási Rendszerben implementált javító intézkedések megegyezzenek a kitűzött követelményekkel, és megvalósítsák az elérendő célokat. [31]

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. Az 5. 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. [1]

5.2.1. 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 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.

Ahhoz, hogy bármilyen biztonságpolitikát meg lehessen határozni, néhány alapkérdést kell tisztázni. Ezek a következők [1]:

- 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. Az adott rendszerre vonatkozó konkrét biztonsági osztályba sorolást 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 (ld. 5. ábra) információvédelmi tájékoztató. Sok cégnél ezt (is) társasági szintű informatikai biztonságpolitikának nevezik (Company Level IT Security Policy).

Mint azt az 5. ábra mutatja, a társasági és a rendszerszintű informatikai biztonságpolitikáknak 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, – a szerkezet és a főleg a biztonsági funkciókat érintő politikák vonatkozásában – meghatározó jelleggel bír a rendszerszintű politikákra nézve, amelyek konkrét politikái (például a jelszókezelési, a hozzáférési politikák) viszont a védelmi rendszerterv kidolgozásához szükségesek.

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;
- 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 készítésekor a korábban megfogalmazott védelmi alapelveket kell figyelembe venni, azok közül is elsősorban a *teljeskörűségre* és a *folytonosságra* törekedve.

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

- a fizikai környezethez,
- az hardver- és szoftver-rendszerhez,
- a kommunikációhoz, számítógépes hálózatokhoz,
- az adathordozókhoz,
- az input/output dokumentumokhoz és a dokumentációhoz,
- a külső és belső személyi környezethez kapcsolódó biztonsági szabályokra kell kiterjednie. [1]

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. [1]

Nagyobb szervezeteknél az informatikai biztonság szabályozását legalább két szinten javasolt megvalósítani (ld. 5. 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, megnevezi az egyes feladatok végrehajtásában kompetens beosztásokat és szervezeteket (felelős, irányító, végrehajtó, ellenőrző stb.). Rendszerszintű Informatikai Biztonsági Szabályzatot minden nagyobb alkalmazásra, a számítóközpontokra és a számítástechnikai infrastruktúrára ki kell alakítani. [1]

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 politika és a szabályzatok érvényesítését, valamint az ezeknek való megfelelés ellenőrzését olyan szervezeti egységek végezzék, amelyeknek a teljes társaságra nézve meg van 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 [1]:

- Minden informatikairendszer-beruházás előkészítésében az informatikai biztonsági rendszerrel kapcsolatos követelményeket, valamint a megvalósításhoz szükséges anyagi és humánerőforrásokat fel kell mérni, be kell állítani a beruházási tervbe, és megfelelő elemzés után jóvá kell hagyatni.
- Vezetői szinten biztosítottnak kell lenni, hogy az informatikai rendszerek megvalósítási projektje 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 biztonságmenedzselési és adminisztrációs funkciók kialakítása, valamint ezek működtetéséhez a megfelelő IT és informatikai biztonságmenedzsment-eszközrendszer és humánfeltételek biztosítása.
- Az informatikai rendszer üzemeltetésből történő kivonása keretében a biztonsági rendszer megszüntetését (jelszavak, jogosultságok megszüntetése, biztonsági adatállományok, adathordozók biztonságos törlés és üzemen kívül helyezése stb.) szabályozottan kell végrehajtani.

5.2.3. Az informatikai biztonsági stratégia

Miért van szükség informatikai biztonsági stratégiára? Stratégiára azért van szükség, hogy kialakítható legyen – egy hosszú, akár többéves 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 pédaként említhető, hogy az e-business fejlesztése a szervezetnél biztosan nagyban befolyásolni fogja a szervezet informatikai biztonságpolitikáját. A stratégiának fel kell tudni 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 szervezeti célkitűzések függvényében többféle út képzelhető el 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 *kulcsprojekteket*, amelyek sikeres megvalósításával a jövőkép elérhető. [1]

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.

5.2.4. Titokvédelmi és Ügyviteli Szabályzat

5.2.4.1. Titokvédelmi Szabályzat

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 [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

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.

A minősített adatok körébe tartozó iratok, információk esetében az 2009. évi CLV. törvény és az ahhoz kapcsolódó rendeletek, utasítások szerint kell eljárni!

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.

Az Ügyviteli Szabályzat térjen ki [1]:

- az ügyvitel szervezeti rendjére;
- az ügyvitel alapelveire;
- az ügyvitelben résztvevők 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.

5.2.5. Üzletmenetfolytonosság-tervezés

5.2.5.1. 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 Társaságnak 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." [1]

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 működés kiesésekből 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 *üzletmenetfolytonosság-tervezés* alatt a vészhelyzeti (katasztrófa[68]) és a nem katasztrofális jellegű üzemzavari 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 humánerőforrások 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. [1]

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, valamint 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 állapotába 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 sebeshetőségi rést – lényeges szerepet játszik a károkozásban, a megkívánt üzletmenet-folytonosság veszélyeztetésében." [1]

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 szolgáltatás-kiesések megelőzését, illetve minimalizálását célzó tervezési lépéseket értjük.

5.2.5.2. Az üzletmenetfolytonosság-tervezés célja

A teljes körű üzletmenetfolytonosság-terv kialakítása a következő előnyöket hozza magával [1]:

- 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 ügyfélszolgáltatások biztonságának növelése,
- a döntéshozatali kényszerek csökkentése az üzemzavar- és katasztrófa-elhárítás folyamatában,
- a jogszabályoknak és a belső szabályzatoknak való megfelelés erősítése.

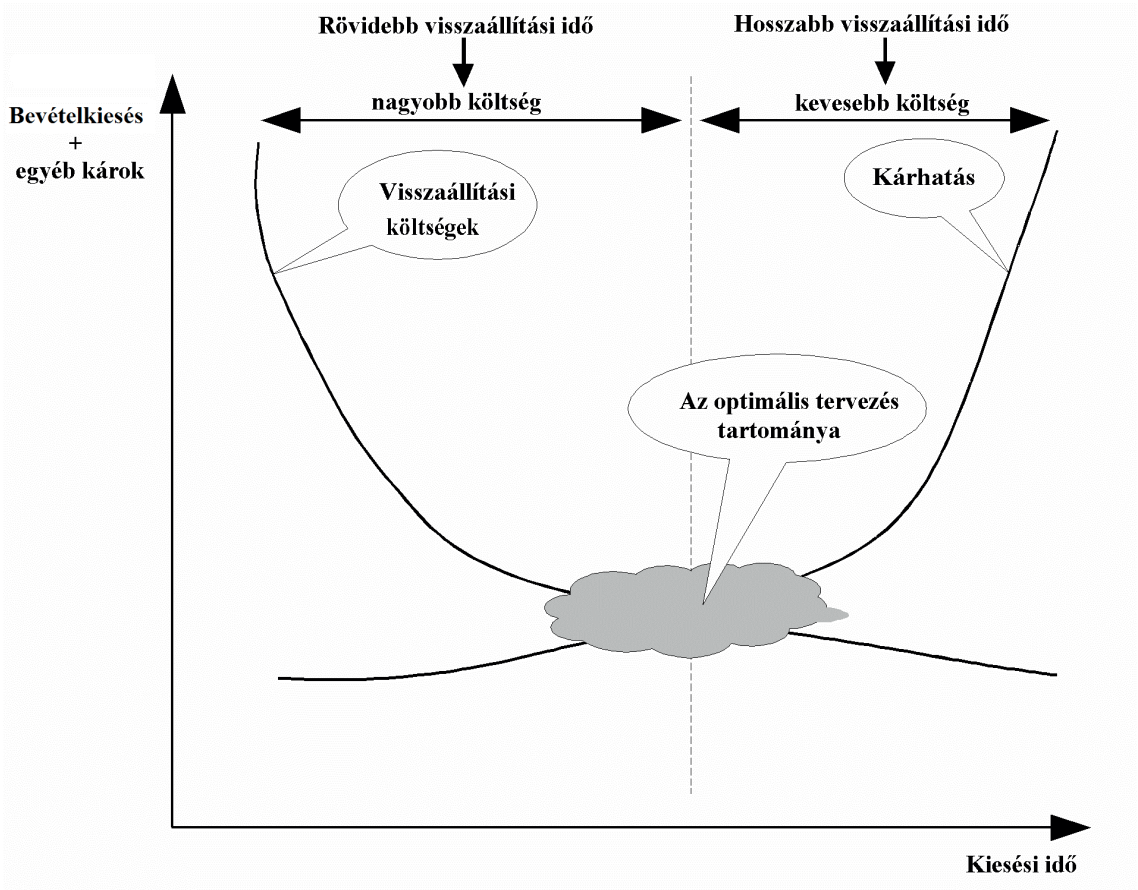
[68] A katasztrófa olyan helyzet, amikor az informatikai rendszert vagy a környezetét olyan természeti csapás, erőszakos beavatkozás vagy műszaki zavar éri, amely a teljes rendszer funkcionális működésének kiesésével, szélsőséges esetben a rendszer vagy környezete fizikai megsemmisülésével jár.

5.2.5.3. 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 rendszerelemeknek 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 normálállapot visszaállítását nem „mindenáron", hanem a valószínűsíthető kárnagyság és bekövetkezési gyakorisággal arányos költség szintjén kell biztosítani, azaz *minimális költségráfordítással maximális kockázatcsökkenést* kell elérni." [1]

Ezt az elvet szemléletesen a 6. ábra mutatja be.



6. ábra A kiesés költségei és a ráfordított idő aránya [1]

5.2.5.4. Az üzletmenet-folytonosság tervezési folyamata

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]:

1. Helyzetfelmérés és értékelés
2. Az üzletmenet-folytonossági terv elkészítése
3. Oktatás, tréning és tesztelés

5.2.5.5. Helyzetfelmérés és értékelés

- Projekt-előkészítő megbeszélés, amelyen megtörténik a részletes projektterv elkészítése.
- Előzetes helyzetfelmérő interjú tervének elkészítése (területek, személyek, előzetes ütemezés).
- Projektindító megbeszélés.
- Az interjúk megszervezése (személyek és időpontok egyeztetése), az interjúterv véglegesítésre kerül.
- Az interjútematikák elkészítése.
- A projektvezető számára 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 üzletmenet-folytonosság 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 folyamatprioritások, 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.

5.2.5.6. 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, illetve annak következetes érvényesítésével és ellenőrzésével megelőzhetők.

A megelőzési terv fontos fejezetét képezi a *tesztelési és tréningterv*, amely meghatározza a tesztelés formáit. Az üzletmenetfolytonosság-tervezés tesztelésének két formája javasolt [1]:

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-tervezési 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 eszközerőforrások haladéktalan mozgósítása, és a visszaállítás a lehető leggyorsabban és szervezetten történjen meg a tervben meghatározott utasítások szerint.

A visszaállítási terv a következőket tartalmazza [1]:
- 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 forgatókönyvei a következő lépésekre:
    - azonnali válasz (riadóterv),
    - futtató környezet helyreállítása,
    - 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.

A visszaállítási terv alapvető céljait a 7. ábra fogalmazza meg tömöten.

7. ábra A visszaállítási terv célja [1]

Az üzletmenet-folytonossági terv elkészítése után véglegesítésre kerül a *helyzetfelmérés és értékelés* projektfázisban elkészített előzetes intézkedéseinek terve, amely tartalmazza mindazon feltételek biztosítására vonatkozó intézkedéseket, amelyek megléte nélkül az üzletmenet-folytonossági terv nem működőképes és a következő projektfázisban elvégzendő üzletmenet-folytonossági terv tesztje és tréningje nem valósítható meg. [1]

5.2.5.7. Oktatás, tréning és tesztelés

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

Az oktatás célja [1]:
- az üzletmenet-folytonosság jelentőségének tudatosítása,
- az üzletmenet-folytonossági tervezés alapismereteinek 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 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 vagy katasztrófaeseményre kivitelezhető.

Az üzletmenet-folytonossági terv tesztje szimulált esemény bekövetkezésével és a terv szerinti 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.

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. Felvetődik a kérdés: miért?

A válasz a többi rendszerelem és az ember közötti lényeges különbségekben rejtőzik [33]:

– Az ember *kreatív intelligenciá*val rendelkezik, amit a legerőteljesebben azzal jellemezhetünk, hogy az ember a meglévő információs bázisára támaszkodva minőségileg új ismereteket, új összefüggéseket tud alkotni. Ha figyelembe vesszük azt is, hogy intelligenciája révén képes új információk, új összefüggések alkotására, illetve 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 humánmenedzsment-eszközöket, amelyekkel elő lehet segíteni meghatározott célok teljesítésére vonatkozó *motiváltság*át, saját belső meggyőződését, valamint a szervezet iránti *lojalitás*át. Végső soron azonban mindig ő dönt arról, hogy ezeket a környezeti befolyásokat magáévá teszi vagy sem. Ez fogja alapvetően meghatározni a *célokkal való azonosulás*át és a *normakövetési hajlandóság*át.
– Az ember *érzelmi lény*. Cselekedeteit és így a normakövetési hajlandóságát sok esetben alapvetően befolyásolják pillanatnyi érzelmei, ennélfogva – 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 következő táblázatban szereplő hatásokat a szervezetnek a szabályozás és a humánmenedzsment eszközeivel úgy kell befolyásolnia, hogy a mérleg nyelve mindig pozitív tartományban legyen. [33]

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 kikerülése 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

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 az emberierőforrás-kezelés vagy humánmenedzsment (Human Resource Management, HR Management) módszerei. Az emberierőforrás-stratégia (megszerzés, fejlesztés, mozgatás, leépítés) vezetői és szervezeti szintű feladatai részben meglevő ismereteken alapulnak, részben további kutatásokat igényelnek.

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

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 [33]:

- 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 emberierőforrás-kezelési feladatok [33]:

- 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.

6.2. 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 szakmai szempontokat előzetesen ki kell dolgozni. Új munkatárs 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 bizalmi munkakörben alkalmazásra kerülő személy életvitele átlátható és társadalmilag elfogadott, káros szenvedélyektől mentes, anyagi helyzete rendezett, nincs olyan adat, amely későbbi zsarolására lehetőségét adna.

A fontos és bizalmas munkakört betöltő személyeknek a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény szerint amennyiben minősített adatot kell megismerniük, egy a törvény mellékletében megadott kérdőívet kell kitölteniük. 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 gazdasági szférában történő – az előzőeknek többé-kevésbé megfelelő –személyellenőrzést életmódvizsgálatnak vagy környezettanulmánynak[69] nevezzük. Ilyen vizsgálatot magánnyomozóval lehet végeztetni. 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 rendezetlensége stb. ellenére alkalmazza-e a jelentkezőt vagy eltekint attól. Az életmódvizsgálatról szóló anyag alapkritériuma az objektivitás.

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.

[69] A környezettanulmányt a szakmai szleng KT-nak nevezi.

6.3. Megtartás – a lojalitás biztosítása

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

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 szervezet irányába, szolgálva ezzel az általános biztonság növelésének igényét is." [33]

Ennek érdekében az ösztönzőrendszer [33]:

- motiválja a munkatársakat,
- 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 menedzsmentfeladatok 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 lojalítás kialakításához tartozik, hogy a szervezet minden szintjén tudatosuljon [33]:

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

6.4. Oktatás-képzés

Az emberi viselkedést számtalan összetevő vezérli. Az eddigiekben érintettük az informatikai biztonsággal kapcsolatos attitűdöket, a szervezethez kapcsolódó lojalitást stb., de a magatartásszintű 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 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.

„A szervezet valamennyi munkatársát, és ahol szükséges, a harmadik fél felhasználóit is, megfelelő képzésben kell részesíteni a szervezet biztonsági szabályairól és eljárásairól. Ezeket az ismereteket rendszeresen naprakész ismeretek közlésével fel kell újítani. A képzés foglalja magába a biztonsági követelményeket, a jogi felelősséget, az üzleti óvintézkedéseket, valamint az informatikai eszközök helyes használatát, például a bejelentkezési eljárást, a szoftverek használatát. A képzést azelőtt kell lefolytatni, még mielőtt a felhasználók megkapnák a hozzáférési jogot (jogosultság) az informatikai rendszerekhez, vagy az adatokhoz.

Az oktatási és képzési dokumentáció és a módszertani kézikönyv megfelelő fejezetei részletesen kell, hogy tartalmazzák a biztonsági oktatásra vonatkozó információkat.

Az általános biztonságtudatosítási képzés mellett, melynek mindenkire vonatkoznia kell a szervezetben, különleges biztonsági képzés is szükséges az informatikai biztonsággal foglalkozó személyzet számára. A biztonsági képzés mélységének az informatikának a szervezeten belüli általános fontosságához kell igazodnia, és az adott szerep biztonsági követelményeinek megfelelően kell változnia. Amennyiben szükséges, sokkal kiterjedtebb oktatást,

például egyetemi kurzusokon való részvételt is biztosítani kell. Egy informatikai biztonsági képzési programot kell kialakítani az összes biztonsághoz kapcsolódó igény lefedésére.

Az informatikai biztonsági képzési program egyik legfontosabb célja a biztosítékok helyes kialakítása és használata. Minden szervezetnek az igényeknek és a létező, valamint a tervezett biztosítékoknak megfelelő módon ki kell alakítania a saját informatikai biztonsági képzési programját." [34]

6.5. Munkaszervezés

A munkaszervezés biztonsági, informatikai biztonsági „aranyszabályai" [33]:

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 munkatársak helyettesítését megfelelő képzettségű és gyakorlattal rendelkező 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 szervezeten belül nem engedhető meg, hogy egymással rokonságban álló személyek kulcsfontosságú munkaköröket betölthessenek.

6.6. A Social Engineering

A social engineering[70] az emberi hiszékenységre, együttműködésre építő támadási forma. Bár ezt az élet sok más területén is kihasználják, a social engineering kimondottan az információ megszerzésére irányul, ezen belül is elsősorban az informatikai eszközökön tárolt adatokra fókuszálva. Az évtizedek során felhalmozott tapasztalat szerint az IT eszközök védelme egyre kifinomultabb, azonban az ezeket használó emberek biztonságtudatossága csak minimálisan növekedett. Így a legjárhatóbb támadási eljárás az emberi erőforrás kihasználása, vagy – ahogy a közkeletű bölcsesség tartja – a legtöbb biztonsági probléma a billentyűzet és a szék között található.

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, amit a nagyon divatos adathalász támadások során is előszeretettel használnak. A kihasználható tulajdonságok között beszélhetünk még a befolyásolhatóságról is, ami megvesztegetés, zsarolás, megfélemlítés útján érhető el. Emellett nem szabad elfeledkezni a munkatársak figyelmetlenségéről, hanyagságáról és alulképzettségéről sem.

De ki a támadó? Az emberi hiszékenységgel való visszaélést számos tényező motiválhatja, így a social engineerek is több csoportba oszthatók:

- hackerek,
- ipari kémek,
- külföldi államok által megbízott hivatásos hírszerzők,
- személyes adatok ellopásával foglalkozó bűnözők,
- elégedetlen munkavállalók,

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

– konkurens vállalkozások megfigyelői,
– magánnyomozók,
– csalók,
– fejvadászok (akár bűnügyi, akár munkajogi értelemben),
– terroristák.

A social engineering típusú támadásokat két csoportba lehet sorolni. Egyrészt beszélhetünk humánalapú módszerekről, melyek közvetlen kontaktust feltételeznek a támadó és az áldozat között, másrészt azonosíthatunk számítógép-alapú technikákat, melyeknél a kapcsolat közvetett, a támadó valamilyen informatikai eszközön keresztül lép kapcsolatba az áldozattal.

A humánmódszerek a következők:
– Segítség kérése
– Segítség nyújtása
– Kölcsönösség kihasználása
– Megszemélyesítés
– Shoulder surfing – képernyő lelesése
– Tailgating – bejutás a bejáraton más embert követve, annak tudtán kívül
– Piggybacking – bejutás a bejáraton más embert követve, annak tudtával
– Dumpster diving – információk felkutatása a hulladékban

A számítógép-alapú támadások köre az alábbiak szerint alakul:
– Scam – hamisított weboldalak
– Adathalászat
    • Phishing – E-mailalapú
    • Vishing – VoIP-alapú
    • Smishing – SMS-alapú
    • Pharming – DNS eltérítésen alapuló
– Whailing – Vezetői IT eszközöket célzó támadás
– Baiting – Adathordozók szétszórása

6.6.1. Humánalapú technikák

A humánalapú technikáknál a támadó nem használ informatikai eszközöket, csupán pszichológiai technikákat vet be. Ennek a támadásnak a legnagyobb kockázata abban áll, hogy az áldozatnak, illetve szélesebb kitekintésben annak a szervezetnek, amelyiknél a célszemély dolgozik, nincs lehetősége műszaki jellegű védelmet kiépíteni.

Ezt a támadási technikát klasszikusan telefonon keresztül hajtják végre, hiszen így a legkisebb a lebukás kockázata, illetve sokkal nehezebb a számonkérés. Amennyiben a távoli támadás valamilyen okból nem kivitelezhető, a social engineernek személyesen kell felkeresnie az áldozatot. Ilyenkor a támadó megjelenhet ügyfélként, alkalmazottként vagy más, legitim módon az objektumban tartózkodó személyként. Esetleg szóba kerülhet még a nem IT eszközökön keresztüli kapcsolattartás, mint a hagyományos postai levél vagy a fax. A lényeg, hogy a felvett személyiség és a kapcsolattartási megoldás illeszkedjen a social engineering támadási stratégiához.

A leghatékonyabb stratégia, mely különösen multinacionális szervezeteknél, elosztott környezetben használható kiválóan az, hogy a támadó a szervezet egy másik munkatársának adja ki magát. Ehhez pontosan kell ismerni a szervezet belső működését, a munkatársak által használt szakzsargont, valamint a szervezeti hierarchiát. Ha a támadó mindezzel tisztában van, esetleg a szervezeti telefonkönyvhöz is hozzáfér, akkor a megfelelő áldozatot telefonon el tudja érni, és egy másik alkalmazottnak kiadva magát, tőle információkat tud szerezni. A legideálisabb áldozatok ebben az esetben az új munkatársak, akik még nem teljesen ismerik a helyi viszonyokat, de fontos információkhoz van hozzáférésük.

Segítség kérése

A legtöbb sikerrel kecsegtető humánalapú technika, hiszen az emberek alapvetően segítőkészek, és nem feltételeznek semmi rosszat egy kétségbeesett kollégáról. A klasszikus támadások alapvetően ezt a módszert követik. Elsődleges célpontjai a különböző ügyfélszolgálati munkatársak, akiknek ráadásul elsődlegesen az a feladatuk, hogy segítsenek a hozzájuk fordulókon. Mivel naponta számos kérést, kérdést kapnak, nem biztos, hogy ki tudják szűrni ezek közül a nem legitimeket.

Tipikus példa erre az, hogy a felhasználó kétségbeesetten telefonál az IT helpdeskre, hogy elfelejtette a jelszavát, és nem tud belépni a rendszerbe, de neki azonnal kell a hozzáférés. Ezt nyomatékosíthatja azzal, hogy ő nagyon fontos ember a szervezetnél és nem tűr halasztást kérésének kiszolgálása. Amennyiben a szervezetnél nem megfelelően

kidolgozott az identitásmenedzsment-eljárás, ez a szituáció könnyen zavart kelthet, és a támadó ilyen módon megszerezheti a kívánt jelszót. Sajnálatos módon azonban még a jól megtervezett folyamatok is támadhatókká válhatnak azzal, hogy ha a biztonsági kérdések valamilyen személyes adatra kérdeznek rá. A közösségi hálózatok elterjedésével ugyanis ezeket az információkat könnyen meg lehet szerezni, így még az olyan biztonsági kérdésekre is egyszerűen választ lehet találni, hogy „Mi a kutyám neve".

Ennek fordított esete az, amikor a támadó a helpdesk nevében keres meg egy kollégát. Ilyenkor valamilyen komoly informatikai problémát felvázolva kéri meg az áldozatot arra, hogy árulja el a jelszavát. A kérésnek az ad nyomatékot, hogy ha ezt az információt nem kapja meg, akkor nem tud kijavítani egy komoly informatikai hibát, például nem tudja megszüntetni azt a vírusfertőzést az áldozat számítógépén, ami az egész céges hálózatot leterheli. A célszemély ilyenkor egyrészt nem érti a valódi problémát az informatikai szakszavak használata miatt, érzi viszont a rá háruló felelősséget, ami akár számonkéréshez is vezethet nála, ezért készséggel kiszolgálja a támadót. A támadás célja egyébként nem csupán a jelszó megszerzése, de esetleg valamilyen kártékony kód lefuttatása is lehet.

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. Azonban a munkakörülményeket jobban megismerve a segítség nemcsak egy hiba kijavításához ajánlható fel, hanem a célszemély munkáját is segítheti a social engineer, például úgy, hogy valamilyen rutinfeladatot helyette végez el.

Ezt a megoldást más néven Reverse Social Engineeringnek is szokták hívni, hiszen, ha a kapcsolatfelvétel jól sikerült, a támadó elhitette az áldozattal, hogy képes minden problémáját megoldani, akkor a célszemély a későbbiekben is kikérheti „jótevője" segítségét, amivel további értékes információk szivároghatnak ki a szervezettől. Lépései:

1. Szabotázs: a támadó valamilyen hibát vált ki, amit a célszemély is érzékelhet.
2. Figyelemfelkeltés: a támadó felveszi a kapcsolatot az áldozattal és tudatosítja benne, hogy az adott hiba megoldására ő a legalkalmasabb.
3. Segítségnyújtás: a probléma megoldása során a beszélgetést úgy irányítja, hogy a számára hasznos információk – és emellett más, később hasznosítható információk is – elhangozzanak. Végül a támadó „megoldja" az általa okozott gondot.

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 olyan olcsó dolgokkal lehet elérni, mint egy ingyenkávé, vagy valamilyen cégemblémás golyóstoll. De ugyanezt a technikát figyelhetjük meg a Keresztapa című klasszikus filmben is, amikor egy nagy szívességért egészen rendkívüli dolgokat lehet megkapni („Eljössz a házamba a lányom esküvőjének napján és azt kéred tőlem, hogy pénzért gyilkoljak." … „Majd egy napon, bár lehet, hogy ez a nap sohasem jön el, viszonzásképpen én kérek szívességet tőled.").

A kölcsönösség feltételezi, hogy a két személy egymással jó viszonyban van, bizalom van közöttük, a támadó tudja úgy irányítani a szívességeit, hogy az a legjobban hasson a későbbiekben. Ez a fajta támadás tehát hosszú távú, komoly stratégiát igénylő eljárás, amire általában nem áll rendelkezésre sem kellő idő, sem kellő erőforrás. Kivéve akkor, ha a megszerzendő információ is olyan rendkívüli értékkel bír, amiért érdemes ekkora energiát befektetni.

Egyszerűbb forgatókönyvek is elérhetők, ekkor azonban már valamilyen informatikai eszközt is igénybe kell venni. Erre példa az olyan e-mail, mely egy regisztráció utána valamilyen apró ajándékot ígér. Ezzel a támadó hozzáférhet a számára szükséges információkhoz.

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. Elsősorban telefonon keresztül kihasználható, de esetleg személyesen vagy hagyományos levélben is kivitelezhető. A támadás jellegzetessége, hogy a támadó vagy egy fontos embernek adja ki magát, vagy azt állítja, hogy egy fontos ember nevében beszél.

A „fontos ember"-támadás arra épít, hogy általában egyetlen munkavállaló sem akadékoskodik, ha „felülről" érkezik egy kérés. Sajnálatos módon ezt erősíti az a tapasztalat, hogy a menedzsment hatalmi szóval ki tud bújni az általános IT biztonsági szabályok alól, ami erősíti azt a benyomást, hogy ennek a rétegnek „mindent szabad". A támadás feltételezi az alapos felkészülést a szervezeti felépítésből, és azt, hogy a támadó jól tudja kiválasztani, ki legyen a megszemélyesített fontos ember. Ehhez hasznos információt nyújt a szervezet honlapja, a megjelent

sajtócikkek, és általában bármi, ami a szervezet működéséhez kapcsolódik. Ha sikerült kiválasztani a „fontos embert", akkor a különböző közösségi hálózatokon fel lehet térképezni a személyét, így még hitelesebben lehet a nevében beszélni.

A támadás első lépése lehet az, hogy az áldozatot előre figyelmeztetjük arra, hogy a „fontos ember" keresni fogja. A figyelmeztetés érkezhet e-mailben, de akár látszólag a menedzser titkárnőjén keresztül is. Ezután következik a „fontos ember" hívása, melynek során a szükséges információkat meg lehet szerezni. Amennyiben az áldozat akadékoskodik, lehet figyelmeztetni a hierarchiabeli különbségekre, és akár más nyomásgyakorlással is lehet élni. Ez általában sikeres szokott lenni.

A felhatalmazásos forgatókönyvvel akkor élhet a támadó, ha valamilyen oknál fogva nem tudja megszemélyesíteni a „fontos embert". Ilyenkor a támadó a vezető egyik beosztottjának, de akár partnercég képviselőjének is kiadhatja magát. Figyelni kell arra, hogy a más nevében való beszélgetés, esetleg fenyegetőzés, kontrahatást válthat ki, az áldozat esetleg megpróbál rákérdezni a „fontos embernél" az állítottak valódiságára, tehát ezt a támadást akkor célszerű kivitelezni, ha a „fontos ember" nem elérhető az áldozat számára.

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. Ez lehet akár egy jelszó, de akár a bankautomatáknál a PIN-kódok megszerzésére is használhatják a megoldást. Tökéletes eljárás arra is, hogy egy egyébként nyílt ügyfélterületen meg lehessen szerezni egy jelszót az ügyintézőtől, folyamatosan nézve az informatikai rendszerrel történő interakcióját.

A támadás végrehajtása sok gyakorlást igényel, ugyanis a felhasználók általában gyorsan gépelnek, és egyszerre kell figyelni mindkét kéz leütéseit, hogy meg lehessen különböztetni például a kisbetű-nagybetű eltéréseket.

Piggybacking

A támadás során az egyébként legitim felhasználó jogosultságait használja ki a támadó. Általában az épültbe való bejutásra szokták ezt a technikát felhasználni. A támadót a célszemély a saját kártyájával engedi előre a bejáraton, tehát tudatos cselekedetről van szó. 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. Tipikus példája ennek az, hogy a támadó elvegyül a belépési jogosultsággal rendelkező munkatársak között, és velük együtt jut be a létesítménybe. Megkönnyíti a támadó dolgát az, ha valamilyen karbantartás vagy rendkívüli esemény következik be. Ilyenkor ugyanis lanyhul a beléptetési fegyelem, tehát könnyebben ki lehet játszani a védelmi kontrollokat.

Dumpster Diving

A papírmentes irodák elterjedése ellenére (vagy ezzel együtt?) a felhasznált iratmennyiség folyamatosan növekszik, így egyre több információt lehet kinyerni a papírhulladékból. Igaz ez akkor is, ha egyébként szakszerű iratmegsemmisítés folyik a szervezetnél. A nem kellően átgondolt informatikai biztonsági intézkedések a legtöbb helyen azt eredményezik, hogy a jelszavak post-it matricákra kerülnek, majd a szemetesbe. 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.

6.6.2. Számítógép-alapú technikák

Az elterjedtebb és egyszerűbb social engineering típusú technikák a közvetett kapcsolattartást preferálják, azaz a támadónak nem kell direkt kapcsolatba lépnie az áldozattal, így kisebb a lebukás veszélye. Erre kiválóan alkalmasak az informatikai eszközökön létrehozott becsapós tartalmak, melyek segítségével a kívánt információ egyszerűen megszerezhető. Gyakorlatilag bármilyen népszerű platformon létrehozható ilyen tartalom, így a következő technikák nem tudják bemutatni teljeskörűen az ilyen fajtájú átverések típusait.

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. Az ajánlat lehet például valamilyen részvétel egy fiktív

sorsolásban. A regisztráció során a felhasználó olyan kérdésekre ad választ, melyek a későbbiekben egy támadáshoz hasznosak lehetnek, például e-mail, jelszó. Nem összekeverendő az adathalász weboldalakkal, melyek megszólalásig hasonlítanak az eredetire, és melyek URL-ét valamilyen közvetlen csatornán tömegesen küldi ki a támadó.

Adathalászat

Az adathalászat vagy más néven phishing célja az, hogy valamilyen üzenet formájában egy valósnak tűnő weboldalra csábítsa a felhasználókat, ahol azok kiadják azonosítójukat. A szó eredete a password harvesting fishing, azaz a jelszólehalászás szóból származik. Magyarországon elsősorban banki weboldalak ellen indított támadásokból ismerhetjük, de gyakorlatilag az összes népszerű, főleg valamilyen pénzügyi értékkel bíró szolgáltatás a célpontok között van. Fajtái a következők:

- Phishing – E-mailalapú
- Vishing – VoIP-alapú
- Smishing – SMS-alapú
- Pharming – DNS eltérítésen alapuló
-

Phishing

E-mailek útján terjedő, hamisított weboldalakra vezető hivatkozásokat tartalmazó üzenetek tartoznak ide. A legrégibb és legelterjedtebb technológia, mely elsősorban pénzintézetek ellen irányul. A támadás során az áldozatot e-mailben értesítik arról, hogy valamilyen fontos okból be kell jelentkeznie a megcélzott szolgáltatásba. Ehhez mellékelnek egy URL-t, ami a hamisított weboldalra mutat. A nyomás fokozása érdekében az ügyfelet arról is tájékoztatják, hogy ha nem lép be a szolgáltatásba, akkor valamilyen kár fogja érni.

A támadás sokszor eredményes, hiszen vagy tömegesen küldik ezeket az üzeneteket, mely kis százalékban eredményes, de ez is több tucat áldozatot jelenthet, vagy célzottan, ekkor viszont magas sikerszázalék jósolható a pontos, ténylegesen hivatalosnak tűnő fogalmazás miatt. Mindez annak ellenére igaz, hogy a legelterjedtebb böngészők és levelezőkliensek fel vannak készítve az adathalász levelek és honlapok kiszűrésére.

Magyarországon a tömeges kísérletek általában sikertelenek, mert az adathalász e-mail valamilyen automatikus fordítóprogrammal készül, rossz magyarsággal, ezért nehezen dőlnek be neki az olvasók. Emellett kialakult az a riasztórendszer, amivel a célzott bankok időben értesíteni tudják ügyfeleiket és a médiát a próbálkozásról. Az eseménykezelő központok közreműködésével pedig órák alatt képesek lekapcsoltatni a földrajzilag távol levő phishing szervereket is. A célzott támadások azonban Magyarországon is komoly károkat tudnak okozni.

Vishing

Olyan adathalászat-típus, mely hanghálózaton, elsősorban VoIP csatornán keresztül terjed (a VoIP a voice phishing szóösszetételből ered). A támadást a bankok azon tanácsa ihlette, hogy ha az ügyfél nem bízik az értesítő e-mailben, akkor telefonon győződjön meg arról, hogy az üzenet hiteles volt-e. A támadó a tömeges tárcsázás (wardialing) módszerével végigtelefonál egy számtartományt, és ahol felveszik a telefont, ott egy előre felmondott üzenetet játszanak le, amiben értesítik az ügyfelet az előző pontban már részletezett „problémák" egyikéről, és megkérik a fogadó felet, hogy hívjon fel egy telefonszámot a probléma megoldása érdekében. A hívott szám másik oldalán szóban kérik be azokat az információkat, amiket egyébként a hamisított weboldalon kérnének.

Mivel a telefon hiteles forrásnak minősül a legtöbb embernél, a támadási módszer pedig kevéssé ismert, meglehetősen sikeresnek tekinthető. Az IP-alapú távközléssel ráadásul olcsóvá vált a kivitelezése.

Bizonyos besorolások szerint ebbe a kategóriába tartozik az azonnali üzenetküldő hálózatokon keresztüli phishing is. A megtévesztő üzenetet általában valamilyen angol nyelvű bevezető szöveg előz meg, ezután következik a hamisított weboldalra mutató URL. A cél itt elsősorban az adott IM szolgáltatás bejelentkező nevének és jelszavának megszerzése, mely egyrészt hasznos információ, másrészt be lehet vele jelentkezni az áldozat profiljába, és az ismerőseinek is el lehet küldeni a megtévesztő üzenetet.

Smishing

A smishing az SMS-en keresztül érkező adathalász üzenetek gyűjtőneve. Az ötletet az adta, hogy számos banknál SMS-ben értesítik az ügyfeleket az egyes internetbanki tranzakciók állapotáról. A smishing típusú üzenet lényege, hogy ebben a formában értesítik az ügyfelet a számláján bekövetkezett problémáról, és megadják azt a telefonszámot, ahol a problémát meg lehet oldani. A telefonszámon az előző pontban leírt megoldással szedik ki az információt az áldozatból. A találati arány viszonylag magas lehet, hiszen nagyon sokan használják az internetbanki megoldásokat. A támadás kivitelezése azonban költséges, hiszen az SMS pénzbe kerül.

Pharming

Új típusú phishing támadás, melynek eszközei azonban régóta ismertek. Ennél a támadásnál a cél az, hogy a legitim szolgáltatást használni kívánó felhasználót a szolgáltatás domain nevének eltérítésével a hamisított weboldalra irányítsa. Ez gyakorlatilag azt jelenti, hogy a felhasználó a megfelelő URL-t írja be a böngészőjébe, de a DNS-szerver más IP-címre irányítja a felhasználót. Lehetőségek:

1. DNS cache poisioning: A helyi számítógép tárolja a gyakran látogatott weboldalak IP-címeit, így a DNS-feloldás hamar megtörténhet. Ha a támadó valamilyen módon be tud avatkozni ennek a DNS cache-nek a működésébe, akkor könnyen el tudja téríteni a felhasználót, hiszen a feloldás elsőként a cache-ben történik. A beavatkozás például kártékony kódok segítségével történhet.
2. Szerveralapú DNS cache poisioning: a szolgáltatónál levő DNS-szerver megtámadásának lehet ez az eredménye, az előző pontban leírt módszerrel. Mivel a szolgáltatói DNS-szerverek kiemelt biztonságúak, az ilyen támadások valószínűsége csekély.
3. Cross-site Scripting (XSS): legitim weboldalba beágyazott nem legitim kód, mely nagyon gyakori hiba a weboldalakon. A támadó a hivatalos oldalon talál egy olyan űrlapot, melyen keresztül perzisztens, azaz állandó módon be tud szúrni egy kódot, ami minden oda látogató felhasználónál lefut. Ez lehet például egy URL vagy átirányítás, ami egy hamisított weboldalra viszi a gyanútlan felhasználót. Itt egy valósnak tűnő bejelentkezési oldal tűnik fel, ami a már ismert módon szerzi meg az áldozat adatait.

Whaling

Bizonyos tanulmányok szerint a phishing egyik alfaja, azonban itt nem új technikáról beszélünk, hanem a célpontok köre szűkül egy bizonyos felhasználói körre. Ez a felhasználói 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.

6.6.3. A támadás forgatókönyve

A social engineering típusú támadás céltól függően más és más környezetben kerül végrehajtásra, de a forgatókönyve általában állandó. A leggyakrabban valamilyen műszaki tesztelés előzi meg a támadást, amikor is felmérésre kerül az az informatikai környezet, amihez a hiányzó információkat ilyen módon lehet megszerezni.

A social engineering típusú támadás 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.

6.6.3.1. 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.

Internetről szerzett információk

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. A főbb információforrásokat az alábbiakban részletezzük.

A szervezet saját honlapja

A saját weblap a támadó első kiindulási pontja. Itt általában megtalálható a szervezet tevékenységi köre, szervezeti hierarchiája, vezetőinek neve, fényképe, elérhetősége. Egyértelműen kiderülnek a címzési konvenciók, sokszor még a szervezet belső telefonkönyve is megtalálható rajta. Minden adott tehát ahhoz, hogy a kezdő információkat össze lehessen szedni. Kitűnően alkalmas ez a forrás a whaling típusú támadások célpontjainak összegyűjtésére is.

Nagyon gyakori, hogy a honlapon keresztül belső dokumentumok is elérhetők akár szándékosan, akár véletlenül. Szintén beszédesek a sajtóközlemények is. A támadás előkészítése során tehát nem lehet elfeledkezni ennek a forrásnak a fontosságáról.

Közösségi hálózatok

A szociológiai kutatások azt mutatják, hogy egy magára adó ember nem teheti meg, hogy nincs fent a közösség hálózatok valamelyikén. Így ugyanis fontos kapcsolatokról, információkról marad le. A közösségi hálózatok működésükből fakadóan viszont olyanok, hogy a felhasználó hajlamos mindent megosztani magáról, még azt is, amit egyébként a valós életben, egy beszélgetés során nem hozna szóba. Egy social engineernek ez valódi aranybánya.

Különösen hasznos a mindennapi időtöltéssel kapcsolatos információkat böngészni, ugyanis a kapcsolatépítés során ezekből lehet jól kiindulni a célszemély behálózásakor. A munka és a szabadidő leírása ezeken az oldalakon összefolyik, egy idő után az ember nem is figyel arra, hogy mit ír le. A sikeres támadás valószínűsége hatványozottan nő azzal, hogy a célszemély mennyire aktív felhasználója ezeknek a szolgáltatásoknak, de tudomásul kell venni, hogy a közösségi média felhasználásának nem lehet, és nem is biztos, hogy szabad gátat szabni.

Keresőoldalak

Az internet világában az információk nem centralizáltan, hanem szétszórva találhatók meg, számosságuk viszont minden korábbinál nagyobb. Ebben a káoszban segítenek rendet vágni a keresőoldalak, mely keresők az internet olyan bugyrait is bejárják, amire egy social engineernek soha nem lesz erőforrása. Az ügyesen megfogalmazott keresőszavakkal akár a céges honlapok rejtett információt vagy a célpontszemély teljes életútját is meg lehet lelni.

Minden keresőoldalnak megvan a saját keresési mechanizmusa, melyek segítenek az egészen összetett keresési feltételekre is releváns eredménnyel szolgálni. A keresőoldalak rosszindulatú felhasználását a szolgáltatók próbálják szűrni, de az igazán célzott támadásokat nem lehet megakadályozni. Számos esetben bizonyosodott már be az, hogy ezzel a módszerrel olyan belső dokumentumok is fellelhetők, melyekről az adott szervezetnél senki nem tudta, hogy kívülről elérhetők.

Telefonon keresztüli információszerzés

Amikor a webes keresés nem éri el a kívánt eredményt, vagy további információkra van szükség, a legcélszerűbb telefonon folytatni az adatgyűjtést. Ez a megoldás abban is segíti a támadót, hogy ne kelljen személyes kapcsolatba kerülnie a célponttal. Minden valószínűség szerint az előzetes információgyűjtés már lehetővé tette, hogy a legmegfelelőbb embert lehessen megtalálni telefonon keresztül. Ehhez nem is kell a telefonszámát tudni, a központ a név bemondása után már kapcsolja is a célszemélyt. A telefonos támadások ezután a korábban tárgyaltak szerint történik meg.

Írásban történő információszerzés

Írásos forma alatt lehet érteni az e-mailt, a faxot és a hagyományos levelet is. A lényeges az, hogy a támadó itt sem kerül közvetlen személyes kapcsolatba a kiszemelt munkatárssal. A módszer nehézsége a telefonon keresztüli érintkezéshez képest, hogy a támadónak nincs lehetősége befolyásolni a történéseket, hiszen a leírt szöveget nem tudja utólag módosítani, a válaszadást pedig nem tudja az általa kívánt irányba terelni. Sok szervezetnél ráadásul ellenőrzik a faxokat, leveleket, tehát nem biztos, hogy az előzetes szűrőn egyáltalán átjut az írásos megkeresés.

Személyes felkeresés

Ha már semmilyen más megoldás nem marad, végső esetben személyesen is fel lehet keresni a kiszemelt szervezetet és személyt. Az információgyűjtés fázisában ez azonban nagyon ritka, hiszen még nem áll a támadó rendelkezésére annyi információ, amennyivel magabiztosan el tudja kerülni a lebukást. A tapasztaltok alapján azonban ez a megoldás esetleg olyan információkkal is szolgálhat, amire a többi forma nem. A legtöbb szervezetnél

ugyanis csak elvben érvényesül a tiszta asztal szabálya, azaz fontos információk hevernek szanaszét az irodában. Ebbe a kategóriába tartozik a hulladék átvizsgálása is, akár a telephelyen belül, akár azon kívül.

6.6.3.2. 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, de ezzel nincs tisztában, azaz 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.

6.6.3.3. Kapcsolat kihasználása

A támadás bonyolultságától függően előbb-utóbb elérkezik az a pillanat, amikor a támadó megkéri a célszemélyt arra, hogy tegyen meg neki valamilyen szívességet. Ez még nem jelenti feltétlenül a támadás elindítását, de ez az ugródeszka szükséges ahhoz, hogy a támadó elérje a célját.

6.6.3.4. Támadás végrehajtása

A social engineering típusú támadás csúcspontja, amikor a támadó hozzájut az őt érdeklő információkhoz, és sokszor olyan adatokhoz is, amiknek létezéséről nem tudott, de később még hasznát veheti. A sikeres támadás egyik következménye lehet, hogy a kiépített kapcsolat hosszabb távon is felhasználható, és a biztonságért felelős szervezet nem is tud a létezéséről.

Az emberi hiszékenységet kihasználó információszerzés, a social engineering az egyik legfontosabb eszköz az informatikai rendszerek támadóinak kelléktárában. Nehezen észlelhető, de hatalmas károkat tud okozni. A jelenséggel tehát foglalkozni kell, még akkor is, ha kivédése szinte lehetetlen.

A legtöbb információbiztonsági ajánlásban szerepelnek olyan elemek, melyek közvetve vagy közvetlenül segítenek a social engineering sikerességét és hatásait csökkenteni. A megfelelő szabályzati rendszer, a biztonságtudatossági oktatás, a gondosan megtervezett authentikációs és authorizációs eljárások, a munkatársak biztonsági ellenőrzése, vagy éppen a beléptetésnél használatos fizikai kontrollok mind-mind segítenek megelőzni a bajt. Ezek hatékonyságáról pedig egy etikus hackelési projektben lehet meggyőződni. Az ember ugyanis mindig a leggyengébb láncszem a védelemben, és ezt a szervezet ellenfelei, ellenségei ki is fogják használni.

7. 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.

A fizikai védelmen túl azonban számos egyéb, a fizikai térben megvalósítandó információvédelmi feladat van, hiszen a tápáramellátás vagy a klimatizálás megfelelő működése is elengedhetetlen.

7.1. A hagymahéj-elv

Az informatikai infrastruktúra különböző funkcionális területeinek jó megválasztásával lehetőség van a fizikai biztonságot veszélyeztető fenyegetések csökkentésére. Mind az eszközök és adathordozók elhelyezése, mind a különböző funkcionális területek térbeli kapcsolata kulcsfontosságú szerepet játszik. Az alábbi kritériumokat kell teljesíteni az informatikai infrastruktúra elhelyezésére kiválasztott hely fizikai biztonságának felbecslésekor [35]:
- minimális kockázatot jelentsenek a szomszédos berendezések és szerkezetek vagy munkafolyamatok,
- a telekommunikációs és közművezetékek, rezgések vagy vegyszerek miatti fellépő, az informatikai rendszerek fizikai biztonságát fenyegető kockázatok elkerülése,
- a természeti katasztrófák (árvíz, viharok, villámlás, földrengés) miatt bekövetkező kockázatok elkerülése – regionális sajátosságok felbecslése,
- a számítóközpont (szerverszoba) funkcionálisan különálló terület legyen,
- rongálással szembeni védelem "védett" hely kiválasztásával,
- a megbízókat érintő potenciális fenyegetések felbecslése a szervezet *társadalmi státusza miatt.*

A számítóközpontok, szerverszob*ák* tervezésekor a különböző funkcionális területeket azok biztonsági követelményei és küldetéskritikus értékük szerint kell elrendezni.

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 biztonsági határvonalak a zónák között elhelyezett ellenőrzött és védett áthaladási pontok, melyek konfigurációja úgy van kialakítva, hogy megfeleljenek a megbízó követelményeinek.

A lehetséges rongálások veszélyének elkerülése érdekében a különböző funkcionális területeket úgy kell elkülöníteni, hogy csak korlátozott hozzáférés legyen megengedett az érzékeny területek esetén.

7.2. Mechanikai védelem

„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, valamint a tűzvédelem szempontjai." [1]

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.

7.2.3.1. Az építményekkel szembeni elvárások

Az informatikai rendszerek fenyegetettsége szempontjából az épületek nagy jelentőséggel bírnak, mivel számítástechnikai alkalmazások jelentős mennyiségben itt kerülnek felhasználásra. A biztonság tervezése szempontjából azonban az épített környezetnek különös jelentősége és többszörös rendeltetése van.

Az országos településrendezési és építési követelményekről szóló 253/1997. (XII. 20.) Korm. rendelet előírásai szerint az építményeket és azok részeit a rendeltetési céljuknak megfelelően, a helyszíni adottságok figyelembevételével úgy kell megvalósítani, hogy feleljenek meg:

- az állékonyság és mechanikai szilárdság,
- a tűzbiztonság,
- a higiénia, az egészség- és a környezetvédelem,
- a használati biztonság,
- a zaj és rezgés elleni védelem,
- az energiatakarékosság és a hővédelem,
- az életvédelem és a más jogszabályok szerint vonatkozó követelményeknek, emellett ne akadályozzák a szomszédos telkek és építmények, önálló rendeltetési egységek zavartalan rendeltetésszerű használatát, továbbá illeszkedjenek a környezet és a környező beépítés adottságaihoz, építészeti megoldásaikkal járuljanak hozzá a táj és a településkép esztétikus alakításához.

7.3. Élőerős védelem

Az élőerőt egyrészről mint reagáló erőt kell alkalmazni, másrészről az élőerővel történő őrzésnek a mechanikai és elektronikai védelemmel egységes egészet kell alkotnia úgy, hogy az élőerő részben kiegészítse, részben megerősítse a mechanikai és elektronikai védelmeket, a beléptető rendszert.

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.

7.4. 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 elektronikai jelzőrendszer feleljen meg az MSZ EN 5013x-x „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." [36]

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. [36]

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. [36]

Teljes körű a tárgyvédelem, ha az elektronikai jelzőrendszer éles üzemmódban az összes védendő tárgyat felügyeli, páncélszekrények és páncéltermek esetében a felügyelet nyitásra, zárásra és áttörésre is kiterjed. [36]

Teljes körű a személyvédelem, ha az elektronikai jelzőrendszer folyamatos üzemmódban az összes védendő, támadásnak kitett személyt „felügyeli". [36]

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." [36]

„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 érzékelőeszközt, 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 érzékelőeszközök 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-fényjelző 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 videó-megfigyelés egészítheti ki."[1]

7.5. 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 tűzoltóeszközök, a beépített tűzjelző és automatikus oltórendszerek. Kialakításukra az építési és tűzvédelmi jogszabályok, szabványok adnak iránymutatást. [1]

Egy szervezeten belül gyakran okoz dilemmát, hogy a szerverhelyiségek tűzvédelme érdekében legyen-e telepítve automatikus működésű oltórendszer akkor is, ha azt jogszabály nem írja elő. A szervezetnek mérlegelni kell az

informatikai rendszerében tárolt és feldolgozott adatok alapján az oltórendszer telepítésének szükségességét, mert előírás híján is szükséges lehet az automatikus beavatkozás.

7.6. 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. 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 földelőrendszerek, valamint a különböző mérő-, szabályozó (épület-felügyeleti, vagyonvédelmi) 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 méreteket is jóval meghaladhatják. 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. [1]

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, ami jelentősen meghaladja a berendezések üzemi szigeteléseire előírt 1 perces szabványos vizsgálófeszültség értékeit. Ez a magyarázata annak, hogy a villámcsapás másodlagos induktív hatása „túlfeszültségként" egyszerre több ponton is átütheti az áramkörök szigetelését.

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

7.7. Kisugárzás- és zavarvédelem

A számítástechnikai eszközök, így például a monitorok[71], 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 minősített adatok esetén, esetleg a legmagasabb szintű bizalmassági 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 kisugárzás-védelemé, 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 EN55024 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 a megfelelőek.

A kisugárzás elleni védelem TEMPEST[72] néven ismert.

---

[71] Nem csak a régi katódsugárcsöves (CRT), de a legmodernebb LCD monitorok is!

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

A védelmi zónából az adatok vezetés vagy sugárzás útján történő kijutását szűréssel és árnyékolással kell megakadályozni. E téren mindig kompromisszumra van szükség a védelmi zóna mérete és az árnyékolás, valamint a szűrés mértéke (és ennek költsége) között. A kompromisszum alapja rendszerint az, hogy a védelmi zóna határán a lehallgatás ne legyen lehetséges az objektum környezetében normális személy- és járműforgalom körülményei között.

Tehát az informatikai berendezések árnyékolását és szűrését úgy kell elkészíteni, és a védelmi zóna méretét úgy kell meghatározni, hogy a zóna határán kívül ne lehessen az információt visszaállítani vagy ilyen célból rögzíteni. Más szóval a védett zónán kívül oly alacsony szintű legyen a sugárzott és vezetett jelek nagysága, hogy azok felfogásának, feldolgozásának költsége (ezek nagyon drága eszközök!) ne érje meg az információ kinyerését, illetőleg működési zavar létrehozása konspiráltan ne legyen lehetséges. Ehhez a védelemnek az 1 KHz és a 10 GHz közötti tartományban, a távolság függvényben 20–100 dB csillapítást kell biztosítania.

Az URH sávban (mintegy 400 MHz felett) még a légkondicionáló befúvónyílása is áthatolhat, ha mérete meghaladja a legrövidebb hullámhossz negyedét.

A kisugárzás- és zavarvédelem további megoldásai:

- a sugárzott információ és zavar csökkentése a helyiség határoló falain kialakított elektromágneses árnyékolást biztosító Faraday kalitkaszerű árnyékoló burkolattal,
- a v*édelmet igénylő adatvezetékek fizikai szeparálása a* védelmet nem igénylő vezetékektől,
- a vezetett információ és zavar leválasztása megfelelően méretezett szűrőáramkörökkel,
- a kisugárzás elleni v*édelemben*, szükség esetén úgynevezett „zajgenerátor” alkalmazása,
- az árnyékolt térbe be- és kilépő árnyékolt átviteli vezetékeken és gépészeti csővezetékeken potenciálkiegyenlítő bekötések elhelyezése, az érintésvédelmi EPH bekötéseken túlmenően.

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. A 4.2. 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 hagyományos eljárással 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 felhasználó-azonosítója 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.

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.

8.1. Dokumentumkezelés az informatikai rendszerekben

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. Jellemző példa volt erre, amikor az egyik informatikai biztonsági vizsgálat során megállapításra került, hogy 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 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.

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. 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.

8.2. Az elektronikus köziratok kezelése

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. Előírja, hogy:

- Az iratokat és az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés, megsemmisítés, valamint a megsemmisülés és sérülés ellen.
- Az iratokkal és az azok kezeléséhez alkalmazott elektronikus adathordozókkal kapcsolatban minden esetben rendelkezni kell a szükséges védelmi intézkedésekről, beleértve a vírusvédelmet és a kéretlen elektronikus üzenetek elleni védekezést is. Biztosítani kell az illetéktelen hozzáférés megakadályozását mind a papíralapú, mind az elektronikus adathordozó esetében.
- A közfeladatot ellátó szervek alkalmazottai csak azokhoz az – akár papíralapú, akár elektronikus adathordozón tárolt – iratokhoz, illetőleg adatokhoz férhetnek hozzá, amelyekre munkakörük ellátásához szükségük van, vagy amelyre az illetékes vezető felhatalmazást ad.
- A szerv vezetője köteles az üzemeltetés és az adatbiztonság olyan szabályozására, amely alapján a feladatok, hatáskörök pontosan meghatározásra kerülnek és végrehajthatók.
- A közfeladatot ellátó szerv vezetője, illetőleg tevékenységi körében iratkezelési feladatokat ellátó vezető, ügyintéző, ügykezelő köteles gondoskodni az iratkezelési szoftver által kezelt adatok biztonságáról, s megtenni azokat a technikai és szervezési intézkedéseket, kialakítani azokat az eljárási szabályokat, amelyek az üzembiztonsági, adatvédelmi szabályok érvényre juttatásához szükségesek.
- A közfeladatot ellátó szervek iratkezelését úgy kell megszervezni, hogy:

a) a szervhez érkezett, ott keletkező, illetve onnan továbbított irat azonosítható, fellelési helye, útja követhető, ellenőrizhető és visszakereshető legyen;
b) az irat tartalma csak az arra jogosult számára legyen megismerhető;
c) az irat kezeléséért fennálló személyi felelősség egyértelműen megállapítható legyen;
d) az irat szakszerű kezeléséhez, nyilvántartásához, kézbesítéséhez, védelméhez szükséges személyi, tárgyi, technikai feltételek biztosítottak legyenek;
e) a beérkezett és továbbított iratok megváltoztathatatlansága biztosított legyen;
f) a rendszeres selejtezés elvégzésével az irattári iratanyag felesleges felhalmozódása megelőzhető, a maradandó értékű iratok megőrzése biztosított legyen;
g) az ügyintézéshez, a döntések előkészítéséhez, a szervezet rendeltetésszerű működéséhez megfelelő támogatást biztosítson.

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.

A fő elvek

1. Feladatok szétválasztása (Separation of Duties)
   - Célja, hogy egy folyamat lépéseit különböző személyek végezzék el.
   - Ehhez a folyamatot meg kell tervezni.
   - Meg kell akadályozni, hogy egy személy a teljes folyamatot ellenőrizze és manipulálja. (Például egy könyvelési osztályon nem fogadhatja be ugyanaz a személy a számlákat, és nem kezdeményezheti ezek kifizetését.)
2. Legkevesebb jogosultság (Least Privilege)
   - Az elv betartásával a rendszer a felhasználók és az alkalmazások erőforrásokhoz való hozzáférését csak a legszükségesebbekre korlátozza.
   - Ehhez meg kell határozni a felhasználók munkájához szükséges jogosultságok minimális halmazát.
   - A felhasználók ehhez a halmazhoz kapnak csak hozzáférést, se többhöz, se kevesebbhez.

A hozzáférés-vezérlésre vonatkozó fenyegetések

A legtöbb információbiztonsági fenyegetés a hozzáférés-vezérlési kontrollok kijátszására irányul. A fenyegetések kihasználásával egy támadó nem engedélyezett hozzáférést szerezhet a rendszerhez, alkalmazásokat futtathat, információt olvashat, hozhat létre, adhat hozzá és törölhet. Az információvédelem legtipikusabb feladata éppen ezért az, hogy a hozzáférés-vezérlési szabályokat kikényszerítse, és az ezekkel kapcsolatos kockázatokat csökkentse. Néhány példa a lehetséges fenyegetésekre, amiket kihasználva a hozzáférés-vezérlést ki lehet kerülni[73]:

- Adatremanencia (data remanence): Akkor következik be, ha egy mágneses adattárolót felülírtak vagy töröltek, de továbbra is kinyerhető belőle információ.
- Átejtés (spoofing): Akkor következik be, amikor egy személy vagy egy alkalmazás másnak adja ki magát az adatok meghamisításával, így szerezve jogosulatlan hozzáférését. Például az IP spoofing során a támadó hamisított IPcímmel megbízható hostnak adja ki magát.
- Beágyazás (tunneling): Egy biztonsági rendszer megkerülése alacsonyszintű rendszerfunkciók elérésével. Például HTTP tunelling, melynek célja legális forgalomba ágyazott nem legális tartalommal kikerülni a tűzfalat.
- Célzott adatbányászat (targeted data mining): Adatbázisok áttekintése meghatározott információkért, melyek érzékeny adatokat szolgáltathatnak a rendszerről.
- Fizikai hozzáférés (physical access): Fizikai hozzáférés egy hálózathoz, berendezéshez vagy támogató rendszerhez.
- Hátsókapu (backdoor): Olyan szoftverbe vagy hardverbe épített eljárás, melynek segítségével ki lehet kerülni az adott entitás hitelesítési eljárásait.
- Jelszótörés (password cracking): olyan eljárás, melynek segítségével a hitelesítést szolgáló jelszavak visszaállíthatók, például gyenge lenyomatból vagy brute force módszerrel.
- Kártékony kód (malicious code): Olyan kód, mely végrehajtása közben megsérti a biztonsági szabályzatot, és a felhasználó tudta nélkül károkat okoz.

[73] Az egyes fenyegetések részletes leírásai megtalálhatóak a Wikipédia angol nyelvű lapjain (http://en.wikipedia.org/wiki/).

- Kémkedés (spying): Hagyományos eszközökkel (például mikrofon, kamera) elkövetett jogosulatlan információszerzés.
- Kifigyelés (shoulder surfing): Érzékeny adatok direkt leolvasása a képernyőről.
- Kisugárzás (emanation): A hardvereszközökből származó elektromágneses sugárzásból visszaállított információk megszerzése.
- Közbeékelődéses támadás (man-in-the-middle attack): olyan támadás, ahol a támadó a két fél közé számukra láthatatlanul kapcsolódva mindegyik fél felé a másik partnerének adja ki magát.
- Kukabúvárkodás (dumpster diving): A támadás célja leselejtezett (vö. kidobott) iratokból érzékeny információk visszaállítása.
- Lehallgatás (eavesdropping): a hálózat adatforgalmának monitorozása abból a célból, hogy érzékeny adatok birtokába jusson a megfigyelő.
- Megszemélyesítés (impersonation): a támadás során a támadó egy hitelesített személynek adja ki magát, így szerez nem hitelesített hozzáférést, például lopott jelszóval.
- Mobil kód (mobile code): Olyan szoftver, ami a hálózaton keresztül érkezik, és a helyi gépen hajtódik végre, általában a felhasználó engedélyével, de károkat okozhat a tudta nélkül. Például rosszindulatú ActiveX vezérlők.
- Objektum-újrafelhasználás (object reuse): Az a lehetőség, hogy egy érzékeny adat rendelkezésre áll egy nem hitelesített felhasználónak, például egy érzékeny adat megmarad a swap memóriában, amit a gép egy másik felhasználója is láthat.
- Puffer-túlcsordulás (buffer overflow): Talán a leggyakoribb támadás. Egy alkalmazás több adatot ír a memóriaterületére, mint amennyit lehetne, így felülír esetlegesen más alkalmazáshoz tartozó érzékeny memóriaterületet. A felülírás például tartalmazhat kártékony kódot vagy kikerülhet hitelesítési eljárást.
- Rejtett csatorna (covert channel): Olyan kommunikációs csatorna, melyen a legális csatornák kapacitását használva nem engedélyezett adatforgalom halad keresztül. Az időzített csatornán az adás előfordulása, a tárolási csatornán a memória adott területének írása/törlése szolgáltat információt.
- Személyes ráhatás (social engineering): olyan gépfüggetlen eljárás, melynek lényege az, hogy a támadó a rendszerrel dolgozó emberektől megszerzett adatok segítségével tör be a rendszerbe.
- Szimatolás (sniffing): Információszerzés a hálózati csomagok elfogásának segítségével. A lehallgatással szemben (ami általános hálózati forgalomra vonatkozik) a szimatolás kimondottan csomagkapcsolt hálózatokra értelmezhető.
- Visszajátszás (replay): A hitelesítési eljárás kijátszása egy hálózati csomag elfogásával és későbbi visszaküldésével.

A hozzáférés-vezérlési kontrollokat mind a szervezeten belülről, mind a szervezeten kívülről számos entitás fenyegeti. A belső támadók azok a hitelesített felhasználók, akik olyan adatokhoz vagy erőforrásokhoz akarnak hozzáférni, ami sérti a legkevesebb jogosultság elvet. Ez lehet szándékos vagy vétlen támadás. Külső támadók azok a nem hitelesített felhasználók, akik a hitelesítési eljárások megkerülésével férnek hozzá az adatokhoz. Ezek lehetnek hackerek, crackerek, hírszerzők stb. A legnagyobb kockázatot a belső támadók jelentik, hiszen ők ismerik a belső informatikai infrastruktúrát, sokszor a védelem egyes elemeit vagy egészét.

9.1.1. Azonosítás, hitelesítés

Az azonosításra, hitelesítésre vonatkozó védelmi intézkedéseket a fenyegetések sokszínűsége miatt a védelem minden dimenziójában meg kell valósítani. Néhány példa:

1. Fizikai:
   - Belépőkártyák
   - Forgóvillák
   - Biztonsági őrök stb.
2. Logikai:
   - Jelszavak
   - Tűzfalak
   - Vírusirtók stb.
3. Adminisztratív:
   - Szabályok és eljárások
   - Biztonsági tudatosság-oktatás
   - Feladatok rotálása stb.

Azonosítás

Röviden: 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.

Az azonosítási folyamat szervezeten belüli kialakításánál néhány alapvető követelményt figyelembe kell venni. Ezek a következők:

- Az azonosítás biztonságos és dokumentált folyamat.
- Az azonosítók formátuma belső szabványban van leírva.
- Az azonosító nem utalhat az entitás funkciójára (például beosztás).
- Egy azonosító nem osztható meg több entitás között.
- Az azonosító ellenőrzése egyszerű folyamat kell, hogy legyen.
- Az azonosító egyedi kell, hogy legyen.

Hitelesítés

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! Ez az erős autentikáció vagy többlépcsős hitelesítés. Az egymástól függetlenül való felhasználás (out-of-band csatorna) azt jelenti, hogy a két hitelesítési eljárás egymással nem összekapcsolható. Tipikus példa erre a bankkártya, ahol egy tudásalapú (PIN-kód) és egy tulajdonalapú (bankkártya) autentikációs megoldást használunk. A PIN-kód a fejünkben, a bankkártya a kezünkben van, egy támadó egyszerre ezt a két faktort nem tudja megszerezni. Ha viszont a PIN-kódot ráírjuk a bankkártyára, már sérül a függetlenség elve, hiszen a bankkártya megszerzésével a tudásalapú faktorhoz is hozzá lehet jutni.

Tudásalapú hitelesítés

Minden olyan hitelesítés eljárás ide tartozik, amit a felhasználó tud. Tipikusan a jelszavak és PIN-kódok tartoznak ebbe a körbe. A jelszóhasználatnál az alábbi szempontokat érdemes figyelembe venni:

- A jelszavak élettartamát korlátozzuk!
- A jelszó ne legyen szótári alakú szó!
- A jelszó tartalmazzon kis- és nagybetűket, számokat és speciális karaktereket!
- Minél hosszabb egy jelszó, annál jobb. Legyen legalább 8 karakter!
- Értékeljük a rendszer kritikusságát, és annak megfelelően más-más jelszavakat használjunk!
- Bizonyos számú hibás próbálkozás után a rendszer zárja ki a felhasználót!

A jelszavak ellen háromféle tipikus támadást szoktak indítani. A jelszavak tárolási gyengeségét kihasználó támadások indoka az, hogy a jelszavaknak általában a lenyomatát tárolják. Ebben az esetben a lenyomatképző függvények gyengeségeinek segítségével vissza lehet állítani az eredeti jelszót. A jelszavak gyengeségeit kihasználó támadások (brute-force támadások) minden karakter végigpróbálását jelentik. A social engineering típusú támadások a legegyszerűbbek. Sokszor elég megkérdezni a jelszót, hiszen az emberek segítőkészek és megmondják azt.

Tulajdonalapú hitelesítés

Azok a hitelesítési eljárások tartoznak ebbe a körbe, amelyek egy felhasználó birtokában levő eszközt vonnak be az autentikációba. Ilyenek például az egyszer használatos jelszavak out-of-band csatornákon:

- O(ne)T(ime)P(assword)-jelszólista
- Mobiltelefonon érkező kód
- Tokenek
- Intelligens kártyák

A tokenek olyan fizikai eszközök, melyek kijelzőjükön valamilyen elv szerint egy számkombinációt mutatnak. Két típusuk használatos: szinkron és aszinkron. A szinkron tokeneken belül megkülönböztetünk:

- Számlálón alapuló tokent: a token és a szerver között van egy szinkronizált közös titkos kulcs, és egy belső számlálóval, ezek lenyomatából jön ki az OTP.
- Időn alapuló token: belső számláló helyett a szinkronizált időt használják fel.

Az aszinkron tokenek kihívás-válasz (challenge-response) alapon működnek.

– A szerver és a token közös kulcsot használ. A szerveren megjelenő kihívást beírva a tokenbe megjelenik a válasz.

Az intelligens kártyák körébe értünk minden olyan kártyát, mely nem mágnescsíkos, memóriachipes vagy közelítőkártya. Az intelligens kártyák megkülönböztetője ugyanis az, hogy mikroprocesszorral látják el ezeket. Ez az adattárolás mellett az adatok feldolgozására is képes, kitűnően használható kriptográfiai műveletek támogatására. Gyakorlatilag nem nyerhető ki a rajta tárolt titkos információ.

A tulajdonalapú hitelesítés elleni legegyszerűbb támadás a lopás. Az egyes megoldásokkal kapcsolatban azonban speciális fenyegetéseket is lehet azonosítani. Az intelligens kártyák ellen például több támadás ismert, azonban ezek költséghatékonysága megkérdőjelezhető:

– Következtetések a kártya fogyasztásából
– A chip módosítása
– Optikai támadás a kártyák ellen

Egyszerűbb a tulajdon és az azt feldolgozó eszköz közötti adatutat támadni.

Tulajdonságalapú hitelesítés

A személyre jellemző biometrikus tulajdonságok alapján történő hitelesítés. Ide tartozik többek között:

– Ujjlenyomat
– Retina
– Írisz
– Hang
– Tenyér
– Aláírás
– Arc

A technika fejlődésével egyre több helyen használják ezt a technológiát, nemcsak nagyvállalati, hanem otthoni körülmények között is. A tulajdonság alapú hitelesítés elleni támadások elsősorban az implementáció gyengeségét próbálják kihasználni. Ezek például:

– Gumiujj – az ujjlenyomat szilikonból készült másolata, melyet számos ujjlenyomat-leolvasó valódinak hisz.
– Másolt ujjlenyomat – az ujjlenyomat-leolvasás számos esetben egyszerű szkenneléssel való ellenőrzést jelent, az ujj élettani mutatóit a megoldás nem vizsgálja. Így egy egyszerű papíralapú fénymásolatot is valódinak lehet beállítani.
– Felvett hangminta – a modern hangkezelő szoftverekkel akár egyes felvett szavakból is értelmes, élethű mintákat lehet előállítani, így a hangalapú azonosítás komoly kihívásokkal küzd. Természetesen meg lehet erősíteni, ha egy tudásalapú faktorral (jelmondat) egészítik ki a megoldást.

A biometrikus eljárások megfelelőségét, használhatóságát több szempont szerint lehet vizsgálni.

1. Megfelelőség:
   – Hibás visszautasítási ráta (False Reject Rate – FRR) – a rendszer hányszor utasít vissza jogosult felhasználót.
   – Hibás elfogadási ráta (False Accept Rate – FAR) – a rendszer hányszor enged be nem jogosult felhasználót.
   – Metszésponti hibaarány (Crossover Error Rate – CER) vagy azonos hibaérték (Equal Error Rate –EER) – a valódi hibaarány, a függvényként értelmezett FRR és a FAR görbéinek metszéspontját mutatja. Javasolt, hogy a biometrikus eszköz azonosítási munkapontja az EER±10%-on belül, erős azonosításnál az EER±5%-on belül maradjon.
2. Feldolgozási sebesség: Mennyi idő alatt képes a rendszer a beolvasott jellemzőt feldolgozni.
3. Felhasználói elfogadás: Az adott technológiát mennyire fogadják el azok, akiknek alá kell vetniük magukat. Például egy vérvétellel történő DNS-elemzés csekély elfogadási rátára számíthat.

Azonosságkezelés

Nagyszámú entitás azonosságának a kezelése egyáltalán nem triviális feladat. Még a közepes méretű szervezetek esetében is több százas, ezres nagyságrendű felhasználó identitását kell kezelni. De ez a szám egy országos közigazgatási rendszer esetében, ahol állampolgárokat szolgálnak ki, akár milliósra is nőhet. Éppen ezért fontos az identitások megfelelő kezelése!

Az entitás életciklusa a következő:

– az azonosító létrehozása – a felhasználónév regisztrálása, amit a személyhez kötnek;
– az azonosító újbóli létrehozása – új paraméter hozzákapcsolása a felhasználóhoz;

– az azonosító leírása – az identitás adatokkal való ellátása, például az egyedi azonosítás érdekében bejegyzik a nevet, a születési helyet, a születési dátumomat, az anyja nevét;
– az azonosító pontosítása – az identitás egyik alapvető paramétere megváltozik, például a felhasználó felveszi a férje nevét, így a név megváltozik;
– az azonosító törlése – az identitást a továbbiakban nem használják a rendszerben.

Az azonosítók életciklusának kezelése összetett esetekben az úgynevezett Identitáskezelő rendszerekben (Identity Management System – IDM) történik. Ennek kiszolgálására olyan könyvtárakat hoznak létre, melyek a felhasználók azonosítóit tárolják. A legismertebb szabvány ezen a területen az LDAP (Lightweight Directory Access Protocol), a legtöbb identitáskezelő szoftver kompatibilis ezzel. Az LDAP könyvtár egy fa, könyvtárbejegyzésekkel. Egy bejegyzés tulajdonságok halmazát tartalmazza. Egy tulajdonságnak van egy neve és egy vagy több értéke. A tulajdonságokat sémákban írják le. Minden bejegyzésnek van egy egyéni azonosítója, ez a Distinguished Name (DN). Létezhet még egy Relative Distinguished Name (RDN) is, mely a DN után áll.

Hozzáférés-kezelés

Miután megoldottuk a felhasználók azonosításának problémáját, meg kell oldani a hitelesítésüket, a felhatalmazásukat és az elszámoltathatóságukat. Erre szolgálnak az úgynevezett AAA-rendszerek (authentication, authorization, accounting). Összetett esetekben az IDM-rendszerek a hozzáférések kezelésével is foglalkoznak, képességeik kiterjeszthetők erre a területre is.

Az AAA-szolgáltatás lépései:

– A felhasználó elküldi az azonosítóját és a jelszavát a hozzáférés-vezérlőnek (NAS).
– A NAS begyűjti az azonosítót és a jelszót.
– A NAS hitelesítési kérést küld az AAA-szervernek.
– Az AAA-szerver visszaküldi a kapcsolódási paramétereket, a felhatalmazást és a protokollinformációkat.
– A NAS jóváhagyja a kapcsolatot és létrehoz egy naplóbejegyzést.

A felhasználók hozzáférésének kezelése történhet centralizált és decentralizált módon. A centralizált modellek legismertebb képviselője a RADIUS (Remote Authentication Dial-In User Service)-protokoll. Ezt tipikusan az internetszolgáltatók használják. A hozzáférési modell tartalmaz egy RADIUS-klienst, ami a NAS-on van, egy RADIUS-szervert és egy UDP-re készített protokollt. A hozzáférés engedélyezésének folyamata során a kliens fogadja a felhasználói kéréseket, amit egy rejtjelezett csatornán továbbít a szervernek, majd a szerver hitelesíti a felhasználót (például egy LDAP-szerveren keresztül) és visszaküldi a felhasználóra vonatkozó konfigurációs információkat. Az autentikáció és az autorizáció része a RADIUS-protokollnak, az elszámoltathatóságot külön kell megoldani.

A másik jellemző centralizált megoldás a TACACS (Terminal Access Controller Access Control Systems)-protokoll. Ez jelenleg a harmadik változatánál tart, ez a TACACS+. A RADIUS-tól annyiban különbözik, hogy az AAA-ból mind a három A-t külön valósítja meg, így mindegyik eleme lecserélhető. Fontos változás, hogy TCP-protokollon folyik a kommunikáció.

A DIAMETER-prokoll a RADIUS továbbfejlesztése. Kiterjeszti a RADIUS lehetőségeit például a VPN, a vezetéknélküli hálózatok és a mobiltelefonok hitelesítésére is. Biztonságos csatornát használ a kommunikációra (IPSec vagy TLS).

Sok felhasználó hozzáférését a centralizált modellekkel meg lehet oldani. De mi a helyzet abban az esetben, ha egy felhasználó több rendszerhez szeretne hozzáférni ugyanazzal a hitelesítéssel? Ekkor használjuk az egyszeribelépés-technológiát (single sign-on – SSO), mely átvezet a decentralizált modellek világába.

SSO-t akkor éri meg használni, ha:

– sok belépési pont van,
– nagyszámú munkaállomást kell kezelni,
– sok alkalmazást használnak a szervezetben,
– a hozzáférés-vezérlés adminisztrációját egyszerűsíteni kell a hatékonyság érdekében.

Az SSO előnyei:

– A felhasználónak csak egyszer kell hitelesítenie magát.
– Nem kell több jelszót megjegyezni, így egyszerűbb erős jelszót kikényszeríteni.
– A jelszómenedzsment és a változáskezelés leegyszerűsödik.
– Könnyebb a felhasználói fiókok felfüggesztése.

Az SSO hátrányai:

– Ha egyszer egy jelszó kitudódik, a támadó mindenhez hozzáfér.
– A heterogén környezetben nehéz a megvalósítása.

A legismertebb SSO-megvalósítás a Kerberos-protokoll. Erre épül például a Microsoft Active Directory is, de más operációs rendszerekben is használják. Az 1980-as években jelent meg az első változata, az MIT Athena projektjének keretében. A modellben a Kerberos hitelesítési szervere (Key Distribution Center – KDC) megbízható

harmadik félnek tekinthető, amivel a hitelesítésben részt vevő felek kommunikálnak. A hitelesítési információk DES rejtjelzési eljárással vannak védve. A hitelesített felhasználók véges ideig érvényes jegyeket (ticketeket) kapnak, amik igazolják a jogosultságaikat. A Kerberos-authentikáció folyamata a következő:

1. A felhasználó beírja a felhasználónevét és a jelszavát.
2. A kliens elkészíti a jelszó lenyomatát, ami a kliens titkos kulcsa lesz.
3. A kliens nyílt szövegű üzenetet küld a Hitelesítési Szolgáltatásnak (Authentication Service – AS), amiben hozzáférést kér egy szolgáltatáshoz.
4. Ha minden rendben, akkor az AS két üzenetet küld vissza. A kliens titkos kulcsával rejtjelzett Kliens/TGS kapcsolati kulcsot és egy Jegymegadó Jegyet (Ticket Granting Ticket – TGT), ami a Jegymegadó Szolgáltatás (Ticket Granting Service – TGS) titkos kulcsával van rejtjelezve. A TGT tartalmazza az kliens-ID-t, a kliens hálózati címét, az érvényességi időt és a kapcsolati kulcsot.
5. A kliens dekódolja a Kliens/TGS kapcsolati kulcsot (a másikat nem tudja, hiszen nem ismeri a TGS titkos kulcsát).
6. A hálózati szolgáltatás elérése előtt a kliens két üzenetet küld a TGS-nek. Az egyik a TGT-t és a kért szolgáltatás azonosítóját tartalmazza, a másik kliens-ID-t és az időbélyeget tartalmazó felhatalmazási kérést, ami a kapcsolati kulccsal van rejtjelezve.
7. Az üzenet fogadásakor a TGS dekódolja a felhatalmazási kérést, és két üzenetet küld. A kliensszerver-jegyet, ami az elérendő szolgáltatás titkos kulcsával van rejtjelezve, és a kliensszerver kapcsolati kulcsot, ami a Kliens/TGS kapcsolati kulccsal van rejtjelezve.
8. A kliens ezután tudja hitelesíteni magát a szolgáltatás felé. Ehhez két üzenetet küld. A kliensszerver-jegyet, és egy új felhatalmazási kérést, ami a kliensszerver kapcsolati kulccsal van rejtjelezve.
9. A szolgáltatás dekódolja a jegyet a saját kulcsával, és egy üzenetet küld a kliensnek, ami a felhatalmazási kérésben talált időbélyegző+1-et tartalmazza a kapcsolati kulccsal rejtjelezve.
10. A kliens dekódolja az üzenetet, és ellenőrzi, hogy az időbélyegzőt rendesen növelték-e. Ezután elkezdi a kapcsolatot a szolgáltatással.
11. A szolgáltatás fogadja a kliens kéréseit.

Behatolás-detektálás

A leggyakoribb hozzáférés-vezérlési felderítő védelmi intézkedés a behatolás detektáló rendszerek (Intrusion Detection System – IDS) használata. Ezek elve azon alapul, hogy a támadásokat különböző hálózati vagy erőforrásbeli jellemzők alapján észre lehet venni. Ezek a jellemzők a rendszer naplóállományaiból vagy a hálózati eszközök információiból derülnek ki. Az IDS-rendszerek tehát a rendszer naplóállományainak és a hálózati forgalom elemzéséből próbálnak támadásokat felismerni.

Egy tipikus IDS három elemből áll:

– Szenzor
– Elemző
– Felhasználói felület

A hálózati IDS-ek (Network IDS) az átviteli csatorna forgalmát monitorozzák valós időben. Passzív eszközök, így nem használják a csatorna erőforrásait. A rendszer a hálózati csomagok felépítését, tulajdonságait vizsgálja. Ha gyanús dolgot észlel, figyelmezteti az operátort. Általában önálló kliensen fut, így nem kell az éles környezetbe beavatkozni, viszont nehezen skálázható. A rejtjelzett csomagokkal nem tud mit kezdeni, itt különböző trükkökre van szükség.

A kiszolgáló-alapú IDS-ek (HIDS) egy kiszolgálóra telepített szenzortól gyűjtenek információkat. A szenzor ennek a kiszolgálónak a naplóállományait elemzi, és ebből próbál információkat szerezni. Ha több hoston van telepítve szenzor, akkor ezek adatait egy központi gépen lehet elemezni.

Az IDS-ek három elv szerint képesek a támadásokat azonosítani:

– Szabályok alapján
– Statisztikai alapon
– Szignatúraalapon

A szabályalapú IDS-ek abból indulnak ki, hogy a támadások leírhatók egy szekvenciában, amik kompromittált állapotba vezetnek. Ezek nem elég rugalmasak, de tipikus támadások kiszűrésére kiválóak.

A statisztikai alapú IDS-ek a szabályalapú IDS-ek gyengeségét hivatottak kiküszöbölni. A naplóállományokat vizsgálják, és a „normális" menettől való eltéréseket próbálják megtalálni. Használatuk hátránya, hogy rengeteg, sokszor irreleváns adatot generálnak.

A szignatúraalapú IDS-ek a hálózati csomagokban található információkat vizsgálják. Hasonlóan a vírusirtókhoz, az ismert támadásokat próbálják azonosítani. Használatuk hátránya szintén az, hogy nem elég rugalmasak.

Az IDS-ek jelzéseire lehet manuálisan (adminisztrátori beavatkozás) és automatikusan (IPS-ek, tűzfalak) is reagálni. A technológia nagy hátránya, hogy rengeteg fals pozitív jelzés érkezik, cserébe viszont kiválóan alkalmasak ellenőrzési nyomok (audit trail) rögzítésére.

Behatolás-tesztelés

A leggyakoribb hozzáférés-vezérlési javító védelmi intézkedés a behatolás-tesztelés. 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 behatolás-tesztelési módszertanok csoportosítására jelenleg nincs egyezményes megállapodás, a tesztelt rendszerek ismeretétől kezdve, a hozzáférés mértékén át, a bevetett tesztelési eszközökig számos taxonómia létezik. Néhány fogalom azonban gyakran előfordul a szakirodalomban, melyek jól bemutatják a lehetséges módszereket.

- Biztonsági funkcionális tesztelés: az újonnan fejlesztett rendszer (alkalmazás) beépített védelmi kontrolljainak megfelelőségi ellenőrzése. Más néven white-box típusú tesztelésnek is hívják, kódközeli megközelítésnek minősül. Például nézzük meg, hogy tényleg legalább 8 karaktert kell-e megadni jelszónak.
- Sérülékenység-vizsgálat: a rendszer (alkalmazás) védelmi kontrolljainál előforduló sebezhetőségek felderítése, tipikusan automatikus eszközökkel. Más néven black-box típusú tesztelésként ismert, modulszintű vizsgálatnak tekinthető. Például egyes bemeneteken olyan adatok megadása, melyekre a rendszer egyébként védett információkat ad át.
- Behatolás-tesztelés: az újonnan fejlesztett vagy már működő rendszer védelmi kontrolljainak kijátszása műszaki megoldásokkal, bármilyen kapcsolódó környezeti infrastruktúra felhasználásával. Két alfaja létezik: a Blue teaming, melynek során a tesztelő pontosan ismeri a tesztelt infrastruktúrát, és a Red teaming, melynél semmilyen ismerettel nem rendelkezik.
- Etikus hackelés: a működő rendszer védelmi kontrolljainak kijátszása bármilyen technikával, a rendszer előzetes ismerete nélkül. Ebbe beletartozik az emberi ráhatással (social engineering) történő támadás is.

A behatolás-tesztelés lépései a következők:

- Felderítés (Discovery) – nyilvános forrásokból hozzáférhető információk megszerzése (például Google).
- Felmérés (Enumeration) – a rendszer részeinek azonosítása technikai eszközökkel (például nmap).
- Sérülékenység hozzárendelése (Vulnerability mapping) – a beazonosított rendszerelemek sérülékenységeinek azonosítása (például Bugtraq).
- Kihasználás (Exploitation) – a hozzáférés-vezérlés kikerülése a sérülékenységeken keresztül (például Metasploit).

Felderítés

Első lépésben a nyílt forrású hírszerzés módszerével az interneten elérhető információkat lehet összegyűjteni. Ezek forrásai lehetnek:

- Céges weboldal
- Kapcsolódó vállalkozások (például cégjegyzék)
- Telephellyel kapcsolatos információk (Google Map)
- Telefonszámok, kontaktszemélyek, e-mail címek
- Aktuális események (például sajtóközlemények)
- Nyilvánosan elérhető műszaki információk (szabályzatok, szabványok stb.)
- Archív információk (például www.archive.org)
- Alkalmazottaktól kiszivárgó információk (például blogok, Facebook)
- Keresők által szolgáltatott információk (például Google hacking)
- Bármilyen más relevánsnak tűnő információ

Ezután következik a hálózati információk, az IP- és DNS-adatok összegyűjtése:

- www.domain.hu
- www.ripe.net
- www.arin.net
- www.dnsstuff.com
- DNS brute-force a másodlagos DNS-címek ellen
- traceroute

A felmérési szakaszban az összegyűjtött információk megfelelőségét lehet leellenőrizni.

Bekapcsolt számítógépek megtalálása:

- fping
- nmap

Nyitott portok azonosítása:
- nmap
  - Általában alacsony portokon vannak érdekes szolgáltatások.
  - Ha alacsony porton nincs semmi érdekes, érdemes a magas, esetleg az UDP portokon is körülnézni.

Operációs rendszer megállapítása:
- nmap -o
  - A TCP stack alapján történik az azonosítás
- telnet
  - A TCP/IP-csomag TTL, ablakméret és DF bitje alapján történik az azonosítás

A hálózati szolgáltatások tulajdonságainak felderítése:
- Sokszor elég csak hozzájuk csatlakozni
- netcat

9.1.2. Hozzáférés-engedélyezés

A hozzáférés-vezérlések jelentős része a közismert *kell, hogy tudja*[74] 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.

A 4 legelterjedtebb politika:
- a szabadbelátás szerinti hozzáférés-vezérlés (Discretionary Access Control – DAC),
- a kötelező hozzáférés-vezérlés (Mandatory Access Control – MAC) és
- a szerepalapú hozzáférés-vezérlés (Role-Based Access Control – RBAC).

A hozzáférés-vezérlési politikák megvalósításához úgynevezett hozzáférésvezérlési modelleket dolgoztak ki. A legismertebb, leggyakrabban alkalmazott hozzáférés-vezérlési modellek:
- háló modell,
- állapotgép modell,
- nem befolyásoló modell,
- információáramlási modell,
- hozzáférés-vezérlő mátrix,
- Bell–LaPadula modell,
- Biba modell,
- Clark–Wilson modell,
- Graham–Denning modell,
- Harrison–Ruzzo–Ullman modell,
- kínai fal (Brewer–Nash) modell.

A hozzáférés-vezérlés legismertebb, általánosan használt eljárása a **hozzáférésvezérlési lista** (access control list, ACL). Ez nem más, mint egy táblázat, ami listaszerűen tartalmazza, hogy az egyes alanyoknak[75] mely objektumon[76] milyen joga van, vagyis az egyes alanyok által az egyes objektumokon elvégezhető lehetséges hozzáférési műveleteket jeleníti meg. Tipikus hozzáférési jogok az olvasás, írás és futtatás, de ez bővíthető például a létrehozási, a módosítási, a törlési (selejtezési) és a másolási, illetve a tulajdonosi, a hozzáférésvezérlés-kezelői, valamint a jogmásolási joggal.

A **szabad belátás szerinti hozzáférés-kezelési politika**, a DAC a legegyszerűbb. „A diszkrecionális hozzáférés-vezérlés alapja az alanyok azonosítása. Az eljárást azért nevezik diszkrecionálisnak, mert legfontosabb jellemzője, hogy amennyiben egy alany rendelkezik egy objektumhoz valamilyen hozzáférési jogosultsággal, akkor ezt a jogosultságot szabad belátása szerint továbbadhatja más alanyoknak, vagyis ez a szabályozási mód az alanyoknak az objektumok feletti jogosultságok kiosztását jelenti. A DAC a gyakorlatban többnyire a hozzáférés-vezérlési lista alkalmazásán alapul.” [37]

„A diszkrecionális hozzáférés-vezérlést használja sok PC-s és hálózati operációs rendszer, így a MS Windows NT és a MS Windows 2000 operációs rendszer, valamint számos hagyományos UNIX és LINUX operációs rendszer hozzáférés-védelme is a diszkrecionális hozzáférés-vezérlésen alapul. A nem nagy biztonságú adatbázis-kezelők is többnyire a diszkrecionális hozzáférés-vezérlést használják.

[74] Angolul: Need to know.
[75] Felhasználók, programok.
[76] Felhasználók, fájlok, eszközök, programok, illetve a processzek közötti logikai vagy fizikai csatornák stb.

A DAC nagy hibája, hogy nem tudja garantálni az adatok bizalmasságát!" [37]

A szabad belátás szerinti hozzáférés-kezelési politika hibáira hamar felfigyeltek. Az, hogy a DAC nem tudja garantálni az adatok bizalmasságát, a minősített adatokat kezelő rendszerekben különösen nagy gondot jelentett. A minősített adatok kezelésére alkalmas *többszintű biztonságos*[77] rendszerekhez rendelte meg a számítástechnika és annak biztonsága területén meghatározó szerepet játszó Amerikai Védelmi Minisztérium (DoD) *a kötelező hozzáférés-vezérlési politikán alapuló hozzáférés-vezérlési modelleket*. E modellek közös tulajdonsága, hogy nem az objektumokkal végezhető műveletekre, hanem az azokban tárolt információ áramlására fektetik a hangsúlyt.

Az informatikai rendszer alanyaihoz és objektumaihoz azok létesítésekor biztonsági címkéket kell rendelni, amit az alanyok – a kitüntetett szerepkörűeket kivéve – nem tudnak megváltoztatni. Az alany címkéje meghatározza, hogy az alany milyen biztonsági szintű adatokhoz és mely adatcsoportokhoz férhet hozzá, a tárgy címkéje a tárgy vagy az általa kezelt adat biztonsági besorolását és a hozzáférés lehetséges módját tartalmazza. Az olvasási jogosultság esetében a személy azonosítója a meghatározó (magasabb vagy azonos értékű) az erőforráséhoz (például fájlhoz) képest, míg az írási jogosultság esetében az erőforrás azonosítója a meghatározó (magasabb vagy azonos értékű) a személyéhez képest.

A szerepalapú (nem diszkrecionális) hozzáférés-vezérlési politika azon alapul, hogy a szervezeten belül a jogokat nem a személyekhez, hanem a betöltött beosztáshoz rendelik hozzá. Ugyanazon szerepkörben két különböző személynek azonos jogai vannak, míg ugyanaz a személy a szervezeten belül más beosztásba kerülve más jogokat kell, hogy kapjon. Ebben a hozzáférés-vezérlés nem engedélyező vagy tiltó jogosultságokat, hanem az egyes szerepkörökhöz kapcsolt szabályrendszert használ, amelyek meghatározzák, hogy adott szerepkörben lévő felhasználók milyen objektumon milyen műveleteket végezhetnek. Az egyes felhasználók több, különböző szerepkört is elláthatnak.

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. A megosztás azt jelenti, hogy az adott munkaállomás tulajdonosa hozzáférési jogosultságot ad a saját gépén elérhető erőforrásokhoz való hozzáféréshez. [38]

A számítógép-hálózatok – mivel többelemű rendszerek– általában nem azonos típusú és konfigurációjú számítógépekből állnak, ezt a hálózat tervezésekor, a megfelelő szabványok és protokollok használatának alkalmazásával figyelembe kell venni. Napjainkban a hálózati végpontok nemcsak számítógépek, hanem gyakorlatilag bármilyen célú, funkciójú eszközök lehetnek. [38]

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 [38]:

– Központi erőforrás használata esetén a hálózati összeköttetés révén a munkaállomások a szerver-számítógép gépének erőforrását használják. A munkaállomásokkal szemben támasztott hardver- és szoftver-igények lényegesen egyszerűsödnek. Biztonsági szempontból kedvező, hogy a központi erőforrásokat tartalmazó szerver-számítógép(ek) jól védhetők mind a fizikai, mind a logikai támadások ellen. [38]
– Osztott erőforrás használata 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. [38]

A hálózatokat általában három nagy csoportba szokták sorolni [38]:

– 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 nagykiterjedésű hálózatokra is.

– Nagykiterjedésű hálózatok (WAN – Wide Area Network)

A nagykiterjedésű hálózatok olyan rendszerek, melyeknek egyes szegmensei (elemei) földrajzilag is távol lehetnek egymástól. Ebben az esetben a kapcsolattartás más speciális módszerekkel valósítható meg.

– Globális hálózatok

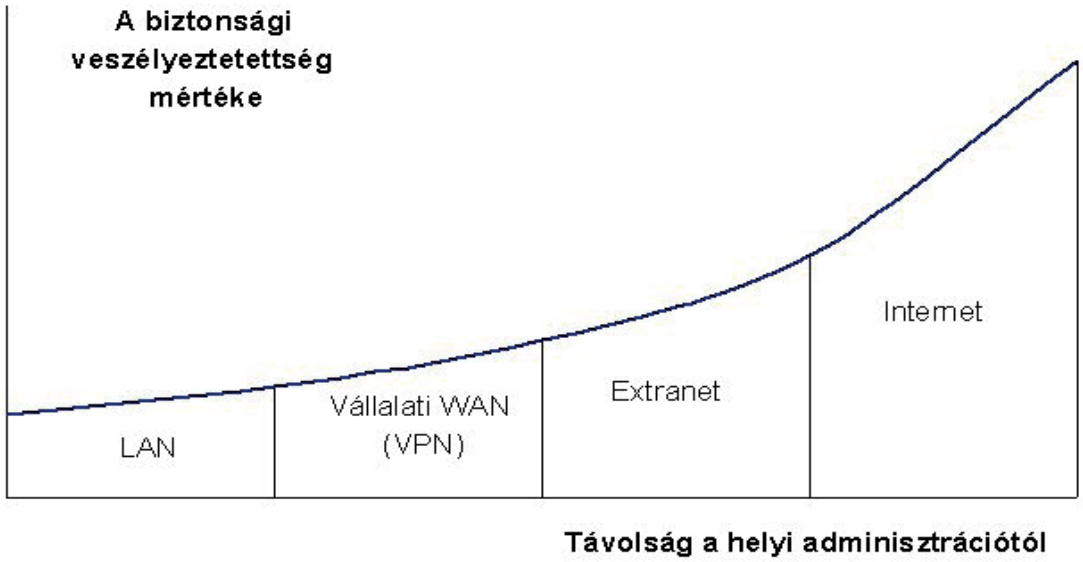
[77] Angolul: multi-level secure (MLS).

A globális hálózatok olyan világméretű hálózati rendszerek, melyek nagyszámú elemet tartalmaznak, eléggé heterogén felépítésűek, nagyon sok számítógépet, illetve részhálózatot foglalnak magukba. Globális hálózat például az internet.

Napjainkban visszaszorulóban van az egyedi számítógépekre szabott informatika. A mobilitás elterjedésével az információkat földrajzilag, és az eszközöket tekintve szinte korlátlanul el lehet érni. A felhőalapú számítástechnika (cloud) elterjedésével megjelentek a határok nélküli vállalatok. Az információkat érintő fenyegetéseket tehát nemcsak a szervezeten belül, hanem azon kívül is kezelni kell! Az internet irányából elsősorban külső támadásoktól kell tartanunk, a belső hálózatokon 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 szinte minden jelentősebb információt számítógépes hálózataikon tárolnak, 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.

Az informatikai hálózatok legtöbbször stratégiai fontosságú adatokat tárolnak. Ezek bizalmasságát még akkor is meg kell őrizni, ha egyébként igény van az internet széleskörű 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 átvilágítani, a gyenge pontokat és a konfigurációs hibákat feltárni.

Mint azt a 8. ábra mutatja, egy informatikai rendszer biztonságát bármilyen kommunikációs kapcsolat csökkenti. A biztonsági veszélyforrások az adminisztrációtól való távolság függvényében egyre jelentősebbek.



8. ábra A veszélyeztetettség mértéke [38]

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. A teljesség igénye nélkül a következőkben bemutatunk egy pár ilyen intézkedést [38]:

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 rejtjelzett 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.

9.2.1. Az OSI modell

A hálózati kommunikáció működését legjobban az úgynevezett OSI modell reprezentálja. Bár a gyakorlatban nem használják, a mai hálózati kommunikáció elméletét tökéletesen meg lehet belőle érteni. Az OSI rétegzett felépítésű, rétegenként különböző feladatokat ellátó modell. Minden réteg kizárólag az alatta lévő szolgáltatásait használja és a felette lévőnek nyújt szolgáltatásokat. Minden réteg új fejléccel látja el a lentről jövő adatokat. Elvileg a rétegek cserélhetőek, ha a szolgáltatások felülete megmarad. Virtuális kapcsolat épül ki minden rétegben a kommunikálók között. Az OSI modell rétegei:

- Fizikai (physical): A fizikai kapcsolat elektromos, mechanikai, eljárásbeli paramétereit definiálja. „A drót egyik végén bemenő bit ugyanúgy jöjjön ki a másik oldalon" (drót: fém, optikai, rádiós stb.). Ezek jellemzően villamosmérnöki szakterületet érintő kérdések.
- Adatkapcsolati (data link): Megbízható kapcsolat a fizikai réteg fölött. Adatkeretek összeállítása, hibadetektálás, címzés az egy fizikai szegmensen lévő állomások között. Két alrétege van:
    - MAC – közeghozzáférési réteg: az egyes állomások hogyan férnek hozzá a fizikai réteghez, MAC-címek (például: ethernet)
    - LLC – logikai kapcsolatvezérlés: a fizikai rétegen kialakított kapcsolatok és különböző felsőbb szintű protokollok támogatása
- Hálózati (network): Hálózati szintű kommunikáció tetszőleges állomások között. Itt történik a hálózati címzés (például: IP-címek) és az útválasztás, csomagok irányítása a teljes hálózatban.
- Szállítási (transport): Megbízható, hibamentes kapcsolat kialakítása a feladata. Itt történik az adatfolyam feltördelése a hálózati szint által elfogadott csomagokra. Megjelenik a virtuális áramkörök kialakításának lehetősége. Feladata az elveszett csomagok újraadása, csomagok sorrendjének biztosítása, a forgalomszabályozás.
- Viszony (session): Ebben a rétegben történik a kommunikációs viszonyok kialakítása és kezelése, a szolgáltatások közötti viszony kezelése, lezárása, újraindítása (bejelentkezés stb.). Az OSI modell szerint is kevés funkcióval rendelkező réteg.
- Megjelenítési (presentation): Feladata az adatok megjelenítése:
    - adatformátumok közötti konverzió
    - rejtjelzés
    - karakterkonverzió
- Alkalmazási (application): a felhasználó által igénybevett alkalmazások megvalósítása történik ebben a rétegben:
    - állomány-átvitel
    - levelezés
    - távoliterminál-szolgáltatás

A gyakorlatban a TCP/IP-protokollt használják, mely az OSI modell elveit követi. Gyakorlati megközelítést alkalmaz, ezért felépítésben különbözik az OSI-tól:

- nem definiálja a fizikai és az adatkapcsolati réteget, tetszőleges alkalmazható (ARP-protokoll köti össze a MAC-címeket az IP-címekkel)
- hálózati réteg megfelel az IP-nek és a routingprotokolloknak
- szállítási réteg a TCP-nek (kapcsolatorientált) és UDP-nek (kapcsolat nélküli)
- további szintek alkalmazásokban vannak megvalósítva

Mára gyakorlatilag egyeduralkodó az általános célú hálózati protokollok között

Lényeges komponensei:

- IP – a hálózati protokoll
- TCP – kapcsolatorientált szállítási protokoll
- UDP – kapcsolatmentes szállítási protokoll
- kiegészítő protokollok: ICMP, DNS, IGMP, különböző routing (RIP, IGRP, OSPF, EGP, BGP)

A hálózatok összekapcsolásában az IP-protokoll az egyik kiemelkedő fontosságú szabvány. Ez 32 bites hálózati címekkel (128 bit az új verzióban: IPv6) teszi elérhetővé a hálózati végpontokat.

Csomag fejléce:

- forrás és célcím
- ellenőrző összeg
- felsőbb protokoll típusa
- jelzők és opciók
- több darabra vágott csomag esetén darabok száma
- TTL – hány ugráson mehet át a csomag

A másik fontos protokoll a TCP, amely az IP-szint feletti rétegben helyezkedik el. Meghatározza a portokat, melyek az adott csomóponton (IP-cím) belül megkülönböztetik a hálózati szolgáltatásokat (alkalmazás, például: 80 http), valamint elvégzi a kapcsolatfelvételt (háromutas kézfogás: SYN – SYN, ACK – ACK) – full-duplex kommunikáció – kapcsolatbontás (irányonként lehet külön).

Fejlécben a következő információk vannak:

- Forrásport, célport
- Sorozatszám (sequence number) és nyugta száma
- Ablakméret
- Opciók és vezérlő bitek

Az UDP-protokoll a TCP-hez hasonló feladatot végez, de olyan esetekben használják, amikor egy-egy információdarab megérkezése nem létfontosságú (például videóátvitel). Itt is portok adják az adott csomóponton (IP-cím) belüli szolgáltatások megkülönböztetését (alkalmazás, például: 53 DNS). Nincs tehát kapcsolatfelépítés vagy megbízható kommunikáció, csak egyszerű datagramszolgáltatás.

Fejlécben:

- forrás- és célport
- ellenőrzőösszeg

További jellegzetes protokollok:

- ARP (Address Resolution Protocol): alacsonyszintű protokoll, IP-címhez megadja a MAC-címet. Megkérdezi egy adatkapcsolati rétegbeli broadcasttal, hogy kihez tartozik a kérdéses IP-cím. Az adott állomás válaszol.
- ICMP (Internet Control Message Protocol): vezérlőprotokoll az IP működéséhez. Hibajelentések (nem elérhető, hibás paraméter stb.) és diagnosztika (echo – „ping”).
- IGMP (Internet Group Management Protocol): multicast használatát menedzselő protokoll.
- DNS (Domain Name System): Nevek és IP-címek elosztott adatbázisból való lekérdezését végző protokoll.
- RIP, OSPF, ISIS: Routingprotokollok hálózaton belüli útválasztáshoz.
- BGP: Routingprotokollok hálózatok közötti útválasztáshoz.
- SMTP (Simple Mail Transfer Protocol): elektronikus levelek továbbítását végző protokoll.
- POP3 (Post Office Protocol 3), IMAP (Internet Mail Access Protocol): levelezőszerverről levelek lekérdezést végző protokollok.
- HTTP (Hipertext Transfer Protocol): web alaprotokollja.
- SSL (Secure Sockets Layer): protokoll szállítási szintű rejtjelzésre (v.ö.: IPSec).
- FTP (File Transfer Protocol): állományok átvitelére szolgál (nem biztonságos lehallgatás ellen!).
- Telnet: távoli terminál (nem biztonságos lehallgatás ellen!).
- SSH (Secure SHell): biztonságos távoli terminál. Kommunikáló felek autentikálva vannak, adatfolyam rejtjelzett. Általános biztonságos átvitelre is használható (tunneling).

9.2.2. Hálózati szintű sérülékenységek

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. Az alábbiakban néhány példa olvasható a hálózati támadásokra.

- ARP spoofing: ARP- alapú támadás. A támadó egy hamisított MAC-címet ír be az Ethernet csomagba.
- IP spoofing: IP-alapú támadás. Az IP-csomagban a forráscím hamisítva van, így megbízhatónak tűnik a hálózat számára.
- Land-támadás: IP-alapú támadás. Az IP-csomagban a forrás és a célcím ugyanaz, amit az áldozat nem tud lekezelni.
- Source routing: IP-alapú támadás. Az IP lehetőséget ad arra, hogy a csomagok routolási útvonalát megadjuk. A támadó olyan csomagot hozhat létre, amivel egy távolról elérhető gépen keresztül védett, belső számítógépet érhet el.
- „Tiny fragment”-támadás: TCP-alapú támadás. A támadó a megengedett legkisebb csomagot hozza létre, amiből kimaradnak a TCP-flagek. Ezek a második csomagban érkeznek, amit a rendszer már nem vizsgál, így ki lehet kerülni a szűrési szabályokat.
- Hálózati szintű sérülékenységek.

– „Overlapping fragment”-támadás: TCP-alapú támadás. A támadó az első csomag fejlécében olyan szolgáltatást ad meg, amit a tűzfal átenged, az utána következő csomagok viszont már egy szűrt szolgáltatás felé irányulnak, kártékony tartalommal.
– SYN flood (elárasztás): TCP-alapú DoS-támadás. A támadó SYN-üzeneteket küld az áldozatnak, aki erre SYN-ACK-választ küld, és erőforrást foglal le. A támadó viszont nem küld ACK-választ, így előbb-utóbb az áldozat leterhelődik.
– Teardrop-támadás: UDP-alapú DoS-támadás. A támadó olyan összezavart UDP-csomagokat küld az áldozat felé, amiket az áldozat nem tud összerakni, így a gép elérhetetlenné válik.
– Fraggle-támadás: a smurf-támadás továbbfejlesztése, ami UDP echo típusú csomagokat küld a hálózatra.
– Smurf-támadás: ICMP-alapú DoS-támadás. A támadás során broadcast ping üzenetet küldenek a hálózatra, forráscímként az áldozat IP-címét megadva. Erre a hálózat összes bekapcsolt gépe válaszol, ezzel minden egyes csomagra akár több száz válaszcsomag érkezhet, ami elárasztja az áldozatot.
– „ICMP flood”-támadás: ICMP- alapú DoS-támadás. A támadó annyi ICMP echo típusú csomagot küld az áldozatnak, hogy az már nem tudja ezt feldolgozni, és elérhetetlenné válik.
– Ping of Death: ICMP-alapú DoS-támadás. A támadó az IP maximális csomagméreténél (65535) nagyobb ping-üzenetet küld, ami természetesen több darabban érkezik meg. Kibontás után azonban az operációs rendszer nem tud vele mit kezdeni, puffer-túlcsordulással lefagy.
– „ICMP redirect”-támadás: ICMP-alapú támadás. A támadó egy hamisított forrású ICMP redirect típusú üzenetet küld az áldozatnak, amiben azt üzeni, hogy a routolás más irányba történik. Így a legális gateway-ről át tudja a forgalmat irányítani saját maga felé. MitM-támadásokhoz használható.

9.2.3. Tűzfalak

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 leggyakoribb tűzfal-alaptípusok az alábbiak.

– Csomagszűrő: Első generációs tűzfal, a szűrés az alapvető IP/TCP/UPDjellemzők (hálózati és szállítási szint) alapján történik, mint forrás és cél IPcímek, forrás- és célportok, opciók és vezérlőbitek. Egyszerű megvalósítás, gyors működés, csak egyszerű szabályok valósíthatóak meg.
– Állapottartó (stateful inspection): Második generációs tűzfal. Különböző rétegekben dolgozik, az egyik rétegből vett információk alapján vezérli más rétegek szabályait. Például alkalmazási protokollból „kinézi”, hogy milyen portokat kell még kinyitni a kapcsolat idejére. A tűzfal minden kapcsolat állapotát tárolja, ebből dönti el, hogy az adott kapcsolat egy új kapcsolat, része egy másik kapcsolatnak, vagy nem része egyetlen kapcsolatnak sem.
– Alkalmazásszintű tűzfal (application layer): Harmadik generációs tűzfal, mely „érti” az egyes hálózati alkalmazások kommunikációját. Hatékony a nem kívánt vagy ismeretlen alkalmazások kommunikációjának szűrésére. Ide tartoznak az egyre elterjedtebb új generációs tűzfalak (Next Generation Firewall – NGFW) és a webapplikációs tűzfalak (web application firewall – WAF) is.

A tűzfalakat különböző topológiák szerint lehet az infrastruktúrába telepíteni. A kiépítést jellemzően az infrastruktúra bonyolultsága és az elérendő cél határozza meg. A legjellemzőbb típusok az alábbiak.

– Kétlábú tűzfal: a külső és a védett hálózat között helyezik el a tűzfalat.
– Háromlábú tűzfal: a külső zóna, a DMZ és a védett hálózat között helyezkedik el. (Fizikailag állhat több tűzfalból is!).
– Personal firewall/bastion host: egy gépet védő tűzfal, magán a védendő gépen telepítve (tudja figyelni az egyes alkalmazásokat is!).

A határvédelem kialakításában ki kell emelni a demilitarizált zóna (DMZ) szerepét! Ez a külső hálózat és a védett hálózat védelmi szintje között elhelyezkedő szegmens. Ide helyezzük a külső szolgáltatásokat nyújtó gépeket, melyek kompromittálódása esetén még mindig van egy védelmi vonal a belső hálózat felé. A DMZ és belső hálózat közötti forgalom erősen korlátozott. Megvalósítás: háromlábú tűzfallal, több tűzfallal lehetséges.

Általában a tűzfalakkal valósítják meg a címfordítást (Network Address Translation – NAT) is. Ennek célja elsősorban az, hogy mivel az IP-címek számossága véges, így meg kell oldani azt, hogy a belső hálózatban privát címeket használhassunk. Belső címből ugyanis elegendő áll rendelkezésre, a külvilág felé pedig elég egy publikus cím, amely a NAT-eszköz „külső” címe. Belülről induló kapcsolat esetén a NAT kicseréli a belső forráscímet a külső címre, megjegyzi a célcímhez tartozó belső címet, visszirányú forgalomnál pedig visszacseréli azt. Kívülről induló kapcsolat nem lehetséges, kivéve, ha statikusan fel van véve az adott belső cím a tűzfalra. Ha többen kommunikálnak ugyanarra/ugyanarról a címről, a forrásportokat is lecserélheti.

A NAT-olás legkomolyabb előnye, hogy csak egy publikus cím kell, a belső hálózat pedig „nagyjából” el van rejtve (fennálló kapcsolaton azért be lehet törni!). Hátránya az, hogy kívülről nem lehet kapcsolatot nyitni és egyes protokollok nem tűrik a címek átírását.

9.2.4. Távoli hozzáférés

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 hozzáféréssel kapcsolatban az alábbi követelményeket kell figyelembe venni:

- Legyen megfelelő felhasználó- és rendszerhitelesítés.
- Megfelelő hozzáférési jogosultságokat kell biztosítani az entitásoknak.
- Gondoskodni kell a bizalmas adatok védelméről.
- Legyen naplózva és auditálva a távoli hozzáférési tevékenység.
- Transzparens hozzáférés kell az erőforrásokhoz.
- Földrajzi helytől függetlenül meg kell oldani a hozzáférést.
- Az összes távoli felhasználó hozzáférését biztosítani kell, ha szükséges.
- Mindezt minimális költséggel kell megoldani.

A távoli hozzáférést többféleképpen meg lehet valósítani, de napjainkban szinte kizárólag az interneten keresztüli elérés dominál. Ezenkívül korábban jellemző volt a telefonhálózaton keresztüli és a dedikált (bérelt) vonalakon történő elérés is.

Az interneten keresztüli elérést virtuális magánhálózatok (VPN) segítségével szokás megvalósítani. Ez olyan megoldások halmaza, melyek a szélessávú internetkapcsolatot felhasználva, a nyílt interneten keresztül kapcsolják össze a felhasználót és a szervezeti hálózatot. Két hálózat összekötése is lehetséges, ekkor az egyik hálózat forgalmát rejtjelezzük és „becsomagoljuk”, így küldjük át a másik hálózatba (tunneling, különböző szinteken lehetséges). Látszólag a két hálózat közvetlenül van összekötve, egy hálózatként működik. A VPN biztosítja a bizalmasságot, az adat sértetlenségét és a hitelesítést. A szabvány támogatja gyakorlatilag minden protokoll összefogását és becsomagolását a forrásnál, továbbítását a 2. vagy 3. rétegen, és kicsomagolását a címzettnél.

Néhány elterjedt formája:

- Internet Protocol Security (IPsec),
- Transport Layer Security (SSL/TLS),
- Datagram Transport Layer Security (DTLS)
- Microsoft Point-to-Point Encryption (MPPE)
- Microsoft Secure Socket Tunneling Protocol (SSTP)
- Multi Path Virtual Private Network (MPVPN)
- Secure Shell (SSH)

A legelterjedtebb szabvány az IPSec. Ez hálózati szintű rejtjelzést és autentikációs keretrendszert valósít meg. 3. rétegbeli protokoll, mely támogatja a hitelesítést és a rejtjelzést. Gyakorlatilag az IPv4 kiterjesztésének fogható fel. A szabvány az IPcsomagokat ellátja IPSec-fejlécekkel, így koordinálva a kommunikációt. A keretrendszerben különböző kriptográfiai és kulcscsere-protokollok használhatóak. A fontosabb fogalmak a következők:

- A Security Association (SA) egy kapcsolat egy irányára jellemző IPSecparamétereket (rejtjelzés, autentikáció típusa, algoritmusa, kulcs stb.) adja meg.
- A SA adatbázis (SADB) az SA-k összessége. Az kommunikáló állomás a forgalom küldésekor/vételekor az SADB-vel konzultál, hogy mely paramétereket kell használni

A három alapprotokollja a következő:

- Authentication Header (AH) – feladata a hitelesítés, általában egy megosztott titok 96 bites lenyomatát tartalmazza,
- Encapsulating Security Payload (ESP) – a tartalom rejtjelzéséért felel, tipikusan 3DES algoritmusú blokkrejtjelzést használ,
- Internet Key Exchange (IKE) – a kapcsolat felépítéséért felelős, feladata a hitelesítéshez és rejtjelzéshez szükséges paraméterek kezelése.

Az IPSec kétfajta üzemmódban tud működni:

- Transzport – végpont-végpont közötti forgalomrejtjelzés,
- Tunnel – tipikusan két alhálózat közötti megbízható kommunikációra használják.

9.2.5. Vezetéknélküli hálózatok

Szintén a mobilitás segíti elő a vezetéknélküli hálózatok (wireless LAN – WLAN, vagy WiFi) elterjedését. Az évek során ez a terület számos biztonsági problémával szembesült, melyek azonban napjainkban kivétel nélkül kezelhetők, így a nagyobb szervezetek is kiválóan, különösebb biztonsági kockázat nélkül használhatják ki ezt a technológiát. Még mindig jellemző azonban, hogy a WiFi-eszközök általában a lehető legkevesebb biztonsági beállítást tartalmazzák alapállapotban. Éppen ezért érdemes a következő tanácsokat figyelembe venni, különösen kisebb hálózatok esetén, kevés végpont használatánál:

- Változtassuk meg a hálózati SSID[78]-t!
- Változtassuk meg a gyári jelszót!
- Kapcsoljuk be a MAC-szűrést!
- Ha tudjuk előre, hogy kik csatlakoznak a hálózathoz, ne kapcsoljuk be a DHCP-t!
- Olyan alhálózati beállítást válasszunk, ami nem triviális (például 10.157.29.0/24)!
- Csökkentsük a szórás hatótávolságát!

Az ajánlások között szokott még szerepelni az SSID-szórás (broadcast) kikapcsolása is, de ezt sokan ellenjavallják, mert komoly védelmet nem nyújt, a hálózatot csak az amatőrök ellőtt takarja el, ugyanakkor a hatókörön lévő kliensek folyamatos csatlakozási szándéka felfedi és támadhatóvá teszi azokat. Másik probléma, hogy egyes mobil eszközök e funkció nélkül nem tudnak a hálózatra csatlakozni.

Alapvető fontosságú, hogy használjunk csatornarejtjelzést is! Megfelelő beállítás esetén a forgalom visszafejtésének kockázatát minimálisra lehet redukálni. Tipikus rejtjelzési beállítások:

- WEP – már nem biztonságos, bár javítottak rajta, de kellő elszántsággal feltörhető,
- WPA – eddig biztonságosnak tartott rejtjelzés, de bizonyos esetekben ez is feltörhető.

A WEP-rejtjelzés használata nem ajánlott, hiszen törése rendkívül egyszerű, egyben jó példája a nem körültekintő biztonsági tervezésnek. A WEP-et 1999-ben szabványosították, RC4-es folyamrejtjelzést használ a bizalmasság megőrzéséhez. A szabványos WEP-kulcs 64 bites, amiből 40 bit a titkos kulcs, amit egy 24 bites inicializációs vektorral (IV) konkatenálnak. A 128 bites WEP-kulcs 26 hexadecimális karakterből és egy 24 bites IV-ből áll. Az egész csomag sértetlenségét CRC-32 algoritmussal védik, ami a csomag megváltoztatása után kicselezhető. A tervezés során elkövetett hibák miatt azonban ez a protokoll nagyon sérülékeny (elsősorban az IV kis mérete miatt).

A WEP gyengeségeinek kihasználása lehetséges:

- Passzív támadással, mellyel a forgalmat lehet dekódolni – statisztikai analízis útján deríthető ki a forgalmazott adathalmaz,
- Aktív támadással, melynek során nem hitelesített állomásról szúrnak be új forgalmat – ismertszöveg-alapú támadással lehet visszafejteni a forgalmat,
- Aktív támadással, mellyel a forgalmat dekódolják – a támadás az AP-vel való trükközésen alapul,
- Szótáralapú támadás – az elmentett adatforgalomból utólag szedik ki a WEPkulcsot.

A törés folyamata:

- Felderítjük a hálózatot, azonosítjuk a célpontot.
- Elfogjuk a célpont és a hozzá kapcsolódó kliensek közötti forgalmat, különös tekintettel az ARP-csomagokra, melyekből a nyíltszöveg-alapú támadással egyszerűbben kinyerhető a kulcs.
- Az elfogott adatcsomagokból „brute-force”-módszerrel kinyerjük a kulcsot.

A WPA egy ideiglenes megoldásnak született a 802.11i szabvány véglegese előtt. A WPA különböző kulcsot rendel mindegyik felhasználóhoz, de az otthoni, kis szervezeti használatban a Preshared Key[79] (PSK) funkcióját szokták kiválasztani. Ebben az esetben minden felhasználónak ugyanaz a 8–63 karakter hosszú (vagy 64 darab hexadecimális számjegyből álló) jelszó a kulcsa a hálózati hozzáféréshez. A WPA-ban került bevezetésre a TKIP (Temporal Key Integrity Protocol = Ideiglenes Kulcssérthetetlenségi Protokoll), amely dinamikusan változtatja az alkalmazott kulcsokat, és más védelmi mechanizmusokat is tartalmaz.

A WPA2-be a TKIP-en túl beépítettek egy AES-alapú rejtjelző algoritmust, amivel a biztonsága tovább nőtt.

A WPA tervezése során komolyan vették a biztonságot, ezért egy roppant jól kezelhető és ellenálló protokollnak tekinthető. A törés gyakorlatilag csak akkor valósítható meg, ha a felhasználó gyenge jelszót választott.

A támadás menete:

- A hitelesített kliens leválasztása az AP-ról deautentikációs kéréssel.
- Az újbóli autentikációs csomagok elfogása.
- Az elfogott csomagokból a jelszó visszaállítása.

[78] A hálózat azonosítója (Service set identification).
[79] Osztott kulcs.

9.3. Alkalmazások

9.3.1. 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, levelezőrendszerek, FTPkliens 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

9.3.2. 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 hozzáférésvédelem, 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.

9.3.3. Adatbázis-kezelők

Az adatbázis-kezelőkön itt most az SQL felületű relációsadatbázis-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 leállásig. Egyidejűleg több adatbázist képesek kezelni és párhuzamosan bejelentkezett több felhasználót kiszolgálni. A nagy adatmennyiséggel, tranzakciókkal jellemezhető felhasználói programok az adatbázis-kezelők 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 szempontból az adatbázis-kezelők

idővel teret nyertek, és ma már az egyfelhasználós videokazettanyilvántartó programocskák is az adatbázis-kezelők szolgáltatásait veszik igénybe.

A jelentősebb adatbázis-kezelők rendelkeznek (Common Criteria szerinti) biztonsági tanúsítvánnyal. Meg kell jegyeznünk, 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 pluszköltséget 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 jelentenek.

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 kideríthet a hiányosságokat, de azok megszüntetése utólag mindig jóval bonyolultabb és költségesebb.

9.3.4. „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 felhasználó számra, 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 a 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 hierarchia szinttől 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 munkatársak egyéb, más szempontból nyilvántartott személyes adatait, vagy fordítva, egy speciális ügykezelő dolgozhat ezen adatokkal, de nem tudhatja, kinek mennyi a bére. A differenciált, szerepkörökhöz kötött hozzáférés mind az adatbáziskezelőben, 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 elkészteni, hogy az operációs rendszer megbízható felhasználó-azonosító rendszerét vagy a szervezetnél alkalmazott biztonsági szerver hasonló szolgáltatásait vegye igénybe. Ez utóbbi biztonsági szerverek általában a heterogén számítástechnikai rendszerrel rendelkező, nagy szervezetek egységes felhasználó-azonosító rendszerének (SSO[80]) biztonsági szerverei, amelyek szabványos protokollon (LDAP[81]) keresztül biztonságos, megbízható módon azonosítják a felhasználót.

9.3.5. Egyéb kiegészítő és segédprogramok

A kiegészítő programok körébe rendkívül sok programtípus beleérthető. Ide tartoznak a mindenféle formátumú szövegfájlok, képek, mozgóképek megtekintésére, szerkesztésére szolgáló programok, binárisfájl-editorok, adatbázis-

[80] SSO: Single Sign On – Egyszeri bejelentkezés
[81] LDAP: Lightweight Directory Access Protocol

lekérdező/módosító eszközök, fájlkezelők, tömörítő, szótár, rajzolóprogramok és egyebek. Ezekre még inkább igaz, mint az irodai programokra, hogy tervezésük során biztonsági szempontokat nem vettek figyelembe.

E programok – minden praktikus hasznuk mellet – 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 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.

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

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

A kriptológia egyik fő területe a *kriptográfia*, magyarul a rejtjelzés (gyakran titkosítás, kódolás, régiesen sifirozás), amelynek alapvető feladata matematikai módszereket alkalmazó **algoritmusok**kal 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 rejtjelzése, 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 szöveg*ből *rejtjelzés* segítségével *rejtjelzett szöveg*et állít elő, majd elküldi a vevőnek, aki azt *visszafejt*ve (megoldva) megkapja az eredeti nyílt szöveget. A rejtjelzési folyamat – kódolás – során a rejtjelzett szöveg előállításához az algoritmuson kívül általában szükséges egy *kulcs* is, amelynek ismerete elengedhetetlen a rejtjelzésnél 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. [1]

9.4.1. Szimmetrikus rejtjelző algoritmusok

A klasszikus rejtjelző eljárások egyetlen kulcsot használnak rejtjelzésre és megoldásra, miközben a megoldó algoritmus nem feltétlenül egy fordított sorrendben végrehajtott rejtjelzés.

„1976 decemberében a *National Bureau of Standards*, USA, bejelentett egy új „Nemzeti Adatfeldolgozási Szabványt" (FIPS No. 46), amelyben a Data Encryption Standard, DES, rejtjelző gépet szabványosították. A DES 64 bites nyílt üzenetblokkokat 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 kormányzata megtiltotta, hogy ezt a hardware-kivitelezést exportálják.

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 chip-megvalósítás 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." [39]

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 Rejtjelző Szabvány)* nevet kapta. A pályázatot 1997 szeptemberében írták ki, közzétéve azon elvárásoknak a listáját, amelyeknek az AES algoritmusnak meg kell felelni. Ugyanakkor deklarálták, hogy a benyújtott rejtjelzési algoritmusok nyilvánosak, szabadon felhasználhatók lesznek. A kiírás szerinti elvárások [39]:

– 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, emellett *egyszerű, világos, bármely programozási nyelven gyorsan programozható*. Ez is számos iterációs lépésben valósul meg.

A szimmetrikus rejtjelző eljárások közül a 168 bit kulcshosszúságú Triple Des, a 128–256 bit kulcshosszúságú AES rejtjelzőeljárásokon 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.

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. ” [39]

A rejtjelzést 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 rejtjelzés 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 rejtjelzett 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 rejtjelzett 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 rejtjelzést a (D,M) titkos kulccsal is el lehet végezni. Ekkor a megoldókulcs a nyilvános (E,M) kulcs lesz.” [39]

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.

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 (message digest) készíti el, amely kizárólag az adott szövegre jellemző. Az algoritmus ugyanazon bementi sorozat esetén ugyanazt a lenyomatot eredményezi." [39]

A gyakorlatban a legelterjedtebben használt hash-függvények az amerikai National Institute of Standards and Technology (NIST) által Szövetségi Informatikai Szabványként[82] (FIPS) elfogadott SHA-1, SHA-2 és, a legújabb, SHA-3. A korábban előszeretettel használt MD5 függvény már nem fogadható el biztonságosnak, mert rá már nem teljesül az ütközés-ellenállóság. A közelmúltban ütköző SHA-1 lenyomatokat is találtak, és már van olyan algoritmus, amellyel további ütköző lenyomatú fájlokat lehet készíteni, bár ez ma még csak elvi probléma, de már új alkalmazásokban nem érdemes felhasználni.

SHA-1 algoritmus inputja egy maximum 2^64 bit hosszúságú dokumentum, az outputja pedig egy 160 bit hosszúságú string. Az SHA-2 több függvény, az SHA-224, SHA-256, SHA-384 és SHA-512 függvények összefoglaló neve, amelyek a nevükben is jelzett hosszúságú lenyomatot állítanak elő. Inputjuk egy maximum 2^128 bit hosszúságú dokumentum. Az SHA-3 szintén több függvény, az SHA3-224, SHA3-256, SHA3-384 és SHA3-512 függvények összefoglaló neve, amelyek a nevükben is jelzett hosszúságú lenyomatot állítanak elő. Inputjukra nincs méretkorlátozás. Az MD5 128 bites hosszúságú lenyomatot állít elő.

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 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 *hitelesítésszolgáltató*n, vagy közismert nevén a Certificate Authority-n (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.

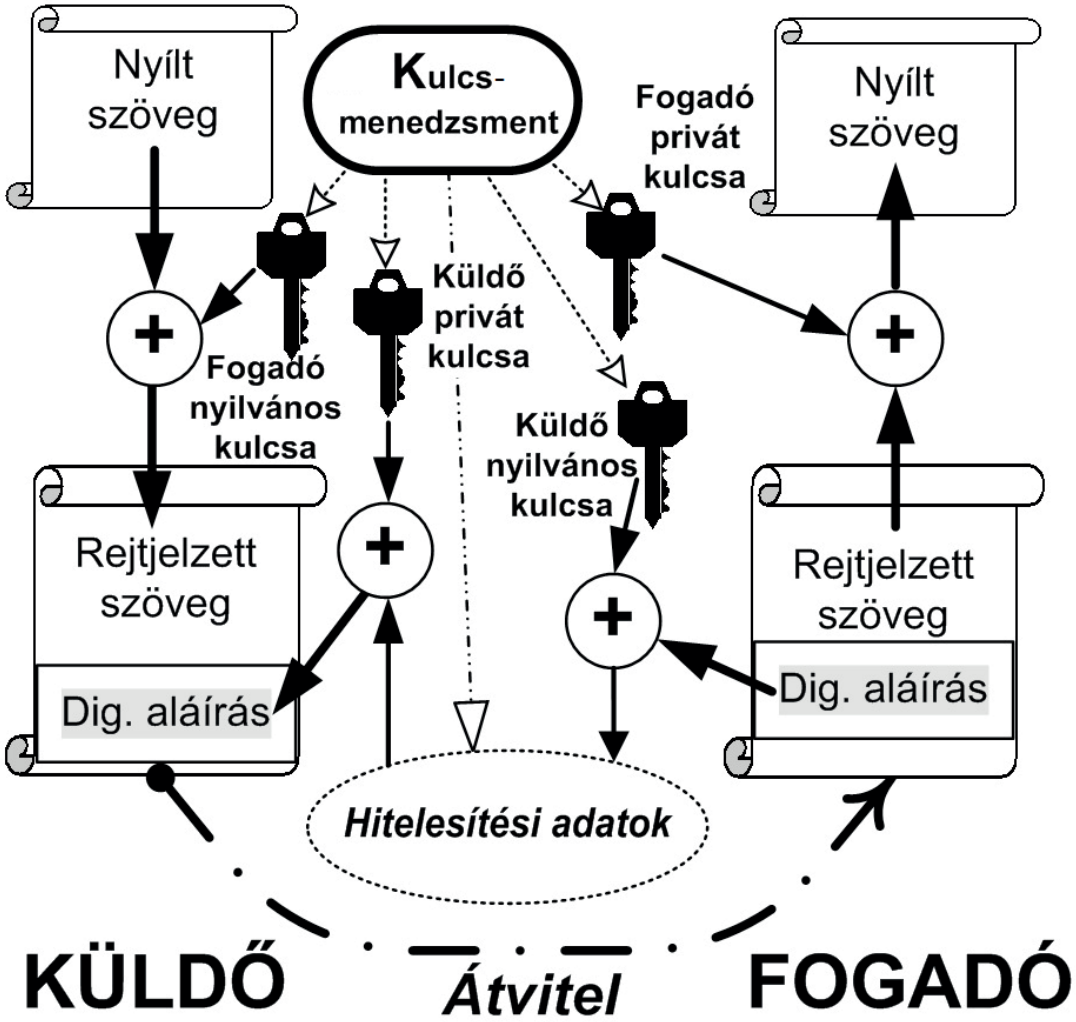
A rendszer legfontosabb eleme a fastruktúra gyökerében elhelyezkedő CA, aki direkt módon bizonyítja egy kulcs valódiságát, amennyiben ő adta ki. A faszerkezet többi szereplője a CAtól vagy egymástól kaphat igazolást egy objektum valódiságáról.

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 rejtjelzés, 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 a 9. ábra vázolja. " [39]

[82] Federal Information Processing Standard



9. ábra Az elektronikus aláírás folyamata [39]

„A hitelesítés-szolgáltatónak feladata ellátásához rendkívül szigorú biztonsági feltételeket kielégítő infrastruktúrával kell rendelkezni. Ezek a biztonságos rejtjelzési módszerek mellett magukban foglalnak számítástechnikai követelményeket, mint például megbízható tűzfalak alkalmazása, de kiterjednek a személyzetre 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. ” [39]

9.4.5. Kriptográfiai protokollok

”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 *szabványgyűjtemények* 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 kulcscsere-protokollokat használunk. 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), bár ezek némelyike annyira összetett, hogy több részprotokollra bontható. Ezekre a séma elnevezés 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." [39]

A protokollok működési elveik alapján három módon csoportosíthatók[39]:

9.4.6. 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.

9.4.7. 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.

9.4.8. 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 típusú támadással elfoghatók a másnak szánt üzenetek.

9.4.9. 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* (amelyekre 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.

9.5. Rosszindulatú programok

9.5.1. Vírusok, férgek, trójai programok,…

A rosszindulatú számítógépes programokat a (nem szakmai) médiumokban vírusnak nevezik. A (valódi) szakma a rosszindulatú programokat malware gyűjtőnéven foglalja össze. (A malware, ami az angol malicious software, azaz rosszindulatú program kifejezésből képzett mozaikszó.) Ide soroljuk az alábbiakat:

- Virus – vírus
- Worm – féreg
- Logic bomb – logikai bomba
- Trojan horse – trójai faló, trójai program
- Backdoor (trapdoor) – hátsóajtó (csapóajtó)
- Mobile Code – mobil kód
- Rootkit – nincs magyar megfelelője, a UNIX-os rendszergazda (root) és az installálócsomag (kit) összevonás*ából ered*
- Keyloggers – billentyűzetfigyelő
- Spyware – kémprogram
- Adware – agresszív reklámprogramok
- Hoax – *átverés, álhír, kacsa*
- Spam – levélszemét

*Vírus*nak egy olyan programot nevezünk, amely képes arra, hogy önmagát reprodukálja, azaz szaporodjon, figyelembe véve mindig változó környezetét. A vírusok számtalan fajtáját különböztethetjük meg. Egy részük a lemezek boot-területét fertőzi meg, ezek a bootvírusok. Mások a bináris programkódot tartalmazó programfájlokat támadják, abban helyezik el a futtatandó víruskódot, ezek fájlvírusok. A harmadik nagy víruscsalád tagjai a fentiekkel ellentétben nem bináris kódú programokat fertőznek, hanem dokumentumfájlok belsejében helyezik el szerkeszthető szövegként vagy védetten, rejtetten programkódjukat, és célpontjaik, támadáspontjaik többsége is elsősorban, bár nem kizárólag, további dokumentumokra irányul. Ezt a víruscsaládot nevezzük makróvírusoknak. Mintegy mellékszolgáltatásként egyes makróvírusok képesek „hagyományos" bináris víruskód elszórására is (dropperek), valamint több tucatnyi makróvírusfejlesztő-készletet is ismerünk, amelyekkel bármiféle előképzettség nélkül is lehet újabb vírusváltozatokat is gyártani. A makróvírusok után egy újabb értelmezőt igénylő víruscsalád is megjelent, a scriptvírusok. Amíg a makróvírusok kódja bonyolult fájlszerkezetű dokumentumfájlokban rejtőzködik, addig a scriptvírusok többsége közönséges szövegfájlokban vagy áttekinthető és dokumentált struktúrát használó HTML-fájlokban található. Az utolsó típus voltaképpen nem a felépítés, hanem a preferált szaporodási mód miatt alkot egy egyre bővülő csoportot. Ez a levelezővírusok csoportja. [40]

A **férgek** a rosszindulatú programok második típusa. A vírusoktól annyiban különböznek, hogy kódjukat nem a lemezek bootszektorába vagy más programok belsejébe építik, hanem azt egyszerűen önálló fájlban tartalmazzák, és ezt másolva sokszorozzák. A szaporodás során természetesen módosítják azokat a fájlokat is, ahonnan programindítás lehetséges. Az elektronikus levelezéssel és a hálózatos alkalmazások elterjedésével a programférgeknek számtalan típusa alakult ki. [40]

A **logikai vagy időzített bombák** olyan programkártevők, amelyek néha külön programként, de jóval gyakrabban nagyméretű és bonyolult szoftverek belső, rejtett rutinjaiként kerülnek be a számítógépes rendszerekbe. Ezek többségét olyan programozók követték el, akik bizonytalan vagy annak érzett pozíciójukat rejtett időzített bombák elhelyezésével igyekeztek megerősíteni. A rosszindulatú, a rendszer leállásával és sokszor teljes összeomlásával járó rutinok akkor aktivizálódtak, ha programozójuk például lekerült a fizetési listákról vagy elmulasztotta átírni a késleltetési periódust megszabó programrészleteket. A levélbombák olyan kisméretű alkalmazások, amelyek egyetlen funkciója a pusztítás. Elnevezésük onnan ered, hogy gyakran érkeznek e-mailekhez csatolva. [40]

A **trójai programok**. közös jellemzője, hogy valamely más program programkódjába rejtve tartalmaznak oda nem illő, rendszerint kártékony hatású programrutinokat. A trójai program – amíg el nem indítják és kártékony munkáját el nem végzi – hasznosnak látszik. Igen gyakran más hasznos, ismert program preparált változata. A trójai programok célpontjai azok a számítógép-felhasználók, akik ellenőrzés nélkül indítanak el az internetről letöltött, elektronikus levélben kapott, vagy más, rendszerint ismeretlen és ellenőrizetlen (sokszor teljesen ellenőrizhetetlen) forrásból származó programokat. Vannak olyan trójai programok is, amelyek kémprogramokat, jelszólopókat, backdoor-programokat tartalmaznak, de ezeken kívül is sok más változatot különböztethetünk meg. [40]

A **backdoor**-program – a megtámadott gép felhasználójának tudomása és engedélye nélkül – a helyi hálózaton, soros vagy párhuzamos porton vagy modemen keresztül összeköttetést teremt és adatcserét biztosít a megtámadott gépre felkerült szerver-komponens és a támadónál üzemelő kliens-komponens között. Így a támadó adatokat tölthet le a megtámadott gépről, illetve azon keresztül a megtámadott hálózatról, vagy ez fordítva, azaz feltöltést (is) biztosít a backdoor. A megoldástól függően, átveheti a vezérlést a rendszer felett. [40]

A **rootkitek** a backdoor-programokhoz hasonlóak. Eredetileg Unix (Linux) platformra találták ki ezeket a kártevőket. A rootkitek igen kisméretűek és valamilyen vírus vagy trójai program segítségével jutatják be a fertőzött számítógép operációs rendszerébe.

A **spywerek** a megfertőzött számítógép memóriájában vagy adattárolóin kutakszanak, míg a **keyloggerek** a billentyűzet leütéseinek a „loggolásával" gyűjtenek információkat, tipikusan felhasználóneveket és jelszavakat, bankszámlaszámokat és a hozzájuk tartozó jelszavakat.

A **hoaxok** rémhírek vagy lánclevelek. E-mail, ami önmagában kárt nem okoz, magától nem terjed. A felhasználók azok, akik gondolkodás nélkül, lelkesen, akár több száz példányban is továbbküldik ezeket, és ezzel az esetleges rémhírterjesztésen kívül még hatalmas fölösleges forgalmat is generálnak a hálózaton. A „küldd el 20 ismerősödnek 5 napon belül, és akkor nagy szerencse ér" vagy a „szegény szerencsétlen rákos gyermekek, akik 1 dollárt kapnak minden elküldött levélért" szövegnél csak „az első tíz beküldő egy … notebookot kap" vagy „ha megnyitod a … fejlécű levelet, akkor a géped azonnal felrobban" szöveg a hatásosabb. [40]

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 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-használatot." [41]

9.5.1.1. 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 munkatársnak. " [41]

A szabályzatnak tárgyalnia kell az alábbi pontokat [41]:

- 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.

9.5.1.2. Hardver-védelem

„A személyi számítógépek hardverkonfigurációval kapcsolatos specifikációi az úgynevezett BIOS(Basic Input-Output System)-beállításokkal változtathatóak. A helyes beállítások alapvető fontossággal bírnak a számítógép működése szempontjából, ezért azoknak a felhasználók által való megváltoztatása nemkívánatos. 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 bootszekvenciabeállítás és a bootszektor-védelem. " [41]

9.5.1.3. 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." [41]

9.5.1.4. Szoftvervédelem

Keresőeszközök

„A vírusok elleni védelem hatékonyabb módszere a vírusszkenner-szoftverek alkalmazása. A szkenner-szoftver a már a gépre került vírusok után keres a bootszektorban, 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." [41]

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 floppy bootszektorát 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 szkennermegoldások esetében." [41]

9.5.1.5. 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." [41]

9.5.1.6. Felhasználói oktatás

„A vírusvédelmi politikában komoly figyelmet kell fordítani a munkatársak megfelelő szintű tájékoztatására. A munkatársak hozzáállásának pozitív befolyásolása a megelőző vírusvédelem első frontját jelenti. Ha a munkatársak kellő odafigyelést tanúsítanak a problémával kapcsolatban, akkor nagymértékben csökkenteni lehet a műszaki megoldások hatékonyságától való függést." [41]

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. A legtöbb információbiztonsági szabvány ebben segít.

Az üzemeltetés azt a környezetet érinti, amelyben az információt a szervezeten belül kezelik. A környezet jelenthet hardvereket, szoftvereket, hálózatot, embereket, épületeket stb. Ezt a környezetet többféle fenyegetés érinti, például:

- Kiszivárgás (bizalmasság).
- Erőforrások megsemmisülése (rendelkezésre állás).
- A feldolgozás megakadása (rendelkezésre állás).
- Sérülés/módosítás (sértetlenség).
- Lopás/eltávolítás (rendelkezésre állás).

A rendszer üzemeltetett elemei

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

A hardverek és szoftverek közül azokra vonatkoznak az üzemeltetés biztonsági kérdései, melyek az információ feldolgozásában részt vesznek, például számítógépek, perifériák, fénymásológépek, operációs rendszerek, alkalmazások stb.

A hardveres környezetre vonatkozó fenyegetések lehetnek például:

- Nem jogosult hozzáférés a tárolt adatokhoz.
- Az erőforrások nem jogosult felhasználása.
- Túlterheléses támadások.
- Eszközhibák.
- Rendszergazdák által elkövetett támadások.
- Nem jogosult csatlakozás a hardvereszközökhöz.

Az alábbiakban a teljesség igénye nélkül néhány fontos védelmi intézkedés található, melyek jelzik, hogy az üzemeltett rendszerek esetén milyen tipikus biztonsági feladatokat kell megoldani.

Jelszóvédelem az IT rendszerekre:

- BIOS-jelszavak használata, mely segít megakadályozni a rendszerbeállítások megváltoztatását.
- Operációs rendszerek jelszavai.
- Egyéb hardveres megoldások is szóba jöhetnek (például hardverkulcs).

Képernyőzár:

- Automatikusan induljon el néhány perc inaktivitás után.
- Csak jelszóval lehessen kilépni belőle.
- A Windows és a Linux ablakozó felületei ezt támogatják.

Víruskereső rendszeres futtatása:

- Folyamatos védelem működtetése (on-access scan).
- Igény szerinti futtatás hetente (on-demand scan).
- Rendszeres frissítés (naponta).

Külső adattárolók (CD, DVD, USB pendrive) kezelése:

- Külső adattárolók eltávolítása a munkaállomásokból.
- Letiltás BIOS-ból vagy operációs rendszerből.
- Speciális szoftver használata a külső adattárolók hozzáférésének engedélyezésére.

Előre beállított jelszavak kicserélése:

- A rendszer egyik elemén sem szabad alapértelmezett jelszót hagyni.
- Különösen igaz ez a határvédelem (router, gateway, tűzfal, PBX) eszközeire.

Rejtjelző szoftverek használata a hordozható eszközökön (laptop, tablet, okostelefon):

- A hordozható eszközök elvesztése egy nagy szervezetnél mindennapos. Néha az eszközön tárolt információ értéke nagyobb, mint az eszközé, ezért a tartalmat rejtjelezni kell.
- Esetlegesen a távoli menedzsmentet, letiltást, törlést is lehetővé kell tenni.

Az alkalmazások beépített biztonsági funkcióinak használata:

- Sok alkalmazást szállítanak olyan kiegészítésekkel, amik biztonságosabbá teszik a működését, de alapbeállításban nem működnek. Ezeket érdemes minden esetben bekapcsolni.

Nem szükséges szolgáltatások tiltása:

– Az operációs rendszerek általában sok olyan szolgáltatást tesznek elérhetővé, amire nincs szükség. Ezek hosszú távon csak gyengítik a rendszert, ezért le kell tiltani őket.

Új hardverek és szoftverek tesztelése:

– Semmilyen eszközt nem szabad egyből az üzemi környezetbe telepíteni, ezért egy tesztkörnyezetet is szükséges üzemeltetni.

Sokszor fordul elő, hogy a szervezet működése szempontjából legkritikusabb rendszerek futnak a biztonságilag leggyengébb hardvereken. A vagyonleltárból kiderül, hogy mire kell a legjobban odafigyelni. Ezeknél a kritikus rendszereknél figyelni kell a pótalkatrészekre és a terméktámogatás idejére!

Hardening

A rendszersérülékenység csökkentésére alkalmazott eljárásokat nevezik hardeningnek. Általában célszerű a rendszerben található szoftverek biztonsági beállításainak használata. Ezeket beállítani azonban nem egyszerű. Szinte minden komolyabb termékhez külön kiadnak egy biztonsági beállításokat tartalmazó kiadványt, úgynevezett hardening guide-ot. Nem lehet azonban egyből a legnagyobb biztonságot beállítani, mert lehet, hogy lesz olyan alkalmazás, ami nem fut az ilyen beállítások mellett. Először tesztelni kell, csak utána lehet élesüzembe állítani!

Az alábbi helyeken lehet hardening guide-okat találni:

– NIST: https://nvd.nist.gov/ncp/repository
– CIS: http://benchmarks.cisecurity.org/

A rendszer elemeinek frissítése

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

1. Készítsünk vagyonleltárt!
2. Az új fenyegetések felderítése érdekében figyeljük a biztonsági forrásokat (Bugtraq, MS Security Bulletin stb.)!
3. Állapítsuk meg, hogy melyik sérülékenységnek nagyobb a prioritása!
4. Készítsünk adatbázist a javítandó sérülékenységekről!
5. Teszteljük le az új frissítéseket a tesztkörnyezetben!
6. Tekintsük át az eredményeket!
7. Tájékoztassuk a helyi rendszergazdákat az eredményekről és teendőkről!
8. Alkalmazzunk automatikus patchelési eszközöket!
9. Az alkalmazásokat állítsuk be automatikus frissítésre!
10. Futtassunk végig automatikus sérülékenységteszteket!

Logmenedzsment

Az elektronikus információs rendszerek biztonságának egyik legfontosabb alapköve a megfelelő naplózás, azaz az infrastruktúrában történt események rögzítése. A naplózás információt nyújt az informatikai elemek általános állapotáról csakúgy, mint a biztonságilag fontos történésekről. Ez a műszaki megoldás nélkülözhetetlen a szabálysértések azonnali érzékeléséhez és akár a hónapokkal későbbi kivizsgáláshoz, esetleg bűnügyi nyomozáshoz is, azaz a számonkéréshez. Fontosságát mi sem jelzi jobban, mint az, hogy iparágtól függetlenül minden informatikai szabályozóban kiemelt jelentőséget kap ez a terület.

Az informatikai rendszerekben történő eseményeket nyomon követni az egyes rendszerek naplóbejegyzéseinek gyűjtésével és értékelésével lehetséges. A naplóbejegyzések azonban rendszerenként eltérő formában és minőségben állnak rendelkezésünkre, arról nem is beszélve, hogy ezek mennyisége olyan, melyet feldolgozni manuálisan nem kifizetődő. Mindemellett megjelenik az a probléma is, hogy a rendszerek teljes jogú felhasználói a naplózási beállításokat és akár a bejegyzéseket is képesek módosítani, törölni.

A naplóbejegyzéseket ezért szokás a keletkezés helyétől távol, a rendszerek adminisztrátorai számára el nem érhető módon tárolni, és a szükséges mértékben feldolgozni. Ez a mérték a szervezet döntésén múlik, és alapja általában a kockázatkezelési folyamat eredménye.

A minimális szint a bejegyzések biztonságos gyűjtése és tárolása egy meghatározott ideig (korrektív intézkedés lehetősége), a teljes kiépítés (SIEM) pedig a beérkező bejegyzések online feldolgozása, korreláció az esetleges visszaélések azonnali felfedezése érdekében (detektív intézkedés). Nem szabad azonban megfeledkezni a rendszer preventív hatásáról sem, hiszen egy ilyen rendszer működtetésének visszatartó ereje vitathatatlan.

A naplóállományok gyűjtése sokszor kötelező, de mindenképp hasznos hibák vagy visszaélések kiderítésére.

Lépései:

– Készítsünk szabályzatot és eljárásrendet a logmenedzsmentre.
– Állítsunk fel prioritásokat.
– Állítsunk fel logmendzsment-infrastruktúrát.
– Oktassuk az érintett alkalmazottakat.
– Működtessük a logmenedzsmentet.

A logmenedzsment működésének lépései:
- Minden logforrás naplózási állapotának ellenőrzése.
- A logcsere és archiválás folyamatának ellenőrzése.
- A naplózó szoftver frissítéseinek folyamatos ellenőrzése.
- Minden logforrás idejének hozzáigazítása a központi órához.
- A logolás hozzáigazítása a mindenkori szabályzatokhoz.
- Az anomáliák dokumentálása és jelentése.

Adathordozók

Olyan adattároló eszközök tartoznak ebbe a körbe, melyek részt vesznek az információ feldolgozásának folyamatában. Tárolhatnak érzékeny fájlokat, alkalmazásokat, naplóállományokat, biztonsági mentéseket. Ilyenek a papír, a mikrofilm, a mágneses, az elektronikus és az optikai adattárolók is.

Az adattárolókra vonatkozó fenyegetések:
- Kukabúvárkodás.
- Nem biztonságos megsemmisítés.
- Objektum-újrafelhasználás.

Az adatokkal, adattárolókkal kapcsolatban többek között a következő üzemeltetési teendők vannak.

A bizalmas információk védelme adattovábbítás és szállítás közben:
- Gondoskodni kell a védelemről a jogosulatlan hozzáférés, módosítás és a helytelen címzés ellen.

A megsemmisítendő bizalmas információk védelme:
- A leselejtezett adathordozókból semmilyen információ ne legyen visszaállítható.

Megőrzési idő és tárolási feltételek:
- Minden információnak van egy bizonyos tárolási ideje, mely akár jogszabályból is eredhet.
- Ennek megfelelően kell kialakítani a tárolási rendet.

Adathordozó-könyvtárat kezelő rendszer:
- Az adathordozókat rendszeresen leltárazni és ellenőrizni kell.

Mentés és helyreállítás:
- Ki kell dolgozni a megfelelő mentési stratégiákat.

Mentések tárolása:
- A mentéseket a telephelyen és a telephelyen kívül is (offsite backup) lehet tárolni.

Archiválás:
- A biztonsági mentéstől különbözik, az archiválás sokkal hosszabb ideig tartó folyamat.

A tárolt adatok sértetlenségének folyamatos fenntartása:
- A mágneses, optikai és elektronikai úton tárolt adatok is sérülhetnek, ezért folyamatosan ellenőrizni kell őket.

Biztonsági mentések

Az egyik legfontosabb korrektív kontroll, mely lehetővé teszi a valamilyen okból elvesztett adatok visszaállítását. Mint ilyen, a biztonsági üzemeltetésben kiemelten fontos szerepet kap.

Típusai:
- Strukturálatlan: szisztéma nélküli mentés, például DVD-re. Tipikusan ilyen az otthoni mentés.
- Teljes + Inkrementális: első lépésben minden adatot lementenek, majd egy inkrementális mentés jön, ami az utolsó teljes vagy az utolsó inkrementális mentés óta megváltozott fájlokat tartalmazza.
    - Előnye, hogy szofisztikáltan lehet visszaállítani, hátránya, hogy nagy mennyiségű adatot kell tárolni.
    - Például pénteken egy teljes mentés, majd naponta egy inkrementális mentés. Így egy hét alatt 1 teljes és 6 inkrementális mentés keletkezik.
- Teljes + Differenciális: a differenciális mentés a teljes mentés utáni összes megváltozott fájlt tartalmazza.
- Előnye az egyszerű visszaállíthatóság.
    - Például pénteken egy teljes mentés, utána naponta egy differenciális mentés. Így egy teljes és egy differenciális mentés keletkezik egy hét alatt.

A mentés időbeliségét tekintve az alábbi lehetőségek vannak:
- Online: a mentés néhány milliszekundumon belül történik. Például merevlemez, SAN. Előnye a gyors visszaállítás, hátránya, hogy egy véletlen törlést nem lehet belőle visszaállítani.
- Közel azonnali: valamilyen mechanikus eszköz igénybevételét feltételező mentés, melyről néhány percen belül megkezdődhet a visszaállítás. Például tape library.

– Offline: A visszaállítás elindításához emberi beavatkozásra van szükség. Ez akkor történik, ha a mentések egy raktárban vannak, ahonnan elő kell hozni őket.
– Más helyszínen történő tárolás: A mentett adatok földrajzilag más helyen vannak, mint a rendszer. Ez katasztrófahelyzetek kivédésére alkalmas.

Biztonságos megsemmisítés

Az információ életciklusának a végén áll a megsemmisítés, amikor gondoskodni kell arról, hogy az adott információ semmilyen körülmények között ne legyen a továbbiakban hozzáférhető. A biztonságos megsemmisítés csak látszólag egyszerű feladat, hiszen az információ sok esetben mentésekben, hordozható eszközökön vagy akár a cloud rendszerekben is megtalálható. Ettől függetlenül törekedni kell arra, hogy a saját hatáskörben levő adathordozókról biztonságos módon kerüljenek eltávolításra a védett információk.

Típusai:

– Ártalmatlanítás: olyan eljárás, amikor az adathordozót egyszerűen kidobják, további törlési eljárások nélkül. Például nyilvános anyagot tartalmazó papírok kidobása.
– Törlés: Ezen a szinten az adathordozóról a törlés után nem lehet adatot visszaállítani hagyományos módszerekkel (például undelete). Általában megoldható egyszeri felülírással.
– Tisztítás: Ezen a szinten az adathordozóról a tisztítás után nem lehet adatot visszaállítani laboratóriumi körülmények között sem. Például lemágnesezés.
– Megsemmisítés: az adathordozó teljes megsemmisítését jelenti. Például bezúzás, elégetés, elolvasztás, szétszedés, darálás.

Konfigurációmenedzsment

Az a folyamat, melynek során a termékek, a környezet és az eljárások követelményeit (különösen a változásukat) menedzselik, így biztosítva a megfelelőséget minden esetben. A konfigurációmenedzsment legfontosabb célja a teljes üzemeltetési folyamat átláthatóságának megteremtése.

A jó konfigurációmenedzsment képes a következőkre:

– Illeszkedjen a változásokhoz.
– Illeszkedjen a szabványokhoz és jógyakorlatokhoz.
– Biztosítsa, hogy minden követelmény világos, lényegre törő és érvényes legyen.
– Biztosítsa a megfelelő kommunikációt.
– Biztosítsa, hogy az eredmények megismételhetők legyenek.

Fenyegetések a konfigurációmenedzsmenttel kapcsolatban:

– Konfigurációmenedzsment hiányában a rendszer bizalmassági, sértetlenségi és rendelkezésre állási tulajdonságai sérülnek.

A konfigurációmenedzsment folyamata az alább felsorolt tevékenységeket tartalmazza.

A konfiguráció nyilvántartása:

– A rendszer elemeiről leltárt kell vezetni.

A konfiguráció bázisának nyilvántartása:

– A bázis az, melyhez a változások után ellenőrzésként vissza lehet térni.

A státusz nyilvántartása:

– Minden tétel aktuális státusza legyen nyilvántartva a múltbeli változásokkal együtt.

A konfiguráció-nyilvántartás kontrollja:

– A nyilvántartás meglétét és konzisztenciáját rendszeresen ellenőrizni kell.

Engedély nélküli szoftverek:

– Egyértelmű szabályok alapján licenszelt szoftvereket kell használni.

A szoftverek tárolása:

– Minden szoftver tárolását meg kell oldani, elválasztva a fejlesztési, tesztelési és élesüzemi fájlokat.

A szoftverekre vonatkozó elszámoltathatóság:

– A szoftvereket azonosítóval kell ellátni, nyilvántartásba kell venni és megfelelő licensszel kell ellátni.

10. Ellenőrzés, auditálás, kockázatelemzés

10.1. Az informatikai rendszerek biztonsági ellenőrzése

10.1.1. Az informatikai biztonsági ellenőrzés célja

„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." [42]

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 [42]:

- az informatikai rendszerek biztonsága megfelel-e a szervezet által elfogadott biztonsági követelményeknek (például KIB 25/28. sz. ajánlás),
- érvényesülnek-e a jogszabályokban, a társasági és a rendszerszintű 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*." [42]

10.1.2. 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." [42]

Az informatikai biztonsági ellenőrzések típusai [42]:

- *informatikai biztonsági vizsgálat* (fenyegetettség, védelmi képesség elemzése 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 [42]:

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

Az ellenőrzések munkaszakaszai [42]:

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

Az ellenőrzések jellegük szerint felosztatók [42]:

- tervezett és rendszeres ellenőrzésekre,
- eseti vizsgálatokra,
- biztonsági esemény kivizsgálásokra.

10.1.3. 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 auditálás**t 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 auditálás**t 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), rendszerszintű 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.” [42]

10.1.4. A szankcionálás

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

A szabályok megsértését általában a következő események merítik ki [42]:

– 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 azt 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.” [42]

Bűncselekményre utaló gyanú vagy körülmény esetén az arra illetékes szervezeti egységgel (általában a jogi vagy a biztonsági 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 szankcionálása lehet munkaügyi vagy büntetőjogi, esetleg polgári jogi (kártérítés). [42]

„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.” [42]

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

– szóbeli megrovás,

– írásbeli figyelmeztetés,
– felfüggesztés,
– elbocsátás.

Az informatikai biztonsági vezető (menedzser) a biztonságsértő eseményekről vezessen folyamatos nyilvántartást, amelyből megállapítható, hogy mikor milyen események történtek, arra hogyan derült fény, mekkora kárt okoztak, kik voltak a felelősök, ki, milyen intézkedéseket foganatosított az esemény kapcsán." [42]

10.2. Az informatikai biztonság ellenőrzési folyamata

10.2.1. Informatikai biztonsági vizsgálat – 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.

Bármilyen kockázatelemzési tevékenység megkezdése előtt a szervezetnek stratégiával kell rendelkeznie az ilyen elemzésekhez, és ennek összetevőit (eljárások, technikák stb.) dokumentálni kell az informatikai biztonságpolitikában. A kockázatelemzési eljárás eszközeit és kritériumait az adott szervezet számára kell megválasztani. A kockázatelemzési stratégiának biztosítania kell, hogy a választott megközelítés alkalmazható az adott környezetre és ott fókuszál a biztonsági erőfeszítésekre, ahol az valóban szükséges."[34]

Részletes kockázatelemzés

„A részletes kockázatelemzés az értéket képező eszközök mélységben történő azonosítását és értékelést, valamint az ezekre irányuló fenyegetések felmérését és a sérülékenységek vizsgálatát jelenti. Ezen tevékenységek eredményeit a kockázatok elemzéséhez, majd a megfelelő biztosítékok kiválasztásához használjuk.

Előnye:

a) valószínűleg minden informatikai rendszer számára megfelelő biztosítékok kerülnek azonosításra,
b) a részletes elemzés eredményei felhasználhatók lesznek az informatikai változások kezelésében.

Hátránya:

a) jelentős időt és erőfeszítést, valamint szakértelmet igényel,
b) fennáll a lehetősége annak, hogy a kritikus rendszerek biztonsági igényei túl későn kerülnek megállapításra, ezért minden informatikai rendszer hasonló részletességű és hosszú idejű vizsgálata szükséges a teljes elemzéshez.

A fenti hátrányok miatt nem ajánlható a részletes kockázatelemzés alkalmazása minden informatikai rendszerre, ha ezt a megközelítést választjuk *a következő lehetséges kivitelezési módok léteznek:*

a) egy standard megközelítés alkalmazása, amely kielégíti a követelményeket,
b) egy standard megközelítés alkalmazása a szervezetnek megfelelő, különböző kockázatmodellező technikák alkalmazása előnyös lehet sok szervezet számára. "[34]

Kombinált megközelítés

„Először magas szintű kockázatelemzést kell végezni minden informatikai rendszerre, minden esetben az informatikai rendszerek szervezet számára jelentett értékére kell összpontosítani és a súlyos kockázatokra, melyeknek ki vannak téve. A szervezet számára fontosként azonosított és/vagy magas kockázatnak kitett informatikai rendszerek esetében részletes kockázatelemzésre van szükség a prioritási sorrend alapján. Minden egyéb informatikai rendszerre az alapszintű megközelítést kell alkalmazni. Ez a megközelítés az előzőek legjobb tulajdonságainak egyesítéseként egy jó egyensúlyt nyújt a biztosítékok azonosításához szükséges idő és erőforrások tekintetében, miközben biztosítja a magas kockázatnak kitett rendszerek megfelelő védelmét.

További előnyök:

a) a kezdeti gyors és egyszerű megközelítés nagy valószínűséggel megkönnyíti a kockázatelemzési program elfogadását,

b) gyorsan fel lehet építeni a stratégiai összképet a szervezet biztonsági programjáról, azaz egy jó tervezési segítséget ad,

c) a követő tevékenységek sokkal eredményesebbek lesznek.

Az egyetlen lehetséges hátrány a következő: mivel a kezdeti kockázatelemzés magas szintű és esetleg kevésbé pontos, néhány rendszer nem biztos, hogy a megfelelő szintű kockázatokkal lesz azonosítva. Ezek a rendszerek az alapszintű módszer szerint lesznek elemezve, bár a későbbiekben újra lehet vizsgálni az alapszintű megközelítés megfelelőségét. "[34]

A magas szintű, részletes kockázatelemzési megközelítés egyesítve az alapszintű megközelítéssel – amennyiben alkalmazható, akkor – a szervezetek többsége számára ajánlott, leghatékonyabb megoldást jelenti.

A kockázatelemzésre számos szabvány és ajánlás létezik.

Az **ISO/IEC 27005:2011** útmutatást ad a biztonsági kockázat kezeléséhez. Az ISO/IEC 27001 célja, hogy segítse az informatikai biztonság kockázatelemzésen alapuló megközelítését. A mintegy 60 oldalas szabvány mindössze 24 oldalas főrészét mellékletekben példák és egyéb információk követik. A szabvány nem nevez meg semmilyen konkrét kockázatelemzési módszert! A szabvány a mennyiségi és minőségi kockázatelemzési módszerek közötti választást is a felhasználóra bízza.

A kockázatelemzés kapcsán a sokat emlegetett **MSZ EN ISO 31000:2015** (Kockázatfelmérés és -kezelés. Alap- és irányelvek), illetve az MSZ EN ISO 31010:2010 (Kockázatkezelés. Kockázatfelmérési eljárások) nem a (biztonsági) kockázatelemzésről, hanem a vállalatirányítási rendszer hatékonyabbá tételét szolgáló kockázatkezelésről szól. Fontos, hogy az ISO 31000 szabvány nem alkalmazható tanúsításra!

A következő részben bemutatott módszertan a KIB 25. számú ajánlásának Informatikai Biztonsági Irányításának Vizsgálata című kötete [43] alapján készült. Az abban leírt kockázatelemzési módszertan a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (továbbiakban: MeH ITB) 8. számú ajánlásán alapul, amely az Egyesült Királyság Központi Számítógép- és Telekommunikációs Ügynökség[83] által kidolgozott CRAMM[84] és a német Szövetségi Információtechnikai Biztonsági Hivatal[85] módszertanainak adaptációja. A kockázatelemzésen alapuló módszer egy olyan modellen nyugszik, amelynek a középpontjában a védendő alapérték, az informatikai rendszerben kezelt adatok által hordozott információk állnak. Ezeket a környezetüket alkotó rendszerelemek veszik körül. A támadások általában nem közvetlenül érik az adatokat, hanem az azokat „körülvevő" rendszerelemeken keresztül.

Valamely informatikai rendszer biztonságának kockázatelemzésen alapuló vizsgálata során elsőként a meglévő, potenciálisan fenyegetett értékeket kell feltérképezni 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 informatika-alkalmazás 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 rendszerelem-csoportokat kell áttekinteni:

Tárgyiasult elemcsoportok:
- környezeti infrastruktúra,
- hardver,
- adathordozók,
- dokumentumok, iratok.

Logikai elemcsoportok:
- szoftver,
- adatok,
- kommunikáció.

Személyi elemcsoport:
- személyzet,
- felhasználók,
- ellenőrök.

[83] Central Computer and Telecommunation Agency – CCTA
[84] CCTA Risk Analysis and Management Method
[85] Bundesamt für Sicherheit in der Informationstechnik

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 **valószínűség**étől és a bekövetkezett **kár nagyság**ától, 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.*

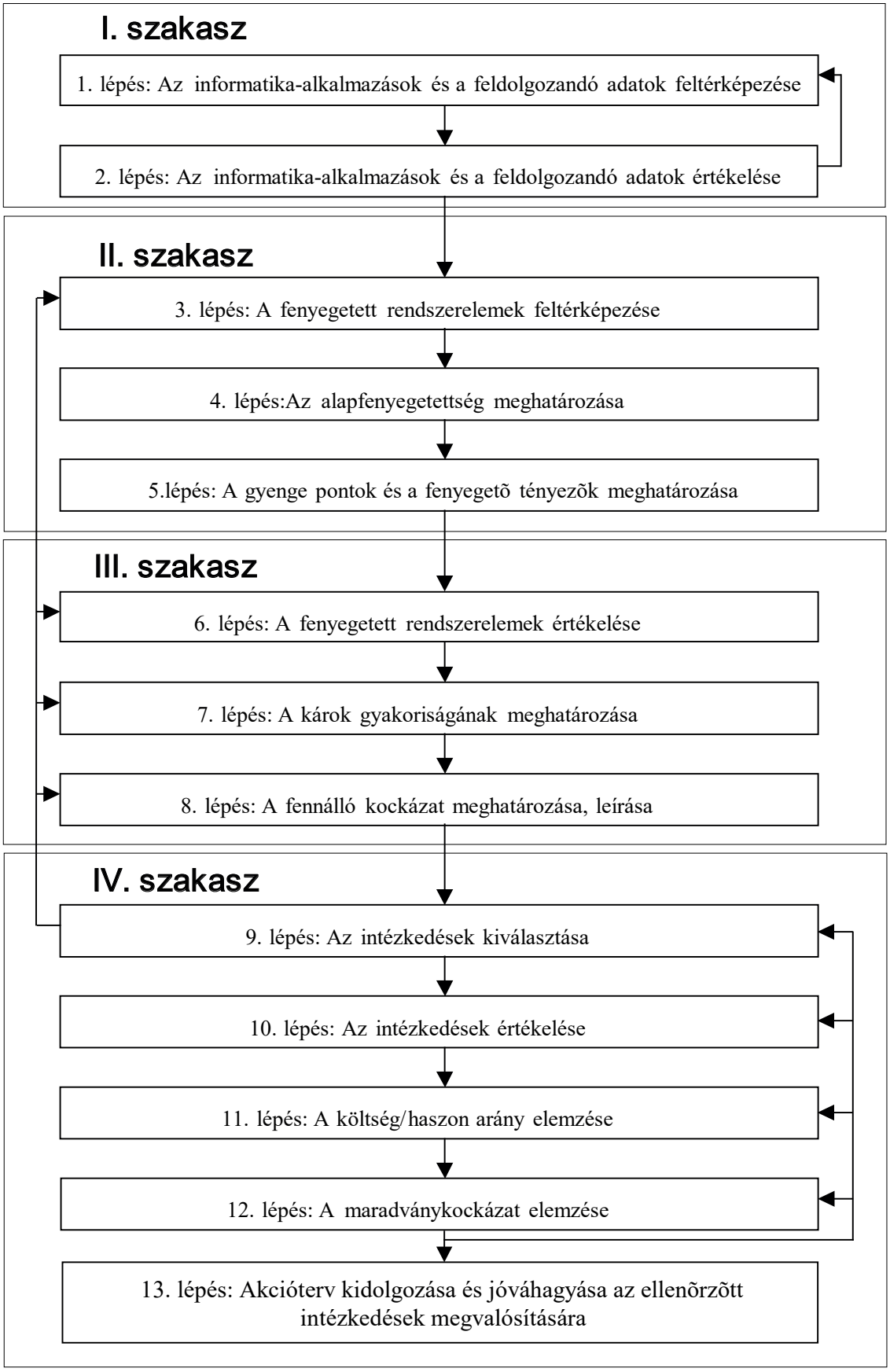
A **biztonsági követelmények** egyenként abból adódnak, hogy kiválasztjuk a túl magas kockázatokat, és ezek alapján meghatározzuk azokat a megfelelő intézkedéseket, amelyek ezeket a kockázatokat elfogadható szintre csökkentik, és a költségek, illetve a haszon szempontjából is igazolhatók.

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 intézkedések**re kell javaslatot tenni, amelyek minimális költségszint mellett maximális kockázatcsökkentést eredményeznek.

Az informatikai biztonsági vizsgálat négy eljárási szakaszra, azon belül pedig 13 lépésre bontható, mint azt a 10. ábra mutatja. Az egyes lépéseket szükség szerint meg kell ismételni.

A kockázatelemzés szakaszainak és lépéseinek részletes leírása



10 ábra Az informatikai biztonsági vizsgálat szakaszai és lépései [43]

10.2.1.1. I. szakasz: a védelmi igény feltárása

A szakasz áttekintése

Az **első szakaszban** ki kell választani és be kell határolni a további vizsgálódások tárgyát. Ehhez meg kell állapítani, hogy értékük alapján mely informatika-alkalmazások 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 informatika-alkalmazások és a feldolgozandó adatok feltérképezése:

1. feladat: Az informatika-alkalmazások feltérképezése;
2. feladat: Igény esetén a különleges szolgáltatások feltérképezése;
3. feladat: Az informatikai rendszerben feldolgozásra kerülő valamennyi adat feltérképezése.

Második lépés: az informatika-alkalmazások és a feldolgozandó adatok értékelése:

1. feladat: A felhasználó védelmi céljainak leírása;
2. feladat: Az ötrészes értékskála rögzítése;
3. feladat: Az értékek hozzárendelése az informatika-alkalmazásokhoz 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 informatika-alkalmazások, 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 informatika-alkalmazást. 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 informatika-alkalmazások értékét egy ötrészes skálán ábrázolhatjuk, mérhetjük fel, amelyek értéktartományát a felhasználónak kell megállapítania. Ezek segítségével lehet azután a károkat durván osztályozni. Az informatika-alkalmazások és adatok értékeléséhez nincs valamiféle egyszerű, általánosan érvényes koncepció. Az értékeket csak maga az alkalmazó állapíthatja meg. Az értékelés során mindenekelőtt saját biztonsági adottságait és követelményeit kell figyelembe venni.

Ha az informatika-alkalmazások 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 vezetésének 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 informatika-alkalmazások csekély értéket képviselnek a szervezet egyéb működéséhez viszonyítva. A nagy értékű informatika-alkalmazások 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 informatika-alkalmazások 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.

10.2.1.2. II. szakasz: fenyegetettségelemzés

A szakasz áttekintése

A **második szakaszban** *kell feltárni mindazon fenyegető tényezőket, amelyek az első szakaszban kiválasztott informatika-alkalmazásokra 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 teljes körűség 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 informatika-alkalmazások 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 informatika-alkalmazások és az információ-feldolgozás megvalósítása függ, illetve 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 rendszerelemeket 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.

10.2.1.3. 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
  • kárnagyság értékekkel,
  • gyakorisági értékekkel és
  • a kockázatok megjelölésével,
– kockázat-áttekintés,
– 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 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 informatika rendszer 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.

10.2.1.4. 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 kockázat-áttekintésbe;
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, majd 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 résztvevők, 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, illetve
- 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.

10.2.2. Az informatikai biztonsági vizsgálati dokumentum tartalmi felépítése

Az informatikai biztonsági vizsgálat (kockázatelemzés) 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. FENYEGETETTSÉGELEMZÉS
   3.1. A fenyegetett rendszerelemek feltárása
   3.1.1. A rendszerelemek feltérképezése
   3.1.1.1. A környezetiinfrastruktúra-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. KOCKÁZATKEZELÉS
5.1. A nem elviselhető kockázatok
5.2. Az informatikai biztonsági intézkedések kidolgozásának szempontjai
5.3. Biztonsági intézkedési javaslatok a kockázatok értékelése alapján
5.3.1. Általános jellegű biztonsági intézkedések
5.3.2. Biztonsági intézkedések a környezeti infrastruktúra védelmében
5.3.3. Biztonsági intézkedések a hardver védelmében
5.3.4. Biztonsági intézkedések az adathordozók védelmében
5.3.5. Biztonsági intézkedések a dokumentumok védelmében
5.3.6. Biztonsági intézkedések a szoftver védelmében
5.3.7. Biztonsági intézkedések az adatok védelmében
5.3.8. Biztonsági intézkedések a kommunikáció védelmében
5.3.9. Biztonsági intézkedések a személyek védelmében
5.4. A társaság egészét érintő, globális intézkedési javaslatok
5.4.1. Általános helyzetkép
5.4.2. Az informatikai biztonság szabályozási hátterének rövid értékelése
5.4.3. Politikai és stratégiai feladatok
5.4.5. Operatív feladatok
5.4.5.1.Globális védelmi intézkedések az informatikai fejlesztés területén
5.4.5.2.Globális védelmi intézkedések az informatikai üzemeltetés területén
5.4.6. Az informatikai biztonság ellenőrzése a szervezetnél
5.4.7. Az informatikai biztonság szervezeti vonatkozásai a szervezetnél
5.5. Akcióterv és költségbecslés a javasolt intézkedésekre
6. ÖSSZEFOGLALÓ
MELLÉKLETEK

10.2.3. 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.

Még a kockázat azonosításakor, mielőtt létrehoznak egy, a kockázat kezelésére szánt biztonsági intézkedést, a szervezet határozza meg a kritériumait annak, hogy az adott kockázat elfogadható-e vagy sem. A kockázatok elfogadhatók, ha például úgy értékelik, hogy a kockázat mértéke csekély vagy a kezelés nem lenne költséghatékony a szervezet számára. Az ilyen kockázatkezelési döntéseket dokumentálni kell, minden azonosított kockázatra vonatkozólag.

A kockázatok kezelésének lehetséges módjai:

a) Megfelelő biztonsági intézkedések alkalmazása a kockázat csökkentésére.
b) A kockázatok tudatos és objektív felvállalása feltéve, hogy azok egyértelműen eleget tesznek a szervezeti politikának és kockázatelfogadási kritériumoknak.

c) A kockázatok elkerülése úgy, hogy a szervezet nem használja azokat a szolgáltatásokat, vagy eljárásokat, ahol az adott kockázatok előfordulnak.
d) Kockázatok áthárítása úgy, hogy a szervezet számára kockázatos szolgáltatásokkal, eljárásokkal kapcsolatos veszélyeket áthárítják más felekre, például a biztosítókra vagy beszállítókra.

A kockázatkezelési intézkedések minden esetben biztosítsák, hogy a kockázatok egy elfogadható szintre csökkenjenek, figyelembe véve a következőket:

a) a nemzeti és nemzetközi jogszabályok és szabályzatok követelményei;
b) szervezeti célok;
c) működési követelmények és előírások;
d) maradványkockázatok mértéke megfelel-e a szervezet követelményeinek és lehetőségeinek.
e) A bevezetés előtt álló kockázatkezelő biztonsági intézkedés minden esetben legyen kockázatarányos, azaz arányos azzal a potenciális kárértékkel, amit a „kivédendő" fenyegetés okozhat.

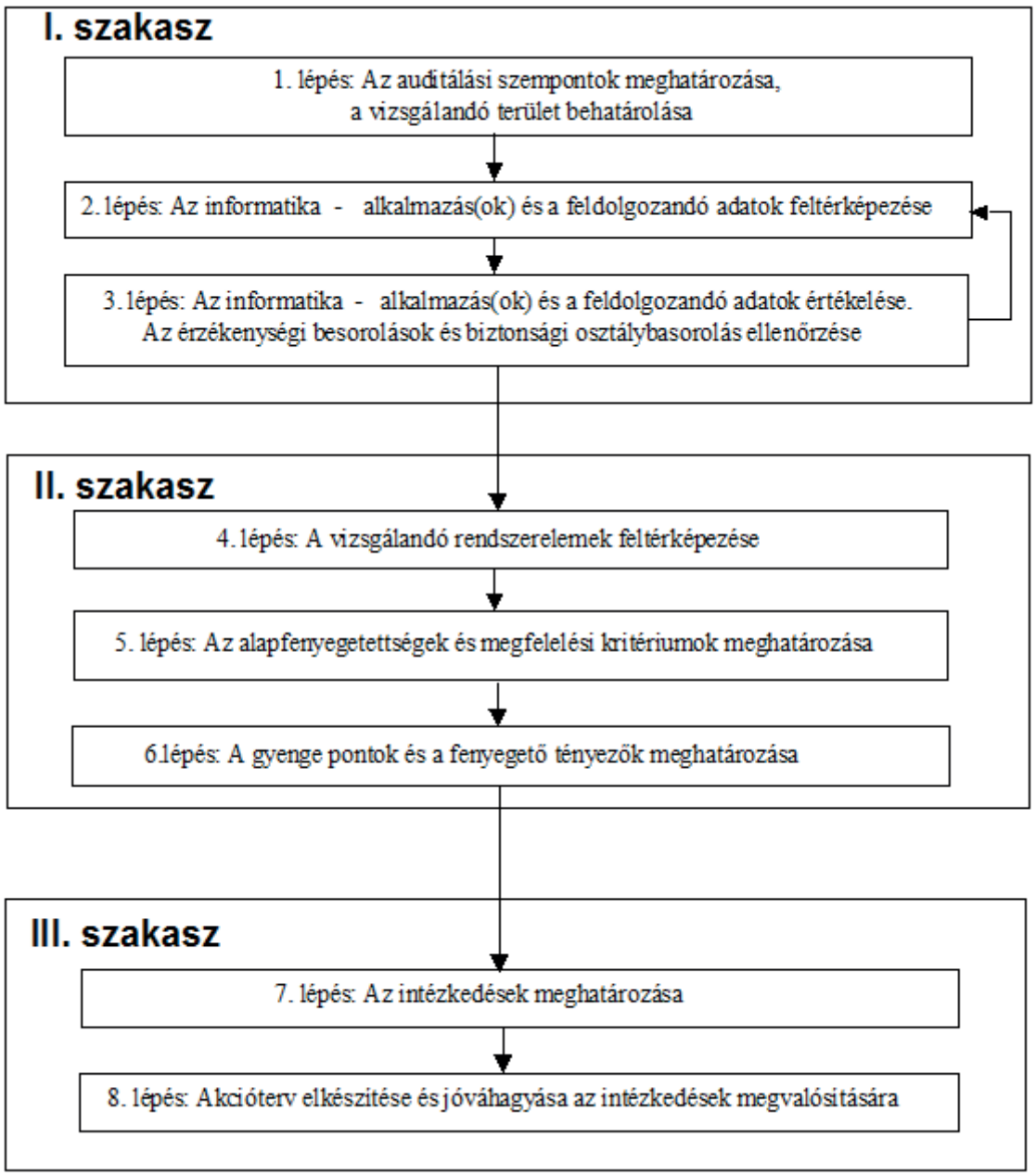
A védelmi intézkedéseket informatikai biztonsági szabványokból vagy ajánlásokból, vagy más intézkedési csoportból is ki lehet választani, vagy akár új speciális intézkedéseket is lehet tervezni, hogy a szervezet meghatározott igényeit kielégítsék.

Mint minden más biztonsági tevékenység, így a kockázatkezelési tevékenység is megfelelő vezetői elkötelezettség és ellenőrzés nélkül nem működik hatékonyan. Kulcskérdés, hogy a kockázatkezelési, informatikai biztonsági intézkedések legyenek összhangban a szervezet működésével és támogassák a szervezeti célokat.

10.2.4. 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). 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 ezeknek való megfelelést vizsgálni. Ez adott esetekben kiegészülhet további követelményekkel, speciális feladatokkal.

Az informatikai biztonsági auditálás során lényegében a kockázatelemzés 11. ábrán bemutatott lépéseit érdemes 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.



11 ábra Az audit lépései [43]

Az előkészítés és a fejlesztés időszakában a kiválasztott fejlesztési módszertan szerint meghatározott fázisokban *tervezett auditálással* kell meggyőződni arról, hogy:

- megvalósultak-e a 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 felhasználó-azonosítás és jogosultságnyilvántartó, valamint az eseményfigyelő-rendszerhez történő csatlakozás,
  - megtörtént-e az üzletmenetfolytonossági- 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 maradványkockázatok 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 rendszerszintű 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 üzletmenetfolytonossági- 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.

10.2.5. Informatikai biztonsági tanúsítás

Az Európai Közösség országaiban elfogadott informatikai biztonsági tanúsítás követelményrendszere informatikai rendszerek esetében az ISO/IEC 27001 vagy eszközök, termékek esetében a Common Criteria. Az informatikai termék, eszköz, vagy rendszer biztonság*ának* tanúsítás*át* engedélyezett, elfogulatlan és független *értékelő által lefolytatott vizsgálat* előzi meg. Az értékelő megvizsgálja, hogy a vizsgált rendszer vagy termék az adott követelményrendszerben meghatározott biztonsági előírásoknak (szintnek) megfelel-e. Az ISO/IEC 27001 esetén az értékelő egyben a tanúsító is. A CC esetében az értékelési eljárás hitelességét független tanúsító vizsgálja, aki ez alapján bocsátja ki a tanúsítást.

11. Informatikai biztonsági fogalmak és definíciók

Adat: Az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas. [12]
A számítástechnikában:
- adat a számítógépes állományok meghatározott része (minden, ami nem program);
- mindaz, amivel a számítógépek működésük során foglalkoznak (ki- és bemeneti, tárolt, feldogozott, továbbított, megsemmisített adat). [44]

Adatállomány: Az informatikai rendszerben logikailag összetartozó, együtt kezelt adatok. [44]

Adatátvitel: Adatok informatikai rendszerek, rendszerelemek közötti továbbítása. [44]

Adatfeldolgozás: Az adatkezeléshez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől. [44]

Adatfeldolgozó: Az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelő részére adatfeldolgozást végez. [44]

Adatgazda: Aki felelős az általa kezelt adatokért, továbbá jogosult minősítés vagy osztályba sorolás elvégzésére. [44]

Adatkezelés: Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása. [45]

Adatkezelő: Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely adatkezelést végez [45]

Adattal rendelkezés:
- a birtokban tartás,
- az adat alapján további adat készítése,
- az adat másolása, sokszorosítása,
- a betekintés engedélyezése,
- a feldolgozás és felhasználás,
- a minősítés (biztonsági osztályba sorolás) felülvizsgálata,
- a minősítés (biztonsági osztályba sorolás) felülbírálata,
- a nyilvánosságra hozatal,
- a titoktartási kötelezettség alóli felmentés,
- megismerési engedély kiadása. [44]

Adattal (információval) szembeni követelmények:
Minőségi (quality) követelmények:
- eredményesség (effectiveness),
- hatékonyság (efficiency).

Bizalmi (fiduciary) követelmények:
- szabályosság (compliance),
- megbízhatóság (reliability).

Biztonsági (security) követelmények:
- bizalmasság (confidentiality),
- sértetlenség (integrity),
- rendelkezésre állás (availability). [46]

Adattovábbítás: Ha az adatot meghatározott harmadik személy számára hozzáférhetővé teszik. [45]

Adattörlés: Az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk nem lehetséges. [44]

Adatvédelem: A személyes adatok védelme. Az adatkezelés során érintett személyek, azok személyiségi jogainak, adataival való önrendelkezési jogának védelme érdekében megvalósítandó/megvalósított, az adatkezelés módjára, formájára, tartalmára vonatkozó szabályozások és eljárások. [44]

Adminisztratív védelem: A védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás. [11]

Akkreditálás: Olyan eljárás, amelynek során egy erre feljogosított testület hivatalos elismerését adja annak, hogy egy szervezet vagy személy felkészült és alkalmas bizonyos tevékenységek elvégzésére. [44]

Alapfenyegetettségek: A fenyegetések általánosított csoportosítása. Alapfenyegetettségek:
- a bizalmasság,
- a sértetlenség,
- a rendelkezésre állás sérülése vagy elvesztése. [44]

Aláírás-létrehozó eszköz: Olyan hardver-, illetve szoftvereszköz, melynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza. [47]

Alkalmazás, alkalmazói program: Olyan program, amelyet az alkalmazó saját igényei, céljai érdekében használ, és amely a hardver és az üzemi rendszer funkcióit használja. [44]

Államtitok: A „szigorúan titkos" minősítésű adat régi megnevezése. Ld. Minősített adat.

Auditálás: Az előírások, elvárások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés. [11]

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. [48]

Behatolási teszt: Az informatikai rendszer, vagy annak elemének olyan ellenőrzése, melynek során megállapíthatóak, hogy vannak-e a gyakorlatban kiaknázható, ismert gyenge pontok. Angolul: Penetration Testing. [44]

Bejelentkezés: Logikai kapcsolat kezdeményezése az operációs rendszerrel vagy egy alkalmazással, amelynek során az azonosítás és – ha szükséges – a hitelesítés eredményesen végrehajtára után az operációs rendszer, illetve az alkalmazás a bejelentkezést végrehajtó számára megengedett funkcióinak használata lehetővé válik. [44]

Betörésdetektáló-eszköz: Olyan rendszer, amely minden észlelt aktivitást valós időben megvizsgálva, egyenként eldönti, hogy az adott aktivitás legális-e vagy sem. Fajtái a mintaalapú betörésdetektáló-eszközök (signatura-based IDS) és a viselkedést vizsgáló betörésdetektáló-eszközök (behavior-based IDS). Angolul: Intrusion Detecting Systems (IDS). [44]

Bizalmasság: Az adat azon tulajdonsága, amely arra vonatkozik, hogy az adatot csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról. [7] Angolul: confidentiality.

Biztonság: A rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. [7]

Biztonsági esemény: Olyan nemkívánt vagy nemvárt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül. Angolul: security incident. [11]

Biztonsági esemény kezelése: Az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység. [11]

Biztonsági mechanizmus: Eljárás, módszer vagy megoldási elv, amely valamilyen biztonsági követelmény(eke)t megvalósít. [44]

Biztonsági osztály: Az elektronikus információs rendszer védelmének elvárt erőssége. [11]

Biztonsági osztályba sorolás: Az elektronikus információs rendszer védelme elvárt erősségének meghatározása a kockázatok alapján. [11]

Biztonsági szint: A szervezet felkészültsége (érettsége) a biztonsági feladatok kezelésére. [11]

Biztonsági szintbe sorolás: A szervezet felkészültségének (érettségének) meghatározása a biztonsági feladatok kezelésére. [11]

Business Continuity Planning (BCP): Ld.Üzletmenetfolytonosság-tervezés.

CA: Certification Authority. Ld. Hitelesítés Szolgáltató.

CIA-elv: A bizalmasság (angolul: confidentiality), a sértetlenség (angolul: integrity) és a rendelkezésre állás (angolul: availability) hármasát szokták az angol kezdőbetűik alapján CIA-elvnek nevezni. [7]

Crack: A programok védelmének „feltörése", kijátszása. A crack eredeti jelentése: valami keménynek (például dióhéjnak) az összeroppantása, feltörése. [44]

Cracker: Az informatikai rendszerbe informatikai eszközöket használva, direkt rombolási céllal betörő személy. Ld. még Hacker. [44]

CRAMM (CCTA Risk Analysis and Management Method): Az Egyesült Királyság Központi Számítógép és Telekommunikációs Ügynöksége (Central Computer and Telecommunication Agency) által kidolgozott kockázatelemzési és -kezelési módszertan. [44]

Csapóajtó: Ld. Rejtett ajtó.

Demilitarizált zóna: Olyan hálózati szegmens, amely szolgáltatásokat nyújt a külső felhasználóknak, de elválasztják a belső, védendő hálózattól. Angolul: Demilitarized Zone (rövidítve: DMZ). [44]

Digitális aláírás: Ld. Elektronikus aláírás.

Disaster Recovery Planning (DRP): Ld. Katasztrófaelhárítás-tervezés.

DDoS (Distributed Denial of Service): Ld. Elosztott szolgáltatásmegtagadás.

Elektronikai hadviselés: Katonai tevékenység, amely az elektromágneses energiát felhasználva meghatározza, felderíti, csökkenti vagy megakadályozza az elektromágneses spektrum ellenfél részéről történő használatát és biztosítja annak a saját oldali hatékony alkalmazását. [49]

Elektronikus aláírás: Az informatikai rendszerben kezelt adathoz csatolt, rejtjelzéssel előállított jelsorozat, amelyet az adat hitelességének és sértetlenségének bizonyítására használható. [47]

Elektronikus dokumentum: Olyan elektronikus eszköz útján értelmezhető adat, mely elektronikus aláírással van ellátva. [47]

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. (Informatikai rendszer) Az elektronikus információs rendszerekhez tartoznak:
- a számítástechnikai rendszerek és hálózatok, ide értve az internet szolgáltatást is;
- a vezetékes, a mobil, a rádiófrekvenciás és műholdas távközlés;
- a vezetékes, a mobil, a rádiófrekvenciás és műholdas műsorszórás;
- a rádiós vagy műholdas navigáció;
- az automatizálási, vezérlési és ellenőrzési rendszerek (SCADA, távmérő, távérzékelő és telemetriai rendszerek stb.);

a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek. [7]

Elektronikus információs rendszer biztonsága: A rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme a rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. (Informatikai biztonság) [7]

Elektronikus információs rendszer elemei: Ld. Rendszerelemek.

Elektronikus információs rendszer védelme: Az elektronikus információs rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának védelme, továbbá a rendszer elemei sértetlenségének és rendelkezésre állásának védelme. (Informatikai védelem) [7]

Elektronikus irat: Olyan elektronikus dokumentum, melynek funkciója szöveg betűkkel való közlése, és a szövegen kívül az olvasó számára érzékelhetően kizárólag olyan egyéb adatokat foglal magába, melyek a szöveggel szorosan összefüggenek, annak azonosítását (például fejléc), illetve könnyebb megértését (például ábra) szolgálják. [47]

Elektronikus kereskedelmi szolgáltatás: Olyan információs társadalommal összefüggő szolgáltatás, amelynek célja áruk, illetőleg szolgáltatások üzletszerű értékesítése, beszerzése, cseréje. [50]

Elektronikus okirat: Olyan elektronikus irat, mely nyilatkozattételt, illetőleg nyilatkozat elfogadását vagy nyilatkozat kötelezőnek elismerését foglalja magában. [47]

Életciklus: Az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam. [11]

Elosztott szolgáltatásmegtagadás: Olyan logikai támadás, amely az informatikai rendszer egy (vagy több) kiszolgálóját tömeges szolgáltatásigénnyel túlterheli, ami a felhasználók hozzáférését nehezíti, vagy akár a kiszolgáló teljes leállásához is vezethet. Angolul: Distributed Denial of Service (rövidítve: DDoS). [44]

Észlelés: A biztonsági esemény bekövetkezésének felismerése. [11]

Fejlesztési környezet: A fejlesztés tárgyának előállítása során érvényesített szervezeti intézkedések, eljárások és szabványok. Angolul: Development Environment. [44]

Fejlesztői biztonság: A fejlesztőnek a fejlesztési környezetére gyakorolt fizikai, eljárási és személyi védelmi szabályozói, biztonsági intézkedései. Angolul: Developer Security. [44]

Felelősségre vonhatóság: Olyan tulajdonság, amely lehetővé teszi, hogy az adott entitás tevékenységei egyértelműen az adott entitásra legyenek visszavezethetők. [44]

Felhasználó: Egy adott elektronikus információs rendszert igénybe vevők köre. [11]

Felhasználói dokumentáció: A fejlesztő által a végfelhasználó részére, a fejlesztés tárgyáról késztett információ. Angolul: User Documentation. [44]

Felhasználói program: Ld. Alkalmazás. [44]

Fenyegetés: Olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemeinek védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát. Angolul: Threat. [11]

Féreg: Olyan program, amely a számítógép hálózaton keresztül, a hálózati funkciók kihasználásával terjed számítógéptől számítógépig és károkozó hatását önmaga – a számítógép összeomlásáig tartó – reprodukálásával, továbbításával éri el. Angolul: Worm. [44]

Fizikai védelem: A fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető-rendszer, a megfigyelő-rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem. [11]

Fokozott biztonságú elektronikus aláírás: Olyan elektronikus aláírás, amely:
a) alkalmas az aláíró azonosítására és egyedülállóan hozzá köthető,
b) olyan eszközzel hozták létre, mely kizárólag az aláíró befolyása alatt áll,
c) a dokumentum tartalmához olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően az iraton, illetve dokumentumon tett – módosítás érzékelhető. [47]

Folytonos védelem: Az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem. [7]

Gyakoriság (Pontosabban: relatív gyakoriság): 0 és 1 közötti érték, amely azt mutatja, hogy valamilyen esemény a kísérletek mekkora hányadában következik be. [44]

Gyenge pont: Az informatikai rendszerelem olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat. [44]

Hacker: Az informatikai rendszerbe informatikai eszközöket használva, kifejezett ártó szándék nélküli betörő személy. A tömegkommunikációban helytelenül minden számítógépes bűnözőre használják. Eredeti jelentése szerint a hacker olyan mesterember, aki fából tárgyakat farag. Ld. Cracker. [44]

Hálózat: Informatikai eszközök közötti adatátvitelt megvalósító logikai és fizikai eszközök összessége. [44]

Hash-függvény: Olyan transzformáció, amely egy tetszőleges hosszú szöveg egyedi, az adott szövegre jellemző fix hosszúságú digitális sűrítményét készíti el. [44]

Hátsó ajt: Ld. Rejtett ajtó. [44]

Hitelesítés-szolgáltató: Olyan mindenki által megbízhatónak tartott, szakosodott szervezet, amely tanúsítványokat adhat ki kliensek és szerverek számára. [47] Elektronikus vagy digitális közjegyzőnek is nevezik.

Hitelesség: Az adat tulajdonsága, amely arra vonatkozik, hogy az adatot bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik. [44]

Hoax: Olyan e-mail, ami valamilyen új – általában fiktív – vírus terjedésére figyelmeztet, és a fertőzés megakadályozása érdekében egy vagy több fájl törlésére ösztönöz (ezek azonban a rendszer működéséhez szükséges, de kevésbé ismert állományok). Az e-mail továbbküldésére is buzdít, hogy a levéláradat – lánclevél – szűkkeresztmetszetet generáljon a hálózaton. [44]

Időbélyegző: Olyan, az elektronikus irathoz, illetve dokumentumhoz végérvényesen hozzárendelt, illetőleg az irattal vagy dokumentummal logikailag összekapcsolt igazolás, amely tartalmazza a bélyegzés időpontját, és amely a dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden – az igazolás kiadását követő – módosítás érzékelhető. [47]

Illetéktelen személy: Valamely legális tevékenység végzésére nem jogosult személy. Az informatikai biztonság esetében tipikusan az objektumba, az informatikai rendszerbe történő belépésre, adatkezelésre nem jogosult személy. [44]

Informatikai biztonság: Ld. Elektronikus információs rendszer biztonsága.

Informatikai biztonságpolitika: A biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása az Ibtv.-ben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok irányítására és támogatására. [11]

Informatikai biztonsági stratégia: Az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere. [11]

Informatikai rendszer: Ld. Elektronikus információs rendszer.

Informatikai rendszer elemei: Ld. Rendszerelemek.

Informatikai védelem : Ld. Elektronikus információs rendszer védelme.

Információ: Bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságot csökkent vagy szüntet meg. [44]

Információs műveletek (információs hadviselés): Hadban álló felek között az információs fölény elérése érdekében végrehajtott, a szemben álló fél információi, információalapú folyamatai, információs rendszerei és számítógépes hálózatai befolyásolására, illetve a saját információk, információalapú folyamatok, információs rendszerek és számítógépes hálózatok védelmére irányuló tevékenységek összessége. [51] Angolul: Information Operation (Information Warfare, röviden: INFOWAR (Nem azonos a kiberműveletekkel!)

Információs önrendelkezési jog: Az egyén joga arra, hogy ellenőrizze vagy befolyásolja azt, hogy ki és milyen vele kapcsolatos adatot kezelhet. [44]

Információs társadalommal összefüggő szolgáltatás: Olyan, elektronikus úton, távollevők részére, rendszerint ellenszolgáltatás fejében nyújtott szolgáltatás, amelyhez a szolgáltatás igénybe vevője egyedileg fér hozzá. [50]

Információvédelem: Az információk bizalmasságának, sértetlenségének és rendelkezésre állásának védelme. [44]

Internet :A TCP/IP-protokollon alapuló, nyilvános, világméretű számítógépes hálózat. Az internet a szolgáltatások széles skáláját nyújtja felhasználóinak (FTP, Gopher, IRC, e-mail, telnet, UUCP, WWW stb.). [44]

Intrusion Detecting System (IDS): Ld. Betörés detektáló eszköz.

Jelszó: Rendszerint karakterfüzérből álló hitelesítési információ, amelyet az azonosított entitás hitelesítésére használnak. Angolul: Password. [44]

Katasztrófaelhárítás-tervezés: Az informatikai rendszer rendelkezésre állásának megszűnése, nagy mértékű csökkenése utáni visszaállításra vonatkozó tervezés [44]

Kibertér: Egy globális tartomány az informatikai környezeten belül, amely tartalmazza az egymással összefüggő informatikai hálózatok infrastruktúráit, beleértve az internetet, a távközlési hálózatokat, a számítógépes rendszereket és beágyazott processzorokat, vezérlőket. [52] (Eredetileg W. Gibson regényéből átvett science-fiction kifejezés, mely a kibernetikus lények birodalma, egy virtuális világ meghatározása. Eszerint a kibertér nem más, mint a hálózatba kötött számítógépek által létrehozott virtuális valóság világa, annak összes objektumával egyetemben.) Angolul: Cyberspace

Kiberműveletek: A kibertér képességek alkalmazása, ahol az elsődleges cél katonai eredmények vagy hatások elérése a kibertérben vagy azon keresztül. (A kiberműveletek nem egyenlőek az információs műveletekkel. Az információs műveleteket el lehet végezni a kibertérben és más területeken egyaránt. A kiberműveletek közvetlenül támogatják az információs műveleteket, és a nem internetes alapú információs műveletek hatással lehetnek a kiberműveletekre.) [53] Angolul: Cyberspace operations, Cyberoperations

Kockázat: A fenyegetettség mértéke, amely valamely fenyegető tényezőből ered, és amelyet a kockázatelemzés során a fenyegető tényezők értékelése révén tárunk fel. A kockázat egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye. [44]

Kockázatelemzés: Az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése. [11]

Kockázatkezelés: Az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása és végrehajtása. [11] Angolul: Risk Management

Kockázattal arányos védelem: Egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel. [44]

Korai figyelmeztetés: Valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni. [11]

Követelmények: A fejlesztési folyamatnak azon szakasza, melyben a fejlesztés tárgyának védelmi célját határozzák meg. Angolul: Requirements. [44]

Közérdekű adat: Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat. [45]

Kriptoanalízis (kriptográfiai bevizsgálás): A rejtjeles üzenetnél az eredeti üzenet visszaállításának illetéktelenek által, azaz eljárás ismerete nélkül, vagy annak részleges ismeretében tett kísérlete. [44]

Kriptográfia: Mindazoknak az eljárásoknak, algoritmusoknak, biztonsági rendszabályoknak kutatását, alkalmazását jelenti, amelyek információnak illetéktelenek előli elrejtését hivatottak megvalósítani. [44]

Kriptológia: A kriptoanalízis és a kriptográfia elméletének és gyakorlatának együttese. [44]

Kritikus infrastruktúrák: Azon létesítmények, eszközök vagy szolgáltatások, amelyek működésképtelenné válása, vagy megsemmisülése a nemzet biztonságát, a nemzetgazdaságot, a közbiztonságot, a közegészségügyet vagy a kormány hatékony működését gyengítené, továbbá azon létesítmények, eszközök és szolgáltatások, amelyek megsemmisülése a nemzeti morált vagy a nemzet biztonságába, a nemzetgazdaságba, vagy a közbiztonságba vetett bizalmat jelentősen csökkentené.[2] A mai magyar jogalkotásban: létfontosságú rendszek és létesítmények

Kritikus információs infrastruktúrák: Azok az infokommunikációs létesítmények, eszközök vagy szolgáltatások, amelyek önmagukban is kritikusinfrastruktúra-elemek, továbbá a kritikus infrastruktúra elemeinek azon infokommunikációs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása vagy megsemmisülése a kritikus infrastruktúrákat vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené. [2] A mai magyar jogalkotásban: létfontosságú információs rendszerelem.

Kulcs: A kriptológiában a rejtjelzés és a megoldás műveleteihez használt szimbólumok sorozata. Az adatbázis-kezelésben egy rekord vagy rekordcsoport azonosítója. A mechanikai védelemben a zárak nyitásához és zárásához használt eszköz. Angolul: Key. [44]

Kulcsmenedzsment: kriptográfiában a rejtjelzés és a megfejtés műveleteihez használt kulcsok előállítása, tárolása, szétosztása, törlése, archiválása és alkalmazása, illetve ezek szabályrendszere. Angolul: Key management. [44]

Különleges adat: A faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat. [47]

Letagadhatatlanság: Valamilyen esemény, tipikusan a kommunikáció során a származás vagy a kézbesítés, megtörténtének garantálása. Angolul: Non-repudiation. [44]

Logikai bomba: Olyan program vagy programrészlet, amely logikailag (funkcionálisan) nem várt hatást fejt ki. Jelentkezése váratlan, hatása pusztító – innen a bomba kifejezés. Angolul: Logic bomb [44]

Logikai védelem: Az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem. [11]

Makrovírus: Olyan dokumentumhoz csatolt (abban tárolt) makrónyelven írt vírus, amely a dokumentumot kezelő és a makrót használni képes alkalmazáshoz kötődik. Hatását a dokumentum használata során fejti ki. [44]

Megelőzés: A fenyegetés hatása bekövetkeztének elkerülése. [11]

Megoldás (desifrírozás): A rejtjeles üzenet legális címzettje által, az eljárás ismeretében az eredeti üzenet visszaállítása. [44]

Megszemélyesítés: Egy entitás (személy, program, folyamat stb.) magát más entitásnak tünteti fel. [44]

Minősítés: Az a döntés, melynek meghozatala során az arra felhatalmazott személy megállapítja, hogy egy adat a tartalmánál fogva a nyilvánosságát korlátozó titokkörbe tartozik. [44]

Minősített adat:

a) nemzeti minősített adat: a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést az e törvényben, valamint az e törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről – a megjelenési formájától függetlenül – a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti (a továbbiakban együtt: károsítja), és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza,

b) külföldi minősített adat: az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza.

Minősítési szintek:

- „Szigorúan titkos!”
- „Titkos!”
- „Bizalmas!” és
- „Korlátozott terjesztésű!” [54]

Minősített elektronikus aláírás: Olyan – fokozott biztonságú – elektronikus aláírás, amely biztonságos aláíráslétrehozó eszközzel készült, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki. [47]

Négy szem elv: Olyan tevékenység, amelyet két személy egymást ellenőrizve végezhet. [44]

Nyilvános Kulcsú Infrastruktúra: A hitelesítésszolgáltatóknak a nemzetközi feltételeket, szabványokat kielégítő, a biztonságos rejtjelzési módszereire, a személyzetre, a fizikai és az informatikai környezetre kiterjedő infrastruktúrája. [44]

Nyilvános kulcsú rendszer: Olyan kriptográfiai rendszer, amelyben a résztvevők két – a használattól függő – kulcsot egy közös algoritmussal használnak rejtjelzésre és a rejtjelzett adatok megoldására, vagy az adatok hitelesítésére (digitális aláírás) és annak ellenőrzésére. A kulcsok egyikét nevükkel együtt nyilvánosságra hozzák (nyilvános kulcs), a másikat titokban tartják (magánkulcs). Az üzenetet küldő a címzett nyilvános kulcsával rejtjelzi, a saját magánkulcsával hitelesíti az adatot (üzenetet), a címzett csak a saját magánkulcsával tudja megoldani a rejtjelzett üzenetet, illetve az aláírt üzenet sértetlenségét (és hitelességét) a küldő nyilvános kulcsával ellenőrizheti. [44]

Nyilvánosságra hozatal: Az adatnak meghatározhatatlan körben, mindenki részére biztosított megismerhetővé, hozzáférhetővé tétele. [44]

PKI (Public Key Infrastructure): Ld. Nyilvános Kulcsú Infrastruktúra. [44]

PGP (Pretty Good Privacy): Philip R. Zimmermann által kifejlesztett, az interneten gyakran használt nyilvános kulcsú kriptográfiai program elektronikus levelek rejtjelzésére és elektronikus aláírására. [44] A PGP kriptográfiai szoftver GPL licenc alatt alternatívája a GNU Privacy Guard (GnuPG or GPG)

Program: A számítógépes utasítások logikailag és funkcionálisan összetartozó sorozata. [44]

Programhiba: A program leírástól (specifikációtól) eltérő működése. [44]

Public Key Cryptosystem: Ld. Nyilvános kulcsú rendszer. [44]

Reagálás :A bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés. [11]

Rejtett ajtó (Csapó ajtó, Hátsó ajtó): Olyan programszegmens, amely a tartalmazó program futtatása során nem dokumentált műveleteket végez illegális, többnyire károkozási célból. Angolul: Backdoor, Trap door. [44]

Rejtjelzés: Nyílt üzenetet kódolása kriptográfiai eljárással, eszközzel vagy módszerrel. A rejtjelzés eredménye a rejtjeles üzenet. [44]

Rendelkezésre állás: Az az elektronikus információs rendszer vagy annak elemének tulajdonsága, amely arra vonatkozik, hogy az (ideértve az abban vagy az által kezelt adatot is) a szükséges időben és időtartamban használható. [11] Angolul: availability

Rendszer: Adott rendeltetésű, egymással kapcsolatban álló eszközök, eljárások, valamint az ezeket kezelő, kiszolgáló és a felhasználó személyek együttese. [11] Angolul: System.

Rendszerelemek:

1. az informatikai rendszer fizikai környezete és a működéséhez szükséges infrastruktúra;
2. hardver;
3. kommunikációs eszközök és hálózat;
4. adathordozók;
5. szoftver;
6. dokumentumok és dokumentáció;
7. személyek. [7]

Az 1–4. elemek az eszközök, az 5–6. az eljárások, míg a 7. az emberek csoportba sorolható. 3E, angolul: 3P (products, procedures, people).

Rendszerprogram (rendszerszoftver): Az operációs rendszer részeként futó programok. [44]

Rendszerterv: A fejlesztési folyamatnak az a szakasza, melyben a fejlesztés tárgyának felső szintű definíciója és terve kerül meghatározásra. Angolul: Architectural Design. [44]

RSA rejtjelzés (RSA encrytion): Ronald Rivest, Adi Shamir és Leonard Adleman 1978-ban szabadalmazott nyilvános kulcsú kriptográfiai algoritmusa. [44]

Sértetlenség: 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), és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanság) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható. [7] Angolul: Integrity.

Sérülékenység: Az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat. [11] Angolul: vulnerability.

Sérülékenységvizsgálat: Az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása. [11]

SET-protokoll (Secure Electronic Transaction protokoll): Az e-üzlet biztonságos elektronikus tranzakciói céljára, kártyakibocsátó és informatikai vállalkozások által közösen kifejlesztett kommunikációs protokoll, amelynek használata a felek közötti rejtett adatátvitelt és a felek biztonságos hitelesítését szolgálja. [44]

SSL (Secure Socket Layer): A Netscape által kifejlesztett nyílt ajánlás (szabvány) biztonságos kommunikációs csatorna létrehozására. [44]

Számítógépes bűnözés: Haszonszerzés vagy károkozás céljából, az informatikai rendszerekben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, illetve a rendszerelemek sértetlensége és rendelkezésre állása elleni bűncselekmények összefoglaló megnevezése. (Az informatikai eszközök felhasználásával elkövetett bűncselekményekre is szokták alkalmazni.) [44]

Szimmetrikus rejtjelző eljárás: A rejtjelzésre és megoldásra egyetlen kulcsot használó rejtjelző eljárás. A megoldó algoritmus nem feltétlenül egy fordított sorrendben végrehajtott rejtjelzés! [44]

Személyes adat: Meghatározott természetes személlyel (az érintettel) kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. [44]

Szoftver: Ld. Program. [44]

Szolgálati titok: A „titkos” minősítésű adat régi megnevezése. Ld. Minősített adat.

Tanúsítás: Egy informatikai biztonsági vizsgálat (értékelés) eredményeit igazoló formális nyilatkozat kibocsátása, melyből kiderül, hogy az értékelési követelményeket, kritériumokat megfelelően alkalmazták. Angolul: Certification. [44]

Támadás: Valamilyen védett érték megszerzése, megsemmisítésére, károkozásra irányuló cselekmény. Támadás alatt nemcsak a személyek, szervezetek által elkövetett támadásokat, de áttételesen a gondatlanságból, nem szándékosan kiváltott veszélyeztetéseket és a környezeti, természeti fenyegetéseket is értjük. A támadás legtöbbször nem közvetlenül éri a védett értéket, hanem a körülményektől függő támadási útvonalon zajlik le. [44]

Teljes körű védelem: Az elektronikus információs rendszer valamennyi elemére kiterjedő védelem. [11]

Termék (eszköz): Egy informatikai hardver és/vagy szoftver, melyet funkcionálisan úgy terveztek meg, hogy alkalmas legyen a használatra, vagy rendszerbe történő beépítésre is. Angolul: Product. [44]

Trójai faló (trójai program): Olyan kártékony program, amelyet alkalmazásnak, játéknak, szolgáltatásnak, vagy más egyéb tevékenység mögé rejtenek, álcáznak. Futtatásakor fejti ki károkozó hatását. Angolul: trojan horse [44]

Üzemeltető: Az a természetes személy, jogi személy, jogi személyiséggel nem rendelkező szervezet, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős. [11]

Üzleti titok: A gazdasági tevékenységhez kapcsolódó minden nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek illetéktelenek által történő megszerzése, hasznosítása, másokkal való közlése vagy nyilvánosságra hozatala a jogosult jogos pénzügyi, gazdasági vagy piaci érdekét sértené vagy veszélyeztetné, feltéve, hogy a titok megőrzésével kapcsolatban a vele jogszerűen rendelkező jogosultat felróhatóság nem terheli. [55]

Üzletmenetfolytonosság-tervezés: Az informatikai rendszer rendelkezésre állásának olyan szinten történő fenntartása, hogy a kiesésből származó károk a szervezet számára még elviselhetőek legyenek. Angolul: Business Continuity Planning (rövidítve: BCP). [44]

Változásmenedzsment: Az informatikai termék vagy rendszer fejlesztési, előállítási vagy karbantartási folyamatai alatt megvalósuló változásokat kezelő rendszer. Angolul: Configuration Control. [44]

Veszély: Ld. Fenyegetés. [44]

Védelmi cél: Az informatikai terméktől vagy rendszertől megkövetelt védettség specifikációja, mely alapul szolgál a biztonsági vizsgálatokhoz. A védelmi cél fogja meghatározni a védelemerősítő funkciókat. Ez fogja továbbá meghatározni a védelmi célkitűzéseket, az ezen célkitűzéseket fenyegető veszélyeket, valamint bármely alkalmazásra kerülő védelmi mechanizmust. Angolul: Security Target. [44]

Védelmi feladatok:
- megelőzés (angolul: prevention) és korai figyelmeztetés (angolul: early warning);
- észlelés (angolul: detection);
- reagálás (angolul: reaction);
- esemény- (angolul: incident management) vagy válságkezelés (angolul: crisis management). [7]

Védelmi mechanizmus: Olyan logikai felépítés vagy algoritmus, amely a termékben egy adott védelemerősítő, vagy a védelem szempontjából fontosnak minősülő funkciót alkalmaz. Angolul: Security Mechanism. [44]

Virtuális Magánhálózat: Olyan logikai hálózat, amelyben a nyilvános hálózat egyes végpontjai biztonságos átviteli csatornán keresztül vannak összekapcsolva, és így a nyilvános hálózaton belül védett kommunikációt valósít meg. Angolul: Virtual Private Network (VPN). [44]

Vírus: Olyan programtörzs, amely a megfertőzött program alkalmazása során másolja, esetleg kis mértékben változtatja (mutálja) önmagát. Valamilyen beépített feltétel bekövetkezésekor többnyire romboló, néha csak figyelmeztető vagy „tréfás" hatású kódja is elindul. Többnyire komoly károkat okoznak, adatot törölnek, formázzák a merevlemezt, vagy az adatállományokat küldik szét e mailban. Angolul: Virus. [44]

Warez-oldal: Olyan internetes oldal, ahonnan illegális szoftvermásolatok – az eredeti másolásvédelmet vagy regisztrációt feltörve, semlegesítve – bárki számára ingyenesen letölthetők. Angolul: Warez-site. [44]

Zárt célú elektronikus információs rendszer: Jogszabályban meghatározott elkülönült nemzetbiztonsági, honvédelmi, rendészeti, igazságszolgáltatási, külügyi feladatokat ellátó elektronikus információs, informatikai vagy hírközlési rendszer. [11]

Zárt védelem: Az összes releváns fenyegetést figyelembe vevő védelem. [7]

12. Irodalom

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

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

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

4. Ameljańczyk, Andrzej (1978): Teoria Gier, WAT, Varsó, WAT wewn. 690/78.

5. 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.

6. Magyar Értelmező Kéziszótár, Akadémiai Kiadó, Budapest, 1978./2003.

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

8. 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.

9. Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation, COM(97) 623, Európai Közösségek Bizottsága, Brüsszel, 1997.12.03. Az Európai Bizottság közleménye: i2010: európai információs társadalom a növekedésért és a foglalkoztatásért, Európai Közösségek Bizottsága, Brüsszel COM(2003) 784, 2005.01.06.

10. Az Európai Bizottság közleménye: i2010: európai információs társadalom a növekedésért és a foglalkoztatásért, Európai Közösségek Bizottsága, Brüsszel COM(2003) 784, 2005.01.06.

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

12. MSZ ISO 2382-1:1994 Információtechnológia. Fogalommeghatározások. 1. rész: Alapfogalmak

13. ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements

14. MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények.

15. Muha Lajos (2009): Infokommunikációs biztonsági stratégia, In: Hadmérnök, IV. évfolyam, 1. szám, Budapest, 214-224. pp.

16. Haig Zsolt – Várhegyi István (2005): Hadviselés az információs hadszíntéren, Zrínyi, Budapest.

17. 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

18. Wiener, Norbert (1948): Cybernetics, or Communication and Control in the Animal and the Machine, MIT Press, Cambridge.

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

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

21. 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről

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

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

24. Muha Lajos: Törvény az elektronikus információbiztonságról, In: ITBN Konferencia, Budapest, 2012.09.25 – 2012.09.26.

25. Szádeczky Tamás (2011): Szabályozott biztonság: Az informatikai biztonság szabályozásának elmélete, gyakorlata és az alkalmazás megkönnyítésére felállított módszertan, PhD értekezés, PTE, Pécs, 2011., 286 p.

26. 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.

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

28. Security within the North Atlantic Treaty Organisation (NATO) – C-M(2002)49

29. Európai Unió Tanácsának Biztonsági Szabályzata (2001/264/EK)

30. Muha Lajos: Az informatikai biztonság mérése, In: Kadocsa László (szerk.): A Dunaújvárosi Főiskola Közleményei XXXI.: A Magyar Tudomány Napja és a Kreativitás és Innováció Európai Év 2009. tiszteletére rendezett interdiszciplináris tudományos Konferenciasorozat előadásai. Dunaújváros, Magyarország, 2009.11.09 – 2009.11.13.

31. 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.)

32. Muha Lajos – Szádeczky Tamás (2014): Irányítási rendszerek, egyetemi jegyzet, Nemzeti Közszolgálati Egyetem, Budapest, 79 p.

33. 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.

34. 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.)

35. Reliable Data Centers Guideline, BITCOM, Berlin-Mitte, 2006.

36. Betöréses lopás- és rablásbiztosítás technikai feltételei (ajánlás), MABISZ, Budapest, 2002. február, Módosítva: Budapest, 2012. március 22.

37. Muha Lajos (2012): Formális biztonsági modellek I.: A diszkrecionális hozzáférés-védelem. In: Hadmérnök, VII. évfolyam, 1. szám, Budapest, 278–284 pp.

38. 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.

39. 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.

40. Vírusvédelmi információs oldal, Veszprog Kft. http://antivirus.hu

41. 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.

42. 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.

43. 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.)

44. Muha Lajos: Fogalmak és definíciók, (2.4. fejezet). In: Muha Lajos (szerk., 2003): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig. Verlag Dashöfer Szakkiadó, Budapest.

45. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

46. Control Objectives for Information and Related Technology (COBIT) v. 4.1, ISACF c IT Governance Institute, Rolling Meadows, 2007.

47. 2001. évi XXXV. törvény az elektronikus aláírásról

48. 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról

49. Allied Joint Doctrine AJP-01(A) Change 1., NATO

50. 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről

51. Field Manual 100–6, Information Operations, USA

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

53. Joint Publication 3-0, Joint Operations, USA

54. 2010. évi CLV. törvény a minősített adatok védelméről

55. 2013. évi V. törvény a Polgári Törvénykönyvről

13. Szabványjegyzék

13.1. De jure szabványok

ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

ISO/IEC 15408-2:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components

ISO/IEC 15408-3:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components

ISO/IEC 18045:2008 Information technology – Security techniques – Methodology for IT security evaluation

ISO/IEC 20000-1:2011 Information technology – Service management – Part 1: Service management system requirements

ISO/IEC 20000-2:2012 Information technology – Service management – Part 2: Code of practice

ISO/IEC TR 20000-3:2012 Information technology – Service management – Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1

ISO/IEC TR 20000-4:2010 Information technology – Service management – Part 4: Process reference model

ISO/IEC TR 20000-5:2013 Information technology – Service management – Part 5: Exemplar implementation plan for ISO/IEC 20000-1

ISO/IEC 27000:2016 – Information technology – Security techniques – Information security management systems – Overview and vocabulary

ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls

ISO/IEC 27003:2017 – Information technology – Security techniques – Information security management system implementation guidance

ISO/IEC 27004:2016 – Information technology – Security techniques – Information security management – Measurement

ISO/IEC 27005:2011 – Information technology – Security techniques – Information security risk management

ISO/IEC 27006:2015 – Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27007:2017 – Information technology – Security techniques – Guidelines for information security management systems auditing

ISO/IEC TR 27008:2011 – Information technology – Security techniques – Guidelines for auditors on information security controls

ISO/IEC 27009:2016 – Information technology – Security techniques – Sector-specific application of ISO/IEC 27001 – Requirements

ISO/IEC 27010:2015 – Information technology – Security techniques – Information security management for inter – sector and inter – organizational communications

ISO/IEC 27011:2016 – Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

ISO/IEC 27013:2015 – Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000 – 1

ISO/IEC 27014:2013 – Information technology – Security techniques – Governance of information security

ISO/IEC TR 27015:2012 – Information technology – Security techniques – Information security management guidelines for financial services

ISO/IEC TR 27016:2014 – Information technology – Security techniques – Information security management – Organizational economics

ISO/IEC 27017:2015 – Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018:2014 – Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC TR 27019:2013 – Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

ISO/IEC 27023:2015 – Information technology – Security techniques – Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002

ISO/IEC 27031:2011 – Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity

ISO/IEC 27032:2012 – Information technology – Security techniques – Guidelines for cybersecurity

ISO/IEC 27033 – 1:2015 – Information technology – Security techniques – Network security – Part 1: Overview and concepts

ISO/IEC 27033 – 2:2012 – Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security

ISO/IEC 27033 – 3:2010 – Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues

ISO/IEC 27033-4:2014 – Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways

ISO/IEC 27033 – 5:2013 – Information technology – Security techniques – Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

ISO/IEC 27033-6:2016 – Information technology – Security techniques – Network security – Part 6: Securing wireless IP network access

ISO/IEC 27034-1:2011 – Information technology – Security techniques – Application security – Part 1: Overview and concepts

ISO/IEC 27034-2:2015 – Information technology – Security techniques – Application security – Part 2: Organization normative framework for application security

ISO/IEC 27034-5:2017 – Information technology – Security techniques – Application security – Part 5: Protocols and application security controls data structure – XML schemas

ISO/IEC 27035:2016 – Information technology – Security techniques – Information security incident management

ISO/IEC 27035:2016-2 – Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response

ISO/IEC 27036-1:2014 – Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts

ISO/IEC 27036-2:2014 – Information technology – Security techniques – Information security for supplier relationships – Part 2: Requirements

ISO/IEC 27036-3:2013 – Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security

ISO/IEC 27036-4:2016 – Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services

ISO/IEC 27037:2012 – Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence

ISO/IEC 27038:2014 – Information technology – Security techniques – Specification for digital redaction

ISO/IEC 27039:2015 – Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems (IDPS)

ISO/IEC 27040:2015 – Information technology – Security techniques – Storage security

ISO/IEC 27041:2015 – Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative methods.

ISO/IEC 27042:2015 – Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence

ISO/IEC 27043:2015 – Information technology – Information technology – Security techniques – Incident investigation principles and processes

ISO/IEC 27050-1:2016 – Information technology – Security techniques – Electronic discovery – Part 1: Overview and concepts

ISO/IEC 27050-3:2017 – Information technology – Security techniques – Electronic discovery – Part 3: Code of Practice for electronic discovery

ISO/IEC 27799:2016 – Health informatics – Information security management in health using ISO/IEC 27002

ISO/TR 13569:2005 Financial services – Information security guidelines

ISO 31000:2018 Risk management – Principles and guidelines

ISO 31010:2009 Risk management –Risk assessment techniques

ISO Guide 73:2009 Risk management vocabulary

MSZ EN 45020:2007 A szabványosítás és az azzal kapcsolatos tevékenységek. Általános szakszótár (ISO/IEC Guide 2:2004)

MSZ EN ISO 27799:2017 Egészségügyi informatika. Az információbiztonság irányítása az egészségügyben az ISO/IEC 27002 alkalmazásával (ISO 27799:2008)

13.2. De facto szabványok, ajánlások, módszertanok

Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1 Release 5, April 2017

Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1 Release 5, April 2017

Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1 Release 5, April 2017

Control Objectives for Information and related Technology (COBIT) 5, ISACA

Information Technology Security Evaluation Criteria (ITSEC)

IT Infrastructure Library (ITIL)

(röv. ITB 8. sz. ajánlás) Informatikai Tárcaközi Bizottság ajánlásai. Informatikai biztonsági módszertani kézikönyv 8. sz. ajánlás. Budapest, 1994

(röv. ITB 12. sz. ajánlás) Informatikai Tárcaközi Bizottság ajánlásai. Informatikai rendszerek biztonsági követelményei 12. sz. ajánlás. Budapest, 1996

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/1. kötet: Magyar Informatikai Biztonsági Keretrendszer (MIBIK) 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/1-1. kötet: Informatikai Biztonsági Irányítási Rendszer (IBIR) 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/1-2. kötet: Informatikai Biztonság Irányítási Követelmények (IBIK) 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/1-3. kötet: Az Informatikai Biztonság Irányításának Vizsgálata (IBIV) 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/2. kötet: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS) 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/2-1. segédlet: MIBÉTS – Modell és Folyamatok 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/2-2. segédlet: MIBÉTS – Útmutató a Megbízók számára 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/2-3. segédlet: MIBÉTS – Útmutató a Fejlesztők számára 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/2-4. segédlet: MIBÉTS – Útmutató Értékelőknek 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/2-5. segédlet: MIBÉTS – Értékelési módszertan 1.0 verzió

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA): 25/3. kötet: Informatikai Biztonsági Iránymutató Kis Szervezeteknek (IBIX) 1.0 verzió

A Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár http://kovetelmenytar.complex.hu/

Trusted Computer Systems Evaluation Criteria (TCSEC)

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

978-615-5870-27-9 (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