AZ INFORMÁCIÓBIZTONSÁG ALAPJAI

Vákát oldal

AZ INFORMÁCIÓBIZTONSÁG ALAPJAI

szerkesztette
Gyaraki Réka

NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL

AZ NKFI ALAPBÓL MEGVALÓSULÓ PROGRAM

Budapest, 2023

A mű A TKP2021-NVA-18 számú projekt az Innovációs és Technológiai Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával, a TKP2021 pályázati program finanszírozásában valósult meg.

Szerzők
Kovács Zoltán
(4, 5, 6, 7, 8. fejezetek)
Muha Lajos
(Előszó, 1, 2, 3 fejezetek)
Sági Gábor
(4,5,6,7 fejezetek)
Tiszolczy Balázs
(9-17. fejezetek)

Szakmai lektor
Gyaraki Réka

TARTALOM

Előszó

Az egyre nagyobb és bonyolultabb információs rendszerekre épül a gazdaság és a társadalom, ezért a biztonságuk megteremtése és fenntartása alapvető feladat.

Az elmúlt évtizedben bekövetkezett kiberbűncselekmények mellett az orosz-ukrán háborúban és az ahhoz kapcsolódó kibertámadások különösen felhívták a figyelmet információk és az azokat kezelő információs rendszerek sebezhetőségére. 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.

„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.”[1]

„Alapvető elvárássá vált, hogy az információs 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 információs 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 információs rendszerek biztonsága érdekében hozott, jól megválasztott védelmi intézkedések segítenek károk megelőzésében, csökkentésében, és a kárfelszámolás meggyorsításában – sikeressé tehetik a szervezetet.”[2]

[1] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, PhD értekezés, ZMNE, Budapest, 2007, 127 p.

[2] Muha Lajos: Az Informatikai Biztonsági Irányítási Rendszer, In: Az Informatika Korszerű Technikái Konferencia, Dunaújváros, 2010.03.05-2010.03.06., pp. 156-164., ISBN:978 963 9915 38 1

1. Az információs rendszerek biztonságának fogalma és tartalma

1.1. Adat és információ

Ahhoz, hogy az információs rendszerekről tárgyaljunk, először magának az információnak a fogalmát kell meghatároznunk. Az információ latin eredetű szó, a jelentése: értesülés, hír, üzenet, tájékoztatás, felvilágosítás.

Az információ keletkezésével, struktúrájával, kezelésével, tárolásával, elérésével és továbbításával, az információ felhasználásával, az információs rendszerekkel foglalkozik az **információelmélet**, amelyet Claude E. Shannon amerikai híradástechnikai mérnök és matematikus alkotott meg.[3] A matematikai információelmélet szerint az információ a hír váratlanságának mértéke, és mint ilyen számmal mérhető. Mértékegysége a bit. Az információ mibenlétéről a kibernetika tudományának megteremtője Norbert Wiener írta le, hogy „*az információ információ, nem anyag vagy energia*”[4].

Természetes, hogy az információ fogalmát az információs társadalomban az egyes tudományágak másként, más szempontok alapján definiálják. Ismeretelméleti megközelítésben az információ olyan ismeret, amely valakinek a tudását megváltoztatja, tehát információ mindaz, ami változást hoz az emberi tudatban, s bizonytalanságot, határozatlanságot oszlat el. A szemantikai információ fogalmán a viselkedést befolyásoló, új ismeretet nyújtó adatok tartalmi jelentését értjük. Az adatok és hírek csupán információhordozók. „Az **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.”[5] és ehhez „az **adat** az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas”[6].

„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)”.[7]

Az alkalmazott eljárástól függetlenül **adatkezelés**nek nevezzük az adatok gyűjtését, felvételét, tárolását, feldolgozását (megváltoztatás, átalakítás, összegzés, elemzés stb.), továbbítását, törlését, hasznosítását (ideértve például a nyilvánosságra hozatalt is), és felhasználásuk megakadályozását, vagyis mindent, amit az adattal meg lehet tenni.

---

[3] Claude E. SHANNON - Warren WEAVER: A kommunikáció matematikai elmélete. Az információelmélet születése és távlatai. 1949. Budapest, 1986.

[4] Wiener, Norbert: Cybernetics, or Communication and Control in the Animal and the Machine, MIT Press, Cambridge, 1948.

[5] MSZ ISO 2382-1:1994 Információtechnológia. Fogalommeghatározások. 1. rész: Alapfogalmak

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

[7] MSZ ISO 2382-1:1994 Információtechnológia. Fogalommeghatározások. 1. rész: Alapfogalmak

Adatfeldolgozás az adatkezeléshez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől. Az információs rendszerben logikailag összetartozó, együtt kezelt adatokat **adatállomány**nak nevezzük. **Adatátvitel** az adatok információs rendszerek, rendszerelemek közötti továbbítása. **Adatgazda** az a személy, aki felelős az általa kezelt adatokért, továbbá jogosult minősítés vagy osztályba sorolás elvégzésére. [8]

1.2. Az információs rendszerek

Napjainkra a magyar nyelvben nagy zavar alakult ki arra nézve, hogy hogyan is nevezzük az adatok kezelésére használt eszközöket. Sokáig számítástechnikai, avagy informatikai eszközöknek neveztük a gépi adatfeldolgozást végző eszközöket és távközlési, angolosan kommunikációs eszközöknek az adatátviteli eszközöket. Az állami és önkormányzati elektronikus információs rendszerek védelméről szól 2013. évi L. törvényben megjelent az elektronikus információs rendszer kifejezés. Mára ezen eszközök között a konvergencia olyan mértékű, hogy a legkülönbözőbb megnevezéseket aggatják rájuk: informatikai és kommunikációs (ang.: IT and communication), infokommunikációs (ang.: infocommunication), ezek rövidítései az ICT és az IKT. A NATO C-M(2002)49-REV1 számú Security Within the North Atlantic Treaty Organization (NATO) című dokumentuma[9] *Communication and Information Systems*, azaz *Kommunikációs és Információs Rendszerek* (röv.: *CIS*) néven nevezi a védendő rendszereket. A 2022-ben frissített ISO/IEC 27001[10] és ISO/IEC 27002[11] szabványok pedig már egyszerűen csak az *information system,* magyarul az ***információs rendszer*** megnevezést használják. Tekintettel arra, hogy ez utóbbi megnevezés minden szempontból a legkényelmesebb a továbbiakban ezt a megnevezést fogjuk használni.

Fontos, hogy összhangban a rendszerelmélettel, valóban rendszerről és ne berendezések, eszközök valamiféle halmazáról beszéljünk. Ludwig von Bertalanffy szerint: „A rendszer egymással kölcsönhatásban álló elemek olyan együttese, amelyre bizonyos

[8] A fenti fogalmakat használja az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény és az állami és önkormányzati szervek elektronikus információbiztonságról szóló 2013. évi L. törvény egyaránt. Ettől szövegezésében egy kicsit eltérő, de azonos jelentésű fogalmakat használ e tárgyban az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (ang.: General Data Protection Regulation, röviden: **GDPR**).

[9] Security within the North Atlantic Treaty Organisation (NATO) – C-M(2002)49-REV1

[10] ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protections – Information security management systems – Requirements

[11] ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information security controls

rendszertörvények alkalmazhatók. Az elem a rendszer olyan része, összetevője, amelyet az egész vizsgálata érdekében célszerű megkülönböztetni."[12] Ezek az elemek:

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 információs rendszerekhez tartoznak:

1. a számítástechnikai rendszerek és hálózatok, ideértve az internet szolgáltatást is;
2. a helyhez kötött, mobil és egyéb rádiófrekvenciás, valamint műholdas elektronikus hírközlési hálózatok, szolgáltatások;
3. a vezetékes, a rádiófrekvenciás és műholdas műsorszórás;
4. a rádiós vagy műholdas navigációs rendszerek;
5. az automatizálási, vezérlési és ellenőrzési rendszerek (vezérlő és adatgyűjtő14, távmérő, távérzékelő és telemetriai rendszerek stb.);
6. a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek.

1.3. A védelem tárgya

Az információbiztonság esetében meg kell határoznunk azt, hogy mire, az információ milyen tulajdonságaira terjed ki a védelemi tevékenység. Az információval szembeni követelményeket az Information Systems Audit and Controll Association (ISACA) nemzetközi szervezet Control Objectives for Information Technologies (COBIT) című kiadványa fogalmazza meg és osztja fel. Az adattal (információval) szembeni követelmények lehetnek[15]:

- Minőségi (ang.: quality) követelmények:
  - eredményesség (ang.: effectiveness),
  - hatékonyság (ang.: efficiency).
- Bizalmi (ang.: fiduciary) követelmények:
  - szabályosság (ang.: compliance),
  - megbízhatóság (ang.: reliability).
- Biztonsági (ang.: security) követelmények:
  - bizalmasság (ang.: confidentiality),
  - sértetlenség (ang.: integrity),
  - rendelkezésre állás (ang.: availability).

Ezek közül a biztonsági követelmények azok, amelyek nemzetközi szinten elfogadott módon a bizalmasság, a sértetlenség és a rendelkezésre állás hármasára osztanak és az angol kezdőbetűik (*Confidentiality, Integrity, Availability*) alapján *CIA-elv*nek szokták nevezni. A Common Criteria szabvány ezen hármas mellett a hitelességet is védendő tuladonságként határozza meg. A NATO C-M(2002)49-REV1 számú Security within the

---

[12] Von Bertalanffy, L.: General System Theory: Foundations, Developments, Applications. New York, Braziller., 1968.

[13] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, In: Bolyai Szemle XVII. 4. szám, Budapest, 2008.

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

[15] Control Objectives for Information and Related Technology (COBIT) v. 4.1, ISACF c IT Governance Institute, Rolling Meadows, 2007

North Atlantic Treaty Organization (NATO) című dokumentumban[16] ugyan a Kommunikációs és Információs Rendszerek esetében a hitelességet és a letagadhatatlanságot is a védendő tulajdonságok közé sorolja.

- **Bizalmasság** az információs rendszer azon tulajdonsága, hogy a benne tárolt[17] adatot, információt csak az arra jogosultak és csak a jogosultságuk szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.[18]
- **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[19]) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanság[20]) is, illetve
  az információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az információs rendszer eleme rendeltetésének megfelelően használható.[21]
- **Rendelkezésre állás** az adat, illetve az információs rendszer elemeinek tulajdonsága, amely arra vonatkozik, hogy az arra jogosultak által a szükséges időben és időtartamra használható."[22]

A sértetlenség esetében a fenti meghatározás kiterjed nem csak az adat tartalmi sértetlenségére, hanem a tulajdonságbéli sértetlenség meghatározásával magába foglalja a *hitelesség* és a *letagadhatatlanság* meghatározására is, így a Common Criteria és a NATO által elvárt követelményekre is kitér,

1.4. 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[23]. Tehát **a védelem tevékenység, amíg a biztonság egy állapot**. Az (amerikai) angol nem tesz különbséget a biztonság és a védelem között, általában

[16] Security within the North Atlantic Treaty Organisation (NATO) – C-M(2002)49-REV1

[17] helyesebb lenne a „kezelt" kifejezés

[18] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, In: Bolyai Szemle XVII. 4. szám, Budapest, 2008.

[19] ang.: authenticity

[20] ang.: non-repudiation

[21] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, In: Bolyai Szemle XVII. 4. szám, Budapest, 2008.

[22] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, In: Bolyai Szemle XVII. 4. szám, Budapest, 2008.

[23] 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.

mindkettőre a security[24] szót használja[25].”[26] 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[27], 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[28] és a védő vesztesége[29] sohasem egyenlítik ki egymást.[30] 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.”[31]

„A biztonság értelmét, tartalmát sokan sokféleképpen magyarázzák. Azt hiszem, hogy *„A biztonság olyan kedvező állapot, amelynek megváltozása nem valószínű, de nem is zárható ki …”* [32] megfogalmazás értelmetlensége magyarázatot nem igényel. A Magyar Értelmező Kéziszótár szerint *„a biztonság veszélytől vagy bántódástól mentes, zavartalan*

---

[24] A biztonságra a safety szót is használja környezet-, munka- és egészségvédelmi dimenzióban.

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

[26] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, PhD értekezés, ZMNE, Budapest, 2007, 127 p.

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

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

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

[30] Ameljańczyk, Andrzej: Teoria Gier, WAT, Varsó, 1978., WAT wewn. 690/78

[31] Muha Lajos: Az informatikai biztonság meghatározása (3.3. fejezet), In: Muha Lajos (szerk.): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig, Budapest: Verlag Dashöfer Szakkiadó, 2004., ISBN:963 9313 12 2

[32] CSÍK B. et al.: Az informatikai biztonság fogalmainak gyűjteménye, BME GTK, Budapest, 2003.

állapot"[33]. 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."[34].

„A fentiek alapján a biztonság a rendszer olyan – az érintett[35] számára kielégítő – állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg."[36]

> **„Teljes körű védelem** alatt azt értjük, hogy a védelmi intézkedések ***a rendszer összes elemére kiterjed***nek.
>
> **Zárt védelem**ről ***az összes releváns fenyegetést figyelembe vevő*** védelem esetén beszélünk.
>
> A **folytonos védelem** az időben változó körülmények és viszonyok ellenére is ***megszakítás nélkül valósul meg***."[37]
>
> „**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.... Ezt az arányt a biztonságpolitika határozza meg, és mint a védelem erősségét is értékelhetjük.

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."[38]

---

[33] Magyar Értelmező Kéziszótár, Akadémiai Kiadó, Budapest, 1978./2003.

[34] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, PhD értekezés, ZMNE, Budapest, 2007, 127 p.

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

[36] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, In: Bolyai Szemle XVII. 4. szám, Budapest, 2008.

[37] Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) 12. számú ajánlása – Bodlaki Ákos-Csernay Andor-Mátyás Péter-Muha Lajos-Papp György-Vadász Dezső: Informatikai Rendszerek Biztonsági Követelményei – Budapest, 1996., 217 p., ISBN:963 03 4264 2

[38] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, PhD értekezés, ZMNE, Budapest, 2007, 127 p.

„A gyakorlatban, sok esetben egy védelmi intézkedésnek a megcélzott rendszerelemen kívül más rendszerelem vonatkozásában is van erősítő vagy gyengítő hatása (pl. 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.”[39]

1.5. Az információs rendszerek biztonsága

Az előzőek alapján az információs rendszerek védelménél a rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint a rendszer elemei sértetlenségének és rendelkezésre állásának megóvása a feladat.

„A biztonság fenti meghatározását elfogadva levezethetjük az információs rendszer biztonságának 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* (pl. a hardver, szoftver, hálózat, személyek, …) keresztül érvényesülnek.”[40]

Ennek figyelembe vételével, a biztonság általános definíciója alapján az információs rendszerek biztonságát a következőképpen határozhatjuk meg: „**Az információs rendszer biztonsága az információs rendszer olyan** – az érintett számára kielégítő mértékű[41] – **állapota, amelyben annak védelme az információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos**.”[42]

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

- az információs rendszer fizikai környezete és infrastruktúrája,

---

[39] Muha, Lajos; Krasznay, Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, Budapest, Magyarország : Nemzeti Közszolgálati Egyetem (NKE) (2014) , ISBN: 9786155491658

[40] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, In: Bolyai Szemle XVII. 4. szám, Budapest, 2008.

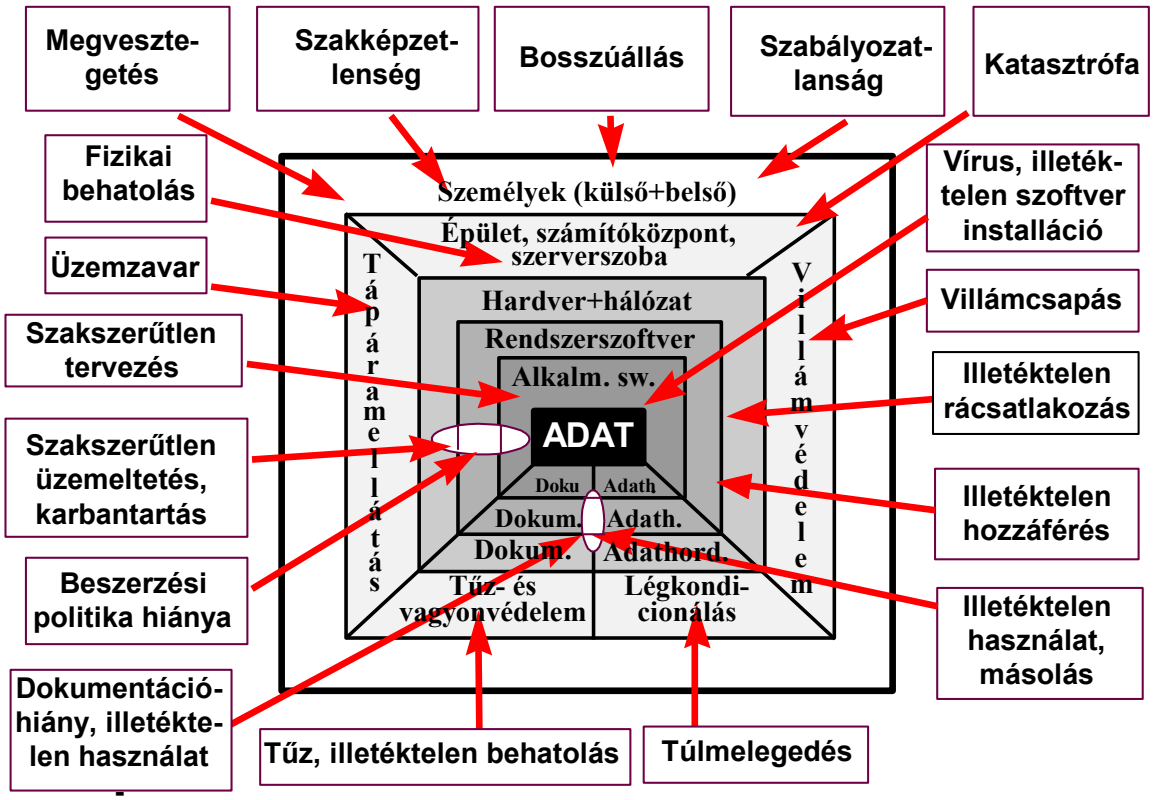
[41] Az érintett alatt a védelem nem kielégítő megvalósítását elszenvedő, a védelmet előíró, továbbá a védelemért felelős személyek és szervezetek együttese értendő. Az „érintett számára kielégítő mértékű” kifejezés a 2013. évi L. törvényben nem szerepel.

[42] Muha Lajos: Az informatikai biztonság egy lehetséges rendszertana, In: Bolyai Szemle XVII. 4. szám, Budapest, 2008.

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



1. ábra Az információs rendszer védelmi modellje[43]

1.6. Kiberbiztonság

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

[43] Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) 12. számú ajánlása – Bodlaki Ákos-Csernay Andor-Mátyás Péter-Muha Lajos-Papp György-Vadász Dezső: Informatikai Rendszerek Biztonsági Követelményei – Budapest, 1996., 217 p., ISBN:963 03 4264 2

A kiber szó magyarázatát a kibernetikával kell kezdeni. A *kibernetika*[44] kifejezést Norbert Wiener (1894–1964) matematikus és filozófus a *kübernétész*, görögül *kormányos* szóból alkotta 1948-ban[45] egy komplex tudományos irányzat megjelölésére, amely a **szabályozás, vezérlés, információfeldolgozás és -továbbítás** általános törvényeit kutatja.

A kiber kifejezés a *kibertér*[46] leegyszerűsítéseként került át a mindennapi szóhasználatba szerte a világon.[47] 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"[48] 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[49] élnek.

Számtalan definíció jelent meg a kibertérről. Számomra a legmeggyőzőbb az USA Védelmi Minisztériuma Katonai és kapcsolódó kifejezések szótárában[50] 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.**"[51]

A c*ybercrime,* magyarul a *kiberbűnözés* egy fontos szakterülete a kiberbiztonságnak. Az Európa Tanács Budapesten, 2001. november 23-án kelt, a 2004. évi LXXIX. törvénnyel kihirdetett nemzetközi *Számítástechnikai Bűnözésről szóló Egyezmény*e[52] (ang.: 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" a *Kiberbűnözésről szóló Egyezmény*ként emlegeti.

A kiberbűnözéshez tartoznak:

---

[44] ang.: cybernetics

[45] Wiener, Norbert: Cybernetics, or Communication and Control in the Animal and the Machine, MIT Press, Cambridge, 1948.

[46] ang.:cyberspace

[47] 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

[48] ang.: meatspace

[49] kibernetikus organizmus (ang.: cybernetic organism, cyborg), azaz gépi és biológiai elemek együttműködése.

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

[51] ang.: „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."

[52] 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről

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

*Kiberterrorizmus*nak a kibertérben elkövetett terrorcselekményeket nevezik.[53]

A több mint egy éve folyó orosz-ukrán háború – sajnos – eklatánsan bemutatja a *hibrid hadviselés*t, ahol a hagyományos és szabálytalan hadviselési taktikák és stratégiák kombinációját jelentik; nem kormányzati szereplőket vonnak be, valamint egyszerű és kifinomult technológiákat használnak. A háború hagyományos formái keverednek a kiberhadviseléssel, a szervezett bűnözéssel, az irreguláris konfliktusokkal, a terrorizmussal. Ez a „szabálytalan háború", amely a hagyományos háború mellett magában foglalja a kiberháborút, és magában foglalja a nukleáris, biológiai és vegyi fegyverek, improvizált robbanóeszközök és információs hadviselés alkalmazását is.

Magyarország Nemzeti Kiberbiztonsági Stratégiája[54] 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". [55]

A Nemzeti Kiberbiztonsági Stratégiában[56] 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.

---

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

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

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

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

2. Hazai és nemzetközi szabványok és ajánlások

Az informatikai biztonság kérdésével számos szabvány és ajánlás foglalkozik. Nemzetközi téren már az 1970-as évek végén megindult (elsősorban az Egyesült Államokban) az informatikai biztonsági értékelés követelményrendszerének kidolgozására vonatkozó tevékenység.

2.1. ISO/IEC 27000 szabványsorozat

Az ISO/IEC 27000 szabványsorozat alapját a Brit Szabványügyi Hivatal[57] által kiadott brit szabvány, a BS 7799 brit szabvány képzi. 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[58] 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 (pl. 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 27xxx-est[59] 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 eredt. Az ISO/IEC nemzetközi szabványügyi szervezetek JTC1 munkabizottság SC27 albizottsága 2022-ben az **Information security, cybersecurity and privacy protection** nevet kapta.

Az ISO/IEC 27xxx szabványsorozat kifejezetten a felhasználók számára nyújt segítséget egy, a teljes szervezetet és minden rendszerelemet átfogó informatikai biztonságmenedzsment rendszer megvalósítására és ellenőrzésére a vonatkozó követelményrendszer kidolgozásával.

Az ISO/IEC:27001 szabvány alapvető célja az Információbiztonsági Irányítási Rendszer[60] (röviden: 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 szervezetre vonatkozó, az összes rendszerelem-csoportot átölelő informatikai biztonsági követelményeket és védelmi

[57] ang.: British Standard Institute, röviden: BSI

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

[59] Mivel a szabványcsalád első tagjának a száma 27000, ezért a szabványcsalád jelölésére a „27xxx” jelölést használom.

[60] Information Security Management System (ISMS)

intézkedéseket tartalmaz a teljes körű informatikai biztonság megteremtéséhez. A de facto nemzetközi szabvánnyá vált ITIL is ezt használja hivatkozási alapként.

Az ISO/IEC 27001[61] és az azt kiegészítő ISO/IEC 27002[62] nemzetközi szabvány többek között azért terjedt el, mert használatával a szervezet bizonyítja az érdekelt feleknek és az ügyfeleknek, hogy elkötelezett az információk biztonságos és biztonságos kezelése iránt. A szabvány előző, 2013-as kiadása óta a kiberbűnözés egyre súlyosabbá és kifinomultabbá válik, nő a kibertámadások száma és érezhetően folytatódni fog ez a növekedés. A globális kiberbiztonsági kihívások kezelése érdekében 2022. februárban megjelent az új ISO/IEC 27002, majd 2022. október 25-én az új ISO/IEC 27001 szabvány is. Melyek a legfontosabb változások ezekben a szabványokban?

Amig korábban az ISO/IEC 27xxx szabványsorozat az informatikai biztonság (Information technology – Security techniques) területén adott támogatást a felhasználóknak, addig 2022-től már új megközelítésben és ehhez igazított új címmel jelennek meg a sorozat szabványai. Az új cím: *Információbiztonság, kiberbiztonság és a magánéletvédelme* (*Information security, cybersecurity and privacy protection*).

Az ISO/IEC 27001:2022[63] szabvány kimondja, hogy a gyorsan változó környezetben a kiberbiztonsági kihívások kezelése érdekében a szervezeteknek fokozniuk kell ellenállóképességüket, és erőfeszítéseket kell tenniük a kiberfenyegetések mérséklésére és a vezetőknek stratégiai megközelítést kell alkalmazniuk a kiberkockázatokkal kapcsolatban. A szabvány holisztikus megközelítése azt jelenti, hogy az egész szervezetet, a személyeket, a technológiát és a folyamatokat is lefedi, nem csak az informatikát. Olyan alapelvek, mint a bizalmasság, sértetlenség és rendelkezésre állás kockázatarányos védelme változatlanul megmaradtak, de ezt az új szabvány kiterjeszti a papíralapú és felhőalapú adatkezelésre is. Ehhez kiegészítő, szektor-specifikus szabványok is vannak, úgymint az ISO/IEC 27016 a felhőszolgáltatásokhoz, az ISO/IEC 27701 a magánéletvédelméhez, az ISO/IEC 27011 a telekommunikációs szervezeteknek és az ISO/IEC 27799 az egészségügyhöz. A fő célkitűzések közé tartozik a **kibertámadásokkal szembeni ellenállóképesség**, a **kiberreziliencia** növelése. A szabvány szerint a kiberrezilienciát alkalmazó szervezetek gyorsan vezető szerepet töltenek be iparágukban.

A szabvány kimondja, hogy a szervezetnek meg kell határoznia és alkalmaznia kell egy információbiztonsági kockázatkezelési folyamatot, melynek során kiválasztja a megfelelő információbiztonsági kockázatkezelési lehetőségeket, figyelembe véve a kockázatértékelés eredményeit és meghatározza az összes intézkedést, amely a választott információbiztonsági kockázatkezelési lehetőség(ek) megvalósításához szükséges. Az intézkedések elsődleges forrása hagyományosan a szabvány A mellékletében felsorolt információbiztonsági intézkedések az ISO/IEC 27002:2022 szabványból származnak. Számomra meglepő, hogy a kockázatkezelés esetében nem az ISO/IEC 27005, hanem az ISO 31000 szabványban meghatározott információbiztonsági kockázatértékelési és kezelési irányelvekre hivatkozik a szabvány.

---

[61] ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protections – Information security management systems – Requirements

[62] ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information security controls

[63] ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protections – Information security management systems – Requirements

Az ISO/IEC 27002:2022 szabvány a korábbi 18 fejezet helyett már csak 8 fejezetből áll, amelyekből korábban is, most is, az első 4 magára erre a szabványra vonatkozik, amelyekkel itt és most nem foglalkozom. A 123 oldalon megadott 4 tartalmi fejezet a következő – nem meglepő – címet viseli:

5. fejezet – Adminisztratív védelem (Organizational controls)
6. fejezet – Személyi védelem (People controls)
7. fejezet – Fizikai védelem (Physical controls)
8. fejezet – Logikai védelem (Technological controls)

Az 5. fejezet 37 pontban írja le a megvalósítandó adminisztratív védelmi intézkedéseket. Ezek közül teljesen új az 5.7 *Fenyegetések felderítése*, az 5.23 *Információbiztonság a felhőszolgáltatások használatához* és az 5.30 *IKT felkészültség az üzletmenet folytonosságára*. Ez utóbbi személy szerint azért szimpatikus, mert egyértelművé teszi régi rögeszmémet, miszerint az üzletmenetfolytonosság biztosítása fontos kérdés, de ez nem az információbiztonsághoz tartozik. A személyi védelme kapcsán nincs új pont, és a fizikai védelem területén is csak a fizikai biztonság monitorozása jelenik meg új intézkedésként. A logikai védelemhez 37 intézkedés tartozik, közölük új a 8.9 *Konfigurációkezelés*, a 8.10 *Információ törlése*, az 8.11 *Adatmaszkolás*, az 8.12 *Adatszivárgás megelőzése*, a 8.16 *Monitoring tevékenységek*, a 8.23 *Webszűrés* és végül, de nem utolsó sorban a 8.28 *Biztonságos kódolás*. Ez utóbbit remélem számon fogják kérni a fejlesztőktől.[64]

Az egyes intézkedésekhez (alfejezetekhez) attribútumok is tartoznak a jobb áttekinthetőség kedvéért. Ezek használatát a 27002:2022 szabvány A melléklete mutatja be. A felhasználat vezérlőelemek a következők:

- szabályozási típus;
- információbiztonsági követelmények;
- kiberbiztonsági feladatok;
- működési képességek;
- biztonsági tartományok.

A Kiberbiztonsági feladatok attribútummal a vezérlőelemeket az ISO/IEC TS 27110 szabványban leírt kiberbiztonsági keretrendszerben meghatározott kiberbiztonsági koncepciókhoz való társítás szempontjából tekintheti át.

A szabvány B mellékletében található az ISO/IEC 27002:2022 megfeleltetése az ISO/IEC 27002:2013 szabványnak és az ISO/IEC 27002:2013 megfeleltetése az ISO/IEC 27002:2022 szabványnak.

A szabványcsalád jelenleg 216 publikált és 72 fejlesztés alatt álló szabványból áll A 2022 elött kiadott elemek már kiadott elemek az *Information technology – Security techniques* főcímet viselik, míg a 2022 utána kiadottak főcíme az ***Information security, cybersecurity and privacy protection***:

- ISO/IEC 27000:2018 – Information security management systems – Overview and vocabulary
- **ISO/IEC 27001:2022 – Information security management systems – Requirements**

[64] Muha Lajos: Egy szabvány változásai, Cyberblog, https://www.ludovika.hu/blogok/cyberblog/2022/11/29/egy-szabvany-valtozasai/, 2022.

- **ISO/IEC 27002:2022 – Information security controls**
- ISO/IEC 27003:2017 – *ISMS* implementation guidance
- ISO/IEC 27004:2016 – Information security management – Measurement
- ISO/IEC 27005:2018 – Information security risk management
- ISO/IEC 27006:2015 – Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007:2017 – Guidelines for information security management systems auditing
- ISO/IEC TR 27008:2019 – Guidelines for auditors on information security controls
- ISO/IEC 27009:2016 – Sector specific application of ISO/IEC 27002
- ISO/IEC 27010:2015 – Information security management for inter – sector and inter – organizational communications
- ISO/IEC 27011:2016 – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013:2015 – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC 27014:2013 – Governance of information security
- ISO/IEC TR 27015:2012 – Information security management guidelines for financial services
- ISO/IEC TR 27016:2014 – Information security management – Organizational economics
- ISO/IEC 27017:2015 –Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2019 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC TR 27019:2017 – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
- ISO/IEC 27023:2015 – Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002
- ISO/IEC 27031:2011 – Guidelines for information and communication technology readiness for business continuity
- **ISO/IEC 27032:2022 – Cybersecurity – Guidelines for internet security**
- ISO/IEC 27033-1:2015 – Network security – Part 1: Overview and concepts
- ISO/IEC 27033-2:2012 – Network security – Part 2: Guidelines for the design and implementation of network security
- ISO/IEC 27033-3:2010 – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues
- ISO/IEC 27033-4:2014 – Network security – Part 4: Securing communications between networks using security gateways
- ISO/IEC 27033-5:2013 – Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
- ISO/IEC 27033-6:2016 –Network security -- Part 6: Securing wireless IP network access
- ISO/IEC 27034-1:2011 – Application security – Part 1: Overview and concepts

- ISO/IEC 27034-2:2015 – Application security – Part 2: Organization normative framework for application security
- ISO/IEC 27034-5:2017 – Application security – Part 5: Protocols and application security controls data structure - XML schemas
- ISO/IEC 27035:2016 – Information security incident management
- ISO/IEC 27035:2016-2 – Information security incident management -- Part 2: Guidelines to plan and prepare for incident response
- ISO/IEC 27036-1:2014 – Information security for supplier relationships – Part 1: Overview and concepts
- ISO/IEC 27036-2:2014 – Information security for supplier relationships – Part 2: Requirements
- ISO/IEC 27036-3:2013 – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security.
- ISO/IEC 27036-4:2016 – Information security for supplier relationships – Part 4: Guidelines for security of cloud services.
- ISO/IEC 27037:2012 – Guidelines for identification, collection, acquisition and preservation of digital evidence
- ISO/IEC 27038:2014 – Specification for digital redaction
- ISO/IEC 27039:2015 – Selection, deployment and operations of intrusion detection systems (IDPS)
- ISO/IEC 27040:2015 – Storage security – Please contact us to buy your copy
- ISO/IEC 27041:2015 – Guidance on assuring suitability and adequacy of incident investigative methods
- ISO/IEC 27042:2015 – Guidelines for the analysis and interpretation of digital evidence
- ISO/IEC 27043:2015 – Security techniques – Incident investigation principles and processes
- ISO/IEC 27050-1:2016 – Electronic discovery -- Part 1: Overview and concepts.
- ISO/IEC 27050-3:2017 – 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

2.2. Az információbiztonsági irányítási rendszer

Egy információs 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 információs rendszer esetén az adott feladat teljesítésére indított projekt keretében kell megvalósulnia.

Az információs rendszerekben kezelt információk biztonsága a sikeres tevékenység egyik alapfeltétele. Az információs rendszerek biztonsági intézkedések megvalósítása nem csak költséget jelent a szervezet számára, hanem segítenek károk megelőzésében, csökkentésében, a kárfelszámolás meggyorsításában, elkerülésében, hanem sikeressé tehetik a szervezetet.

Az ISO/IEC 27001 szabványban meghatározott Információbiztonsági Irányítási Rendszer 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.

„Az IBIR létrehozása és működtetése ugyanolyan megközelítést igényel, mint sok más irányítási rendszer. Az ISO 27001-es szabvány erre a célra az OECD[65] által is támogatott PDCA, magyarul TVEB[66] folyamatmodell használatát vezette be az Információbiztonsági 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.”[67]

A TVEB modell négy szakaszból áll[68]:

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.

---

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

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

[67] Muha Lajos: Az Informatikai Biztonsági Irányítási Rendszer, In: Az Informatika Korszerű Technikái Konferencia, Dunaújváros, 2010.03.05-2010.03.06., pp. 156-164., ISBN:978 963 9915 38 1

[68] 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.

2.3. 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)[69].

„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).”[70]

A CC három részből áll:

1. Bevezetés és általános modell[71]
2. A biztonság funkcionális követelményei[72]
3. A biztonság garanciális követelményei[73]

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.

---

[69] 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.

[70] Szádeczky Tamás: Információbiztonsági szabványok, egyetemi jegyzet, Nemzeti Közszolgálati Egyetem, Budapest, 2014., 50 p.

[71] ang: Introduction and general model

[72] ang: Security functional requirements

[73] ang: Security assurance requirements

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 hozzáférésjogosultság-rendszer szerepkörökön alapul.
- Különböző tűzfalak védelmi profiljai:
  - Hálózati/szállítási szinten működtetett csomagszűrő tűzfal
  - Application Gateway tűzfal
  - USA Kormányzati tűzfal

A CC funkcionális követelményrendszere gyakorlatilag egy funkcionális komponenskatalógus, amelyből összeállítható a vizsgált rendszerre (*Target of Evaluation, TO*E) 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”.

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

EAL1: Funkcionálisan tesztelt:

Minimális – gazdaságossági megfontolásokkal indokolható – védelmi szint, csak a legnyilvánvalóbb hibákat detektálja a lehető legkisebb költséggel. Kicsi az esélye annak, hogy a rejtett gyengeségek kiderüljenek.

EAL2: Strukturálisan tesztelt:

A létező szabványok megfelelő alkalmazásával, kellő odafigyeléssel minimálisan növelt 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.

2.4. A NIST kiadványai

A NIST (National Institute of Standards and Technology[74]) 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.

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.

A ***NIST SP 800-53 Rev4.*** (*Security and Privacy Controls for Information Systems and Organizations*) volt 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 szóló a 41/2015. (VII. 15.) BM rendelet alapja. *2020-ban kiadták a NIST SP 800-53 Rev5.*-t.

[74] Nemzeti Szabványügyi és Technológiai Intézet

3. A védelem megvalósítása

A védelem megvalósítása nem csupán egy eszközrendszer megvalósítását, hanem egy szervezet teljes, azaz az adminisztratív, a személyi, a fizikai és a logikai védelmi rendszerére vonatkozóan a tervezéstől a megvalósításig terjedő folyamatát jelenti

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.[75]

3.1. Adminisztratív védelem

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.[76]

Az adminisztratív védelem során az ISO/IEC 27001 szabvány elvárásai szerint szabályozni kell a következő területeket:

1. Információbiztonsági szabályzat
2. Információbiztonsági szerepkörök és felelősségek
3. A feladatok elkülönítése
4. Vezetői felelősségek
5. Kapcsolatfelvétel a hatóságokkal
6. Kapcsolattartás speciális érdekcsoportokkal
7. Fenyegetések felderítése
8. Információbiztonság a projektmenedzsmentben
9. Az információk és egyéb kapcsolódó eszközök leltározása
10. Az információk és egyéb kapcsolódó eszközök elfogadható felhasználása
11. Eszközök megtérülése
12. Az információk osztályozása
13. Az információk címkézése
14. Információátvitel
15. Hozzáférés-vezérlés
16. Identitáskezelés
17. Hitelesítési információk
18. Hozzáférési jogok
19. Információbiztonság a szállítói kapcsolatokban
20. Az információbiztonság kezelése a szállítói szerződéseken belül

[75] Muha, Lajos; Krasznay, Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, Budapest, Magyarország : Nemzeti Közszolgálati Egyetem (NKE) (2014) , ISBN: 9786155491658

[76] Muha Lajos, Bodlaki Ákos: Az informatikai biztonság, Budapest: PRO-SEC KFT, 2007. 176 p., ISBN:963 86022 6 0

21. Az információbiztonság kezelése az IKT-ellátási láncban
22. A beszállítói szolgáltatások nyomon követése, felülvizsgálata és változáskezelése
23. Információbiztonság a felhőszolgáltatások használatához
24. Információbiztonsági incidensek kezelésének tervezése és előkészítése
25. Információbiztonsági események értékelése és döntéshozatala
26. Reagálás információbiztonsági incidensekre
27. Tanulás az információbiztonsági incidensekből
28. Bizonyítékgyűjtés
29. Információbiztonság zavar esetén
30. IKT felkészültség az üzletmenet folytonosságára
31. Jogi, törvényi, szabályozási és szerződéses követelmények
32. Szellemi tulajdonjogok
33. Nyilvántartások védelme
34. A személyes és a személyazonosításra alkalmas (PII) adatok védelme
35. Az információbiztonság független felülvizsgálata
36. Az információbiztonsági irányelveknek, szabályoknak és szabványoknak való megfelelés
37. Dokumentált működési eljárások

Az adminisztratív védelem alapja az *információbiztonsági politika*. Ennek az irányelvnek az a szerepe, hogy a szervezet teljes egészére vonatkozóan, egységes szemlélettel megfogalmazza azt a vezetői akaratot, amely meghatározza minden munkatárs viszonyát az információs 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 stabilok maradjanak. Az információbiztonsági politikának meg kell fogalmaznia egy olyan tájékoztatási politikát is, amely biztosítja a megfelelő külső és belső tájékoztatást.

Ahhoz, hogy bármilyen szabályozás elkészíthető legyen néhány alapkérdést kell tisztázni. Ezek a következők[77]:

- 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 információs 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 információs 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 információs rendszerét biztonsági osztályba kell

[77] Muha Lajos, Bodlaki Ákos: Az informatikai biztonság, Budapest: PRO-SEC KFT, 2007. 176 p., ISBN:963 86022 6 0

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.

Ahhoz, hogy a szabályozási folyamat megfelelően működjön, a következő feltételek szükségesek[78]:

- 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 információbiztonsági szabályozására is – érvényesek.

Az Információbiztonsági 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 Információbiztonsági 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.[79]

A folytonosság követelménye azt jelenti, hogy az Információbiztonsági Szabályzatnak át kell fognia az információs rendszer teljes életciklusát, azaz az előkészítés, a tervezés, a megvalósítás, az üzemeltetés fázisait egészen a kivonásig/rekonstrukcióig.[80]

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

---

[78] Muha Lajos, Bodlaki Ákos: Az informatikai biztonság, Budapest: PRO-SEC KFT, 2007. 176 p., ISBN:963 86022 6 0

[79] Muha Lajos, Bodlaki Ákos: Az informatikai biztonság, Budapest: PRO-SEC KFT, 2007. 176 p., ISBN:963 86022 6 0

[80] Muha Lajos, Bodlaki Ákos: Az informatikai biztonság, Budapest: PRO-SEC KFT, 2007. 176 p., ISBN:963 86022 6 0

Érvényesítés az információs rendszer teljes életciklusában[81]:

- Minden információs rendszer-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 információs rendszerek megvalósítási projektje szerves része legyen a biztonsági rendszer tervezése és megvalósítása. Információs 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 információs 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.

A **dokumentumkezelés** az információbiztonság szempontjából fontos terület, amelynek biztosítani kell, hogy a dokumentumok útja pontosan követhető, ellenőrizhető és visszakereshető legyen, amely támogatja a szervezet tevékenységének hatékonyságát, ellenőrizhetőségét és a dokumentumok, iratok épségben, illetve használható állapotban való megőrzését.[82]

„Az informatikai rendszerek megbízható működése területén meghatározó tényező az **üzletmenet-folytonosság** (Business Continuity Planning, röviden: BCP) biztosítása. Alapvető célja az, hogy a szervezetnek az üzleti folyamatait támogató informatikai erőforrásai a rendelkezésre álló üzemidőben a lehető legjobb időkihasználással és a legmagasabb funkcionalitási szinten működjenek – figyelembe véve az üzemzavari és katasztrófaesemények széles skáláját – annak érdekében, hogy az üzleti folyamatok zavara által okozott közvetlen és közvetett károk minimálisak legyenek.”[83]

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 szoftver-összetevőinek 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

---

[81] Muha Lajos, Bodlaki Ákos: Az informatikai biztonság, Budapest: PRO-SEC KFT, 2007. 176 p., ISBN:963 86022 6 0

[82] Muha, Lajos; Krasznay, Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, Budapest, Magyarország : Nemzeti Közszolgálati Egyetem (NKE) (2014) , ISBN: 9786155491658

[83] Muha Lajos, Bodlaki Ákos: Az informatikai biztonság, Budapest: PRO-SEC KFT, 2007. 176 p., ISBN:963 86022 6 0

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[84]) 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.[85]

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."[86]

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

---

[84] 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.

[85] Muha Lajos, Bodlaki Ákos: Az informatikai biztonság, Budapest: PRO-SEC KFT, 2007. 176 p., ISBN:963 86022 6 0

[86] Muha Lajos, Bodlaki Ákos: Az informatikai biztonság, Budapest: PRO-SEC KFT, 2007. 176 p., ISBN:963 86022 6 0

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.

3.2. Személyi biztonság

Az információs 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.[87]:

- Az ember kreatív intelligenciával rendelkezik, amit a legerőteljesebben azzal jellemezhetünk, hogy az ember a meglévő információs bázisára támaszkodva minőségileg új ismereteket, új összefüggéseket tud alkotni. 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 motiváltságát, saját belső meggyőződését, valamint a szervezet iránti lojalitását. Végső soron azonban mindig ő dönt arról, hogy ezeket a környezeti befolyásokat magáévá teszi vagy sem. Ez fogja alapvetően meghatározni a célokkal való azonosulását és a normakövetési hajlandóságát.
- Az ember érzelmi lény. Cselekedeteit és így a normakövetési hajlandóságát sok esetben alapvetően befolyásolják pillanatnyi érzelmei, ennélfogva – ellentétben a műszaki rendszerekkel – várható cselekedetei nem jósolhatók meg minden esetben logikusan és racionálisan.

A személyi védelem során az ISO/IEC 27001 szabvány elvárásai szerint szabályozni kell a következő területeket:

1. Szűrés
2. A foglalkoztatás feltételei
3. Információbiztonsági tudatosság, oktatás és képzés
4. Fegyelmi eljárás
5. Felelősségek a munkaviszony megszűnése vagy megváltozása után
6. Titoktartási vagy titoktartási megállapodások
7. Távmunka
8. Információbiztonsági események jelentése

[87] Komor Levente, Nagy Béla: Az emberi tényező jelentősége az informatikai biztonságban (5.5. fejezet), In: In: Muha Lajos (szerk.): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig, Budapest: Verlag Dashöfer Szakkiadó, 2000., ISBN:963 9313 12 2

A személyi védelem a belépéstől a szervezet elhagyásáig végig kíséri a munkatársakat.

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

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.

„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."[88]

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 munkaszervezés biztonsági, információbiztonsági „aranyszabályai"[89]:

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.

[88] Komor Levente, Nagy Béla: Az emberi tényező jelentősége az informatikai biztonságban (5.5. fejezet), In: In: Muha Lajos (szerk.): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig, Budapest: Verlag Dashöfer Szakkiadó, 2000., ISBN:963 9313 12 2

[89] Komor Levente, Nagy Béla: Az emberi tényező jelentősége az informatikai biztonságban (5.5. fejezet), In: In: Muha Lajos (szerk.): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig, Budapest: Verlag Dashöfer Szakkiadó, 2000., ISBN:963 9313 12 2

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.

3.3. Fizikai védelem

A fizikai védelem során az ISO/IEC 27001 szabvány elvárásai szerint szabályozni kell a következő területeket:

1. Fizikai biztonsági határok
2. Fizikai belépés
3. Irodák, helyiségek és létesítmények biztosítása
4. Fizikai biztonsági megfigyelés
5. Fizikai és környezeti veszélyek elleni védelem
6. Munkavégzés biztonságos területeken
7. Tiszta asztal és tiszta képernyő
8. A berendezések elhelyezése és védelme
9. A vagyontárgyak biztonsága az üzlethelyiségen kívül
10. Adathordozók
11. Támogató segédprogramok
12. Kábelezés biztonsága
13. Berendezések karbantartása
14. A berendezés biztonságos ártalmatlanítása vagy újrafelhasználása

Az információs és kommunikációs 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 információs és kommunikációs infrastruktúra elhelyezésére kiválasztott hely fizikai biztonságának felbecslésekor[90]:

- minimális kockázatot jelentsenek a szomszédos berendezések és szerkezetek vagy munkafolyamatok,
- a telekommunikációs és közművezetékek, rezgések vagy vegyszerek miatti fellépő, az információs 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,

[90] Reliable Data Centers Guideline, BITCOM, Berlin-Mitte, 2006.

- a megbízókat érintő potenciális fenyegetések felbecslése a szervezet társadalmi státusza miatt.

A számítóközpontok, szerverszobák 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 információs és kommunikációs 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.

3.4. Logikai védelem

A logikai védelem során az ISO/IEC 27001 szabvány elvárásai szerint szabályozni kell a következő területeket:

1. Felhasználói végpont eszközök
2. Kiemelt hozzáférési jogok
3. Információhoz való hozzáférés korlátozása
4. Hozzáférés a forráskódhoz
5. Biztonságos hitelesítés
6. Kapacitásmenedzsment
7. Védelem a rosszindulatú programok ellen
8. Technikai sérülékenységek kezelése
9. Konfigurációkezelés
10. Információ törlése
11. Adatmaszkolás
12. Adatszivárgás megelőzése
13. Információk biztonsági mentése
14. Az információfeldolgozó létesítmények redundanciája
15. Naplózás
16. Monitoring tevékenységek
17. Óra szinkronizálása
18. Privilegizált segédprogramok használata
19. Szoftver telepítése operációs rendszerekre
20. Hálózatbiztonság
21. A hálózati szolgáltatások biztonsága
22. A hálózatok elkülönítése
23. Webszűrés
24. A kriptográfia használata
25. Biztonságos fejlesztési életciklus
26. Alkalmazásbiztonsági követelmények
27. Biztonsági rendszerarchitektúra és műszaki elvek
28. Biztonságos kódolás

29. Biztonsági tesztelés a fejlesztés és az átvétel során
30. Kihelyezett fejlesztés
31. A fejlesztési, teszt- és gyártási környezetek szétválasztása
32. Változáskezelés
33. Vizsgálati információk

A logikai védelem során a felhasználói végponti eszközökön tárolt, feldolgozott vagy azokon keresztül hozzáférhető információkat védeni kell. A kiváltságos hozzáférési jogok kiosztását és használatát korlátozni és kezelni kell. Az információkhoz és egyéb kapcsolódó eszközökhöz való hozzáférést a hozzáférés-ellenőrzésre vonatkozó, meghatározott témakörspecifikus politikával összhangban kell korlátozni.

A forráskódhoz, a fejlesztőeszközökhöz és a szoftverkönyvtárakhoz való olvasási és írási hozzáférést megfelelően kell kezelni. A biztonságos hitelesítési technológiákat és eljárásokat az információhoz való hozzáférés korlátozása és a hozzáférés-ellenőrzésre vonatkozó témaspecifikus politika alapján kell végrehajtani. Az erőforrások felhasználását nyomon kell követni, és a jelenlegi és várható kapacitásigényeknek megfelelően kell kiigazítani.

A rosszindulatú szoftverek elleni védelmet megfelelő felhasználói tudatossággal kell megvalósítani és támogatni.

Információt kell szerezni a használt információs rendszerek műszaki sebezhetőségéről, értékelni kell a szervezet ilyen sebezhetőségeknek való kitettségét, és megfelelő intézkedéseket kell hozni.

A hardver, a szoftver, a szolgáltatások és a hálózatok konfigurációit, beleértve a biztonsági konfigurációkat is, ki kell alakítani, dokumentálni, végre kell hajtani, nyomon kell követni és felül kell vizsgálni.

Az információs rendszerekben, eszközökön vagy más adathordozókon tárolt információkat törölni kell, ha már nincs rájuk szükség. Az adatmaszkolást a szervezet hozzáférési ellenőrzésre vonatkozó tematikus politikájával és más kapcsolódó tematikus politikákkal, valamint az üzleti követelményekkel összhangban kell alkalmazni, figyelembe véve az alkalmazandó jogszabályokat. Az adatszivárgást megakadályozó intézkedéseket kell alkalmazni az érzékeny információkat feldolgozó, tároló vagy továbbító rendszerekre, hálózatokra és egyéb eszközökre.

Az információk, szoftverek és rendszerek biztonsági másolatait a biztonsági mentésre vonatkozó, elfogadott tematikus politikával összhangban kell fenntartani és rendszeresen tesztelni.

Az információfeldolgozó létesítményeket a rendelkezésre állási követelmények teljesítéséhez elegendő redundanciával kell megvalósítani.

A tevékenységeket, kivételeket, hibákat és egyéb releváns eseményeket rögzítő naplókat kell készíteni, tárolni, védeni és elemezni. A hálózatokat, rendszereket és alkalmazásokat figyelemmel kell kísérni a rendellenes viselkedés szempontjából, és megfelelő intézkedéseket kell tenni az esetleges információbiztonsági incidensek értékelése érdekében.

A szervezet által használt információfeldolgozó rendszerek óráit szinkronizálni kell a jóváhagyott időforrásokkal.

Az olyan segédprogramok használatát, amelyek képesek lehetnek a rendszer- és alkalmazásvezérlések felülírására, korlátozni és szigorúan ellenőrizni kell.

Eljárásokat és intézkedéseket kell bevezetni a szoftverek operációs rendszerekre történő telepítésének biztonságos kezelésére.

A rendszerekben és alkalmazásokban lévő információk védelme érdekében a hálózatokat és a hálózati eszközöket biztosítani, kezelni és ellenőrizni kell. A hálózati szolgáltatások biztonsági mechanizmusait, szolgáltatási szintjeit és szolgáltatási követelményeit meg kell határozni, végre kell hajtani és nyomon kell követni. Az információs szolgáltatások, felhasználók és információs rendszerek csoportjait el kell különíteni a szervezet hálózataiban.

A külső weboldalakhoz való hozzáférést úgy kell kezelni, hogy csökkentse a rosszindulatú tartalomnak való kitettséget.

Meg kell határozni és végre kell hajtani a kriptográfia hatékony használatára vonatkozó szabályokat, beleértve a kriptográfiai kulcsok kezelését is.

A szoftverek és rendszerek biztonságos fejlesztésére vonatkozó szabályokat kell megállapítani és alkalmazni. Az alkalmazások fejlesztése vagy beszerzése során azonosítani, meghatározni és jóváhagyni kell az információbiztonsági követelményeket.

A biztonságos rendszerek tervezésének elveit meg kell határozni, dokumentálni, fenntartani és alkalmazni kell minden információs rendszerfejlesztési tevékenységre. A szoftverfejlesztés során a biztonságos kódolás elveit kell alkalmazni. A biztonsági tesztelési folyamatokat a fejlesztési életciklusban kell meghatározni és végrehajtani. A szervezet irányítja, ellenőrzi és felülvizsgálja a kiszervezett rendszerfejlesztéssel kapcsolatos tevékenységeket. A fejlesztési, tesztelési és termelési környezeteket el kell különíteni és biztosítani kell.

Az információfeldolgozó eszközök és információs rendszerek változásaira változáskezelési eljárásokat kell alkalmazni.

A vizsgálati információkat megfelelően kell kiválasztani, védeni és kezelni.

Felhasznált irodalom:

2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről

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

Ameljańczyk, Andrzej: Teoria Gier, WAT, Varsó, 1978., WAT wewn. 690/78

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

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

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

Betöréses lopás- és rablásbiztosítás technikai feltételei (ajánlás), MABISZ, Budapest, 2002. február, Módosítva: Budapest, 2012. március 22.

Control Objectives for Information and Related Technology (COBIT) v. 4.1, ISACF c IT Governance Institute, Rolling Meadows, 2007.

Claude E. SHANNON - Warren WEAVER: A kommunikáció matematikai elmélete. Az információelmélet születése és távlatai. 1949. Budapest, 1986.

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

Endrédi Gábor: Hálózatok (5.8.2. fejezet), In: Muha Lajos (szerk.): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig, Budapest: Verlag Dashöfer Szakkiadó, 2000., ISBN:963 9313 12 2

Európai Unió Tanácsának Biztonsági Szabályzata (2001/264/EK)

Farmosi István: Vírusok és más logikai támadó eszközök (6.6. fejezet), In: Muha Lajos (szerk.): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig, Budapest: Verlag Dashöfer Szakkiadó, 2000., ISBN:963 9313 12 2

ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protections – Information security management systems – Requirements

ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information security controls

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

Komor Levente, Nagy Béla: Az emberi tényező jelentősége az informatikai biztonságban (5.5. fejezet), In: In: Muha Lajos (szerk.): Az informatikai biztonság kézikönyve:

Informatikai biztonsági tanácsadó A-tól Z-ig, Budapest: Verlag Dashöfer Szakkiadó, 2000., ISBN:963 9313 12 2

Magyar Értelmező Kéziszótár, Akadémiai Kiadó, Budapest, 1978./2003.

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

Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) 12. számú ajánlása – Bodlaki Ákos-Csernay Andor-Mátyás Péter-Muha Lajos-Papp György-Vadász Dezső: Informatikai Rendszerek Biztonsági Követelményei – Budapest, 1996., 217 p., ISBN:963 03 4264 2

Muha Lajos: Az informatikai rendszerek biztonsági ellenőrzése (5.9.1. pont), In: Muha Lajos (szerk.): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig, Budapest: Verlag Dashöfer Szakkiadó, 2001., ISBN:963 9313 12 2

Muha Lajos: Fogalmak és definíciók, (2.4. fejezet), In: Muha Lajos (szerk.): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig, Budapest: Verlag Dashöfer Szakkiadó, 2003., ISBN:963 9313 12 2

Muha Lajos: Az informatikai biztonság meghatározása (3.3. fejezet), In: Muha Lajos (szerk.): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig, Budapest: Verlag Dashöfer Szakkiadó, 2004., ISBN:963 9313 12 2

Muha Lajos: Az informatikai biztonság jogi szabályozása (3.4. fejezet), In: Muha Lajos (szerk.): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig, Budapest: Verlag Dashöfer Szakkiadó, 2004., ISBN:963 9313 12 2

Muha Lajos, Bodlaki Ákos: Az informatikai biztonság, Budapest: PRO-SEC KFT, 2007. 176 p., ISBN:963 86022 6 0

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

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

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.

Muha Lajos: Az Informatikai Biztonsági Irányítási Rendszer, In: Az Informatika Korszerű Technikái Konferencia, Dunaújváros, 2010.03.05-2010.03.06., pp. 156-164., ISBN:978 963 9915 38 1

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

Muha Lajos: Formális biztonsági modellek I.: A diszkrecionális hozzáférés-védelem, In: Hadmérnök VII. évf. 1. szám, pp. 278-284, Budapest, 2012.

Muha Lajos: Törvény az elektronikus információbiztonságról, In: ITBN Konferencia, Budapest, 2012.09.25-2012.09.26.

Muha Lajos, Szádeczky Tamás: Irányítási rendszerek, egyetemi jegyzet, Nemzeti Közszolgálati Egyetem, Budapest, 2014., 79 p.

Muha, Lajos; Krasznay, Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, Budapest, Nemzeti Közszolgálati Egyetem 2019., ISBN: 9786155491658

Muha Lajos: Egy szabvány változásai, Cyberblog, https://www.ludovika.hu/blogok/cyberblog/2022/11/29/egy-szabvany-valtozasai/, 2022.

MSZ ISO 2382-1:1994 Információtechnológia. Fogalommeghatározások. 1. rész: Alapfogalmak

Nemetz Tibor: A rejtjelzés, az elektronikus dokumentumok azonosítása és a digitális aláírás (6.4. fejezet), In: Muha Lajos (szerk.): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig, Budapest: Verlag Dashöfer Szakkiadó, 2004., ISBN:963 9313 12 2

Reliable Data Centers Guideline, BITCOM, Berlin-Mitte, 2006.

Security within the North Atlantic Treaty Organisation (NATO) – C-M(2002)49-REV1

Szádeczky Tamás: Terrorizmus a kibertérben, In: Infokommunikáció és jog, pp. 200-205., 5. évf. 6. szám, Budapest, 2008.

Szádeczky Tamás: Szabályozott biztonság: Az informatikai biztonság szabályozásának elmélete, gyakorlata és az alkalmazás megkönnyítésére felállított módszertan, PhD értekezés, PTE, Pécs, 2011., 286 p.

Szádeczky Tamás: Információbiztonsági szabványok, egyetemi jegyzet, Nemzeti Közszolgálati Egyetem, Budapest, 2014., 50 p.

Vírusvédelmi információs oldal, http://antivirus.hu,Veszprog Kft.

Von Bertalanffy, L.: General System Theory: Foundations, Developments, Applications. New York, Braziller., 1968.

Wiener, Norbert: Cybernetics, or Communication and Control in the Animal and the Machine, MIT Press, Cambridge, 1948.

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

4. Az információbiztonság alapjai a gyakorlatban

Az előző fejezetek ismertették az információbiztonság elméleti alapjait, annak fogalmát és tartalmát, valamint az ahhoz kapcsolódó fontosabb jogszabályokat és azok főbb elemeit. A következőkben ezek gyakorlatban történő átültetéséről, megjelenéséről lesz szó.

Jogosan merül fel a kérdés, miért van szükség az információbiztonság gyakorlati megjelenésének ismertetésére, miért nem elég csupán az elméleti alapok ismertetése? Ennek több oka is van. Egyrészt az információbiztonság elméleti alapjaival számos könyv, tanulmány, tudományos értékű mű foglalkozik, ugyanakkor ennek gyakorlatba történő átültetésével már jóval kevesebb. Pedig a gyakorlati szakemberek számára ezek legalább olyan fontos információk, mint az elméleti alapok. Sokaknak közülük ugyanis nehézséget okozhat, hogyan képezzék le az elméletet a cégük specialitásait is figyelembe véve, hogyan illesszék azokat a cég felépítéséhez, humán-, és technikai erőforrásaihoz, hogyan valósítsák meg a jogszabályok által előírt kontrollokat a gyakorlatban, a hiányzó részeknél milyen prioritásokat és ütemezést adjanak stb. Másrészt a gyakorlati felhasználó számára fontos információ lehet, hogy – a törvényi előírásokon kívül – melyek legyenek azok a védelmi lehetőségek, amelyekre érdemes és/vagy kell koncentrálni a hatékony kibervédelem kialakításához. A gyártók ugyanis számos megoldást kínálnak, ezek rengeteg opcióval rendelkeznek, ám drágák, a fenntartásuk, használatuk pedig képzett munkaerőt igényel. Ezek közül a valóban szükségesek, hatékonyak és a cég számára is megfelelők kiválasztásához a gyakorlati megközelítés sokat tud segíteni. Harmadrészt az információbiztonság komplex megközelítése és kezelése rendkívül fontos. A jogszabályokban rögzített elektronikus információs rendszerek védelmét, az adatvédelmet és a jogszabályokban nem rögzített, ám a vállalatok számára különösen értékes vállalati érzékeny adatok és üzleti titkok védelmét ellátó rendszerek, intézkedések nem lehetnek különállóak. Ehhez pedig szintén sok hasznos információval tud szolgálni egy gyakorlati megközelítésű leírás.

Ennek megfelelően a következő fejezetek az információbiztonság gyakorlati megvalósításáról szólnak. Jelen fejezet az információbiztonsági alapelvek gyakorlatban történő megjelenéséről, és az ott felmerülő problémákról, kérdésekről szól. Ezt követően a logikai, az adminisztratív és a fizikai védelem gyakorlati kérdéseiről lesz szó, hangsúlyosan kiemelve a logikai védelmi kérdéseket. Végül egy példarendszert kiragadva bemutatásra kerül, hogyan lehet a korábban ismertetetteket az adott rendszer esetében a gyakorlatban is felhasználni.

4.1. CIA[91] elv a gyakorlatban

Az információbiztonsági egyik legfontosabb és legismertebb alapelve az ún. CIA elv. Muha fogalommagyarázata szerint *„Az elektronikus információs rendszer biztonsága az elektronikus információs rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű,*

[91] CIA egy rövidítés, ahol a C a Confidentiality, magyarul bizalmasság; az I az Integrity, magyarul sértetlenség; az A pedig az Availability, magyarul rendelkezésre állás. Ezeket együtt szokták CIA-elvnek hívni.

folytonos és a kockázatokkal arányos."[92] Az Ibtv.[93] megfogalmazása szerint pedig: *„Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme."*[94] Ezen megfogalmazásokból jól látszik, hogy minden vállalat, intézmény, így az állami szervek számára is kiemelten fontos ezen elv alkalmazása. Az Ibtv. a bizalmasság, sértetlenség, rendelkezésre állás kapcsán az alábbi definíciókat adja:

- *„**bizalmasság**: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;*
- ***sértetlenség**: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;*
- ***rendelkezésre állás**: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek."*[95]

A fenti definíciókat teljes mértékben elfogadva és átvéve használja jelen könyv is a három fogalmat. Itt szükséges megjegyezni, hogy jelen könyv sok helyen hivatkozik az Ibtv. vagy a 41/2015. (VII. 15.) BM rendelet[96] előírásaira, veszi át azok fogalmait. Teszi mindezt azért, mert ugyan ezek hatálya alá meghatározott szervezetek tartoznak, ám olyan nemzetközi ajánlásokon, sztenderdeken alapszik (pl. NIST 800-53), amelyek bármely nem a hatálya alá tartozó társaságnál, vállalatnál, intézménynél használhatóvá teszi, és az ezekben használt fogalmak is rendkívül széles körben ismertek és elfogadottak.
A CIA elv tehát alapelvárásnak tekinthető minden, elektronikus információkat tároló, kezelő, továbbító stb. rendszer védelme tekintetében. Az elméleti leírások, ajánlások, előírások és jogszabályok (pl. Ibtv.) is erre építik fel a védelem kialakítását, a gyakorlati

---

[92] Muha Lajos – Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése. 2018. Nemzeti Közszolgálati Egyetem. p. 13.

[93] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény.

[94] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény. https://net.jogtar.hu/jogszabaly?docid=a1300050.tv letöltve: 2023.01.22.

[95] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény. https://net.jogtar.hu/jogszabaly?docid=a1300050.tv letöltve: 2023.01.22.

[96] 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 szóló 41/2015. (VII. 15.) BM rendelet.

megvalósítást szolgáló ajánlások, jogszabályok (pl. 41/2015. (VII. 15.) BM rendelet) pedig szintén e logika mentén adják meg a védelem kialakításánál alkalmazandó kontrollokat. Ugyanakkor, mint ahogy a következő alfejezetben részletesebben is kifejtésre kerül, a védelmet biztosító személyek esetében már nem található például kizárólag bizalmasságért felelős személy, de ugyanez mondható el a sértetlenségről és a rendelkezésre állásról is. A CIA elvben megjelenő hármast ugyanis az adminisztratív, fizikai és logikai biztonsági kontrollokkal biztosítják a jelentősebb ajánlások, szabványok, jogszabályok. Az Ibtv. és úgy fogalmaz, hogy a fent idézett, az elektronikus információs rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának megfelelő védelméhez logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatároznia, amelyek támogatják:

a. a megelőzést és a korai figyelmeztetést,
b. az észlelést,
c. a reagálást,
d. a biztonsági események kezelését.

Az Ibtv. esetében ezeket a tv. által meghatározott külön jogszabályban, a 41/2015. (VII. 15.) BM rendeletben találjuk.

4.1.1. Logikai védelem

A logikai védelem Ibtv. szerinti definíciója a következő: *„az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem”*[97]. Ennek alapján a gyakorlatban a logikai védelemhez tartozik minden olyan hardver és szoftver elem, amely az elektronikus úton megvalósított, azaz a kibertérből érkező támadások ellen védenek, irányuljanak azok a bizalmasság, sértetlenség vagy a rendelkezésre állás ellen. Ilyen támadások lehetnek például a tűzfalak, vírusvédelmi szoftverek, behatolás jelző eszközök stb. A logikai védelem gyakorlati kialakítása a következő fejezetekben részletesebben is kifejtésre kerül.

4.1.2. Fizikai védelem

A fizikai védelem meghatározását az Ibtv. a következő szerint adja meg: *„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”*[98]. Az idézett definíció szinte felsorolás szerűen meg is adja azokat az alkategóriákat, amelyekre figyelemmel kell lenni. A gyakorlatban tehát a fizikai védelem kategóriába tartoznak a fizikai térből érkező támadások és egyéb fenyegetések elleni védelem eszközei. Ilyenek például a beléptetőrendszerek, a kamerarendszerek, riasztórendszerek, a tűzjelző rendszerek, rácsozatok, de ide tartoznak a szünetmentes tápellátást biztosító eszközök, az őrség stb. A fizikai védelemről egy későbbi fejezetben szintén esik még szó.

---

[97] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény. https://net.jogtar.hu/jogszabaly?docid=a1300050.tv letöltve: 2023.01.22.

[98] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény. https://net.jogtar.hu/jogszabaly?docid=a1300050.tv letöltve: 2023.01.22.

4.1.3. Adminisztratív védelem

Az adminisztratív védelem fogalmát az Ibtv. a következők szerint adja meg: *„a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás”*[99]. A gyakorlatban ide tartoznak azok a szabályzatok, előírások, munkautasítások, amelyek kiegészítve a logikai és fizikai védelmi elemeket, egyértelműsítik, hogy akikre vonatkozik mit tehetnek meg, mit nem szabad tenniük, valamint azt is, hogy a szabályok megsértése milyen konzekvenciákat von maga után. Az adminisztratív védelmi elemek közé tartoznak a gyakorlatban például az adott intézmény, vállalat informatikai biztonságpolitikája, az informatikai biztonsági szabályzat (IBSZ), az üzletmenet-folytonossági tervek (BCP[100]), a katasztrófaelhárítási vagy más nevén vészhelyzeti helyreállítási tervek (DRP[101]), biztonságtudatosító anyagok, képzések[102] stb.

4.2. CIA elvet a gyakorlatban megvalósító személyek

A vállalatoknak, intézményeknek az elektronikus információs rendszerek zárt, teljes körű, folytonos és a kockázatokkal arányos biztonsága érdekében a CIA elvben megjelenő hármast, azaz a bizalmasságot, a sértetlenséget és a rendelkezésre állást szükséges biztosítaniuk. Ugyanakkor, amint az az előző fejezetben már említésre került, a védelmet biztosító személyek esetében már nem található például kizárólag bizalmasságért felelős személy, de ugyanez mondható el a sértetlenségről és a rendelkezésre állásról is. Helyette a gyakorlatban a logikai, fizikai és adminisztratív biztonság megteremtése mentén, de ott is többnyire szeparáltan, több funkcióban találhatunk kijelölt személyeket. A gyakorlatban a vizsgálandó biztonsági kérdésekért felelős személyek tekintetében az alábbi csoportokat célszerű felállítani:

1. Elektronikus információk és információs rendszerek biztonságáért felelős személyek;
2. Üzembiztonságért felelős személyek;
3. Adatbiztonságért felelős személyek;
4. Fizikai biztonságért felelős személyek;
5. Adminisztratív biztonságért felelős személyek;
6. Törvényes ellenőrzésért felelős személyek.

4.2.1. Elektronikus információk és információs rendszerek biztonságáért felelős személyek

Ebbe a kategóriába tartoznak azok a személyek, akik a legnagyobb részt lefedik a bizalmasság, a sértetlenség és bizonyos mértékig a rendelkezésre állás hármasból. Ők gondoskodnak jellemzően a logikai védelmek kialakításáról és működtetéséről, koordinálják a fizikai védelem előírt elemeinek megvalósítását és ebben szorosan együttműködnek az általában elkülönülten megjelenő és működő, a fizikai biztonságért felelős vállaltbiztonsági csapattal, feladataik közé tartozik az információbiztonsági

---

[99] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény. https://net.jogtar.hu/jogszabaly?docid=a1300050.tv letöltve: 2023.01.22.

[100] BCP: Business Continuity Plan, magyarul üzletmenet-folytonossági terv

[101] DRP: Disaster Recovery Plan, katasztrófaelhárítási terv, vagy más nevén vészhelyzeti helyreállítási terv

[102] angolul security awareness training

irányítási rendszer (IBIR) kialakítása és működtetése, valamint releváns szabályzók megalkotásával biztosítják az adminisztratív védelem bizonyos elemeit. Ők felelősek az elektronikus információk biztonságával kapcsolatos ügyekben a megfelelő szervezetekkel és hatóságokkal (pl. NKI[103], NEIH[104]) az egyedüli kapcsolattartásért. Ezek a személyek az Ibtv. által is nevesített az elektronikus információs rendszer biztonságáért felelős személy (IBF), valamint jellemzően az egyes intézményeknél, vállalatoknál különböző névvel illetett ITbiztonsági, kiberbiztonsági, informatikai biztonsági szervezeti egység tagjai is.

4.2.2. Üzembiztonságért felelős személyek

Az ebbe a kategóriába tartozó személyek, leginkább rendelkezésre állásért felelősek, kisebb mértékben közreműködnek a bizalmasság és a sértetlenség biztosításában is. Azért nem lehet egyértelműen kijelenteni, hogy kizárólag ők felelősek a rendelkezésre állásért, mert pl. egy DDoS[105] támadás is alapvetően a rendelkezésre állást sérti, annak kezeléséért pedig az előző alpontban említett személyek, szervezeti egységek a felelősök. Elhatárolásként azt lehet mondani, hogy a szervezet által használt rendszerek, eszközök meghibásodásaira, műszaki problémáira visszavezethető, azaz nem külső vagy belső támadók által okozott rendelkezésre állási gondok kezeléséért és megoldásáért felelősek. Fontos megemlíteni, hogy sok esetben egy probléma észlelésekor még nem lehet eldönteni, hogy az valamilyen meghibásodás vagy kibertámadás következménye, így annak eldöntéséig minden esetben szorosan együtt kell működnie a kiberbiztonságért felelős szervezeti egységnek az üzemeltetésért felelőssel. De nem csak az eldöntésig, hanem az esetek döntő többségében a kibertámadások esetén a kezelésben, a károk enyhítésében, felszámolásában, az eredeti működés visszaállításában is. Az üzembiztonságért felelős személyek működtetik, javítják az adott vállalatok, intézmények infokommunikációs rendszereit, működnek együtt az üzemeltetésbe bevont külső vállalkozókkal, szállítókkal, felhőszolgáltatókkal. Ezek a személyek az adott intézményeknél, vállalatoknál üzemeltetett infokommunikációs rendszerek üzemeltetői, valamint azok vezetője, pl. informatikai igazgató.

4.2.3. Adatbiztonságért felelős személyek

Az ebbe a kategóriába tartozó személyek speciális felelősséggel rendelkeznek. Jellemzően az Infotv.[106] által is nevesített adatkörök, így pl. a személyes adatok, különleges adatok stb. védelméről gondoskodnak, jellemzően az adott intézményeknél, vállalatoknál szervezeti egységeken átívelő feladatszabó, -koordináló és azok elvégzését ellenőrző módon. Ők felelősek az adatvédelmi ügyekben a megfelelő hatóságokkal (pl. NAIH[107], NMHH[108]) az egyedüli kapcsolattartásért. Szorosan együtt kell működjenek az előző két alpontban felsorolt személyekkel, szervezeti egységekkel több ok miatt is.

---

[103] NKI: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet

[104] NEIH: Nemzeti Elektronikus Információbiztonsági Hatóság

[105] DDoS: Distributed Denial of Service, elosztott szolgáltatásmegtagadással járó támadás, vagy más néven elosztott túlterheléses támadás.

[106] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

[107] NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság

[108] NMHH: Nemzeti Média- és Hírközlési Hatóság

Egyrészt egy kibertámadásnak lehetnek adatvédelmi aspektusai, amelyet az adatbiztonságért felelős személyeknek kell kezelnie. Másrészt a kifejezettem adatvédelmi incidensként induló bejelentések kivizsgáláshoz, kezeléséhez az előző pontokban felsorolt szervezeti egységektől, felelősöktől kapják meg a adatbiztonságért felelős személyek a szükséges információkat, velük együtt tudnak sok esetben technikai megoldást találni a problémák kezelésére (pl. adatszivárgás okainak kivizsgálása, megszűntetése). A vállalat méretétől és feladataitól függően vagy csupán az Infotv által is nevesített adatvédelmi tisztviselő[109], vagy esetleg az őt segítő kis létszámú stábja található itt.
Fontos megjegyezni, hogy a kötelezően ellátandó adatvédelmi feladatok esetében is már nagy szerepe van a kibervédelemért felelős területnek. Erre jó példa, hogy a GDPR[110] bevezetése okán változó Infotv.[111], és az azok előírásának teljesítése érdekében teendő intézkedések. Ezek jó összefoglalását adja az adatvedelem.hu oldalon található „Felkészülés az adatvédelmi rendeletre" című cikksorozat[112], amely 12 pontban foglalja össze azokat az elemeket, feladatokat, amelyeket teljesítenie kell, amelyekre készülnie kell egy szervezetnek. Ezek a következők:

1. **Adatvédelmi tudatosság** – meghatározni, mire van hatással
2. **Tárolt adatok** – személyes adatok származása, kezelése, megosztása, auditálása
3. **Tájékoztatás** – adatvédelmi tájékoztató felülvizsgálata (megfelelő-e)
4. **Az érintettek jogai** – belső szabályozók felülvizsgálata (hozzáférés, helyesbítés, törlés)
5. **Az érintettek hozzáférési joga** – kérelmek kezelése, igény szerinti tájékoztatás nyújtása, ezek határideje, díjazása
6. **A személyes adatok kezelésének jogalapja** – dokumentálni, az adatvédelmi tájékoztatóban is
7. **Hozzájárulás** – ezek megszerzése, kezelése, dokumentálása
8. **Gyermekek jogai** – kor igazolása, szülő hozzájárulása
9. **Az adatok kiszivárgása** – adatvagyon felmérése, beépített védelmek felülvizsgálata, incidensnél jelentés, kivizsgálás

---

[109] angolul DPO: data protection officer

[110] GDPR: General Data Protection Regulation vagy általános adatvédelmi rendelet, azaz AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról.

[111] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

[112] Felkészülés az adatvédelmi rendeletre. 1-5. rész.

https://www.adatvedelmirendelet.hu/adatvedelmi-rendelet/elso-lepesek-tudatossag-es-tarolt-adatok/

https://www.adatvedelmirendelet.hu/adatvedelmi-rendelet/folytatas-tajekoztatas-es-szemelyhez-fuzodo-jogok/

https://www.adatvedelmirendelet.hu/uncategorized/kovetkezo-harom-lepes-kervenyek-jogalap-es-beleegyezes/

https://www.adatvedelmirendelet.hu/uncategorized/felkeszules-az-adatvedelmi-rendeletre-4-resz/

https://www.adatvedelmirendelet.hu/uncategorized/felkeszules-az-adatvedelmi-rendeletre-5-resz/ Letöltve: 2023.02.11.

10. **Beépített adatvédelem, adatvédelmi hatásvizsgálat** – hatásvizsgálat tervezés, végrehajtás, kapcsolódás más folyamatokhoz
11. **Adatvédelmi tisztviselő** – kijelölés
12. **Nemzetközi szint** – multi cégeknél adatvédelmi felügyelet kijelölése

Ezekből a 9. és a 10. pontban leírtak szorosan kapcsolódnak a kibervédelemhez, hiszen azok teljesítéséhez alapvetően kibervédelmi eszközök is szükségesek. A kibervédelem és az adatvédelem szoros kapcsolatát igazolja az alábbi 1. táblázat kibervédelmi technológiák és az adatvédelem kapcsolata is. Ez azt mutatja, hogy az egyes kibervédelmi elemek, technológiák mely adatvédelmi folyamatokat támogatják és a GDPR melyik követelményét elégítik ki.

Technologies	Processes supported	Ref. to GDPR Requirements
1 GRC Tools	Personal Data Processing Register, Data Mapping, Risk Analysis, Data Protection Impact Assessment, DPO monitoring activities, Internal Audit, Third party management	Art 12 , Art.15, Art 18-21, Art 30, 32, 33, 35
2 DLP	Data Loss Prevention, Data Classification	Art.32
3 SIEM	Security Incident Event Management: log management and correlation to identify, monitor and manage internal security incident, Data Breach Management	Art.33, Recital 49, 87, 88
4 SOC	Security Operation Centre: effective and quickly security management by a continuous monitoring of the internal and external security events.	Art.32, Recital 49, 87, 88
5 IAG	Digital Identity Governance, Users and Profiles review, reporting, auditing,	Art.32
6 IAM	Identity Provisioning, self service provisioning	Art.32
7 PAM	Privileged Access Management, System Administration Management, SA password securing	Art.32
8 Encryption/Data Masking	Encryption and / or masking for specific data category or personal data process	Art. 32 Security Measures
9 Malware Detection	Anti Malware	Art. 32 Security Measures
10 IDS	Intrusion Detection System, Data Breach Management	Art. 32 Security Measures
11 CMDB and ITSM	SDCL, Security & Data Protection by Design	Art. 25 Privacy by Design
12 Data Labelling	Tag and labelling of classified data	Art. 32 Security Measures

Technologies	Processes supported	Ref. to GDPR Requirements
13 Third Party	Security Third Party Security Assessment and Monitoring	Art. 32 Security Measures Art. 28 External Data Processor
14 DMS & Digitalization	Document Management Systems & Digitalization	Art. 32 Security Measures

1. táblázat kibervédelmi technológiák és az adatvédelem kapcsolata

Szerkesztette: a szerző RSA Summit Rome 2018. alapján

4.2.4. Fizikai biztonságért felelős személyek

Ebbe a kategóriába tartoznak azok a személyek, akik a bizalmasság, a sértetlenség és a rendelkezésre állás hármas kapcsán mindhárom elem vonatkozásában a fizikai biztonsági elemek meglétéért, azok üzemeltetéséért felelősek. Önállóan jellemzően nem tartanak kapcsolatot információbiztonsági szervezetekkel és hatóságokkal (pl. NKI, NEIH, NAIH, MNHH stb.), hanem az adott, erre kijelölt és az előző alpontokban említett szakterületek felkérésére szolgáltatnak adatokat, vesznek részt auditokban. A logikai, fizikai adminisztratív védelem fizikai és az azokhoz kapcsolódó adminisztratív védelmi elemeit valósítják meg, szorosan együtt működve a kibervédelmi területtel. Ez azt jelenti, hogy önállóan kiépíthetnek, működtethetnek olyan fizikai biztonsági elemeket is, amelyek nem a kibervédelmi előírásokban (pl. Ibtv.-ben és a 41/2015. (VII. 15.) BM rendeletben) megfogalmazottak miatt, hanem az adott vállalat, intézmény egyéb érdekei okán létesítenek, ám ezeknek vagy magukban is teljesíteniük kell a kibervédelmi előírásokat, vagy ki kell egészíteni ezeket a hiányzó elemekkel. Ezek meglétéről adnak jelentést a kibervédelmi és az adatvédelmi területek felé. Ezek a személyek jellemzően a vállalatbiztonsági terület[113] munkatársai és ezek vezetője, jellemzően a biztonsági igazgató. Kiemelendő, hogy sok esetben a létfontosságú rendszerelemekkel is rendelkező intézmények, vállalatok esetében a létfontosságú rendszerelemekkel összefüggő feladatok koordinálást is ez a terület biztosítja, a jogszabályokban nevesített biztonsági összekötő is itt található. Bár e feladatok tekintetében (pl. üzemeltetési biztonsági terv elkészítése, benyújtása, felülvizsgálata, incidensek bejelentése stb.) önállóan tart kapcsolatot az illetékes hatóságokkal (pl. NMHH, OKF), de a kiberbiztonsághoz kapcsolódó feladatok esetében azokat jellemzően a kibervédelmi terület látja el (pl. kapcsolódó rendszerek osztályba sorolása, OVI tábla[114] kitöltése, benyújtása, kiberbiztonsági incidensek jelentése stb.).

4.2.5. Adminisztratív biztonságért felelős személyek

Ebbe a kategóriába tartoznak azok a személyek, a bizalmasság, a sértetlenség és a rendelkezésre állás hármas kapcsán mindhárom elem vonatkozásában jellemzően az általános, a fentieknél külön nem említett adminisztratív biztonsági elemek meglétéért, azok üzemeltetéséért felelősek. Jellemzően ők működtetik a nyílt és a titkos irattárat, látják el a belső szabályozások elkészítését, koordinálását, kiadását. Jellemzően ezek nem egy helyen találhatók meg a vállalati, intézményi szervezeti rendszerben, hiszen egyrészt

[113] angolul corporate security

[114] Az Ibtv. által előírt ún. „Osztályba sorolás és védelmi intézkedés űrlap”

a nyílt és a titkos irattár szervezeti elhelyezése több szervezeti egységnél is lehetséges, erre sokféle megoldás is látható, ráadásul a minősített iratok kezeléséért felelős biztonsági vezető jellemzően a vállalatbiztonsági terület vezetője is egyben, másrészt a szabályozások koordinálását, kiadását jellemzően a jogi területnél találjuk, harmadrészt a szükséges szabályzók rendszerének kialakítása (pl. biztonsági politika, IBSZ stb.), azok tartalmi elkészítése jellemzően a korábban felsorolt területek vezetőinek és vezető tisztségviselőinek (IBF, DPO, biztonsági összekötő, biztonsági vezető stb.) feladata. Az adminisztratív biztonságért felelős személyek tehát jellemzően a kiberbiztonságért, a vállaltbiztonságért, valamint az üzemeltetésért felelős vezetők, a jogi, szabályozási terület munkatársai, valamint az irattári egység dolgozói.

4.2.6. Törvényes ellenőrzésért felelős személyek

A jogszabályok által előírt törvényes ellenőrzés (adatszolgáltatás, lehallgatás) kapcsán az egyes vállalatok, intézmények eltérő feladatrendszerrel rendelkeznek. Általában a kötelezően végrehajtandó feladatokat a kiberbiztonsági és a vállalatbiztonsági terület látja el, vagy ha az mások bevonását is igényli (pl. üzemeltetés), akkor koordinálja. Ezek a területek önállóan, a felhatalmazásuknak megfelelően tartják a kapcsolatot az illetékes nemzetbiztonsági szolgálatokkal és rendvédelmi szervekkel. A törvényes ellenőrzésért felelős személyek tehát jellemzően a kiberbiztonságért és a vállaltbiztonságért felelős vezetők, bár a kisebb méretű, vagy a törvényes ellenőrzési feladatokkal csak kevéssé érintettszervezetek esetében (pl. nem infokommunikációval, banki szolgáltatásokkal stb. foglalkozó szervezetek) ennek a feladatnak az ellátásával a jogi terület vezetőjét bízzák meg.

4.3. Üzletvezérelt biztonság

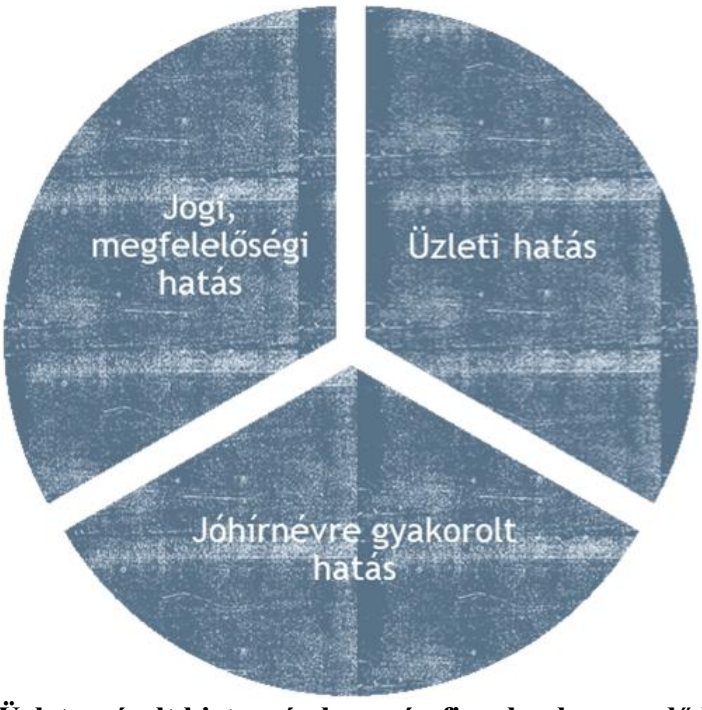
Az előző alfejezetben megvizsgáltuk a CIA elv gyakorlati átültetését és azt, hogy kik azok a személyek, akik feladat és felelősségi körébe tartozik ez. Az információbiztonság és ezen belül a kiberbiztonság gyakorlati megvalósításának egy másik fontos aspektusa, ahogy azt az idézett Muha fogalommagyarázat és az Ibtv. definíció is tartalmazta. Érdemes tehát megvizsgálni, hogyan lehet a kockázatarányos védelmet kialakítani. Természetesen kockázatelemzéssel, amelynek leírására már számtalan mű született. Jelen könyv arra koncentrál, hogy milyen kockázatokat érdemes figyelembe venni az ún. üzletvezérelt biztonság[115] kialakítása érdekében.

Az üzletvezérelt biztonság fogalma kapcsán több elemet is célszerű körbejárni. Az első az üzlet szó. Itt természetesen nem csak a piaci alapon működő vállalatok hagyományos értelemben vett üzleti céljait kell érteni, hanem az adott vállalat, intézmény tevékenységeit, amellyel feladatait ellátja. Ilyen lehet például egy állami intézmény jogszabályban meghatározott feladatrendszere, vagy egy nonprofit vállalat tevékenységi köre is. A második rész az üzletvezérelt elnevezés. Ez azt takarja, hogy – természetesen a különböző jogszabályok által kötelezően előírtakon kívül, vagy felül – melyek a kiemelt kockázatok, milyen adatokat, információkat, rendszereket vagy rendszerelemeket kell kiemelten védeni.

[115] üzletvezérelt biztonság, angolul business driven secutity. forrás: RSA Summit Rome 2018

Az információbiztonság kapcsán az intézményeknek, vállalatoknak az alábbi 2. ábra Üzletvezérelt biztonság kapcsán figyelembe veendő hatásokszerinti hatásokat célszerű figyelembe venniük:

1. Jogi, megfelelőségi hatás;
2. Üzleti hatás;
3. Jóhírnévre gyakorolt hatás.



2. ábra Üzletvezérelt biztonság kapcsán figyelembe veendő hatások

Szerkesztette: a szerző RSA Summit Rome 2018. alapján

4.3.1. Jogi, megfelelőségi hatás

A jogi, megfelelőség hatás alatt azt értjük, hogy milyen elemeket kell megvalósítani, amelyeket valamely jogszabály előír, azok esetleges be nem tartása milyen következményekkel járhat, mekkora büntetéseket kaphat az adott intézmény, vállalat. Ide tartoznak a kötelezően betartandó hazai jogszabályi előírások, mint pl. Ibtv., 41/2015. (VII. 15.) BM rendelet, Infotv., vagy a kijelölt létfontosságú rendszerelemeket működtető szervezetek esetében az Lrtv.[116] és annak ágazati előírásait tartalmazó jogszabályok, de a törvényes ellenőrzéssel kapcsolatos jogszabályok, mint pl. Nbtv.[117], vagy az adott ágazatra vonatkozó jogszabályok, mint pl. a telekommunikációs ágazatot érintő Eht.[118] stb. is. Szintén ide sorolandók azon külföldi jogszabályok, amelyeket az adott vállalatoknak figyelembe kell venniük. Ilyen lehet egy nemzetközi háttérrel rendelkező cég esetében az anyavállalatnál kötelező honos országbeli jogszabályok, amely a leányvállalatok számára is előírtak, vagy egy külföldi piacra dolgozó vállalat esetében a célország hatályos jogi szabályai. Ugyancsak itt kell megemlíteni az adott szervezet,

[116] A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény

[117] A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény

[118] Az elektronikus hírközlésről szóló 2003. évi C. törvény

vállalat saját célkitűzéseinek megvalósítását segítő megfelelőségek teljesítését. Tipikusan ilyenek lehetnek a különböző irányítási rendszerek, mint pl. az ISO 9001 Minőségirányítási Rendszer (MIR), az ISO/IEC 27001 Információbiztonsági Irányítási Rendszer (IBIR) vagy az ISO 22301 Üzletmenet-folytonosság Irányítási Rendszer[119].
Az adott vállalatnak, intézménynek az összes rá vonatkozó kötelező és önkéntesen vállalt elemről érdemes nyilvántartást vezetnie. Ez lehet központi, de lehet egy adott, általában nagyobb vállalaton belül a kijelölt szervezeti egységekre szétosztott is. Ez utóbbira példa, hogy amíg az Ibtv. előírásaiért a kiberbiztonságért felelős szervezeti egység a felelős, addig az Infotv. betartásáért az adatvédelmi felelős. A nyilvántartásban szereplő összes elem maradéktalan betartása nem minden esetben lehetséges. Amikor egy vállalatnak jelentős költségcsökkentéssel kell szembe néznie, vagy egy új terméket akar gyorsan piacra dobni és nincs idő mindennek megfelelni, akkor mérlegelnie kell. Vannak olyan tételek, amelyek esetében ez egyszerű. Ilyen lehet egy kötelező jogszabály be nem tartása esetén a vállalat működési engedélyének visszavonási kockázata, pl. Nbtv. előírások esetében találunk ilyet. Ugyanakkor más büntetési tételek esetén a kockázatok és következmények alapján dönthet arról, hogy bizonyos büntetések, ezek jellemzően pénzbírságok, kockázatát felvállalja-e, és e mellett az előírások teljesítését egy későbbi időpontra tolja. Ennél talán egy fokkal könnyebb döntési helyzet az önkéntesen vállalt előírások, így pl. irányítási rendszer előírásainak teljesítését szolgáló beruházások későbbre halasztása. Ebben az esetben alapvetően szervezet reputációjában következik, következhet be csökkenés.
Kiemelendő, hogy minden esetben a kockázatok mérlegelését követő tudatos döntés következményének kell lennie egy nem megfelelőségnek. Ennek érdekében a lehető legteljesebb mértékben ki kell zárni azokat a lehetőségeket, amelyek emberi mulasztásra (pl. valaki elfelejti, hogy határidőre teljesíteni kell egyjogszabályban előírt elemet), esetleg a belső vállalati folyamatok hiányára (nincs felelős szervezet kijelölve, így mindenki a másikra vár, hogy megcsinálja) visszavezethetően történjen előírás mulasztás.
A kockázatelemzés és -kezelés egy későbbi fejezetben még részletesen elemzésre kerül.

4.3.2. Üzleti hatás

Az üzleti hatások elemzésénél az adott szervezet tevékenységi köreit szükséges figyelembe venni. Ehhez kell ezek után meghatározni, hogy számára melyek a prioritások az információvédelemben, és mely veszélyeket, kérdéseket lehet hátrébb sorolni. Így például amíg egy webshopokat üzemeltető vállalkozás esetén egy szolgáltatásmegtagadással járó támadás[120] vagy elosztott szolgáltatásmegtagadással járó támadás, vagy más néven elosztott túlterheléses támadás[121] jelenthet kiemelt problémát, addig egy kutató vállalat esetében a kibertérben folytatott üzleti kémkedéshez használt kémprogramok jelenthetik a fő veszélyt. Az állami intézmények esetében pedig az államilag szponzorált támadók által használt kifinomult, folyamatosan fennálló fejlett fenyegetések[122], azaz az ún. APT támadások szolgáltathatják a legfőbb problémát.
Az üzleti hatást, mint azt már korábban említettük, mindig az adott szervezet tevékenységei köreihez kell értelmezni, így egy állami szerv esetében is megragadhatók

[119] angolul: Business Continuity Management Systemmel (BCMS)

[120] angolul: Denial of Service (DoS)

[121] angolul: Distributed Denial of Service (DDoS)

[122] angolul: Advanced Persistent Threat (APT)

ezek. Azaz ebben az összefüggésben az üzleti szónak a tágabb értelmezését kell figyelembe venni. Ha az előző példákat át akarjuk fordítani az állami szektorra, akkor elmondhatjuk, hogy amíg például az állampolgárokat kiszolgáló webes rendszerek (pl. Ügyfélkapu+, magyarorszag.hu stb.) esetében a DoS, DDoS támadások jelenthetik az egyik legnagyobb problémát, addig egy minisztérium számára az APT támadások és az azokban használt kémprogramok okozhatják a legfőbb veszélyt.
Az üzleti hatást a profitorientált vállalatok esetében akár minden esetben pénzügyi hatásnak is nevezhetjük, míg állami szervezetek esetében már kicsit vegyesebben a kép. Egy nagy bevételt hozó állami rendszer (pl. autópályamatricák értékesítését ellátó rendszer) kiesése szintén jelentős pénzügyi hatásokat válthat ki, így ebben az esetben szintén pénzügyi hatást említhetünk. Ugyanakkor egy kormányablak leállása pénzügyi értelemben nem feltétlenül jelentős, ám az alapfeladatát a leállás alatt nem fogja tudni ellátni. Ebben az esetben tehát nem csak pénzügyi hatást jelent az üzleti hatás. Hozzá kel tenni, hogy itt még a következő alfejezetben kifejtésre kerülő jó hírnévre gyakorolt hatásról még nem beszélünk.
Ebben az esetben is alapos kockázatelemzés és -értékelés után kell meghatározni azokat a védelmi elemeket, amelyeket akár a kötelező (pl. Ibtv., 41/2015. (VII. 15.) BM rendelet által meghatározott) védelmi kontrollokat meghaladóan telepíteni és üzemeltetni kívánunk. Így például a túlterheléses támadások ellen volumetrikus és alkalmazás szintű DDoS védelmi eszközöket alkalmazni, vagy az APT jellegű támadások mielőbbi felismerése érdekében viselkedés alapú kontrollokat bevezetni (pl. végpontvédelmi és elhárítási eszközök[123], hálózati és email védelmi sandboxok, azaz olyan elszeparált szoftveres vagy hardveres környezetek, amelyekben megvizsgálhatók, hogy pl. egy letöltött fájl hogyan viselkedik, lesznek-e a megnyitásának káros következményei, miközben ennek nem lesz hatása az éles rendszerre). Az itt felhasználható védelmi lehetőségek, képességek egy későbbi fejezetben részletesebben is kifejtésre kerülnek.

4.3.3. Jóhírnévre gyakorolt hatás

A jóhírnévre, vagy idegen szóval a reputációra gyakorolt hatás sok esetben legalább olyan fontos, mint az üzleti (vagy ha úgy tetszik, pénzügyi) hatás. Egy profitorientált vállalat esetében komoly reputációs veszteséget okozhat egy sikeres kibertámadás, ennek kapcsán például ügyfeleiket is érintő rendszerleállások bekövetkezte, vagy akár szenzitív és/vagy személyes adatok eltulajdonítása, kiszivárgása. Számos példát láttunk már ilyenre, amely után az adott vállalatban az ügyfelek bizalma megingott, versenytársakat vettek igénybe, így a vállalat bevételei már akár rövidtávon is jelentősen csökkentek, sőt volt, akit csődbe is vitt. Az állami szférában a jóhírnévre gyakorolt hatás sok esetben sokkal jelentősebb tud lenni, mint az üzleti hatás. A magyaroroszag.hu leállásának önmagában csekély az üzleti (itt értsük úgy, pénzügyi) kockázata, ám a leállást követően nagyon rövid időn belül címlapokra kerül a dolog.
Akárcsak az előző esetben, jóhírnévre gyakorolt hatás esetében is alapos kockázatelemzés és -értékelés után kell meghatározni azokat a védelmi elemeket, amelyeket akár a kötelező (pl. Ibtv., 41/2015. (VII. 15.) BM rendelet által meghatározott) védelmi kontrollokon túlmutatóan alkalmazni szükséges az adott vállalatnak, intézménynek. Ilyenek lehetnek az előző alfejezetben példaként hozott DDoS védelmi eszközök, az APT jellegű támadások mielőbbi felismerése érdekében viselkedés alapú kontrollok, de ide érthetők akár a rendelkezésre állást magasabb szinten biztosító redundáns rendszerelemek

[123] angolul: Endpoint Detection and Response (EDR)

használata is. Természetesen ez utóbbi is lehet akár üzleti hatások enyhítését szolgáló megoldás is. Éppen ezért az itt felhasználható védelmi lehetőségek, képességek nem önállóan kerülnek részletesebben kifejtésre egy későbbi fejezetben, hiszen az előző alfejezetben leírt üzleti hatások, valamint az itt említett jóhírnévre gyakorolt hatások kapcsán jelentkező veszélyek enyhítésére szolgáló eszközök azonosak. Az pedig, hogy egy adott védelmi elem (pl. DDoS védelmi eszköz) mely hatást mennyire enyhítheti, az az adott vállalat, intézmény feladataitól függ.

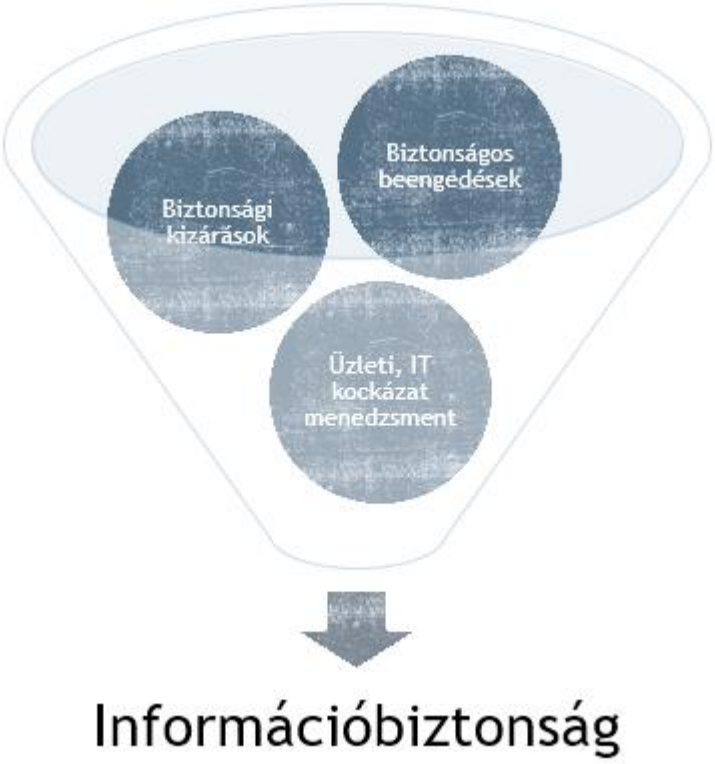
Az üzletvezérelt biztonság kapcsán megvizsgált elemek tekintetében összességében elmondható, hogy az előzőekben vizsgált hatások, azaz az üzleti hatás, a jóhírnévre gyakorolt hatás és a jogi, megfelelőség hatás tehát szorosan kapcsolódnak egymáshoz, sokszor át is lapolódnak. Ezek együttes elemzése, az ezek kapcsán feltárt kockázatok együttes értékelése után lehet dönteni bizonyos védelmi elemek megerősítéséről, vagy adott esetekben a kockázatok felvállalása mellett más védelmi elemekről való lemondásról vagy korlátozott mértékű megvalósításáról.

4.4. Üzletvezérelt információbiztonság

Az üzletvezérelt biztonság című alfejezetben megvizsgáltuk a miért kérdésre a válaszokat, kis mértékben megemlítve azt is, hogy milyen eszközökkel lehet bizonyos kihívásokra feleletet adni. Ám ott ezek csak példálózó jellegűek voltak. Ebben az alfejezetben a hogyan kérdésre keressük a választ, azaz hogyan lehetünk képesek a gyakorlatban elérni a CIA elvben leírtakat úgy, hogy azok üzletvezérelt módon biztosítsák információink biztonságát.

Ehhez szintén csoportokat érdemes felállítani, és azt mondani, hogy az információbiztonságot három nagy alappillér köré szervezzük meg. Ezek az alábbi 3. ábra Üzletvezérelt biztonság kapcsán megjelenő információbiztonsági feladatokáltal is bemutatott:

1. Biztonsági kizárások;
2. Biztonságos beengedések;
3. Üzleti, IT kockázatmenedzsment.



3. ábra Üzletvezérelt biztonság kapcsán megjelenő információbiztonsági feladatok
Szerkesztette: a szerző RSA Summit Rome 2018. alapján

Ezen három alappillér mindegyikéhez tartozó, a gyakorlatban használt elemek részletesen bemutatásra kerülnek a következő fejezetekben, itt csupán azok elméleti megalapozására kerül sor.

4.4.1. Biztonsági kizárások

A biztonsági kizárások alkategória azon védelmi kontrollokat foglalja magába, amelyek azt szolgálják, hogy illetéktelenek ne férhessenek hozzá az adott vállalat, intézmény adataihoz, információihoz és/vagy azokat ne módosíthassák és/vagy törölhessék és/vagy ne vihessen be adatokat, információkat, és/vagy ne tehessék azokat elérhetetlenné a jogosultak számára, ne legyenek képesek a rendszer működésének gyengítésére, korlátozására vagy akár teljes leállítására. A gyakorlatban ez azt jelenti, hogy az itt alkalmazott védelmi kontrollok biztosítják azt, hogy a külső támadókat kizárjuk az adott szervezet rendszereiből, megakadályozzuk az azokba történő behatolást, amennyiben ez mégis megtörténik, akkor a lehető leghamarabb észrevegyük azokat, meg tudjuk akadályozni a további ténykedést, a lehető leghamarabb képesek legyünk enyhíteni az okozott károkat, felmérni a támadás részleteit és visszaállítani az eredeti állapotot. De ehhez hasonlóan a belső támadók káros tevékenységének a felderítését, megakadályozását stb. ugyanígy biztosítják.
A biztonsági kizárások eszközrendszerébe tartoznak a védekezés különböző szintjein, így például az adat, az alkalmazás, szerverek, a hálózat stb. szintjein megjelenő azon védelmi

elemek, amelyek a fent leírtakat szolgálják. Ezek lehetnek a PreDeCo[124] elv szerinti prediktív (azaz megelőző), detektív (azaz érzékelő, megfigyelő), korrektív (azaz elhárító) intézkedések megtételéhez szükséges kontrollok egyaránt. A biztonsági kizárások természetesen lehetnek fizikai, adminisztratív és logikai elemek is, itt a következőben a logikai elemekkel foglalkozunk részletesebben.
A biztonsági kizárásokat szolgáló elemek lehetnek aktívak vagy passzívak. Az aktív elemek azok, amelyek megelőző támadásokat, ellentámadásokat vagy az aktív megtévesztést szolgálják. Ezek közül a vizsgált téma szempontjából csupán az aktív megtévesztés az érdemleges, megelőző vagy válaszcsapást ugyanis csak speciális jogosítvánnyal rendelkező szervezetek tehetnek, ez viszont nem tárgya jelen könyvnek. Aktív megtévesztést szolgáló eszközökre jellemző példa az ún. Honeypot amely egy szándékosan gyenge védelemmel ellátott rendszer, amely a támadók tevékenységének rögzítésére szolgál. A passzív védelmi elemek közé tartoznak a szabály vagy szignatúra vagy anomália alapú védelmi eszközök, mint például a „klasszikus" kibervédelmi eszközök, így például a tűzfalak, vírusírtók, a behatolás érzékelő és megakadályozó eszközök[125], de ide sorolhatók a loggyűjtő és elemző rendszerek, de ide tartoznak a korábban már említett viselkedésalapú védelmi eszközök (sandboxok, végpontvédelmi eszközök stb.) is. Szintén a biztonsági kizárásokat szolgáló elemek közé sorolhatók a nem kívánt oldalak, tartalmak elérését korlátozó, internetes szűrést szolgáló rendszerek, de a fájlok integritását ellenőrző eszközök is. Ugyancsak ide tartoznak az adathordozók adatmentesítését szolgáló eszközök, de a belső támadások kizárását, észlelését szolgáló elemek, mint például a kiemelt jogosultsággal rendelkező felhasználó felügyeletét ellátó rendszerek, vagy a hordozható eszközök távoli felügyeletét ellátó rendszerek (pl. MDM[126]) is. A fentieken felül a sérülékenységmenedzsment összes eleme (pl. sérülékenységvizsgálatok, javítófolt vagy angol nevén patch menedzsment, a sérülékenység kihasználását ellehetetlenítő elkerülő megoldások alkalmazása stb.) szintén ide sorolandó. Ugyancsak itt kell megemlíteni a biztonsági információk és események kezelésére szolgáló eszközöket[127], amelyek különböző forrásokból gyűjtött eseménynapló-adatok valós idejű elemzését a szokatlan tevékenységek azonosítását és bizonyos védelmi intézkedések azonnalos megtételét biztosítják, vagy a kibervédelmi elemek tevékenységét felülről felügyelő és irányító eszközrendszereket az ún. SOAR-t[128].

4.4.2. Biztonságos beengedések

A biztonságos beengedések alkategóriába azok a védelmi kontrollok található, amelyek azt biztosítják, hogy az arra jogosultak, jogosultsági szintüknek megfelelően férjenek hozzá az adott vállalat, intézmény adataihoz, információihoz. A gyakorlatban ez azt jelenti, hogy az itt alkalmazott védelmi kontrollok biztosítják azt, hogy azok a belső munkatársak vagy külső közreműködők, akiknek bármilyen tevékenységet kell végeznie az adott rendszerben, legyen az felhasználói, üzemeltetői, megfelelően azonosításra kerüljenek, a szükséges jogosultságaik pedig kiosztásra kerüljenek. Ezek a kontrollok biztosítják, hogy az adott személy csak és kizárólag a számára szükséges minimum

[124] Pre: preventive, De: detective, Co: Corrective angol hármas rövidítéséből

[125] angolul IDS: Intrusion detection systems, IPS: intrusion prevention systems

[126] MDM: Mobile Device Management

[127] angolul: SIEM: Security Information And Event Managegement

[128] SOAR: Security Orchestration, Automation, and Response

jogosultságokkal rendelkezzen, csak azokhoz az adatokhoz, információkhoz férjen hozzá, amely a munkájához elengedhetetlen, azokat viszont biztosan és főleg biztonságosan elérhesse és használhassa.
A biztonságos beengedések eszközei közé tartoznak a hozzáférésvezérléshez szükséges elemek, amelyek megadják, hogy KI? MIHEZ? és HOGYAN? férhet hozzá. A hozzáférésvezérlésnek négy alaplépése van, amelyek a következők. Az első az azonosítás (Identification), amely a „Kivagy?" kérdésre adja meg a választ. A második a hitelesítés (Authentication), amely a „Valóban az vagy-e?" kérdésre felel. A harmadik az engedélyezés vagy felhatalmazás (Authorization), amely a „Van-e jogod hozzá?" kérdésre válaszol, azaz itt történik a jogosultságok megadása és felügyelete. Végül a negyedik az elszámolás vagy könyvelés (Accounting), ami a „Mi történt (vagy fog történni)?" kérdésre ad feleletet, azaz itt történik a hozzáférések naplózása a biztonsági audithoz, vagy akár a pénzbeli elszámoláshoz is.
A biztonságos beengedéseket szolgáló elemekhez tartoznak a hitelesítenél használt eszközök és rendszerek, legyenek azok tudás alapúak (pl. jelszavak, PIN kódok stb.), tulajdon alapúak (pl. hard vagy soft tokenek, proximity kártyák stb.), tulajdonság alapúak (pl. ujjlenyomat, arc, retina stb.), vagy viselkedés alapúak (pl. aláírásdinamika, járásmód, szóhasználat stb.). A jogosultságkezelésnél használt eszközök ellenőrzik, hogy az azonosított entitás a biztonsági házirend és a saját jellemzői alapján rendelkezik-e elégséges jogosultsággal a kért erőforrás használatához. Az elérés kritériumai függhetnek szerepköröktől, csoporttagságtól, helytől, időtől, vagy akár az adott tranzakció típusától is.
A hozzáférés vezérlések esetében négy jellemző modellel dolgoznak a rendszerek. Az első a kötelező hozzáférés-vezérlés[129] modell, amely esetén a hozzáféréseket a rendszer előre meghatározott szabályok alapján engedélyezi, az entitások nem szólhatnak bele még az általuk birtokolt erőforrások elérésébe sem. Ez a legszigorúbb szintű szabályozás, de nagyon alapos előzetes tervezést és komoly adminisztrációt igényel. A második az ún. diszkrecionális, belátáson alapuló v. önkényes[130] modell. Ebben az esetben a felhasználók saját adataikhoz a hozzáféréseket saját belátásuk, azaz „diszkréciójuk" alapján határozzák meg. Ez a modell igényli a legkisebb adminisztrációt, így ebből a szempontból ez a legkényelmesebb megoldás, de az emberi hibák okán ez egyben a legsérülékenyebb is. A harmadik a szerepkör alapú[131], vagy más néven nem-diszkrecionális hozzáférés-vezérlési modell. Ennél a modellnél az egyes adott szerepkörök tagjai azonos jogosultsággal rendelkeznek. Végül a negyedik a szabályrendszer alapú[132] modell, amelyben a hozzáféréseket a rendszergazdák által meghatározott szabályok vezérlik. Ezekről a későbbiekben még részletesen lesz szó.
A legtöbb kibertámadás egyik leglényegesebb eleme az emelt szintű jogosultságok megszerzése és azután az azokkal történő visszaélés, legyen az külső támadó, vagy akár rossz szándékú belső munkatárs. Éppen ezért a kiemelt felhasználók felügyeletének kiemelt szerepe van a védelemben. Ezek azok az eszközök, amelyek a kiemelt jogosultságú felhasználók tevékenységének valós idejű felügyeletét, monitorozását ellátják, akár olyan szintig, hogy azok teljes tevékenysége videófolyamként rögzítésre

[129] angolul: Mandatory Access Control (MAC)

[130] angolul: Discretionary Access Control (DAC)

[131] angolul: Role Based Access Control (RBAC)

[132] angolul: Rule Based Access Control (RBAC)

kerül és így utólag teljes mértékben visszajátszhatóvá válik. Ezek is részletesebben kifejtésre kerülnek a későbbi, a biztonságos beengedésekről szóló fejezetben.

4.4.3. Üzleti, IT kockázatmenedzsment

Amíg a biztonsági kizárások és a biztonságos beengedések alkategóriákba a kibervédelmet közvetlenül érintő eszközök, rendszerek tartoznak, addig az üzletvezérelt információbiztonság harmadik alappillérét alkotó üzleti, IT kockázatmenedzsment közvetetten gyakorol hatást a kibervédelemre. Minden gyakorlati védelem alapja a kockázatokkal arányos védelem kialakítása, ám ehhez először is az adott intézmény, vállalat szempontjából fel kell mérni a releváns kockázatokat, azokat értékelni kell, meg kell határozni melyek az elfogadható szintűek és melyekre kell védelmi intézkedéseket hozni az előbb említett két alappillér megfontolásai mentén.
Az üzleti, IT kockázatmenedzsment kapcsán három nagyobb csoportot különíthetünk el, ezek az ún. GRC modell mentén megjelenő:

- G: Governance (irányítás);
- R: Risk (kockázatok);
- C: Compliance (megfelelés)

kérdéskörei.
Governance vagy irányítás kapcsán az adott szervezet meghatározza az információbiztonsági célkitűzéseket (objectives), ehhez igazítva elkészíti a szükséges irányelveket és szabályzatokat (policies). A vezetés különböző szintjei ezen irányelvek mentén hozzák meg a döntéseiket a saját hatáskörüknek megfelelően, de a felsővezetés sincs abban a helyzetben, hogy a lefektetett irányelvektől eltérhessen.
Risk vagy kockázatok kapcsán szükséges a jól ismert kockázatkezelés lépéseit megvalósítani. fel kell mérni azokat a belső és külső befolyásoló tényezőket, amelyek bizonytalanná teszik, hogy elérik-e, illetve mikor érik el a céljaikat a szervezetek, ezeket a forrásokat azonosítani, elemezni, értékelni, majd kezelni kell. Ez utóbbi lehet a kockázatok elkerülése, felvállalása (tudatos döntéssel!), megosztása, a kockázatforrás eltávolítása, a bekövetkezési valószínűség csökkentése vagy a következmények megváltoztatása.
Compliance vagy megfelelés témakörébe tartoznak az üzletvezérelt biztonság jogi, megfelelőségi hatás kapcsán már említett külső szabályzóknak való megfelelés mellett a belső szabályzók (pl. informatikai biztonságpolitika, informatikai biztonsági stratégia, Informatikai Biztonsági Szabályzat stb.) elkészítése és alkalmazása, valamint az adott szervezet által használt infokommunikációs rendszerekben lévő komponensek tekintetében a kötelezően vagy szervezeti döntés alapján alkalmazott termékbiztonsági előírások (pl. Common Criteria (CC)) következetes betartása.
Az üzleti, IT kockázatmenedzsment kérdéskörei is részletesebben kifejtésre kerülnek a következő fejezetekben.

Felhasznált irodalom

Muha Lajos – Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése. 2018. Nemzeti Közszolgálati Egyetem.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény

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 szóló 41/2015. (VII. 15.) BM rendelet

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról.

Felkészülés az adatvédelmi rendeletre. https://www.adatvedelmirendelet.hu/adatvedelmi-rendelet/

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény

A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény

Az elektronikus hírközlésről szóló 2003. évi C. törvény

RSA Summit Rome 2018. előadásainak anyagai

5. Logikai védelem a gyakorlatban- Kizárások és beengedések

Az informatikai rendszerek védelme a három alapelv mentén szokták megfogalmazni. Ezen hármas a rendelkezésre állás, bizalmasság, sértetlenség biztosítása. Amikor gyakorlatban kezdünk el egy védelmet tervezni, akkor ezen hármas mellett nagyon nehéz ezt megtennünk, mivel a védelem szempontjából ezen alapelvek kevésbé szétválaszthatóak, ez kimondottan igaz a sértetlenség és a bizalmasság viszonyára, mivel mindkét esetben a elektronikus információs rendszer hozzáféréséről beszélünk csak a hozzáférés módja eltérő, bizalmasság biztosításakor elsősorban a láthatóság korlátozása a cél, sértetlenség biztosítása esetén, pedig a látható adatok módosításának kontrollja a feladat – nagyon ritka azon esetek száma, ahol a láthatóságot nem, de a módosíthatóságot biztosítani kell. Nagyon kevés az olyan fizikai, logikai, adminisztratív kontroll, amely tisztán külön-külön biztosít védelmet a két alapelv biztosításához.
A rendelkezésre állás biztosítása jelentősen eltér kontrollok, védelmi lehetőségek tekintetében a bizalmasság/sértetlenség biztosításához szükséges eszközrendszertől. Általánosságban elmondható ugyanakkor, ha rendelkezésre állás nincs biztosítva, akkor a bizalmasság, sértetlenség sem értelmezhető, mivel az adott informatikai rendszer nem elérhető, akkor általában nem tud a bizalmasság, sértetlenség elve sem sérülni. Természetesen ez alól lehetnek kivételek, például egy sikeres kibertámadás esetén, ahol a rendszer üzemeltetőit kizárják a rendszerből, de ez szerencsére nem túl gyakori eset.
Gyakorlati szempontból létezik egy másik megközelítés, amely a kizárások és beengedések eszközeivel élve tudja leírni egy információs rendszer védelméhez szükséges kontrollokat. Ennek a megközelítés alapja, hogy zárjuk ki azokat, akiket nem szeretnénk az információs rendszerben látni, ugyanakkor biztosítsuk a rendszer megfelelő szintű elérését azok számára, akik az adott pillanatban jogosultak a rendszer elérésére, azon a szinten, ahogy a jogosultságuk engedi. Ezen megközelítés mellett a három alapelvnem történő megfelelés könnyen biztosítható.
Az elkövetkező fejezetekben részletesen leírásra kerülnek a legfontosabb logikai védelmi megoldások, amelyekkel hatékonyan biztosítható egy elektronikus rendszer védelme. Fontos azonban megjegyezni, hogy a védelmi eszközök számossága, fajtái nagymértékben függ vagy függhetnek az információs rendszer védelmi szintjétől.

5.1. Biztonságos kizárások

A biztonsági kizárások alkategória azon védelmi kontrollokat foglalja magába, amelyek azt szolgálják, hogy illetéktelenek ne férhessenek hozzá az adott vállalat, intézmény adataihoz, információihoz és/vagy azokat ne módosíthassák és/vagy törölhessék és/vagy ne vihessen be adatokat, információkat, és/vagy ne tehessék azokat elérhetetlenné a jogosultak számára, ne legyenek képesek a rendszer működésének gyengítésére, korlátozására vagy akár teljes leállítására. A gyakorlatban ez azt jelenti, hogy az itt alkalmazott védelmi kontrollok biztosítják azt, hogy a külső támadókat kizárjuk az adott szervezet rendszereiből, megakadályozzuk az azokba történő behatolást, amennyiben ez mégis megtörténik, akkor a lehető leghamarabb észre vegyük azokat, meg tudjuk akadályozni a további ténykedést, a lehető leghamarabb képesek legyünk enyhíteni az okozott károkat, felmérni a támadás részleteit és visszaállítani az eredeti állapotot. De ehhez hasonlóan a belső támadók káros tevékenységének a felderítését, megakadályozását stb. ugyanígy biztosítják.
A biztonsági kizárások eszközrendszerébe tartoznak a védekezés különböző szintjein, így például az adat, az alkalmazás, szerverek, a hálózat stb. szintjein megjelenő azon védelmi

elemek, amelyek a fent leírtakat szolgálják. Ezek lehetnek a PreDeCo[133] elv szerinti prediktív (azaz megelőző), detektív (azaz érzékelő, megfigyelő), korrektív (azaz elhárító) intézkedések megtételéhez szükséges kontrollok egyaránt. A biztonsági kizárások természetesen lehetnek fizikai, adminisztratív és logikai elemek is, itt a következőben a logikai elemekkel foglalkozunk részletesebben.
A biztonsági kizárásokat szolgáló elemek lehetnek aktívak vagy passzívak. Az aktív elemek azok, amelyek megelőző támadásokat, ellentámadásokat vagy az aktív megtévesztést szolgálják. Ezek közül a vizsgált téma szempontjából csupán az aktív megtévesztés az érdemleges, megelőző vagy válaszcsapást ugyanis csak speciális jogosítvánnyal rendelkező szervezetek tehetnek, ez viszont nem tárgya jelen könyvnek. Aktív megtévesztést szolgáló eszközökre jellemző példa az ún. Honeypot amely egy szándékosan gyenge védelemmel ellátott rendszer, amely a támadók tevékenységének rögzítésére szolgál. A passzív védelmi elemek közé tartoznak a szabály/szignatúra vagy anomália alapú védelmi eszközök, mint például a „klasszikus" kibervédelmi eszközök, így például a tűzfalak, vírusírtók, a behatolás érzékelő és megakadályozó eszközök[134], de ide sorolhatók a loggyűjtő és elemző rendszerek, de ide tartoznak a korábban már említett viselkedésalapú védelmi eszközök (sandboxok, végpontvédelmi eszközök stb.) is. Szintén a biztonsági kizárásokat szolgáló elemek közé sorolhatók a nem kívánt oldalak, tartalmak elérését korlátozó, internetes szűrést szolgáló rendszerek, de a fájlok integritását ellenőrző eszközök is. Ugyancsak ide tartoznak az adathordozók adatmentesítését szolgáló eszközök, de a belső támadások kizárását, észlelését szolgáló elemek, mint például a kiemelt jogosultsággal rendelkező felhasználó felügyeletét ellátó rendszerek, vagy a hordozható eszközök távoli felügyeletét ellátó rendszerek (pl. MDM[135]) is. A fentieken felül a sérülékenységmenedzsment összes eleme (pl. sérülékenységvizsgálatok, javítófolt vagy angol nevén patch menedzsment, a sérülékenység kihasználását ellehetetlenítő elkerülő megoldások alkalmazása stb.) szintén ide sorolandó. Ugyancsak itt kell megemlíteni a biztonsági információk és események kezelésére szolgáló eszközöket[136], amelyek különböző forrásokból gyűjtött eseménynapló-adatok valós idejű elemzését a szokatlan tevékenységek azonosítását és bizonyos védelmi intézkedések azonnalos megtételét biztosítják, vagy a kibervédelmi elemek tevékenységét felülről felügyelő és irányító eszközrendszereket az ún. SOAR-t[137].

5.2. Védelmi rendszerek csoportosítása

A védelmi rendszerek működése szempontjából számos csoportosítási lehetőség van. Ezen csoportosítási lehetőségek elsősorban asz eszközök szerepe, működési módja határozhatja meg, ugyanakkor szinte mindegyik védelmi eszköznek van olyan funkciója, ami a csoportosítás egyik csoportjába, míg a másik funkció a másik csoportba tehető be.

[133] Pre: preventive, De: detective, Co: Corrective angol hármas rövidítéséből

[134] angolul IDS: Intrusion detection systems, IPS: intrusion prevention systems

[135] MDM: Mobile Device Management

[136] angolul: SIEM: Security Information And Event Managegement

[137] SOAR: Security Orchestration, Automation, and Response

5.2.1. A védelem fázisai szerint csoportosítás: preventív, detektív, korrektív

Ez informatikai rendszer védelme trichotom, azaz három jól elkülöníthető részre osztható. Az információs rendszer kialakításakor és üzemeltetése során törekedni kell a rendszer ellenállóképességének minél magasabb szintre fejlesztésével. Ezt úgy tudjuk elérni, hogy hatékony preventív, detektív és korrektív kontrollokat, tevékenységeket alkalmazunk a védelem során.
A preventív intézkedések vagy kontrollok célja, hogy a támadók nem férjenek hozzá az információs rendszerhez, az abban tárolt adatokhoz, azaz kerüljön megelőzésre egy sikeres támadás. Amennyiben a preventív kontrollok jól működnek, úgy a rendszer ellenálló a támadásokkal, üzemzavarokkal szemben. Preventív kontrolok például a fizikai behatolást megakadályozó eszközök, a különféle adminisztratív kontrollok (például tudatosítás), illetve azon logikai kontrollok, amelyek képesek felismerni egy támadást és be is tudnak avatkozni, azaz megakadályozzák a támadás sikeres lefutását.
Bármennyire is szeretnénk, de egy kibertámadás sok esetben nem előzhető meg, egyrészről mert mindig lesznek, másrészről mindig lesz olyan támadó, aki ki tudja cselezni a védelmi rendszert. Itt lépnek be azon védelmi eszközök, amelyek detektálni tudják a támadást, azaz látnak, de nem tudnak beavatkozni (például biztonsági naplógyűjtő és elemző rendszer).
Amennyiben a kibertámadás detektálásra került, úgy már „már csak” be kell avatkozni és meg kell akadályozni a támadás kiterjesztését, a további károk okozását. A korrektív védelmi eszközök ezen cél teljesítésében nyújtanak segítséget.

5.2.2. Beavatkozási képesség szerint: beavatkozó vagy monitorozó

A védelmi rendszer alapvetően kétfajta üzemmódban tudnak működni. Vagy monitoroza a felügyelt rendszert vagy be is avatkozik, amennyiben káros tevékenységet észlel. Komplex védelmi rendszerek esetén (például végpontvédelem, vagy különféle behatólás detektáló eszközök) elképzelhető, hogy bizonyos tevékenység esetén blokkol a rendszer, más esetekben pedig csak jelzést küld a beállított szabályoktól függően.
Amennyiben egy eszköz nem avatkozik be, úgy az incidenskezelés során ez többlet feladatot jelent a kibervédelmi szakemberek számára, ugyanakkor egy automatikus beavatkozásnak is lehetnek olyan hatásai, amelyek nem kívántak (például téves detektálás esetén).

5.2.3. A védelmi módja szerint: aktív, passzív

A két megközelítés között a fő különbség, hogy míg aktív esetén a védekező egyben végrehajt valamifél támadás vagy megtévesztést, addig a passzív védelem esetén a védekező fél kontrollokat üzemeltet, amelyek megakadályozzák a támadást. Aktív védelem esetén a védekező fél:

- megelőző támadást indíthat
- ellentámadást indíthat
- illetve élhet a megtévesztés eszközével.

Az első kettő képesség alkalmazása csak és kizárólag jogszabályban meghatározott szervek számára biztosított hazánkban, viszont az aktív megtévesztést bárki alkalmazhat.

A megtévesztés célja kettős lehet, egyrészről a támadás lassítása, másfelől a támadási technika feltérképezése (mindkét célt csapdarendszerek telepítésével és üzemeltetésével lehet elérni).
A passzív védelmi megoldások közé azon kontrollokat soroljuk, amelyek egy támadás megelőzésére, detektálására, vagy a beavatkozásra szolgálnak, legyen szó adminisztratív, logikai vagy fizikai kontrollokról.

5.3. Az észlelés módja szerint mintaillesztés alapú, anomália detektálás alapú

5.3.1. Mintaillesztés

A hagyományos védelmi eszközök alapvetően mintaillesztés metodikáját használják ahhoz, hogy az adott erőforrás elérhető az entitás számára vagy sem. Ebben az esetben létezik egy minta, amihez történő illeszkedést vizsgál a védelmi eszköz. Ha a minta illeszkedik a vizsgált adathoz, akkor a rendszer működésétől függően vagy beengedi az entitást, vagy kizárja. Ilyen megoldást alkalmaznak például a hagyományos tűzfalak, amelyek egy forrás címet és portszámot hasonlítja össze a tűzfal adatbázisában lévő adatokkal. Amennyiben talál egyezőséget, úgy a konfigurációnak megfelelően vagy beengedi a forgalmat, vagy nem. Amennyiben nincs illeszkedés, akkor is a tűzfal konfigurációja dönti el, hogy beengedje-e a forgalmat vagy sem. Az, hogy milyen konfiguráció kerül beállításra, nagymértékben függ a védett szolgáltatástól, illetve az elérés korlátozásának szigorától. Nyilván más szabályrendszert kell beállítani egy publikus internetoldalhoz, mint egy nagyon védett rendszerhez.
Egy másik gyakori példa a mintaillesztésre a vírus vagy káros kódok elleni védelem hagyományos módja, ahol egy vírus adatbázis tartalmát hasonlítja össze a védelmi rendszer a vizsgált állománnyal.
Ennek a metódusnak előnye, hogy rendkívül gyors, és „biztosít” döntést tud hozni, hátránya ugyanakkor, hogy a minta adatbázist fel kell építeni és karban kell tartani, a nagy adatbázis használata például performanciális problémát okozhat. Az adatbázis optimalizálása miatt előfordulhatnak például olyan esetek, hogy egy régi vírus az adatbázisból kikerülve újra éledhet. További hátrány, hogy nem ismert minta esetén a védelmi rendszer nem biztos, hogy megfelelően tud működni, amire jó példa egy új vírus megjelenése, amely addig nem lesz detektálva, amíg annak valamely része nem kerül be az adatbázisba.
Az előző két példa konkrét adatbázisban meglévő adatot hasonlít össze más adattal, de vannak olyan védelmi eszközök is, amelyek egy eseménysorozatot hasonlítanak össze az adatbázisban lévő leírásokkal.
A mindennapjainkban a mintaillesztés a leggyakrabban használt technológia, a fenti mintákon kívül például ilyen módszert alkalmazunk a hitelesítés folyamat során is.

5.3.2. Anomális felismerésén alapúló detektáció

A mintaillesztésen alapú védelmi rendszerek gyengeségeinek kiküszöbölésére lehet alternatíva a viselkedésű alapú rendszerek. Akár a hozzáférés biztosításakor, káros emberi tevékenység detektálásakor akár egy állomány lefuttatása nem egy mintaadatbázisban keresi az egyezőségeket, hanem egy előre definiált szempontrendszer szerint értékeli a tevékenységet kockázati alapon. Ezen működés szemléltetésére jó példa lehet, egy dokumentum megnyitásának folyamata. Általában egy dokumentum megnyitása a dokumentum szerkesztéséhez használt programot hívja meg – ez általában még nem tekinthető gyanús esetnek, de amikor ez a dokumentum megnyitása után elkezd

kommunikálva a világgal és még le is szeretne tölteni valamit, akkor az már mindenképpen vizsgálandó esemény, ha pedig elkezd egy olyan céllal kommunikálni, amelyet korábban még nem volt, akkor az már majdnem biztosan biztonsági incidens. Egy tevékenység kockázatát általában a támadók által használt technikák figyelembevételével szokták „meghatározni".
A viselkedés alapú detektációnak előnye, például, hogy korábban nem ismert támadásokat lehet detektálni, ugyanakkor az esetek jelentős részében nincs biztos verdikt, csak valószínűség, hogy történik valami nem kedvező.
Ezen védelmi megoldás jellemzően valamilyen mesterséges intelligencia ágat használnak a védelem biztosítására, azaz képesek tanulni és a tanulási tevékenység manipulásával akár rosszra is taníthatóak a rendszerek, de ezek jóval hosszabb folyamtok, mint egy új mintájú káros kód legyártása. Hátránya tovább ezen rendszereknek, hogy a folyamatos figyelés és kockázatszámítás jelentős erőforrást igényel.
Elsősorban hálózati forgalom elemzésére, illetve elektronikus levelezés védelmére úgynevezett sandbox-ot szoktak használni, amely célja, hogy az esetleges káros tartalmat megvizsgálja, annak szeparált környezetben történő (sanbox) futtatásával.

5.3.3. Védelmi eszközök

Az informatikai rendszerek védelme számos egymásra épülő eszköz együttes használatával biztosítható. A védelem ugyanakkor csak akkor tud hatékony lenni, ha a már a rendszer kialakításakor megfelelő ellenállási képesség (reziliencia) kialakításra kerül. A legjobb védelmi üszkökkel sem, vagy csak nagyon drágán lehet megvédeni egy számos gyengeséggel rendelkező rendszert.
A következő fejezetekben kerülnek bemutatásra azon védelmi eszközök, amelyek minimálisan szükségesek egy információs rendszer védelmének biztosításához.

5.3.4. Határvédelmi rendszerek

Egy vállalat, egy információs rendszer legfontosabb határvédelmi eszköze a tűzfal. Ahogy az egyes védelmi eszközök egyre több feladatot látnak el, úgy a napjainkban használt tűzfalak is sok új funkcióval rendelkeznek a kezdetekben megalkotott funkciókhoz képest.

5.3.5. Túlterheléses támadások elleni védelem

Napjaink egyik legelterjedtebb támadási vektora a túlterhelés támadás. Ezen támadás jellemzően a rendszerek elérhetőségét, rendelkezésre állását hivatott megvalósítani. Korábban a túlterheléses támadások elleni védelmet tűzfalakkal, behatolás megelőző eszközökkel, alkalmazástűzfalakkal valósították meg. Napjainkra azonban ez a helyzet megváltozott, megszülettek azon eszközök, amelyek kimondottan ezen támadási vektorok ellen nyújtanak védelmet, jellemzően azonban a hatékony túlterheléses támadások elleni védelem a korábban is használt eszközökkel együttesen valósítható meg. A túlterheléses támadások elleni védelmet biztosító eszközöknek egyrészről kezelni kell az úgynevezett volumetrikus támadásokkal szemben, de biztosítani kell kommunikációs protokollok kihasználó támadásokkal szemben is. A helyi túlterheléses támadások mellett, akár azt kiváltva lehetőség van felhő alapú védelmi képesség bevezetése, akár úgy is, hogy a szolgáltatás „földi" környezetben kerül biztosításra, de akkor is, ha a szolgáltatás maga is a felhőben fut.

5.3.6. Behatolás detektáló, megelőző eszköz

Az internet irányú támadások felismerésére és/vagy megakadályozására szolgálnak
Internet forgalom korlátozásának lehetősége

5.3.7. Káros kódok elleni védelem

A káros kódok elleni védelem a hagyományos megközelítéssel ellentétben nem akkor kezdődik, amikor azt a káros állományt le szeretnénk futtatni, hanem már a kód bejutását szeretnénk megakadályozni. A védelem folytatódik akkor is, amikor lefut a káros kód és elkezdi a tevékenységét. és akkor fejeződik be, amikor az incidens lezárásra kerül.

5.3.8. Hálózati forgalom elemző eszközök

A hálózati forgalom elemző eszközök a védett környezetek forgalmát hivatottak felügyelni, káros forgalom esetén akár beavatkozni, blokkolva a káros tevékenységet. A forgalom vizsgálat kiterjedhet az adott hálózati szegmens belső forgalmára, az egyes szegmensek közötti fogalomra, illetve a kifele Menő/befele jövő forgalomra.

5.3.9. Elektronikus levelezés védelem

Napjainkra az elektronikus levelezés lett a leggyakrabban használt kommunikációs eszköz (az instant üzenetküldők után), amely könnyű lehetőséget biztosít bárki számára, hogy kéretlen üzeneteket küldjön számunkra. Az üzenetek jelentős része valamilyen termék vásárlására, szolgáltatás igénybevételére ösztönöz, ugyanakkor ezen levelek között számos esetben találhatunk károsnak minősített levelet, amelyek közvetlenül adataink megszerzésére vagy káros program telepítésére próbálják rávenni a gyanútlan felhasználót. A marketing célú és az ismert vírusokat tartalmazó levelek eljutását a felhasználóhoz az úgynevezett spam és vírus szűrők hivatottak megakadályozni, amelyek jellemzően mintaillesztés segítségével próbálják kiszűrni a káros tartalmat.
Az új és/vagy célzott támadások ellen azonban ezen eszközök nem nyújtanak védelmet, mivel nem rendelkeznek a káros kódról semmilyen információval. Ahhoz, hogy ezen támadások elleni védelem is biztosít vagy legyen további védelmi megoldásokat célszerű bevezetni. Ilyen eszközök lehetnek a különböző viselkedési anomáliákat vizsgáló eszközök. Ezen eszközök vizsgálata az elektronikus levél mellékleteként kapott állomány megnyitásakori tevékenységének vizsgálatára és/vagy a levélben levő hivatkozások mögött weboldal viselkedésére irányúl. Amennyiben ezen vizsgálat eredménye pozitív, úgy a védelmi eszköz beállításától függően jut el a levél a címzetthez vagy kerül a levél karanténba.
Működésükből fakadóan ezen eszközök is rendelkeznek gyengeségekkel, amelyek miatt önmagukba nem képesek az elektronikus levélben beérkező káros tartalmak teljeskörű szűrésére, ilyenek például amikor a hivatkozott oldal tartalma a vizsgálat időpontjában még nem káros (például egy éjféli levél beküldésnél), de a levél megnyitásakor másnap reggel már az, vagy olyan viselkedési mintát tartalma, ami még nem teszi gyanússá és csak később derül ki, hogy ténylegesen az. Ezen gyengeségek kiküszöbölésére a gyártók számos technikát alkalmaznak.

5.3.10. végpontvédelem

A tűzfalak után talán a legrégebbi és legszélesebb körben használt védelmi megoldás. A védelem célja a végpontokon zajló káros tevékenységek felismerése és lehetőség szerint megakadályozása. A hétköznapi életbe a „vírusvédelemet" egyenértékűnek szokták tekinteni a végpontvédelemmel, de ezek a megoldások többet szoktak biztosítani, például

- exploitok elleni védelem, zsroló virusok elleni védelem
- kód injektálás elleni védelem
- host alapú tűzfal funkcionalitás
- böngészési adatok, kódok vizsgálata
- alkalmazás engedélyezés/tiltás funkciók

Bár a funkcionalitás látszólag elég széles védelmet nyújt, de hamis biztonságérzetet ad, mivel a vírusvédelem jellemzően mintaillesztés alapon működik, amely a fejlett (célzott) támadásokkal szemben kevésbé nyújt védelmet. Vállalti környezetben javasolt azonban olyan végpontvédelmi megoldás használata, amely egyrészről képes a fejlett támadások felismerésér, másrészről hatékonyan tudja támogatni az incidenskezelési tevékenységet. A hagyományos végpontvédelmi megoldásokat Endpoint protection platform (EPP), a fejlett támadások elleni megoldást Enpoint detection and response (EDR) hívjuk.

5.3.11. Integritás védelem

Az integritás védelem célja a felügyelt rendszer működése szempontjából fontos állományok változásának figyelése. Amennyiben például egy konfigurációs állomány módosul, de annak oka nem ismert (például nem történik rendszer karbantartás), az nagy valószínűséggel biztonsági incidens. A védelmi képesség hasznossága akkor aknázható ki igazán, ha a szervezet megfelelő változáskezelési folyamattal rendelkezik, azaz, amikor az integritás ellenőrző rendszer integrálva van változáskezelő rendszerhez és gyorsan el lehet dönteni, hogy egy változás jogos vagy támadók hajtották végre.

5.3.12. Adatszivárgás elleni védelem

Az adatszivárgás elleni védelem (Data Lost/Leak Prevention, azaz DLP) célja, hogy megakadályozza a vétlen vagy szándékos adatszivárgást. Vétlen adatszivárgás klasszikus példája, amikor egy levél címzettjei közé felveszünk valakit, akivel szándékunk szerint nem akartuk megosztani az információt, de ilyen eset az is, amikor elvesztünk egy adathordozót – ilyen esetekről már mindenki hallott, vagy lehetnek tapasztalatai. Mivel az adatszivárgás többféle módon is megtörténhet, így a megelőzéshez is összetett eszköz, kontrollrendszer szükséges.
Az adathordozók általános – adatkörtől független - védelmét, legyen szó egy munkaállomásban lévő meghajtóról, vagy külső adathordozóról titkosítással lehet az egyik leghatékonyan módon megtenni, feltéve, ha a titkosítás feloldásához szükséges kulcsot nem együtt tároljuk az adathordozóval, szigorúbb megoldás lehet, hogy a szervezet logikai úton megakadályozza a külső adathordozó csatlakoztatását a munkaállomásokhoz.
Az adathordozók védelmén kívül természetesen oda kell figyelni az egyéb lehetséges kommunikációs csatornákra, mint az internet, az azon nyújtott szolgáltatások (például otthoni storage, felhő alapú fájlmegosztók, publikus email szolgáltatók, instant üzenetküldő szolgáltatások, információ megosztására alkalmas szolgáltatások (Instagram, twitter, telegram stb.), illetve a vállalat által biztosított levelező szolgáltatás

is. Természetesen az adatszivárgás megelőzésének vannak szofisztikáltabb megoldásai. Ezen megoldások bevezetése és működtetése azonban jelentős feladatot ró a szervezetre. Talán a legfontosabb és a legnehezebb is annak meghatározása, hogy milyen adatvagyonnal rendelkezik a szervezet és az adatvagyon részeit képező egyes adatokat miként kell védeni. Ha a szervezet tisztában van azokkal az adatkörökkel, amelyeket védeni szeretne, akkor már csak fel kell állítani azt a szabályrendszert, amellyel ezen adatok szivárgása korlátozható, ilyen szabály lehet például, amikor a szervezeten kívülre nem küldhető olyan dokumentum, amelynek besorolása „Belső használatra", de szervezeten belül szabadon továbbítható.

5.3.13. Mobil eszköz védelem

Manapság egyre elterjedtebb, hogy a felhasználók mobil eszköz segítségével érik el a szervezet rendszereit (például levelezés, informatikai szolgáltatások). Ilyen eszközök elsősorban a mobil telefonok, tabletek, laptopok védelmét szoktuk érteni, általában a külső adathordozók védelmét nem. A védelem célja, hogy az elveszett vagy eltulajdonított eszközről illetéktelen személyek ne tudjanak adatot megszerezni.
A különböző gyártók többféle megoldást alkalmaznak, amelyet a szervezet számos módon tud konfigurálni. A funkció megvalósítása valamiféle konténer segítségével történik, amely konténer lehet maga a mobil eszköz, de lehet annak csak egy része is. A szervezet dönti el, hogy a konténerben milyen szolgáltatásokat ajánl ki, azaz a felhasználó milyen vállalati erőforrásokhoz fér hozzá (első lépésként a levelezést szokták bevezetni, ma is, majd később olyan szolgáltatásokat, amelyek vállalati információt nyújtanak vagy éppen megkönnyítik a felhasználók napi tevékenységét).
Ezen védelmi megoldások nyújthatnak segítséget a felhasználó által használt eszközön (Bring your own device, BYOD) lévő vállalati adatok védelméhez is.

5.4. Az informatikai rendszerek biztonsági állapotának tesztelése

Az előző fejezetekben felvázolt védelmi eszközök csak akkor tudnak hatékony védelmet nyújtani, ha a védett informatikai rendszer ellenállóképessége nem megfelelő. Ahhoz, hogy egy információs rendszer önmagában is képes legyen ellenállni valameddig egy kibertámadásnak, számos tevékenység együttese szükséges. Ezen tevékenységek már a rendszer tervezésénél elkezdődik, amikor olyan rendszert „találnak" ki, amelyben bele vannak építve azon kontrollok, amelyek az alapvető támadásokkal szemben nyújtanak védelmet. Ezen kontrollok lehetnek magában az üzleti funkciók megfelelő kialakítása, a különféle beviteli mezők ellenőrzése, de a megfelelő szoftver komponensek kiválasztása és azok biztonsági szempontú beállítása is ebbe a körbe tartozik.
Amikor kész van egy „termék", azaz létrehozása került egy új rendszer vagy egy új komponens egy meglévő rendszerben, akkor annak ellenőrzése, mint a mű élesítése előtti utolsó tevékenység hivatott a pecsét megszerzésére, azaz annak igazolására, hogy a tervezés és az implementáció során maximálisan figyelembe vettük a biztonsági elvárásokat. Ezen tevékenységet szokták sérülékenységvizsgálatnak nevezni, ami bár gyűjtő szó sokféle tevékenységet jelent, jelenthet.
A sérülékenységvizsgálat célját a megrendelő határozza meg az információs rendszer kockázatainak ismeretében. Az NKI alapvetően 4 fajta sérülékenységvizsgálat típust végez:

- *első informatikai biztonsági vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek a során az érintett szervezet informatikai rendszerének sérülékenységvizsgálata a belső hálózati végpontról közvetlenül történik;

- *külső informatikai biztonsági vizsgálat:* az informatikai rendszer internet felőli, külső sérülékenységvizsgálata, amelynek a során az interneten fellelhető, nyilvános adatbázisokban való szabad keresésre, célzott információgyűjtésre, valamint az elérhető számítógépek szolgáltatásainak, sebezhetőségének feltérképezésére kerül sor;
- *webes vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek a során automatizált és kézi vizsgálatok útján kerülnek feltárásra a webes alkalmazások sérülékenységei;
- *vezeték nélküli hálózat informatikai biztonsági vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek a során a vezeték nélküli hozzáférési és kapcsolódási pontok keresése, feltérképezése, titkosítási eljárások elemzése, titkosítási kulcsok visszafejthetőségének ellenőrzése célszoftverek és kézi vizsgálat útján történik.[138]

A fenti csoportosításba tartozó vizsgálatok célja elsősorban az információs rendszerben megkeresni azokat az ismert sérülékenységeket, amelyek már ismertek, azaz nem célja az esetlegesen ismeretlen sebezhetőségek feltárása.
Az ismeretlen sebezhetőségek feltárására a behatolás tesztelést (penetration test) szolták segítségül hívni. Ezen esetben a vizsgálatot végző olyan kódot, technikát alkalmaz, amely akár teljesen au adott információs rendszerre van írva.
Az NKI által végzett vizsgálatok jellemzően jól automatizálhatók, vannak célszoftverek, amelyeket lehet használni, illetve a vizsgálat végén az eredmények megerősítésére szokás manuális ellenőrzéseket végezni, de itt nem cél a rendszerbe történő behatolás. A behatolás tesztelés során az automatikusan vagy manuálisan feltárt sérülékenységek kihasználása a cél, azaz a vizsgálatot végzőnek be kell hatolnia a rendszerbe és ott lehetőség szerint „át kell vennie" az irányítást a rendszer felett.
A vizsgálathoz kapott információk alapján három csoportot különböztethetünk meg:

1. Black box: amikor a vizsgálattal megbízott nem kap semmijen információt a vizsgálandó rendszerről. Ez a módszer áll legközelebb egy valódi támadáshoz, hiszen általában a támadó sem rendelkezik információval a célpontról
2. Gray box: ebben az esetben a vizsgálatot végző kap információt a vizsgálandó rendszerről, esetleg kap bizonyos hozzáféréseket is. Ezzel időt lehet megtakarítani és pontosítható a vizsgálat.
3. White box: a vizsgálatot végző megkapja a rendszer dokumentációját, így a vizsgálat lényegesen rövidebb és pontosabb lehet, nem kell a vizsgálónak a rendszer feltérképezésével foglalkoznia és garantáltan minden rendszerelemre ki fog terjedni a vizsgálat.

Sem a sérülékenység keresés, sem a behatolás tesztelés jellemzően nem tárja fel azon sérülékenységeket, amelyek olyan kódrészletben vannak, amely az alkalmazás során nem fut le például tesztelés után véletlenül benne maradt a kódban vagy a támadó szándékosan helyzete el ott, hogy később, a az alkalmazás használata során használja a sérülékenységet. Ezen sérülékenység vizsgálatára célszerű egy kódellenőrzést végezni.
Az informatikai rendszer gyengeségeinek feltárásának lehetséges módja az úgynevezett bug-bounty program, amely során felhatalmazást kapnak a szervezettel közvetlenül

[138] 71/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól

kapcsolatban nem lévő személyek, hogy megtalálják a gyengeségeket. A bug-bounty program keretében a programot működtető szervezetek pénzdíjat vagy egyéb jutalmat ajánlhatnak fel korábban nem ismert sérülékenységek feltárásáért cserébe. Ilyen programot működtet például a Microsoft, az Apple, a Google, de kevés számmal ugyan de voltak hazai bug-bounty programok, például a Trezorit vagy a Prezi. A bug-bounty programok előnye, hogy akár sokkal olcsóbb is lehet, mint egy hagyományos sérülékenységviszgálat, illetve ha megfelelően magas a felajánlott díj, akkor igazán komoly „támadók" is részt vehetnek a programban, ami növelheti a rejtett hibák feltárásának esélyét, további előny, hogy vélhetően olyan módszereket alkalmaznak a programban részt vevők, mint a valódi támadók. Másrészről egy program megalkotása hossza előkészítést igényel és a résztvevők által beküdött információk ellenőrzése is komoly szaktudást igényel. Kockázatot jelenthet, hogy a programban résztvevők között elbújhatnak valódi támadók, akik tevékenységét nehezebben vagy késleltetve lehet csak észre venni, így az esetleges beavatkozásra is rövidebb idő áll rendelkezésre.
Mind a sérülékenység-vizsgálat, mind a bog-bounty program esetén a vizsgálatot végzők felhatalmazást kapnak a tevékenység végzésére, a különbség mindössze annyi, hogy a sérülékenységvizsgálat esetén konkrét szervezet vagy személy kapja meg a meghatalmazást, így ismert a vizsgáló személye, ellentétben bug-bounty programoknál, amikor is mindenféle kontraktus nélkül végezhető a vizsgálat. Mindkét esetben fontos, hogy pontosan definiálva legyen a vizsgálat scope-ja, illetve a vizsgálatra rendelkezésre álló idő.

5.5. Sérülékenység menedzsment

A sérülékenység vizsgálat egy rendszer adott pillanatban meglévő biztonsági állapotát mutatja, azonban könnyen előfordulhat, hogy néhány, nap vagy hét elteltével megjelenhetnek újabb sérülékenységek, amelyek érinthetik a védendő információs rendszert. Ezen sebezhetőségek megismerése és kezelése kiemelkedően fontos, hiszen a támadók sem tétlenkednek, egy komolyabb sérülékenység napvilágra kerülése után néhány órával akár az egész világon meg tudják nézni, hogy mely rendszerek sérülékenyek. Nagyon fontos, hogy a rendszereinkben meglévő sérülékenységekről minél hamarabb szerezzünk információt. Az információ szerzés történhet automatikus sérülékenységvizsgáló eszközökkel (például az NKI által üzemeltetett ASR-rel), saját sérülékenységvizsgáló rendszerrel, ütemezett – vagy szükség esetén ad-hoc – vizsgálatokkal, illetve különféle sérülékenységi információs szolgáltatásokkal (például cvs vagy az információs rendszer komponensei gyártói oldalainak folyamatos figyelésével.

5.6. Sérülékenység javítása

Az információs rendszerek fejlesztése során számos esetben előfordul, hogy olyan szoftverelemek kerülnek az alkalmazásba, aminek javítása az információs rendszer működésképtelenségét eredményezheti, így a rendszer olyan sérülékenységeket fog tartalmazni, amit támadók ki tudnak használni. Amennyiben a szervezet rendelkezik olyan védelmi megoldással, úgy a rendszer sebezhetőségét helyettesítő kontroll segítségével meg lehet oldani. Elsősorban komplex hálózatok esetén ezen sérülékenységek komoly kockázatot hordozhatnak, mivel az egyes rendszerek integrálása miatt előfordulhat, hogy egy nem átgondolt konfiguráció módosítás (például tűzfalnyitás) megnyithatja az utat a támadó előtt.
Automatikus sebezhetőség vizsgálat

5.7. Biztonság mérése

Az előző fejezetekben elsősorban az információs rendszerek védelmét biztosító eszközökről esett szó, de nem esett szó magának a védelmi eszközök, a védelemhez kapcsolódó folyamatok, illetve a védelem humán aspektusairól. Jelen fejezet célja bemutatni, hogy miként lehet a védelmi ökoszisztéma hatékonyságát mérni. A hatékonyság mérése egyrészről irányulhat arra, hogy a meglévő védelmi eszközrendszer mennyire képes detektálni és megelőzni egy kibertámadást.
A mérés lehet alkalmiszerű, vagy akár folyamatos is, attól függően, hogy milyen eszközrendszer áll rendelkezésre.
Az alkalomszerű vizsgálat során a „támadó" vagy másnéven a red team csapat megpróbálja kompromittálni a célrendszer, amelyet a védekező fél vagy blue team megpróbál detektálni és elhárítani a támadást. Vannak olyan validálást segítő rendszerek, amelyek ezen tevékenységet támogatják, azaz automatikusan indítják a „támadásokat" előre beállított paraméterek alapján, részben vagy egészben leutánozva egy valódi támadó tevékenységét. A fejlettebb validációs eszközök integrálhatók a védelmi eszközökhöz, így egy szimuláció során könnyen kiderülhet, hogy egy védelmi eszköz konfigurációja nem megfelelő és még időben, egy tényleges támadás előtt finomhangolható – ez a funkció kiemelkedően fontos lehet olyan rendszerek esetén, ahol a védelem biztosításához sok manuális munka lehet szükséges például biztonsági naplóelemzés.
A védelemben részt vevők folyamatos képzését teszik lehetővé a különböző online vagy helyi platformok (például a HackTheBox, a TryHackme vagy BlueTeamlabs), de akár a szervezet is működtethet ilyen platformot, igaz ennek napi használatához sok-sok belső erőforrás is szükséges. Amennyiben komplexebb feladattal kívánjuk az elemzők tudását mérni, javítani sokat tudnak segíteni a CTF (Capture The Flag) jellegű „játékok", amellyel vizsgálhatjuk a kollégák felkészültségét, gyorsaságát is.

5.8. Egyéb védelmi funkciók

5.8.1. Adatmentesítés

Az információs rendszer életciklusának utolsó lépése az információs rendszeren tárolt adatok végleges törlése, hogy illetéktelenek ne férhessenek hozzá az adatokhoz, azokat nem tudják használni. Ezt a tevékenységet szokták adatmentesítésnek nevezni.
Az adatmentesítés célja, hogy az adathordozón (például meghajtón, telefonon, virtuális gépen) tárolt adat visszaállíthatatlanul és dokumentáltan törlésre kerüljön. A cél elérhető az adathordozó fizikai megsemmisítésével vagy logikai úton. Nem számít visszaállíthatatlan módon történő törlésnek az adathordozó letörlése (még SHIFT+DEL-el sem), particionálása, gyári beállítás visszaállítása vagy a virtuális gép törlése sem.
A fizikai megsemmisítés történhet az adathordozó tényleges fizikai megsemmisítésével (például ledarálásával, összezúzásával) és/vagy demagnetizálással. Bármelyik eljárást is válasszuk, az adathordozó többet már nem lesz használható.
A logikai adattörlés során az adathordozó teljes tartalma – az eljárástól függően – több alkalommal felülírásra kerül. A felülírások száma és azok randomizált módja adja a törlés visszaállíthatatlanságának „erejét".
Amennyiben auditált/szabványos megoldással történt az adatmentesítés, úgy arról tanúsítást ad ki a adatmentesítést végző.

5.9. Fenyegetettségi információk menedzsmentje

Számos – elsősorban fenyegetettség információ (angolul Indicator of Compromise – IoC) kezelésében jártas - szakértő nyilatkozott úgy az elmúlt időszakban, hogy az operatív

kibervédelem át fog alakulni a mai detektálás alapú incidenskezelésről, az információ alapú incidenskezelésre. Ebben lehet némi igazság, de célzott, az adott szervezetre írt támadás esetén valószínűleg nem lesz előzetes információnk a támadásról, ugyanakkor az is igaz, hogy más támadásokról kapott információk segíthetnek a szervezetet érő támadás megelőzésében.
De nézzük milyen fenyegetettségi információk vannak:

- stratégiai
- taktikai
- technikai

A fenyegetettségi információk forrása lehet kibervédelmi cégektől/fenyegetettség információ szolgáltatótól kapott (ingyenes vagy előfizetéses alapú), publikus weboldalak, fórumok, dark web és minden, ami a kibertérben megtalálható.
A rengeteg napi új információ feldolgozását és megosztását teszik könnyebbé az úgynevezett fenyegetettségi információs platformok (Threat Intelligence Platfrom - TIP). A TIP platformok általában többet tudnak, mint az IoC-k feldolgozása, képesek lehetnek egy incidens során keletkező információk összerakására, akár grafikus ábrázolással, riport készítésével.

5.10. Naplózás

A tűzfalak mellett a legrégebbi védelmi lehetőség az információs rendszerben keletkező eseményekről készült naplóbejegyzések gyűjtése és biztonsági szempontú elemzése. A naplózás az egyik legjobban dokumentált követelmény mind az Vhr.-ben, mind egyéb szabványokban, ajánlásokban az incidensek feltárásának is egyik fontos eleme, ugyanakkor a detektálás szempontjából már nem ennyire egyértelmű a használhatósága.
Amennyiben egy információs rendszer naplózása megfelelő, úgy egy biztonsági incidens minden eleme bekerül a naplóelemző rendszerbe és akár teljes kőrűen kivizsgálható az incidens.
Fontos megjegyezni, hogy a naplózás már megtörtént eseményekről szól, azaz nem alkalmas megelőzésre, illetve korlátozottan alkalmas a támadás első faizásainak megakadályozására. Abban az esetben, ha a naplóelemző rendszer készültek incidens detektálásához szükséges forgatókönyvek (korrelációk vagy más néven use case-ek) és/vagy a naplóelemző rendszer integrálva van fenyegetettségi információ forráshoz, úgy van esély egy támadás időbeni felderítéséhez már a kezdeti fázisokban.
De mit is kell naplózni? A rövid válasz az, hogy mindent, hosszabban, mindent, ami egy biztonsági incidens során releváns információ lehet.

5.11. Naplózási architektúra

Nagyvállalati környezetben a naplózás több rétegből tevődik össze.
Az első naplózási pont maga az információs rendszer vagy annak egy eleme, ahol a naplóállomány keletkezik. Jellemzően ez az a pont, ahol a legtöbb naplóállomány található és ezen naplóállományokat vizsgálják az üzemeltetésben résztvevő munkatársak. A naplók ezen ponton néhány napig, hétig érhetőek el, utána automatikusan törlésre kerülnek.
A második réteg a naplóállományok központi tárolását biztosító naplógyűjtő rendszer. Ide már csak azon naplóbejegyzések érkeznek meg, amelyeket az a rendszer üzemeltetői „átküldenek” ide. Ezen a ponton történik a naplók hosszabb idejű (akár éves vagy azon si túlnyúló) – de nem végleges -tárolása. Ebben a rétegben jellemzően nincsenek fejlett elemzői lehetőségek, de nem is ez a cél, viszont az adatok még relatív gyorsan elérhetők és visszakereshetők, például egy hatósági megkeresés miatt.

A harmadik réteg az adatok külső adathordozón (például szalagos mentőegység) történő tárolása. Innen a mentett adatok csak visszatöltés után érhetőek, el amely hosszabb folyamat is lehet.
Amennyiben a szervezet megfelelő erőforrásokkal rendelkezik, úgy a biztonsági naplózási funkciókat külön naplógyűjtő és elemző rendszer (SIEM – Security Information and Event Management) segítségével végezheti. A SIEM rendszerbe már csak a biztonsági események naplói jutnak el, kerülnek eltárolásra és feldolgozásra. A naplók tárolási idejét a rendelkezésre álló kapacitások és a védendő információs rendszer szokta meghatározni.

5.12. Napló megőrzése

A naplóbejegyzések megőrzése néhány eset kivételével a szervezet döntésén alapszik. ez alól kivétel, amikor jogszabály írja elő, hogy az információs rendszer adatainak, azokon történő változtatásokról mennyi ideig kell adatokat megőrizni.
Amennyiben jogszabály által került meghatározásra vagy jogszabályból levezethető a naplók megőrzésének ideje, úgy a naplóállományokat a meghatározott ideig kell és lehet hiteles módon megőrizni. A szervezet által meghatározott megőrzési idő meghatározásánál figyelembe kell venni a hazai és az európai unió által hozott jogszabályokat (például GDPR).
Fontos, hogy a naplók megőrzési ideje már az információs rendszer bevezetésére létrehozott projekt tervezési fázisában ismert legyen, hiszen a naplóállományok tárolását és feldolgozását is tervezni kell.

5.13. Naplók törlése

A naplóállományokat a megőrzési idő lejártával törölni kell. Ez sok esetben egyáltalán nem könnyű feladat, hiszen meg kell oldani olyan problémákat is, mint:

- az adatok többféle adathordozón lehetnek,
- az adathordozón különböző megőrzési idejű adat lehet,
- a hiteles adatnak továbbra is hitelesnek kell maradni,
- az adatok konzisztenciáját meg kell őrizni,
- az adattörlést dokumentálni kell.

A törlés módja a naplózó rendszertől függően lehet egy egyszeri törlő eljárás vagy az új naplók általi felülírás.

5.14. Naplózás események (pl rendszer leállítása)

Mivel a naplózás az egyik legfontosabb incidensfelderítési rendszer, így a keletkező naplóállományok szerepe is igencsak fontos lehet. Amennyiben nem érkeznek meg a naplóbejegyzések az elemző rendszerekbe, úgy az esetleges incidensek detektálása sem tud megtörténni. Egyrészről a fejlett támadók igyekeznek a nyomaikat eltüntetni, ezt pedig úgy tudják legkönnyebben megtenni, ha a naplózási szolgáltatást manipulálják (például a naplózási folyamat leállításával vagy a naplóállományok törlésével). Másrészről üzemeltetői hiba miatt is sérülhet a naplózási funkció (például tárhely elfogyása), ami szintén veszélyeztetheti egy esetleges incidens feltárását. Ezen okok miatt is nagyon fontos, hogy a naplózási funkció normálistól történő eltérése mielőbb feltárásra kerüljön. Elsősorban kritikus rendszerek esetén képzelhető el, hogy a naplózás leállása esetén az informatikai rendszer leállítását is el kell végezni.
Egy információbiztonsági esemény (vagy nem megfelelő tervezés) esetén előfordulhat, hogy a naplóállományok elfogyasztják a számukra dedikált tárterületet, ami akár az informatikai rendszer leállását is okozhatja. Ennek elkerülésének érdekében a tervezés során érdemes odafigyelni, hogy ilyen eset ne tudjon megtörténni.

5.15. Időszinkron

A naplózással foglalkozó jogszabályok, szabványok, ajánlások szinte kivétel nélkül előírják, hogy az egyes informatikai rendszerelemek egymással időben szinkronizálva legyenek. De miért is fontos ez? Amikor egy incidenst elkezd a szervezet vizsgálni, akkor az esemény bekövetkezésének időpontja az egyik legfontosabb kapocs a különféle rendszerelemek vonatkozásában. Ha ez a kapocs nem megfelelő, akkor az incidenskezelők csak jelentős nehézségek árán tudják az egyes eseményeket összekötni, illetve a naplóelemző rendszer által végzett automatikus korrelációk sem tudnak működni. Jellemzően a szervezet az időszinkron biztosítására belső vagy külső szolgáltatást vesz igénybe (NTP szolgáltatás)

5.15.1. incidensmenedzsment

Amennyiben a szervezet rendelkezik védelmi eszközökkel, rendelkezik az incidenskezeléshez szükséges folyamatokkal, illetve a szervezetben dolgoznak megfelelő szaktudással rendelkező személyek, akkor a szervezet feltehetően képes egy biztonsági incidens detektálására, kezelésére.

5.16. Beengedések

A biztonságos beengedések alkategóriába azok a védelmi kontrollok található, amelyek azt biztosítják, hogy az arra jogosultak, jogosultsági szintüknek megfelelően férjenek hozzá az adott vállalat, intézmény adataihoz, információihoz. A gyakorlatban ez azt jelenti, hogy az itt alkalmazott védelmi kontrollok biztosítják azt, hogy azok a belső munkatársak vagy külső közreműködők, akiknek bármilyen tevékenységet kell végeznie az adott rendszerben, legyen az felhasználói, üzemeltetői, megfelelően azonosításra kerüljenek, a szükséges jogosultságaik pedig kiosztásra kerüljenek. Ezek a kontrollok biztosítják, hogy az adott személy csak és kizárólag a számára szükséges minimum jogosultságokkal rendelkezzen, csak azokhoz az adatokhoz, információkhoz férjen hozzá, amely a munkájához elengedhetetlen, azokat viszont biztosan és főleg biztonságosan elérhesse és használhassa.

5.16.1. A hozzáférés folyamata

A biztonságos beengedések eszközei közé tartoznak a hozzáférésvezérléshez szükséges elemek, amelyek megadják, hogy KI? MIHEZ? és HOGYAN? férhet hozzá. A hozzáférésvezérlésnek négy alaplépése van, amelyek a következők. Az első az azonosítás (Identification), amely a „Kivagy?” kérdésre adja meg a választ. A második a hitelesítés (Authentication), amely a „Valóban az vagy-e?” kérdésre felel. A harmadik az engedélyezés vagy felhatalmazás (Authorization), amely a „Van-e jogod hozzá?” kérdésre válaszol, azaz itt történik a jogosultságok megadása és felügyelete. Végül a negyedik az elszámolás vagy könyvelés (Accounting), ami a „Mi történt (vagy fog történni)?” kérdésre ad feleletet, azaz itt történik a hozzáférések naplózása a biztonsági audithoz, vagy akár a pénzbeli elszámoláshoz is.
A biztonságos beengedéseket szolgáló elemekhez tartoznak a hitelesítenél használt eszközök és rendszerek, legyenek azok tudás alapúak (pl. jelszavak, PIN kódok stb.), tulajdon alapúak (pl. hard vagy soft tokenek, proximity kártyák stb.), tulajdonság alapúak (pl. ujjlenyomat, arc, retina stb.), vagy viselkedés alapúak (pl. aláírásdinamika, járásmód, szóhasználat stb.). A jogosultságkezelésnél használt eszközök ellenőrzik, hogy az azonosított entitás a biztonsági házirend és a saját jellemzői alapján rendelkezik-e

elégséges jogosultsággal a kért erőforrás használatához. Az elérés kritériumai függhetnek szerepköröktől, csoporttagságtól, helytől, időtől, vagy akár az adott tranzakció típusától is.

5.16.2. Az azonosítás – ki vagy

Az hozzáférés során az első lépés annak megadása, hogy ki vagyok, azaz mi a felhasználói azonosítóm vagy nevem. Ez az azonosító az adott rendszer vonatkozásában egyedi, azaz mindenki másnak más lesz az azonosítója. Ilyen azonosítók lehetnek az email címünk, vagy a Windows belépéshez szükséges felhasználói nevünk, de akár egy kódsorozat is. Ezek az azonos0tó adatok egy rendszer vonatkozásában általában szabványos formátumúak. Nagyon fontos, hogy a felhasználói azonosítót önmagában nem hiteles0t bennünket, mivel ezen adatok nyilvánosak is lehetnek például egy email cím esetében.

5.16.3. A hitelesítés - az vagy-e, akinek mondod magad

A második lépés, hogy a felhasználó hitelesítése. A hitelesítés során a felhasználó bebizonyítja, hogy valóban az, akinek kiadja magát, azaz ad valamit, amitől elhiszi az azonosításért felelős rendszer, hogy Ő az a felhasználó, akinek kiadja magát. A hitelesítést négy féle képpen tudja megtenni a felhasználó:

1. **Tudás** alapú: 'Something you **know**' – tud valamit
2. **Tulajdon** alapú: 'Something you **have**' – van valamilye
3. **Tulajdonság** alapú: 'Something you **are**' – rendelkezik valami tulajdonsággal
4. **Viselkedés** alapú: 'Something you are **doing**' – valahogy viselkedik

Amikor ebből a négyesből két különbözőt alkalmazunk, azt erős hitelesítésnek (strong authentication) nevezzük vagy két/több faktoros hitelesítésnek.

5.16.4. Tudás alapú hitelesítés

A tudás alapú hitelesítés a legkönnyebben megvalósítható és egyben a legelterjedtebb hitelesítési metódus. A hitelestéshez olyan információ kell, amit tudunk, mint például egy jelszó vagy egy PIN kód.
A tudás alapú hitelesítés előnye, hogy a hitelesítő adat könnyen cserélhet (jelszócsere funkció vagy az elfelejtett jelszó funkció segítségével), viszont hátránya, hogy nem tudunk tunk több tíz jelszót fejben tartani, azaz vagy leírjuk őket vagy sok rendszerben ugyanaz a jelszó kerül használatra – mind kettőnek komoly kockázatai vannak. Nehézséget okoz továbbá a megfelelő hosszú és komplexitású jelszó használata. Jelen fejezet írásakor minimálisan 12 karakter hosszú jelszó javasolt, amiben van kisbetű, nagybetű, szám és legalább egy speciális karater. És ami még talán ennél is fontosabb, hogy ne legyenek a jelszavak kitalálhatóak, azaz kerüljük:

- az értelmes szavakat a jelszóban
- a jelszó ne tartalmazzon személyes adatunkat (például becenév, kutyánk neve, vagy születési dátum)
- ne használjuk ugyanazt a jelszót különböző rendszerekben

A fenti követelményeknek történő megfelelés hatékonyan csak jelszó menedzsment alkalmazások segítségével oldható meg biztonságos módon, bár ezen alkalmazásoknak is megvannak a maguk kockázatai.

A tudás alapú hitelesítés során a hitelesítő adat illetéktelenek általi megismerése komoly kockázatokat rejthet magában, hiszen a felhasználói nevünk és a hitelesítő adatunk birtokában vissza lehet élni személyiségünket. Fokozottan kell figyelni nyilvános helyeken, például tömegközlekedési eszközön, nyilvános helyen, hogy nem figyeli-e valaki közvetlenül vagy akár kamera segítségével a belépési folyamatunkat. Illetve figyeljünk arra, hogy jelszavainkat ne osszuk meg mással, például kollégával, rendszerüzemeltetővel és ne dőljünk be olyan weboldalaknak, amelyek megpróbálják megtévesztve bennünket megszerezni adatainkat.

Tulajdon alapú hitelesítés

A tulajdon alapú hitelesítés a leggyakrabban használt második hitelesítés faktorként alkalmazzák. ilyen hitelesítés, mikor például sms-ben kapjuk meg a banki oldalhoz szükséges belépési kódot.

Ezen hitelesítési metódus alkalmazása esetén olyan eszközre támaszkodunk, amely a tulajdonunkban van és ezzel igazoljuk, hogy azok vagyunk, akinek mondjuk magunkat. Ilyen eszközök lehetnek például az eSzemélyi igazolvány, fizikai token, mobil telefonszám vagy akár fizikai kulcs is. A tudás alapú hitelesítéshez képest előnynek tekinthetjük, hogy az eszköz elvesztését hamarabb észre lehet venni, mint a jelszavak kiszivárgását, az hitelesítés során fizikailag ott kell lenni az eszköznek, azaz például távolról sokkal nehezebben kerülhető ki, mint a tudás alapú hitelesítés. Hátránya ugyanakkor, hogy a fizikai eszköz elvesztése, ellopása esetén annak pótlását nehezebb megvalósítani. Azt, hogy az egyes eszközök közül melyiket választja a szervezet, elsősorban a védett informatikai rendszer kockázata, az iparágban elterjedt megoldások, illetve a lehetőségek határozzák meg.

Tulajdonság alapú hitelesítés

A tulajdonság alapú hitelesítés széles körű felhasználása az elmúlt néhány évben indult el, a mobil telefonok számítási kapacitásainak növekedés miatt (ujjlenyomat és arcfelismerés), korábban ezen hitelesítést csak magasabb kockázatú informatikai rendszerek esetén alkalmazták.

A hitelesítés alapja valami olyan tulajdonság, amivel rendelkezünk (ujjlenyomat, ujj- és kézgeometria, kézerezet, arc, arcthermogram, retina (recehártya- erezet), írisz (szivárványhártya), szag, DNS). A tulajdonság alapú hitelesítés előnye, hogy nem, vagy csak nagyon nehezen lehet ezen tulajdonságokat reprodukálni, nem lehet őket „elveszteni”, ellopni, viszont hátránya lehet a cserélhetőség hiánya, illetve az egyes tulajdonságok változása miatti bizonytalanság növekedése (például szakáll növesztés, vagy akár új haj stílus viselete). Az egyes hitelesítési megoldások nagyon eltérő minőségben tudnak biztosan azonosítani, illetve az azonosítás sikerességét nagymértékben befolyásolja az eszközzel szemben elvárt pontosság: minél nagyobb az elvárt fontosság, annál valószínűbb, hogy csak a jogosult személy esetén lesz sikeres a hitelesítés, ugyanakkor a pontosság növelése óhatatlanul magával hozza a fals pozitív találatokat is, azaz olyan személyek esetén is sikertelen lesz a hitelesítés, aki rendelkeznek a hitelesítéshez szükséges tulajdonsággal (például arcgeometria vizsgálat eseten egy bedagadt fog is alutasításhoz vezethet). Meg kell ugyanakkor jegyezni, hogy ezen biometrián alapúló hitelesítési rendszerek egyre jobb teljesítményt nyújtanak már a hétköznapi életben is.

A tulajdonság alapú hitelesítés a hétköznapokban elsődleges hitelesítésként szokták alkalmazni, különösen védett környezetekben jellemzően együtt alkalmazzák a tulajdon alapú hitelesítéssel.

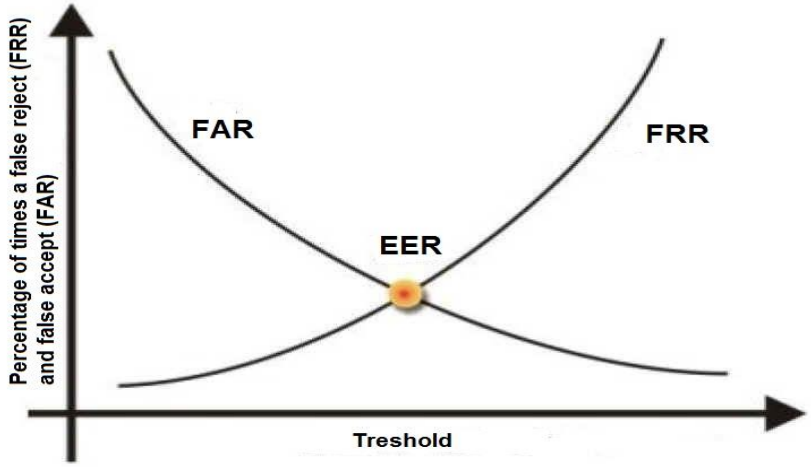
5.16.5. Viselkedés alapú hitelesítés

A mindennapi életünkben a legkevésbé elterjedt biometria alapú hitelesítés során a viselkedésünk (aláírás-dinamika, hanganalízis, egérmozgás, gépelési minta, járásmód, mimika, szóhasználat) alapján kerül személyazonosságunk hitelesítésre. Ezen megoldások csak magas szinten védett informatikai rendszerek esetében kerülnek bevezetésre, jellemzően egyéb hitelesítési eljárásokkal párhuzamosan.

5.16.6. Biometrikus azonosítások értékelése

A tudás és a tulajdonlás alapú hitelesítés esetén a hitelesítő rendszer biztos döntést tud hozni, mivel a döntés mintaillesztés alapú, azaz vagy illeszkednek az adatok, vagy nem. A biometrikus azonosítás esetén a hitelesítő rendszer az előzetesen rögzített mintát veti össze a hitelesítéskor érzékelt mintával. A mintavételi pontok számának és a mintaillesztés szigorúságának növelésével javítható a hitelesség biztonsága. A biometrikus azonosítás során három alapfogalmat érdemes megjegyezni:

- **FRR** (False reject rate - Hibás visszautasítási ráta): Jogosult felhasználó visszautasítása, a használhatóságot veszélyezteti.
- **FAR** (False accept rate - Hibás elfogadási ráta): Illetéktelen felhasználó engedélyezése, a biztonságot veszélyezteti.
- **CER** (Crossover Error Rate - Metszésponti hibaarány): Az FFR és FAR megegyező értéke, melyet az érzékenység állításával tudunk elérni.



4. ábra: http://www.biometria.sk/en/principles-of-biometrics.html

A biometrikus azonosítás előnyeként kell megemlíteni, hogy azok nem, vagy csak nagy nehézség árán tulajdoníthatóak el, más hitelesítési megoldásokkal együtt alkalmazva nagy biztonságot tudnak nyújtani, ugyanakkor ezen hitelesítési módnak vannak hátrányai is:

- Hamisítható (gumiujj, felvett minták),
- A háttéradatbázist és a kommunikációs csatornát kiemelten kell védeni,
- Az alkalmazhatóság korlátai (ikrek, fogyatékkal élők, betegségek, változó azonosítók),
- Felhasználói elutasítás (pl.: szembe világítás, vérvétel, privát szféra védelme),
- Lassú lehet a feldolgozás,
- A valóban biztonságos technológiák ma még igen költségesek.

5.16.7. Jogosultság kezelés – azaz mihez férhetsz hozzá

A felhasználó hitelesítését követően

1. A hozzáférés vezérlések esetében négy jellemző modellel dolgoznak a rendszerek. Az első a kötelező hozzáférés-vezérlés[139] modell, amely esetén a hozzáféréseket a rendszer előre meghatározott szabályok alapján engedélyezi, az entitások nem szólhatnak bele még az általuk birtokolt erőforrások elérésébe sem. Ez a legszigorúbb szintű szabályozás, de nagyon alapos előzetes tervezést és komoly adminisztrációt igényel. A második az ún. diszkrecionális, belátáson alapuló v. önkényes[140] modell. Ebben az esetben a felhasználók saját adataikhoz a hozzáféréseket saját belátásuk, azaz „diszkréciójuk" alapján határozzák meg. Ez a modell igényli a legkisebb adminisztrációt, így ebből a szempontból ez a legkényelmesebb megoldás, de az emberi hibák okán ez egyben a legsérülékenyebb is. A harmadik a szerepkör alapú[141], vagy más néven nem-diszkrecionális hozzáférés-vezérlési modell. Ennél a modellnél az egyes adott szerepkörök tagjai azonos jogosultsággal rendelkeznek. Végül a negyedik a szabályrendszer alapú[142] modell, amelyben a hozzáféréseket a rendszergazdák által meghatározott szabályok vezérlik. Ezekről a későbbiekben még részletesen lesz szó.
2. A legtöbb kibertámadás egyik leglényegesebb eleme az emelt szintű jogosultságok megszerzése és azután az azokkal történő visszaélés, legyen az külső támadó, vagy akár rossz szándékú belső munkatárs. Éppen ezért a kiemelt felhasználók felügyeletének kiemelt szerepe van a védelemben. Ezek azok az eszközök, amelyek a kiemelt jogosultságú felhasználók tevékenységének valós idejű felügyeletét, monitorozását ellátják, akár olyan szintig, hogy azok teljes tevékenysége videófolyamként rögzítésre kerül és így utólag teljes mértékben visszajátszhatóvá válik. Ezek is részletesebben kifejtésre kerülnek a későbbi, a biztonságos beengedésekről szóló fejezetben.

Az előző fejezetben bemutatott védelmi megoldások elsősorban a rossz szándékú rendszer hozzáférést akadályozták meg. Jelen fejezet célja elsősorban azon eljárások, technikák bemutatása, amelyek hozzáférést engednek a rendszer jogosultak számára történő eléréséhez.

---

[139] angolul: Mandatory Access Control (MAC)

[140] angolul: Discretionary Access Control (DAC)

[141] angolul: Role Based Access Control (RBAC)

[142] angolul: Rule Based Access Control (RBAC)

6. Információbiztonsági irányítási rendszer, kockázatelemzés, megfelelés

Amíg a biztonsági kizárások és a biztonságos beengedések alkategóriákba a kibervédelmet közvetlenül érintő eszközök, rendszerek tartoznak, addig az üzletvezérelt információbiztonság harmadik alappillérét alkotó üzleti, IT kockázatmenedzsment közvetetten gyakorol hatást a kibervédelemre.
Minden gyakorlati védelem alapja a kockázatokkal arányos védelem kialakítása, ám ehhez először is az adott intézmény, vállalat szempontjából fel kell mérni a releváns kockázatokat, azokat értékelni kell, meg kell határozni melyek az elfogadható szintűek és melyekre kell védelmi intézkedéseket hozni az előbb említett két alappillér megfontolásai mentén.
Az üzleti, IT kockázatmenedzsment kapcsán három nagyobb csoportot különíthetünk el, ezek az ún. GRC modell mentén megjelenő:

- G: Governance (irányítás);
- R: Risk (kockázatok);
- C: Compliance (megfelelés)

kérdéskörei.
Governance vagy irányítás kapcsán az adott szervezet meghatározza az információbiztonsági célkitűzéseket (objectives), ehhez igazítva elkészíti a szükséges irányelveket és szabályzatokat (policies). A vezetés különböző szintjei ezen irányelvek mentén hozzák meg a döntéseiket a saját hatáskörüknek megfelelően, de a felsővezetés sincs abban a helyzetben, hogy a lefektetett irányelvektől eltérhessen.
Risk vagy kockázatok kapcsán szükséges a jól ismert kockázatkezelés lépéseit megvalósítani. fel kell mérni azokat a belső és külső befolyásoló tényezőket, amelyek bizonytalanná teszik, hogy elérik-e, illetve mikor érik el a céljaikat a szervezetek, ezeket a forrásokat azonosítani, elemezni, értékelni, majd kezelni kell. Ez utóbbi lehet a kockázatok elkerülése, felvállalása (tudatos döntéssel!), megosztása, a kockázatforrás eltávolítása, a bekövetkezési valószínűség csökkentése vagy a következmények megváltoztatása.
Compliance vagy megfelelés témakörébe tartoznak az üzletvezérelt biztonság jogi, megfelelőségi hatás kapcsán már említett külső szabályzóknak való megfelelés mellett a belső szabályzók (pl. informatikai biztonságpolitika, informatikai biztonsági stratégia, Informatikai Biztonsági Szabályzat stb.) elkészítése és alkalmazása, valamint az adott szervezet által használt infokommunikációs rendszerekben lévő komponensek tekintetében a kötelezően vagy szervezeti döntés alapján alkalmazott termékbiztonsági előírások (pl. Common Criteria (CC)) következetes betartása.
Az üzleti, IT kockázatmenedzsment kérdéskörei is részletesebben kifejtésre kerülnek a következő fejezetekben.

6.1. Információbiztonsági kockázatelemzés

Az információbiztonsággal kapcsolatban először is fontos tudni, hogy a kockázatok és a fenyegetések mindig jelen vannak. Az információbiztonsági kockázatelemzésnek a célja, hogy az adott szervezet tájékozott legyen a kockázatok és fenyegetések jelenlétével kapcsolatban, ezzel lehetőséget adva az egyértelmű és megalapozott döntések meghozatalára az információbiztonság területén. Az információbiztonsági kockázatelemzés lépéseit részletesen bemutatom alábbiakban:

1. Az értékek meghatározása: Első lépésként az adott szervezetnek fel kell mérnie, hogy milyen értékes információik vannak. Ez lehet üzleti titok, ügyfél vagy munkavállaló adatai, vagy más olyan információk, amelyeknek súlyos következményei lehetnek az illetéktelenek általi elérése esetén.
2. A fenyegetések azonosítása: Az információbiztonsági kockázatelemzés következő lépése azoknak a fenyegetéseknek az azonosítása, amelyek befolyásolhatják az értékes információkat. Egyes fenyegetések lehetnek külső forrásokból, például hackerek, míg mások belső forrásokból, mint például szándékos vagy véletlenszerű hibák.
3. A kockázatok értékelése: Az értékelés során meg kell határozni a kockázatok súlyosságát és valószínűségét. Ebben a fázisban a szervezetnek meg kell határoznia, hogy mennyire valószínű, hogy egy adott fenyegetés bekövetkezik, és milyen hatással lehet az értékes információkra, ha ez megtörténik.
4. A megelőzési módszerek és intézkedések meghatározása: Az információbiztonsági kockázatelemzés utolsó lépése az, hogy a szervezet megfelelő megelőzési módszereket és intézkedéseket határoz meg. Ilyenek lehetnek például a tűzfalak, a rendszeres adatmentések, az erős jelszórendszer és a hasonlók. Információbiztonsági irányítás: Az információbiztonsági irányítás olyan folyamat, amelynek célja az, hogy a szervezet biztosíthassa a megfelelő eszközöket és eljárásokat a különböző információbiztonsági kockázatok kezeléséhez.

6.2. Az értékek meghatározása

Az informatikai kockázatelemzés során több módszer és eljárás használható az értékek meghatározására. Néhány példa:

1. Interjúk: A leggyakoribb és hatékony módszer, amely lehetővé teszi az érintettek véleményének megismerését és az értékek meghatározását.
2. Szubjektív módszerek: Olyan módszerek, amelyek lehetővé teszik az értékek felmérését, például az osztályozás, a csoportosítás és az értékek hierarchiájának megállapítása.
3. Kockázatelemzési módszerek: Számos kockázatelemzési módszer használ az értékek becslésére, például a valószínűségi és hatáserősségi skálák, a pénzügyi értékelés, a pénzügyi modellezés stb.
4. Benchmarking: A benchmarking módszer lehetővé teszi más szervezetek teljesítményének összehasonlítását és az értékek meghatározását.

Ezen módszerek alkalmazása lehetővé teszi a szervezetek számára, hogy az értékeiket az üzleti folyamatok és az informatikai rendszerek kockázatelemzése során hatékonyan meghatározzák.

6.3. Fenyegetések meghatározása

Hasonlóan az értékek meghatározásához számos módszer és eljárás áll rendelkezésre a fenyegetettségek meghatározására:

1. Rendszer-támadási szimulációk: Olyan megközelítés, amelyben a szervezet által használt rendszerekre támadásokat szimulálnak annak érdekében, hogy azonosítsák a sebezhetőségeket és a fenyegetettségeket.
2. Adatvédelmi hatásvizsgálatok: Olyan elemzések, amelyek célja az adatvédelmi kockázatok azonosítása és azok kezelése a jogszabályi előírásoknak megfelelően.
3. TI stratégia felülvizsgálat: Az információtechnológia (TI) rendszerek felülvizsgálata, és annak meghatározása, hogy milyen kockázatokkal jár a jelenlegi TI stratégia és azonosítani azokat a javítási lehetőségeket.

4. Sebezhetőség felmérések: A rendszer vagy alkalmazás sebezhetőségeinek azonosítása olyan eszközökkel és eljárásokkal, mint a megfigyelés, szkennelés vagy penetrációs tesztelés.

Ezek csak néhány példa a sokféle módszerből, amelyek rendelkezésre állnak a fenyegetettségek meghatározására az informatikai kockázatelemzés során.

6.4. Kockázat értékelési módszerek

Az informatikai kockázatelemzés során több kockázat értékelési módszer is használható. Néhány példa:

1. Kockázati mátrix: A kockázati mátrix olyan táblázat, amely a kockázat súlyosságát és annak valószínűségét osztályozza. Ez a módszer lehetővé teszi, hogy az értékelők meghatározzák, mely kockázatokkal kell prioritást adni.
2. Failure Modes and Effects Analysis (FMEA): A FMEA módszer az egymásra ható események elemzésére összpontosít. Ezt a módszert általában az előrejelzések vagy tervezési folyamatok során alkalmazzák, és segít a kockázat hatásainak minimalizálásában.
3. Kvantitatív kockázatelemzés: A kvantitatív kockázatelemzés általában az üzleti folyamatok és IT rendszerek hozzáadott értékének értékelésére összpontosít, és lehetővé teszi, hogy az értékelők mérjék a kockázatok valószínűségét és súlyosságát.
4. Kvalitatív kockázatelemzés: A minőségi kockázatelemzés szubjektívebb módszer, mivel tapasztalatokra, szakértelemre és szubjektív értékelésekre támaszkodik. A módszernek az a célja, hogy meghatározza a kockázatok okait, hatásait és valószínűségét, és segít prioritást adni azok kezelésének.

6.5. Kvalitatív kockázatelemzés

A kvalitatív kockázatelemzés egy olyan módszer, amelyet a kockázatok súlyosságának, valószínűségének és hatásának becslése alapján végzünk. Ez az elemzési módszer a következő lépésekből áll:

1. Minden kockázat meghatározása - Az első lépés a kockázatok meghatározása és azonosítása. Meg kell határozni az összes olyan fenyegetést, amelyek befolyásolhatják az adott rendszert.
2. Kockázati hatás - Az összes kockázatot osztályokba kell sorolni annak hatása és súlyossága alapján. Egyes kockázatok sokkal súlyosabbak lehetnek, mint mások, és megállapításra kerül, hogy melyek a legveszélyesebbek.
3. Kockázati valószínűség - A kockázatok valószínűségét is meg kell határozni. Fontos megjegyezni, hogy a rendszer egyes elemeinek a sérülése nem biztos, hogy ugyanakkora esélyű, így ezeket a kockázatokat is osztályokba kell sorolni.
4. Kockázati prioritás - Az előző két lépés alapján minden kockázat egy kockázati prioritása kerül meghatározásra. A prioritás felállítását a várható hatások súlyossága, és valószínűsége alapján határozzuk meg. A kvalitatív kockázatelemzés általában egyszerűbb és gyorsabb megoldás, mint a kvantitatív elemzés, és segít a legkritikusabb tényezők belső áttekintésében az üzleti döntéshozatalban.

6.6. Kvantitatív kockázatelemzés

A kvantitatív kockázatelemzés egy olyan módszer, amely numerikus értékelést alkalmaz a kockázatokkal kapcsolatos adatokra, például a valószínűségre, az expozícióra és az okozott veszteségre vonatkozóan. Ez a módszer általában a következő lépésekből áll:

1. Azonosítsuk azokat a kockázati tényezőket, amelyek lehetséges káros hatással lehetnek az üzleti folyamatokra vagy szervezetre.

2. Határozzuk meg a kockázati tényezők valószínűségét, az expozíció mértékét és az okozott veszteségeket.
3. A kockázati tényezők súlyosságának értékelése.
4. Az összes kockázati tényező összetett hatásának értékelése.
5. Hatékony kockázatkezelési stratégia meghatározása a jövőbeli kockázatok minimalizálására. Az eredmények numerikus értékekben jelennek meg, amelyek százalékos értékek lehetnek. Ezután az értékelést a kockázati tolerancia szintjével összehasonlítják, hogy az észlelt kockázat elfogadható-e vagy sem.

A kvantitatív kockázatelemzés hasznos lehet a nagyobb szervezetek számára, mivel lehetővé teszi a hatékony stratégiák kialakítását és az erőforrások megfelelő elosztását a kockázatok kezelésére.

6.7. A megelőzési módszerek és intézkedések meghatározása

Az informatikai kockázatok kezelése érdekében számos kockázatkezelési lehetőség áll rendelkezésre.

1. Kockázat elfogadása: Elfogadjuk a kockázatot, és nem teszünk semmit a kockázat csökkentése érdekében.
2. Kockázat csökkentése: Olyan intézkedések, amelyeket a kockázatok csökkentése érdekében hozunk, például a biztonsági rendszerek és eljárások implementálása.
3. Kockázat áthárítása: Azaz, hogy a kockázatot olyan harmadik feleknek áthárítjuk, akiknek ellenállóbb megoldásuk van, vagy akiknek nincs annyi szükségük a bizalmi viszonyunkra.
4. Kockázat elkerülése: Olyan intézkedések vagy döntések hozása, amelyek teljesen elkerülik az adott kockázatot, például a bizonyos tevékenységek és projektek elkerülése.
5. Kockázat finanszírozása: Azaz, hogy olyan pénzügyi megoldásokat alkalmazunk, mint a biztosítás, ami segít csökkenteni azoknak a következményeknek a pénzügyi terheét, amelyekből a kockázat teljesülése adódhat.

6.8. Az információbiztonság irányítás

Az információbiztonsági irányításnak számos eleme van, amelyek mindegyike hozzájárul az átfogó információbiztonsági stratégiához.

Az információbiztonsági irányítás egyik fontos eleme az információbiztonsági politika. Ez a dokumentum határozza meg azokat a szabályokat és előírásokat, amelyeket a szervezet minden tagjának követnie kell. Az információbiztonsági politikának egyértelműnek, konzisztensnek és megfelelő erőforrásokkal kell rendelkeznie annak érdekében, hogy hatékonyan működjön. Az információbiztonsági irányításnak a vezetői szinten való támogatása is fontos. A vezetőknek meg kell érteniük az információbiztonsági kockázatokat és a védelmi intézkedések fontosságát. A vezetőknek el kell készíteniük az információbiztonsági stratégiát, amelynek célja az információbiztonsági irányítási program létrehozása és a végrehajtás megerősítése.

Az ISO/IEC 27000 szabvány vagy más néven ISO 27001 az információbiztonsági irányítási rendszerek (Information technology — Security techniques — Information security management systems — Requirements) nemzetközi szabványa. A szabvány célja az információbiztonsági irányítási rendszer (ISMS) fejlesztése és működtetése, figyelembe véve a biztonsági kockázatokat és az üzleti követelményeket. Az ISO 27001 definiálja az információbiztonságra vonatkozó követelményeket, és az ISMS gyakorlati megvalósítását és értékelését szabályozza. A szabvány átfogó keretrendszer azzal a céllal, hogy az információbiztonsággal kapcsolatos kockázatokat hatékonyan kezeljük, és biztosítsuk az információk bizalmas, rendelkezésre álló és változatlan állapotát. Az ISO

27001 alapelvei az ismertető képesség, hozzáférhetőség, sértetlenség és az adatvédelem. Ez magában foglalja a bizalmasság, az integritás, az elérhetőség, a hitelesség és az elszámoltathatóság követelményeit. Az ISO 27001 nem csak az információbiztonsági követelmények standardizálására szolgál, hanem segít megfelelni az adatvédelmi jogszabályoknak és a hatóságok által elvárt előírásoknak is. Ezenkívül az ISO 27001 segítséget nyújt a cégeknek abban, hogy betartsák az iparági szabályokat és az ügyfeleik elvárásait. A szabvány alkalmazása elősegíti az információ védelmét, az üzleti folyamatok és a szervezet működőképességének biztonságát. A sikeresebb információbiztonsági irányítási rendszer megvalósítása érdekében érdemes a ISO 27001 szabvány előírásainak követése mellett biztonsági szakértők jelenlétében megvalósítani azokat.

Az ISO 27000 szabványcsalád tartalmazza a következő alapvető irányelveket és ajánlásokat az információ biztonsági irányítási rendszerek tekintetében:

1. ISO 27001 - az információbiztonsági irányítási rendszerek követelményei
2. ISO 27002 - az információbiztonsági irányítási rendszerek gyakorlati alkalmazása
3. ISO 27005 - az információ és technológiai kockázatértékelés módszertana
4. ISO 27006 - az információbiztonsági rendszerek szervezeti tanúsítványozása
5. ISO 27011 - az információbiztonsági irányítási rendszerek javasolt alkalmazása a telekommunikációs ágazatban
6. ISO 27017 - felhőszolgáltatás biztonsági ajánlásai
7. ISO 27018 - személyes adatok védelme felhőkörnyezetben
8. ISO 27701 - a személyes adatok védelméhez kapcsolódó adatvédelmi kutatás, elemzés és értékelés irányelvei és ajánlásai.

Az ISO 27000 tanúsítás folyamata általában az alábbi lépéseket foglalja magában:

1. Előtanúsítvány: Az előtanúsítvány célja, hogy az érintett szervezetet felkészítse az ISO 27001 tanúsítási folyamatára. Ebben a szakaszban az érintett szervezetnek fel kell állítania egy belső auditot, amely során a szervezet belső folyamatait ellenőrizni kell az ISO 27001 szabvány szerint.
2. Tanúsítási audit: A tanúsítási audit során az auditáló szakemberek ellenőrzik a szervezet információbiztonsági irányítási rendszerét az ISO 27001 szabvány alapján. Ezenkívül további beszélgetéseket és közvetlen vizsgálatokat folytatnak annak érdekében, hogy a szervezet alkalmazza-e az ISO 27001 szabvány előírásait.
3. Tanúsítvány kiadása: Ha a tanúsítási audit sikeresen lezárul, akkor az auditáló szervezet kiadja az ISO 27001 tanúsítványt a szervezetnek.
4. Surveillance audit: A tanúsítvány fenntartásához rendszeresen el kell végezni a felülvizsgálatokat. Az auditáló szervezet ellenőrzi, hogy a szervezet továbbra is megfelel-e az ISO 27001 szabvány előírásainak.
5. Re-certification audit: Az ISO 27001 tanúsítványt általában 3 évente kell újra minősíteni. A re-certification audit az előző auditálási folyamatok ismétlődését jelenti, és azt ellenőrzi, hogy a szervezet továbbra is megfelel-e az ISO 27001 szabvány előírásainak.

Az ISO 27000-n kívül számos más információbiztonsági tanúsítási rendszerek is léteznek, amelyek a következők lehetnek:

1. Az Amerikai Könyvvizsgálói Kamara (AICPA) által kibocsátott tanúsítvány, amely az információ biztonságossága, rendelkezésre állása, adatvédelmi magatartása és feldolgozási integritása terén ellenőrzi a vállalatokat és szervezeteket.
2. PCI DSS: A fizetési kártyák iparági szabványa, amely azt biztosítja, hogy a kártyaelfogadók és a feldolgozók védik az érzékeny banki kártya adatokat.

3. HIPAA: Az Amerikai Egészségügyi és Szociális Minisztérium által létrehozott rendszer, amely az egészségügyi adatok védelmét és biztonságát biztosítja.
4. FedRAMP: A Szövetségi Államok kormánya által kibocsátott rendszer, amelyet a felhőszolgáltatók használnak, hogy megfeleljenek a kormányzati szerződésekhez kapcsolódó biztonsági követelményeknek.
5. CSA STAR: A Felhőbiztonsági Szövetség által kibocsátott tanúsítvány, amely az adatvédelmi és biztonsági standardokat ellenőrzi és rangsorolja a felhőszolgáltatásokat.

6.9. Megfelelés

Az információ biztonsága az egyik legfontosabb tényező a modern vállalatok számára, tekintettel arra, hogy az információkat az interneten keresztül tárolják és osztják meg mind az ügyfelekkel, mind a munkavállalókkal. Az információ biztonságos kezelésének kulcsa a megfelelési szabványok betartása, amelyek biztosítják az információ biztonságát, valamint a megfelelő adatvédelmi intézkedések biztosítását. Az információbiztonsági megfelelési (Compliance) szabályozásokat testreszabták, hogy biztosítsák az információkat, hogy azok a nem megfelelő kezelésükből eredő bűncselekményekben nem szereplő időnként rengeteg pénzügyi veszteséget okozhatnak. Lehet, hogy a vállalat számára a megfelelési eljárások betartása alaposan megfontolt döntést igényel a folyamatosan változó kilátásokban és azzal a kihívással, amelyek azt jelenthetik, hogy például biztosnak kell lennie arról, hogy az adatvédelmi politika az összes alkalmazandó törvényi rendelkezésnek megfelel. Ha egy vállalkozás megfelel a megfelelési szabályozásoknak, akkor az abban az értelemben fontos, hogy a vállalatok biztosak lehetnek abban, hogy adataik biztonságban vannak, és a jogszabályoknak megfelelően kezelik őket. A megfelelési rendszer használata és betartása lehetővé teszi, hogy a vállalkozások megtartsák a fogyasztók, ügyfelek és befektetők bizalmát, valamint biztosítsák, hogy az esetleges bírságokat elkerüljék. Az információbiztonsági megfelelési szabályozások alapvetően a biztonsági szabályozásokról szólnak, amelyek megfelelő biztosítást adnak magukról a problémákat és a veszélyeket jelentő tényezőkről. Az előírásoknak az információbiztonsági megfelelősségre vonatkozó fontosabb részei az adatvédelmi, biztonsági és vírusmegelőző alkalmazások, valamint az adatbiztonsági feladatokkal kapcsolatos kommentárok és dokumentációk. Az adatvédelmi politika megfogalmazása az információbiztonsági megfelelőséghez szükséges. Ez a politika arra szolgál, hogy egyértelművé tegye, hogyan kezelik a vállalkozás adatait, és hogyan biztosítják azok védelmét a külső veszélyekkel és a belső kockázatokkal szemben. Az adatvédelmi politika megfogalmazásának kulcsa az, hogy az információ biztonságát a vállalkozás értékeire és azokat veszélyeztető tényezőkre alapozzuk. A biztonsági alkalmazások és eszközök megfelelő párhuzama az adatvédelmi rendszerekkel kulcsfontosságú a megfelelő információ biztonságának biztosításában. Az ilyen alkalmazások az adatok biztonságos tárolását, osztályozását és idejét biztosítják. Az adatbiztonsággal kapcsolatos kérdések megértése és megoldása kulcsfontosságú a hatékony és megfelelő adatvédelem szempontjából. A vírusvédelem fontos elem az információbiztonsági megfelelőség szabályozásaiban. Számos káros szoftver és kártékony vírus teszi ki az információ biztonságának kockázatát. Azonban a vírusvédelem használata az IT infrastruktúrán belül segít biztosítani, hogy az adatok védettek legyenek ezen fertőzésekkel szemben. Az adatvédelmi feladatok kapcsán az információ biztonságának ellenőrzése és valóságos körülmények közötti bemutatása kulcsfontosságú a megfelelő információ biztonságának megteremtéséhez. Az adatbiztonsági feladatoknak tartalmaznia kell a változások áttekintését és módosítását annak érdekében, hogy a törvényi rendelkezéseknek megfelelően megfeleljenek az adatvédelmi sztenderdeknek. A

megfelelőség biztosítása iránti erőfeszítések az állandó változásoknak megfelelően frissítve és aktualizáltak kell legyenek. A megfelelő adatvédelem biztosításának kulcsa az is, hogy folyamatosan ellenőrizni és kiértékelni az adatvédelmi megoldások hatékonyságát csökkenthetők a kockázatok és biztonságos környezetet teremthetünk a vállalat számára. A megfelelőségi szabályozások folyamatos frissítése kulcsfontosságú a megfelelő információ biztonság fenntartásához.

6.10. Az Ibtv alá tartozó szervekkel szembeni elvárások

A 41/2015 BM rendelet az elektronikus hírközlési szolgáltatók tevékenységének szabályozására és biztosítására vonatkozó előírásokat tartalmazza Magyarországon. Az előírások célja annak biztosítása, hogy a hírközlési szolgáltatók végrehajtsák azokat az intézkedéseket, amelyek biztosítják a felhasználók jogait és érdekeit. A rendelet a hírközlési szolgáltatók számára az adatvédelemmel és az adatbiztonsággal kapcsolatos követelmények részletes listáját tartalmazza, és az intézkedéseknek megvalósításra kell kerülniük, hogy biztosítva legyenek a személyes adatok védelme, valamint az adatvesztések és más biztonsági incidensek kockázatának csökkentése. Az előírások szerint a hírközlési szolgáltatóknak hatékony biztonsági intézkedéseket kell végrehajtaniuk, amelyekkel szemben a szolgáltatók teljes mértékben felelősek az adatok biztonságának biztosításáért. Az ilyen intézkedéseket azonban rugalmasan kell kezelni, hogy a hírközlési szolgáltatók is képesek legyenek az innovatív megoldásokra. A rendeletben lekötött követelményeknek való megfelelés feladata a hírközlési szolgáltatóként működő vállalkozásoknak, amelyek számára az elvárt biztonsági szintek kialakítása bizonyos költségekkel járhatnak. Az adatvédelemmel és az adatbiztonsággal kapcsolatos jogszabályok nemcsak azonban jogi kötelezettségként, hanem többletérték is eredményezhetnek. Az elvárt biztonsági szintek ugyanis nemcsak a felhasználók jogainak, hanem az adatok megbízhatóságának, illetve az ügyfelek elégedettségének a garantálásáért is felelősek. Az előírt biztonsági intézkedéseknek megvalósításához a hírközlési szolgáltatóknak elsősorban az adatvédelmi és az adatbiztonsági szakértőkkel kell dolgozniuk. Az ilyen szakértőknek szükségük van minden technológiai trendre, valamint minden felmerülő adatvédelmi és adatbiztonsági kockázatot kell értékelniük. A hatékony védelem érdekében a hírközlési szolgáltatóknak dokumentálniuk kell az intézkedéseket és azok hatásait, hogy a hatékonyabb védelem ennek köszönhetően elérhető legyen. Az előírások nemcsak a hírközlési szolgáltatóknak, hanem a felhasználóknak is számos előnyt jelentenek. Az adatvédelmi és adatbiztonsági szabályok betartása például garantálja a felhasználók jogainak védelmét, és növeli az ügyfélbizalom szintjét. Az adatok biztonságának garantálása csökkenti az adatvesztések és a biztonsági bejelentések kockázatát, mivel az előírt intézkedéseknek köszönhetően ezek az incidensek alacsonyabb eséllyel fordulnak elő. Az előírt követelményeknek való megfelelés nagy kihívást jelent a hírközlési szolgáltatók számára, de ugyanakkor előnyt is jelenthet a számukra, mivel növelheti az ügyféltapasztalat és elhivatottság szintjét. Ennek eredményeként hosszú távon további üzleti lehetőségeket tudnak kialakítani. Az információbiztonsági megfelelés az előírt szabályok és követelmények betartását jelenti, amelyek célja a személyes adatok védelme, valamint az adatbiztonság és az ügyfélbizalom növelése. Bizonyos kihívást jelenthet a hírközlési szolgáltatók számára, de ez a megfelelő szakértőkkel és az innovatív megoldásokkal való együttműködéssel megvalósítható. Az előírt követelményeknek megfelelés előnyöket jelenthet mind a hírközlési szolgáltatók, mind a felhasználók számára, biztosítva az adatok biztonságát, és növelve az ügyféltapasztalatot és elégedettséget.

7. Adminisztratív védelem a gyakorlatban

Az előző fejezetek bemutatták az információbiztonság legfontosabb elméleti ismereteit, az azokhoz kapcsolódó fontosabb jogszabályokat, majd ismertették ezek gyakorlatba történő átültetésének alapjait. Ezt követően részletesen bemutatásra kerültek a logikai védelmi elemek kialakításának gyakorlati kérdései, azok is oly módon, hogy a jogszabályi előírások mellett milyen üzletvezérelt információbiztonsági megfontolásokat célszerű figyelembe venni a hatékony védelem elérése érdekében.
Az adminisztratív védelem kialakítása elengedhetetlen része az információbiztonságnak. Az Ibtv. szerint ez *„a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás”*[143]összességét jelenti. Ez a gyakorlatban azt jelenti, hogy így biztosíthatjuk:

- az információvédelemi intézkedések kereteinek egységes kialakítását és értelmezését;
- a különböző kiemelten védendő információk – legyenek azok minősített adatok, üzleti titokok, banktitokok, személyes adatok stb. – védelméhez szükséges keretek és adminisztratív teendők kialakítását;
- a logikai és fizikai védelmi elemekkel le nem fedett területek védelmének kialakítását, legyen szó a felismert hiányzó és még meg nem valósított vagy a kockázatelemzés következményeként tudatosan felvállalt elemekről.

(A minősített adatok védelmére külön előírások vannak, ezek részletesen megtalálhatók például a „Titkos ügykezelői ismeretek” című könyvben[144], így ezekkel itt nem foglalkozunk. Ugyanakkor meg kell jegyezni, hogy ebben az adminisztratív intézkedések és feladatok ellátásához alapvetően szükséges nem minősített iratforgalom kezeléséhez is számos hasznos megoldást találhatunk, amelyeket a megfelelő könnyítésekkel adaptálhatunk, legyenek az iratok papír alapúak vagy elektronikus formában megjelenők. Ilyenek például a nyilvántartásokról, az iratok nyilvántartásba vételéről, a más szervtől érkezett iratok átvételéről vagy feléjük történő továbbításáról, iratok szerven belül történő átadásáról, visszavételéről, irattározásról szóló részek,)
Steven Schlarman ún PPT[145] modelljében[146] három alapelemre vezeti vissza az információbiztonsági kérdéseket. Bár ebben a modellben a második „P” alatt a szerző a policy-t, azaz a szabályozást érti, de ennél a process, azaz a folyamat elnevezés és

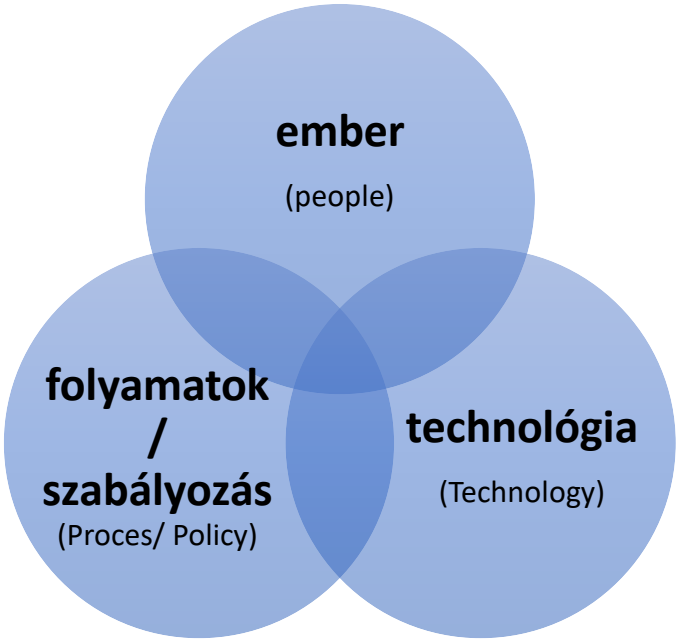
[143] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény. https://net.jogtar.hu/jogszabaly?docid=a1300050.tv letöltve: 2023.01.22.

[144] Tapa Barna – Hegedűs Tamás: Titkos ügykezelői ismeretek. Ötödik hatályosított kiadás. Nemzeti Közszolgálati Egyetem. 2022. ISBN 978-963-498-465-8 https://tudasportal.uni-nke.hu/xmlui/static/pdfjs/web/viewer.html?file=https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/17544/Titkos%20ugykezeloi%20ismeretek%202022.pdf?sequence=1&isAllowed=y Letöltve: 2023.03.15.

[145] PPT: People, Process vagy Policy, Technology, azaz ember, folyamatok vagy szabályozás technológia

[146] Steven Schlarman: The People, Policy, Technology (PPT) Model: Core Elements of the Security Process. Information Security Journal: A Global Perspective p. 1-6 2006.12.21. https://www.tandfonline.com/doi/abs/10.1201/1086/43315.10.5.20011101/31719.6#preview letöltve: 2023.03.04.

értelmezés is elterjedt[147], ezért ez is feltüntetésre került. Ezt mutatja be az alábbi 5. ábra PPT modell.



5. ábra PPT modell

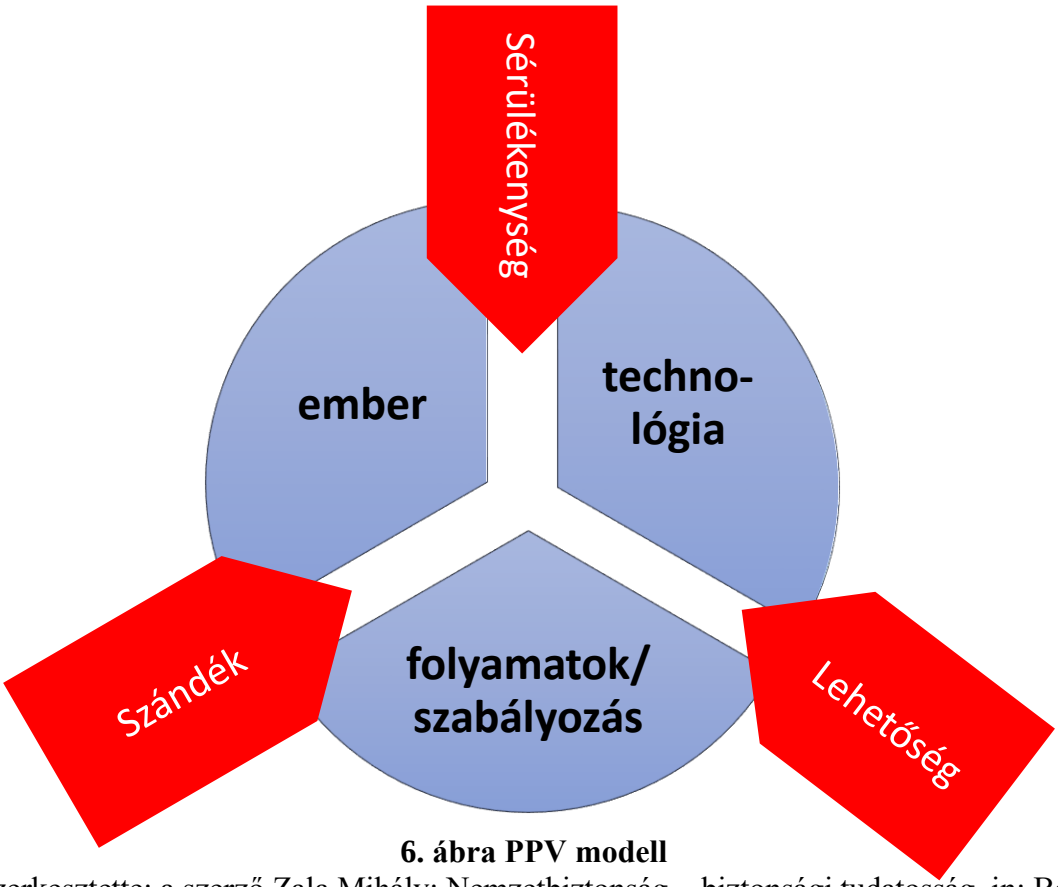
Szerkesztette: a szerző S. Schlarman: The People, Policy, Technology (PPT) Model: Core Elements of the Security Process. alapján

Az ebben megjelenő elemek közül az adminisztratív intézkedésekkel az ember és a folyamatok/szabályozás kérdését lehet kezelni, míg a technológiai kérdésekre a logikai és a fizikai intézkedések adnak választ. Az adminisztratív intézkedések kapcsán hozott folyamatok és szabályok, valamint az emberek (felhasználók) képzése segíti, hogy a meglévő technikai képességeknek megfelelően maximalizáljuk az információvédelmet, megtiltsuk és a megfelelő konzekvenciákat érvényesítsük, érvényesíthessük a leírt folyamatok be nem tartása, a szabályok megszegése, vagy az ismerten technológiával le nem fedett részek kihasználása esetén, valamint az embereinket a lehető legjobban felkészítsük a gondatlanságból bekövetkező információbiztonsági incidensek megelőzésére.

Az ún. PPV[148] modell szerint a PPT modellben megjelenített hármas, azaz ember, a folyamatok/szabályozás és a technológia bármelyikének nem megfelelősége, gyengülése, azaz ezek eltávolodása egymástól lehetőséget teremt a szándék, lehetőség, sérülékenység kockázatok erősödésének. Ezt mutatja be az alábbi 6. ábra PPV modell.

[147] Boda J. – Dobák I. (szer.): A nemzetbiztonság technikai kihívásai a 21. században. Nemzeti Közszolgálati Egyetem. 2015.

[148] PPV: Purpose, Possibility, Vulnerability azaz szándék, lehetőség, sérülékenység



6. ábra PPV modell

Szerkesztette: a szerző Zala Mihály: Nemzetbiztonság – biztonsági tudatosság. in: Boda J. – Dobák I. (szer.): A nemzetbiztonság technikai kihívásai a 21. században. Nemzeti Közszolgálati Egyetem. 2015. alapján

A fenti leírásban:

- szándék: ebben az esetben ez azt jelenti, hogy az ember és a szabályozás eltávolodik, így a szabályozás vagy nem írja elő kellően a követendő magatartást és emiatt lehetőséget biztosít az ártó szándékú felhasználóknak büntetlenül elkövetni bizonyos cselekedeteket, vagy fordítva, hiába a precíz előírások, ha azokat az ember szándékosan vagy gondatlanul nem tartja be. Mindkettő csökkenti az információvédelem elvárt vagy elérhető szintjét.
- lehetőség: ebben az esetben ez azt jelenti, hogy a logikai, fizikai védelmi elemek képességei a szabályozástól eltávolodva nem képesek teljesítik az azokban leírt követelményeket, vagy épp fordítva a szabályozás olyan lefedetlen területeket biztosít, amely technológiai oldalról kezelhetők lennének, ám ezek hiányában alkalmazásuk nem lesz kötelező. Itt is mindkettő csökkenti az információvédelem elvárt vagy elérhető szintjét.
- sérülékenység: ebben az esetben ez azt jelenti, hogy az ember tudása a meglévő technológia képességektől eltávolodva vagy nem képes kihasználni az azokban rejlő lehetőségeket, vagy az eszközök nem lesznek képesek az ember által elvárt és beállítandó biztonsági szolgáltatásokat nyújtani. Itt is mindkettő csökkenti az információvédelem elvárt vagy elérhető szintjét.[149]

Az elektronikus információk védelme kapcsán az adminisztratív védelem kialakításakor megjelenő konkrét kontrollok listáját a 41/2015. (VII. 15.) BM rendeletben lehet megtalálni. A téma szempontjából praktikus ezen végigmenni és megnézni ezek

[149] Mádi-Nátor Anett, Kardos Zoltán: Információbiztonság-tudatosság gyakorlat. Nemzeti Közszolgálati Egyetem. 2014.

kialakítását a gyakorlatban, függetlenül attól, hogy az Ibtv. hatálya alá tartozó vagy nem tartozó szervezetről beszélünk. Minden esetben teszünk kitekintést is, hogy a 41/2015. (VII. 15.) BM rendeletben leírtak mellett még mit érdemes figyelembe venni a hatékony adminisztratív védelem kialakítása érdekében.

7.1. Szervezeti szintű alapfeladatok

A 41/2015. (VII. 15.) BM rendeletben ebben a pontban az informatikai biztonsági szabályzat (IBSZ), az elektronikus információs rendszerek biztonságáért felelős személy, az intézkedési terv és mérföldkövei, az elektronikus információs rendszerek nyilvántartása, valamint az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás jelenik meg kontrollként.
Ezek fontosak és elengedhetetlen részét képezik az védelemnek, de a felsorolt feladatokat a gyakorlatban célszerű ennél kiterjesztettebben megvalósítani egy adott szervezeteknél. A korábbi fejezetekben már említett információbiztonsági irányítási rendszer (IBIR) kialakítása és üzemeltetése mindenképp megcélzandó feladat. Az IBIR a Muha – Krasznay szerzőpáros szerint: *„egy általános irányítási rendszer, amely az üzleti kockázatelemzésén alapul, megállapítja, megvalósítja, üzemelteti, ellenőrzi, karbantartja és javítja az információbiztonságot … magában foglalja a szervezetet, a struktúrát, a szabályzatokat, a tervezési tevékenységeket, a felelősségeket, a gyakorlatokat, az eljárásokat, a folyamatokat és az erőforrásokat.”* [150]
Egy viszonylag nagyobb szervezet esetében ez saját alkalmazottakkal képes működni, de a kisebb méretű szervezeteknél erre a feladatra külső vállalkozó bevonása is megoldás lehet. Ennek lényeges részei a biztonsági dokumentumok meghatározása, elkészítése és lefogadása. Ebbe a körbe tartozik a korábban már szintén említett és a 41/2015. (VII. 15.) BM rendeletben külön is megjelenő IBSZ-en felül az informatikai biztonsági politika és a stratégia, de ide tartoznak az adott szervezet információbiztonságot érintő egyéb belső szabályzatai, munkautasításai is. Ilyenek lehetnek például a következők:

- informatikai biztonságpolitika
- IBIR kézikönyv;
- integrált kockázatkezelési szabályzat;
- gépterem üzemeltetési szabályzat;
- vállalatbiztonsági szabályzat;
- fegyelmi szabályzat;
- incidenskezelési szabályzat;
- nemzetbiztonsági ellenőrzésről szóló szabályzat;
- adatközpont- és gépteremüzemeltetési biztonsági szabályzat;
- hozzáférési- és jogosultságkezelési szabályzat;
- sérülékenység menedzsment szabályzat;
- üzletmenetfolytonossági tervek;
- katasztrófaelhárítási tervek;
- stb.

Az elektronikus információs rendszerek biztonságáért felelős személy kijelölése kötelező elem az Ibtv. hatálya alá tartozó szervezeteknél. Amit a gyakorlatban érdemes figyelembe venni, hogy egyrészt még az Ibtv. hatálya alá tartozó szervezeteknél is lehetnek olyan infokommunikációs rendszerek, amelyek nem az Ibtv. definíciója szerinti elektronikus

[150] Muha Lajos – Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése. 2018. Nemzeti Közszolgálati Egyetem. p.39.

információs rendszer fogalomkörbe esnek, ám védelmükről gondoskodni kell, másrészt a nem az Ibtv. hatálya alá tartozó szervezetek infokommunikációs rendszereit is védenie kell valaki(k)nek. A nagyobb vállalatok, intézmények önálló kiberbiztonsági szakembert foglalkoztatnak, jobb esetben több emberből álló csapatot, míg a kisebbek ezt a képességet külsős vállalkozóval, vagy céggel oldják meg. Adott esetben a kisebb szervezeteknél kötelező elektronikus információs rendszerek biztonságáért felelős személy is lehet külsős vállalkozó, akár több szervezetnél párhuzamosan is betöltve ezt a pozíciót. A kiberbiztonsági szervezeteket működtető nagyobb vállalatok esetében ebben a csapatban olyan feladatokat láthatnak el, mint a fentebb említett IBIR kialakítása, működtetése, ennek kapcsán a kockázatelemzés, -kezelés, kiberbiztonsági szabályozások gondozása, a cég infokommunikációs fejlesztéseinél a biztonsági szempontok érvényesítése, incidenskezelés, beleértve a hatósági kapcsolattartást is, kiberbiztonsági adatszolgáltatási tevékenység végzése, a 41/2015. (VII. 15.) BM rendeletben is előírt kiberbiztonsági intézkedési tervek gondozása, az elektronikus információs rendszerek és más infokommunikációs rendszerek nyilvántartása, valamint az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárások végigvitele.

7.2. Kockázatelemzés

A 41/2015. (VII. 15.) BM rendeletben ehhez a kategóriához a kockázatelemzési és kockázatkezelési eljárásrend, a biztonsági osztályba sorolás és a kockázatelemzés van felsorolva.

A biztonsági osztályba sorolás az Ibtv. által előírt elem, ám az jól alkalmazható a nem a hatálya alá tartozó szervezeteknél is.

A kockázatelemzési eljárásrend rögzíti azokat az alapokat, amelyek mentén a kockázatelemzést el kell végezni, A gyakorlatban érdemes a szervezetnél egységes elvek szerint megtenni ezt minden olyan helyen, ahol kockázatelemzést alkalmaznak. Érdemes az alkalmazott módszer kiválasztására is odafigyelni. Egy multinacionális vállalatnál honi cégénél lehetséges, hogy az anyavállalat által előírt módszert kell alkalmazni, ám ha nemzeti létfontosságú rendszerelemekkel is rendelkezik, akkor az OKF[151] által kiadott sablon[152] alapján mindenképp el kell végezni a kockázatelemzést. Éppen ezért azon cégeknél, akik nemzeti létfontosságú rendszerelemet üzemeltetnek, célszerű az OKF sablon szerinti módszertan alapján egységesen végezni a kockázatelemzést, még akkor is, ha a vizsgálandó elemek el is térnek a sablonban rögzítettektől. Ez azonban a nem kötelezett cégeknél i s egy jó, és főleg elfogadott módszertan lehet, így számukra is ajánlható ennek a használata.

Az OKF sablonban található módszertan a következő:

Gyakoriság:	
*1.**nagyon ritka:***	10 éven belül legalább egyszer bekövetkezik
*2.**ritka:***	5 éven belül legalább egyszer bekövetkezik
*3.**alkalmankénti:***	5 éven belül többször bekövetkezik
*4.**gyakori:***	1 éven belül legalább egyszer bekövetkezik
*5.**nagyon gyakori:***	1 éven belül többször bekövetkezik

[151] OKF: Országos Katasztrófavédelmi Főigazgatóság

[152] OKF: Letölthető dokumentumok és kitöltési segédletek https://www.katasztrofavedelem.hu/35635/letoltheto-dokumentumok-es-kitoltesi-segedletek

Hatás:	
1. elhanyagolható:	- csekély negatív hatása van a rendszerelem belső folyamataira (1 napon belül megoldható) - a szervezet belső és külső megítélését nem érinti - nincs érzékelhető informatikai kiesés - fokozott üzemszintű meghibásodás a kritikus erőforrásokban - személyi állományában bekövetkezett változás - vagyoni kár nem mérhető
2. alacsony:	- alacsony negatív hatás van a rendszerelem belső folyamataira (1 napon túl de 5 napot el nem érően megoldható) - kizárólag a szervezet belső megítélését érinti - csekély mértékű informatikai kiesést okoz - okozott üzemszintű meghibásodás a kritikus erőforrások állományában és folyamataiban - a vagyoni kár az üzemeltető éves költségvetésének 1%-át el nem érő összeg
3. közepes:	- negatív hatás a rendszerelem belső folyamataira (5 napon túl megoldható) - a szervezet belső és külső megítélését egyaránt érinti - informatikai rendszer(ek) kevesebb, mint 30 perc kiesése - üzletfolytonosság részleges vagy teljes időbeli leállása a kritikus erőforrások állományában és folyamataiban - a vagyoni kár az üzemeltető éves költségvetésének 1%-át meghaladó, de 5%-át elnem érő összeg
4. magas:	- a rendszerelem csökkentett mértékben képes alapfeladatainak megfelelni - a szervezet belső és külső megítélését jelentősen érinti (részleges bizalomvesztés) - a redszerelem tekintetében kritikus informatikai rendszer kiesése 30 perc – 4 óra időtartam között - kritikus erőforrások részleges vagy teljes (30 percnél több, de 4 óránál kevesebb) leállása - a vagyoni kár az üzemeltető éves költségvetésének 5%-át meghaladó, de 25%-át el nem érő összeg
5. katasztrofális:	- a rendszerelem nem képes alapfeladatainak megfelelni - a szervezet belső és külső megítélését igen jelentősen érinti (teljes bizalomvesztés) - a redszerelem tekintetében kritikus informatikai rendszer kiesése 4 óra időtartamot meghaladóan - a kritikus erőforrások 4 órát meghaladó leállása - a vagyoni kár az üzemeltető éves költségvetésének 25%-át meghaladó összeg

a bekövetkezési valószínűség	nagyon ritka	1
	ritka	2
	alkalmankénti	3
	gyakori	4
	nagyon gyakori	5

veszélyeztető hatások szintje	elhanyagolható	1
	alacsony	2
	közepes	3
	magas	4
	katasztrofális	5

kitettség értékei	nincs kitettség	0
	egy fél felé van kitettség	1
	több fél felé van kitettség	2

	elhanya-golható	**alacson y**	**közepes**	**magas**	**kataszt-rofális**
nagyon ritka	1	2	3	4	5
ritka	2	4	6	8	10
alkalmankénti	3	6	9	12	15
gyakori	4	8	12	16	20
nagyon gyakori	5	10	15	20	25
kitettség értékelése (a hatás értékét növeli)					
nincs kitettség	0				
egy fél felé van kitettség	1				
több fél felé van kitettség	2				

Kockázati értékek besorolása	
20-25	azonnali beavatkozást, megelőző védelmi intézkedést igénylő kockázat
15-19	megelőző védelmi intézkedést igénylő kockázat
10-14	intézkedést igénylő kockázat
5-9	tervezett, későbbi intézkedést igénylő kockázat
1-4	elhanyagolható kockázat

A számítás metódusa	A kockázati érték kiszámítása a következő képlettel történik: (veszélyeztető hatás szintje + kitettség) × bekövetkezési valószínűség. Annak érdekében, hogy ne haladja meg a mátrix legfelső értékét, a kapható eredmény értéke 25-ben került limitálásra. Tehát 25-nél magasabb kockázati érték esetében a "Kockázatelemzés KIV' munkalap" jelenlegi kockázat" ('L') oszlopában található cellákban 25 kerül megjelenítésre.

A **kitettség** érték számítása: olyan hatások (főként szolgáltatások) vehetők figyelembe, melyek a létfontosságú rendszerelem által nyújtott szolgáltatás nyújtását befolyásolják, és amelye(ke)t a létfontosságú rendszereleme a szolgáltatása nyújtásához igénybe vesz mástól. Ilyen lehet különösen (de nem kizárólag) az áram-, vagy az internetellátás, esetlegesen különböző karbantartási szolgáltatások, melyeket az üzemeltető más cégtől, vesz igénybe, ám az általuk nyújtott szolgáltatásra nem, vagy korlátozott a ráhatása.

7. ábra OKF kockázatelemzési módszertan magyarázat

Forrás: 80174.xlsx https://www.katasztrofavedelem.hu/35635/letoltheto-dokumentumok-es-kitoltesi-segedletek Letöltve: 2023.03.11.

A kockázatelemzést ennek alapján az egyes rendszerekre el lehet végezni, majd ennek alapján össze lehet állítani a szükséges intézkedéseket és el lehet készíteni hozzá az ütemtervet, valamint fel lehet vállalni bizonyos kockázatokat. Ennél is nagyon fontos a korábban már említett üzletvezérelt biztonság és üzletvezérelt információbiztonság megközelítés.

7.3. Rendszer és szolgáltatás beszerzés

A 41/2015. (VII. 15.) BM rendeletben ebben a kategóriában a beszerzési eljárásrend és erőforrás igény felmérés, a beszerzések, a védelem szempontjainak érvényesítése a beszerzés során, a védelmi intézkedések terv-, és megvalósítási dokumentációi, a funkciók - protokollok – szolgáltatások, az elektronikus információs rendszerre vonatkozó dokumentáció, a biztonságtervezési elvek, a külső elektronikus információs rendszerek szolgáltatásai, a független értékelők, a folyamatos ellenőrzés és a független értékelés szerepelnek.

A gyakorlatba átültetve ez azokat a feladatokat fogja össze, amelyek egy új infokommunikációs szolgáltatás és az ahhoz kapcsolódó rendszerek esetében az ötlet felmerülésétől az üzembe helyezésig jelentkeznek. Itt már az első pillanattól kezdve következetesen érvényesíteni kell az információbiztonsági alapelveket, amelyeket a korábbi részben leírt dokumentumok (pl. IBSZ) tartalmaznak. Itt is kockázatelemzés alapján kell dönteni a jogszabályi előírásokon felül megvalósítandó kontrollokról, figyelve arra, hogy azok jól illeszkedjenek az adott szervezet már meglévő védelmi elemeihez.

Kiemelendő, hogy. a hazai jogszabályok az Ibtv. és a 41/2015. (VII. 15.) BM rendelet alapvetően a NIST 800-53[153] előírásain alapulnak annak is a korábbi változatain (rev.4.), és egyértelműen arra a modellre épülnek, amikor az elektronikus információs rendszer teljes egészében az azt használó szervezeté, akárcsak az abban kezelt adatok és azok kezelésének, feldolgozásának összes folyamata is. Ennek megfelelően az ezekben a jogszabályokban előírt információbiztonsági kontrollok megvalósítását is egységesen

[153] Security and Privacy Controls for Federal Information Systems and Organizations NIST Special Publication 800-53 Revision 4. 2013. 04. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

kezelik, a mára oly jellemző felhő alapú rendszerek használata és az abból adódó feladat és felelősség elhatárolásának a gondolata megjelenik ugyan a szövegben, ám azok tényleges, egyértelmű szétválasztása már nem történt meg. Márpedig a felhő alapú rendszerek használata nem csupán a magánszférában, hanem az államiban is elterjedt. Amíg a magánszféra vállalatai jellemzően a nagyobb publikus szolgáltatások (pl. Microsoft Azure, AWS stb.) közül választanak, addig az állami szereplők a NISZ Zrt.-től, mint központi kormányzati infokommunikációs szolgáltatótól vehetnek igénybe ilyen szolgáltatásokat. Ám amíg a NISZ Zrt.-re az Ibtv. és a 41/2015. (VII. 15.) BM rendelet előírásai egy adott rendszer esetében ugyanolyan kötelező érvényűek, mint a rendszert használó intézményre, addig ez a más felhő szolgáltatókról nem mondható el. Ma már a publikus felhőszolgáltatók is számos biztonsági funkciót kínálnak, amelyek közül a felhasználó választhat, ám a korábban is említett zárt, teljes körű, folytonos és a kockázatokkal arányos védelem kialakítása érdekében a felhasználónak a biztonsági kérdéseketalaposan körül kell járnia és érvényesítenie kell partnerei, így a felhőszolgáltató irányába is.
Az előző bekezdés alapvetően a felhőszolgáltatásokról szólt, de az utolsó mondatban nem véletlenül szerepelt már a jóval tágabb partnerek kifejezés. Ugyanis nem csupán felhőszolgáltatók lehetnek az adott intézmény partnerei egy infokommunikációs rendszer kapcsán, épp ezért a teljes ellátási láncban biztosítani kell az adott vállalatnál, intézménynél előírt információbiztonsági követelményeket. Sokszor ugyanis a támadók számára sokkal könnyebb célpontot jelentenek az ellátási lánc szereplői, akiknél ezek a követelmények gyengébbek lehetnek. Erre mutat példákat az ENISA 2021-ben kiadott tanulmánya[154] is erre hívja fel a figyelmet. Tanulmányukban 24 olyan publikusan is bejelentett és igazolt, az ellátási láncot ért támadást elemeznek, amelyeket 2020. január és 2021. július között következtek be. A NIST 800-53 legújabb, rev5. változatában[155] már önálló pontként szerepel az ellátási lánc kezelése (CHAPTER THREE: THE CONTROLS, 3.20 SUPPLY CHAIN RISK MANAGEMENT), amelyet mindenképp célszerű felhasználni az infokommunikációs rendszerek és szolgáltatások beszerzése során.

7.4. Üzletmenet (ügymenet) folytonosság tervezése

Az üzletmenetfolytonosság kapcsán is meg kell jegyezni, hogy akárcsak az üzletvezérelt biztonság fogalmánál, ebben az esetben is tágabban kell értelmezni az üzletmenet fogalmát, Itt természetesen egy állami intézmény jogszabályban meghatározott feladatrendszerét, vagy egy nonprofit vállalat tevékenységi körét ugyanúgy figyelembe kell venni, ahogy a piaci alapon működő vállalatok hagyományos értelemben vett üzleti céljait.
A 41/2015. (VII. 15.) BM rendeletben ebben a kategóriában 33 kontroll szerepel, így az üzletmenet folytonosságra vonatkozó eljárásrendtől kezdve a kritikus rendszerelemek meghatározásán, a folyamatos működésre felkészítő képzés, szimuláción, vagy az üzletmenet folytonosság helyreállításán keresztül a helyreállítási időig találunk elemeket. Jellemző, hogy ezek döntő többsége csupán a 4-es biztonsági osztálytól felfelé kötelező elem, és a 33-ból csupán 5 db. 3-as, vagy annál alacsonyabb besorolásnál.

---

[154] ENISA Threat Landscape for Supply Chain Attacks. 2021. július. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks Letöltés ideje: 2021. 08. 31.

[155] Security and Privacy Controls for Information Systems and Organizations NIST Special Publication 800-53 Revision 5. 2020. 09. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Az üzletmenetfolytonosság tervezés elméleti alapjait kiválóan foglalja össze a Muha – Krasznay szerzőpáros „Az elektronikus információs rendszerek biztonságának menedzselése”[156] című könyv 5.2.5. fejezetében.
A gyakorlati megvalósítás kapcsán az alábbiakat célszerű figyelembe venni. Az üzletmenetfolytonosság menedzselését (BCM[157]) jellemzően még a nagyobb szervezeteknél is csupán 1-2 erre kijelölt ember végzi, kisebb szervezetek esetében akár külsős vállalkozó, cég is elláthatja ezt a feladatot. Ők a gyakorlatban összefogják ezt a munkát és a szervezet egyéb területein kijelölt kapcsolattartókkal szorosan együttműködve biztosítják a szükséges feladatok elvégzését. A BCM összefogásáért felelős szakemberek jellemzően a vállalatbiztonságon belül kapnak helyet, ők állítják össze a feladatterveket, készítik el a teljes szervezeten átívelő üzletmenetfolytonosság terveket (BCP[158]), mint például a pandémiás terv, bombariasztás miatti kiürítési terv stb. és készíttetik el a kijelölt kapcsolattartókon keresztül szervezet adott egységeinek speciális terveit, pl. számlázási rendszer kiesését lefedő tervet.
Fontos kiemelni, hogy a BCP-k rövid időszakot, jellemzően maximálisan 1-2 napot fednek le és az üzletmenet minimálisan szükséges helyreállításáról szólnak, időt adva a normál üzletmenet, azaz a korábbi teljes folyamat visszaállítására. Így a fenti példánál megmaradva a pandémiás tervnek be kell mutatnia, hogy mi a teendő egy tömeges fertőzés esetén, amikor pl. egyszerre esik ki a munkából egy váltásban dolgozó meghatározó mennyiségű munkatárs, hogyan történjenek a váltások átalakítása, a berendelések, a dolgozók beszállítása a tömegközlekedés kikerülésével, hogyan csökkentsük minimálisra a munkahelyi továbbfertőzések lehetőségét stb. Szintén fontos kiemelni, hogy azokat a BCP-ket, amelyek már az adott szervezet speciális területeinek üzletmenetfolytonosságát hivatottak biztosítani, az érintett részlegeknek szükséges nem csupán kidolgoznia, de azt is meghatároznia, hogy milyen tervek szükségesek. Ugyanis ők ismerik legjobban a munkafolyamataikat és látják azt, melyek kritikusak és hol vannak olyan szűk keresztmetszetek, melyek adott esetben teljesen megbéníthatják a normál folyamatokat.
A BCP-khez szorosan kapcsolódnak az ún. DRP-k, azaz a vészhelyzeti helyreállítási tervek. Ezek szolgálnak például egy adott rendszerben bekövetkezett leállás (pl. zsarolóvírus támadás okozta kiesés) után az adott rendszer üzemének teljes visszaállítására. Ezeket azonban jellemzően nem a BCP-vel foglalkozó szakemberek készítik, készíttetik el, hanem az vagy az adott részleg (pl. IT üzemeltetés) önálló feladata, vagy esetleg a kibervédelemért felelős szervezeti egység összefogásával valósul meg, a BCM mintájára, kijelölt kapcsolattartókon keresztül. Az viszont már így is egyértelműen látszik, hogy egyrészt ezeknek a terveknek egymással összhangban kell elkészülnie, másrészt üzletmenetfolytonosságban és a vészhelyzeti helyreállításban dolgozó kollégáknak szorosan együtt kell működnie. Erre jellemző példa, hogy az 41/2015. (VII. 15.) BM rendelet által is előírt szimulációkat (gyakorlatokat) legtöbbször együtt tartják meg. Definíció szerint a szimuláció alatt a következőt kell érteni: „a folyamatos működésre felkészítő képzésben szimulált eseményeket kell alkalmazni, hogy elősegítse a személyzet hatékony reagálását a kritikus helyzetekben”[159].

---

[156] Muha Lajos – Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése. 2018. Nemzeti Közszolgálati Egyetem. pp.44.-19.

[157] BCM: Business Continuity Management

[158] BCP: Business Continuity Plan

[159] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre,

7.5. A biztonsági események kezelése

A 41/2015. (VII. 15.) BM rendeletben ebben a kategóriában szintén jelentő számú, 15 kontroll szerepel, ezek közül csupán 6 db. kötelező 3-as, vagy annál alacsonyabb biztonsági osztály besorolásnál. Az itt található kontrollok egy része a logikai és fizikai biztonsági elemekből származó események és riasztások kezelésének rendjét hivatottak adminisztratív módon kezelni. Ilyenek például a biztonsági eseménykezelési eljárásrend, az információ korreláció, vagy a biztonsági események jelentése. Tekintettel a nagyszámú biztonsági eseményre (egy közepes méretű vállalatnál a logikai védelmi elemekből naponta több tíz-, vagy több százezer (!) esemény – az Ibtv. és a 41/2015. (VII. 15.) BM rendeletben incidensnek nevezik – keletkezhet) ezek kezelését a lehető legnagyobb mértékig automatizálni kell. Ezekre is találhatók előírások, mint például az automatikus eseménykezelés, az automatizált jelentés, az automatizált támogatás, vagy akár az automatizált képzési környezet. Ez utóbbi rögtön át is vezet a másik nagy halmazhoz, hiszen az itt felsorolt kontrollok egy másik része az események kezeléséhez szükséges képzéssel és támogatással foglalkozik, mint például a biztonsági eseménykezelési terv, a képzés a biztonsági események kezelésére, vagy a biztonsági események kezelésének tesztelése.

Kiemelendő, hogy az Ibtv. és a 41/2015. (VII. 15.) BM rendelet szóhasználata eltér az angolszász irodalom szóhasználatától. Az Ibtv. szerint biztonsági esemény: *„nem kívánt vagy nem várt 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;”*[160], míg erre pl. a NIST 800-53 az incident (incidens) kifejezést használja, míg az egyedi. de az elektronikus információs rendszer által hordozott információ bizalmasságát, sértetlenségét, hitelességét, funkcionalitását vagy rendelkezésre állását még nem feltétlenül sértő biztonsági eseményre használja az event (esemény) kifejezést.

A gyakorlatban a biztonsági események kezelését általában egy központban végzik, itt végződtetik azokat a logikai és/vagy fizikai védelmi elemeket, amelyeket az adott vállalat vagy intézmény használ. A nagyobb szervezeteknél jellemzően saját operatív központot tartanak fenn, míg a kisebbek jellemzően ezt igénybe veszik valakitől. A csak a logikai védelmi elemekből származó események kezelését végző központot CSOC-nak, (CyberSecurity Operation Center – kiberbiztonsági operatív központ), míg a fizikai vagy fizikai és kiberbiztonsági eseményeket kezelőket SOC-nak (Security Operation Center – biztonsági operatív központ) szokták nevezni. Ezek jellemzően – a 41/2015. (VII. 15.) BM rendeletben is megjelenítettek szerint – magas fokú automatizálást használnak, a heterogén védelmi eszközparkból érkező nagyszámú esemény közül jellemzően egy egységes felületen csak a szakemberek által beállított szabályoknak megfelelő incidenseket (Ibtv. szerinti eseményeket) jelenítik meg valamilyen SOAR[161] eszköz segítségével, így biztosítva az incidensek magas szintű egységes megjelenítését, gyors felismerését és kezelését. Természetesen a SOC-ban ülő operátorok elérik a biztonsági

termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet.

[160] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény. https://net.jogtar.hu/jogszabaly?docid=a1300050.tv letöltve: 2023.01.22.

[161] SOAR: security orchestration, automation and response biztonsági incidensek összehangolt, automatizált kezelését, és lereagálását lehetővé tévő eszköz

eszközöket és azok saját felületein mélyebb elemzést is végre tudnak hajtani azon incidenseknél, ahol erre szükség van.
Amennyiben a kiberbiztonsági és a fizikai eseményeket, incidenseket kezelő központ külön található – erre számtalan vállalat, intézmény esetében van példa, ahol a fizikai eseményeket a vállalatbiztonsági, a kibertérből származókat pedig a kiberbiztonsági csapat kezeli – akkor ezek összehangolt együttműködését mindenképp meg kell teremteni. Ez szintén adminisztratív úton, például szabályzók kiadásával lehetséges.
Szintén fontos kiemelni, hogy amíg egy nem az Ibtv. hatálya alá eső szervezet maga dönt a sérülékenységvizsgálatról, hogy azt adott esetben mely külső vállalkozótól rendeli meg, addig erre az Ibtv. hatálya alá eső szervezetek esetében komoly előírások vannak. Bizonyos szervezetek esetében ugyanis csak a Nemzeti Kibervédelmi Intézet (NKI) végezhet ilyen tevékenységet, más szervezetek számára pedig kizárólag az Alkotmányvédelmi Hivatalnál regisztrált vállalkozások láthatnak el sérülékenységvizsgálati feladatokat. A sérülékenységvizsgálat azonban egy pillanatképet biztosít csak, azt mondja meg, hogy az adott pillanatban hol vannak problémák a vizsgált rendszer(ek)ben. Ugyanakkor a SOC tevékenység már nincs ilyen módon szabályozva, azaz ezt bármely Ibtv. alá eső szervezet bármely vállalkozótól igénybe veheti. Itt a SOC alatt most a kiberbiztonsági eseményeket (is) kezelő központot értjük. Pedig ez lényegesen magasabb kockázatot rejt, hiszen egy SOC-ban nem statikus hanem dinamikus képet láthatunk a vállalatról, amely jóval nagyobb kitettséget jelent. Éppen ezért az Ibtv. hatálya alá eső szervezet esetében a sérülékenységvizsgálatnál alkalmazott jogszabályi korlátokhoz hasonlóan a biztonság mint szolgáltatás esetében is ki kell dolgozni a jogszabályi kereteket, egyértelműen rögzítve, hogy mely szolgáltatók milyen feltételek mellett működhetnek, az állami, önkormányzati szerveknek mikor kell vagy lehet adott esetben az Nemzeti Kibervédelmi Intézetet, mikor a NISZ Zrt.-t, és mikor külső gazdálkodó szervezetet mint menedzselt biztonsági szolgáltatót igénybe venniük, és ezt milyen feltételekkel tehetik meg. A nem az Ibtv. hatálya alá eső szervezeteknél pedig nagy körültekintéssel kell kiválasztani azt a partnert, akitől ilyen szolgáltatást igénybe kívánnak venni és a szerződésben gondosan ügyelni kell a teljes körű szabályozottságra.

7.6. Emberi tényezőket figyelembe vevő - személy – biztonság

A személybiztonsági résznél található 9 db. adminisztratív intézkedések két nagyobb csoportba sorolható. Az elsőbe tartoznak a belső munkatársakkal és külső közreműködőkkel kapcsolatos védelmi előírások, mint például a munkakörök, feladatok biztonsági szempontú besorolása, a személyek ellenőrzése, az érintett szervezettel szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények, vagy a fegyelmi intézkedések. A másik csoportba tartozik a viselkedési szabályok az interneten. Ez utóbbit célszerű az IBSZ-ben leszabályozni, természetesen az adott szervezet működési területét, specialitásait figyelembe véve.
A gyakorlatban az első csoportba tartozó kontrollokat jellemzően a vállalatbiztonság és a HR terület fogja össze. A megbeszélt megosztás alapján ők végzik a belépők és a külső közreműködők előzetes ellenőrzését, adott esetben kezdeményezik azok nemzetbiztonsági ellenőrzését vagy annak megújítását, rögzítik a szakterületek bevonásával az egyes munkakörök biztonsági besorolást, hajtják végre a fegyelmi eljárásokat és az ahhoz szükséges belső vizsgálatokat stb. Ezen feladatokat nem csupán az Ibtv. által érintett személyek és munkakörök, hanem jellemzően a teljes vállalatra, intézményre célszerű elvégezni. A vállalatbiztonság és a HR közötti feladatmegosztás nagyban függ az adott szervezetnél meglévő viszonyoktól, például, hogy a HR

gyakorolja-e a munkáltatói jogokat vagy sem, így a helyi sajátosságokra mindig figyelemmel kell lenni.

7.7. Tudatosság és képzés

A 41/2015. (VII. 15.) BM rendeletben ebben a kategóriában összesen 6 kontroll szerepel, ezek közül csupán 1 db. van, amely csak 4-es biztonsági osztály besorolástól kötelező. A képzéssel kapcsolatos kontrollok mellett (képzési eljárásrend, biztonság tudatosság képzés, szerepkör vagy feladat alapú biztonsági képzés, a belső fenyegetések felismerésére szolgáló oktatások és a biztonsági képzésre vonatkozó dokumentációk) egy tudatossággal összefüggő kontrollt (kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével, és az e célt szolgáló ágazati szervezetekkel) találhatunk.

A gyakorlatban a tudatosító és képzési feladatokat jellemzően a vállaltbiztonsági és a kiberbiztonsági területek látják el, kezdve a belépéskor kiadott biztonsági alapszabályokat rögzítő pl. 10 pontos szórólaptól a rendszeres időközönként megjelentett belső tudatosító hírleveleken, a kötelezően elvégzendő elearning oktatásokon át az eseményhez kötött (pl. adathalász emailkampányt követően) tudatosító anyagok elkészítéséig. Ide tartozik a kiberbiztonsági terület által készített tudatosító adathalász levelek kiküldése és kiértékelése, amelyek többszöri alkalmazásával egyre kifinomultabb formában készíthetik fel a dolgozókat ezen veszélyek felismerésére és elkerülésére. De ide tartoznak a pszichológiai manipulációt (angol nevén social engineering) használó tudatosító képzések is, amelyekkel fel lehet ismertetni például pl. egy elejtett pendrive vagy egy pizzásdobozokkal teli kéz miatt kártyalehúzás nélkül beléptetést kérő nem ismert „kolléga” okozta veszélyét.

Érdemes a gyakorlatban a különböző biztonsági és azokkal szorosan összefüggő területeknek időnként összefogott kampányokat indítani. Így például a vállalatbiztonság, a kiberbiztonság az adatvédelmi felelőssel és a megfelelőségért felelős vezetővel és a korrupcióellenes tevékenységért felelős vezetővel együtt biztonsági hetet rendezhet, ahol különböző játékos formában (pl. kvízek, szabadulószoba stb.) megtartott eseményeken fokozhatják a dolgozó biztonságtudatosságát.

Szintén fontos tudatosító tevékenység a külföldre utazó kollégák információbiztonsági felkészítése. Így például ennek keretében el lehet mondani, hogy mire figyeljenek a céges adatokat tartalmazó laptopjuk tárolásakor, hol és hogyan használják úgy, hogy annak kijelzője más számára nem legyen olvasható, az ingyenes WiFi hálózat használatának milyen veszélyei vannak stb. Ugyancsak fontos terület a kilépő kollégák figyelmének felhívása a szervezeti adatok további védelmének követelményéről. Ezek történhetnek személyes megbeszélés, de akár írásos formában átadott „tananyag” segítségével, míg a külföldre utazás esetén akár egy elearning képzés is szóba jöhet.

7.8. Adatosztályzás

Ami a 41/2015. (VII. 15.) BM rendeletben nem szerepel az adminisztratív intézkedések között, pedig bevezetése az Ibtv. hatálya alá tartozó szervezetek esetében is fontos lenne, azaz adatosztályzás. Az állami szférában ezt a minősített adatokon kívül nem használják, míg a nem állami vállalatok esetében ezt, elsősorban a nagyobb és információbiztonság érettebb szintjén lévő vállalatoknál igen. A minősített adatokról itt nem beszélünk bővebben, a téma szempontjából kizárólag a nem minősített adatok osztályozása érdekes. A nem minősített adatok osztályozása két szempontból is fontos. Az egyik az, hogy minden vállaltnak, intézménynek vannak védendő adatai. Az adott intézménynél előállított különböző dokumentumok azonban nem egyformán védendők. Például amíg egy megbeszélés meghívó illetéktelen kezekbe kerülése, ami tartalmazza a meghívottak

körét, témáját, esetleg egy csatolt prezentációt, kellemetlen, de az esetek többségében csupán rövid távú vagy kis mértékű negatív hatást fejt ki az adott szervezetre, addig egy rövid feljegyzés, emlékeztető egy megbeszélésről tartalmazhat fontos információkat, amely már jobban védendő, de egy stratégiai, vagy döntés előkészítő anyag illetéktelen kezekbe kerülésének akár hosszú távú vagy jelentős hatású következményei is lehetnek. Ezek besorolását pedig akkor lehet megtenni, ha – a minősített adatokhoz hasonlóan – világos szabályok kerülnek ehhez lefektetésre. A másik szempont pedig az, hogy a megfelelő, hatékony védelmet akkor tudjuk kialakítani, ha az adatok osztályzására már előzetesen sor került. Így például a fontosabb adatok csak megfelelő titkosító algoritmussal védve kerüljenek tárolásra már a vállalat szerverein is, vagy az adatszivárgás elleni rendszer (DLP[162]) meg tudja akadályozni azok véletlen vagy szándékos kimásolását pendrive-ra, kiküldését vállalaton kívüli email címre, és egyben riasztást is generáljon a biztonsági szakemberek felé.
Az alábbiakban egy lehetséges módszert mutatunk be az adatok osztályozására. Egy adott szervezetnél kezelt adatok biztonságos feldolgozásához, tárolásához azok információtartalmán alapuló megfelelő bizalmassági (B) szintű besorolása az alábbiak szerint tehető meg. Az adatokat alapvetően 5 kategóriába oszthatjuk:

- B0 szintű adatok vagy magán adatok, amelyek nem védendők, tetszőleges módon és helyen, így akár nyilvános felhőben is tárolhatók. Ezek illetéktelen kézbe kerülése nem, okozhat anyagi vagy reputációs veszteséget a szervezetnek. Ilyenek lehetnek például:
    - magánlevelek,
    - magán dokumentumok.
- B1 szintű adatok vagy nyilvános adatok. amelyek nem védendők, tetszőleges módon és helyen, így akár nyilvános felhőben is tárolhatók. Ezek illetéktelen kézbe kerülése nem, okozhat anyagi vagy reputációs veszteséget a szervezetnek. Ilyenek lehetnek például:
    - közérdekű adatok,
    - közérdekből nyilvános adatok, közérdekű adatok,
    - sajtóközlemények,
    - nyilvánosságnak szánt tudatósító anyagok, cikkek, fehér könyvek stb.
- B2 szintű adatok vagy vállalati, intézményi belső, nem nyilvános adatok. amelyek már korlátozott mértékben védendők, de még tetszőleges módon és helyen, így akár EGT tagálamban elhelyezkedő nyilvános felhőben is tárolhatók. Ezek illetéktelen kézbe kerülése nem, vagy csak elhanyagolható mértékben okozhat anyagi vagy reputációs veszteséget a szervezetnek. Ilyenek lehetnek például:
    - napi operatív munkavégzéshez szükséges levelezés,
    - megbeszélés meghívók,
    - belső, intézményi használatra szánt dokumentumok, irányelvek,
    - olyan harmadik félhez tartozó adatok, amelyek nem képezik titoktartási megállapodás tárgyát,
    - minden olyan dokumentum/adat, ami intézményi/kormányzati körön belül terjeszthető.
- B3 szintű adatok vagy vállalati, intézményi belső, bizalmas adatok, amelyek már nagy mértékben védendők, a vállalat rendszereiben is titkosítottan tárolhatók,

[162] DLP: Data Loss Prevention, adatszivárgás megelőzés/védelem.

adott esetben felhőszolgáltatóhoz csak megfelelő szabályok betartásával vihetők (állami intézmény esetében ez csak kormányzati felhő lehet) és minden esetben ott is csak titkosítottan tárolhatók. Ezek illetéktelen kézbe kerülése jelentős anyagi vagy reputációs veszteséget okozhat a szervezetnek Ilyenek lehetnek például:

- szervezeti szintű szabályzatok, szabályozások,
- projektdokumentumok,
- személyes adatok,
- kis értékű beszerzések dokumentumai,
- árazási dokumentumok,
- ajánlatok.

- B4 szintű adatok vagy vállalati, intézményi belső, titkos adatok, amelyek a lehető legnagyobb mértékben védendők, a vállalat rendszereiben is titkosítottan tárolhatók, adott esetben felhőszolgáltatóhoz csak nagyon szigorú szabályok betartásával vihetők (állami intézmény esetében ez csak kormányzati felhő lehet) és minden esetben ott is csak titkosítottan tárolhatók. Ezek illetéktelen kézbe kerülése kritikus mértékű anyagi vagy reputációs veszteséget okozhat a szervezetnek Ilyenek lehetnek például:
  - különleges vagy tömeges személyes adatok,
  - üzleti titok,
  - törvénytervezetek,
  - költségvetési számok,
  - HR listák, fizetésjegyzékek,
  - vezetői döntéselőkészítő anyagok,
  - pénzügyi- és kontrollingadatok,
  - műszaki tervdokumentációk,
  - biztonsági incidensekhez, azok kivizsgálásához kapcsoló dokumentumok.

Ezt és a felhőben tárolás lehetőségét foglalja össze az alábbi 2. táblázat Adatok besorolása és felhőben tárolása lehetséges engedélyei.

Besorolás	Jellemző	Kormányzati közösségi felhő	EGT Publikus felhő	Publikus felhő
B1	Közérdekű adatok, közérdekből nyilvános adatok, valamint minden olyan adat tartozik ebbe a kategóriába, amit a szervezet nyilvánosként sorol be, így szervezeten belül és kívül szabadon terjeszthetők.	Igen	Igen	Igen
B2	Napi operatív munkavégzéshez szükséges, vagy a szervezet által keletkezett belső használatú adatok, így kiemelten a kormányzati igazgatási dokumentumok, olyan harmadik félhez tartozó adatok, amelyek nem képezik titoktartási megállapodás tárgyát, minden olyan dokumentum/adat, ami intézményi/kormányzati körön belül terjeszthető.	Igen	Igen	Nem
B3	A szervezet egyéb belső szabályozásában hozzáférés-korlátozás alá eső adatok, személyes adatok, valamint egyéb jogszabállyal védett titok. Olyan adatok és információk, amelyek nyilvánosságra kerülése anyagi, jogi, vagy reputációs kárt okozhat a szervezetnek.	Igen	Nem	Nem
B4	Különleges adatok, üzleti titok, valamint tömeges személyes adat. Olyan adatok és információk, amelyek nyilvánosságra kerülése jelentős anyagi, jogi, vagy reputációs kockázatot okozhat. Törvénytervezet, költségvetési számok.	Igen	Nem	Nem

2. táblázat Adatok besorolása és felhőben tárolása lehetséges engedélyei

Fontos megjegyezni, hogy a fent leírtakra az állami szférában (még) nincsenek szabályok, ám ezeket célszerű lenne minél előbb bevezetni, a magánszférában pedig vállalatonként

eltérő szabályozás is lehet, ha egyáltalán van ilyen. Így a fentiek csupán egy lehetséges megoldásnak tekinthetők.

Felhasznált irodalom

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény

Steven Schlarman: The People, Policy, Technology (PPT) Model: Core Elements of the Security Process. Information Security Journal: A Global Perspective p. 1-6 2006.12.21. https://www.tandfonline.com/doi/abs/10.1201/1086/43315.10.5.20011101/31719.6#preview letöltve: 2023.03.04.

Boda J. – Dobák I. (szer.): A nemzetbiztonság technikai kihívásai a 21. században. Nemzeti Közszolgálati Egyetem. 2015.

Mádi-Nátor Anett, Kardos Zoltán: Információbiztonság-tudatosság gyakorlat. Nemzeti Közszolgálati Egyetem. 2014.

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 szóló 41/2015. (VII. 15.) BM rendelet

Muha Lajos – Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése. 2018. Nemzeti Közszolgálati Egyetem.

OKF: Letölthető dokumentumok és kitöltési segédletek. https://www.katasztrofavedelem.hu/35635/letoltheto-dokumentumok-es-kitoltesi-segedletek Letöltve. 2023.03.11.

Security and Privacy Controls for Federal Information Systems and Organizations NIST Special Publication 800-53 Revision 4. 2013. 04. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf Letöltés ideje: 2017. 03. 18.

ENISA Threat Landscape for Supply Chain Attacks. 2021. július. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks Letöltés ideje: 2021. 08. 31.

Security and Privacy Controls for Information Systems and Organizations NIST Special Publication 800-53 Revision 5. 2020. 09. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf Letöltés ideje: 2023. 03. 10.

8. Fizikai biztonság a gyakorlatban

Az előző fejezetek bemutatták az információbiztonság legfontosabb elméleti ismereteit, az azokhoz kapcsolódó fontosabb jogszabályokat, majd ismertették ezek gyakorlatba történő átültetésének alapjait. Ezt követően a korábban ismertetett CIA elv alapján részletesen bemutatásra kerültek a logikai és adminisztratív védelmi elemek kialakításának gyakorlati kérdései, azok is oly módon, hogy a jogszabályi előírások mellett milyen üzletvezérelt információbiztonsági megfontolásokat célszerű figyelembe venni a hatékony védelem elérése érdekében. Jelen fejezet a CIA elv harmadik alappillérének, a fizikai biztonság gyakorlatban történő alkalmazásának a kérdéseit vizsgálja.

A fizikai védelem kialakítása ugyancsak elengedhetetlen része az információbiztonságnak. Az Ibtv. szerint ez *„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”*[163] összességét jelenti.

Az elektronikus információk védelme kapcsán a fizikai védelem kialakításakor megjelenő konkrét kontrollok listáját a 41/2015. (VII. 15.) BM rendeletben lehet megtalálni. Ezen téma szempontjából is célszerű ezt kiindulási alapnak tekinteni és megnézni az ezek kialakításához szükséges gyakorlati elemeket, függetlenül attól, hogy az Ibtv. hatálya alá tartozó vagy nem tartozó szervezetről beszélünk. A fizikai védelmi elemek gyakorlati kialakítása esetében a megvalósítás szerint csoportosítjuk azokat, valamint itt is teszünk kitekintést arra vonatkozóan, hogy a 41/2015. (VII. 15.) BM rendeletben leírtak mellett még mit érdemes figyelembe venni a hatékony fizikai védelem kialakítása érdekében.

A fizikai biztonsági elemek számosságát tekintve a legkisebb a három kontrollcsoport között, ami logikus is, hiszen egyrészt alapvetően logikai kontrollokra szükséges koncentrálni, másrészt a fizikai kontrollok régebb óta jelen vannak, jól körülhatároltak és kevésbé változnak, mint a logikai kontrollok. Ráadásul a fizikai biztonsági elemeket minden iparágban használták/használják, így azok természetesen beemelésre kerültek az elektronikus információs rendszerek védelmébe is. Mindemellett kiemelendő, hogy még 3-as biztonsági osztály esetén is csupán 11 kontrollt kötelező alkalmazni a megjelenített 30 közül, 2-es biztonsági osztály esetén pedig csupán 3-at.

A 41/2015. (VII. 15.) BM rendelet az alábbi bontásban adja meg a fizikai védelmi kontrollokat:

- Fizikai védelmi eljárásrend
- Fizikai belépési engedélyek
- A fizikai belépés ellenőrzése
    - Hozzáférés az információs rendszerhez
- Hozzáférés az adatátviteli eszközökhöz és csatornákhoz
- A kimeneti eszközök hozzáférés ellenőrzése
- A fizikai hozzáférések felügyelete
    - Behatolás riasztás, felügyeleti berendezések
- Az elektronikus információs rendszerekhez való hozzáférés felügyelete
- A látogatók ellenőrzése

[163] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény. https://net.jogtar.hu/jogszabaly?docid=a1300050.tv letöltve: 2023.01.22.

    - Automatizált látogatói információkezelés
- Áramellátó berendezések és kábelezés
    - Tartalék áramellátás
    - Hosszú távú tartalék áramellátás a minimálisan elvárt működési képességhez
- Vészkikapcsolás
- Vészvilágítás
- Tűzvédelem
    - Automatikus tűzelfojtás
    - Észlelő berendezések, rendszerek
    - Tűzelfojtó berendezések, rendszerek
- Hőmérséklet és páratartalom ellenőrzés
- Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem
    - Automatizált védelem
- Be- és kiszállítás
- Az elektronikus információs rendszer elemeinek elhelyezése
- Ellenőrzés
- Szállítási felügyelet
- Karbantartók
    - Karbantartás fokozott biztonsági intézkedésekkel
    - Időben történő javítás[164]

Amennyiben a fent felsorolt fizikai védelmi kontrollokat megvizsgáljuk és csoportosítjuk, akkor láthatjuk, hogy ezek egyrészt az ember által teremtett szándékos vagy véletlen veszélyek kiküszöbölését, másrészt a környezetből származó veszélyek minimalizálását szolgálják.
Az ember által teremtett veszélyek esetében a szándékos és a véletlen veszélyek kerültek említésre. A fizikai védelmi elemeknek ezért egyrészt szolgálniuk kell azt, hogy fizikailag illetéktelenek ne férhessenek hozzá a rendszerekhez, így az azokban kezelt, tárolt, továbbított stb. adatokat, információkat ne szerezhessék meg, azokat ne módosíthassák, töröljék stb. Másrészt meg kell valósítaniuk azt is, hogy biztosítsák az illetékességgel rendelkezők számára a fizikai hozzáférést, ám azokat kontrollált módon, így csak a szükséges helyekre engedjék a belépéseket, oly módon, hogy azok idejét, időtartamát stb. pedig rögzítsék.
A környezeti veszélyek minimalizálása érdekében elvárás, hogy észleljék és lehetőség szerint automatikus beavatkozzanak tűz, víz, villámcsapás, áramkimaradás, megemelkedő hőmérséklet és/vagy páratartalom esetén.
A fizikai védelem biztosítása érdekében az ún. hagymahéj-elvet célszerű alkalmazni, azaz különböző biztonsági besorolású zónákat kialakítani, és azokat, valamint az áthaladási pontokat a besorolásnak megfelelően védeni.[165]

---

[164] 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 szóló 41/2015. (VII. 15.) BM rendelet. https://net.jogtar.hu/jogszabaly?docid=a1500041.bm letöltve: 2023.01.22.

[165] Muha Lajos – Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése. 2018. Nemzeti Közszolgálati Egyetem. p.61.

A fent említett, és a 41/2015. (VII. 15.) BM rendeletben a fizikai védelmi intézkedések alatt megjelenő kontrollok kialakítása érdekében a hatékony gyakorlati megvalósításhoz a fizikai védelmi megoldásokat három kategóriába célszerű sorolni:

- mechanikai védelmi megoldások;
- elektronikus védelmi megoldások;
- élőerős védelem.

8.1. Mechanikai védelmi megoldások

A mechanikai védelmi megoldások több funkciót is ellátnak egyszerre az adott térben elhelyezett infokommunikációs eszközök, valamint az azokon tárolt adatok védelme kapcsán. Egyrészt védik azokat a környezeti behatások okozta ártalmaktól (eső, villám, por, egyéb szélsőséges időjárási tényezők stb.). Ilyenek lehetnek a falazatok, tető, födém, nyílászárók stb. Másrészt, megfelelő kialakítás esetén azzal, hogy hozzájárulnak a tűz terjedésének megakadályozásához, a tűz okozta ártalmak ellen nyújtanak bizonyos megoldást. Itt gondolhatunk például tűzvédelmileg falakkal elválasztott területek, a tűzgátló ajtók, túlnyomásos (füstmentes) lépcsőházak kialakítására. Harmadrészt, szintén megfelelő kialakítás esetén, segítik a káros kisugárzás elleni védelmet. Ezt segítik elő a falazatba épített rácsok, speciális ablakfóliák stb. Negyedszer pedig illetéktelenek bejutásának, így az adott térben elhelyezett infokommunikációs eszközökhöz és az azokon tárolt adatokhoz való fizikai hozzáférést akadályozzák. Ilyenek lehetnek a kerítések, vastagított falazat kialakítása, erősített, biztonsági nyílászárók, rácsozat felszerelése, de akár az előbb említett falazatban elhelyezett, kisugárzás elleni rácsozat is segítheti az ilyen védelem erősítését. Szintén a mechanikai védelmi megoldásoknál kell megemlíteni a belső értéktárolók, így akár a hordozható infokommunikációs eszközök és/vagy adathordozók, de akár a papír alapú dokumentumok tárolására is alkalmas értékmegőrzőket, lemez-, és páncélszekrényeket stb., de pl. a laptopok, monitorok stb. asztalhoz rögzítését biztosító ún. Kensington zárakat is.

Az így felépített megoldások védelmi képességéről több dolgot is szükséges megemlíteni. Először azt, hogy természetesen ezen elemek egyike sem biztosít tökéletes védelmet. A kialakítás során éppen ezért figyelembe kell venni a beépítendő elemek specifikációját (pl. tűzgátló ajtók esetében a tűz továbbterjedésének idejét, vagy behatolásvédelemet is szolgáló ajtók esetén azok áttörésgátlási idejét). Másrészt a mechanikai védelmi elemek ellenállóképessége is jelentősen növelhető, ám azok ára is ennek megfelelően növekszik. A tervezéskor éppen ezért a korábbi fejezetben már taglalt kockázatelemzést szükséges alapul venni, és annak alapján meghatározni az alkalmazandó védelmi elemeket és az azokkal szemben támasztott követelményeket.

Felsorolásszerűen megadva a legjellemzőbb mechanikai védelmi megoldások az alábbiak:

- kerítések;
- falazat (beleértve a födém elemeket is);
- nyílászárók (ajtók, ablakok);
- zárak (lakat, biztonsági zár);
- rácsok;
- speciális fóliák (törés, kisugárzás védelemmel);
- értékmegőrzők, lemez-, és páncélszekrények;
- zárható biztonsági rack, szerver ház;
- Kensington zár.

A mechanikai védelmi megoldások tervezése során a kockázatelemzés mellett is számos tényezőt figyelembe kell venni. Ilyen lehet az épület elhelyezkedése (pl. önálló épület vagy egy belvárosi, a másik házzal közös fallal rendelkező épület), az adott területre. épületre vonatkozó építészeti előírások (pl. műemlékvédelem alatt álló épület esetén külső megjelenésre vonatkozó szabályok betartása vagy meghatározott magasságú, formájú épület kialakításának előírása), az adott iparági egyéb előírások (pl. veszélyes anyagokat előállító, felhasználó üzem), a meglévő épület adta lehetősége és korlátok (pl. adott a falazat vastagsága) stb. Ezek mind befolyásolhatják a kialakítható védelmi elemeket.
A mechanikai védelmi megoldások fontos elemei a fizikai védelemnek, de önmagukban egyrészt nem elégségesek, másrészt szinte minden esetben (pl. tűzvédelem, illetéktelen hozzáférés elleni védelem, villámvédelem, káros kisugárzás elleni védelem stb.) elválaszthatatlanok az elektronikus védelmi megoldásoktól, csak azokkal együtt értelmezhetők és/vagy biztosítanak kockázat alapú megközelítés esetén hatékony védelmet.

8.2. Elektronikus védelmi megoldások

A fizikai védelmi elemek másik nagy csoportját az elektronikus védelmi megoldások alkotják. Ezen megoldások, ahogy az az előző alfejezet végén is megemlítésre került, a legtöbb esetben a mechanikus védelmi elemekkel együtt nyújt megoldást a fizikai védelmi igényekre. Ennek megfelelően ezekkel mérhetünk, jelezhetünk, riasztást generálhatunk, sőt akár automatikus be is avatkozhatunk az általunk meghatározott esetekben és/vagy küszöbértékek elérésekor. Ilyenek lehetnek bizonyos környezeti behatások (pl. víz, tűz vagy más ok miatt fellépő hőmérséklet emelkedés, villámcsapás vagy más ok miatt fellépő túlfeszültség) érzékelése, riasztások generálása, és adott esetben automatikus beavatkozás indítása (pl. oltórendszer bekapcsolása, vízszivattyú elindítása, hűtési rendszer teljesítményének növelése, vagy akár az infokommunikációs rendszer lekapcsolásának elindítása stb.). De ide tartoznak az illetéktelen behatolás érzékelését, akadályozását segítő rendszerek is. Ezek a hagyományos értelemben vett riasztó és kamerarendszerek, beléptetőrendszerek. Ez utóbbiak esetében nem csak az illetéktelenek belépésének akadályozását, hanem a jogosultsággal rendelkező kollégák mozgásának követését, bizonyos területekre történő bélépének korlátozást, de akár a munkaidejének a nyilvántartását is megoldhatjuk. Sőt, adott esetekben akár az infokommunikációs rendszerek jogosultságkezelő rendszerével is összeköthetők, aki „nem lépett be” az épületbe, az „nem léphet be” a belső hálózatba elv érvényesítésére. A káros kisugárzás elleni védelmet akár zavaró berendezések üzemeltetésével is növelhetjük, amelyek szintén az elektronikus védelmi eszközök csoportjába tartoznak.
A mechanikus védelmi megoldásokhoz hasonlóan az elektronikus védelmi megoldások egyike sem nyújt tökéletes védelmet. Ezek kiépítettségét, bonyolultságát, képességeit, beavatkozási jellemzőit szintén a kockázatokkal arányos módon szükséges tervezni és kivitelezni. Már csak azért is, mert ebben az esetben is elmondható, hogy az elektronikus védelmi elemek ellenállóképessége is jelentősen növelhető, ám azok ára is ennek megfelelően növekszik.
Felsorolásszerűen megadva a legjellemzőbb elektronikus védelmi megoldások az alábbiak:

- beléptető rendszerek (kártyás, biometrikus stb.);
- riasztórendszerek, behatolás jelző rendszerek;
- kamerarendszerek;
- tűzvédelmi jelző- és oltórendszerek;

- villámvédelemi rendszerek;
- üzemeltetést támogató elektronikai rendszerek (hőmérséklet, pára, víz, por stb. érzékelő és jelző rendszerek);
- megfelelő áramellátás biztosítása (dupla vagy tripla elektromos áram betáplálás, szünetmentes tápellátás, generátorok stb.);
- hűtés-fűtés rendszerek (infokommunikációs eszközök, hálózatok esetén kiemelten fontos a megfelelő hűtés).

Az elektronikus védelmi megoldások tervezése során is találkozhatunk a kockázatelemzés mellett is figyelembe veendő tényezőkkel. Ilyenek lehetnek például az épület tulajdonságai, annak a kábelezés kialakítására gyakorolt hatásai (pl. műemlékvédelem miatti korlátozások, vagy akár tiltás). De figyelembe kell venni az eszközök egymáshoz integrálhatóságát is, azaz meg kell oldani a jelzések egy (biztonsági) központba történő eljuttatását, feldolgozását, lehetőség szerint egységes kezelő felületen. Figyelembe kell venni a biztonsági központ méretét, az ott dolgozó személyek számát is. Így például egy rendkívül kiterjedt, és akár több száz kamerával ellátott objektum esetén a kamerákból érkező képek hatékony feldolgozására nem több száz monitort és ugyanennyi munkatársat kell alkalmazni, hanem automatizált rendszert, amely mindig az érdekes eseményeket (pl. emberi mozgás észlelése) jeleníti meg a központban dolgozó biztonsági munkatársak előtt.
Az elektronikus védelmi megoldásokról is elmondható, hogy fontos elemei a fizikai védelemnek, de önmagukban egyrészt nem elégségesek, másrészt elválaszthatatlanok a mechanikus védelmi megoldásoktól is, de főleg az élőerős védelemtől. Ez utóbbiról szól a következő alfejezet.

8.3. Élőerős védelem

A fizikai védelmi elemek harmadik nagy csoportját az élőerős védelmi megoldások alkotják. Az élőerős védelem több szinten telepíthető és így több szinten láthatja el a feladatát. A korábban leírt feladatokhoz kapcsolódóan elláthatják a portaszolgálatot, végezhetik a beléptetést, a vendégek fogadását, útba igazítását, felügyelhetik a beléptetést, ellenőrizhetik a belépők és a futárszolgálattal érkező csomagokat, a be-, és kiszállításokat végzőket és szállítmányok tartalmát, elkülönített helyen speciális vizsgálatokat (pl. levél vagy csomagbontás robbanószerkezet vagy fertőző küldemény pl. Anthrax utáni kutatásokat, kereséseket) végezhetnek, kísérési feladatokat láthatnak el (látogatók, karbantartók stb. estében). Természetesen őrzés-védelmi feladatokat is elláthatnak telephelyek, objektumok, épületrészek, eszközök, csomagok vagy akár személyek tekintetében is. Bizonyos esetekben akár távfelügyelti jelleggel is elláthatnak őrzést, jellemzően olyankor, amikor a kockázatelemzés alapján a személyes jelenlét nem indokolt, vagy a kockázat tudatosan felvállalt (pl. sok kis telephely, vagy kis értékű bentlévő eszközállomány esetén).
Az élőerős őrzés egyik központi eleme az ún. biztonsági operatív központ működése, működtetése. Jellemzen 7/24-ben, azaz folyamatosan ellátott szolgálat mellett, itt felügyelik az előző alfejezetekben említett védelmi rendszerekből (pl. beléptető rendszerek, riasztórendszerek, behatolás jelző rendszerek, kamerarendszerek, tűzvédelmi jelző- és oltórendszerek stb.) érkező jelzéseket, intézkednek az incidensek kezelésére, a károk enyhítésére. Jellemzően itt történnek meg a fizikai belépésekhez igényelt jogosultságok kiosztása, visszavonása, felülvizsgálata (pl. belépési engedélyek), az azokhoz tartozó kártyák kiadása, valamint a szükséges nyilvántartások vezetése. Jellemzően az egyéb biztonsági területhez tartozó adminisztratív tevékenység végzése is

itt folyik (pl. a szükséges nemzetbiztonsági ellenőrzések nyilvántartása, kezdeményezése, telephelybiztonsági tanúsítvány igénylése stb.)
Egyéb adminisztratív feladatok ellátása szintén itt történhet, ilynek például a minősített anyagok fogadása, kezelése, tárolása, az ezekhez szükséges feltételek (a jogszabályok szerint előírt helyiség és védelmi elemek pl. riasztó, páncélszekrény stb.) kialakítása, azok állapotának nyomon követése, a kötelező karbantartások elvégeztetése stb.
Az élőerős védelmi megoldások tervezése során a kockázatelemzés mellett a törvényi előírások adnak megkerülhetetlen szempontokat, de erősen befolyásolja, befolyásolhatja a létszámot és az ellátandó feladatokat a szervezet mérete, felépítése (pl. egy nagy méretű, tagolt szervezet esetén bizonyos, jellemzően adminisztratív feladatok más szervezeti egységnél kerülhetnek elhelyezésre), a használt felügyeleti rendszerek (pl. beléptető rendszerek, riasztórendszerek, behatolás jelző rendszerek, kamerarendszerek, tűzvédelmi jelző- és oltórendszerek stb.) száma, mérete, integráltsága és egyéb jellemzői is.
Az élőerős védelemről is elmondható, hogy fontos elemei a fizikai védelemnek, de önmagukban egyrészt nem elégségesek, másrészt elválaszthatatlanok a mechanikus és elektronikus védelmi megoldásoktól. A fentiek alapján látszik, hogy hatékony megoldást csak a három fizikai védelmi csoport, azaz a mechanikus, elektronikus és az élőerős védelmi megoldások kombinálása, azok a kockázatelemzés és az egyéb vonatkozó előírások figyelembevételével történő tervezés utáni kialakítása adja, adhatja meg.

8.4. A fizikai védelmi elemek kapcsolódása logikai védelmi elemekhez

A fizikai védelmi elemek természetesen nem különálló életet élnek, hanem az adminisztratív és a logikai elemekkel együtt, egymással szinergiában biztosítják az infokommunikációs rendszerek védelmét. A védelem kialakítása során használt kockázatelemzés végeredményeképpen előállnak azok az adatok, amelyek alapján dönteni tudunk a védelmi kérdésekben. Hogyan akarjuk kialakítani a védelmet, ahhoz milyen eszközöket, rendszereket használjunk fel, hogy hatékony és kockázatarányos legyen, sőt arról is, hogy hol vállaljuk fel a kockázatot egyéb intézkedések megtétele nélkül. Vannak olyan esetek, amikor dönthetünk arról is, hogy bizonyos védelmet logikai védelmi elem helyett adminisztratív úton (pl. tiltó rendelkezéseket tartalmazó szabályzóval) vagy éppen fizikai eszközzel valósítunk meg.
A fizikai védelmi elemek kialakításának a célja kettős. Egyrészt szerepet játszanak a fent már kifejtett a vállalat, intézmény által használt elektronikus információs rendszerek, infokommunikációs rendszerek és az azokban kezelt adatok védelmében, másrészt a vállalat, intézmény egyéb értékeinek így pl. vagyontárgyak, nem elektronikusan megjelenő (pl. papír alapú vagy szóban elhangzó) információk stb. védelmében is. A kettős cél természetesen nem jelenti azt, hogy különálló fizikai védelmi elemeket, rendszereket kell kialakítani az adott feladatokra, sőt! Ezen feladatok ellátása sok esetben a különálló szervezeti egységként megjelenő vállalatbiztonsági csapat feladata és felelősségi köre, amely ugyanazokat az elemeket használja fel mindkét cél elérése érdekében. Így például a szerverszobába vagy a vállalati pénztár helyiségbe történő behatolás észlelésére is ugyanazt a riasztórendszert használják fel, valamint ugyanazok az élőerős őrzést végző szakemberek avatkoznak be szükség esetén.
Sok esetben a fizikai védelem megvalósításához az adott intézmény, vállalat saját biztonsági operatív központot (SOC[166]) tart fenn, amelynek kizárólagos feladata a fizikai biztonsági események észlelése, kezelése. Ugyanakkor a kiberbiztonsági események észlelésére, kezelésére a szervezeteknél jellemzően egy másik, különálló egységet, az ún.

[166] SOC: Security Operation Center, magyarul biztonsági operatív központ

kiberbiztonsági operatív központot (CSOC[167]) üzemeltetnek. Amennyiben a két biztonsági központ különállóan létezik egy adott szervezeten beül, akkor ezek együttműködését, összehangolását mindenképp meg kell valósítani. Egyik oldalról a fent említett biztonsági események észlelése, kezelése okán fontos, hogy minden információ eljusson a védelemért felelős szakemberekhez, hiszen egy fizikai behatolásnak, vagy akár annak kísérletének is lehet célja az elektronikus információs rendszerekhez való fizikai hozzáférés. Az információk összefuttatása így nagy mértékben elősegíti a hatékony védelem megvalósítását. Másik oldalról pedig a kibervédelmi követelmények megvalósításakor, legyen annak célja az Ibtv.-nek, az ISO 27001-nek, vagy akár saját vállalati előírásnak való megfelelés, szintén együtt eljárva kell kialakítani az összes elvárt fizikai védelmi elemet, az auditálás során együtt kell bemutatni az erről szóló bizonyítékokat, és amennyiben valamilyen javítandó elemet tárt fel az audit, akkor szintén együtt kell azokat javítani is.

Léteznek olyan megoldások is, ahol egy adott szervezetnél a két biztonsági operatív központ egyetlen egészként jelenik meg, egy felügyelet alatt működve. Ebben az eseteben az összehangoltság adott, itt arra kell figyelni, hogy a fent említett kettős fizikai biztonsági feladatrendszer, azaz a vállalat, intézmény által használt elektronikus információs rendszerek, infokommunikációs rendszerek és az azokban kezelt adatok, másrészt a vállalat, intézmény egyéb értékeinek védelme, teljeskörűen megvalósulhasson.

[167] CSOC: Cybersecurity Operation Center, magyarul kiberbiztonsági operatív központ

Felhasznált irodalom

Muha Lajos – Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése. 2018. Nemzeti Közszolgálati Egyetem.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény

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 szóló 41/2015. (VII. 15.) BM rendelet

9. Biztonságtechnikai rendszerek védelme, biztonságos üzemeltetése

A gyengeáramú biztonságtechnikai eszközök alapvető építőkövei a komplex biztonsági rendszereknek és napjainkban az informatikai kiszolgálókra, kliensekre jellemző hálózati csatlakozásokkal, kommunikációs protokollokkal, felhasználói interfészekkel, menedzsment lehetőségekkel, valamint azokkal megegyező fizikai és logikai veszélyeztetettséggel rendelkeznek, ezért esetükben ugyanazon informatikai biztonsági, információbiztonsági képességek megléte és alkalmazása indokolt.[168] Ez a megállapítás nem csak a technikai adottságokra, hanem az üzemeltetés adminisztratív és személyi feltételeit tekintve is érvényes. A biztonságtechnikai rendszerek tervezésének, kivitelezésének és üzemeltetésének számos műszaki és adminisztratív aspektusa szakirodalmi szinten részletesen már feldolgozásra került,[169] azonban hiányként jelentkezett olyan átfogó elméleti ismeretek szintetizálása, amelyek alapvetően az egyes rendszerek és a rajtuk tárolt adatok, információk védelméhez, illetve magának a védelmi funkció zavartalan ellátásának biztosításához (rendelkezésre állás, szabotázsvédelem) szükségesek.

A többcélúság és a széleskörű hasznosíthatóság okán az információbiztonsághoz és a biztonságos üzemeltetéshez szükséges ismereteket olyan részletességgel és megközelítésben tárgyaljuk, amelyből az általános célú információs rendszerek védelmével kapcsolatos megfontolások is levezethetők, megismerhetők.

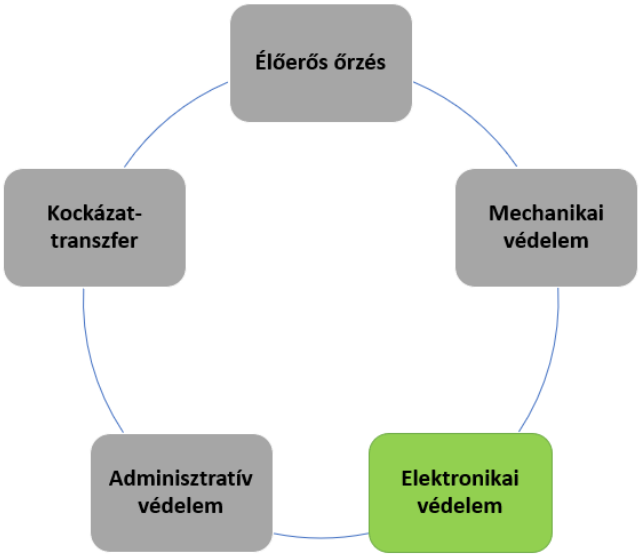
Ezen fejezet elsajátításával a hallgató alapvető, a téma feldolgozásához elengedhetetlenül szükséges ismereteket szerez a biztonságtechnikai rendszerek funkcióiról, képes lesz megérteni a rendszerek hálózati biztonságának alapvetéseit, megismeri azok információvédelmi aspektusait, továbbá a rendszerek fizikai biztonsági követelményeit és legfontosabb önvédelmi képességeit. Képes lesz meghatározni a rendszerek rendelkezésre állásával kapcsolatos és az üzemeltetés adminisztratív, valamint személyi biztonsági követelményeit. Az ismeretanyag feltételez némi előzetes tudást az informatika, kifejezetten a hálózatok területéről és a biztonságtechnikai rendszerek működéséről, mindazonáltal annak szem előtt tartásával készült, hogy olyan hallgatók is haszonnal forgathassák, akiknél ezen alapismeretek hiányoznak. Ennek okán az alapvető fogalmakat röviden megmagyarázzuk, de nem tárgyaljuk részletesen a biztonságtechnikai eszközök típusait, funkcióit, illetve működési elvüket.

[168] Dr. Tiszolczi Balázs Gergely: Fizikai biztonsági kontrollok tervezésének és alkalmazásának. gyakorlata az ISO/IEC 27001 szabvány elvárásainak tükrében. Magyar Rendészet, 2019/2-3. szám. p. 233—249

[169] Lásd például: Tóth Attila – Tóth Levente: Biztonságtechnika. Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar, Budapest, 2014. ISBN 978-615-5305-56-6

10. Röviden a biztonságtechnikai rendszerekről

Az egyének és a szervezetek biztonságának megteremtésében kiemelkedő szerepet játszanak a személy- és vagyonvédelmi eszközök és intézkedések, azaz a mechanikai és az élőerős védelem, a különböző szervezetszabályozók, valamint az elektronikai jelző és megfigyelő (biztonságtechnikai) rendszerek. A felsorolt rendszerelemek egy esetleges kárkövetkezmény enyhítését szolgáló biztosítással együtt optimális biztonságot képesek nyújtani a szervezet számára. Teljes körű, százszázalékos védelem még így sem valósítható meg, ezért számolnunk kell maradék kockázattal, mely a magánszemély vagy egy gazdasági szervezet esetén a menedzsment tudatos kockázatvállalását jelenti azzal, hogy az egyes veszélyforrásokra nem, vagy csak részben reagál védelmi megoldással. [170]



8. ábra[171] Az elektronikai védelem helye a komplex biztonság rendszerében

Napjainkban az egyes biztonságtechnikai rendszerek választékának rendkívül széles a skálája, így számos megvalósítási lehetőség áll rendelkezésre a komplex vagyonvédelem megtervezésére és kialakítására. Ezeknek a rendszereknek a feladata az illetéktelen behatolás kísérletének detektálása, a már végrehajtott cselekmény tényének jelzése, az utólagos eseményvizsgálat biztosítása, tűzjelzések megvalósítása, az egyes vészhelyzetek esetén a környezetben tartózkodók figyelmének felhívása, különböző, általában automatikus vezérlések végrehajtása.[172] Jelen tankönyv keretében biztonságtechnikai rendszerek alatt a beléptető, a video-megfigyelő (kamera vagy elektronikus megfigyelő), a behatolásjelző (riasztó) és a tűzjelző, tűzoltó rendszereket értjük, amelyek alapvető működési jellemzőiről, funkcióiról és főbb részegységeiről alábbi 3-6. táblázat nyújt áttekintést.

[170] Tóth Attila – Tóth Levente: Biztonságtechnika. Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar, Budapest, 2014. ISBN 978-615-5305-56-6

[171] A szerző saját szerkesztésű ábrája.

[172] Tóth Attila – Tóth Levente: Biztonságtechnika. Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar, Budapest, 2014. ISBN 978-615-5305-56-6

Beléptető rendszer	Főbb részegységek
• Elsősorban vagyonvédelmi rendszer. • Személyhez kötött belépési jogosultságok kiadása, visszavonása, törlése. • A mozgások teljes körű naplózása, visszaellenőrzése (terminál és user szinten, mozgás ideje alapján). • Azonosításhoz szükséges személyes adatok és jogosultságok tárolása. • Belépési jogosultságok többszintű megadása (idő és területi zónák, terminál jogosultság csoportok kezelése). • Riasztás és hibaesemények megjelenítése. • Vészhelyzeti programok indítása. • Áthaladást gátló eszközök vezérlése.	• Vezérlő terminálok • Vezetékhálózat • Hálózati csatolók • Azonosítók • Azonosítást végző eszközök (kártyaolvasók, kód tasztatúra stb.) • Áthaladást gátló eszközök • Applikációs szerverek, adatbázisok • Kezelői és menedzsment szoftverek

3. táblázat Biztonságtechnikai rendszerek funkciói és részegységeik - 1.

Elektronikus megfigyelő rendszer	Főbb részegységek
• Elsősorban vagyonvédelmi rendszer, de életvédelmi célokra is alkalmazható. • Személyek, tárgyak, folyamatok megfigyelése. • Események rögzítése, utólagos képi vizsgálata. • A legösszetettebb biztonságtechnikai rendszer, funkcionalitásában több eszköz feladatát képes ellátni. • Hiba és szabotázsjelzés. • Analitikai alapú riasztások és vezérlések elvégzése.	• Kamerák • Tápegységek • Hálózati eszközök • Vezetékhálózat • Rögzítők (stand-alone, szerver alapú) • Hálózati adattárolók • Megfigyelő állomások • Kezelői és menedzsment szoftverek

4. táblázat Biztonságtechnikai rendszerek funkciói és részegységeik - 2.

Behatolásjelző rendszer	Főbb részegységek
• Elsősorban vagyonvédelmi rendszer. • Elsődleges feladata az illetéktelen behatolás jelzése (kültéri védelem, felületvédelem, térvédelem, tárgyvédelem, jelzés lokálisan és távolra). • Egyes esetekben személyvédelem (pánikjelzés, dőlésérzékelő). • Alapvető vezérlések megvalósítása. • Hiba és szabotázsjelzés.	• Behatolásjelző központ • Tápegységek • Zónabővítő modulok • Vezetékhálózat • Hálózati csatolók • Érzékelő eszközök (PIR, nyitás-érzékelő, üvegtörés érzékelő stb.) • Hang és fényjelző eszközök • Kezelők • Kezelői és menedzsment szoftverek

5. táblázat Biztonságtechnikai rendszerek funkciói és részegységeik - 3.

Tűzjelző rendszer	Főbb részegységek
• Elsősorban életvédelmi, másodsorban vagyonvédelmi rendszer. • Tűzjelzés megvalósítása. • Vezérlések elvégzése (liftek, hő és füstelvezetés elemei, menekülési útvonalak fizikai akadályai). • Hangvezérlés, riasztás megvalósítása. • Hibajelzés.	• Tűzjelző központ • Tápegységek • Tűzjelző érzékelők • Vezetékhálózat • Vezérlő modulok • Hang és fényjelző eszközök • Kézi jelzésadók • Másodkezelők/kijelzők • Térképes felügyelet • Kezelői és menedzsment szoftverek

6. táblázat Biztonságtechnikai rendszerek funkciói és részegységeik - 4.

11. A biztonságtechnikai rendszerek információvédelmi aspektusai

Napjainkban az információbiztonság alapvető fontosságú egy vállalat működése szempontjából, így ennek megfelelően a legtöbb szervezet kialakította az információik védelméhez szükséges folyamatokat, kiépítette és üzemelteti védelmi rendszereit, az információbiztonsági, informatikai biztonsági szabályzók rendelkezésre állnak. A hatékony információvédelmi rendszer sarokköve a megfelelő fizikai védelem, azon belül is különösen sok múlik a kiválasztott, tervezett, kiépített és üzemeltetett gyengeáramú megfigyelő és jelzőrendszereken. Sok esetben azonban ezek a folyamatok és az abban részt vevő szakemberek – és így a mindennapi gyakorlat – nem foglalkoznak kellő mélységben a biztonságtechnikában alkalmazott technológia információbiztonsági aspektusaival.

Történik az annak ellenére, hogy a fizikai biztonsági rendszerben használt gyengeáramú eszközök jelentős része gyakorlatilag az informatikai kiszolgáló és kliensrendszerekre jellemző, hálózati csatlakozásokkal, kommunikációs protokollokkal, felhasználói interfészekkel, menedzsment lehetőségekkel és az azokra jellemző fizikai és logikai veszélyeztetettséggel rendelkezik.[173] Ez a megállapítás nem csak a technikai adottságokra, hanem az üzemeltetés adminisztratív és személyi feltételeit tekintve is érvényes.

A biztonságtechnikai eszközök a működési céljuk és a bennük kezelt, tárolt felhasználói, és sok esetben üzleti információk okán a telepítési környezettől is függően számos kockázatnak vannak kitéve, így a védelmük tekintetében is számos fókuszpont határozható meg. Ilyenek lehetnek többek közt a rendszereken tárolt, a hozzáférést biztosító felhasználói információk, a működés során regisztrált és rögzített személyes adatok, de ide sorolhatók a ritkábban figyelembe vett, a technológiai felügyeletet is ellátó (pl. video-megfigyelő) rendszerek által kezelt és tárolt üzleti információk. A telepített kamerák képeinek kompromittálása alkalmas lehet ipari kémkedésre (különösen, ha azok a képi tartalom mellett hangot is rögzítenek), vagy képmáshoz fűződő jogok megsértésére, a vállalat reputációjának rontására, de otthoni alkalmazások esetén súlyosan sérthetik a magánszemélyek alapvető jogait.

A tárolt adatok mellett az eszközök technológiai kialakítása is számos kockázat forrása lehet. Azon vállalati hálózatok esetében, ahol a fizikai vagy logikai struktúra nem kellően szegmentált és védett, megfelelő hálózati autentikáció hiányában vagy az eszközöket érintő szoftveres sérülékenység esetében azok belépési pontot jelenthetnek egy komolyabb támadás megvalósításához, a hálózati szegmens lehallgatásához, felderítéséhez. A hagyományos informatikai rendszerektől némileg eltérően az eszközök sikeres támadása a fizikai környezetet is veszélyezteti. A behatolásjelző és beléptető rendszerek kompromittálásával, a riasztási zónák kikapcsolásával, a vezeték nélküli kommunikáció megzavarásával, az áthaladást biztosító eszközök távoli vezérlésével, vagy akár egy illetéktelen személy számára mozgási jogosultságot biztosító azonosító létrehozásával és felhasználásával is komoly károk okozhatók egy szervezet számára. Talán még a gyakorló a szakemberek számára is kevésbé nyilvánvaló, hogy a beléptető rendszerek tűzeseti, úgynevezett fail-safe, életvédelmi üzemmódja fizikai hozzáférést

[173] Dr. Tiszolczi Balázs Gergely: Fizikai biztonsági kontrollok tervezésének és alkalmazásának gyakorlata az ISO/IEC 27001 szabvány elvárásainak tükrében. Magyar Rendészet, 2019/2-3. szám. p. 233—249.

adhat egy támadónak a védett létesítményekhez, az automatikus tűzjelző rendszer indokolatlan működtetéséből pedig sok vállalkozásnál ma már alternatív működési folyamatok indulnak, amelyek legtöbbször kevesebb vagy gyengébb fizikai védelmi, logikai kontrollt alkalmaznak, emiatt könnyebben kompromittálhatók. A biztonságtechnikai eszközök legegyszerűbben kivitelezhető támadási módja az eszközök fizikai szabotálása, rongálása, ezért fontos, hogy e tekintetben is megfelelő önvédelmi képességekkel rendelkezzenek és azokat a tervezők, telepítők minden esetben alkalmazzák.

Az eszközök veszélyeztetettsége – és így a védelmi igények, megfontolások – azok rohamos fejlődésével párhuzamosan szinte napról napra változik. A fizikai biztonsági rendszerben alkalmazott megoldásokat sem kerülheti el a digitális transzformáció, a rendszerek és hálózatok konvergenciája (mélyebb beépülésük, integrálódásuk a létesítményfelügyeleti, informatika rendszerekbe), aminek hatására az információáramlás gyorsabbá, a rendszerekkel megvalósított, automatikus, eseményvezérelt beavatkozások számossága megnő, megszűnt a biztonságtechnikai rendszerek ún. szigetrendszer jellege. A védendő technológiák felhőbe költöztetésének, a gépi tanulásnak és a fejlett arcfelismerő megoldásoknak köszönhetően amellett, hogy csökken a helyszíni fizikai biztonsági (élőerős, technológiai) igény, megjelennek a PSaaS[174] megoldások, a védelmi lehetőségek egy részének üzemeltetéséért külső fél felel, így a hagyományos biztonságszervezési ismereteken túl hangsúlyt kapnak a különböző compliance megoldások, a megfelelő szerződéses garanciák beépítésének követelményrendszere, amelyek ezidáig nem feltétlenül képezték a fizikai biztonságért felelős szakember védelmi eszköztárának szerves részét. A hálózati integráción túl napjainkra jellemző a funkciók integrálása is, így például a megfigyelő rendszerekben eszköz és szerver oldalon is alkalmazott analitika megváltoztatja az érzékelés módját, távolságát, egyszerre biztosít többek közt behatolás-érzékelést, tárgyvédelmet, kiváltva jónéhány klasszikus eszköz funkcióit, így egyetlen eszköz sikeres támadása sokkal súlyosabb hatásokkal járhat.[175]

Az utóbbi évek tapasztalatai alapján nyilvánvalóvá vált, hogy a fejlesztések egy része nemcsak biztonságunk növelésére szolgál, hanem ezekkel vagy ezeken keresztül újabb és újabb támadási vektoroknak, felületnek lehetünk kitéve.[176] A rendszereket érintő jellemző fenyegetettségeket és a kapcsolódó védelmi igényeket az alábbi, 7. számú táblázat foglalja össze.

[174] Physical Security as a Service, fizikai biztonság, mint (felhő alapú) szolgáltatás.

[175] Dr. Tiszolczi Balázs Gergely: Fizikai biztonsági kontrollok tervezésének és alkalmazásának gyakorlata az ISO/IEC 27001 szabvány elvárásainak tükrében. Magyar Rendészet, 2019/2-3. szám. p. 233—249.

[176] Tóth Levente: A komplex objektumvédelem kihívásai napjainkban, Bolyai Szemle, XXVII. évfolyam, 1. szám, p. 35-44. ISSN: 1416-1443

A RENDSZEREKET ÉRINTŐ JELLEMZŐ FENYEGETÉSEK	A RENDSZEREK VÉDELMI IGÉNYE
Rendszerszabotázs, a védelmi képesség megszüntetése, rongálás.	Fizikai biztonság, szabotázs elleni védelem.
Rendszeren tárolt adatok, felhasználói információk megszerzése.	A rendszerben kezelt személyes adatok védelme.
Ipari kémkedés a rendszerek képességeinek kihasználásával.	Jelzésátviteli utak biztonsága, a jelzések megbízhatósága.
Közveszéllyel fenyegetés a rendszerek rosszindulatú működtetésével.	Stabilitás, üzemeltethetőség biztosítása.
A rendszerek felhasználása a vállalati IT infrastruktúrát érintő támadás megvalósításához. A rendszerek felhasználása független rendszerek támadására pl. DDoS.	Információbiztonság (informatikai biztonság).
Rendelkezésre állás megszűnése.	Rendelkezésre állás biztosítása.
Compliance hiányosságok.	Jogi, szerződéses garanciák.

7. táblázat[177] **Jellemző fenyegetések és védelmi igények**

A biztonságtechnikai rendszerek működési jellemzőiről és a velük kapcsolatos, napjainkban tapasztalható fejlődési trendekről a 8. számú táblázat nyújt vázlatos összefoglalást.

[177] A szerző saját szerkesztésű táblázata.

A RENDSZEREK MŰKÖDÉSI JELLEMZŐI	TRENDEK
Kritikus védelmi feladatokat látnak el, a vállalat fizikai biztonságának építőkövei.	Digitális transzformáció, a rendszerek és hálózatok konvergenciája.
Magasan integrált, bonyolult szoftveres és hardveres kialakítás.	A rendszerekkel megvalósított, automatikus, eseményvezérelt beavatkozások számossága nő.
Üzemeltetésük, karbantartásuk magas szakértelmet igényel.	Megszűnt a rendszerek „sziget” jellege. A zártság ma már nem alapkövetelmény, kvázi hátrány.
Működésüket, telepítésüket, kezelésüket jogszabályok szabályozzák.	PSaaS megoldások Physical Security as a Service, fizikai biztonság, mint (felhő alapú) szolgáltatás.
Sokszor nagy mennyiségű személyes adatokat kezelnek.	A védelmi képességek integrációja, különösen video-megfigyelő rendszereknél.
Az informatikai kiszolgáló és kliensrendszerekre jellemző, hálózati csatlakozásokkal, kommunikációs protokollokkal, felhasználói interfészekkel, menedzsment lehetőségekkel és az azokra jellemző veszélyeztetettséggel (is) rendelkeznek.	Jelentőséget kapnak a különböző compliance és informatikai ismeretek, a megfelelő szerződéses garanciák az üzemeltetés során.

8. táblázat[178] A rendszerek működési jellemzői, trendek

[178] A szerző saját szerkesztésű táblázata.

12. A tudásolló kinyílik

Az egyes szakirodalmak a biztonsági kihívások között mindig előkelő, általában az első helyen említik az emberi tényezőt. A legtöbb technikai rendszerre igaz az állítás – és nincs ez másképpen a biztonságtechnikai rendszerek esetében sem – hogy a felhasználók magatartása és a biztonságra vonatkozó ismeretek hiánya még a kellő módon biztonságtudatosan létrehozott rendszerek esetében is jelentős kockázati tényezőt rejt magában. A biztonságtechnikai eszközök felépítésükben, működésükben és funkcióikban ma már olyan összetettséget valósítanak meg, amelyet nem csak az átlagos felhasználók, de még a rendszerek tervezésében, telepítésében jártas szakemberek sem mindig látnak át teljeskörűen. Különösen ez utóbbi csoport tekintetében kockázatos, ha nem rendelkeznek elégséges ismeretekkel az eszközökre vonatkozóan. Még több veszélyt rejt magában, ha nem csupán az eszközeik (biztonsági) alapfunkcióit nem ismerik, de az általuk telepített applikációk, alkalmazások lehetőségeivel, illetve beállításaival is csak igen korlátozott mértékben vannak tisztában.[179]

A biztonságtechnikai tervezői, telepítői jogosultságokat a mai magyar szabályozás hatósági engedélyhez köti. A tervezőnek rendelkeznie kell a 2005. évi CXXXIII. a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló törvényben (röviden: Szvmt.) meghatározott biztonságtechnikai (elektronikai) vagyonvédelmi rendszertervezésre jogosító végzettséggel és a rendőrség által kiállított érvényes igazolvánnyal, a szerelést, telepítést végző kollégáknak az Szvmt. igazolványt, és biztonságtechnikai rendszerek szerelésére jogosító szakképesítést ír elő. A törvény végrehajtására kiadott 22/2006. (IV. 25.) BM rendelet konkrétan és viszonylag széles körben meghatározza az e tekintetben elfogadható szakképesítések körét. A felhasználó közreműködésének módját és mértékét nem degradálva, nem kerülhetjük meg a tervező, telepítő elsődleges felelősséget abban, hogy a rendszerek nagyfokú biztonsággal üzemeljenek. Az információvédelmi, hálózatbiztonsági fókuszú paradigmaváltás, a szükséges szakmai kompetenciák még nem jelentek meg a képzések tematikájában, így ma még számos hagyományos biztonságtechnikai mérnöki, vagyonvédelmi rendszerszerelői képzésben végzett szakember dolgozik a területen, akik közül viszonylag kevés számú az, aki felismeri ezen ismeretek alkalmazásának szükségességét, de ők is legtöbbször iskolarendszeren kívül, önszorgalomból, vagy tudatos megrendelői nyomásra kezdenek el foglalkozni a rendszerek védelmi képességeinek és beállításainak jobb megismerésével. A legjobb technikus és mérnök sem biztos, bármennyire is jó saját szakterületén, hogy tisztában van a szükséges informatikai működési sajátosságokkal, pedig ma már alapvető elvárás lenne velük szemben, hogy járatosak legyenek legalább a szerver oldali operációs rendszerek kezelésben, az applikációs és hálózati szintű védelemi megoldások implementálásában, azok ellenőrzésében, dokumentálásában, tisztában legyenek az egyes kommunikációs protokollok alkalmazási lehetőségeivel és korlátaival, az üzleti informatikai hálózatokra történő csatlakoztathatóság alapvető feltételeivel, az egyes aktív hálózati eszközök működési módjával és biztonsági sajátosságaival. A tudatos biztonságtechnikai vállalkozásoknak nagy hangsúlyt szükséges fektetni a kollégái képzésére, ahol az egyes gyártóspecifikus megoldások a biztonsági szempontokra is kiterjednek, hogy a nem megfelelő tervezés vagy a telepítéskor elkövetett hibás beállítások és a védelmi szempontok figyelmen kívül hagyása ne rontsa az eszközök, így a megrendelő (vállalkozás vagy magánszemély) biztonságát.

[179] Bányász Péter–dr. Bodó Attila Pál–Kapitány Sándor–Orbók Ákos–dr. Zámbó Nóra: Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára. Nemzeti Közszolgálati Egyetem, 2016., p. 133

Manapság az otthoni felhasználásra szánt, mindenki számra elérhető kisebb, akár telepítői ismeretek nélkül is alkalmazható, főleg vezeték nélküli eszközök elterjedtsége miatt a műszaki vénával rendelkező felhasználók is belevághatnak otthonaik védelmi rendszereinek megvalósításába. Körükben különösen nagy a hajlandóság, hogy berendezéseiket úgy építsék ki, hogy azok a helyi hálózaton kívülről, applikációkkal vezérelhetőek legyenek, képesek legyenek videóképeket fogadni az otthonukból, vagy távolról beszélni a látogatókkal. Igen kényelmes és hatékony védelmi eszköz lehet ez, de csak olyanok kezében, akik megértik és képesek alkalmazni a rendszerek biztonsági funkcióit, különben nem csak vállalkozásaik, de otthonuk és magánéletük is könnyen ismeretlenek áldozatává válhat.

13. Security by design, avagy a tudatos biztonságra tervezés

Minden rendszerépítésre igaz, hogy a biztonság megteremtése a tervezésnél kezdődik. Amikor tervezésről beszélünk, a biztonságtechnikai rendszerek funkcionális tervezési követelményeivel, a védelmi feladat ellátáshoz szükséges eszközök meghatározásával, azok paraméterezésével, szerelési előírásaival ezen könyv keretén belül annak jellege és célja miatt nem foglalkozunk, a tervezés témáját kizárólag a rendszerek bevezető fejezetben bemutatott védelmi igényeinek tekintetében tárgyaljuk. Erre azért van szükség, hogy a szakemberek megfeleljenek egy rendkívül komplex, többszereplős kiválasztási és tervezési eljárás követelményeinek, generálisan képesek legyenek az összes szakmai szempont – beleértve az adatvédelmi, információbiztonsági szempontokat is – integrálására, és a lehető legjobb, az összes érintett fél számára megfelelő megoldás kiválasztására.

13.1. Gyártói követelmények

Egy tervezési folyamatban, amennyiben az összes felhasználói igényt specifikáltuk és a szükséges funkcionalitást meghatároztuk, kiválasztásra kerülnek azok a gyártók, amelyek potenciálisan szóba kerülhetnek az érintett műszaki megoldás megvalósításakor. Az eszközök biztonsága tekintetében igen sok múlik azon, hogy különböző gyártók hogyan kezelik az információbiztonságot fejlesztési, gyártási, beszerzési folyamataikban. Előfordul ugyanis, hogy funkcionalitásban kiváló termékeket fejlesztenek, azonban biztonsági szintben jelentősen elmaradnak a napjainkban elvárhatótól. A rendszerek tervezéséért felelős szakember feladata, hogy a funkcionális és teljesítményjellemzőkön, műszaki paramétereken túl tervezze és megfelelően specifikálja a műszaki kiírásban azokat a biztonsággal kapcsolatos igényeket, amelyeket a megoldás kiválasztásánál a gyártónak és a terméknek biztosítania kell ahhoz, hogy lefedje a vállalati szabályzatokban és a vonatkozó jogszabályokban foglalt információbiztonsági és adatvédelmi követelményeket, rendelkezésre állási igényeket. A kiválasztási folyamat során ezért indokolt specifikálni és keresni olyan bizonyítékokat, iparági minősítéseket, külső feles auditokat stb., amivel a gyártó igazolja, hogy a fejlesztés, gyártás és forgalmazás során figyelembe vették a rendelkezésre állásra, adatvédelemre és információbiztonságra vonatkozó szempontokat.

A gyártók több esetben rövid tájékoztatókban (ún. white paper) vagy a műszaki leírások keretében megadják, milyen módszertanok alapján végzik a termékek fejlesztését, milyen garanciákat építettek be és érvényesítettek a tervezés, termékfejlesztés, gyártás és tesztelés során. A kritikusabb alkalmazások során szempont lehet, hogy a termék, a fejlesztési folyamat feleljen meg a Common Criteria (CC) valamelyik szabványban rögzített szintjének. A CC egy termékfejlesztési keretrendszer, amely nemzetközileg elfogadott, egységes értékelési alapelvek szerint, különböző szinteken képes garantálni egy informatikai termék információbiztonsági követelményeket megvalósító funkcióit (bizalmasság, sértetlenség, rendelkezésre állás).[180] Sajnálatos módon a tanúsított termékek közt nem találunk nagyszámú biztonságtechnikai alkalmazást, azonban ezen eszközök tekintetében a megfelelőség tanúsítása nem példanélküli.[181] A CC egy termékfejlesztési szabvány, így alkalmazása nem képes minden, a termékkel kapcsolatos

[180] A minősített termékek listája elérhető: https://www.commoncriteriaportal.org/products/

[181] Hikvision Achieves Common Criteria Certification https://www.prnewswire.com/il/news-releases/hikvision-achieves-common-criteria-certification-696212031.html (letöltés ideje: 2022.09.27.).

kockázatot kiküszöbölni, olyanokra nem nyújt megoldást, mint a tervezési, gyártási helyszín fizikai és humánerőforrás biztonsága. E tekintetben érdemes olyan gyártói minősítéseket keresni, amelyek kielégítik ezeket az igényeket is. A leggyakrabban alkalmazott és keresett megoldás az ISO 27001 szabvány, amely lefedi egy információbiztonsági irányítási rendszer (IBIR) követelményeit. A CC kizárólagos alkalmazása továbbá a tekintetben is korlátos, hogy sok esetben nem definiál konkrét védelmi megoldásokat, pl. az alkalmazott titkosítási eljárások tekintetében sem. Ha garanciát keresünk rá, hogy a termékünkben alkalmazott titkosítási eljárások biztonságosak, és kielégítik a vonatkozó követelményeket, akkor az ún. FIPS megfelelést érdemes keresni. A FIPS egy mozaikszó, ami az amerikai Federal Information Processing Standards (kb. szövetségi információfeldolgozási szabványok) rövidítése. A FIPS 140-2 szerinti megfelelés esetén a megoldás kizárólag a FIPS szabvány szerinti algoritmusokat és módszereket használ, amelynek hatására az alkalmazott titkosítási eljárás kellő mértékben ellenálló lesz a feltételezett támadásokkal szemben.

A tervezési és a gyártási folyamat biztonsága tekintetében a garanciáknak túl kell mutatnia az érintett vállalkozás saját hatáskörben végrehajtott folyamatain, a teljes körű megbízhatósághoz hozzátartozik a beszállító lánc és a harmadik féltől származó, sok esetben GNU licence alá tartozó szoftverkódok biztonsági szempontú értékelése. A beszállítói láncok menedzselésével kapcsolatos irányítási rendszerszabvány az ISO 28000, amely tanúsítás megléte egyfajta biztosítéka lehet annak, hogy a gyártó megfelelően kezeli a biztonsági kérdéseket (is) a beszállítói relációkban. A szabvány alkalmazása (és alapvetően a beszállítói lánc ellenőrzése) azért is indokolt, mert az ellátási láncok integrált információs rendszereinek optimális működése nemcsak információtechnológiai kérdés. A hálózatba szervezett vállalatok számára létfontosságú, hogy ki, mikor és hogyan férhet hozzá a számára szükséges információkhoz, ill. mikor indíthat el vagy nyúlhat bele egy vállalaton belüli vagy vállalatok közötti tranzakcióba. A kockázatok kezelése nem szétválasztható az anyagi- és információs folyamatokban, valamint az információtechnológiában.[182] Több esetben bebizonyosodott, hogy egyes (legtöbbször kínai), telefongyártók már a gyártósoron, vagy később a forgalmazók olyan kémprogramokat telepítenek az eszközre, amelyeknél nem lehet tudni, kihez kerülnek a rólunk gyűjtött adatok. 2015-ben a Lenovo laptopok esetében fedezték fel, hogy a gyártó olyan hirdetéskezelő rendszert és gyökérszintű tanúsítványt telepített a számítógépeire, amely támadások lebonyolítására is alkalmas lehet.[183] Említhető e tekintetben speciálisan olyan, a legnagyobbak közé tartozó kamerarendszer gyártó, amelynek eszközeiben 2021-ben egy igen komoly sebezhetőséget fedeztek fel a kiberbiztonsági kutatók. Gyakorlatilag egyetlen, megfelelően formázott üzenettel kompromittálható a kamera, segítségével egy olyan root shellhez (parancsértelmező felület) lehet hozzáférni, amely magasabb jogosultsági szintet biztosít, mint a rendeltetésszerűen a tulajdonos által használható, limitált parancssori hozzáférés. Ha a kamera beépített webkiszolgálója elérhető az internet felől, akkor viszonylag könnyen adminisztrátori hozzáférést lehet szerezni az eszközhöz, aminek segítségével a hálózat többi eszköze is támadhatóvá válik, tehát nem

[182] Dr. Michelberger Pál - Lábodi Csaba: Vállalati információbiztonság szervezése. https://kgk.uni-obuda.hu/sites/default/files/10_Michelberger_Labodi.pdf, p. 266. letöltés ideje: 2022.10.02.

[183] Bányász Péter–dr. Bodó Attila Pál–Kapitány Sándor–Orbók Ákos–dr. Zámbó Nóra: Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára. Nemzeti Közszolgálati Egyetem, 2016., p. 107

csak a kamera, hanem az érintett hálózati szegmensbe telepített eszközök is veszélybe kerülhetnek.[184]
Hasonló sebezhetőségek természetesen bármelyik gyártó termékében előfordulhatnak, azokat kizárni teljesen nem lehet, de előfordulási valószínűségüket csökkenteni igen. A Bosch saját maga által közölt információi szerint az IP alapú elektronikus megfigyelő rendszerein mintegy 30.000 behatolástesztet és sebezhetőségi vizsgálatot végzett.[185] A gyártók egy másik csoportja kevesebb hangsúlyt fektet a hasonló ellenőrzési folyamatokra, vélhetően kevésbé tartják fontosnak ezen garanciákat, amely marketing szempontból (sem) szerencsés.
Lényeges különbségek az egyes gyártók közt a fejlesztési és gyártási folyamat biztonsága mellett még abban lehetnek, milyen megbízható és hosszútávú támogatást nyújtanak mind a hardver mind a szoftvertermékeik tekintetében, amelynek keretében a funkcionális fejlesztések mellett azt is biztosítják, hogy az időközben feltárt sérülékenységek javítása elfogadható határidővel megtörténik. A már feltárt sebezhetőségek tekintetében fontos, a gyártó mennyire transzparensen kezeli azokat, milyen gyorsan reagál a különböző javításokkal az eszközök esetében, illetve mennyire segíti elő a még feltáratlan sebezhetőségek tudomásra jutását pl. bug bounty[186] programok indításával, illetve a sebezhetőségek bejelentését elősegítő, titkosított csatornák üzemeltetésével.
Amikor a megfelelőséget tárgyaljuk, e tekintetben nem mehetünk el napjaink egyik legnagyobb hatású jogszabálya, a GDPR mellett sem. A GDPR mozaikszó, a General Data Protection Regulation (nemzetközi adatvédelmi rendelet) rövidítése. Az általános adatvédelmi rendelet egy Európai Uniós rendelet, amely részletes követelményeket határoz meg a vállalkozások és szervezetek részére a személyes adatok gyűjtése, tárolása és kezelése tekintetében. Ezek a szabályok az EU területén személyes adatokat kezelő európai uniós székhelyű szervezetekre, továbbá azokra az EU-n kívüli szervezetekre vonatkoznak, amelyek európai uniós lakosok személyes adatait kezelik.[187] A rendelet meghatározza azokat a jogokat, amelyeket az érintettek gyakorolhatnak személyes adataik tekintetében, illetve igen szigorú adatvédelmi követelményeket ír elő azok védelme érdekében. A biztonságtechnikai rendszerek jelentős része személyes adatkezelést valósít meg, technikai oldalról az érintetti jogok biztosításában nagy szerepük van. A GDPR hatálybalépése előtt az adatkezelés idejét és feladatait leíró, a személy- és vagyonvédelmi tevékenységek szempontjából releváns Szvmt. kényelmes volt a tekintetben, hogy konkrétan meghatározta a különböző rendszerekben kezelt személyes adatok tárolhatóságának idejét, míg ma már a legtöbb esetben adminisztratív eljárásokkal, egyedileg kell igazolni az adatkezelés szükségességét, arányosságát, az érintetti jogok biztosítása pedig komoly tervezési megfontolások elé állítja a szakembereket, különösen a felejtéshez és az adathordozhatósághoz való jog alkalmazása

---

184 https://kiber.blog.hu/2021/09/21/sokmillio_kamera_kerulhet_veszelybe_hikvision_armageddon_kozeleghet letöltés ideje: 2022.08.11.

185 Bosch IP Video and Data Security Guidebook, p.6 https://resources-boschsecuritycdn.azureedge.net/public/documents/Data_Security_Guideb_Special_enUS_900722159061 2491.pdf letöltés ideje: 2021.04.01.

186 A bug bounty programok keretében a gyártók valamilyen (általában pénz) jutalmat ajánlanak fel azoknak, akik sebezhetőségeket tárnak fel termékeikben.

187 https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_hu.htm

esetén. Az adminisztratív „korlátozások” mellett azonban a GDPR bizonyos eljárásokban, mint például az incidensmenedzsment, nagyobb mozgási teret is ad számunkra. Az Szvmt. video-megfigyelő rendszerekre korábban érvényes, generálisan három napban korlátozott (speciális esetekben ennél több is megengedett volt) adatkezelési határidejével ellentétben érdekmérlegelési teszt alapján már 30-60 nap is indokolt lehet, megnövelve ezzel a vizsgálati eljárások sikerének valószínűségét. Napjainkban azonban a személyes adatot kezelő fizikai biztonsági rendszerelemeknek is teljesíteniük kell a GDPR előírásait, és jogos üzleti igény, hogy a jogszabályból származó egyes követelményeket lehetőleg rendszeres emberi interakció nélkül, automatikus módon valósítsák meg. Különösen az elektronikus beléptető- és megfigyelő rendszerek esetében szükséges biztosítani, hogy képesek legyenek a személyes adatokat a meghatározott ideig tárolni, azokon az előre beállított paraméterek alapján végrehajtani az adattörlési műveleteket és műszakilag támogatni az érintettek megismeréshez és adathordozhatósághoz való jogát.[188]
A legfontosabb érintetti jogokat, és a kapcsolódó rendszerfunkciókat összefoglalóan az alábbi, 9. számú táblázat mutatja be.

ÉRINTETTI JOG MEGNEVEZÉSE	A JOGOK GYAKORLÁSÁT BIZTOSÍTÓ RENDSZERFUNKCIÓ
A személyes adatok törléséhez és „elfeledtetéshez” való jog.	Automatikus, emberi interakció nélküli törlési, anonimizálási lehetőség az érdekmérlegelési tesztekben megfogalmazott intervallumoknak megfelelően. Privacy masking funkció.
Személyes adatok hordozhatóságának joga.	Az adatok hordozható, az érintett által felhasználható formában történő exportja.
Személyes adatokhoz való folyamatos hozzáférés joga.	Az adatok nagy rendelkezésre állásának biztosítása (RAID megoldások, rendszeres mentések).

9. táblázat[189] Érintetti jogok és rendszerfunkciók

13.2. Technológiai kompatibilitás, megfelelőség tervezése

A fizikai biztonság kialakításánál, különösen az elektronikus rendszerek tervezésénél a meglévő és/vagy a jövőben alkalmazásra kerülő technológiával kapcsolatos integrálhatósági, kompatibilitási szempontokra kiemelt figyelmet kell fordítani, továbbá compliance oldalról is meg kell felelnünk a vonatkozó belső szabályzók és jogszabályi előírások rendelkezéseinek.

[188] Dr. Tiszolczi Balázs Gergely: Fizikai biztonsági kontrollok tervezésének és alkalmazásának gyakorlata az ISO/IEC 27001 szabvány elvárásainak tükrében. Magyar Rendészet, 2019/2-3. szám. p. 233—249.

[189] A szerző saját szerkesztésű táblázata.

Ha a szervezetnél a bekövetkezett rendkívüli események kezelésére, az incidensmenedzsment támogatására SIEM[190] rendszert alkalmaznak, szükséges annak előzetes megállapítása, van-e igény az elektronikus biztonsági eszközök SIEM (vagy bármilyen loggyűjtő) rendszerbe történő integrációjára. Az integrációs igény meghatározza többek közt, hogy milyen naplózási képességekkel, jelzési és riasztási funkciókkal szükséges a tervezett megoldásnak rendelkezni. Szintén fontos szempont az alkalmazott hálózati védelmi, és/vagy autentikációs követelményekre vonatkozó előírásoknak történő megfelelés, hogy az eszköz képes legyen a vállalati informatikai hálózatra történő szabályos csatlakozásra (802.1x), megvalósítsa az igényelt autentikációs metódust (AD integráció), és kielégítse a szervezet általi egyéb követelményeket, amelyek vonatkozhatnak többek közt jelszó komplexitásra vagy titkosítást biztosító adatátviteli protokollok használatára. A különböző információbiztonsági szempontú technológiai megszorítások, különösen a felhő alapú megoldások igénybevételének tiltása determinálja a kizárólag on-premise rendszerek alkalmazását, ebben az esetben vizsgálni kell a szervezetben alkalmazott informatikai rendszerekkel és üzemeltetési eljárásokkal való kompatibilitást, illeszthetőséget (alkalmazott operációs és adatbázis kezelő rendszerek, mentési eljárások).

Amennyiben igényként merül fel, hogy a munkavállalók okoseszközeiket (telefon, tablet stb.) az elektronikus beléptető rendszerekben történő azonosításához (vagy esetleg kameraképek távoli megfigyeléséhez stb.) használhassák, úgy a technológia kiválasztásánál figyelembe kell venni az alkalmazott készülékek operációs rendszereit, az azonosításhoz felhasználható adatkapcsolati lehetőségeit (BLE – Bluetooth Low Energy, NFC – Near Field Communications), továbbá a tervezett használat módját, lehetőségeit. Ha az elektronikus beléptető rendszerek funkcióit dokumentumkontrollra is alkalmazni kívánják – legjellemzőbben hálózati nyomtatók proximity kártyával történő integrációjában – akkor a megfelelő biztonsági szint szem előtt tartásával olyan kártyaszabványt válasszunk, amelyet az alkalmazott nyomtatógyártó technológiája támogat. Az egyedi kódolást alkalmazó rendszerek esetében elképzelhető, hogy az nem, vagy csak nagy költséggel integrálható külső gyártók rendszereivel.

Kapacitástervezés szempontjából gondoljuk végig a szervezet közép és hosszútávú növekedési terveit és lehetőségeit létszám, feladat és erőforrás tekintetében, ennek megfelelően tervezzük a rendszerek műszaki paramétereit (zónaszám, rögzítési kapacitás, átbocsátó képesség, integrálhatóság stb.).[191]

13.3. Igények felmérése, összehangolása

A „hagyományos” biztonságtechnikai tervezési eljárástól eltérően a rendszer működésében érintett felek, az úgynevezett stakeholderek számossága és igényei megnőttek. A biztonságtechnikai rendszerberuházások előkészítése olyan komplex döntés-előkészítő eljárássá nőtte ki magát, amely a műszaki-gazdasági optimum elérése okán számos szakterület szoros együttműködését, egyedi szempontjainak integrálását igényli, és ezt nem megfelelően kezelve az egész beruházás veszélybe kerülhet, vagy a hatékony és biztonságos üzemeltetés ellehetetlenülhet.

A legtöbb esetben a biztonsági vezetőn kívül a gazdasági döntéshozót, a biztonságtechnikai tervezőt, az adatvédelmi tisztviselőt (DPO, Data Protection Officer),

[190] SIEM: Security Information and Event Management, biztonsági incidensmenedzsmentet támogató eseménykezelő/jelző rendszer.

[191] Dr. Tiszolczi Balázs Gergely: Fizikai biztonsági kontrollok tervezésének és alkalmazásának gyakorlata az ISO/IEC 27001 szabvány elvárásainak tükrében. Magyar Rendészet, 2019/2-3. szám. p. 233—249.

az informatikai rendszerüzemeltetésért felelős területet, továbbá az információbiztonsági felelőst (CISO, Chief Information Security Officer) szükséges bevonni, és segítségükkel felmérni mindazon követelményeket és elvárásokat, amelyek a beszerzés tárgyával szemben, annak egész élettartama során felmerülnek. Ennek keretében igényként fogalmazódhat meg többek közt, hogy az adott termék képes legyen egyes, a szakterületek szempontjából speciális műveletek elvégzésére, biztonságosan kezelje az adatokat, végezzen vezérlési feladatokat, biztosítsa az érintettek személyes adatokhoz való jogait, legyen képes a szervezetben alkalmazott hálózati autentikációs metódusok implementálásra. A megfelelő kommunikációval, együttműködéssel csökkenhet egy beruházási projekt kockázata úgy, hogy az igényeket maradéktalanul kielégítik a javasolt alternatívák, és nem tartalmaznak felesleges (műszaki) megoldásokat, adott esetben ezzel járó költségeket.[192]
A 9. számú ábra összefoglalóan szemlélteti az érdekelt feleket és főbb megfontolásaikat.

9. ábra[193] Érdekelt felek megfontolásai a tervezési folyamat során

[192] Tiszolczi Balázs Gergely: A vállalati biztonságtechnika gazdaságtani megközelítése. Szakdolgozat. Budapesti Gazdasági Főiskola, Pénzügyi és Számviteli Kar, 2015

[193] A szerző saját szerkesztésű ábrája.

14. Hálózati követelmények

Az (infó)kommunikációs hálózatok fejlődése az elmúlt években soha nem látott méreteket öltött. Alapvető elvárás, hogy a szükséges információ bármikor, bárhonnan, pár kattintással elérhető legyen. Korábban a biztonságtechnikai rendszerelemek meghatározó jellemzője volt a zártság, a dedikált és kizárólagos adatátviteli utak, az ún. szigetüzemű működés. Jó példa erre a hagyományos CCTV hálózat, amely – ahogy a neve is mutatja – zárt láncú rendszert alkotott (Closed Circuit TeleVision, zárt láncú televízióhálózat). A biztonságtechnikai rendszerek e zártságnak köszönhetően saját szabályaik szerint működhettek, nem, vagy csak igen minimális mértékben volt szükség alkalmazkodni más rendszerek, alkalmazások igényeihez. A technológiai fejlődés lehetővé, és egyszersmind szükségessé tette, hogy az egyes eszközeink különálló hálózatait egyetlen integrált, ún. konvergált hálózatba szervezzük. Ezen konvergált hálózatok jellemzője, hogy segítségükkel képesek vagyunk osztott, közösen használt átviteli csatornán egyszerre továbbítani bármilyen elektronikus adatot (kép, hang, szöveg stb.). A fejlődés egy másik fő iránya a különböző lokális, helyi hálózatok egyetlen, összefüggő rendszerré történő összekapcsolása (Internet), amely lehetővé teszi egyben azt is, hogy a felhasználók azonnal, bármikor közvetlen kapcsolatba kerülhessenek a konvergált hálózataikra kapcsolódó rendszereikkel, elérhetik a rajtuk tárolt információkat, kihasználhatják funkcióikat. Az alkalmazásaik számos módon és számos eszközzel menedzselhetők, sok esetben a világ bármely pontjáról, számítógépek, táblagépek, okostelefonok segítségével.

A vállalati, konvergált hálózatra történő csatlakozás és az összekapcsolt hálózatokkal együtt járó távoli hozzáférés lehetősége ma már alapkövetelmény a biztonságtechnikai rendszerek tekintetében is az egyszerű menedzselhetőség, az online felügyelet, a kényelmes kezelés továbbá a rugalmas rendszerarchitektúra, a skálázhatóság okán, azonban ezen számos előny mellett jónéhány hátránnyal is szükséges szembenéznünk. A különböző típusú és funkciójú rendszerek együttélése elkerülhetetlenné teszi bizonyos közös szabályok bevezetését, illetve az egymás működési sajátosságaiból származó kockázatok kezelését. Először is az adatok küldéséhez az egyik lokális hálózaton (LAN, Local Area Network) lévő eszközről egy másik LAN-on lévő eszközre (gyakorta interneten keresztül), szabványos kommunikációs metódusokra van szükség, amelyet ma már a biztonságtechnikai eszközöknek is ismerniük kell. Alapvetően az utóbbi időben telepített rendszerek jelentős része az ügyviteli hálózatra csatlakozó informatikai kliens és szervereszközökhöz hasonlóan a TCP/IP protokollcsalád szabályai szerint kommunikál (és azokhoz hasonló veszélyeztetettséggel is rendelkezik), ezért jelen fejezetben ezen ismeretekre fókuszálunk. A működési elvárások a hatékony kommunikációs protokoll mellett igényelnek hibatűrést, szolgáltatási minőséget és nem utolsó sorban nagyfokú biztonságot is.

A biztonságtechnikai rendszerek a hálózati biztonsággal összefüggésben több okból is érdekesek. Egyrészt, a rendszereknek kezelni szükséges a kommunikációs platform nyitottságával és konvergált mivoltával kapcsolatos kockázatokat, amely működési sajátosságok könnyedén elérhetővé, felderíthetővé, hozzáférhetővé teszik azokat, illetve az osztott kommunikációs közeg sok esetben ronthatja többek közt a jelzésbiztonságot is. Másik oldalról, maguk a biztonságtechnikai rendszerek jelentenek a hálózat számos más eszközére, az eszközökön kezelt, tárolt információkra nézve kockázatot. Ez a kockázat abból adódik, hogy a végpontok egy jelentős része funkciójukból adódóan a hálózatok perifériáján található (kamerák, behatolásjelző rendszerek érzékelői stb.), így megfelelő védelem hiányában viszonylag könnyen hozzáférhetők (és rajtuk keresztül a hálózat többi

eleme is) illetve egyes eszközök adatforgalma – alkalmas szabályok nélkül – működésfolytonossági problémákat idézhet elő.

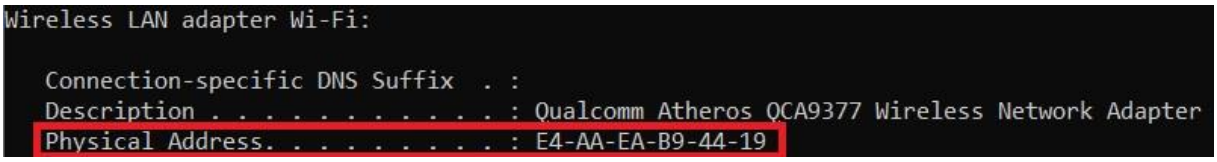
14.1. A hálózatról általában

Ahogy arról a bevezetőben szó volt, az adatok küldése az egyik lokális hálózaton lévő eszközről egy másik LAN-on lévő eszközre szabványos kommunikációs metódusokat igényel, amelyet a bevezetőben tárgyalt okokból ma már a biztonságtechnikai eszközöknek is ismerniük kell. Alapvetően az utóbbi időben telepített rendszerek jelentős része az ügyviteli hálózatra csatlakozó informatikai kliens és szervereszközökhöz hasonlóan a TCP/IP protokollcsalád szabályai szerint kommunikál, IP-cím alapú címzést használnak a saját hálózaton kívüli kommunikációhoz (azonos helyi hálózati szegmensen a fizikai ún. MAC-címek használata elegendő a kommunikációhoz, lásd később.)
Az IP-címzés (Internet Protocol), nélkülözhetetlen az egyes hálózatokon lévő eszközök számára egymás helyének azonosításához és a köztük végbemenő kommunikáció biztosításához. Ezért minden hálózati eszköznek rendelkeznie kell vezetékes vagy vezetéknélküli hálózati csatolóval és IP-címmel, amelyet vagy statikusan, kézzel állítanak be, vagy ún. DHCP (lásd később) protokollon keresztül igényelnek az IP címek kiosztására rendszeresített kiszolgálótól. Az IP címek (pontosabban azok IPv4-es verziója, a másik, ún. IPv6 verziójával jelen tankönyvben nem foglalkozunk) 128 bites bináris (kettes számrendszerbeli) azonosítók, azonban a könnyebb olvashatóság okán decimális formában adják meg, és ponttal elválasztva négy darab 0-255 közötti számmal jelenítik meg. Az IPv4-címek az interneten kommunikáló eszközök esetében mindig egyedi, publikus logikai azonosítók. A nyilvános, szervezethez vagy személyhez rendelt IP-címet egy internetszolgáltató osztja ki, amelyet lehet dinamikusan változó vagy statikus formában is igényelni.
Más a helyzet a kizárólag egy adott lokális hálózaton belül alkalmazott ún. privát IP címekkel, amelyek a különböző belső hálózatokban újra felhasználhatók, azonban az interneten ezek a címek nem jelenhetnek meg, a forgalomirányítók (routerek) azokat nem továbbíthatják. Az IP címek működésüket tekintve logikai címek (ellentétben az ún. MAC címekkel, amelyeket eszközökhöz dedikálnak) így a berendezés típusáról nem, kizárólag a helyéről szolgáltatnak információt. Minden IP-címhez tartozik egy ún. alhálózati maszk (speciális formátumú IP cím), amely meghatározza, hogy az eszköz egy nagyobb hálózat melyik rész (al)hálózatához tartozik. Összefoglalva a hálózatra kapcsolt, hálózati kártyával rendelkező eszközök (ún. node-ok) helyét minden esetben az IP cím és a hozzá tartozó alhálózati maszk azonosítja.
A MAC cím a node OSI modell[194] szerinti adatkapcsolati réteg azonosítója, ún. fizikai címe. A MAC-cím egy 48 bites, hexadecimális formában megadott számsorozat, amelyet a gyártó „éget bele" a hálózati kártyákba. A MAC cím első hat hexadecimális számjegye a gyártót azonosítja, a második fele egyedi számsorozat. Azonos alhálózatban lévő eszközök között a MAC cím az elsődleges kommunikációs azonosító.
Az egyes eszközökön megtalálhatók vagy belőlük kiolvashatók az IP és a MAC címek, valamint a hálózati maszkok, a Windows operációs rendszert használó eszközökből a

[194] Az OSI (Open Systems Interconnection Model) egy olyan elvi, szabványosított modell, amely hálózatban kommunikáló felek egymáshoz való kapcsolati viszonyait definiálja. Az egyes rétegek különböző feladatot valósítanak meg a kommunikációs folyamatban, vertikálisan egymásra épülnek, egymásnak szolgáltatásokat nyújtanak a többi réteg belső működésének ismerete nélkül, lehetővé téve ezáltal különböző szabványok szerint implementált kommunikációs protokollok problémamentes együttműködését. A modell 7 egymásra épülő réteget határoz meg.

parancssor megnyitása után (keresőbe cmd betűsort begépelve) *ipconfig/all* paranccsal ellenőrizhetjük.

10. ábra[195] **IP cím és alhálózati maszk**



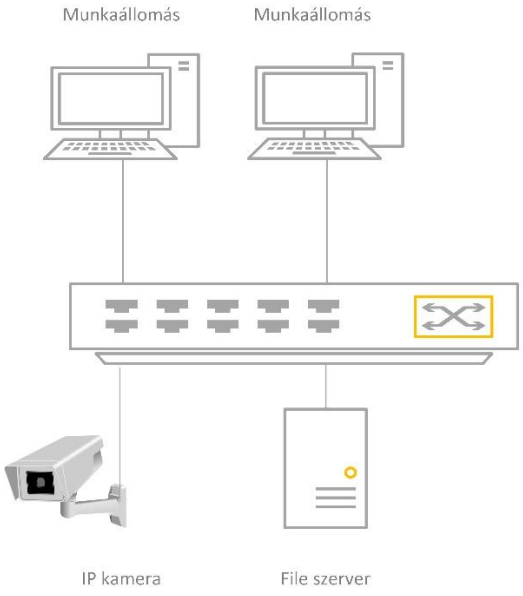
11. ábra[196] **MAC cím**

Ahogy említettük, a MAC cím beégetett cím, amellyel a gyártó látja el az eszközöket. Ezzel ellentétben az IP cím egy logikai azonosító, amely az eszköz telepítési helyétől függően változik, és megadható manuálisan a telepítő által, vagy automatikusan, felhasználói beavatkozás nélkül, DHCP (Dynamic Host Configuration Protocol) használatával. A DHCP-t egy szerverszolgáltatás biztosítja, amely általában minden helyi hálózatban megtalálható. Igen nagy előnye (később tárgyalandó biztonsági hátránya mellett), hogy a telepítőnek nem szükséges megadnia manuálisan minden hálózatra való csatlakozás alkalmával az IP-címet, az alhálózati maszkot, az alapértelmezett átjárót, azokat az eszköz hálózati kártyája igényli az erre dedikált kiszolgálótól.
Az eddig tárgyalt kommunikációs azonosítók arra voltak alkalmasak, hogy egy adott eszközt (kamera, NVR, beléptető vezérlő, PC, nyomtató stb.) azonosítsanak, elérése érdekében meghatározzák annak helyét a hálózaton, segítsék a forgalom irányítását az erre dedikált berendezéseknek. A gyakorlatban azonban sok esetben nem csak egy adott node helyét szükséges ismernünk, hanem az azon futó alkalmazásokat is pontosan tudnunk kell azonosítani. Ennek oka, hogy egy eszközön, akár kliens, akár kiszolgáló funkciót tölt be, számos szolgáltatás futhat, számos alkalmazás igényelhet és fogadhat hálózati kommunikációt (egy szerveren egy időben futhat e-mail, file és adott esetben videomenedzsment szerver is) ezért lényeges megismerkedni a portok, illetve a portszám fogalmával.
A port (annak száma) egy adott szolgáltatást vagy alkalmazást határoz meg úgy, hogy a fogadó szerver tudni fogja, hogy a rajta futó melyik szolgáltatásnak kell feldolgoznia a hozzá beérkező adatokat, illetve a kliens küldéskor meg tudja címezni azt a konkrét alkalmazást, amitől ő szolgáltatást (pl. video streamet) szeretne igényelni. A portszámok 0 és 65535 között változhatnak. Egyes alkalmazások olyan portszámokat használnak, amelyek szabványban rögzített, ún. well-known vagy jól ismert portok, és amelyet az erre létrehozott nemzetközi szervezet, az internetes azonosítókat kiosztó és nyilvántartó Internet Assigned Numbers Authority (IANA) hozzájuk rendelt. Például egy webkiszolgálót a böngészők mindig a 80-as (vagy titkosított, TLS kapcsolat esetén a 443-as porton) érnek el. A portszámot nem szükséges külön megadni, a böngészők azokat

[195] A szerző saját szerkesztésű ábrája.

[196] A szerző saját szerkesztésű ábrája.

automatikusan használják. Amennyiben a webszerver adminisztrátor a weboldalak kiszolgáláshoz másik portot állítana be, akkor a browser kliensek képtelenek lennének az erőforrások elérésére automatikus módon.
Látható tehát, hogy a teljes értékű hálózati kommunikációhoz elengedhetetlen a portszám ismerete, ugyanis az IP cím és az alhálózati maszk nem elég ahhoz, hogy azonos hálózati címen futó szolgáltatásokat megfelelően megcímezzünk, ehhez az adott szolgáltatás tényleges kommunikációs azonosítja, portszáma szükséges. A TCP/IP protokollcsalád alkalmas arra, hogy a portszámokat automatikusan igényelje és alkalmazza, annak használatához nem szükséges a legtöbb esetben a felhasználó közreműködése. Fontos megjegyezni, hogy a portnak létezik egy, az informatikában elterjedt másik értelmezése is, mely szerint az egy hozzáférési pontot határoz meg, amely fizikai csatlakozási lehetőséget biztosít egy adott eszközhöz (pl. switchek Ethernet portjai, számítógépeken lévő USB portok).
A kommunikációs címzési eljárásokon kívül mind telepítési, üzemeltetési, mind biztonsági szempontból alapvetően fontos a biztonságtechnikai szakembereknek azon eszközök ismerete, amelyek a két node közti hálózati adatátvitelt, forgalomirányítást biztosítják, illetve egyes esetben forgalomszűrő, forgalomkorlátozó, esetleg priorizáló funkciót valósítanak meg. Ezek közül jelen tankönyv keretein belül a hálózati kapcsolókat (switch), az útválasztókat (router), és a tűzfalakat tárgyaljuk röviden.
A switcheknek, vagy más néven hálózati kapcsolóknak fizikai portjai és a fizikai portjain elhelyezkedő eszközök MAC címeinek összerendelésével elsődleges feladata az azonos alhálózati szegmensben a forgalom kapcsolása, fizikai (kábelen keresztüli) összeköttetés biztosítása, tehát a kapcsolódó eszközök közti adatforgalom elősegítése.

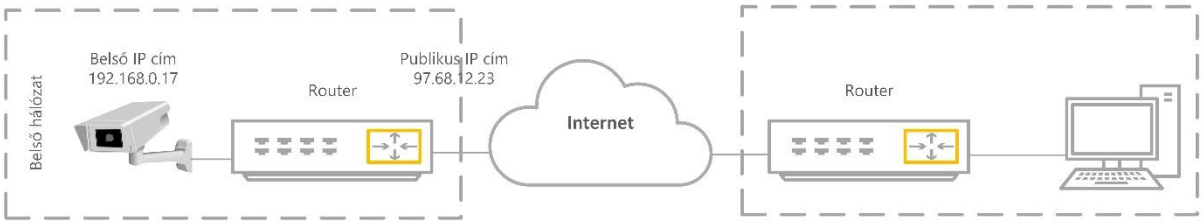


12. ábra[197] Egyszerű switchelt infrastruktúra

A switchek kizárólag azonos hálózatba rendelt eszközök esetében működnek, az adatcsomagok továbbítása egyik LAN-ról egy másik LAN-ra, vagy az interneten keresztül hálózati útválasztókon, úgynevezett routereken keresztül valósul meg. A router

[197] A szerző saját szerkesztésű ábrája.

IP-címek és alhálózati maszkok alapján továbbítja az adatokat egyik hálózatból a másikba. Az útválasztót kis vagy otthoni hálózatok (ún. Smart Office Home Office, SOHO hálózatok) esetében szinte kizárólag a LAN hálózat internethez való csatlakoztatására használják. A router gyakorta valósít meg hálózati címfordítási, ún. NAT (Network Address Translation) szolgáltatást. A NAT szolgáltatás lényegében az interneten nem routolható, irányítható belső hálózati IP címeket cseréli olyan nyilvános, az adott szervezet számára az internetszolgáltató által kiosztott IP címre, amelynek segítségével az publikus hálózaton (internet) keresztül is képes távoli erőforrások elérésére. Az otthoni hálózatokban az internetszolgáltató által biztosított útválasztó (modem) ezzel a módszerrel biztosítja a felhasználói hálózatra privát IP címekkel csatlakoztatott eszközök internetelérését.
A 6. számú ábra belső oldalon egy, a DHCP szerver által kiosztott privát hálózati IP cím fordítását mutatja be. Ha kíváncsiak vagyunk, mi a szolgáltató által biztosított publikus IP címünk, látogassunk el böngészőnkben a *whatismyip.com* oldalra, amely megmutatja nekünk.

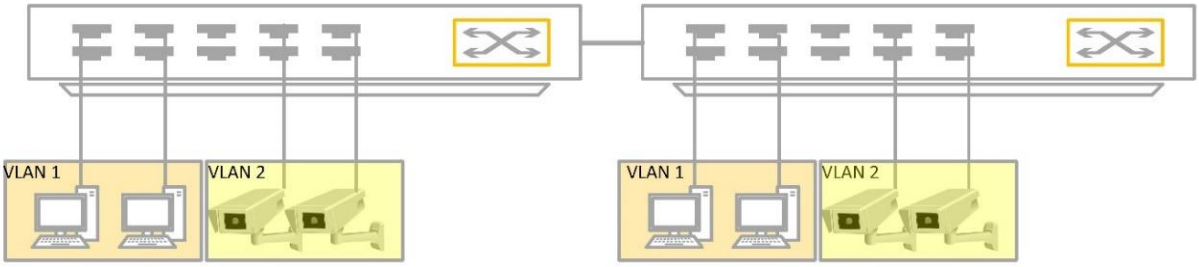


13. ábra[198] Hálózatok összekapcsolása interneten keresztül, router segítségével

A szervezet méretével együtt a hálózatok mérete is (sokszor organikus módon) növekszik. A már említett, fizikai hálózati csatlakozást lehetővé tévő switchek hálózatszervezési feladatukat a rendszer mérete okán nem tudják megfelelően ellátni. Egy idő után a szórási tartományok kezelhetetlen méretűvé válnak, illetve a biztonsági és a teljesítménnyel kapcsolatos szegmentációs igények is megjelennek. Sokszor szükség van arra, hogy különböző fizikai lokáción lévő, de azonos feladatköröket ellátó, azonos erőforrásokat használó felhasználók elhelyezkedésüktől függetlenül tartozzanak, szerveződjenek egy adott hálózati szegmensbe. Ezen igények szolgálják ki az úgynevezett virtuális helyi hálózatok, vagy más néven VLAN-ok (Virtual Local Area Network). A VLAN-ok lehetővé teszik a fizikai topológiától és lokációtól függetlenül a hálózati eszközök előre megadott szempontok szerinti szegmentálását (funkció, biztonság, biztonságtechnikai és ügyviteli (irodai) hálózati elkülönítés, lásd később). Az eszközök egy VLAN-on belül úgy kommunikálnak egymással, mintha közvetlenül ugyanarra a fizikai hálózati eszközre csatlakoznának, de köztük nem fizikai, hanem logikai kapcsolatok vannak. Valamennyi VLAN egy elkülönített logikai hálózatnak tekintendő, és az adott VLAN-hoz nem tartozó eszközök irányába tartó hálózati forgalom célba juttatásához már a különböző hálózatokat összekapcsoló eszközre (router, vagy routing funkciót is megvalósító kapcsoló) van szükség. Ez a fajta elválasztás lehetővé teszi azt is, hogy az adott szeparációs logikának megfelelő hozzáférési és biztonsági házirendeket valósítsunk meg, ugyanis a forgalmat köztük gyakran tűzfalak, vagy hozzáférési listák is korlátozzák (ACL, Access Control

[198] A szerző saját szerkesztésű ábrája.

List). Különböző fizikai eszközökre kapcsolt, de egy logikai alhálózatba tartozó eszközökre mutat példát az 14. ábra.



14. ábra[199] VLAN

A tűzfalak más alkalmazásokban is kiemelten fontos részei a hálózatoknak, ugyanis a hatékony és biztonságos működéshez a hálózatból ki kell zárni az illetéktelen, nem engedélyezett forgalmat (felhasználókat, alkalmazásokat) is. A tűzfalak célja, hogy megakadályozzák egyes védett hálózatokhoz vagy hálózati szegmensekhez történő jogosulatlan hozzáférést. Tűzfalakkal hardveres és szoftveres formában is találkozhatunk. A tűzfalak az átmenő forgalom szabályozását (engedését vagy tiltását) leggyakrabban IP cím (címtartományok) és/vagy portszám alapján végzik, de vannak ezeknél fejlettebb ún. applikációs szintű megoldások is, amelyek a teljes adatfolyamot ellenőrizni, a szabványos kommunikáció követelményeinek megfeleltetni tudják.

14.2. Hálózati kialakítás

A biztonságtechnikai eszközök a gyakorlatban jellemzően három különböző hálózati topológiába szerveződnek, a köztük való választás sok esetben nem pusztán üzemeltetési, hanem biztonsági kérdés is. Biztonsági szempontból a legmegfelelőbb, ám az üzemeltetést, menedzselhetőséget tekintve a legkedvezőtlenebb, ha az eszközöket teljesen elszigeteljük a (vezetékes vagy vezeték nélküli) vállalati ügyviteli hálózattól, így azok saját fizikai topológiával önálló, zárt rendszert alkotnak. Ez azt is jelenti, hogy az operátoroknak, kezelőknek helyi hozzáférés szükséges a rendszerekhez, dedikált, kötött, kevés számú földrajzi helyszínen képesek elvégezni a felhasználói menedzsmentet, vagy adott esetben az eszközbeállításokat, külső hálózati elérések[200] hiányában a frissítéseket manuális módon szükséges telepíteni. Maguk az eszközök magas szintű önvédelmi képességekkel (szabotázsvédelem, kábelvédelem, lásd későbbi fejezetek) rendelkeznek, ez nagyfokú biztonságot nyújt egyes kompromittálási technikák ellen, azonban, különösen nagyvállalati, sokfelhasználós környezetben adminisztrációjuk aránytalan erőforrás felhasználást igényel, illetve a jelzésekre történő reakciót, a hibajavítást, a gyors beavatkozási lehetőséget ez a fajta kialakítás megnehezíti, ezért ma már kevésbé elterjedt, egyes nagy biztonságú alkalmazásokban találkozhatunk még vele.
A másik megoldás, hogy a teljes hálózati szeparáció helyett a rendszerek perifériáit, például az elektronikus megfigyelő rendszerek kameráit vagy a beléptető rendszerek áthaladást biztosító eszközeinek vezérlő termináljait saját, független, lokális elérésű

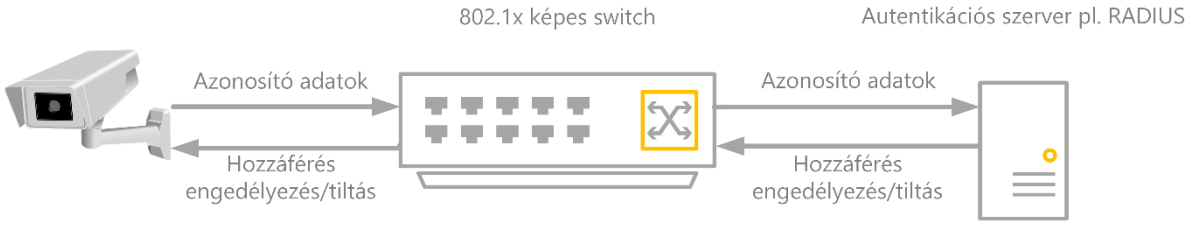
[199] A szerző saját szerkesztésű ábrája.
[200] A teljes képhez hozzátartozik, hogy a zárt rendszerekben is lehetőség van különböző geolokációról történő külső elérésre, monitorozásra, rendszeradminisztrációra, ezek megoldásait a tankönyv későbbi fejezetei ismertetik.

hálózatba szervezik (nem feltétlenül TCP/IP kommunikációt megvalósítva), a rendszerek központi egységei esetében (videó rögzítő vagy menedzsment szerver, beléptető kommunikációs szerver) biztosítják mind a zárt hálózati, mind az ügyviteli hálózati elérést, megoldva ezáltal a távoli menedzsment lehetőségét, de megfelelően elzárva a perifériák közvetlen elérését a külső hálózatokból. Ezt a megoldást leggyakrabban a központi eszközökben elhelyezett két hálózati kártyával (Network Interface Card, NIC) valósítják meg. Az eszköz így mindkét hálózatba „belelát", a kártyák önálló, az adott hálózati szegmensre jellemző IP címekkel rendelkeznek.
A harmadik eset az ügyviteli hálózatot megvalósító fizikai eszközökre történő integráció. Ennek két alváltozata lehetséges. Az elsőben az ügyviteli forgalommal fizikai és logikai szinten is közös infrastruktúra (hálózati eszközök, kábelezés stb.) ám ez annyira előnytelen megoldás mind forgalomszervezés mind biztonsági szempontból, hogy ezzel a módszerrel a gyakorlatban szerencsére csak ritkán találkozhatunk, és nem is javasolt ezen kialakítás megvalósítása. A második lehetőség, hogy az eszközök fizikai lokációjuktól függetlenül azonos VLAN-ba, úgynevezett biztonságtechnikai VLAN-ba szerveződnek. Ahogy láthattuk, a VLAN-ok ismertetésénél, ebben az esetben az átviteli közeg és a hálózati eszközök közösek, de az adatkommunikáció logikailag teljesen függetlenített. Ez egy igen jó szakmai és gazdasági kompromisszum a teljes fizikai szeparáció, illetve a közvetlen ügyviteli hálózati csatlakozás közt. Az önálló logikai hálózatba szervezéssel jól lehet megvalósítani az eszközök hálózati elérésének korlátozását mind hálózati (IP), mind szállítási (port) szinten, a későbbiekben ismertetésre kerülő QoS (Quality of Service, szolgáltatásminőség) követelmények implementálása is könnyebben megoldható, egyszerűbbé, áttekinthetőbbé válik továbbá az eszközök menedzsmentje, csökkennek azok kivitelezési, üzemeltetési költségei.

14.3. Csatlakozás a hálózathoz

A biztonságtechnikai rendszereink tervezésénél bármilyen fizikai kialakítást is választunk, elsődleges kérdés annak meghatározása, milyen védelmet biztosítunk a hálózat perifériáján, annak csatlakozási pontjain. Egy (részben) ügyviteli vagy tisztán biztonságtechnikai hálózathoz történő illetéktelen hozzáférés számos kockázatot hordoz magában. A DHCP kiszolgáló tárgyalásánál láthattuk, hogy használatával egyes felhasználók (így a rosszindulatú felhasználók is) bárhol csatlakozhatnak az adott hálózathoz Ethernet kábellel vagy vezeték nélkül, és azonnal hozzájuthatnak a kommunikációhoz szükséges IP cím információkhoz, amellyel a hálózati szegmens más eszközeivel interakcióra képesek. Egy, a használati célja miatt sokszor publikus, látható, elérhető helyre felszerelt hálózati biztonságtechnikai eszköz eltávolításakor (pl. kamera) a támadó megfelelő csatlakozási védelem hiányában saját alkalmazásaival hozzáférést szerezhet a hálózati szegmenshez, eléri az oda dedikált eszközöket, azokon rosszindulatú szkennelést folytathat a sebezhetőségek felderítése és kihasználása érdekében, illetve különböző adatkapcsolati rétegbe tartozó támadásokat irányíthat az eszközök ellen (ARP poisoning, DHCP starvation, root bridge forgery stb. ezen támadási formák tárgyalása meghaladja jelen tankönyv célját és lehetőségeit). Azért, hogy ezt elkerülhessük, szükséges megvalósítanunk valamilyen autentikációs metódust, amelynek segítségével kizárólag a megbízható kliensek csatlakozását engedélyezzük a hálózatunkon.
Az egyes hálózati eszközök (vezetékes LAN hálózat esetén tipikusan access, ún. hozzáférési rétegben elhelyezett switchek) egy része a rá kapcsolódó eszközök MAC cím alapú autentikációját támogatják. Ez a gyakorlatban (és kissé leegyszerűsítve) azt jelenti, hogy a hálózati rendszeradminisztrátor pontosan megmondja az eszköznek, milyen egyedi azonosítójú fizikai címet fogadhat el a rajta átmenő forgalom engedélyezéséhez. Ez a megoldás rendkívül egyszerű, MAC cím minden hálózati eszköz esetében

rendelkezésre áll, és a switchek szinte ma már kivétel nélkül támogatják fogadó oldalról ezt a megoldást. Hátránya azonban, hogy ez nem tekinthető biztonságos azonosítási módnak, ugyanis a MAC cím speciális ismereteket nem igénylő módszerekkel megváltoztatható. A biztonságon kívül problémát is okozhat abban az esetben, ha a vállalati hálózatbiztonsági szabályok egy switchporthoz egyetlen MAC cím azonosítását engedélyezik (gyakorlatban lehetőség van egy csatlakozási porthoz több MAC címet is előre definiáltan, vagy intelligens tanulással hozzárendelni). WIFI hálózatokon is lehetőség van MAC cím alapú szűrésre white list, ún. engedélyező lista alapú hozzáférés kialakításával, ahol egy adott vezeték nélküli hálózatra az előre definiált listában szereplő MAC címmel rendelkező eszközök csatlakozhatnak.
A biztonsági probléma megoldását jelenti a hálózati aktív eszközökön az ún. 802.1x szintű azonosítás bevezetése (Port Based Authentication, IEEE 802.1x szabvány). Ezzel a módszerrel az eszköz szintén csak sikeres azonosítás után jogosult a hálózat használatára, azonban az azonosító ebben az esetben nem a MAC cím, hanem egy megadott felhasználó-jelszó páros vagy tanúsítvány. A metódus lefutásához szükség van a háttérben egy autentikátorra, amely az eszköz azonosítóit tartalmazza, és amin a jogosultság ellenőrzése megtörténik. Ez leggyakrabban egy RADIUS szerver, amely mögött sokszor a vállalati címtár, pl. Active Directory áll. Az azonosítási protokoll a kérdés-válasz alapú EAP (Extensive Authentication Protocol). Magát a folyamatot egyszerűen leírva, a hálózati hozzáférést engedélyező vezetékes switch vagy vezetéknélküli Access Point (WIFI AP) bekéri a csatlakozni kívánó eszköz azonosítóit, amelyet egy, a felhasználói azonosítókat kezelő háttérrendszeren (pl. RADIUS szerver) validáltat. A RADIUS szerver sokszor nem tárolja a felhasználói azonosítókat, hanem azokat a vállalati címtárból kéri le és az autentikáció eredményét minden esetben szolgáltatja a switch/AP felé, aki az alapján engedélyezi vagy tiltja a hálózat használatát. A hitelesítés sikertelensége esetén az eszköz semmilyen módon nem tud a hálózaton megjelenni, és így annak tekintetében kockázatot sem jelent. További előnye az eljárásnak, hogy dinamikusan ACL (tűzfal) szabályokat és egyéb restrikciókat lehet rákényszeríteni a csatlakozó kliensre annak szerepköre, funkciója alapján, amely így további védelmet jelent. Az EAP autentikáció leegyszerűsített, sematikus működését az alábbi, 8. számú ábra szemlélteti.



15. ábra[201] 802.1x autentikáció sematikus folyamata

Természetesen az autentikáció vezeték nélküli hálózatra történő csatlakoztatás során is megvalósítható és szükséges. Az autentikációs metódus a kliens felhasználónevén és jelszaván is alapulhat, azonban biztonságosabb, ha erre a célra a csatlakozó eszköz részére kibocsátott publikus kulcsú tanúsítványt alkalmazunk.

[201] A szerző saját szerkesztésű ábrája.

E helyütt szükséges kitérni röviden a digitális tanúsítványt alkalmazó technikai ökoszisztéma ismertetésére. Az információbiztonság számos területén alkalmazott eszközök és eljárások összessége az ún. Publikus Kulcsú Infrastruktúra (PKI), mely elektronikus, szabványos formátumú tanúsítványra és aszimmetrikus titkosítási módra épül. Azért, hogy valamely titok, például publikus hálózaton átvitt adat bizalmasságát megőrizzük, szükségünk van egy metódusra, amellyel titkosítjuk azt (az információtechnológiában ezt egy szoftveres vagy hardveres működésű titkosító algoritmussal valósítják meg) és egy közös egy kulcsra, amely a titkosító algoritmus bemeneteként a nyílt információt kizárólag a kommunikációban részt vevő felek számára megismerhető módon transzformálja. Az ún. szimmetrikus kulcsú titkosítási metódusok esetében a titkokat kicserélni kívánó felek – egy kommunikációs kapcsolat két végpontja – ugyanazzal a titkosító kulccsal rendelkezik, amelyet megosztottak egymás közt. A gyakorlati probléma ezzel az, hogy a sokszor igen nagy távolságra lévő felek közt, nyílt csatornákat használva kellene a titkosító kulcsot biztonságosan eljuttatni. Erre a problémára megoldást a publikus kulcsú kriptográfia nyújt. Ennek lényege, hogy a két fél nem ugyanazt a közös kulcsot használja, hanem egy matematikai módszerrel előállítanak egy ún. privát és egy publikus kulcsot. A privát kulcs, ahogy az elnevezése is mutatja, soha nem fedhető fel, nem kerülhet ki a tulajdonosa birtokából, míg a nyilvános kulcsot bárki elérheti, felhasználhatja. A gyakorlatban bármelyik nyilvános kulcsú titkosító algoritmus implementálható, a nem hivatalos szabvány az RSA, sok titkosítást használó megoldás alapul ezen.[202] A küldő fél az adatokat a fogadó fél publikus kulcsának segítségével titkosítja, amely kizárólag a fogadó oldalon, annak privát kulcsának felhasználásával fejthető vissza. A digitális tanúsítványok a tulajdonosra vonatkozó azonosító adatokat és a publikus kulcsokat is tárolják, így valamely entitást (amely lehet személy, szervezet vagy számítógép is) képes minden kétséget kizáróan azonosítani, és a tanúsítványban tárolt publikus kulcs segítségével titkosított csatornát építhetünk fel a hálózati kommunikációban részt vevő felek közt.[203]

A rövid kitérő után visszatérve, az EAP-TLS egy olyan metódust jelent, amely biztonságos, teljes mértékben titkosított és az eszközök kölcsönös hitelesítésén (azonosság ellenőrzésén) alapuló autentikációt képes biztosítani számunkra. Ehhez a megoldáshoz mindkét oldalnak (kliens és szerver) rendelkeznie kell előre telepített, megbízhatónak tekintett, érvényes tanúsítvánnyal, amelyet az azonosítási folyamat során prezentálnak egymásnak. A szerver oldalon is szükség van ellenőrzésre annak biztosítására, hogy a kliens is csak megbízható szerver irányába küldje meg azonosító adatait, kivédve ezzel a megszemélyesítéses (ún. man-in-the-middle) alapú támadásokat. Egyes hálózati biztonságtechnikai eszközök rendelkeznek előre telepített, saját aláírású tanúsítvánnyal,[204] azonban az azonosítási folyamat biztonságához elengedhetetlen, hogy ezeket a tanúsítványokat egy megbízható CA (Certification Authority, tanúsítvány kibocsátó entitás) állítsa ki (és szükség esetén vonja vissza) az eszközök részére, és, hogy

[202] S. Tanenbaum, Andrew, J. Wetherall, David: Számítógép-hálózatok. 13. magyar nyelvű kiadás, Panem Könyvek, Taramix Kft, 2013, Budapest

[203] A PKI digitális életünk számos területén jelen van, annak használatával építjük fel például azokat a titkosított hálózati kapcsolatokat, amelynek segítségével biztonságosan végezhetjük banki tranzakcióinkat az interneten. Számlavezető bankunk nevét a böngészőbe begépelve a címsorban a legtöbb esetben egy zöld lakat és a HTTP protokoll után illesztett S (secure) betű jelzi, hogy kapcsolatunk biztonságos, titkosított (HTTPS).

[204] A saját aláírású tanúsítványok használatát lehetőleg belső alkalmazások során is kerülni kell, a saját aláírás azt jelenti, hogy a tanúsítvány tulajdonosának „személyazonosságát” kizárólag saját maga ellenőrizte.

ezt az eszközök ellenőrizni is képesek legyenek. Ez az entitás általában a vállalati tanúsítványkibocsájtó szerver, amely a teljes informatikai infrastruktúrában elfogadható és megbízhatónak tekintett tanúsítványokat állít elő, és amelyeket előre fel kell telepíteni az eszközökre. A megoldás alkalmazásánál figyelni kell rá, hogy a tanúsítványok többféleképpen előállíthatóak, a biztonságtechnikai eszközünknek támogatnia szükséges a vállalatnál használt digitális formátumokat, illetve egyes alkalmazásokban a tanúsítványok méretkorlátozására is találhatunk példákat.[205]
Fentieket összefoglalva, mindenképpen javasolt a biztonságosnak tekintett EAP-TLS autentikáció megvalósítása ott, ahol az eszközök ezt támogatják, illetve új telepítések esetén már ezzel érdemes tervezni, különösen akkor, ha WIFI hálózaton keresztül csatlakozó eszközöket is tervezünk, ott az egyszerűbb illetéktelen közeghozzáférés miatt határozottan indokolt. A teljes képhez hozzátartozik, hogy lehetnek olyan installációk, ahol az eszközök elhelyezése, illetve későbbi fejezetekben tárgyalt önvédelmi képességek feleslegessé teszik a hálózati autentikáció kikényszerítését. Abban az esetben, ha például egy beléptető terminál hálózati (LAN) csatolója szabotázsvédett, minden illetéktelen nyitást jelezni képes dobozban kerül elhelyezésre, illetve a csatlakozást biztosító switch zárt, behatolásjelző rendszerbe kötött rackszekrényben vagy helyiségben működik, ahol a hozzáférés erősen korlátozott, alacsony a kockázata annak, hogy egy rosszindulatú támadó ezzel a módszerrel próbálná kompromittálni a hálózatunkat, de természetesen a döntést minden esetben kockázatarányosan, a helyi működési sajátosságok és adottságok ismeretében kell meghoznia a felelős szakembernek.

14.4. Titkosítási intézkedések

A biztonságtechnikai rendszerek tervezőinek és alkalmazóinak minden esetben az infrastruktúra kialakításától függően azonosítani kell, hol lehet szükség biztosítani a kommunikációs adatfolyam (data on the fly) biztonságát, rendelkezésre állását és integritását. A biztonságtechnikai alkalmazásokban ezek alapvetően a kamera streamek, a beléptető rendszerben keletkezett alkalmazás szintű adatok, a behatolásjelző rendszerek technikai és támadásjelzései, loginformációk, illetve minden esetben azok a konfigurációs adatok, illetve felhasználói azonosítók, amelynek megismerését szigorúan korlátozni szükséges. A titkosításra vonatkozó követelményeket alapvetően befolyásolják a teljesítményigények, a hálózati kialakítás, a hálózati autentikáció megléte, illetve a hálózat zártsági szintje. Egy szigetüzemű rendszerben, ahol minden periféria és központi egység szabotázsvédett, vagy egy dedikált VLAN-ba szervezett, szigorú hálózati autentikációt és hozzáférési lista alapú szeparációt alkalmazó megoldás teljesen más megfontolásokat követel a titkosított hálózati kommunikáció tekintetében, mint egy rosszul mikroszegmentált, ügyviteli hálózatra kapcsolódó, publikus, külső hálózaton keresztül közvetlenül elérhető és menedzselhető rendszer.
Titkosítási követelményekre releváns példa a már említett videokép átvitel, amely sok esetben a tartalom miatt (vállalati titkos, személyes adatok) kiemelt bizalmassággal bír. Az alkalmazott titkosítási mód függ a gyártó által egyedileg fejlesztett és használt vezérlő jelek és videokép-folyam megoldástól, továbbá a videókép-folyam típusától (unicast, multicast), illetve a felhasználás feltételeitől, például olyan követelményektől, hogy a szabványos streameket támogató, gyártótól független külső rendszerek és lejátszó programok pl. VLC player stb. is értelmezhessék, lejátszhassák azokat.

[205] Bosch: Network Authentication - 802.1x, Secure the Edge of the Network, https://resources-boschsecurity-cdn.azureedge.net/public/documents/WP_802.1x_Special_enUS_22335867275.pdf letöltés ideje: 2023.01.02.

Jellemző, gyártófüggetlen megoldás, ezért példának is kiváló, hogy a kamerák az általuk feldolgozott audio és video tartalmat sok esetben RTP (Real-time Protocol) segítségével továbbítják. Az RTP az OSI modell szerinti alkalmazási és szállítási réteg határán helyet foglaló protokoll, általában UDP fölött használják olyan alkalmazásokban, ahol a csomagvesztés nem okoz nagy problémákat a felhasználás során. Önmagában az RTP protokoll semmilyen védelmet nem biztosít az adatcsomagoknak. Praktikus okokból (pl. hozzáférési szabályokkal, tűzfalakkal jól védett hálózati környezetben a webes kommunikációra alkalmazott 80-as HTTP port gyakorta elérhető, felhasználható) a video adat és vezérlő parancs csomagokat (RTSP/RTCP) TCP fölött működő HTTP kérésekbe és válaszokba csomagolják, amely megoldás önmagában szintén nem biztosít védelmet, ezért javasolt egy autentikáló, titkosító réteg beiktatásával továbbítani az adatforgalmat. A probléma kezelésre a gyakorlatban kétféle elterjed megoldást implementáltak a gyártók. Az egyik az RTP titkosított változata, az SRTP protokoll alkalmazása, a másik a HTTP protokoll védett formája (HTTPS). A HTTPS kommunikáció egy ún. tunnelt épít ki a kliens és a szerver közt, addig az SRTP minden RTP csomagot egyesével titkosít, ami által csak a stream-folyam titkosítására képes. Ha a kliensen szükséges bármilyen adminisztráció elvégzése, pl. konfiguráció módosítása, akkor védett kommunikációs formának a HTTPS jöhet szóba.[206] A megoldás szintén a már ismertetett digitális tanúsítványokon alapul (lásd: TLS, Transport Layer Security).

Manapság már alapvető követelmény, hogy egyes videotechnikai termékek egymással együttműködni legyenek képesek, megoszthassák egymással funkcióikat, képességeiket. Erre a célra a nagyobb gyártók közreműködésével létrejött az ONVIF (Open Network Video Interface Forum) protokoll, amely lehetővé teszi a különböző gyártók különböző eszközeinek együttműködését, video, vezérlő és metaadataik átvitelét, feldolgozását. A különböző alapfunkciók megvalósításához az ONVIF több profilt specifikál, eltérő funkcionalitással és hangsúlyokkal. Biztonsági szempontból kritikus alkalmazásokban olyat érdemes választani, ami a védett TLS kommunikációt lehetővé teszi, pl. ONVIF Q profil.[207]

A tanúsítvány alapú TLS kommunikációt a biztonságtechnika számos további területén alkalmazzák. Szinte minden eszköz (video-megfigyelő, beléptető, behatolásjelző rendszer) kínál a felhasználóknak a gyors és kényelmes kezeléshez asztali vagy web alapú applikációkat, ahol szintén szükséges lehet a szerver-kliens kapcsolat titkosításának megoldása. De nem szabad megfeledkezni a kritikus információk további irányairól sem, így szükséges lehet a támogatott értesítési, távoli logküldési megoldásokban, továbbá az applikációs/kommunikációs szerver és a kezelő kliensprogramok között titkosítás alkalmazása. Abban az esetben, ha adat és/vagy konfigurációmentés is zajlik a különböző hálózati csatornákon keresztül, a mentési irányokat az elsődleges adatforgalomnak megfelelő bizalmassággal szükséges kezelni.

A titkosítási intézkedések egy igen gyakori formája a beléptető rendszerekben alkalmazott, proxymity azonosítókon (belépőkártya) tárolt adatok védelme az autentikációs metódus során. A titkosítatlan, egyirányú kommunikációt alkalmazó technológiák (jellemzően 125Khz-es frekvenciát használó azonosítók) esetében csak az azonosító küld adatokat az olvasó felé, és minden esetben ugyanazt a kódsorozatot. Ezek a rendszerek lehallgatás és másolás ellen védhetetlenek, a tárolt adatok, nagyobb, akár méteres távolságról az erre a célra épített berendezésekkel a tulajdonos tudta nélkül is

[206] Axis Communications: Encrypting network streams: An overview of why and how to encrypt network video letöltés ideje: 2022.01.12.

[207] https://www.onvif.org/wp-content/uploads/2019/01/ONVIF_Profile_Q_Specification_v1-2.pdf letöltés ideje: 2022.03.01.

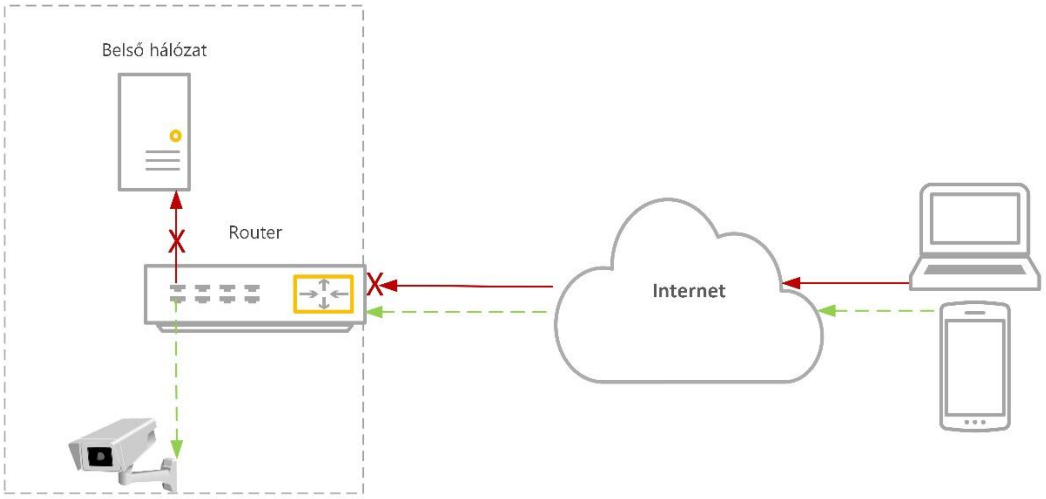
hozzáférhetők. Minden belépési ponton, de minimum a kritikus biztonságú helyszíneken (pl. szervertermek) érdemes megfontolni olyan nagy biztonságú azonosítók használatát (AES kódolású rendszerek, legalább 128 bites titkosítással, pl. MIFARE Plus X vagy DESFire), amelyek kétirányú kommunikációval kölcsönösen ellenőrzik egymást és tikosított adatátvitelt biztosítanak az autentikációs folyamat során.[208]
Minden titkosítási rendszerben, így a tanúsítvány alapú alkalmazásokban is gondoskodni kell a kulcsok megfelelő védelméről, amely sok esetben nem csak azok bizalmasságát, hanem a rendelkezésére állását is jelentik. A kulcsok, tanúsítványok kompromittálódása, elvesztése, sérülése tragikus következményekkel járhat az üzemeltetők számára, ezért kiemelt kérdés annak meghatározása, ki, milyen módon férhet hozzá, állíthatja elő és tárolhatja ezeket. A kulcsok mentéséről és biztonságos külső tárolásáról gondoskodni kell, hogy szükség esetén a forrásrendszeren visszaállításra kerülhessenek. Szintén lényeges az egyes titkosítási eljárások folyamatos nyomon követése és értékelése, hogy a kiválasztott és telepített biztonságtechnikai rendszerekben a titkosítás kizárólag az iparági sztenderdeknek megfelelő, ismert, biztonságosnak tekintett kriptográfiai megoldásokkal (titkosítási algoritmus, kulcskezelést, integritást biztosító Hash algoritmusok stb.) legyen implementálva.

14.5. Külső hálózati hozzáférések biztonsága

A hálózati forgalom bizalmassága tekintetében külön figyelmet érdemelnek azok az esetek, amikor az adatokat külső, megbízhatatlan hálózat irányába szükséges továbbítani, és/vagy a rendszerek elérését, menedzsmentjét ezekből az irányokból szükséges megoldani, sokszor mobilkommunikációs végponti eszközök segítségével. Ennek biztonságos megvalósítása a gyakorlatban nem triviális egyszerűségű, a belső, lokális hálózaton helyet foglaló eszközeink elérését ugyanis a legtöbb esetben NAT megoldást is magukba foglaló, a hálózatot a külvilágtól erős tűzfalmegoldásokkal védő technológiák korlátozzák, amelyek szinte kivétel nélkül megakadályozzák a belső előzmény nélküli, kívülről kezdeményezett hálózati csatlakozási kérelmeket. Ennek oka, hogy a rendszerarchitektúra a legtöbb esetben kliens-szerver megvalósítású, amelyeknek alapvető tulajdonsága, hogy a kiszolgáló (szerver) nem kezdeményez kapcsolatot a kliens irányába. A tűzfalak egy jelentős része ún. stateful (állapottartó vagy állapotalapú) működésű, kizárólag olyan kapcsolatokat engedélyez létrehozni és fenntartani, amelyekről valamilyen állapotinformációval rendelkezik, és külön beállítások nélkül a kívülről érkező kérések elől a belső hálózati eszközöket hermetikusan elzárja. Amennyiben mégis szükségünk van a rendszereinek távoli hálózatokból történő hozzáférésére, ezen védelmi intézkedések „megkerülésére” több megoldás is rendelkezésre áll.
A külső hálózati elérésekben az egyik megoldási mód az ún. port-forward (port-továbbítási) technológia alkalmazása. Ez a technológia amellett, hogy a legrégebbi, a legkevésbé biztonságos megoldást is nyújtja. Alapvető működése a következő: a külső hálózati elérést biztosító eszközön (pl. NAT router) egy külső portot nyitunk, amely a csatlakozási kérelmet a beállított porttovábbítási szabály szerint átadja egy megadott eszköznek. Ez a megoldás rendkívül kockázatos, mert az így megnyitott hozzáférésen bárki az internet irányából elérheti az eszközünket, és még abban az esetben is, ha nem tudja megkerülni az alkalmazott autentikációs eljárásokat (pl. jelszó-felhasználónév páros), és ezáltal nem képes közvetlen hozzáférést szerezni, de képes rá, hogy

[208] https://www.securinfo.hu/termekek/beleptetorendszerek/1277-az-azonositas-biztonsaga-a-beleptetorendszereknel-i-resz.html letöltés ideje: 2022.11.07.

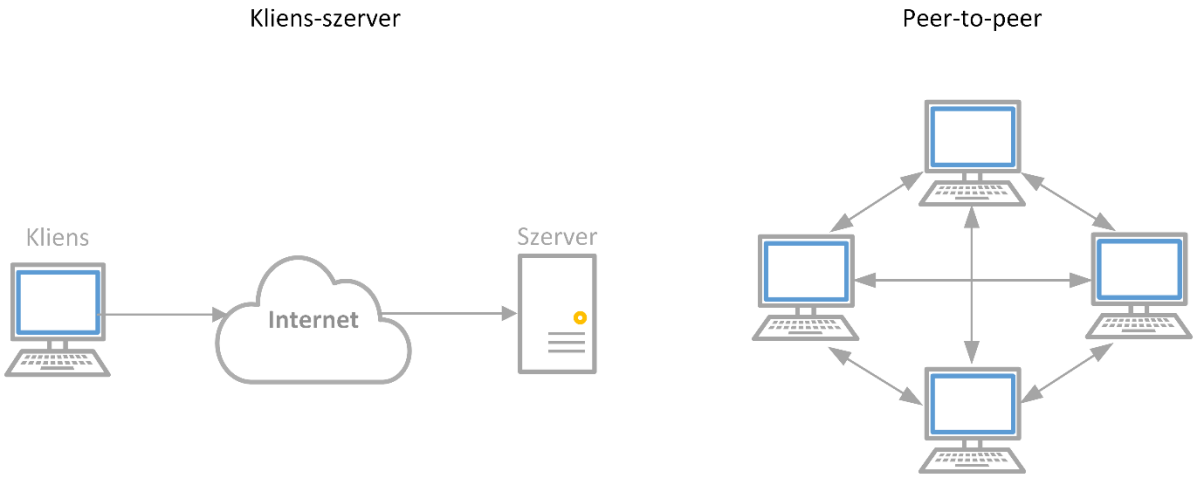
meghatározza az érintett megoldás típusát, gyártóját, egyéb azonosítóit, amelynek segítségével egy esetleges ismert sebezhetőséget kihasználva kompromittálhatja azt.



16. ábra[209] Port-forward

A már ismertetett kliens-szerver működési modellen kívül egy másik jellemző rendszerarchitektúra is elterjedt a hálózatok világában, amelyet bizonyos biztonságtechnikai megoldásokban, kifejezetten az elektronikus megfigyelőrendszerekben is egyre gyakrabban alkalmaznak. A P2P (Peer-to-Peer, egyenrangú társak hálózata) egy kommunikációs protokoll, amely, szemben a szerver-kliens kapcsolatokkal – ahol a kommunikációs kezdeményezésért a kliens oldal a felelős – az eszközök egymás közötti direkt, kezdeményezési szabályok nélküli kommunikációját teszi lehővé. A P2P tehát egy olyan modell, amely lehetővé teszi a társak számára, hogy központi szerver nélkül osszák meg egymással az erőforrásokat, P2P-hálózat minden egyes csomópontja kiszolgálóként és kliensként is működik, közvetlenül kommunikálnak egymással. A két architektúra közti alapvető különbséget a 10. számú ábra szemlélteti.

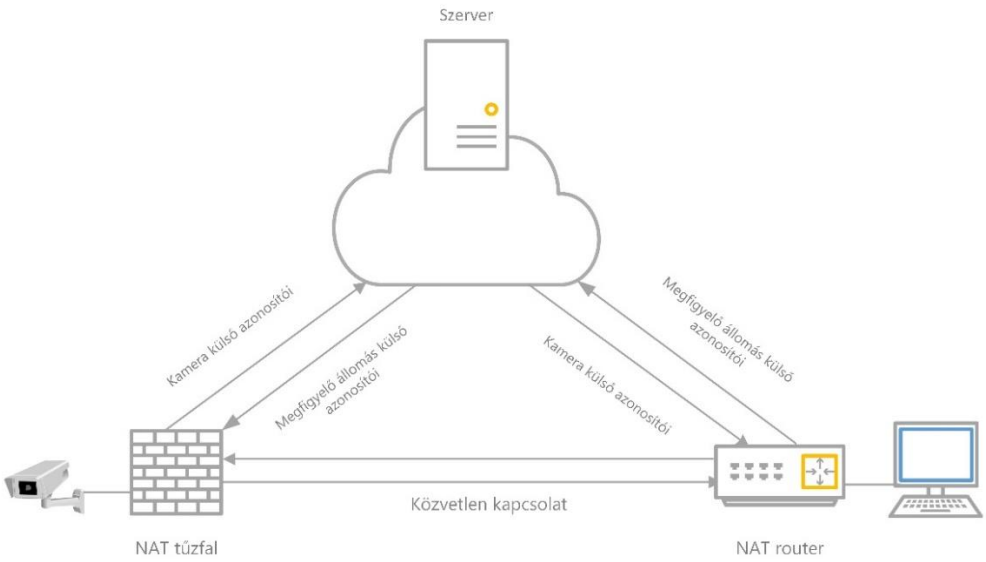
[209] A szerző saját szerkesztésű ábrája.



17. ábra[210] Kliens-szerver és P2P architektúra

Ahogy arról már szó volt, külső hálózati elérési igény esetén a küldő és a fogadó oldal (kommunikációs felek) NAT eszközök, például tűzfalak, routerek két oldalán helyezkednek el, belső hálózati IP címeket használva, amely nem teszi lehetővé, hogy a nyilvános hálózaton lévő hosztok elérjék egymást, azonban a P2P kommunikációs modell megköveteli, hogy mindkét kommunikációs fél képes legyen proaktívan hozzáférni a privát hálózaton lévő hosztokhoz. Ezért a P2P kapcsolatok felépítése előtt egy olyan módszert kell alkalmazni, amely képes megkerüli a NAT technológiát. Ilyen NAT megkerülési (NAT traversal) megoldásból számosat ismerünk, a leggyakoribb az ún. UDP hole-punching. A biztonságtechnikai gyakorlatban alkalmazott technológiák a legtöbb esetben valamely közvetítő szerver (nyomkövető szerver) közbeiktatását igénylik, amin keresztül leegyeztetik a közvetlen kapcsolathoz szükséges technikai részleteket. Ebben a megoldásban a kommunikációs felek külön-külön UDP-kapcsolatot létesítenek egy, a gyártó által felállított, publikus internethálózaton elérhető központi kiszolgálóval. A NAT mechanizmus után a kliensek belső IP-címei és portszámai lefordításra kerülnek a kliensek nyilvános IP-címére és portszámára, amelyet a nyomkövető szerver kicserél a kommunikációs felek közt. Miután a felek megkapják egymás belső és nyilvános IP-címét és portszámát a központi kiszolgálótól, UDP adatcsomagokat küldenek egymásnak, amely kommunikáció létrehoz egy munkamenet-bejegyzést a küldő oldalak NAT eszközén, beütve rajtuk egy „kommunikációs lyukat” (ahonnan a név, UDP hole-punching ered), és ily módon megkezdődik a felek közti közvetlen P2P adatátvitel.[211]

[210] A szerző saját szerkesztésű ábrája.
[211] Huawei HoloSens,2020, Intelligent Vision, Tech Express.
https://support.huawei.com/enterprise/en/doc/EDOC1100172551 letöltés ideje: 2022.10.27.

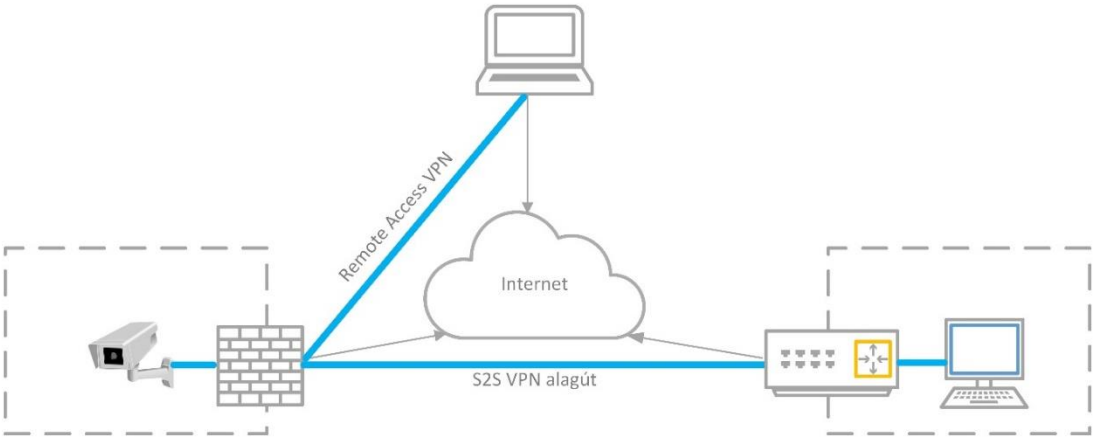


18. ábra[212] UDP hole-punching sematikus ábrája

A P2P kommunikációt biztosító eszközök biztonságosabbnak tekinthetőek az előzőekben tárgyalt port-forwarding megoldásnál, azonban számos aggály felmerül az alkalmazásukkal kapcsolatban, ugyanis a gyakorlatban sok múlik rajta, az egyes gyártók hogyan implementálják megoldásaikat a szoftvereikben. Napjainkban számos, a biztonságtechnikai eszközöket, főleg a kamerákat érintő, P2P szoftversebezhetőséget tártak fel, amelyen keresztül az eszközök kompromittálhatóvá váltak.
A harmadik, és egyben utoljára tárgyalt külső hálózati elérést biztosító megoldás a legbiztonságosabb mind közül, az az úgynevezett VPN, vagyis virtuális magánhálózat kialakítása (Virtual Private Network). A VPN biztonságos, titkosított kapcsolatot hoz létre publikus hálózat fölött két kommunikációs entitás közt, úgy, hogy egy virtuális „alagutat" épít ki közöttük. Segítségével képesek vagyunk elérni a belső hálózaton lévő erőforrásokat úgy, mintha mi is az adott hálózatban „ülnénk", a topológia látszólag megegyezik a privát hálózattal. A VPN kapcsolatot létrehozó eszközök leggyakrabban két vállalati telephelyet összekötő VPN gatewayek (átjárók), amelyek lehetnek erre dedikált eszközök, de lehet a router vagy a tűzfal részeként is megvalósítva (ún. Site-to-Site, S2S VPN). Egy másik típusa, az ún. remote access VPN, amely mobil eszközök számára nyújt biztonságos elérést, egyik végpontja általában a vállalati VPN gateway, míg a másik oldalon valamely mobil eszközre (telefon, tablet, laptop) előre telepített, vagy operációs rendszerbe épített szoftveres megoldás biztosít csatlakozási lehetőséget. A technológia segítségével, internetelérés birtokában lokációtól függetlenül, bárhonnan, akár mozgás közben is csatlakozhatunk a vállalati hálózatra. A leggyakoribb VPN megoldások (pl. IPSec VPN) a titkosításon kívül a felek hitelesítését és a forgalom integritásellenőrzését is biztosítják.[213] A 12. számú ábra a VPN kapcsolatok sematikus felépítését mutatja.

[212] A szerző saját szerkesztésű ábrája.

[213] S. Tanenbaum, Andrew, J. Wetherall, David: Számítógép-hálózatok. 13. magyar nyelvű kiadás, Panem Könyvek, Taramix Kft, 2013, Budapest.



19. ábra[214] VPN

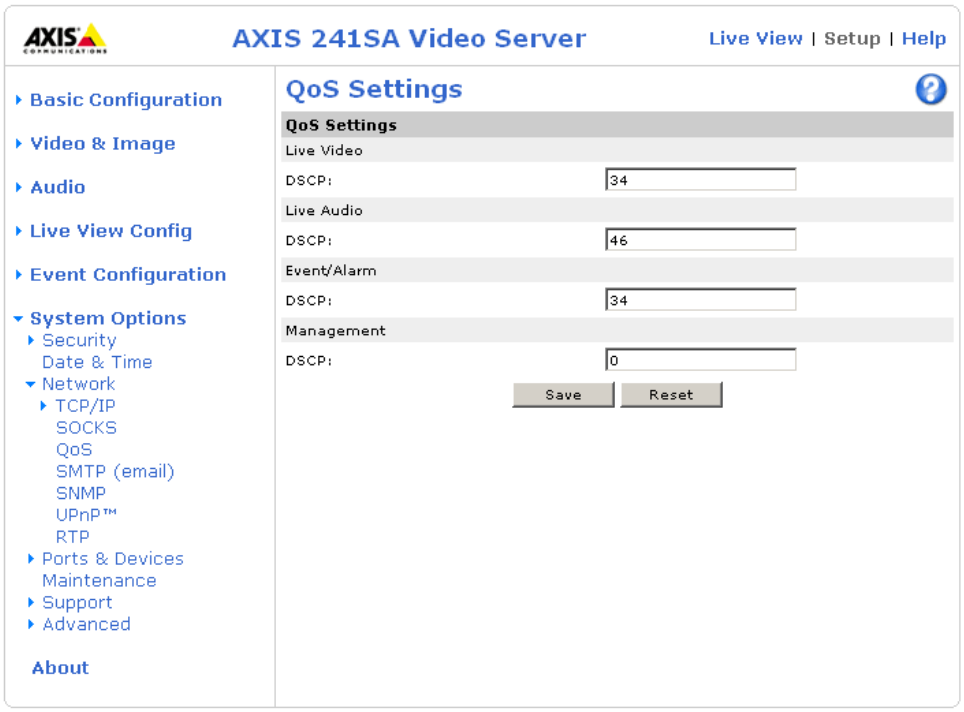
14.6. Szolgáltatásminőség (QoS)

A bevezetőben bemutatott, hálózati konvergált forgalom azt is jelenti, hogy a forgalom hibáira (adatvesztés, késleltetés, jitter stb.) különböző mértékben érzékeny alkalmazások, pl. fájlátvitel, e-mail, VoIP (Voice over IP, hálózati hangátvitel), az elektronikus megfigyelőrendszerek videostreamjei vagy a biztonságtechnikai rendszerek riasztásjelzései osztoznak fizikailag azonos átviteli közegen, felülről korlátos sávszélességen, amely okozhat problémákat a hatékony működésben. Egy adott szegmensben az átvitel során a hálózati eszközök alap működési elvéből adódóan bármely típusú forgalom azonos eséllyel, az ún. FIFO elv alapján (First In-First Out) kerül továbbításra, illetve, ha a forgalom nagysága miatt torlódás lép fel, eldobásra/késleltetésre. A switcheken és a routereken megvalósított forgalompriorizálási opció, ún. QoS (Quality of Service) megoldja ezt a problémát azáltal, hogy az előre megadott szabályok és kommunikációs igények alapján képes a hálózati teljesítményoptimalizálást és a sávszélesség hatékony kihasználását lehetővé tenni, illetve biztosítani, hogy a késleltetésre érzékenyebb és/vagy a kritikus feladatot megvalósító szolgáltatások (pl. videostream, riasztásjelzés) elsőbbséget kapjanak a hálózati átvitel során. Ehhez az szükséges, hogy egy adott hálózat összes eszköze képes legyen a QoS funkció megvalósítására. A forgalompriorizálási opció implementálható az OSI modell több rétegében, legjellemzőbben az adatkapcsolati (L2) és a hálózati (L3) rétegben.

Az IEEE 802.1p az Ethernet (L2) keret fejlécében egy mezőt alkalmaz, amelyben nyolc, 0-7 tartományú, növekvő prioritású szint fér el (CoS, Class of Service). A hálózatra csatlakozó eszközök a LAN-ba küldött forgalom kereteiben megadják a prioritás értékét. Az adatkapcsolati eszközök (jellemzően switch) a kereteket a prioritásnak megfelelő várakozási sorok segítségével kezelik. A mechanizmus csak alhálózaton belül működik, különböző hálózatok között nem érvényesül. A manapság leggyakrabban alkalmazott, ún. DiffServ forgalomkezelő mechanizmus egy OSI L3 szintű QoS mechanizmus, amely az IP csomagok fejrészében DSCP (DiffServ CodePoint) nevű mezőt helyez el. A végfelhasználói eszközök a DiffServ hálózatba küldött forgalom minden egyes csomagját a megfelelő DSCP értékkel látják el. A DiffServ hálózatban lévő routerek minden csomagra a DSCP érték alapján történő osztályozás szerint specifikus várakozásisor-

[214] A szerző saját szerkesztésű ábrája.

kezelő algoritmust alkalmaznak. A DSCP értékek 0-63 tartományban oszthatóak ki, növekvő prioritás mellett.[215]
Bár a 802.1p CoS jól működik, nem skálázható, és nem tud végponttól végpontig tartó (hálózatok közti) garanciákat nyújtani. A ma forgalmazott hálózati kapcsolók képesek az L3 (IP DSCP) QoS és az L2 CoS közt leképezést biztosítani, így főleg a DiffServ mechanizmus alkalmazott széleskörűen a biztonságtechnikai eszközök esetében is, amelyek az adott típusnak megfelelően egyedileg, külön is priorizálhatják forgalmukat, más értékeket választva pl. a riasztásjelzéseknek, a menedzsment forgalomnak vagy az élő videoképeknek.[216]
Az alábbi, 13. számú ábra egy Axis termék forgalompriorizálási opcióit mutatja be.



20. ábra[217]

QoS beállítás

14.7. Hálózati időszinkron

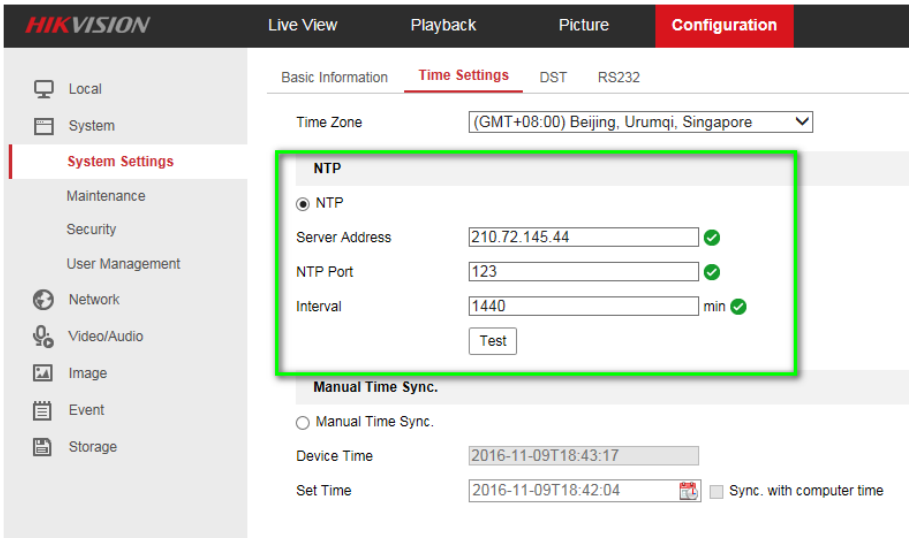
A (hálózatba kapcsolt) biztonságtechnikai eszközök működéséhez kiemelten fontos a megfelelő idő és dátumbeállítás. A kamerarendszerek esetében egy utólagos kiértékelés során a videofolyamban elhelyezett időbélyeg megjeleníti a felvétel pillanatában aktuális dátumot és időt, ami megadja, hogy egy adott cselekmény pontosan mikor történt, vagy nagyobb rendszer, több kamera esetén, hogy az egyes cselekmények egymáshoz képest mikor történtek. A beléptető rendszer adatbázisában tárolt mozgási adatok megfelelő értékeléséhez szintén szükséges a dátum-idő pontossága, de legyen szó bármilyen rendszerről, a hibaelhárításhoz, az egyes felhasználói interakciók ellenőrzéséhez használt logbázis hitelességéhez alapvetően elengedetlen, hogy a rendszerek idejét a lehető

[215] Gál Zoltán, Balla Tamás: A QoS hatása az infokommunikációs alkalmazásokra. Híradástechnika. LXII. 7-16., 2007

[216] QoS in Axis Video Products, technical note, Rev: 1.0 Updated 2006-02-15 letöltés ideje:2022.11.14.

[217] Az ábra forrása: QoS in Axis Video Products, technical note, Rev: 1.0 Updated 2006-02-15 letöltés ideje: 2022.11.14.

legpontosabban konfiguráljuk, annak minden egyes eleme a tényleges pontos időhöz legyen szinkronizálva.[218]
A dátum-idő beállítások működhetnek gyakori ellenőrzésekkel manuális módon is, azonban a legjobb gyakorlatnak megfelelően automatikus módon is elvégezhetjük, úgynevezett NTP szolgáltatás igénybevételével (Network Time Protocol). Az NTP, ahogy a nevében is benne van, egy hálózati kommunikációs protokoll, amelyet informatikai rendszerek óráinak szinkronizálására fejlesztettek ki. Az NTP használatához fontos, hogy az eszközünkben implementálásra kerüljön NTP kliens (amely ma már szinte minden rendszer integráns része), és szükséges ismernünk a telepítés helyszínének lokális hálózatában alkalmazott NTP időszerver IP címét, melyhez szinkronizálni szükséges. Abban az esetben, ha nincs ilyen, akkor használhatóak megbízható publikus NTP szolgáltatók, pl. time.google.com. Ebben az esetben nehézségekbe ütközhetünk, ha a belső vállalati hálózati szabályok nem támogatják a külső NTP szolgáltatás igénybevételét, az időszinkron módját és lehetőségeit minden esetben még a tervezés során a hálózati rendszergazdával egyeztetni szükséges.
Az NTP szolgáltatás alapvetően a jól ismert, szabványos (well-known) portok egyikén (123 UDP) működik, ez egyszerűbbé teheti a külső szerver használatát. Jó gyakorlat lehet, ahol lehetséges, pl. a hálózati videorögzítők esetén, az NTP-t (és DST-t, lásd lentebb) ne minden kameránál állítsuk be, hanem (NAT-olt rögzítési hálózaton belül) az adott eszköz ezeket a rögzítőről lekérje.[219]
Az NTP beállítások elvégzése a legtöbb rendszer esetében viszonylag egyszerű, a szerver IP címén és a portszámon kívül a szinkronizációs időintervallumot szükséges megadnunk. A jó gyakorlat szerint 30-60 perc indokolt, azonban egyes alkalmazásoknál a napon belüli szinkronizáció is elegendő lehet. Az alábbi, 14. számú ábra egy Hikvision hálózati rögzítő konfigurációs beállításait mutatja.



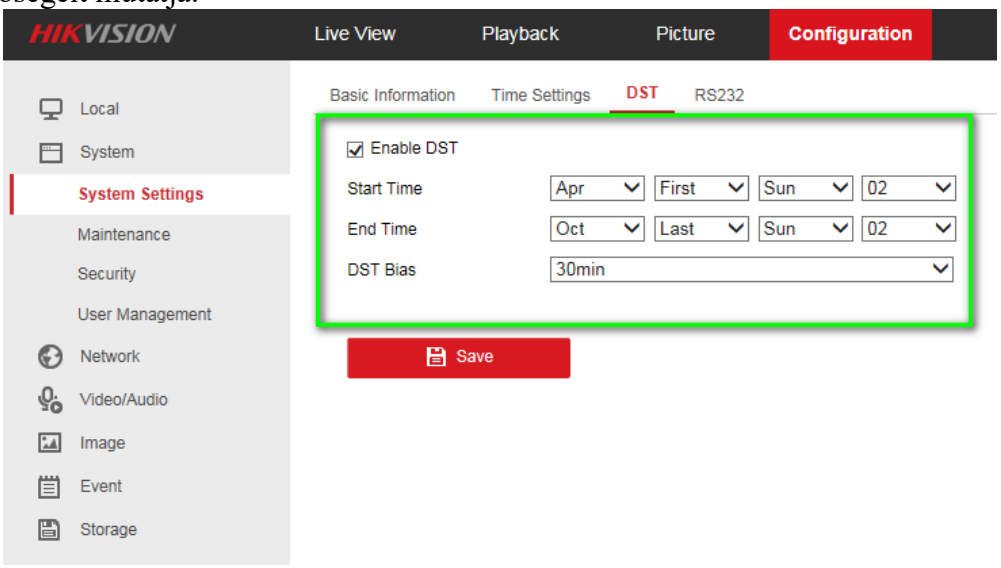
21. ábra[220] NTP konfiguráció

[218] https://www.riel.hu/tamogatas/tudastar/video/hikvision-ntp-es-dst-beallitas letöltés ideje: 2022.02.13.

[219] https://www.riel.hu/tamogatas/tudastar/video/hikvision-ntp-es-dst-beallitas letöltés ideje: 2022.02.13.

[220] Az ábra forrása: https://www.hikvision.com/content/dam/hikvision/en/support/download/how to/nvr/How%20to%20configure%20NTP%20and%20DST.pdf letöltés ideje:2022.02.13.

Az NTP beállítások mellett javasolt, hogy a nyári időszámítás (DST-Daylight Saving Time, Európában: summer time) alapvető beállításait is elvégezzük az eszközön. Ha az NTP mellett a DST beállításait nem végezzük el, elképzelhető, hogy az eszköz nem szinkronizál a helyi DST idővel. A 15. számú ábra a fenti eszköz nyári időbeállításainak lehetőségeit mutatja.

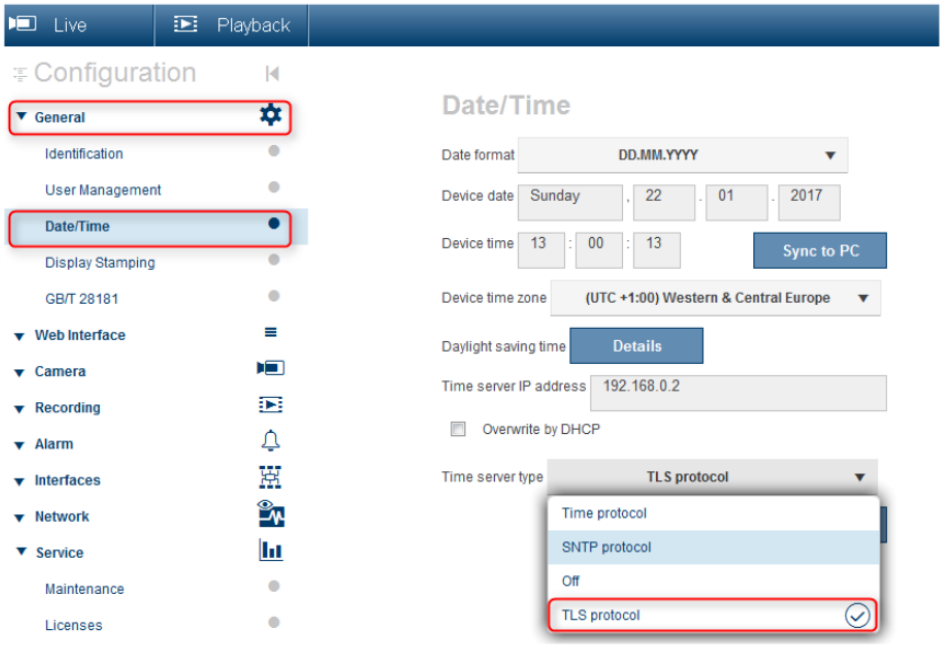


22. ábra[221] DST beállítás

Maga az NTP protokoll semmilyen beépített védelmet (pl. titkosítás, autentikáció) nem tartalmaz, és ez néhány fokozott biztonságú alkalmazásban probléma lehet. Az is előfordulhat, hogy nincs a rendszerek számára használható NTP szerver az adott hálózatban és/vagy a külső NTP források nem igényelhetők, a hálózati rendszeradminisztráció tiltja a 123-as port megnyitását publikus irányokba. Erre az esetre létezik egy érdekes, a gyakorlatban kevésbé alkalmazott, ám néhány gyártó termékeiben már elérhető megoldás, amely az NTP protokoll teljeskörű mellőzésével képes az automatikus időbeállításra. Ez a megoldás az ún. TLS-date, amely, ahogy a neve is mutatja, TLS protokoll használatával biztosítja az időszinkront. A TLS protokollt bevezető RFC két olyan függvényt is definiál a HTTPS kapcsolatiniciáló (handshake) folyamatban, amelyben időbélyeg használata szükséges. Ennek segítségével bármelyik, a hálózatban elérhető HTTPS szervert képesek lehetünk használni időszinkronra. Természetesen ez a megoldás egy úgynevezett best effort megoldás, amely nem garantálja, hogy a forrásszerver időbeállításai teljesen pontosak, de néhány alkalmazásban ez is elég lehet. További kockázat lehet, hogy a pontos rendszeridő egy nem erre a célra tervezett megoldástól függ, amely a szabvány módosításával eltűnhet a gyakorlatból.[222] A 16. számú ábra egy Bosch videó eszköz beállítási lehetőségét mutatja, ahol a TLS alapú időszinkron elérhető.

[221] Az ábra forrása: https://www.hikvision.com/content/dam/hikvision/en/support/download/how to/nvr/How%20to%20configure%20NTP%20and%20DST.pdf letöltés ideje:2022.02.13.

[222] Allan Liska: NTP Security: A Quick-Start Guide, Apress, 2016, p.83 ISBN:9781484224120



23. ábra[223] **TLS-date beállítás**

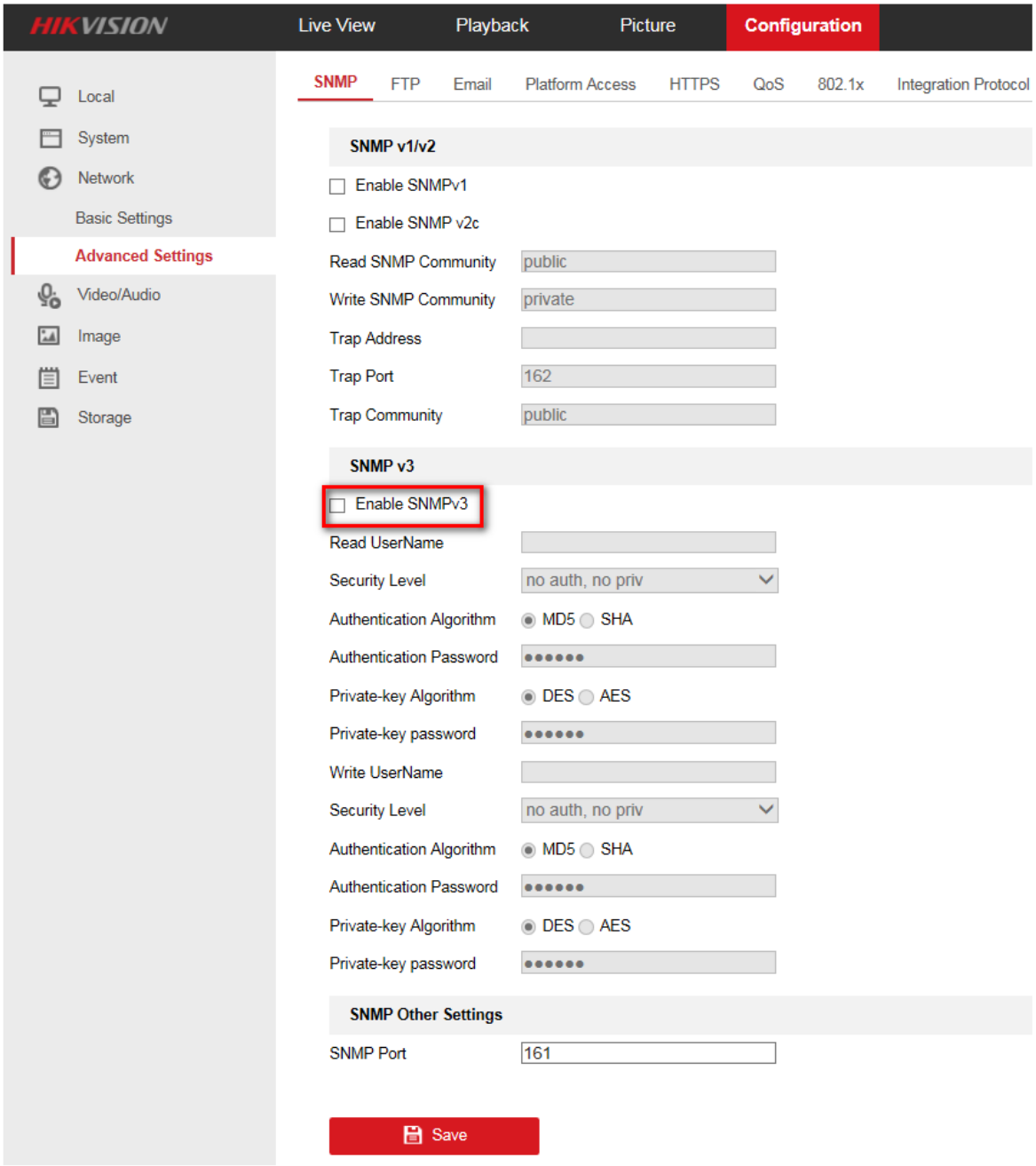
14.8. Hálózati felügyelet

A biztonságos és megbízható működéshez a biztonságtechnikai eszközeinket és azok teljes hálózati infrastruktúráját is felügyelni szükséges, különösen ott, ahol a bizalmasság, a rendelkezésre állás, illetve az erőforrásokkal való hatékony gazdálkodás kiemelt jelentőségű. A felügyelet ebben az esetben azt jelenti, hogy (közel) valós időben legyünk képesek a működést érintő egyes biztonsági eseményekre, hibákra reagálni, másrészt lehetőségünk legyen az események utólagos vizsgálatára, az egyes hibák okainak mélyebb elemzésére. A valós idejű (real-time) felügyelet megvalósítására a gyakorlatban sokféle módszerrel találkozhatunk, az e-mail riasztásokon át az SMS üzenetekig, azonban a legjobb, és leginkább elterjedt megoldás az ún. hálózati menedzsment protokollok alkalmazásával kért és küldött jelzések, információk feldolgozása. A szabványos, eszközfüggetlen megvalósítású hálózati menedzsment protokollok célja, hogy információt szolgáltassanak az üzemeltető személyek számára a felügyeletük alá rendelt eszközök úgy, mint biztonságtechnikai végpontok (pl. kamerák, vezérlők), szerverek, aktív hálózati eszközök szoftveres és hardveres működéséről, állapotáról. A hálózati menedzsment protokolloknak több fajtáját és típusát is ismerjük, azokat is többféleképpen csoportosíthatjuk. Architektúrájukban lehetnek egyszerűek (pl. az ún. ping parancs, vagy ICMP ECHO, amely az egyes node-ok hálózaton keresztüli elérhetőségéről és a hálózati kapcsolat sebességéről szolgáltat nekünk információt) vagy összetettek, illetve működési módjukban passzív, ún. lekérdezéses (polling) továbbá aktív (eseményvezérelt) megvalósításúak. A hálózati felügyeleti megoldásokban az egyik legyakrabban alkalmazott SNMP (Simple Network Management Protocol) egy kliens-szerver architektúrájú, alkalmazási szintű protokoll, amelyet eredetileg a „klasszikus” hálózati eszközök felügyeletére alkalmaztak, azonban ma már a legtöbb biztonságtechnikai alkalmazás szolgáltat SNMP segítségével típusáról, állapotáról és működésében bekövetkezett szoftveres (típus, gyártó, szoftververzió stb.) és hardveres (CPU, memória,

[223] Bosch IP Video and Data Security Guidebook p.26. letöltés ideje: 2022.07.21.

tárhely információk, hőmérsékleti adatok stb.) változásokról információkat. Az SNMP funkció működése nem alapértelmezett, annak használatát az eszközök telepítése és üzembe helyezése során engedélyezni és konfigurálni kell a vállalatnál alkalmazott központi hálózatfelügyeleti alkalmazással történő kommunikációhoz. A vállalati felügyeleti rendszer központi része jellemzően egy menedzsment szerver, amely összegyűjti és megjeleníti a felügyelt rendszerelemek (SNMP agent vagy ügynök) összes adatát. Az SNMP protokoll definiálja mind a passzív (SNMP query) mind az aktív módot (SNMP trap). Az első esetben a menedzsment szerver a beállított gyakorisággal lekérdezi a klienseket azok státuszáról, míg trap alkalmazása esetén az eszközök saját maguk aktívan értesíthetik a menedzsment szervert a rendszer állapotában történt változásról.
A két megoldás közti döntés alapvetően a rendszer sajátosságainak és az egyes eszközök működési kritikusságának függvénye. A lekérdezés biztonságosabb a tekintetben, hogy válasz hiánya esetén információt kapunk arról, hogy a rendszerünk egyik eleménél hiba van, hátránya, hogy erről csak az előre beállított időközönként (polling time) értesülünk. Az SNMP trap legtöbbször megbízhatatlan kézbesítést biztosít, így nem garantált, hogy az üzenet eljut a menedzsment szerverig, cserébe az eszköz azonnal tud reagálni az egyes eseményekre. A polling time, vagy lekérdezési idő túl gyakori beállítása egy nagyobb hálózat esetén olyan hálózati overhead-et (túlforgalmat) generálhat, ami problémákat okozhat a hálózati szegmens működésben.
Az egyes biztonságtechnikai eszközök gyártótól függően különböző mértékben szolgáltatnak információkat magukról. Ezeket a szolgáltatott információkat egy szabványos Management Information Base-ban, az úgynevezett MIB fájlban tárolják. Némi egyszerűsítéssel a MIB fájlok azon információk halmazát jelentik, amelyet a felügyeleti szerver képes polling eljárással lekérdezni a felügyelt eszközből, vagy a felügyelt eszköz trapként képes elküldeni a felügyeleti szerver irányába. A szabványos MIB objektumok nagyszámú teljesítményfelügyeleti paramétert definiálnak, amelyek általában minden hálózati eszközre, gyártófüggetlenül érvényesek, illetve léteznek privát MIB kiterjesztések a gyártóspecifikus teljesítményfelügyeleti paraméterek lefedésére. Ezeket az információs objektumokat az adatbázisban egy úgynevezett OID-vel (object identifier) azonosítjuk. Az egyes gyártók ezeket a file-okat a termékkel együtt biztosítják és/vagy publikus csatornákon keresztül elérhetővé teszik a felhasználók számára a hálózati felügyeleti rendszerbe való integrálás érdekében, mert a menedzsment szervernek minden ügynöktípus esetében ismernie kell a privát kérdéseket is. Az eszközök által küldött üzenetek bizalmas adatoknak minősülnek, illetéktelen kezekbe kerülve értékes információkat szolgáltathatnak a rendszerek kompromittálásához. Az egyes performancia kérdések mellett a biztonság tekintetében jelentősége van, hogy az SNMP-nek a gyakorlatban alkalmazott három, kronológiai sorrendben egymást követő, de még egymás mellett élő különböző változata közül melyik típust alkalmazzuk. Az SNMPv1 és v2 verziója semmilyen bizalmassággal nem rendelkezik, az SNMP információk, illetve a menedzsment szerver és az ügynökök közt autentikációhoz használt jelszó titkosítatlanul (clear text) megy át a hálózaton, ezért csak akkor engedélyezzük azokat, ha feltétlenül szükséges. Használatuk csak akkor javasolt, ha biztosítható, hogy a hálózat fizikailag és logikailag is védve van az illetéktelen hozzáféréstől és lehallgatástól (pl. az SNMP ügynökök és a menedzsment szerver logikailag egy VLAN-ban található, a hálózathoz történő fizikai csatlakozás autentikációhoz kötött stb.) Az SNMP 3. verziója (SNMPv3) a csomagok titkosítása és a megfelelő autentikációs metódusok révén már

megfelel a bizalmassági, hitelesítési és integritásra vonatkozó követelményeknek.[224] Az alábbi, 17. számú ábra egy Hikvision eszköz SNMP beállítási lehetőségeit szemlélteti.

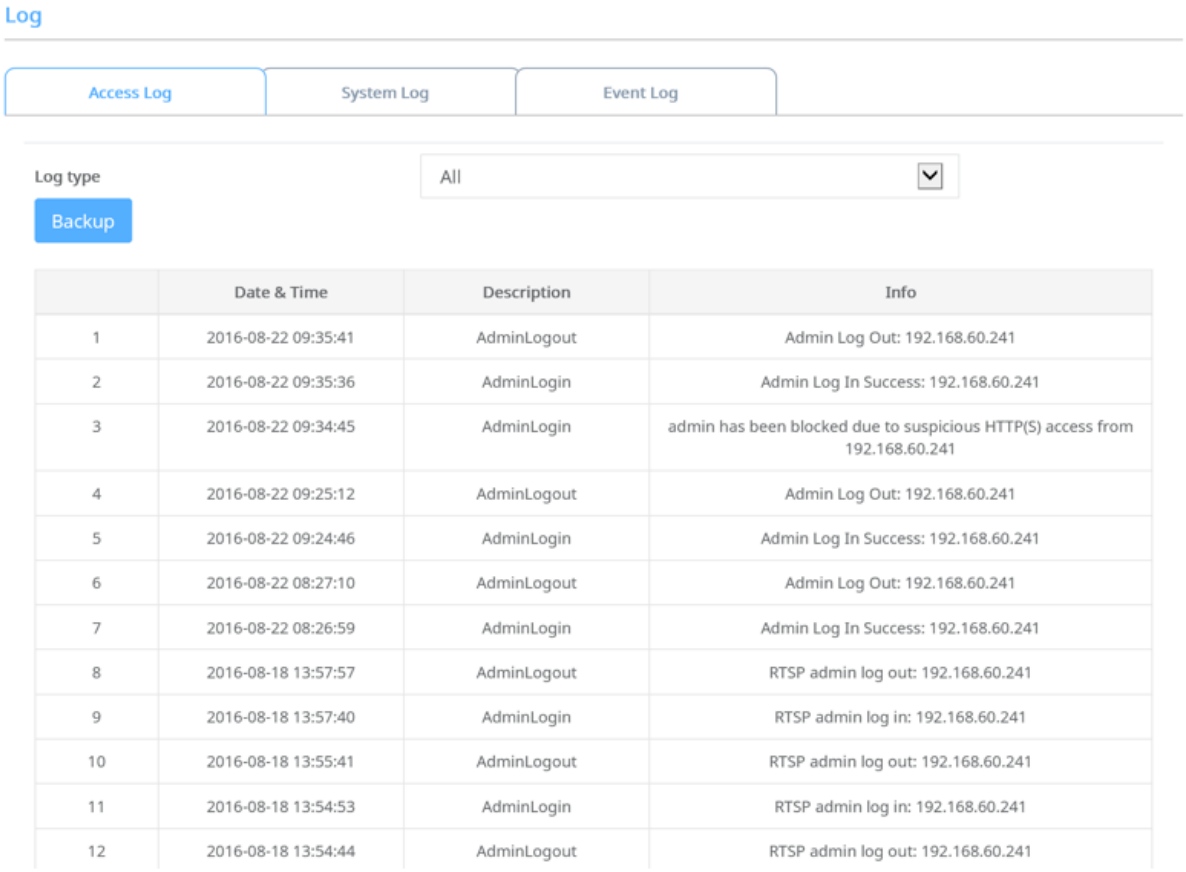


24. ábra[225] SNMP beállítás

Ahogy a bevezetőben említésre került, az egyes működési események valós idejű kezelésén kívül szintén lényeges, hogy egy olyan információs bázisunk legyen, amely hibaelhárítás, hibakeresés, biztonsági események vizsgálata, rendszer vagy biztonsági

[224] What should you know about SNMP and Bosch cameras SNMP support?https://community.boschsecurity.com/t5/Security-Video/What-should-you-know-about-SNMP-and-Bosch-cameras-SNMP-support/ta-p/27034 letöltés ideje: 2023.02.28.
[225] Hikvision: Network Camera Security Guide, January 2018 letöltés ideje: 2022.09.17.

audit, esetleg forenzikus vizsgálat során megfelelő támogatást biztosít számunkra. Ezt a támogatást a biztonságtechnikai eszközök alkalmazásszintű eseménylogolása nyújtja. A ma elérhető legtöbb eszköz rendelkezik saját, lokálisan tárolt logállománnyal, amely tartalmazza az esemény, illetve rendszerlogokat, a rendszerhez történő hozzáférésre vonatkozó információkat, azonban ennek a lokális logbázisnak felügyeleti és vizsgálati szempontból korlátai vannak. Egyrészt, a lokális naplóállományok manuális vizsgálata rendkívül erőforrásigényes tevékenység, a gyakorlatban szinte sehol sem alkalmazzák, másrészt a korlátozott tárhelykapacitás miatt az applikációs és a rendszerlogok rotálásra, felülírásra kerülnek, vagy egyes rendszerműveletek (pl. gyári reset) esetén elveszhetnek.[226] A 18. számú ábra egy kameraeszköz hozzáférési (access) logjait mutatja be.



25. ábra[227] Hozzáférési jogok

Jó gyakorlat, ha a rendszerünkbe olyan biztonságtechnikai és aktív hálózati eszközöket tervezünk, amelyekkel a lokális tároláson kívül a hálózaton keresztüli központi loggyűjtés és felügyelet megvalósítható. Ennek leggyakrabban alkalmazott eszköze a Syslog, amely az informatikai rendszerek naplózásnak egyik elterjedt, szabványos megoldása. Segítségével megoldható az eszközök naplóinak központi, hosszútávú tárolása, felügyelete, elemzése, archiválása, azáltal, hogy szabványos formátumával lehetővé teszi

[226] Egy tervezett, gyári, ún. factory reset esetén mindig mentéseket kell készítenünk a logbázisról, és szükség szerint a konfigurációs adatokról is.
[227] Hanwha Techwin America: Cyber Security White Paper, Securing Video Surveillance Devices to Close Network Vulnerabilities letöltés ideje: 2023.01.12.

az integrációt harmadik féltől származó Syslog szerverekkel. Az SNMP-hez hasonlóan a logok gyűjtését egy központi, ún. kollektor szerver végzi, ezek a gyűjtő és elemző eszközök a gyakorlatban képesek ellátni az előzőekben ismertetett, az SNMP üzenetek feldolgozásához és kezeléséhez szükséges központi menedzsmenti feladatokat is. A Syslog szabvány az információtartalom részletessége tekintetében nyolc súlyossági szintet (severity level) határoz meg, amely a hibaelhárításhoz és kereséshez szükséges, részletes ún. debugging információktól a kizárólag vészhelyzeti (emergency) eseményekig terjed. A felügyeleti igényeknek és a hálózati lehetőségeknek megfelelően egyedileg meghatározható, hogy az eszközök mely súlyossági szintről küldjenek üzeneteket a távoli Syslog szervernek. A Syslog szervereknek a piacon többféle változata elérhető (Nagios, Syslog-NG, SolarWinds stb.), az egyszerű loggyűjtőkön át olyan alkalmazásokig, amelyek a logok gyűjtésén kívül lehetőséget biztosítanak a valós idejű elemzésre, auditálásra, egyes küszöbértékek definiálása után riasztások küldésére stb. Egy igen magas biztonsági szintet képes garantálni az ún. SIEM (Security Information and Event Management) rendszerekbe történő integráció, amely a fent ismertetett funkciókon túl már logkorrelációt (azonos forrásból származó vagy több különböző forrásból származó naplóesemények egymáshoz történő viszonyítása, azok egy biztonsági eseményként történő kezelése, előre beállított szabályok esetén riasztások generálása), illetve széleskörű riportolási lehetőségeket is biztosít. A biztonságtechnikai eszközök esetében is definiálhatók azok a szabályok, amelyek az ún. IoC-k (Indicator of Compromise) felismeréséhez és jelzéséhez szükségesek. Ilyenek lehetnek a teljesség igénye nélkül ez egyes autentikációs események (pl. account lockout, illetve adott időn belüli sikertelen belépési kísérletek magas száma) vagy a rendszerek konfigurációs változására vonatkozó információk. Ezek nem jelentik természetesen automatikusan az eszközök kompromittálását vagy annak kísérletét, azonban az egyes támadások, biztonsági események eszkalációjának megakadályozásához elengedhetetlen, hogy ezekről az információkról a lehető leghamarabb és megbízható módon értesüljünk.

Az SNMP információkhoz hasonlóan a Syslog üzenetek is érzékeny információk, azért azokat szintén titkosítási intézkedésekkel védeni szükséges, amelynek legbiztonságosabb módja, ha a rendszerünk erre lehetőséget ad az előző fejezetekben már tárgyalt TLS fölötti logküldés implementálása.

Az SNMP és a Syslog naplóüzenetek szerverre történő küldéséhez az eszköznek és a kiszolgálónak ugyanazon port/protokoll páros használatával kell kommunikálnia. Mind az SNMP (161, 162) mind a Syslog (514 UDP, 601 TCP, 6514 Syslog over TLS) szabványos, ún. well-known portokat használnak. Az egyes menedzsment protokollokat a hálózati rendszergazdák biztonsági és performancia okokból korlátozni szokták (SNMP, ICMP), ezért némely hálózati implementációkban gondoskodnunk kell róla, hogy a megfelelő ACL-ek, tűzfal szabályok rendelkezésre álljanak az eszközök közti kapcsolat biztosításához. Az egyes rendszerek közti átjárás biztosításán túl meg kell akadályozni, hogy az SNMP és a Syslog csomagok megjelenjenek a hálózat arra illetéktelen részein, különösen, ha azokat valamilyen akceptálható okból kevésbé biztonságos verzióban implementáljuk. További megfontolás, hogy ahol lehetséges, a TCP fölötti üzenetküldést válasszuk, ugyanis UDP használata esetén nincs garancia a csomagok rendeltetésszerű célba jutására.

14.9. Egyéb hálózati biztonsági megfontolások

A fejezetben ezidáig bemutatott hálózati védelmi megoldások mellett számos további lehetőség elérhető, amelyek alkalmazásával biztonságosabbá tehetjük rendszereinket.

A tűzfalak tárgyalásánál láthattuk, hogy az IP szerinti szűrést meg lehet valósítani a hálózati eszközök ACL listáival, de számos biztonságtechnikai eszköz tartalmaz beépített

IP szűrési funkciót, amelynek használata szintén javasolt. Az IP filtering kizárólag az engedélyezett VLAN-okból, adott esetben csak azokról az ismert állomásokról engedélyezzen hozzáférést, ahonnan igazolt kezelői feladatok vannak. Az IP címek mellett egyes eszközökön megbízható MAC-címeket lehet beállítani, amely további korlátozást jelent a hozzáférés tekintetében.
A szigorú biztonságú alkalmazásokban indokolt lehet a biztonságtechnikai hálózatból kifelé menő kommunikációra vonatkozóan is szabályok megállapítása. Ezen hálózatok jellemzője, hogy aránylag nagy pontossággal kiszámítható, milyen felhasználói interakciókra van szükség (pl. menedzsment), milyen szolgáltatásokat szükséges elérni (pl. DNS, NTP stb.), így VLAN szint felett portszinten is lehet korlátozni a kimenő forgalmat, csökkentve ezáltal annak esélyét, hogy belülről egy kompromittált eszköz támadásban (pl. DDoS) vegyen részt, vagy rosszindulatú hálózatfelderítést hajtson végre. Amennyiben megoldható, a publikus internet felé menő kommunikációt tiltani érdemes, bár ebben az esetben bizonyos nehézségekkel is szembesülhetünk az üzemeltetés során, például a gyártói frissítéseket manuálisan kell keresnünk, illetve telepítenünk.
Fentieken túl további restrikciót szükséges alkalmazni az elérhető portok és protokollok tekintetében. A biztonságtechnikai eszközök egyes menedzsment szolgáltatásai különböző portokon érhetőek el, gyártóként egyedi, ám gyártón belül a legtöbbször azonos beállítással (kivéve szabványos, well-known portok). Hálózatfelderítő szoftverek alkalmazásával az egyes portok számából és állapotából azonosíthatók a mögöttük futó szolgáltatások, amelynek segítségével kereshetők az ismert sebezhetőségek, vagy kihasználhatók az adott protokoll gyengeségei. Javasolt kizárólag a szükséges portok engedélyezése, a nem használatos portok tiltása, illetve a szükséges szolgáltatások esetében, amennyiben a vállalati hálózati szabályok ezt megengedik, a default portszámok megváltoztatása, a menedzsment szolgáltatások áthelyezése, továbbá egyes, nem biztonságos protokollok használatának mellőzése. Ilyenre jellemző példa a 23-as porton elérhető TELNET titkosítatlan távoli (parancssori) kommunikációt, ezáltal nem biztonságos bejelentkezést és menedzsmentet lehetővé tevő protokoll helyett a 22-es porton elérhető SSH titkosított csatorna használata, a webes elérést biztosító, 80-as portot használó HTTP helyett a 443-as HTTPS protokoll használata, illetve a manapság népszerű UPnP (Universal Plug and Play) protokoll tiltása. Az UPnP szolgáltatás segítségével az eszközök és a routerek emberi beavatkozás nélkül képesek egyeztetni és engedélyezni azokat a kommunikációs portokat, amelyekre az eszközöknek szüksége lehet a működéshez, adott esetben port-forward lehetőségét megteremteni, és ezáltal engedélyezni az internet felől az eszközhozzáférést. Az utóbbi időszakban több olyan sérülékenység jelent meg, amelyek az UPnP hibás implementációjából, illetve eredetileg is gyenge biztonsági képességéből, vagy magából a működésből adódnak. Javasolt, hogy ilyen szolgáltatás még a privát hálózaton belül se kerüljön használatra.[228]
Teljesítmény és sávszélesség kímélési okokból a megfigyelőhálózatokban gyakori az ún. multicast forgalom bonyolítása. A multicast hálózati forgalom – ellentétben az egyesküldésű, ún. unicast forgalommal, ahol minden megfigyelőállomás számára egyesével küldjük a hálózati csomagokat – lehetővé teszi, hogy az adatcsomagok egyetlen átvitelben elküldhetőek legyenek az arra jogosult node-ok egy csoportjának. Amennyiben multicastot bonyolítunk, biztosítani kell, hogy az összes hálózati eszközünk megfelelően kezelje ezt a fajta forgalmat. A switchek, amelyek nem rendelkeznek a multicast forgalom megfelelő kezeléséhez szükséges tulajdonságokkal (kézi beállítás vagy ún. IGMP

[228] Kocsis Tamás: Hazai kamerák az interneten – Ki figyeli az őrzőket? 2020. https://alverad.hu/wp-content/uploads/2021/08/alverad-ki-figyeli-az-orzoket_-1.pdf letöltés ideje: 2023.01.17.

snooping), azok minden portjukra (kivéve, amelyiken beérkezett) kiküldik a multicast csomagokat, amelyek így illetéktelen állomások számára is megismerhetővé válhatnak. Néhány eszköz beépített módon tartalmaz ARP mérgezés elleni védelmet, amely támadási módszer már régóta ismert, azonban aránylag egyszerűen kivitelezhető, ezért, ahol rendelkezésre áll, javasolt alkalmazni ezt a védelmi funkciót. A fejezet elején tárgyaltak szerint egy IP-hálózaton minden egyes csomópont rendelkezik mind MAC-címmel, mind IP-címmel. Mindkét cím használata szükséges annak érdekében, hogy egy állomás adatokat küldhessen és fogadhasson. Ahhoz, hogy egy a küldő node egy adott Ethernet kapcsolaton megtalálja a cél MAC-címét, az ARP protokollt használja. A protokoll leírása jelen téma tárgyalása szempontjából mellőzhető, azonban azt tudni szükséges, hogy bizonyos esetekben az ARP használata potenciális biztonsági kockázatot jelenthet. Az ARP spoofing (hamisítás) vagy az ARP mérgezés egy-egy olyan technika, amely által a támadó hamis MAC-cím összerendeléseket juttat a hálózatra hamis ARP-kérések segítségével. Ha a támadó meghamisítja egy eszköz MAC-címét, akkor azután a kereteket már nem a megfelelő helyre fogják küldeni.[229] Az ARP védelmi funkció aktiválásával megakadályozható, hogy egy rosszindulatú támadó meghamisítsa pl. a router szerepkörét, és jogosulatlanul ismerje meg ezáltal az eszközök által generált hálózati forgalmat.

[229] Hálózati eszközök programozása, https://irh.inf.unideb.hu/~cisco/cisco/doku.php?id=itn:09._fejezet_-_cimfeloldas letöltés ideje: 2023.01.17.

15. Fizikai biztonság, működésfolytonosság

Az eddigi fejezetekben főként a biztonságtechnikai rendszerekben keletkezett, tárolt adatok, információk védelméhez szükséges tudnivalókat ismertettük, azonban az eszközök az alkalmazási céljuk okán fizikai valójukban (hardveresen) is támadás célpontjává válhatnak. A támadás irányulhat rongálásra, a működőképesség megszakítására, lopásra, a tárolt adatok fizikai hozzáféréssel történő megszerzésére, az eszközök konfigurációjának módosítására stb. A rendszerek nagyfokú önvédelmi képességekkel rendelkeznek ezen támadások ellen, azonban a beépített szabotázs elleni védelem és a megerősített kialakítások nem minden esetben jelentenek elégséges megoldást, az érzékelő és jelző perifériák különösen ki vannak téve a fizikai támadásoknak, míg a központi részegységek (központok, bővítők, szerverek, NVR-ek) rendszertechnikailag jóval védettebb helyszíneken is elhelyezhetők, így az illetéktelen hozzáférés kockázata lényegesen alacsonyabbra csökkenthető.
A működés elvesztésének másik módja nem a szándékos szabotázsban, hanem alapvetően magában a technológiában (meghibásodás), a működtető infrastruktúrában (pl. tápellátás problémái) vagy emberi mulasztásban (hibás tervezés, telepítés) keresendők, az ellenük való védekezés módszereit a fizikai védelemmel együtt jelen fejezetben tárgyaljuk.

15.1. Fizikai kialakítás, elhelyezés és szabotázs elleni védelem

Az egyes perifériás eszközök megerősített, védett fizikai kialakítása mellett szinte minden rendszer esetében építettek be a gyártók olyan metódusokat, amelyek biztosítják, hogy az üzemszerű működés fizikai hozzáféréssel ne legyen szabotálható (vagy arról minden esetben jelzés generálódjon), illetve egyes alapvető funkciók, pl. a beléptető rendszerek azonosítási metódusai ne legyenek megkerülhetők akár az azonosítási technológia másolásával, vagy a beépített intézkedések megkerülésével (anti-passback).
Az illetéktelen hozzáférés, a szándékos károkozás megakadályozásának egyik első lépése, ha a perifériák telepítésére, illetve kialakítására megfelelő figyelmet fordítunk. Az érzékelő és jelző eszközöket a technológiai leírásokban foglalt telepítési magasságok és irányok figyelembevételével lehetőleg úgy kell elhelyezni, hogy segédeszköz nélkül, szabadkézzel ne legyenek elérhetők (megfelelő magasság, süllyesztett szerelés), vagy a megerősített kialakítás biztosítsa az eszköz rongálás elleni védelmét. Nagy biztonságú alkalmazásokban védett téren belüli (ha szükséges, rejtett) elhelyezéssel, kamerák esetében a látószög átlapolásával vagy eszközredundanciával (egy kritikus területet, eszközt, vagy folyamatot több kamera is figyel, behatolásjelző rendszer esetében hang és/vagy fényjelző berendezések különböző falsíkokra történő szerelésével) is csökkenthetjük a rosszindulatú hozzáférések kockázatait. A rendszerek kábelezését az illetéktelen fizikai hozzáférést gátló módon védőcsőben, kábeltálcán vagy műanyag csatornában szereléssel valósítsuk meg, amennyiben a jelvonalakat saját területen kívül vezetjük, érdemes komolyabb mechanikai védelemről, pl. fém védőcsőben történő szerelésről gondoskodni.
Kameraperifériák esetén a fizikai védelmet megerősített szilárdságú házakkal, burkolatokkal, illetve a hálózati csatlakozási pontok fizikai védelmével biztosíthatjuk, hogy megbontás nélkül a csatlakozás ne legyen hozzáférhető. Ezt a funkciót egyes gyártók tampervédett csavarozással is kiegészítik. Egy gyakran alulértékelt, de igen fontos kérdés a fizikai védelem szempontjából, hogy az eszközök feleljenek meg a működési környezet tulajdonságainak, különös tekintettel a hőmérsékleti, időjárási és az elektromágneses környezettel szemben támasztott műszaki követelményeknek (IP védettség, túlfeszültség védelem, elektromágneses kompatibilitás, árnyékolási követelmények).

A vezérlő, illetve központi részegységek elhelyezésénél jó gyakorlat, ha azokat érzékelőkkel védett térben helyezzük el. Kameraszerverek, beléptető rendszerek szervereit lehetőség szerint informatikai gépterembe telepítsük. Az informatikai géptermek nagy része ugyanis megfelelő fizikai biztonsági intézkedésekkel védett, és rendelkezik a működésfolytonosságot biztosító technológiai megoldásokkal (szünetmentes tápellátás, hűtési megoldások stb.). Szervertermen belül is indokolt az elkülönített elhelyezés, ahol lehetséges, különálló rackszekrény alkalmazásával, hogy a védett téren belül is kizárólag a szükséges mértékben és személyeknek biztosítsunk felügyelhető hozzáférést. Kritikusabb esetben a rackszekrényt el lehet látni nyitás és üvegtörés érzékelővel, ebben az esetben az eszközöket behatolásjelző rendszeren külön partícióba szükséges szervezni és a partíciókódot csak a kezelésre jogosultakkal megismertetni. A folyamatos személyes felügyeletet igénylő alkalmazásokban (tűzjelző és oltórendszerek központjai), a felügyelet nélküli időszakokra a helyiség zárásáról és/vagy valamilyen illetéktelen kezelést kizáró megoldásról, pl. kulcsos kapcsolóról gondoskodni szükséges.

A biztonságtechnikai rendszerek részegységei szabotázsvédelmi lehetőségekkel vannak ellátva az illetéktelen hozzáférés (nyitás) illetve rongálás ellen. A behatolásjelző és beléptető rendszer központi részegységeit, bővítőmoduljait, tápegységeit javasolt szabotázskapcsolóval ellátott fémdobozba (a műanyag dobozok nem biztosítanak kellő szintű védelmet, használatukat kerülni kell) elhelyezni. A behatolásjelző rendszer jelvonalait tampervédett módon, vonalvéglezáró ellenállások alkalmazásával (érzékelőbe épített vagy utólag szerelt) szükséges telepíteni. A kettős lezárású hurok, az ún. DEoL (Double End of Line) megoldás biztosítja, hogy a központ megkülönböztesse az egyes perifériás események során a riasztás, szabotázs vagy hibajelzéseket (szakadás vagy rövidzár). A rendszerek olvasói, kódbeviteli perifériái (kezelői) illetve a jelző perifériák (nyitásérzékelő, passzív infra) szintén szerelhetők szabotázsvédelemmel, mind megbontás (fedélnyitás) mind eltávolítás esetére.

A passzív infravörös mozgásérzékelők hatástalanításának egyik módja, ha letakarják, vagy lefestik. Ezen szabotálási kísérletek esetén a kitakarás elleni védelem alkalmazása lehet megoldás, ahol a védett mozgásérzékelőkben egy aktív infravörös adó által kibocsátott fény a vevőbe visszaverődik, így az érzékelő jelzést generál. A felületi nyitásérzékelésre leggyakrabban alkalmazott, ún. Reed-relés érzékelő egyik szabotálási módja, hogy a jelfogók érintkezőinek pozícióját külső mágnessel befolyásolják. Léteznek a piacon olyan Reed-relés nyitásérzékelők, amelyek több, egymáshoz képest elforgatott jelfogót és az ellendarabban ezek helyzetének megfelelően polarizált mágneseket tartalmaznak, így külső mágnessel történő szabotálásuk gyakorlatilag lehetetlen.[230] A behatolásjelző rendszereken a szabotázsvédelmet ún. 24 órás felügyelt zónaként szükséges programozni, amely azt jelenti, hogy a védelem akkor is aktív, amikor a behatolásjelző élesítetlen állapotban van.

A passzív infra mozgásérzékelőknél már ismertetett, kitakarásos szabotálási mód a kameraperiféria esetén is megvalósítható, kiegészítve azzal, hogy a kamerákat pozíciójukból elforgatva, vagy az objektívet szándékosan elállítva, ezáltal fókuszvesztést okozva is lehetséges az eszköz támadása. A korszerű eszközök biztosítanak a leírt manipulációk esetére megfelelő detektációs és riasztási megoldásokat.

Az eszközök szabotázsvédelme tekintetében speciálisak a rádiós megoldások, így néhány szóban érdemes külön foglalkozni velük. A vezeték nélküli behatolásjelző rendszerek

[230] Tóth Attila – Tóth Levente: Biztonságtechnika. Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar, Budapest, 2014. ISBN 978-615-5305-56-6

(rádiós rendszerek) esetében nemcsak a jelvezetékek, hanem a tápkábelek is hiányoznak a kiépítésből, ezért a rendszer egyes elemeinek kihelyezett (lokális) tápellátását biztosítani kell. Ez általában kis méretű és súlyú telepek segítségével történik. Az ilyen tápellátás felügyelete nem valósítható meg a vezetékezett rendszerekéhez hasonlóan, valamint nincs mód másodlagos tápellátás használatára. Ennek a problémának az enyhítésére szolgál, hogy a rádiós eszközök telepeik kimerülését valamilyen módon jelzik a központ és ezáltal a felhasználó felé. A vezetékezés hiánya miatt a fedélbontással történő szabotálásra sincsen szüksége a támadónak, elegendő, ha az eszközt pozíciójából eltávolítják, elforgatják, így esetükben a felfogatási felületről való eltávolításra irányuló cselekményeket is jelezni és felügyelni szükséges.[231] A kábelezés hiánya miatt a jelzésátviteli utak biztonsága is gyengébb, a rádiós eszközök esetében gyakori támadási mód a rádiófrekvenciás zavarás. Kereskedelmi forgalomban viszonylag egyszerűen vásárolhatók olyan széles spektrumú zavarók, ún. jammerek, amelyek a leggyakrabban használt frekvenciákon (beleértve a GSM és a WiFi frekvenciákat is) képesek interferenciákat okozni, csökkentve ezáltal a jelzésétvitel hatékonyságát vagy teljesen megszüntetni azt. Ennek kiküszöbölésére, a szabotázs detektálására az eszközök egy jelentős része periodikus jelzéseket ún. heartbeat signal-t használ, amely segítségével a periféria előre beállított gyakorisággal jelzi a rendszer felé, hogy él a kapcsolat, a központ ezen jelzések elmaradása esetén pedig riasztást generál. Egyes fejlettebb megoldások az eszközvesztés előtt képesek a rádiófrekvenciás interferencia észlelésére, jelzésére.
A másik jelentős megoldandó kérdés az eszközök tekintetében a jelzésátviteli utak redundanciája. A szabotázsvédelem mellett erre azért is szükség van, mert a redundancia nélküli kommunikációs csatornával kialakított rádiós rendszerek műszakilag is megbízhatatlanok (térerő problémák, adatkeret kimerülés stb.). Jó gyakorlat lehet, ha a biztonságtechnikai rendszereink felügyeletére, rádiós vagy vezetékes kialakítástól függetlenül (Ethernet vagy biztonságtechnikai kábel is szabotálható) redundáns távoli jelzésátviteli megoldásokat alkalmazunk. A több, lehetőleg különböző fizikai közeget (rádiós és vezetékes) használó kommunikációs csatorna nagyobb biztonsággal képes értesíteni a felügyeletet a riasztás vagy hibajelzésekről. A távoli rendszerjelzések mellett nem szabad megfeledkeznünk a lokális riasztásjelzések fontosságáról sem. A behatolásjelző rendszerek esetében helyi hang és fényjelző biztosítása szükséges, míg a beléptető rendszerek tekintetében legalább a kényszerített (illetéktelen), nyitást, az időn túli nyitvatartást hangjelző (leggyakrabban az olvasókba integrált zümmer) jelezze.

15.2. Működésfolytonosság biztosítása

A biztonságtechnikai rendszerek esetében funkcióvesztés nem kizárólag kívülről érkező szándékos fizikai behatások (szabotázs, rongálás) eredményeképpen állhat elő, a biztonságos üzemeltetéshez szükséges számolnunk a meghibásodásból eredő működési problémákkal, és e tekintetben is biztosítanunk kell a megfelelő mértékű ellenálló képességet (rezílienciát). Ez a gyakorlatban főként azt jelenti, hogy a rendszereinknek mind hardveresen, mind szoftveresen, mind az energiaellátó rendszerekre vonatkozóan annyi redundanciát kell tartalmazniuk, melyet a működési környezet és az alkalmazási cél rendelkezésre állás szempontjából megkövetel. A szabványos üzletmenet-folytonossági eljárásokban a BIA (Business Impact Analysis, üzleti hatáselemzés) alapján szükséges meghatározni a rendszereink kritikusságát, elvesztésük esetén bekövetkező kármérték alapján a szükséges rendelkezésre állási mértéket jellemző mutatókat. Az egyik legfontosabb mutató ezen tekintetben az MTD, a Maximum Tolerable Downtime, amely

[231] Tóth Attila – Tóth Levente: Biztonságtechnika. Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar, Budapest, 2014. ISBN 978-615-5305-56-6

azt az időszakot jelöli, amelyen belül a rendszereink elvesztése még nem okoz kárt a vállalatnak. Az RTO (Recovery Time Objective) és az RPO (Recovery Point Objective) a rendszerek elvárt visszaállítási idejére és az adatvesztési toleranciára vonatkozó célértékeket jelöli. Az RTO alacsony értéke szélsőséges esetben a rendszerarchitektúra kialakítása tekintetében akár különböző geolokációkon kialakított failover konfigurációs, míg az extrém alacsony idejű RPO – amely közvetve meghatározza az adatmentési gyakoriságot – akár folyamatos, tranzakciószintű mentéseket is jelenthet. A rendszerek elvárt hibatűrési szintjét számos megoldással lehet fokozni, amelyből a biztonságtechnikai gyakorlatban jópárat alkalmazunk is.

A tápellátás folyamatossága tekintetében a tűzjelzők, oltó, behatolásjelző és beléptető rendszerek központi részegységei (és rajtuk keresztül az érzékelő perifériák is) alapvetően rendelkeznek saját szünetmentes megoldással (akkumulátor) amelynek az áthidalási kapacitását az elvárt működésfolytonossági követelmények (tűzjelző és oltórendszerek esetén jogszabályi előírások) figyelembe vételével szükséges megválasztani, de jó gyakorlat lehet, ha legalább 12-24 óra, nyugalmi állapotú folyamatos működést biztosítunk a rendszerelemek számára az elsődleges hálózati tápforrás kiesése esetén. A szünetmentesítési eljárások az elektronikus megfigyelőrendszerek esetében már bonyolultabb megoldásokat és alaposabb megfontolásokat igényelnek, azonban bármelyik mellett is döntünk, a legfontosabb, hogy minden szükséges rendszerelem (rögzítő, aktív hálózati eszközök, kamerák, megfigyelő számítógépek stb.) tartalék tápellátásáról gondoskodjunk. Gyakori, és az egyik legjobban alkalmazható megoldás, hogy a kamerák központi tápellátását Ethernet hálózaton keresztül PoE (Power-Over-Ethernet) képes hálózati rögzítő vagy switch (önállóan vagy külső tápfeladóval) biztosítja, a központi eszközöket lokális vagy hálózati UPS berendezéssel (nagyobb áthidalási igény esetén aggregátorjogos hálózatról) támogatjuk. Nagyobb rendszerek és/vagy kritikusabb alkalmazások esetén javasolt a rögzítés és a tápellátás szétválasztása, mert előfordulhat, hogy a hálózati rögzítő Ethernet port hibája csak a rögzítési megoldás időszakos kiesésével orvosolható.

Hardveres és szoftveres meghibásodás esetére a rendszerekben alkalmazott, szerverszolgáltatásokat (kritikus esetben a kliensek is) megvalósító informatikai hardverelemek feleljenek meg a funkcióhoz rendelt rendelkezésre állási követelményeknek (pl. redundáns tápegységek alkalmazása). Az adatbiztonságot tárolási oldalról az alkalmazott merevlemezek ún. RAID tömbbe történő szervezésével (Redundant Array of Inexpensive Disks vagy Redundant Array of Independent Disks) biztosíthatjuk. A RAID megoldás célja, hogy az egyébként függetlenül működő merevlemezek egy logikai egységbe szervezésével, tükrözés vagy redundancia hozzáadása révén meghibásodás esetén is (üzem közben cserélhető, ún. hot swap megoldással leállás nélkül) megőrizze a tárolt adatok egységét.[232] Az alacsony RTO-val rendelkező alkalmazások esetén szükség lehet rá, hogy a központi rendszerek (pl. alkalmazási és/vagy adatbázis szerverek) georedundáns módon, földrajzilag is elkülönült telepítéssel, failover módban támogassák a magas rendelkezésre állási követelményeket, a folyamatos működést.

Az egyes funkciók megőrzését a hardveres és a szoftveres redundancia mellett megfelelő architektúratervezéssel is biztosíthatjuk, így az adatbiztonság tekintetében többek közt

[232] A RAID tekintetében több szintet definiáltak (pl. RAID 1,5, 6,10), amely mindegyik egy önálló megoldást jelent, különböző működési logikával, saját előnyökkel és hátrányokkal, köztük olyannal, amelyet kétszeres lemezmeghibásodás áthidalására terveztek, azonban ezek részletes ismertetése meghaladja jelen tankönyv tartalmi lehetőségeit.

elosztott tárolási, adatkezelési megoldásokat alkalmazhatunk. A beléptető rendszerek a legtöbb kialakításban lokálisan, vezérlő moduljaikba szerelt memória segítségével képesek biztosítani a működést a kommunikációs szerverrel való kapcsolat kiesése esetére is a már felvitt jogosultságok és a lokális eseményadatok tárolása tekintetében. Kamerafelvételek rendelkezésre állását lokális SD kártyára rögzítéssel is támogathatjuk, amely áthidalást jelenthet a központi rögzítés vagy a hálózati kapcsolat meghibásodása esetére. A rögzítés megvalósulhat közvetlenül nagy rendelkezésre állást biztosító, külső felhőszolgáltatás igénybevételével is, azonban minden esetben gondolnunk kell az alkalmazott megoldás hátrányaira is. A lokális, eszközszintű rögzítés esetén a kamerák eltulajdonításával a felvételek is elveszthetnek, illetve a felhő alapú tárolás további információbiztonsági, illetve személyes adatvédelmi, GDPR kérdéseket is felvethet, gondoskodnunk kell továbbá igen stabil, internetelérést biztosító hálózati kapcsolatról.
Azokban az esetekben, ahol a működés folyamatossága alapkövetelmény és/vagy korlátozott ráhatásunk van a rendszerarchitektúra kialakítása és így az egyszeres meghibásodási pontok (Single Point of Failure, SPOF) elkerülésére (pl. ügyviteli hálózati integráció esetén, ahol az aktív hálózati eszközök menedzsmentje kívül esik a vállalatbiztonság hatókörén), azonos jelzési feladatot vagy riasztási, megfigyelési területet lefedő eszközök redundáns telepítésében is gondolkodhatunk. Ezen koncepció keretében egy kritikus biztonságú látóteret több kamerával is lefedhetünk (ebben az esetben, ha lehetőség van rá, javasolt az átviteli utakat is minél jobban elszeparálni, minimálisan a kamerákat eltérő hálózati switchekhez csatlakoztatni), vagy behatolásjelző rendszer esetén külön buszvonali bővítőket alkalmazva több, azonos funkciójú érzékelőt is felszerelhetünk. A működésfolytonosságot támogató rendszerarchitektúra mellett az üzemeltetési eljárásainkat is gondosan kell terveznünk, ugyanis egyes szükséges feladatok is problémákat okozhatnak a folyamatos működés tekintetében. Az eszköz leállásával járó karbantartási műveleteket (szoftver vagy firmware upgrade) például olyan időszakokra szükséges tervezni kiegészítő védelmi intézkedések mellett, amikor a rendszer részleges vagy teljes funkcionális kiesése nem okoz elfogadhatatlan biztonsági kockázatot.
A nagy rendelkezésre állást biztosító műszaki és tervezési megoldásokon túl szükség van rá, hogy a bizonságtechnikai rendszereink tekintetében megfelelő mentési és visszaállítási eljárásokat is alkalmazzunk. Ennek keretén belül a mentési megoldás biztosítsa a rendszerekben kezelt összes beállítás és adat (konfigurációs adatok, naplók, felhasználói, kezelői és jogosultsági információk, képek stb.) mentését, és a rendszer mentésből történő visszaállíthatóságát. A mentések módját és gyakoriságát a rendszerek működése, és a bennük keletkezett adatok sűrűsége, kritikussága, a személyes adatok tárolási biztonságára, rendelkezésre állására vonatkozó jogi és szervezeti szabályok, illetve az adatvesztési tolerancia (RPO) alapján kell meghatározni. Fontos szempont a mentési megoldásnál, hogy kellő számú mentési példányt biztosítson, amelyek közül javasolt egy példányt a forrásrendszerektől elkülönített földrajzi lokáción tárolni. A rendszereknek írott mentési szabályokkal kell rendelkezni, amelyekben a mentési mód és gyakoriság feladatai és felelősségei mellett meg kell határozni a mentésre alkalmazott átviteli utak (data on the fly) és tárolt mentési állományok (data at rest) védelmének követelményeit, azokat a forrásrendszerével azonos biztonsági szint mellett kell megvalósítani. Amennyiben arra lehetőség van, a mentési adatokat időnként ellenőrizni, a visszaállítási eljárásokat pedig tesztelni szükséges. A mentéseket rendszertől függően manuálisan és automatizált módon is el lehet végezni, azonban szükséges, hogy a mentések megfelelő időközönkénti megvalósítását, az automatikus lefutás helyességét minden esetben ellenőrizzük, azokról meggyőződjünk. Homogén technológiai és biztonsági környezetben elképzelhető, hogy az előzetesen jóváhagyott és mentett konfigurációs állományokat

templateként is fel tudjuk használni, biztosítva a (biztonsági) beállítások egyenszilárdságát és az új telepítések megkönnyítését.
Lényeges, hogy a biztonságtechnikai rendszereken kívül gondoskodjunk a rendszerek hálózati kapcsolatait biztosító aktív eszközök konfigurációinak mentéséről is, különös figyelemmel arra az esetre, amikor azok nem az ügyviteli hálózattól elkülönített rendszert alkotnak. Amennyiben fizikailag, vagy logikailag a hálózati eszközök a vállalati ügyviteli rendszer részei, és adott esetben külső menedzsment (pl. informatikai részleg) felügyelete alá tartoznak, minden esetben vegyük figyelembe, hogy egyes hálózati eszközök a konfigurációs beállításokat titkosítatlan formában, ún. cleartext-ben, olvasható szöveges állományként mentik (pl. FTP szerverre), így a mentési mechanizmusnál a biztonságos kommunikációs csatorna meglétét, a mentések biztonságos tárolását és külső hozzáférhetőségét minden esetben ellenőrizzük, ugyanis azok nagyban befolyásolhatják a rendszereink bizalmasságát.
Egyes alkalmazásokban elfordulhatnak olyan esetek, amikor maguk a biztonságtechnikai rendszerek okozhatnak nagy biztonságú rendszerek működésfolytonosságában, használatában problémákat, vagy okoznak biztonsági szempontból többletkockázatokat, ezeket minden esetben szükséges elkerülnünk. Amennyiben a vonatkozó működésfolytonossági követelmények alapján nagy értékű, és/vagy koncentráltan elhelyezett információfeldolgozó eszközök helyiségébe (adatközpont, szerverterem) automatikus oltórendszer is telepítésre kerül, azt úgy szükséges megválasztani, hogy a technológia ne jelentsen járulékos kockázatot az informatikai eszközök és a munkát végző kollégák számára. Nem javasolt az ún. nagynyomású vízködös oltórendszer, valamint az aeroszolos, illetve egyéb visszamaradó anyaggal oltó rendszer használata.[233]
A gázzal oltó rendszereket, azok közül is az egészségre nem ártalmas megoldások alkalmazását (pl. INERGEN) érdemes előnyben részesíteni, amellyel az egészségkárosító kockázatok elkerülése mellett lehetőség adódik a helyiségekben az elsődleges emberi beavatkozások haladéktalan elvégzésére,[234] továbbá nem igényli az oltás előtt a védett technológia áramtalanítását. Az oltórendszer elemeit úgy kell elhelyezni, hogy az biztosítsa a technológia leállítása, mozgatása nélkül a hozzáférést, karbantarthatóságot, az időszakosan szükségessé váló cseréket. A téves jelzések és az oltások szintén problémát okozhatnak a rendszerek működésében, így a helyiségekben javasolt valamely hatékony jelzésverifikáció megoldás megvalósítása, például nagy érzékenységű aspirációs tűzjelző érzékelő telepítése, amely pontszerű füstérzékelőkkel kiegészülve kettős jelzésfüggést alkalmaz a téves beavatkozás, és oltások elkerülése érdekében. A szerverek szükségtelen leállítását elkerülve javasolt, hogy a helyiség villamos szempontból az épület központi hálózatától különálló módon legyen lekapcsolható, ezt azonban a vonatkozó jogszabály alapján szakhatósági egyeztetésnek szükséges megelőzni. A helyiségek technológiai hűtését a károk minimalizálása érdekében javasolt tűzjelző oldali vezérléssel jelzés esetén lekapcsolni, azonban gondoskodni kell róla, hogy jelzéstörlés után a berendezés automatikus úton újra induljon.
A használatot esetlegesen akadályozó, nehezítő, vagy járulékos kockázatokat okozó lehetőségeket egyéb eszközök tekintetében is végig kell gondolni. A beléptető rendszereknél, különösen a biometrikus (vagy bizonyos kockázati szint fölött a

[233] BME Informatikai Központ: Tervezés az IT biztonság szempontjából, Miniszterelnöki Hivatal, 2008, p. 36.

[234] A megoldás alkalmazása során meg kell valósítani a kapcsolódó építészeti követelményeket, így pl. a nyomáslevezető zsalu kiépítését, vagy a tartási időnek megfelelő integritású épületszerkezetek biztosítását.

többfaktoros) azonosítást alkalmazó megoldások esetében igen fontos figyelembe venni e tekintetben a megbízható működés két lényeges mérőszámát, a FAR-t (False Acceptance Rate, téves elfogadási arány) és az FRR-t (False Rejection Rate, téves elutasítási arány).[235] A biztonság szempontjából kritikus helyiségekben alapvető, hogy elkerüljük a jogosulatlan hozzáférést, ezért cél a téves elfogadás minél alacsonyabbra történő csökkentése. Minél pontosabb azonosítást követelünk meg azonban egy azonosítótól, annál többször fordulhat elő, hogy nem ismeri fel a belépésre jogosultat a rendszer. Míg a legtöbb szakember számára nyilvánvaló, hogy a téves elfogadás komoly biztonsági kockázatot rejt magában, azonban a téves elutasítás kockázatai már nem ennyire egyértelműek. A gyakori téves elutasítás ugyanis a felhasználókat arra sarkalhatja, hogy megkerüljék a számukra kényelmetlen védelmi megoldásokat, ezért a tervezés során meg kell találni azt az egyensúlyi állapotot, ahol még elfogadható mértékű a FAR és az FRR, amely pontot EER-nek (Equal Error Rate), egyenlő hibaaránynak nevezünk, vagy más, kiegészítő intézkedésekkel szükséges biztosítani, hogy a felhasználó ne legyen képes az alkalmazott kontroll megkerülésére.[236] A beléptető rendszerek tekintetében érdemes megismerkedni még a fail safe és a fail secure üzemmódok jelentésével. Fail safe az áthaladást szabályozó eszköz működése, ha meghibásodás, vagy a normáltól eltérő, ún. vészeseti működés során az életvédelmi szempontokat helyezi előtérbe.[237] Fail secure üzemmódban az eszköz reteszel, biztosítva ezzel a vagyonvédelmi követelmények érvényesülését. Az egyes rendszerek működését jogszabályi előírások alapján kötelezően fail safe módban tervezzük, a kiürítés biztosítására vonatkozó szabályok előírják ugyanis a menekülési útvonalak akadálytalan használhatóságát.[238] Ezen két üzemmód alkalmazása minden esetben egyedi, alapos megfontolásokat és gondos tervezést kíván, hogy sem a védett térhez történő illetéktelen hozzáférés, sem a létesítményben tartózkodó személyek egészségének szempontjából ne jelentsen többletkockázatot.[239]

Az áthaladást biztosító rendszerelemekkel történő együttműködés során a beléptető rendszer mechanikai kialakítás és kapacitás tekintetében is biztosítsa a tervezett áthaladási sűrűséghez szükséges működési sebességet, továbbá támogassa az egyes esetekben szükséges különleges áthaladási formákat, pl. mozgáskorlátozott személyek esetén. A biztonságtechnikai rendszerek telepítése során be kell tartani a már említett menekülési utak akadálytalan használatának biztosításán túl az egyéb, különösen az Országos Tűzvédelmi Szabályzatban előírt tűzvédelmi követelményeket, így a teljesség igénye nélkül az egyes helyiségeken átvezetett villamos vagy gépészeti vezetékrendszerek, technológiák átvezetési helyein, a vezeték és az építményszerkezet

[235] A téves elfogadási arány megmutatja, hogy az azonosítás milyen arányban ismert fel jogosulatlan felhasználót jogosultként, míg a téves elutasítási arány megmutatja, hogy az azonosítás milyen arányban utasít el jogosult felhasználót. (Bunyitai Ákos: A ma és a holnap beléptető rendszereinek automatikus személyazonosító eljárásai biztonságtechnikai szempontból, Hadmérnök, VI. évfolyam 1. szám, p. 22-35., ISSN 1788-1929).

[236] Tóth Attila: Tűzjelző rendszerek, beléptető rendszerek, in: Christián László–Major László–Szabó Csaba (szerk.): Biztonsági vezetői kézikönyv. Budapest, Dialóg Campus, 2019

[237] Erre példa, ha tápkimaradás esetén (amely lehet műszaki okból, vagy a tűzjelző rendszer vezérlő jelének hatására) az eszköz állapota nyitottá, átjárhatóvá válik. (Bunyitai Ákos: A ma és a holnap beléptető rendszereinek automatikus személyazonosító eljárásai biztonságtechnikai szempontból, Hadmérnök, VI. évfolyam 1. szám, p. 22-35., ISSN 1788-1929).

[238] Bunyitai Ákos: A ma és a holnap beléptető rendszereinek automatikus személyazonosító eljárásai biztonságtechnikai szempontból, Hadmérnök, VI. évfolyam 1. szám, p. 22-35., ISSN 1788-1929

[239] Dr. Tiszolczi Balázs Gergely: Fizikai biztonsági kontrollok tervezésének és alkalmazásának gyakorlata az ISO/IEC 27001 szabvány elvárásainak tükrében. Magyar Rendészet, 2019/2-3. szám. p. 233—249.

közötti résben, nyílásban a tűz átterjedését az átvezetéssel érintett építményszerkezetre előírt tűzállóságiteljesítmény-követelmény időtartamáig meg kell gátolni. Amennyiben egy biztonságtechnikai rendszer elemeit tűzgátló nyílászáróra szükséges szerelni, az legyen előkészítve a rendszerelemek fogadására, a tűzgátló szerkezetek utólagos megbontása a védelmi képesség esetleges sérülése miatt nem megengedett.

16. Adminisztratív eljárások

Az előző fejezetekben bemutatott technológiai védelmi intézkedések alkalmazása nélkülözhetetlen a biztonságtechnikai rendszerek üzemeltetése során, azonban önmagukban a megfelelő beállítások, konfigurációk és titkosítási mechanizmusok nem képesek azok teljeskörű biztonságának garantálására. A fizikai és logikai védelem nem működőképes, ha a felhasználók nem követik a bevált információbiztonsági gyakorlatokat, eljárásokat.

16.1. Felhasználó menedzsment, jogosultságkezelés

Az információbiztonságban alapvetés, hogy a megfelelő hozzáférés-szabályozás és felhasználói menedzsment olyan eljárásrend, amely alkalmazása nélkül szinte lehetetlen biztosítani adataink, információs rendszereink védelmét. Nincs ez másként a biztonságtechnikai eszközök esetében sem, ezért lényeges, hogy a rendszerek implementációjáért, üzemeltetéséért felelős szakemberek tisztában legyenek a legalapvetőbb hozzáférési keretekkel, a legszükségesebb ismeret és a legszükségesebb feladatvégrehajtás („need to know” és „need to do”) elveivel, és azokat a gyakorlatban is alkalmazni legyenek képesek. A megfelelő hozzáférések beállítása mellett ugyanilyen fontos még a különböző jogosultságok biztonságos igénylési rendjének kialakítása, azok rendszeres felülvizsgálata, szükség esetén visszavonása.

Általánosságban elmondható, hogy a technikai rendszerekhez történő logikai hozzáférésnek (belépéseknek), a privilegizált, emelt szintű jogosultságokkal rendelkező felhasználói azonosítók kialakításának, kezelésének is megvannak a rendszerekbe implementált, általános, és egyes esetekben egyedi, sajátos szabályai, azonban az alkalmazás módjait és mértékét nagyban determinálja a fizikai és logikai infrastruktúra, illetve a működési környezet speciális szervezeti szabályai. Az alkalmazott hozzáférési rendet így gondos tervezés kell, hogy megelőzze, annak érdekében, hogy az adminisztrátorok és a felhasználók egyedi jogainak és jogcsoportjainak kiosztása, a szükséges legkisebb ismeret elvének betartása, a hozzáférések (funkció, idő és terület szerinti) kialakítása, testre szabhatósága illeszkedjen az adott infrastruktúrához, a szervezet működési, munkavégzési sajátosságaihoz. A tervezés és a hozzáférési rend implementálása után pedig a szükséges eljárásokkal folyamatosan biztosítanunk kell, hogy a rendszer menedzseléséhez és kezeléséhez alkalmazott szoftverek és fizikai kezelőelemek minden kezelési ponton kizárólag az arra jogosultak számára biztosítsanak hozzáférést, továbbá kizárólag a felhasználó számára ténylegesen szükséges beállítások elvégzését és funkciók használatát engedélyezzék, a kezelési feladatok minden esetben biztonságos autentikációs és autorizációs metódusok alapján legyenek végrehajtva.

Az említett autentikációs folyamat célja annak eldöntése, hogy az egyes rendszerekhez hozzáférési jogosultságot kérő entitás (humán vagy gépi) valóban az, akinek ő mondja magát. Ettől elkülöníthető folyamatlépés az autorizáció, amikor is a validált személyazonosság alapján annak vizsgálata történik, hogy a felhasználó számára mely adatok elérése és rendszerfunkciók használata engedélyezett, azokon milyen jellegű műveleteket végezhet. A biztonságtechnikai szerverek és kliensek tekintetében az autentikáció során alapvetően a mai napig felhasználónév és a hozzá tartozó jelszó (számkód) párosa alkalmazott, így kiemelten ezek használatával foglalkozunk. Az autorizációs mechanizmus tekintetében többféle generális modellt ismerünk, a biztonságtechnikai rendszerekben legtöbbször az egyes felhasználók kezelési joga műveleti szintre lebontva, az ún. role-based, szerepköri hozzáférési modellben kerül implementálásra. (RBAC, Role-based Access Control). A modell rövid lényege, hogy alkalmazása az egyes általános vagy kiemelt jogú felhasználók számára a szervezetben

betöltött szerepkörüknek megfelelő kezelési jogosultságot és annak megfelelő információs hozzáférést biztosít. Az egyes funkciók és adatok (objektumok) eléréséhez szükséges jogosultságok nem az egyedi felhasználóhoz, hanem a definiált szerepkörökhöz kapcsoltak és a modellben egy felhasználó több szerepkört is betölthet.
A rendszerek telepítése és üzemeltetése során mind az autentikációra, mind az autorizációra szigorú alkalmazási szabályokat javasolt meghatározni. Az autentikáció tekintetében a jelszóházirend minden esetben feleljen meg a szervezetben alkalmazott informatikai biztonsági szabályoknak (hosszra, összetettségre, lejárati időre, jelszócserére vonatkozó szabályok). A technológia mai fejlettségi szintjét tekintve javasolt legalább 12 karakter hosszúságú jelszót választani, amely tartalmaz kis- és nagybetűket, számot, továbbá speciális karaktert. Az egyes felhasználóknak hozzáférési szinttől függetlenül egyedi azonosítókkal szükséges rendelkezni, a közös azonosítók, illetve különböző eszközökön, alkalmazásokban ugyanazon azonosítók használatát kerüljük. Ezen generális szabályok mellett az alábbi követelményekre fordítsunk figyelmet:

- az üzembe helyezés során minden esetben vonjuk vissza a gyári, ún. default azonosítókat, korlátozzuk a default adminisztrátori felhasználókat;
- lehetőség szerint legalább az adminisztrátori jogosultsággal rendelkező személyek esetén alkalmazzunk multifaktoros (többtényezős) autentikációt;
- a menedzsment felületeken legyen implementálva valamilyen fajta csillapítás a brute force alapú, jelszavak elleni támadások kivédésére, engedélyezzük az ún. lockout funkciókat (pl. IP címek és/vagy az érintett felhasználók blokkolása az előre megadott számú, adott időtartamon belül megvalósuló sikertelen bejelentkezési próbálkozások esetén).

Ezidáig az egyszerűsítés okán nem került említésre, azonban fontos legalább részben tárgyalni, hogy az autentikációs folyamat során a hozzáférést igénylő entitás a felhasználónév/jelszó pároson kívül más adatot (pl. tanúsítványt) is szolgáltathat személyazonosságának eldöntéséhez, illetve arról dönthet maga a biztonságtechnikai alkalmazás, vagy valamilyen külső, központosított, vállalati hozzáférési menedzsmentet megvalósító szolgáltatás (LDAP, IAM), amelyekhez az egyes, erre felkészített biztonságtechnikai rendszerek is csatlakozhatnak (pl. Active Directory integráció). A központosított jogosultságkezelésnek (autentikáció és autorizáció) több előnye van, egyrészt az azonosítók kezelése biztonságosabb egy erre alkalmazott vállalati címtárban, mint decentralizált módon, az egyes rendszerek adatbázisában. A felhasználók életciklusának (kiadás, módosítás, felfüggesztés, visszavonás) központosított kezelésével egyszerűsödik a user right menedzsment folyamat, a megoldás transzparenssé és jól szabályozottá teszi az egyes erőforrásokhoz történő hozzáférést, illetve képes kikényszeríteni bizonyos szervezeti szabályokat (jelszóházirend) és kiküszöbölni a decentralizált rendszerek legjellemzőbb kockázatait (legjellemzőbben az ún. „beragadt” felhasználók).
A szerepköri funkciók tekintetében, ahogy a modell neve is sugallja, az egyes felhasználókat szerepköri csoportokba szükséges sorolni, az esetenként nélkülözhetetlen egyedi jogokat a lehető legkisebb számúra kell korlátozni. A szerepköri jogosultságok kialakításánál kritikusan határozzuk meg azokat a ténylegesen igényelt funkciókat, amelyeket egy-egy szerepkörhöz szükséges hozzárendelni. Például egy kizárólag élőképes megfigyelést bonyolító diszpécsernek nincs szüksége a rögzített felvételekhez történő hozzáférésre, esetleg azok exportjára, egy vendég (ideiglenes) belépőkártyát kiadó recepciós vagyonőr számára nincs szükség a szervezeti mozgási adatok monitorozására, megfigyelésére, egy adott fizikai területhez hozzáférési jogosultsággal

nem rendelkező felhasználónak nem indokolt a behatolásjelző rendszer érintett területi partíciójának kezelése.
Az autentikáció és autorizáció mellett igen fontos fogalom az elszámoltathatóság vagy felelősségre vonhatóság (accountability) amelynek célja, hogy az egyes rendszerekben a felhasználók interakcióit ellenőrizni legyünk képesek és esetleges számonkérhetőségük biztosítható legyen. A biztonságtechnikai rendszerek ma már szinte mindegyike naplózza a felhasználói aktivitásokat, a naplóbejegyzések pedig tartalmazzák a legalapvetőbb eseményinformációkat (belépések, ki, mit, mikor, hol végzett az érintett rendszerben), rendszereseményeket, konfigurációs állományváltozásokat stb. A lokális naplózáson kívül kapcsolódhatunk az erre a célra alkalmazott távoli loggyűjtő megoldásokhoz is.
A felhasználói menedzsment nem lenne teljes körű, ha nem alkalmaznánk olyan adminisztratív eljárásrendeket, amelyek alapján a felhasználói azonosítók biztonságos kiadása, módosítása, időszakos vagy végleges visszavonása megtörténhet. A felhasználókról és a szerepköri funkciókról javasolt a szükséges mértékű nyilvántartás vezetése, az egyes felhasználók hozzáférési jogainak időszakos felülvizsgálata, ellenőrzése, ennek eredményeképpen a szükségtelen felhasználók rendszerekből való törlése (felfüggesztése), a szükséges jogosultsági módosítások elvégzése. A rendszerek naplófájljainak vizsgálatával észlelhetők a jogosulatlan hozzáférések és rendszerinterakciók, ezért javasolt azok meghatározott időszakonkénti ellenőrzése. A rendszerek tervezésénél, telepítésénél fontos annak szisztematikus és teljeskörű átgondolása, hogy a nyilvánvaló jogosultságellenőrzési pontokon túl (szerver és kliensalkalmazásokhoz történő hozzáférés, eszközmenedzsment) hol lehet még szükség jogosultságok korlátozására. Példaként említhető a kamerák RTSP streamje, és az RTSP hitelesítés, amely biztosítja, hogy csak az arra jogosult felhasználók férhessenek hozzá a kamera által kiszolgált videofolyamhoz, vagy ha multifaktoros implementációkban második lépcsőként mobil hitelesítő alkalmazást használunk, az applikáció jogosulatlan hozzáférés elleni védelmét biztosítani szükséges (jelszó, jelkód vagy biometrikus azonosítás).
Mindegyik típusú biztonságtechnikai rendszernél említhető olyan eset, amikor a rendszerek információinak jogosulatlan megismerése nem szándékosan, hanem rossz tervezésből, implementációból vagy hibás eljárásrendek alkalmazásából származik, amelyek elkerülésére törekednünk kell. Behatolásjelző rendszereknél jellemző példa az egyes beviteli tasztatúrák (kódtasztatúrák) nem megfelelő körültekintéssel végzett kezelése. Beléptető rendszerek esetében a mobiltelefonos azonosítás során rövid hatótávolságú kommunikációs technológia (BLE) alkalmazása esetén a nem szándékolt nyitások elkerülése érdekében gondoskodni kell róla, hogy kizárólag szándékos felhasználói interakcióval biztosítsuk a területekhez történő hozzáférést pl. a mobiltelefon autentikációt követő feloldása után, vagy a mobilkészülék rotációjával az olvasás során (HID Twist & Go). Az egyes kezelő vagy megjelenítő egységek, munkaállomások információi (tűzjelző központ, térképes megjelenítő, felügyeleti PC stb.) kizárólag a megfelelő autentikáció után legyenek hozzáférhetők, a kezelőegységek elhelyezése akadályozza meg az illetéktelenek számára a betekintést.

16.2. Sebezhetőség és patch menedzsment

Ahogyan az informatikai rendszerek üzemeltetése során, úgy a bizonságtechnikai rendszerek esetében is elengedhetetlen, hogy azokat folyamatosan naprakészen tartsuk, monitorozzuk az esetleges sebezhetőségeket, aktív intézkedéseket tegyünk azok kiküszöbölésére, az eszközök védelmi képességeit megerősítsük (hardening). Az egyes szoftverek (firmwarek) gyártók által kiadott legújabb verzión tartására az üzemeltetőknek kiemelt figyelmet szükséges fordítani, annak elmaradása egyes esetekben magas

kockázatokat okozhat a rendszerek működésében, a biztonsági hibákat tartalmazó alkalmazások a szervezetet számos belső, illetve a kibertérből származó veszélynek tehetik ki. A patch menedzsment (javításkezelés) egy olyan folyamat, amelynek keretén belül az üzemeltetők gondoskodnak az egyes szoftverek naprakészen tartásáról. Ennek fontos része, hogy az ismert és feltárt sebezhetőségek javítására kiadott gyártói frissítések az elvárt mértékben, módon és határidőn belül telepítve legyenek.
A patch menedzsmentben gyakori a kockázat alapú megközelítés alkalmazása, ugyanis az egyes változásokkal új sebezhetőségek is a rendszerbe integrálhatók, és nem megkerülhető az a kérdés sem, hogy egy javítás vagy verzióváltás gyakran működési és/vagy kompatibilitási problémákhoz vezethet. Ennek okán minden – beleértve az eszközök fizikai módosítását is, pl. bővítés – a rendszerek üzemszerű és biztonságos működését befolyásoló változást szigorú kontroll alatt kell tartani, be kell vonni egy ún. változáskezelési (change management) folyamatba, amely képes biztosítani, hogy a szervezet megfelelő mértékben értékelje a változásból származó működési kockázatokat. Az egyes javítások, frissítések alkalmazását, az alkalmazás határidejét számos kockázati szempont szerint lehet mérlegelni, a vizsgálati kérdéseket leginkább, de nem kizárólagosan a szoftveres és/vagy hálózati architektúra befolyásolja. A biztonságtechnikai rendszeralkalmazások gyakorta beágyazott, lecsupaszított, csak a legszükségesebb funkciókat implementáló, nyílt forráskódú (pl. Linux) operációs rendszerre épülnek, és/vagy adott feladatra tervezett célszoftverek, esetleg alapvetően zárt hálózatra lettek tervezve, így az egyes javítások elmaradásából származó kockázat lényegesen alacsonyabb annál, mint amit egy hibás frissítés a rendszerek megfelelő működése tekintetében jelenthet. Mindazonáltal egyre gyakoribb az általános célú, pl. Windows operációs rendszerre alkalmazott szerver vagy kliensalkalmazás, így alapvetően akkor sem megkerülhető az egyes javítási szcenáriók részletes kockázatértékelése, ha a telepítés során a célfeladatokhoz nem szükséges folyamatokat leállítjuk és/vagy a rendszereket restriktív hálózati környezetben alkalmazzuk. E helyütt érdemes megjegyezni, hogy ez a fajta kockázatalapú megközelítés determinálhatja még többek közt az egyes sebezhetőségek hatásainak csökkentésére, kiküszöbölésre alkalmazott, pl. kártékony kódok elleni védelmi megoldások (ún. anti-vírus szoftverek) alkalmazásának szükségességét is.[240] A kockázatértékelés alapján szükségesnek ítélt javítások tekintetében is vannak olyan biztonságot érintő szabályok, amelyeket a patch menedzsment folyamatban javasolt betartani, ezek közül a leglényegesebbek:

- az alkalmazásokon engedélyezzük a frissítési figyelmeztetéseket, lehetőség szerint azok automatikus telepítését azonban el kell kerülni;
- az egyes javításokat kizárólag biztonságos forrásból, biztonságos hálózati kapcsolaton (pl. HTTPS) keresztül telepítsük;
- a biztonságos forrásból származó csomagok is legyenek digitálisan aláírva, és azokat az alkalmazás validálja.

A patch menedzsment folyamat fontos része, hogy rendelkezzünk visszaállítási, ún. roll-back tervvel arra az esetre, ha egyes frissítések nem várt hibákat okoznának a rendszerek működésében. Egyes biztonságtechnikai rendszerek gyártói a frissítések telepítése után nem engedik a régi verzióra történő visszalépést, az úgynevezett downgrade-et. Ez kétélű fegyver a tekintetben, hogy egyrészt a felhasználó nem tud visszaállni egy sebezhető szoftververzióra, azonban hiba esetén a működés ellehetetlenül, ezért javasolt az egyes javítások korlátozott mennyiségű élés üzemű eszközön történő előzetes tesztelése, vagy

[240] A kártékony kódok esetében fontos, hogy azok manuálisan se tudjanak a rendszerekre kerülni, ezért javasolt korlátozni az egyes fizikai adatbeviteli csatornákat (pl. USB portok), ami által az egyes adatszivárgások is hatékonyabban megelőzhetők.

amennyiben szükséges, tesztrendszerek felállítása és működtetése. A javítási folyamat végén az egyes változtatásokat a biztonságtechnikai rendszerdokumentáción minden esetben át kell vezetni.

Az egyedi gyártói biztonsági javítások egy szélesebb körben ismert, vagy kizárólag a gyártó által felismert sebezhetőségre kínálnak megoldást, azonban a rendszerek tekintetében sebezhetőséget okozhatnak egyes hibás beállítások, konfigurációk vagy rossz gyakorlatok. Igen fontos, hogy az üzemeltető proaktív módon, ezen típusú biztonsági kockázatok folyamatos keresésével (lehetőleg automatikus módon ún. automata sebezhetőségvizsgáló alkalmazások használatával) folyamatosan növelje a rendszerei biztonságát.[241] Ez a fajta vizsgálat kritikus alkalmazások esetében kiegészülhet ún. behatolási tesztekkel (etikus hacking) is, amely folyamat nem kizárólag a sebezhetőségek felderítésére irányul, hanem arra is választ ad, hogy a sebezhetőségek a gyakorlatban hogyan, milyen módon és mértékben használhatók ki a támadók által, és azok milyen mértékű károkat okozhatnak a rendszerekben. A biztonságos üzemeltetés támogatására, a hibás konfigurációkból származó sebezhetőségek kiküszöbölésére a gyártók ún. hardening guide-okat biztosítanak rendszereikhez, amelyek dokumentált, részletes útmutatást nyújtanak a biztonságtechnikai termékek telepítéséhez, beállításához, üzemeltetéséhez. Fontos, hogy a hardening eljárások minden rendszerelemre terjedjenek ki a biztonságtechnikai hálózatban, így az egyes alkalmazások alatt működő operációs rendszerekre, adatbázisokra, illetve a kommunikációs infrastruktúrában telepített hálózati és mobil eszközökre is.

16.3. Incidensmenedzsment

A biztonságtechnikai rendszerek egyik fő funkciója, hogy a kezelők számára megfelelő információkat állítsanak elő, riasztásokat, generáljanak, ezért céljukat és feladatukat nem tölthetik be teljeskörűen anélkül, hogy jelzéseikre a folyamatos reagálás, emberi beavatkozás biztosított legyen. A jelzések lehetnek technikai üzenetek (AC vagy hálózatvesztés, vonalszakadás stb.) riasztások (tűzjelzés, támadásjelzés, behatolásjelzés, analitikai riasztás) és szabotázsjelzések (tamper, érvénytelen azonosítójú mozgás, kényszerített nyitás beléptetőrendszerek esetén, elektronikus megfigyelőrendszerekben kameraszabotázs). A jelzésekre a legjobb gyakorlatok szerint előre elkészített forgatókönyvek, ún. incidenskezelési tervek szerint szükséges reagálni, amelyekben szabályozni kell az egyes, súlyosság szerint besorolt eseményekre történő intézkedés módját, felelősségét és feladatait. Az elkészített akcióterveket az érintett személyekkel igazoltan meg kell ismertetni, azokat folyamatosan és dokumentáltan tesztelni és időszakosan felülvizsgálni, aktualizálni szükséges. Néhány speciális jelzés, illetve alkalmazási környezet esetén az incidenskezelési tervekben figyelembe kell venni egyes jogi szabályzók elvárásait. A tűzjelző rendszerek jelzéseinek felügyelete tekintetében legjellemzőbben az Országos Tűzvédelmi Szabályzatban foglalt személyes felügyeletre, a felügyelet létszámára, illetve a kötelező átjelzések biztosítására vonatkozó előírásokat, míg a pénzügyi intézménynek vonatkozásában a Magyar Nemzeti Bank fizikai biztonsági és az informatikai rendszerek védelmére vonatkozó ajánlásaiban megfogalmazott, a fizikai biztonsági eseményekkel kapcsolatos reagálási elvárások említhetők.

A biztonságtechnikai rendszerek információi nem egyszer bizonyítékként szolgálhatnak büntetőjogi eljárásokban, vagy olyan vállalati belső vizsgálatokban, amelyeknek polgári vagy munkajogi következményei lehetnek. Ilyen információk lehetnek többek közt a különböző kameraképek eseményei, a beléptetőrendszerekben keletkezett mozgási

[241] Természetesen ezek az eszközök alkalmasak arra is, hogy azonosítsák az egyes ismert gyártói szoftversebezhetőségeket is.

adatok, vagy a behatolásjelző rendszerekben keletkezett kezelési adatok (aktiválás, inaktiválás időpontja, annak végrehajtója stb.). Amennyiben a biztonságtechnikai rendszereket a fizikai biztonsági incidensek kapcsán hatósági, büntető vagy polgári jogi peres eljárásokban kívánják felhasználni vagy ennek lehetőségét megteremteni, akkor alapvető, hogy a rendszerek technológiai sajátosságait, illetve a kezelési (hozzáférési), a bizonyítékgyűjtési eljárásokat úgy válasszák meg, hogy azok megfeleljenek a mindenkor hatályos bizonyítási szabályoknak, többek közt nyomon követhető legyen ki, milyen formában, mértékben fért hozzá a bizonyítékként használható felvételekhez, rendszerlogokhoz, azokon milyen műveleteket végzett, végezhetett (chain of custody). Egyes alkalmazások, pl. elektronikus megfigyelő rendszerek támogatják a letagadhatatlanságot és az integritást, a kamerarendszer képes digitális vízjellel ellátni vagy olyan fájlformátumban exportálni a rögzített felvételeket, amely kizárja az utólagos manipuláció lehetőségét.[242]

16.4. Dokumentáció, rendszernyilvántartás

A rosszul dokumentált, nem megfelelő módon menedzselt és ellenőrzött biztonságtechnikai rendszerek már rövid távon üzemeltetési és biztonsági problémákat, némely alkalmazási környezetekben nagyfokú compliance kockázatokat jelentenek a szervezet számára. Fontos, hogy az eszközök menedzsmentje, azon belül is kiemelten a jogosultságok beállítása, kiadása, módosítása, az egyes rendszerfunkciók kiosztása, az eszközökkel kapcsolatos hibák bejelentése, a bővítési, módosítási igények, azok alapján a telepítések ellenőrzött, dokumentált, adott esetben minőségbiztosítási okokból SLA-ban[243] garantált határidőkkel védett módon, transzparensen legyenek megvalósítva, illetve olyan szintű, aktuális rendszerdokumentációval rendelkezzünk, amely támogatja az egyes karbantartási, hibaelhárítási folyamatokat illetve megfelelő tudásbázissal szolgál az üzemeltető és kezelő személyek számára feladatuk hibamentes ellátásához.
Igen jó, de ma még a biztonságtechnikai eszközök esetében ritkán alkalmazott gyakorlat, ha az üzemeltetés során felmerülő igényeket az informatikai rendszerekhez hasonlóan úgynevezett igénykezelő vagy más néven ticketing rendszerbe csatornázzuk, ahol az egyes típusú feladatok manuálisan vagy automatikusan a hozzájuk rendelt megoldó személyeknek kidelegálásra kerülhetnek, a bejelentő, igénylő személy azok aktuális státuszáról információkat kaphat. Az igénykezelő rendszerek egy igen hasznos tulajdonsága, hogy a feladott igények – pl. belépőkártya jogosultsági igény – áteshet egy többszintes, elektronikusan rögzített és igazolt jóváhagyási folyamaton, amely szignifikánsan csökkenti annak az esélyét, hogy egyes rendszerekbe nem indokolt, esetleg kompromittáló célú jogosultságok kerüljenek felrögzítésre. Ezzel a megoldással egy audit során minden jogosultság esetén igazolni tudjuk, hogy azok valamilyen üzleti igény alapján jöttek létre és átestek a szükséges validációs folyamaton, illetve az igénylőnek is lehetősége van menedzselni a leadott igényeit, visszajelezni azok megoldási módjával, esetleges hiányosságaival kapcsolatban. Az igénykezelő rendszer másik nagy előnye, hogy abból rendkívül hasznos és megfelelően vizualizált statisztikai adatokat nyerhetünk többek közt a feladatokkal eltöltött időről, az egyes státuszokban tartás átlagos idejéről, amely hozzájárulhat a hatékonyabb munkaszervezéshez és releváns mérőszámok,

[242] Dr. Tiszolczi Balázs Gergely: Fizikai biztonsági kontrollok tervezésének és alkalmazásának gyakorlata az ISO/IEC 27001 szabvány elvárásainak tükrében. Magyar Rendészet, 2019/2-3. szám. p. 233—249.

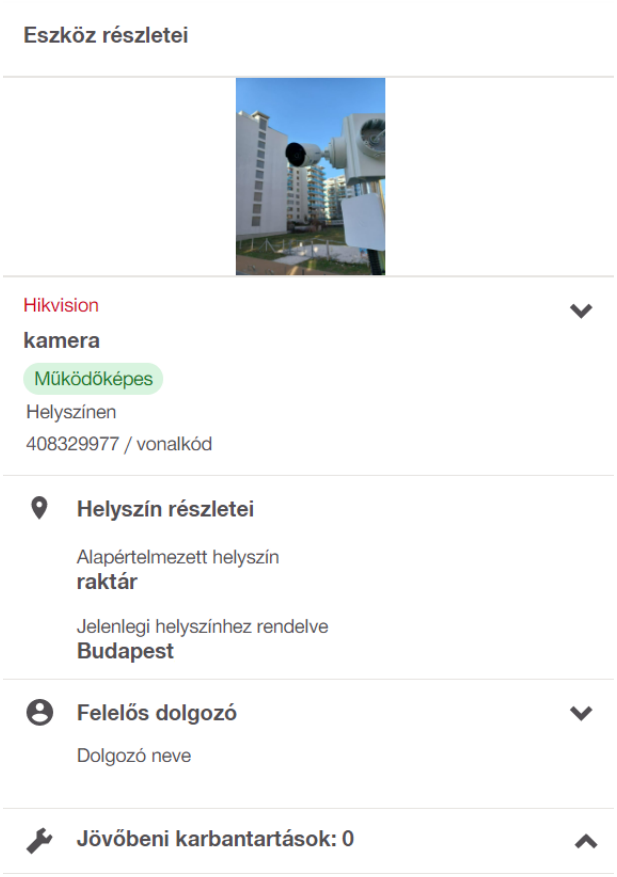
[243] A szolgáltatási szint megállapodás (Service Level Agreement) egy, az ügyfél és a szolgáltató közt keletkezett megállapodás, amely tartalmazza a szolgáltatás minőségével kapcsolatos elvárásokat és célokat, továbbá azok mérhető pontjait és a mérőszámokat.

úgynevezett KPI-k (Key Performance Indikátor, kulcs teljesítménymutatók) felállítása mellett alakulásuk nyomon követésével felügyelni tudjuk és ellenőrizhetjük folyamataink megfelelőségét, az elvárt teljesítmények megvalósulását.

26. ábra[244] Igénybejelentési felület (kezdőlap)

Az eszközök fizikai nyilvántartására, a karbantartások kontrollálására elérhető a piacon olyan eszközmenedzsment alkalmazás, amelyben egyszerűen nyomon követhetőek a rendszerkomponensek, azok telepítési helye, egyedi azonosítói, a garanciális időszakok, műszaki állapotinformációk, illetve mozgatás esetén követhető az eszköz megváltozott helyszíne. Igény esetén a számlázáshoz szükséges pénzügyi adatok is feltölthetőek, illetve kinyerhetőek a rendszerből. Az eszközleltárakat elősegítő módon az alkalmazás QR kód vagy vonalkód olvasás alapján automatikus leltári íveket generál, illetve az eszközökön elhelyezett címkék elektronikus leolvasásával az elvégzett karbantartási eseményekről log generálódik, amellyel ellenőrizni tudjuk a karbantartói feladatvégzést. A karbantartást szintén elősegíti, hogy a telepítési helyszín jelölése fényképekkel is lehetséges, amely támogatja a feladattal megbízott személyt az eszközök pontos helyének gyorsabb feltárásában (20. számú ábra).

[244] Az ábra forrása: A KÉSZ Csoport igénymenedzsment rendszerének biztonsági szolgáltatások üzletág bejelentő felülete.



27. ábra[245] HILTI ON!Track nyilvántartási felületének részlete

A dokumentációs rendszer kialakítása tekintetében a funkcionális működés támogatásán túl további elvárásoknak is kell megfelelni, a megvalósulási tervekben javasolt kitérni minden, a rendszerek biztonságos működését befolyásoló, jelen tankönyvben is összefoglalt információra és beállításra is (jogosultsági beállítások, titkosítási intézkedések, hálózati csatlakozás, tanúsítványok kezelése stb.) A rendszerekkel összefüggő minden változást (így a biztonságot érintőket is), változáskezelési eljárás alá szükséges vonni, és azokat a rendszerdokumentáción minden esetben át kell vezetni. A rendszerdokumentáció egy lényeges elemét képzik a kezelési, működési leírások mind az adminisztrátorok, mind a felhasználók számára. Ebben a tekintetben figyelembe kell venni, hogy a gyakorlatban a rendszerek fejlődéséhez a kezelői állomány egy része kevésbé tud alkalmazkodni életkori, képzettségi sajátosságaik miatt, ezért változó mértékű technikai hiányosságaik lehetnek, amelyek a működésben kockázatokat okozhatnak, a jelzésekre történő reagálás hiányosságokat szenvedhet, vagy a hibás kezelésekből származó téves jelzések miatt megroppanhat a rendszerekbe vetett bizalom. Ezen kockázatok csökkentésére a kezelési, üzemeltetési utasítások olyan részletességgel és az egyes kezelők képességeit is figyelembe vevő tartalommal készüljenek el, hogy hatékonyan legyünk képesek kizárni a hibás kezelésből származó problémákat, továbbá az az általános kezelési feladatokon túl megfelelő információt is biztosítson a jelzések pontos felismeréséhez és értelmezéséhez, a szükséges incidenskezelési intézkedések megtételéhez.

[245] Az ábra forrása: Felhőalapú HILTI ON!Track eszközkezelő rendszer nyilvántartó felületének részlete.

A kezelési leírások mellett a biztonságtechnikai rendszerekkel kapcsolatos minden üzemeltetési folyamatot a felelősségek, határidők megjelölése mellett belső normatív utasításba szükséges foglalni. A szabályzatnak az általános szabályzati kellékek mellett (tárgy, hatály, az egyes rendelkezések végre nem hajtásból származó szankciók) teljeskörűen meg kell határoznia és munkakörhöz szükséges rendelnie a rendszerek élettartama alatt felmerülő összes műszaki, adminisztratív és compliance vonatkozású feladatot, úgy mint:

- rendszerdokumentációk köre és azok kezelése;
- az üzemeltetés, üzemfenntartás felelősségi körei, beleértve a mentésének elvégzését és azok gyakoriságát;
- az egyes rendszerekben keletkezett információk és jogosultsági adatok kezelésére feljogosított munkakörök;
- különböző kezelési szintek, és a szintekhez tartozó jogosultságok kialakítása (jogok kiadása, visszavonása, ellenőrzése, rendszerbeállítások elvégzése stb.);
- a rendszerekbe történő belépési jogok kiadására, visszavonására (automatikus is), módosítására igénylésének, ellenőrzésének, monitorozásának rendjére vonatkozó előírások;
- kódcserék, jelszócserék szabályai, gyakorisága;
- a rendszereszközök, adatbázisok fizikai és informatikai védelmére vonatkozó szabályok meghatározása, a betartás ellenőrzése;
- a mozgási, hozzáférési, képi és egyéb személyes adatok kiadhatóságának szabályai;
- az érdekmérlegelési tesztekben, adatkezelési tájékoztatókban foglalt tárolási, megsemmisítési idők érvényesítése;
- hatósági megkeresések kezelésének rendje;
- a rendszer működésével összefüggő tájékoztatási szabályok;
- meghibásodás és rendkívül helyzet esetén teendők, a védelem fenntartásának szabályai rendkívüli helyzet esetén;
- az újonnan telepített, átépített rendszerek átadás-átvételére vonatkozó szabályok, a műszaki megfelelőség értékelésének kérdései;
- karbantartás, hibajavítás, tesztelés feladatai, felelősségei, beleértve a biztonsági funkciók ellenőrzését is;
- a rendszerek megszüntetésének feladatai, beleértve a selejtezési és hulladékkezelési kérdéseket is.

17. Átadás-átvétel, üzembe helyezés

A biztonságtechnikai rendszerek teljeskörű biztonságához elengedhetetlen, hogy a tervezett és szükséges védelmi intézkedések a kivitelezés során implementálásra kerüljenek, és azokat a megrendelő az átadás-átvételi eljárás keretében teljeskörűen tesztelje, győződjön meg azok működőképességéről. Jelen fejezetben a funkcionális működési szempontok ellenőrzését nem érintve olyan módszereket mutatunk be, amellyel a biztonsági beállítások, védelmi intézkedések megfelelősége előzetes szakértelmet nem, vagy kis mértékben igénylő módon a megrendelő számára is ellenőrizhető, illetve számonkérhető.

Az első és legfontosabb vizsgálati szempont a megvalósulási dokumentáció megléte, ugyanis a biztonságtechnikai rendszerekben a megfelelő dokumentáltság nem csak a karbantarthatóság, hibajavítás és kezelésbiztonság miatt fontos, szintén nagy szerepet kap a rendszerek biztonságának fenntartásában és ellenőrzésében is. A biztonságtechnikai rendszerek egyes rendszerelemei és a kapcsolódó külső interfészek közti kommunikáció ellenőrzése, annak biztonsága az egyik leglényegesebb kérdés az üzemeltetési feladatok során. A megvalósulási dokumentáció részeként meg kell követelni a biztonsági és védelmi intézkedések leírását, illetve olyan szintű infrastruktúra tervet, amely tartalmazza az OSI adatkapcsolati, hálózati és szállítási rétegbeli azonosítóit, különösen a MAC, IP címeket, portszámokat, az alkalmazott kommunikációs protokollokat, kapcsolati irányokat, VLAN azonosítókat. A biztonsági szakembereken kívül igen fontos, hogy a hálózat az informatikai üzemeltetők számára is transzparens módon működjön, a szükséges beállításokat, hozzáférési restrikciókat megfelelően el tudják végezni. A tervekben szereplő különböző logikai és fizikai eszközelhelyezési rajzok segíthetnek azonosítani a rendszerelemeket, a rajtuk keresztül beérkező, azokon kimenő adatokat. A tervekben meg kell jeleníteni minden olyan inputot és outputot, ahol a biztonságtechnikai rendszerekbe információ be vagy kivitel történik. Ez kiterjed a bejövő videóképekre, a behatolásjelző rendszerek egyes felhasználói által használt tasztatúrakódokra, vagy a beléptető rendszerekben alkalmazott azonosítók (leggyakrabban proximity, smartcardok) használatával történő autentikációs adatok bevitelére, vagy a különböző menedzsment alkalmazásokon (webes, asztali, mobil) keresztüli hozzáférésekre. Kimenet lehet minden, ahol felvételeket, eseményeket figyelünk meg, elemzünk, nyomtatunk, adatot exportálunk (fizikai adathordozóra is), vagy más külső alkalmazásokkal a rendszereinket API-n keresztül összekötjük. Ennek fontossága kiemelt, leggyakrabban az input, output felületeken keresztül lehet kompromittálni a rendszereket, illetve az alattuk lévő hálózatot, tekintettel a rendszerelemek nagyfokú önvédelmi (szabotázs elleni védelmi) képességeire. Ezzel összhangban a hozzáférési szabályok megfelelőségét kell tesztelnünk, minimálisan alábbi tartalommal:

- ellenőrizzük, hogy az alapértelmezett (default) illetve a telepítői felhasználók visszavonásra, inaktiválásra kerültek-e;
- ellenőrizzük, hogy a telepítők az összes alkalmazás és rendszerelem tekintetében megváltoztatták-e a gyártói default jelszavakat;
- vizsgáljuk meg, hogy a rendszerekben tiltják-e a közös használatú vagy nem nevesített felhasználókat, illetve az előírt jelszókomplexitási és jelszólejárati követelmények érvényesítését, a kiemelt jogú felhasználók esetében alkalmazzák-e az elvárt multifaktoros autentikációt, azok megfelelően beállításra kerültek-e (biztonságtechnikai alkalmazás és az alkalmazott operációs rendszer tekintetében is);

- a kezelői beállítások ellenőrzésénél vizsgáljuk meg, hogy az egyes felhasználók a szerepkörüknek megfelelő jogosultsági szinteken kezelik-e a rendszert (pl. egy megfigyelésére alkalmazott munkaállomáson csak az élőképek legyenek engedélyezettek, recepciós munkakörben kizárólag a vendégkártya menedzsment legyen végrehajtható, illetve behatolásjelző rendszeren csak az adott felhasználóhoz tartozó partíciók kezelése legyen lehetséges);
- annak megállapítása, hogy az eszközök elhelyezése lehetővé teszi-e az illetéktelen betekintést (kódtasztatúrák, megfigyelő állomások, beléptető rendszerek kezelőfelületei), ezáltal az adatok illetéktelen megismerését;
- engedélyezetten túli belépési próbálkozások végrehajtásával ellenőrizzük, hogy a beépített brute force elleni védelmi megoldások (csillapítás), a lockout funkciók megfelelően működnek-e;
- minden esetben ellenőrizzük a rendszerek ki és bemeneti elemeinek fizikai védettségét, a fizikai hozzáférést korlátozó intézkedések megfelelőségét.

17.1. Szabotázsvédelem és a jelzésátvitel biztonságának tesztelése

A rendszerek következő ellenőrzési feladata az alkalmazott szabotázs elleni védelmi megoldások és a különböző jelzések működési tesztje alábbiak szerint:

- behatolásjelző rendszerek esetében a vonali szabotázs tesztelése, az érzékelők (passzív infra, nyitásérzékelők stb.) a bővítő, a táp és központdobozok szabotázs elleni védelmi próbája nyitással, a kitakarásvédett érzékelők kitakarás tesztje, a rádiós érzékelő eltávolításának próbája (nagyszámú érzékelő periféria esetén elégséges bizonyos százalék véletlenszerű tesztelése);
- a beléptető rendszerek esetében a tápok, vezérlő és hálózati csatoló dobozok szabotázs elleni védelmének ellenőrzése nyitással, a kényszerített nyitások jelzésének tesztelése autentikáció nélküli áthaladással, az áteresztő pontok mechanikai eszközeinek véletlen vagy szándékos nyitott állapotát jelző lokális zümmerek (hangjelzők) tesztelése az áteresztési pont nyitott állapotban tartásával;
- kamerarendszerek esetében, amennyiben a rendszerbeállítások lehetővé teszik, a szabotázs ellenőrzési funkció terjedjen ki az elforgatásra (pozícióváltoztatásra), a letakarásra és a fókuszvesztés érzékelésének tesztelésére;
- éles pánikriasztás szimulálása pánikkapcsoló vagy duress kód működtetésével;
- éles behatolásjelzés tesztelése a rendszer élesbe állításával, és aktív zóna megsértésével;
- beléptető rendszer esetén jogosultan azonosítók használatával, vagy kényszernyitással végzett teszt;
- vészhelyzeti állapotok szimulálása vésznyitó, tűzjelző kézi jelzésadó stb. segítségével;
- ellenőrizzük, hogy a biztonságot befolyásoló hiba és egyéb technikai jelzések megfelelően működnek, ahol indokolt, vonali szakadás, rövidzár, hálózati hiba, illetve legalább a hálózati feszültség és a másodlagos tápellátás hibájának tesztelésével, kamerajel vesztés szimulálásával;
- a helyi és távoli hang és fényriasztások, a jelzésátviteli út megfelelőségének tesztelése a távfelügyeleti, vagy távoli felügyeleti hely irányába (a felügyeleti

helyet és a helyszíni felhasználókat minden esetben előzetesen értesíteni szükséges a tesztelés időpontjáról és időtartamáról).

17.2. Hálózati beállítások biztonságának tesztelése

Amikor a kommunikáció biztonságának ellenőrzéséről beszélünk, a kommunikációs folyamat folytonosságán (jelzésátviteli biztonság) túl annak bizalmasságát, a kommunikációs végpontok közt átvitt adatok, információk titkosságának megfelelő megvalósítását is ellenőriznünk szükséges. Ott, ahol a biztonsági követelmények előírják, a titkosítatlan hálózati adatfolyam (pl. HTTP, Telnet, FTP, RTSP) illetve a nem biztonságos és/vagy szükségtelen protokollok korlátozása, továbbá a szükségtelen szolgáltatások tiltásának ellenőrzése az egyik legfontosabb feladat, amelynek végrehajtásához sokszor nem elegendő az eszközök biztonsági beállításainak vizsgálata. Jó gyakorlat lehet, ha a telepítés és a hálózati beállítások befejező műveleteként elvégezzük alábbi ellenőrzési feladatokat:
Az eszközök nyitott portjainak, a mögöttük futó szolgáltatások külső ellenőrzése. Ennek egyik legegyszerűbb módja valamely hálózati szkenner applikáció használata. A hálózati, vagy más néven portszkennerek olyan szoftvereszközök, amelyek a hálózatba telepített node-ok és a rajtuk futó szolgáltatások felderítését végzik, kommunikációs csomagok küldésével és a visszakapott válaszok kiértékelésével. Az egyik, legszélesebb körben alkalmazott ilyen eszköz az Nmap hálózati szkenner, amely ingyenesen letölthető, Windows és Linux operációs rendszerre is elérhető, parancssori és GUI felülettel is rendelkezik.[246] Egyszerű parancsok futtatásával felfedezhetőek a nem biztonságos, és/vagy a dokumentációban nem szereplő, nem megengedett hálózati szolgáltatások az egyes eszközökön. Az alábbi, 21. számú ábra egy felderítési parancs kimenetét mutatja, amelyen számos, nem biztonságosnak tekintett protokoll használata látható (a vizsgált IP azonosító kitakarásra került).

```
Starting Nmap 7.40 (https://nmap.org) at 2023-01-04 12:02 UTC
Nmap scan report for
Host is up (0.067s latency).
rDNS record for
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
80/tcp   open     http
3389/tcp open     ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.18 seconds
```

28. ábra[247] Hálózati szkenner kimenete

Bizonyos esetekben, ahol értelmezhető, pl. operátori, vagy központi felügyeleti számítógépeken használhatjuk a parancssorból elérhető netstat (network statistics) alkalmazást is, hogy ellenőrizzük, a számítógépünk milyen hálózati kapcsolatot tart fenn más eszközökkel, megtekinthetjük a kapcsolat állapotát, az alkalmazott portszámokat, a

[246] https://nmap.org

[247] A szerző saját szerkesztésű ábrája.

kapcsolathoz tartozó folyamatazonosítókat. Az alkalmazás segít nekünk abban is, hogy megállapítsuk, folytat-e az eszköz nem kívánt kommunikációt külső irányokba. A netstat parancsnak számos kapcsolója érhető el, Windows rendszerű számítógépen a parancssorba a *netstat -a -o* parancsot gépelve mi magunk is ellenőrizhetjük számítógépünk hálózati kapcsolatait és a hozzájuk tartozó folyamatazonosítókat. A következő, 22. számú ábrán a parancsot Linux rendszerű számítógépen futtatva alábbi eredményt kapjuk (cél IP címek kitakarva):

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	10.0.2.15:36786	:https	ESTABLISHED	1469/firefox-esr
tcp	0	0	10.0.2.15:46072	:http	ESTABLISHED	1469/firefox-esr
tcp	0	0	10.0.2.15:42718	:http	TIME_WAIT	-

29. ábra[248] Netstat parancs kimenete

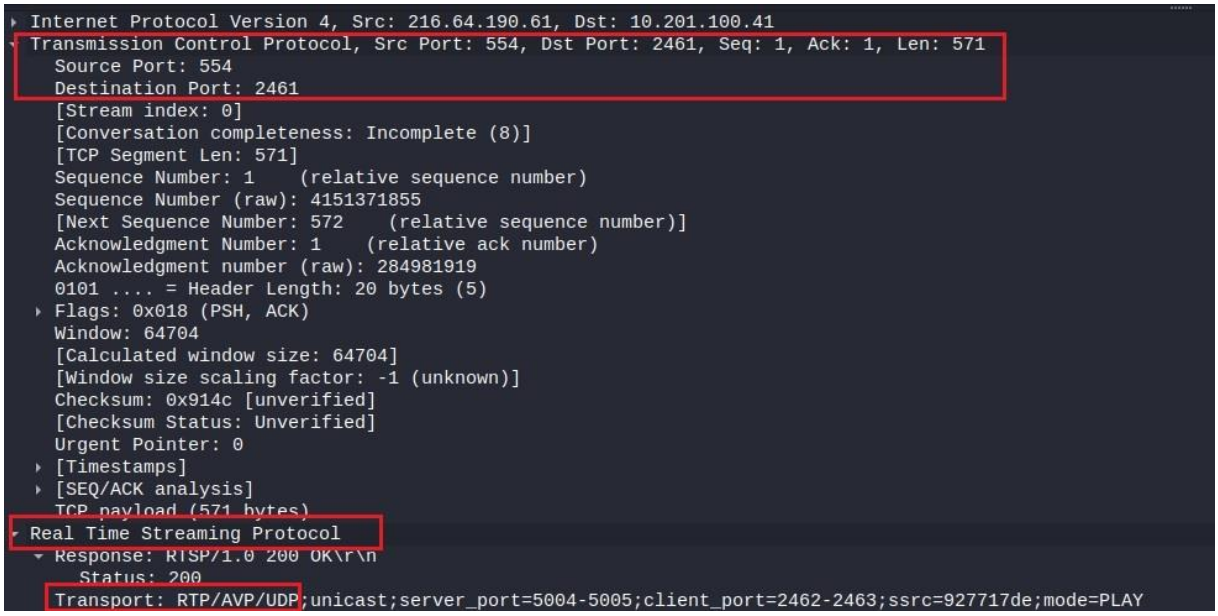
A proto mező az alkalmazott szállítási rétegbeli protokoll típusa, a local address a helyi számítógépünk címe, illetve portszáma, a foreign address mező a távoli kommunikációs állomás IP címe (kitakarva) és portszáma, a state mező a kapcsolat aktuális állapotát mutatja, míg a PID mezőben pedig a kapcsolatot fenntartó (birtokló) alkalmazás azonosítója és neve látható.
Egy komolyabb szakértelmet igénylő mód, azonban mindközül a legalaposabb, ha a rendszereink által generált hálózati forgalmat teljeskörűen, egy erre alkalmas monitorozó eszközzel ellenőrizzük. A szakértelem ebben az esetben ki kell terjedjen a szoftver használatára, a kinyert protokollinformáció értelmezésére, illetve annak azonosítására, a hálózatunk mely pontja és eszköze, eszközei alkalmasak arra, hogy a rajtuk keresztül továbbított, vagy az általuk küldött/fogadott adatok megfigyelése (rögzítése) és elemzése elégséges információt nyújtson számunkra a hálózati forgalom biztonságáról. Erre a feladatra egy alkalmas eszköz lehet a Wireshark, amely a világ legszélesebb körben használt hálózati protokollelemzője. Segítségével részletesen láthatjuk, és elemezhetjük a hálózati adatforgalmat az OSI réteg minden szintjén. Akár rögzített, úgynevezett capture fileokból, akár real time, azonos időben is láthatja, mi történik a hálózaton, és felhasználóbarát felületével segíti a szakembereket az adatok keresésében, értelmezésében.[249] Az alábbi ábra egy Wireshark capture file-t mutat, ahol az RTSP protokoll szerinti kliens és a szerver inicializálás egyik fázisa látható. Az RTSP egy hálózati vezérlőprotokoll, amely streaming médiaszerverek vezérlésére szolgál, széleskörben alkalmazott biztonságtechnikai megfigyelőrendszerekben. A protokollt a végpontok közötti médiaszekciók létrehozására és vezérlésére használják, pl. elindítás, megállás, folytatás, lejátszási sebesség vezérlése stb. Az RTSP továbbítja a video/audio adatokat a hálózati fejezetben már említett és vizsgált RTP (Real-Time-protokoll használatával.[250] A Transport mezőből látható, hogy maga a médiafolyam UDP fölött, titkosítatlan RTP protokoll használatával fog a hálózaton keresztül továbbítódni. Ez egyébként a TCP fejlécből is kiolvasható, a kiszolgáló az RTSP standard, well-known

[248] A szerző saját szerkesztésű ábrája.

[249] https://www.wireshark.org/

[250] https://www.modernalarm.hu/tervezesi-segedletek/wisenet-tippek/rtsp-stream-hasznalata letöltés ideje: 2022.12.03.

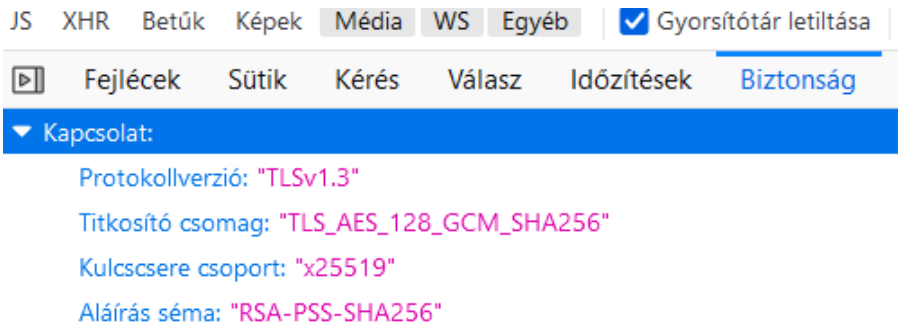
portját használja (554). A legtöbb biztonságtechnikai alkalmazásban a kiszolgálók eltérő portot használnak a titkosítatlan (RTSP/RTP) és a titkosított (RTSPS/SRTP) kapcsolatok során.



30. ábra[251] **Wireshark RTSP capture**

Abban az esetben, ha a biztonságtechnikai rendszereink kezelése, menedzsmentje webes alkalmazáson, böngészőn keresztüli eléréssel történik, viszonylag egyszerűen ellenőrizhetjük a hálózati kapcsolat biztonságát. A kiszolgáló webcímét a böngészőbe begépelve a címsorban a legtöbb esetben egy zöld lakat és a HTTP protokoll után illesztett S (secure) betű jelzi, hogy kapcsolatunk biztonságos, titkosított (HTTPS). A legtöbb mai böngésző jól képes jelezni, és a kapcsolatot a felhasználó további engedélyéhez kötni abban az esetben, ha a kiszolgáló a hálózati fejezetben bemutatott ún. önaláírt tanúsítványt használ, amelynek engedélyezését lehetőleg belső alkalmazások során is kerülni kell, annak ellenére, hogy ez lehet teljesen valid megoldás, azonban indikálhat megszemélyesítéses, ún. man in the middle alapú támadásokat is, amelynek egy kevésbé képzett és/vagy figyelmes felhasználó egyszerűbben áldozatul eshet. A titkosított kapcsolat megléte mellett az is fontos, hogy az alkalmazások az iparági gyakorlatnak megfelelő, biztonságos és elfogadott titkosítási készletet, ún. cipher suite-ot használjanak, amely szintén egyszerűen ellenőrizhető a böngészőnk segítségével. A Mozilla Firefox esetében a további eszközök/webfejlesztő eszközök beállításánál képesek vagyunk a hálózati kapcsolat főbb jellemzőinek, így az alkalmazott titkosítási megoldások megtekintésére is (24. ábra).

[251] Az ábra forrása: https://wiki.wireshark.org/SampleCaptures



31. ábra[252] Titkosítási paraméterek

Az egyes rendszerekben beállított hozzáférési restrikciók teszteléséhez próbáljuk ki, hogy a kiszolgálókon beállított, engedélyező egyedi IP és/vagy MAC címektől eltérő azonosítójú munkaállomásokról képesek vagyunk-e hozzáférést szerezni, illetve külső VLAN-ból történő csatlakozási kísérlettel ellenőrizhetjük a hálózati eszközökön beállított ACL-ek megfelelőségét.
Az egyes eszközök fizikai hálózati csatlakozási helyszínein, illetve az adatkapcsolatot biztosító switchekre történő idegen eszköz csatlakoztatásával ellenőrizhetjük a beállított portvédelmet, illetve a nem használt fizikai portok letiltását.

17.3. Egyéb tesztelési feladatok

A hozzáférések, a szabotázsvédelem, a jelzésátvitel és a hálózati kommunikáció biztonságán túl számos olyan szempont van, amelyeket a teljes körű megfelelés érdekében funkcionálisan is ellenőriznünk szükséges. Az egyes eszközökön beállított rendszeridő megtekintésével validálhatjuk az időszinkronizációs beállításainkat, hogy az összes rendszerünk egy időbázison működik-e. Ugyanúgy fordítsunk figyelmet annak ellenőrzésére, hogy a kliensek és a szerveralkalmazások a legfrissebb szoftver (firmware) verziót használják, illetve, hogy a beállított e-mail és/vagy logküldési megoldások helyesen, az igényelt adattartalommal, és gyakorisággal működnek. Ellenőrizzük, hogy a kezelők megfelelően ismerik-e a jelzésekre történő reagálás szabályait, az alkalmazások kezelését, végre tudják-e hajtani az összes szükséges feladatot. Az alkalmazott mentési eljárások tekintetében nem csak a lefutást, hanem az egyes mentési állományok visszaállíthatóságát is validálni javasolt. Fontos életvédelmi kérdés, hogy a rendszerek erősáramú szerelése végén az érintésvédelem megfelelőségéről minden esetben győződjünk meg, a minősítő okiratban feltárt esetleges hiányosságokat azonnal javítsuk.
Nagy biztonságú alkalmazásokban, vagy ott, ahol a megrendelő szeretne teljeskörűen meggyőződni a telepített rendszerek funkcionális és biztonsági megfelelőségéről, ott érdemes egy erre szakosodott vállalkozással a már kialakított megoldásokat auditáltatni, így külső szakértői forrásból is meggyőződhetünk, hogy a rendszereink összes részegysége, a kapcsolódó folyamatok és a kezelést végző humán erőforrás valóban alkalmas a feladatuk szakszerű, hatékony és biztonságos ellátására. A külső audit keretén belül számos vizsgálatra lehetőség nyílik, ez megrendelői igényektől és lehetőségektől függően kiterjedhet a dokumentációk vizsgálatára, a jelen fejezetben foglalt ellenőrzési feladatok szakértői végrehajtására, a rendszerek hálózati és IT biztonságát értékelő sérülékenységi és behatolástesztekre (penetration teszt), kiegészítve a fizikai hozzáférés elleni védelem tesztelésével (pl. próbabehatolás).

[252] A szerző saját szerkesztésű ábrája.

Felhasznált irodalom

Könyvek, folyóiratok, tanulmányok

Allan Liska: NTP Security: A Quick-Start Guide, Apress, 2016., ISBN:9781484224120

Bányász Péter–dr. Bodó Attila Pál–Kapitány Sándor–Orbók Ákos–dr. Zámbó Nóra: Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára. Nemzeti Közszolgálati Egyetem, 2016.

BME Informatikai Központ: Tervezés az IT biztonság szempontjából, Miniszterelnöki Hivatal, 2008.

Bunyitai Ákos: A ma és a holnap beléptető rendszereinek automatikus személyazonosító eljárásai biztonságtechnikai szempontból, Hadmérnök, VI. évfolyam 1. szám, p. 22-35., ISSN 1788-1929

Dr. Michelberger Pál - Lábodi Csaba: Vállalati információbiztonság szervezése. https://kgk.uni-obuda.hu/sites/default/files/10_Michelberger_Labodi.pdf (letöltés ideje: 2022.10.02.)

Dr. Tiszolczi Balázs Gergely: Fizikai biztonsági kontrollok tervezésének és alkalmazásának
gyakorlata az ISO/IEC 27001 szabvány elvárásainak tükrében. Magyar Rendészet, 2019/2-3. szám. p. 233-249

Gál Zoltán, Balla Tamás: A QoS hatása az infokommunikációs alkalmazásokra. Híradástechnika. LXII. 7-16., 2007.

Kocsis Tamás: Hazai kamerák az interneten – Ki figyeli az őrzőket? 2020. https://alverad.hu/wp-content/uploads/2021/08/alverad-ki-figyeli-az-orzoket_-1.pdf (letöltés ideje: 2023.01.17.)

S. Tanenbaum, Andrew, J. Wetherall, David: Számítógép-hálózatok. 13. magyar nyelvű kiadás, Panem Könyvek, Taramix Kft, 2013, Budapest

Tiszolczi Balázs Gergely: A vállalati biztonságtechnika gazdaságtani megközelítése. Szakdolgozat. Budapesti Gazdasági Főiskola, Pénzügyi és Számviteli Kar, 2015

Tóth Attila: Tűzjelző rendszerek, beléptető rendszerek, in: Christián László–Major László–Szabó Csaba (szerk.): Biztonsági vezetői kézikönyv. Budapest, Dialóg Campus, 2019.

Tóth Attila – Tóth Levente: Biztonságtechnika. Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar, Budapest, 2014. ISBN 978-615-5305-56-6

Tóth Levente: A komplex objektumvédelem kihívásai napjainkban, Bolyai Szemle, XXVII. évfolyam, 1. szám, p. 35-44. ISSN: 1416-1443

Technikai leírások, adatlapok, egyéb internetes források

Axis Communications: Encrypting network streams: An overview of why and how to encrypt network video (letöltés ideje: 2022.01.12.)

Bosch IP Video and Data Security Guidebook https://resources-boschsecuritycdn.azureedge.net/public/documents/Data_Security_Guideb_Special_enUS_9007221590612491.pdf (letöltés ideje: 2021.04.01.)

Bosch: Network Authentication - 802.1x, Secure the Edge of the Network, https://resources-boschsecurity-cdn.azureedge.net/public/documents/WP_802.1x_Special_enUS_22335867275.pdf (letöltés ideje: 2023.01.02.)

Hanwha Techwin America: Cyber Security White Paper, Securing Video Surveillance Devices to Close Network Vulnerabilities (letöltés ideje: 2023.01.12.)

Hálózati eszközök programozása, https://irh.inf.unideb.hu/~cisco/cisco/doku.php?id=itn:09._fejezet_-_cimfeloldas (letöltés ideje: 2023.01.17.)

Hikvision Achieves Common Criteria Certification https://www.prnewswire.com/il/news-releases/hikvision-achieves-common-criteria-certification-696212031.html (letöltés ideje: 2022.09.27.)

Hikvision: Network Camera Security Guide, January 2018 (letöltés ideje: 2022.09.17.)

Huawei HoloSens, 2020, Intelligent Vision, Tech Express. https://support.huawei.com/enterprise/en/doc/EDOC1100172551 (letöltés ideje: 2022.10.27.)

https://www.commoncriteriaportal.org/products/

https://www.onvif.org/wp-content/uploads/2019/01/ONVIF_Profile_Q_Specification_v1-2.pdf (letöltés ideje: 2022.03.01.)

https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_hu.htm

https://kiber.blog.hu/2021/09/21/sokmillio_kamera_kerulhet_veszelybe_hikvision_armageddon_kozeleghet (letöltés ideje: 2022.08.11.)

https://www.securinfo.hu/termekek/beleptetorendszerek/1277-az-azonositas-biztonsaga-a-beleptetorendszereknel-i-resz.html (letöltés ideje: 2022.11.07.)

https://www.hikvision.com/content/dam/hikvision/en/support/download/how to/nvr/How%20to%20configure%20NTP%20and%20DST.pdf (letöltés ideje: 2022.02.13.)

https://www.modernalarm.hu/tervezesi-segedletek/wisenet-tippek/rtsp-stream-hasznalata (letöltés ideje: 2022.12.03.)

https://nmap.org

https://www.riel.hu/tamogatas/tudastar/video/hikvision-ntp-es-dst-beallitas (letöltés ideje: 2022.02.13.)

https://wiki.wireshark.org/SampleCaptures

https://www.wireshark.org/

QoS in Axis Video Products, technical note, Rev: 1.0 Updated 2006-02-15 (letöltés ideje: 2022.11.14.)

What should you know about SNMP and Bosch cameras SNMP support?https://community.boschsecurity.com/t5/Security-Video/What-should-you-know-about-SNMP-and-Bosch-cameras-SNMP-support/ta-p/27034 (letöltés ideje: 2023.02.28.)

Egyéb felhasznált források

A KÉSZ Csoport igénymenedzsment rendszerének biztonsági szolgáltatások üzletág bejelentő felülete.

Felhőalapú HILTI ON!Track eszközkezelő rendszer nyilvántartó felül