NEMZETI KIBERVÉDELMI INTÉZET

Felhasználói kézikönyv

A 41/2015. BM rendelet által meghatározott védelmi intézkedésekhez

2021. december

Tartalom

1. A Kézikönyv célja

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet által kiadott Kézikönyv célja, hogy a 41/2015. (VII. 15.) BM rendelet 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 rendelet (továbbiakban: Rendelet) által meghatározott elvárásokhoz, védelmi intézkedésekhez **magyarázatot adjon, és példát biztosítson a pontosabb megértés, könnyebb testreszabhatóság és implementáció érdekében.** A Kézikönyv iparági jó gyakorlatokkal, illetve előremutató példákkal segíti az információbiztonsági felelősök munkáját. A Kézikönyv kiegészítéseként létrehozott részletes védelmi intézkedés gyűjtemény kifejezetten hasznos azon szervezetek számára, amelyek törvényi kötelezettségükből fakadóan, vagy információbiztonságuk növelése érdekében szintet kívánnak lépni. Segítségével gyorsan átláthatják a következő biztonsági osztályhoz szükséges további védelmi kontrollokat és azok gyakorlati megvalósítását. A Kézikönyv alapvetően azon Ibtv. hatálya alá tartozó szervezetek vezetőinek, információbiztonsági felelőseinek szól, de hasznos segítséget nyújthat mindenkinek, aki szeretné megerősíteni a szervezete információbiztonságát.

A Kézikönyv a Rendelet által meghatározott védelmi intézkedésekről és azok értelmezéséről ad átfogó képet. Kitér arra, hogy milyen céllal alkalmazandó az adott védelmi intézkedés, illetve milyen területekre terjed ki. **A Kézikönyv célja, hogy hidat képezzen a Rendelet jogi szövegezése és az információbiztonsági szakemberek egyéni értelmezése között.**

A Kézikönyvben a fejezetek az egyes védelmi intézkedés pontjával összhangban készültek el, a Rendelet keretrendszerét alapul véve három nagy csoportra bontva: Adminisztratív védelmi intézkedések, Fizikai védelmi intézkedések és Logikai védelmi intézkedések. Az egyes védelmi intézkedés csoportokhoz egy részletes védelmi intézkedés gyűjtemény tartozik, amely leírja az egyes intézkedések célját és magyarázatát, példát ad rá, valamint több esetben felvázolja az iparági jó gyakorlatot és előremutató megvalósítást. Részletek, praktikus tanácsok és gyakorlatban alkalmazható megoldások a dokumentumcsomag részét képező Excel táblázatban találhatóak.

2. Védelmi intézkedések általános bemutatása

A 41/2015 BM rendelet az elektronikus információs rendszerek, az azokban tárolt adatok és információk, valamint az azokat működtető személyzet és infrastrukturális elemek védelmére három különálló, de szorosan együttműködő területre osztotta a védelmi intézkedéseket. A szervezeti szintű stratégiával, szabályozással és irányítási feladatokkal, valamint a különféle jogszabályi megfelelőségekkel az **adminisztratív** védelmi intézkedési rész foglalkozik. A hardverelemek és épületek **fizikai** sérüléstől, eltulajdonításától és bárminemű rongálásától védő intézkedési kontrollok a fizikai védelmi intézkedések részben találhatók. Ide tartozik a véletlen esemény pl.: természeti katasztrófa és a szándékos pl.: szabotázs akció is. Az **elektronikus információs rendszerek** (**EIR**) technológiai, szoftverrel megvalósítható védelmi tevékenységek csoportja a **logikai** védelmi intézkedésekhez tartozik. Az ebbe a fejezetbe tartozó kontrollok a teljes EIR védelmére fókuszálnak, átfogó jellegükből adódóan a jelenleg ismert kibertérben létező fenyegetésekre kockázatcsökkentő előírásokkal rendelkeznek.

2.1 Adminisztratív védelmi intézkedések

Az adminisztratív védelmi intézkedések célja, hogy a Szervezet már szabályozási szinten kialakítsa azokat a kontrollokat, amelyek elősegítik az EIR védelmét az adott biztonsági osztályokban, ezáltal megteremtve a szervezet biztonsági igényeire szabott **információbiztonsági irányítási keretrendszer**t. Az adminisztratív védelmi intézkedések célja, hogy a szervezet mindennapi életével, üzletmenetével és szabályozásaival összhangban kialakítson, definiáljon olyan folyamatokat, amelyek a gyakorlatban megvalósíthatók és az elektronikus információs rendszer védelmét szolgálják.

Az adminisztratív védelmi intézkedések kiterjednek a szervezet alapfeladataira, a kockázatelemzésére, azon feladatokra amelyek a beszerzési folyamatokkal, üzletmenet-folytonosság tervezésével kapcsolatosak, illetve a biztonsági események kezelését is meghatározza. Ezek az intézkedések megadják továbbá, hogy a munkakörökkel kapcsolatban milyen biztonsági folyamatokra van szükség, illetve a munkavállalók tudatosságának fontosságát is kiemelik.

2.1.1 Szervezeti szintű alapfeladatok

A szervezeti szintű alapfeladatokkal kapcsolatos védelmi intézkedések célja, hogy a Szervezet meghatározza **szabályzati szinten** az informatikai biztonságának alappilléreit. Ehhez a Szervezet számára **Informatikai Biztonsági Szabályzat**ot (IBSZ) kell készítenie, amelynek célja, hogy az adatvédelmi és információbiztonsági folyamatokat meghatározza: definiálja a biztonsági eljárásokat, felelősöket határozzon meg, jól követhető folyamatokat alakítson ki.

Az IBSZ mellett egy informatikai biztonsági felelősre (a továbbiakban: **IBF**) is szükség van, aki az EIR-ek biztonságáért felel és ellátja a 2013. évi L. törvény (továbbiakban Ibtv.) 13. §-ában meghatározott feladatokat. Az IBF kizárólag olyan személy lehet, aki büntetlen előéletű, valamint felsőfokú végzettséggel és megfelelő szakképzettséggel is rendelkezik. A pozíció betöltése megoldható egy dedikált személy felvételével, de ha a Szervezetnél van olyan munkavállaló, aki megfelel a törvényi követelményeknek, elláthatja a biztonsági felelős feladatait is. Amennyiben a Szervezetnél nincs ilyen házon belüli kompetencia, akkor bevett szokás, hogy egy külsős vállalkozással (vagy vállalkozóval) köt szerződést a Szervezet, aki megbízási szerződés alapján biztosítja az IBF-et. Ilyen esetben is egy konkrét személyt kell bejelenteni a Hatósághoz. Rá is ugyanolyan törvényi követelmények vonatkoznak, mint egy szervezeten belüli IBF-re. Kiszervezni csak a feladatot lehet, a felelősséget nem - tehát egy kiszervezett IBF nem hozhat a Szervezetet érintő döntéseket, csak szakmai javaslatokat tehet.

A szervezeti szintű alapfeladatok közé tartozik továbbá az **EIR rendszerek nyilvántartása**, ami elősegíti, hogy egy helyen megtalálható legyen mindegyik rendszer leírása, illetve annak a személynek a neve és elérhetősége aki a rendszert felügyeli. A nyilvántartás biztonsági probléma esetén elősegíti a gyors reakciót, ami fontos, hiszen a hiba minél korábbi detektálásra, kijavításra kerül, annál kisebb kárt okozhat a rendszerekben. Fontos, hogy a nyilvántartás teljes és naprakész legyen.

Az EIR rendszerekkel kapcsolatos **engedélyezési eljárás** definiálása, valamint az **intézkedési terv** és mérföldköveinek meghatározása is a szervezeti szintű alapfeladatokhoz tartozik. Az új vagy módosított EIR rendszerek csak engedélyezési eljárást követően kerülhetnek használatba, ehhez az üzemeltetésért felelős szervezeti egység vezetője vagy az információbiztonságért

felelős személy indítja el az engedélyezési folyamatot. Attól függően, hogy a NATO, EU követelménye és a jogszabályok szerint milyen engedélyezési eljárásra van szükség, azt a szervezetet/szervet kell bevonni az engedélyeztetésbe.

Fontos, hogy **a szervezeti szintű alapfeladatokat minden szervezetnek el kell végeznie,** függetlenül attól, hogy milyen biztonsági osztályba tartozó EIR-eket használ.

2.1.2 Kockázatelemzés

A biztonsági kockázatelemzés célja, hogy felmérje, azonosítsa a leggyengébb pontokat, amelyek a legnagyobb kockázatot, veszélyforrást jelentik. A kockázatelemzés-, és értékelés folyamatának, felelőseinek, elvárt minőségének belső **szabályozásban, vagy a kockázatelemzési és kockázatkezelési eljárásrendben való rögzítése** biztosítja, hogy a kockázatelemzést rendszeresen és konzisztensen végezze el a Szervezet. A felmért biztonsági kockázatok elemzésének eredményét fontos az érintettekkel megismertetni, hogy kialakítható legyen a kockázattal arányos védekezés. Továbbá a kockázatelemzés az alapja a biztonsági osztályba illetve szintekbe sorolásnak is. A kockázatelemzést praktikusan az információ biztonságért felelős személy végzi / irányítja, a változó kockázatok miatt kétévente érdemes megismételni (az osztályba sorolást legalább három évente szükséges felülvizsgálni). Kritikus rendszerek esetében a felülvizsgálat gyakrabban ajánlott (évente), illetve nagyobb volumenű rendszerváltozás esetén szintén szükséges felülvizsgálni azt.

Ajánlott saját, testreszabott kockázatelemzési módszertan kialakítása, de elérhetőek nemzeti és nemzetközi jó gyakorlatok és keretrendszerek is. Ezekről és további részletekről a vonatkozó táblázatban található bővebb információ.

Fontos, hogy **a kockázatelemzés minden biztonsági osztályra vonatkozik!**

2.1.3 Rendszer és szolgáltatás beszerzés

Amennyiben a Szervezet igénybe vesz szoftvert, vagy informatikai szolgáltatást harmadik féltől, akkor annak beszerzése szabályozott keretek között kell, hogy történjen a biztonsági osztálytól függően (beszerzési eljárásrendre a 3-as biztonsági osztálytól van szükség). A beszerzéssel kapcsolatos elvárásokat, folyamatokat és felelősöket szabályzatban vagy eljárásrendben

szükséges rögzíteni - ez lehet az IBSZ is, de nagyobb szervezeteknek, ahol gyakoriak a beszerzések, ajánlott a különálló beszerzési szabályzat kialakítása.

Az informatikai rendszer, szolgáltatás beszerzése során különös figyelmet kell fordítani a biztonságra: elkülönített erőforrásokat kell biztosítani a beszerzési folyamatban, valamint a beszállító számára egyértelmű biztonsági követelményeket szükséges kialakítani, amelyek ellenőrizhetők.

Alapvetően a Rendelet célja, hogy ugyanazok a biztonsági elvárások vonatkozzanak harmadik féltől vásárolt informatikai rendszerekre, mint amelyek vonatkoznak egy esetleges saját fejlesztésre. Ezzel is megőrizve az informatikai rendszerek zártságát - hiszen hiába biztonságos 5-ből 4 saját fejlesztésű rendszer, ha az ötödik hiányosságait kihasználva sérülhetnek az adatok, incidensek történhetnek.

Előremutató gyakorlat: érdemes olyan szolgáltatót választani, aki rendelkezik valamilyen *harmadik fél által nyújtott* tanúsítvánnyal (pl. SOC1, SOC2, ISO 27001 stb.). Ezek a tanúsítványok biztosíthatják a Szervezetet arról, hogy a szolgáltatást nyújtó fél megfelel az adott keretrendszer biztonsági elvárásainak, alapvető kontrolljainak.

2.1.4 Üzletmenet (ügymenet) folytonosság tervezése

Az **üzletmenetfolytonosság alapvetően a váratlanra készít fel** - az üzletileg kritikus folyamatok esetleges kiesésére ad praktikus választ. A Rendelet eltérő típusú és mélységű elvárásokat fogalmaz meg az egyes biztonsági osztályokhoz. Ami viszont közös és 2-es biztonsági osztálytól minden szervezet által elvégzendő feladat: számba venni azon kritikus erőforrásokat (emberi, létesítmény, IT stb.) és folyamatokat, amelyek kiesése alapvetően akadályozná a szervezet fő célját, működését és ezek kiesésére átgondolt cselekvési tervet készíteni.

Az üzletmenetfolytonosság segítségével csökkenthető a felmért kockázatokból eredő, valamint a különböző valószínűségű események (pl. hacker támadás, social engineering támadás, pandémia, természeti katasztrófa) bekövetkezésének következményei. Az üzletmenetfolytonossági terv írja le azokat az eljárásokat, lépéseket, amelyek biztosítják, hogy bizonyos események bekövetkezésekor az alternatív folyamatok időben életbe lépjenek, majd a helyreállítás gördülékenyen történjen.

Az üzletmenetfolytonossági terv (BCP) elkészítése előtt készített Üzleti Hatáselemzés (BIA) és kockázatelemzés segít meghatározni azon üzleti folyamatokat amelyek kritikusak a szervezet számára és így BCP-t kell készíteni ezen folyamatokra.

2.1.5 A biztonsági események kezelése

A biztonsági események kezelését alapvetően 3-as biztonsági osztálytól várja el a Rendelet.

Biztonsági eseménynek számít minden olyan nem várt esemény vagy eseménysorozat, ami az EIR rendszerekben kedvezőtlen változást vagy ismeretlen helyzetet idéz elő és amely hatással van az EIR rendszerben található információk bizalmasságára, sértetlenségére, hitelességére funkcionalitására, vagy az az EIR rendszer rendelkezésre állására. Biztonsági esemény például az áramellátás ingadozása vagy megszűnése, adathalász e-mailek vagy túlterheléses támadás (DoS-támadás). A biztonsági események kezelésének teljes folyamatát, amely az előkészületektől, az esemény észlelésén, vizsgálatán, elszigetelésén és megszüntetésén át a helyreállításig tart, szabályzatban vagy eljárásban szükséges rögzíteni annak érdekében, hogy a biztonsági események kezelése időben és meghatározott folyamatot követve történhessen.

A biztonsági eseménykezelés folyamatát össze kell kapcsolni az Üzletmenetfolytonossági folyamattal, mivel az üzletmenetfolytonosságot veszélyeztető helyzetek a gyakorlatban biztonsági incidensekből alakulnak ki. Világos folyamatok és felelősségek meghatározása szükséges arra az esetre, amikor egy incidens már nem oldható meg és az Üzletmenet-folytonossági tervnek (BCP) kell életbe lépnie.

2.1.6 Emberi tényezőket figyelembe vevő - személy - biztonság

Köztudott tény, hogy információbiztonsági szempontból a "leggyengébb láncszem" az ember. Éppen ezért kell különös figyelmet fordítani a munkavállalók információbiztonsági képzésére, tudatosságára és figyelembe venni az *emberi tényezőt* amikor információbiztonságról beszélünk.

Az EIR-ek védelméhez a munkavállalóknak és a rendszerekkel kapcsolatba kerülő külső személyeknek is hozzá kell járulniuk. Ehhez a Szervezetnek szükséges kialakítania egy személybiztonsággal kapcsolatos eljárásrendet, ami kiterjed a munkakörök biztonsági

besorolására, valamint a jogosultságok ellenőrzésére, kezelésére. Fontos, hogy a kialakított folyamatok ne csak a jogosultságok megadására vonatkozzanak, hanem azokra az esetekre is, amikor a munkavállaló vagy külső fél munkakört vált a Szervezeten belül vagy pedig elhagyja azt. **Információbiztonsági kutatások szerint számos adatvesztés, biztonsági incidens jelenlegi vagy volt munkavállaló közreműködése által történik, éppen ezért fontos kiemelt figyelmet fordítani erre a területre.**

A munkavállalóknak a viselkedése az interneten, hogy milyen információkat oszt meg, milyen oldalakat látogat és milyen tartalmakat ér el, befolyásolhatja az EIR rendszerek és a Szervezet biztonságát. Az internetes viselkedési szabályokat a Szervezetnek belső szabályzatban kell meghatároznia - legalább az IBSZ egy fejezetét erre kell szánni.

2.1.7 Tudatosság és képzés

Az előző fejezettel (2.16) összhangban **kulcsfontosságú a munkavállalóink biztonságtudatosságának javítása.** Nem véletlen, hogy a Rendelet is külön alfejezetben tárgyalja ezt a területet.

Az EIR rendszer és a Szervezet biztonságát a munkavállaló nem csak az internet elővigyázatlan használatával veszélyeztetheti. A rosszindulatú támadók módszerei széles skálán mozognak, legyen szó akár social engineeringről (pszichológiai manipuláció) vagy egyszerű adathalász levélről. **Ha a munkavállalók tisztában vannak a támadási módszerekkel, felületekkel, akkor könnyebben tudják észlelni a gyanús tevékenységet.**

Az információbiztonsági tudatosság fenntartása, fejlesztése sokkal inkább egy folyamatos tevékenység mintsem egyszeri feladat.

A munkavállalók belépésekor egyszeri és a későbbiekben folyamatos (legalább évente javasolt), valamint a szerepkör szerinti biztonsági képzése elősegíti a munkavállalók biztonságtudatosságának növelését. A biztonságtudatossági képzés sokféleképpen történhet: lehet tantermi, online (e-learning), történhet játékos formában (gamification) és formalizáltabban is. Javasolt a különféle módszerek és tanulási technikák vegyítése. Amennyiben a Szervezeten belül nem áll rendelkezésre a megfelelő oktatói szakértelem, lehetséges a feladat kiszervezése, külső oktató igénybevétele.

2.2 Fizikai védelmi intézkedések

Az információbiztonság hármas céljából (adatok bizalmasságának, integritásának és elérhetőségének biztosítása) elsősorban az adatok elérhetőségét kívánja biztosítani a fizikai védelmi intézkedések.

A fizikai védelmi intézkedések biztosítják továbbá azt, hogy az elektronikus információs rendszereket alkotó eszközökhöz ne férhessen hozzá bárki és okozhasson károkat bennük, vihessen el információkat, vagy juttathasson be közvetlenül pl. rosszindulatú kódot. A fizikai védelmi intézkedések biztosítják továbbá a környezetből fakadó behatások minimalizálását (pl. tűz, beázás, áramkimaradás).

A fizikai védelmi intézkedések kiterjednek az épület, irodarészek és kiemelt fontosságú helységek védelmére.

A fizikai védelmi intézkedések nagy része praktikusan a szervertermek védelméről szól - így értelemszerűen, amely szervezet nem rendelkezik saját IT infrastruktúrával (pl. mert felhő alapon vesz igénybe IT szolgáltatást) arra nem vagy nem teljesen vonatkoznak az elvárások. Ugyanakkor ebben az esetben sem feledkezhet meg a Szervezet a fizikai védelmi kontrollokról. Már csak azért sem, mert gondoskodni kell az irodákban hozzáférhető munkaállomások, hálózati nyomtatók fizikai védelméről, továbbá a szolgáltatóval kötött szerződés útján a szolgáltató -szolgáltatásban érintett- hardver eszközei fizikai védelméről is - hiszen a feladatot kiszervezheti, de a felelősséget nem.

2.3 Logikai védelmi intézkedések

A **logikai védelmi intézkedések csoportjába a törvényalkotó szándéka szerint azon intézkedések tartoznak, amelyek az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal valósíthatók meg.** Elsősorban a számítógépes programokkal és az eszközökön futó protokollokkal, valamint eljárásrendekkel kialakított védelmi intézkedésekről van szó.

A három intézkedési csoport közül a logikai tartalmazza a legtöbb kontrollt, a számítógépes rendszereken alkalmazott szoftverek és kapcsolatok általános védelmi irányításától kezdve egészen a rendszer- és kommunikációvédelemig terjed. Ahogy az adminisztratív védelmi intézkedési csoportnál, itt is több "kontroll fejezetre" osztotta a Rendeletet alkotó a védelmi követelményeket. Az egyes fejezeteken belül igyekezett az egy rendszerre, illetve technológiai eszközre (pl.: adathordozók) vagy a hasonló típusú kontrollokra (pl.: konfigurációkezelés) helyezni a hangsúlyt, ezzel is segítve a megfelelő védelmi rendszer kiépítését.

Fontos megjegyezni, hogy az 1-es biztonsági osztályba sorolt elektronikus információs rendszerek tekintetében a logikai védelmi intézkedések csoportja nem értelmezhető, hiszen ebben az esetben a rendszer nem tartalmaz számítógépes, elektronikus megoldásokat. **Számos logikai biztonsági intézkedés csupán 3-as biztonsági osztálytól kezdve szükséges.**

Figyelem: a logikai védelmi intézkedések kötelező alkalmazását a Szervezet egyes elektronikus információs rendszereinek a bizalmasság, sértetlenség és rendelkezésre állás szerinti külön osztályozás dönti el!

2.3.1 Általános védelmi intézkedések

Az általános védelmi intézkedések fejezete a szoftverekre vonatkozó vagy szoftverekkel végrehajtható védelmi intézkedések irányításával foglalkozik. Ezen fejezet a hasonló típusú kontrollokkal megvalósítható védelmi intézkedéseket fogja össze, amelyek lényege a **szoftveres megoldásokkal végrehajtható utasítások integrálása az adminisztratív védelmi irányítás keretrendszerébe**. Tehát a logikai védelmi elvárások általános strukturálása a cél, melyet négy kontrollpont - az EIR kapcsolódásai, belső rendszerei, külső kapcsolódásaira vonatkozó korlátozások, valamint a személybiztonság - elvégzésével biztosíthat a Szervezet,

természetesen a Szervezet vezetője által elfogadott biztonsági osztályokra való alkalmazás figyelembevételével.

2.3.2 Tervezés

A Tervezés fejezet a teljes logikai védelmi intézkedési csoportra vonatkozó tervezési, előkészítési fázist jelöli. Ezen fejezet szintén a hasonló típusú kontrollokkal megvalósítható védelmi intézkedéseket fogja össze, amelyek célja írásba foglalni a rendszert felépítő, felülvizsgáló és módosító folyamatokat, valamint tudásanyagot, például a biztonságtervezési szabályzatot, a rendszerbiztonsági tervet, vagy szükség szerint az információbiztonsági architektúra átfogó leírását. Továbbá ez a fejezet tárgyalja a **Cselekvési terv**et, amelyet akkor kell készítenie egy Szervezetnek, amennyiben a biztonsági osztályba sorolásnál hiányosságot talál - pl. a kockázatok miatt 3-as osztályba kellene sorolnia az adott rendszert, de csak 2-es osztálynak felel meg.

Ezen dokumentumok megléte biztosítja a Szervezet számára a tervezhető folyamatok megismétlését, ellenőrzését és fejlesztését, amely elengedhetetlen a biztonságos működés megteremtéséhez. A Rendelet ezen védelmi fejezetet öt kontrollpont megvalósításával kívánja biztosítani a Szervezet számára.

2.3.3 Rendszer és szolgáltatás beszerzés

Ez a fejezet nem vonatkozik azon szervezetekre, amelyek nem szereznek be informatikai eszközt, szolgáltatás, továbbá meglévő informatikai rendszereiket nem fejlesztik.

A védelmi intézkedési fejezetek közül a rendszer és szolgáltatás beszerzés az, amelyik **a fejlesztés és beszerzés biztonsági aspektusai**val foglalkozik. Ez a kontrollcsoport minden olyan eshetőséget biztonsági szempontból vizsgál és azok számára követelményeket ír elő, amely bármiféle változást generál az EIR-ben. Az adminisztratív védelmi intézkedési részben is találunk hasonló nevű kontroll csoportot, amely a téma szabályozási, irányítási kérdéseivel foglalkozik. A logikai védelmi intézkedési részhez tartozó (ezen) fejezet, ahogy a logikai részben az összes további is, a **technikai jellegű védelmi tevékenységekre fókuszál**, az adminisztratív védelmi intézkedések által eljárásrendben/szabályzatban meghatározott folyamatokra, védelmi intézkedésekre ad megvalósítási példát.

Információbiztonsági szempontból az egyik legkritikusabb pont a rendszerek fejlesztése: a feladat természeténél fogva magas kockázattal jár, ezért fontos a logikai (hozzáférések kezelése, dokumentáció, oktatás stb.) védelmi intézkedések szigorú betartása és betartatása.

2.3.4 Biztonsági elemzés

Ezen fejezet a biztonsági ellenőrzések és értékelések csoportjába tartozó, elsősorban magas szintű szabályozási eljárásrendeket tartalmazó védelmi intézkedéseket foglal magában, alapvetően a 3-as osztálytól kezdődően.

Írásba foglaltatja a biztonság tesztelésének eljárásrendjét, technikáit és mérésének módszertanát. **Alapja a Szervezet jelen és jövőben várható kiber fenyegetettségi szintjének figyelembevételével kialakított értékelési terv, amely a kockázatok csökkentésére bevezetett kontrollok hatékonyságát, eredményességét méri.** Az ellenőrzés és mérési módszertan pontos folyamatleírása és további fejlesztési lehetőségeinek feltárása szintén ezen fejezet keretein belül valósul meg. A valósághű tesztelés érdekében a kontrollok közül a Speciális értékelés (4-es szinttől) nevű előírás egy a Szervezet által szimulált rosszindulatú támadást is tartalmaz, amely alapján könnyebben felderíthetők a gyenge, potenciális támadási felületek. A négy védelmi intézkedésből álló fejezet célja, hogy a Szervezet előre definiált, átlátható, ezáltal fejleszthető módon végezhesse a saját biztonságára vonatkozó elemzési, értékelési tevékenységét.

2.3.5 Tesztelés, képzés és felügyelet

Ezen védelmi intézkedéseket magában foglaló fejezet az elektronikus információs rendszerelemekre és az azokon futó alkalmazásokra (hardver és szoftver egyaránt) vonatkozó biztonsági teszteléssel, és megerősítéssel foglalkozik. **A hasonló típusú kontrollok célja a gyenge pontok feltárása és célzott megerősítése, amely által a jövőbeni lehetséges támadó nem, vagy csak sokkal nagyobb erőfeszítések árán érheti el a védett információkat, rendszereket.** A potenciális támadási felületek felderítése érdekében a Szervezet ezen kontroll fejezet alapján saját magára vonatkozó **sérülékenységi teszt**et is végezhet, ami a megfelelő képességek birtokában akár belső erőforrásból, azok hiányában pedig külső erőforrás bevonásával is megvalósítható. A vizsgálat elvégzésének gyakorisága a Szervezet saját szabályzataitól függ,

illetve minden esetben ajánlott, ha a saját EIR-re vonatkozó új típusú sérülékenységről szerez tudomást. A viszonylag alacsony erőfeszítéssel megszerezhető információk és módosítható rendszerelemekről és konfigurációkról lista készül, amely segíti a védelmi potenciál célzott javítását.

Fontos kiemelni, hogy az ICS (ipari) rendszerrel rendelkező szervezetek számára a tesztelések végrehajtása különösen nagy körültekintést igényel!

2.3.6 Konfigurációkezelés

Az elektronikus információs rendszerek és rendszerelemek, valamint az azokban kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának is **kulcsfontosságú eleme a jól beállított, biztonsági szempontból is kezelt konfigurációk megléte és folyamatos biztosítása.** A Konfigurációkezelés nevű védelmi intézkedési fejezet a fenti problémakör tervezett, szabályozott és felügyelt, valamint továbbfejlesztett végrehajtására kíván formalizált teret adni. A rendkívül sokrétű konfigurációkezelés sikerességének alapvető eleme a dedikált eljárásrend, amely értelmezési keretet ad a tevékenységek tervszerű alkalmazására és meghatározza azokat az eseteket, amikor a beállítások biztonsági szempontból történő ellenőrzését mindenképpen vagy ajánlott módon kell elvégezni. A konfiguráció kezelés alapja, hogy naprakész információval rendelkezzen a szervezet az egyes infrastruktúra elemek konfigurációjáról. Ez **lehet például erre a célra kialakított konfigurációmenedzsment adatbázis (CMDB).**

A konfigurációk naplózása, megőrzése, elemzése és változásának pontosan dokumentált rögzítése szintén ezen fejezethez tartozik, amellyel a rendszert érintő bárminemű biztonsági beállításban bekövetkezett változásának megléte később az esetleges incidensek kivizsgálásakor elengedhetetlen támogatást nyújt a szakembereknek. **Hiába van a piacon elérhető legfejlettebb biztonsági rendszerünk, ha annak releváns beállításai/konfigurációi hibás működést eredményeznek.**

2.3.7 Karbantartás

A Karbantartás elnevezésű fejezet célja, hogy a rendszert és azok elemeit ütemezett módon, a szabályzatoknak és előírásoknak megfelelően, valamint dokumentálva tartsák karban,

miközben a folyamat minden lépésénél biztosítják a Szervezet által megkövetelt biztonsági előírások teljesülését. A távoli karbantartás illetve a külső helyszínen végzett karbantartás biztonsági kockázatainak kezelése és pontos feljegyzése szintén ezen fejezet intézkedéseinek feladata.

A karbantartás (üzemeltetés) jellegénél fogva magas kockázatú tevékenység, hiszen különös jogosultságú (privilegizált) felhasználók vesznek részt a folyamatban, valamint a rendszer normál ügymenetétől eltérő feladatokat hajtanak végre. Éppen ezért különösen fontos az egyértelmű és pontos szabályzatok megfogalmazása, és azok betartatása.

2.3.8 Adathordozók védelme

Az adathordozók (pl.: pendrive, külső merevlemez, CD-DVD, okos eszközök, SD kártya, telefon) védelme fontos a Szervezet számára, hogy ne szivároghasson ki információ sem véletlenül, sem szándékosan, valamint ne kerülhessen be a Szervezethez rosszindulatú kód, információ (pl.: zsarolóvírus).

Az adathordozók védelmére vonatkozó eljárásrendben szükséges rögzíteni az adathordozók kezelésének folyamatát, valamint azokat a védelmi intézkedéseket, amelyek megakadályozzák a fentieket. A **gyakorlatban ez azt jelenti**, **hogy különböző adminisztratív** (pl.: csak engedéllyel, felettesi jóváhagyással lehet adathordozót használni) **és logikai / technikai** (pl.: Jelszóval védett pendrive, titkosított merevlemezek) **védelmi intézkedésekkel kell biztosítani az adathordozók védelmét.**

Fontos, nem elég a Szervezet adathordozóit védeni, de a munkavállalók eszközeit (jellemzően saját mobiltelefon) is érdemes ellátni bizonyos védelmi eszközökkel, főleg ha elérik rajta a vállalati infrastruktúrát, levelezést.

2.3.9 Azonosítás és hitelesítés

Az azonosítás és hitelesítés célja, hogy az elektronikus információs rendszerekhez és erőforrásaikhoz csak olyan személyek férhessenek hozzá, akik megfelelő jogosultsággal rendelkeznek. Ehhez a Szervezet számára szükség van egy eljárásrendre, amelyben rögzíti, azt, ahogyan kezeli az azonosítókat (hogyan rendeli a felhasználókat a munkavállalókhoz és hogyan

kezeli a későbbiekben azt), milyen hitelesítési módszereket alkalmaz (pl.: többlépcsős azonosítás, távoli hozzáférés esetében fizikai token stb.), illetve azokat hogyan ellenőrzi. Az azonosítás és hitelesítés kiterjed a hálózati hozzáférésekre és a helyi hozzáférésekre is.

2.3.10 Hozzáférés ellenőrzése

A hozzáférések ellenőrzése teszi lehetővé, hogy időben észlelhető legyen, ha olyan személy fér hozzá az elektronikus információs rendszerekhez, akinek nincs arra jogosultsága. A hozzáférések ellenőrzése már a megfelelő jogosultság kiosztásnál, illetve a kiosztott ideiglenes és állandó hozzáférések megfelelő gyakoriságú ellenőrzésénél elkezdődik. Fontos, hogy amennyiben lehetséges, akkor a felhasználók rendszer tevékenysége naplózva legyen, legalább privilegizált felhasználók szintjén. Ez segíti az auditálhatóságot, illetve a visszakövetést.

Az információbiztonság egyik alapja a megfelelő hozzáféréskezelés, a jól kidolgozott jogosultság-menedzsment. A fejezet célja, hogy a Szervezetek megfelelő kontrollokkal fedjék le ezt a területet, a jelszóbeállításoktól kezdve a többlépcsős azonosításon át a kiemelt felhasználók kezeléséig.

2.3.11 Rendszer és információ sértetlenség

Ezen fejezet a teljes elektronikus információs rendszer védelmi potenciáljának ellenőrzésére, megtartására és fejlesztésére szolgáló intézkedéseket foglalja magában. **A Szervezet kizárólag abban az esetben mentesül a felelősség alól, ha jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltatót, illetve központi adatkezelőt és adatfeldolgozó szolgáltatót vesz igénybe**. Egyéb esetekben szerződéses kötelemként kell rögzíteni. Az azonos céllal bíró, de különböző élőerőt és szoftveres alkalmazásokat előíró kontrollok segítségével a biztonságos állapotot fenntartó védelmi intézkedések frissessége, helyes beállítása és naprakész információval való ellátása hajtható végre. A folyamatosan változó kiberfenyegetési környezet a szervezetnél üzemeltetett elektronikus rendszerre és az azokban tárolt információk sértetlenségére van hatással, amelyet ezen fejezet hivatott megvédeni.

2.3.12 Naplózás és elszámoltathatóság

A fejezet célja az elektronikus információs rendszerben és akörül történt események pontos nyomon követése érdekében, hogy a rendszer az előre meghatározott módokon rögzítsen minden előre definiált tevékenységet. Ezen elvárások az azonos típusú védelmi intézkedésekkel elvégezhető tevékenységek közé sorolhatók, amelyek az incidensek felderítésére és kivizsgálására adnak lehetőséget a szakemberek számára. A naplózás az elszámoltathatóság egyik legjobb eszköze, amit ennél fogva, az adott technológiai kereteket figyelembe véve minél szélesebb körben és minél mélyebben érdemes végezni. A bejegyzett információk valós idejű és késleltetett elemzésére dedikált szoftverrendszerek és személyek rendelhetők, így biztosítva az értékes információ kinyerését az adathalmazból.

2.3.13 Rendszer- és kommunikáció védelem

Ezen védelmi intézkedési fejezet a teljes elektronikus információs rendszer és az azon keresztül vagy általa megvalósított elektronikus kommunikáció technikai jellegű védelmi tevékenységeit részletezi. Az eltérő típusú kontrollokkal megvalósítható védelmi intézkedések az egy rendszerre és folyamatra irányuló kontrollok kategóriájába esik. Mind a rendszer és annak hardver elemei, mind a szoftver és az azok segítségével tárolt és továbbított adatok és információk a fejezet tárgyát képzik.

2.4 Eltérések alkalmazhatósága

A 41/2015 BM rendelet bizonyos, a Rendeletben részletesen vázolt körülmények fennállásakor lehetőséget biztosít a védelmi intézkedési katalógusban feltüntetett kontrolloktól meghatározott szinten való eltérésre a szervezetek számára. Az úgynevezett eltérések alkalmazására a Rendelet alapjául szolgáló 2013/L.törvényben foglalt alapelvek vonatkoznak, s azokat minden esetben ezen alapvetések figyelembevételével érvényesítheti a Szervezet.

A Rendeletben is hivatkozott “high water mark” elv a gyakorlatban alátámasztja a legmagasabb biztonsági szükséglet kielégítésére vonatkozó törekvések megkerülhetetlenségét abban az esetben, ha az a kockázatarányos védelem elvével összeegyeztethető. **Ez a valóságban azt jelenti, hogy abban az esetben, ha a Szervezet saját kockázatfelmérése alapján egy bizonyos**

kockázat alacsonyabb szinten lévő biztonsági kontrollal kezelhető, akkor nem szükséges a leginkább védendő rendszerelem magasabb rendű védelmi intézkedését alkalmazni rá. Tehát például egy szervezet legerősebben védendő értékének biztonságát szavatoló intézkedéseket nem kell azonos szinten megvalósítani egy jóval kevésbé fontos, egyébként is nehezen támadható rendszerelemnél. Természetesen ennek érvényesítésére, ahogy az eltérések valamennyi formájában, a Rendeletben foglalt körülmények és kötelezettségek meglétét és maradéktalan betartását várja el, és különösen rávilágít a megfelelő és alátámasztott kockázatelemzési folyamat kiemelt szerepére.

Fontos megjegyezni, hogy habár a jogalkotó a fentiek alapján lehetőséget biztosít az eltérések alkalmazására, azonban a biztonság tekintetében különösen igaz a mondás, miszerint **a rendszer csak olyan erős, mint a leggyengébb láncszeme.** A bizalmasság, a sértetlenség és a rendelkezésre állás az elektronikus információs rendszerek, azok elemei és az azokban kezelt adatok és információk összességére vonatkozó, gyakorlatban is érvényesíthető fogalmak, amelyek mentén kialakított védelem nemcsak a törvényi és jogszabályi megfelelést, hanem a valódi védelmet is nagymértékben növeli. Ezeket is figyelembe véve, csak valóban indokolt esetekben ajánljuk az eltérések alkalmazását.

2.5 Helyettesítő biztonsági intézkedések alkalmazhatósága

Alapelv szerint helyettesítő biztonsági intézkedést egy Szervezet kizárólag abban az esetben alkalmazhat, ha a 41/2015 BM Rendeletben az adott biztonsági osztálynál eredetileg **meghatározott védelmi kontrollal minimum azonos szinten és hatékonysággal képes ellátni védelmi feladatát az alternatív megoldás alkalmazásával.** Fontos alkalmazhatósági kritérium továbbá, hogy törvényi megfelelésnek és a Szervezet saját belső szabályzatainak nem lehet akadálya a helyettesítő intézkedés alkalmazása, tehát mindenképpen meg kell felelnie az említett szabályozókban leírtaknak.

A Rendelet kiköti, hogy melyek azok a feltételek, amelyeknek általánosságban teljesülniük kell az EIR védelmére használt alternatív biztonsági megoldások alkalmazhatóságánál:

- az EIR védelmére vonatkozó szabványban vagy hazai ajánlásban fellelhető vagy ennek hiányában a célnak megfelelő egyéb védelmi intézkedést alkalmazhat csupán,

- a Szervezetnek elsősorban a védelmi intézkedési katalógusból kell választania alternatív megoldást, ha ez nem lehetséges, akkor csak végső esetben lehet azoktól eltérő intézkedést foganatosítania,
- amennyiben alternatív védelmi kontrollt vesz igénybe, akkor a Szervezetnek részletesen be kell mutatnia, hogy ezt miért teszi és azt is, hogyan fog megfelelni a helyettesítő intézkedés az eredeti célnak,
- az előző pontban leírt indoklásnak a biztonsági követelményszint szerinti részletezettséggel és szigorúsággal kell bírnia,
- a Szervezetnek fel kell mérnie és el kell fogadnia a helyettesítő intézkedés alkalmazásából fakadó lehetséges egyéb kockázatokat is, valamint
- a teljes folyamatot dokumentálni szükséges és jóváhagyatni az illetékes személlyel.

A Rendeletben meghatározott védelmi intézkedések hármas tagolása alapján az adminisztratív és fizikai védelmi intézkedésekre a gyakorlatban meglehetősen nehezen találni alternatív védelmi megoldást, azonban **a logikai védelmi intézkedések tekintetében már jóval egyszerűbb és adott esetben célszerűbb lehet helyettesítő megoldás használata.** A Szervezetnek saját magára és elektronikus információs rendszerei vonatkozó kockázatelemzése alapján kell eldöntenie, hogy az alternatív megoldás az adott előírásnak jobban megfelel-e, mint a Rendeletben előírt kontroll. Ez legtöbb esetben a rendszer speciális jellemzőin vagy a rendeltetési helyszín különleges tulajdonságain múlik.

Jelen Kézikönyv kiegészítéseként elkészített védelmi intézkedési katalógus táblázatban külön dedikált részben találhatók az egyes kontrollok esetén szükség esetén alkalmazható helyettesítő védelmi intézkedésekre vonatkozó gyakorlati tanácsok.