Magyar Rendészet 2019/2–3. 233–249. DOI: 10.32577/mr.2019.2-3.12

Fizikai biztonsági kontrollok tervezésének és alkalmazásának gyakorlata az ISO/IEC 27001 szabvány elvárásainak tükrében

TISZOLCZI Balázs Gergely[1]

Az információ és az információs rendszerek megfelelő védelme körültekintő tervezést és számos kontroll implementálását igényli a vállalkozások részéről, amelynek sok esetben valamely információbiztonsági keretrendszer, legtöbbször az ISO/IEC 27001 nemzetközi szabvány bevezetésével tesznek eleget. A szabvány rendelkezései közt hangsúlyosan foglalkozik többek közt az információs rendszerek fizikai védelmének kialakításával. Jelen tanulmány olyan tervezési, üzemeltetési megfontolásokat tárgyal, amely segíthet, hogy a felelős szakemberek a szabvány elvárásainak megfelelő fizikai biztonsági rendszereket hozzanak létre.

Kulcsszavak: *fizikai biztonság, szabvány, 27001, tervezés*

Bevezetés

Napjainkban az információ az egyik olyan vagyonelem, amely szektortól és tevékenységi körtől függetlenül minden vállalkozás működésében kiemelt szerepet tölt be, és hasonlóan más fontos vagyontárgyhoz, megfelelően védeni kell. Ez különösen igaz az egyre inkább egymással összekapcsolódó, dinamikusan változó, az új technológiák gyors implementációs kényszerében lévő üzleti környezetben, ahol az információ folyamatosan növekvő számú és széles körű fenyegetésnek van kitéve. A megfelelő biztonságot számos intézkedés együttes alkalmazásával érhetjük el, beleértve a védelmi célt szolgáló szabályzatokat, folyamatokat, eljárásokat, biztonságtechnikai eszközöket, informatikai rendszerek esetében pedig bizonyos szoftver- és hardverfunkciókat.[2]

Az összetett feladatrendszer indokolhatja, hogy a védelemhez szükséges kontrollok tervezését, implementálását és működtetését a vállalkozás komplex szemléletben, valamely információbiztonsági keretrendszer bevezetésével támogassa. Ezen célra az (MSZ) ISO/IEC 27001 nemzetközi szabvány (továbbiakban: szabvány) bevezetésének egyik

[1] TISZOLCZI Balázs Gergely dr., PhD, CISM, CEH, tanársegéd, NKE Rendészettudományi Kar Magánbiztonsági és Önkormányzati Rendészeti Tanszék
Gergely Balázs TISZOLCZI PhD, CISM, CEH, assistant lecturer, NUPS Faculty of Law Enforcement
https://orcid.org/0000-0001-6708-0138, tiszolczi.balazs@gmail.com

[2] MSZ ISO/IEC 27002 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve. 22.

előnye azon túl, hogy egységes keretbe foglalja az információ védelméhez szükséges feladatokat, elismerhető módon bizonyítja, hogy a szervezet megfelel a tevékenységében érintett felek (szabályozó szervek, üzleti partnerek, magánszemélyek stb.) információvédelemre vonatkozó elvárásainak is.

A szabvány A11 Fizikai és környezeti biztonság fejezete ismerteti azokat a fizikai biztonsági kontrollokat, amelyek célja az információfeldolgozó rendszerek védelme érdekében biztosítani többek közt a fizikai határok kialakítását, a szükséges beléptetési intézkedéseket, a külső fenyegetések elleni védelem megvalósítását, a biztonsági területeken történő munkavégzés szabályainak meghatározását, a közműszolgáltatások folytonosságát.

A fizikai biztonsági intézkedések elsődleges funkciója, hogy az információhoz vagy az információfeldolgozó eszközökhöz[3] történő jogosulatlan hozzáférést megakadályozza, jelezze annak kísérletét, biztosítson információt a hozzáférések lényeges jellemzőiről (idejéről, módjáról, az érintett személyekről), és tegye a szervezetet ellenállóbbá a külső környezeti fenyegetésekkel szemben. Ennek megvalósítására a gyakorlatban élőerős őrzés-védelem, elektronikus beléptető és megfigyelő rendszerek, behatolásjelző berendezések, a környezet jellemzőit felügyelő szenzorok, mechanikai biztonságtechnikai megoldások, automata tűzjelző- és oltórendszerek alkalmazásával, szabályozási intézkedések bevezetésével, vészhelyzeti tervezés biztosításával és a felhasználók oktatásával, képzésével kerül sor.

Hatékonyságuk ellenére ezen eszközök és módszerek sok esetben csak másodlagos fontossággal bírnak, amikor az információvédelmi kontrollok tervezéséről, implementálásról van szó. Ennek oka, hogy a gyakorlatban – dacára az információ számos megjelenési formájának – erősen IT-technológia-orientált az adatok[4] védelme.[5] Az elektronikus formán túl azonban biztosítani kell többek közt a papíralapú és a szóban elhangzó információk védelmét, amelyet informatikai eszközökkel nem, vagy nem teljes mértékben lehet megvalósítani. Egyes információfeldolgozó rendszerek, vagy a működtető infrastruktúra elleni támadási módokat[6] sem lehet végrehajtani az eszközökhöz történő fizikai hozzáférés nélkül (szabotázs, rongálás, eszközök hálózatra történő csatlakoztatása, lehallgató berendezések telepítése), de a legjobban tervezett hálózati védelmi megoldások is könnyedén megkerülhetők fizikai biztonsági kontrollok hiányában. A vírusok ugyanis az e-mail-csatolmányokon túl szeretnek mobil adathordozón is terjedni, a felügyelet nélkül hagyott számítógépek fizikai csatlakozási lehetőségei ideálisak egy keylogger[7] telepítésére, egy live CD-vel már meg is van az offline töréshez

[3] Az MSZ ISO/IEC 27002 szabvány alapján információfeldolgozó eszköz bármely információfeldolgozó rendszer, szolgáltatás vagy infrastruktúra, továbbá a fizikai helyek, amelyek befogadják azokat.

[4] Bár különbség van az adat és az információ fogalmi értelmezésében, a cikk keretein belül a szavakat egymással felcserélhető módon használom.

[5] Hutter (2016) 1.

[6] Ebben a tekintetben a támadás alatt nemcsak az adatok bizalmasságát veszélyeztető akciókat kell érteni, hanem minden olyan fenyegetést is, amely a rendszer megbízható működését, ezáltal az adatok rendelkezésre állását veszélyezteti. Tervezés az IT biztonság szempontjából (2008) 20.

[7] Keylogger: a felhasználói billentyűzet leütéseket rögzítő és egyes esetekben továbbító, hardveresen vagy szoftveres úton megvalósított alkalmazás.

szükséges jelszóhash, egy lezáratlan gép esetén akár a távoli hálózati elérést biztosító VPN-beállítások is megszerezhetők. A belépések korlátozása nélkül egyes nem túl kifinomult, és egyszerűen alkalmazható social engineering módszerek (shoulder surfing,[8] dumpster diving[9]) alkalmazásával megszerezhetők a felhasználók azonosítói, de a területen jogosulatlan tartózkodás sokszor ezen megfigyelési technikák alkalmazása nélkül önmagában elegendő az azonosítók megszerzésre, ha a felhasználók nem a szabályoknak megfelelően tárolják azokat (cetlik naptárakon, monitorokon stb.).

A fizikai biztonsági és az informatikai jellegű kontrollok (kiegészülve természetesen más, ugyanilyen fontos adminisztratív kontrollokkal) egyenértékű szerepet töltenek be az információk védelmében, azt megfelelően garantálni csak a módszerek optimális arányú kombinálásával, együttesen lehet. Jelen írásnak nem célja tételesen ismertetni a szabvány fizikai biztonságára vonatkozó követelményeit, sokkal inkább olyan sok éves szakmai és audittapasztalatokon alapuló tervezési, üzemeltetési megfontolásokat tárgyal, amely segíthet, hogy a fizikai biztonság tervezéséért felelős szakemberek a szabvány elvárásainak, de ami talán fontosabb, szellemének megfelelő, integrált, könnyen üzemeltethető fizikai biztonsági rendszereket hozzanak létre, a kontrollok közti minél jobb szinergiák és összefüggések felismerésével és kihasználásával pedig hozzájáruljanak az információbiztonsági erőfeszítések hatékonyságához.

Napjaink trendjei

A kontrollok tervezését, az alkalmazandó megoldások kiválasztását napjainkban számos olyan globális trend befolyásolja, mely iparágtól és vállalati működéstől függetlenül alapjaiban befolyásolja a biztonsági szakemberek lehetőségeit, nagyfokú alkalmazkodási kényszert és szemléletmódváltást követel az érintettek részéről.

A fizikai biztonsági eszközöket és megoldásokat sem kerülheti el a digitális transzformáció, a rendszerek és hálózatok konvergenciája, aminek hatására az információáramlás gyorsabbá, a beavatkozások automatikussá válnak. A védendő technológiák felhőbe költöztetésének, a gépi tanulásnak és a fejlett arcfelismerő megoldásoknak köszönhetően csökken a helyszíni fizikai biztonsági (élőerős, technológiai) igény, megjelennek a PSaaS[10] megoldások. A kamerákban alkalmazott analitika megváltoztatja az érzékelés módját, távolságát, egyszerre biztosít többek közt behatolás-érzékelést, tárgyvédelmet, kiváltva jónéhány klasszikus eszköz funkcióit. A személyfelismerés már annyira fejlett, hogy akár az információfeldolgozó eszközökhöz történő multifaktoros autentikáció egyik eleme is lehet, továbbá autorizációs intézkedések tervezésére is alkalmas, fontos és felismerendő integrációs lehetőséget biztosítva a szakemberek számára.

---

[8] Magyarul kifigyelés, közvetlen megfigyelési technika, szó szerint valaki válla fölött történő információszerzés. Forrás: https://hu.wikipedia.org/wiki/Kifigyelés (2019. 08. 22.)

[9] Hulladékból történő információgyűjtés.

[10] Physical Security as a Service, fizikai biztonság mint (felhőalapú) szolgáltatás.

A fejlesztések egy része azonban nemcsak biztonságunk növelésére szolgál, hanem ezekkel vagy ezeken keresztül újabb támadásoknak lehetünk kitéve.[11] A fizikai biztonsági védelmi rendszerben alkalmazott technikai eszközök jelentős része gyakorlatilag az informatikai kiszolgáló és kliensrendszerekre jellemző, hálózati csatlakozásokkal, kommunikációs protokollokkal, felhasználói interfészekkel, menedzsmentlehetőségekkel, és az azokra jellemző veszélyeztetettséggel rendelkezik, ezért esetükben ugyanazon IT-biztonsági képességek megléte és alkalmazása indokolt.

A vállalkozások működésére nagyban jellemző, hogy az információ tárolása, vagy az ahhoz történő hozzáférés decentralizált módon, hordozható eszközök segítségével történik, a távmunkavégzés, a vállalati adatokat (is) tartalmazó mobil kommunikációs és informatikai eszközeink ma már mindennapunk részei. Az eszközök vállalati fizikai határok alól történő kikerülése a technológiának köszönhetően már régóta nem jelenti azt, hogy az eszközkontrollnak is ki kell kerülnie a biztonságirányítás alól, azonban a 2018. május 25-én hatályba lépett GDPR[12] előírásai okán erősebben jelent meg követelményként a fizikai biztonsági tervezésben a „privacy", azaz a személyes adatok védelme, és a hozzájuk kapcsolódó érintetti jogok biztosítása. Legjellemzőbb példa erre a manapság divatos BYOD[13]-irányzat, ahol igen körültekintően kell alkalmazni az egyes kontrollokat, különösen a készülék fizikai lokációját meghatározó, úgynevezett trackeralkalmazásokat, vagy elvesztés esetén a távoli adattörlési megoldásokat, illetve a személyiségi jogokra tekintettel szükséges lennünk a készülékek ellenőrzésénél, és az adathordozók fizikai megsemmisítésénél. A mobil, sokszor saját tulajdonú eszközök megfelelő kezelésén túl további feladat az elektronikus biztonságtechnikai rendszerek jogszabályoknak megfelelő személyes adatkezelésének biztosítása. A 2005. évi CXXXIII. törvény (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 esetén. Az adminisztratív „korlátozások" mellett azonban a GDPR bizonyos eljárásokban, mint például az incidensmenedzsment, nagyobb mozgási teret is ad számunkra, az SzVMt. elektronikus megfigyelő rendszerekre korábban érvényes három napos adatkezelési határidejével ellentétben érdekmérlegelési teszt alapján már 30-60 nap is indokolt lehet, megnövelve ezzel a vizsgálati eljárások sikerének valószínűségét.

Napjaink ezen jellemző trendjei azt jelentik, hogy a fizikai biztonsági kontrollok helyes és időtálló gyakorlatba ültetéséhez a szakembereknek új(abb) kompetenciákat szükséges szerezni, új megfontolásokat szükséges figyelembe venni a rendszerek tervezése során. A technikai ismeretek iránya eltolódik, egyre inkább előtérbe kerül az informatika, azon belül is kiemelten a hálózatismeret és az informatikai biztonság. A GDPR hatály-

[11] Tóth L. (2018) 35–44.
[12] GDPR: Európai általános adatvédelmi rendelet.
[13] BYOD: Bring Your Own Device, azaz saját eszközök használata a vállalati feladatok elvégzéséhez.

balépése és a felhőtechnológiák növekvő számú igénybevétele miatt megváltozik az ellenőrzés és a megfelelőség értékelésének módszere, előtérbe kerülnek a jogi, szervezési és compliance ismeretek, a hagyományos biztonságszervezési gyakorlat nem feltétlenül lesz elegendő a megfelelő intézkedések kialakításához. A BYOD és a távmunka elterjedése miatt kiemelt feladat hárul a felhasználókra az információk védelmében, az ő tudatosságuk, felkészültségük e téren kritikus fontossággal bír a védelmi rendszer sikerességében. A biztonsági szakembereknek jártasságot kell szerezniük a tudatossági képzések elméletében, a technikák alkalmazásában, hogy ismeretátadással minél jobban képesek legyenek támogatni a felhasználókat a szükséges intézkedések végrehajtásában.

A kontrollok tervezése, a vonatkozó követelmények azonosítása

A szabvány lényeges elvárásként fogalmazza meg, hogy az információvédelem tekintetében a szervezetnek fel kell mérnie az érdekelt felek elvárásait és meg kell felelnie azoknak. A vállalati gyakorlatban jellemző érdekelt felek a munkavállalók, a szolgáltatást igénybe vevők, a beszállítók, és tágabb értelemben a társadalom, amelynek elvárásait a jogalkotó jogszabályok formájában fogalmazza meg. Jogi normákban megfogalmazott fizikai biztonsági kontrollokra vonatkozóan számos példa akad, a 2013. évi L. törvény és végrehajtására kiadott rendelet az állami és önkormányzati szervek elektronikus információbiztonságához kapcsolódóan ír elő konkrét követelményeket, míg a 42/2015. (III. 12.) Korm. rendelet és a 7/2017-es MNB ajánlás a pénzügyi szervezetek, biztosítók tekintetében teszi ugyanezt. A 42/2015 (III. 12.) Korm. rendelet által előírt kötelező zártsági ellenőrzés alapját az NIST[14] 800-53 rev4 kontrolljai képezik, míg minősített adatkezelés esetében a minősített adat védelméről szóló 2009. évi CLV. törvény és a végrehajtására kiadott rendeletben foglalt előírások alkalmazása kötelező. A szervezetnek a jogi kötelezettségeken túl azonosítania kell a szerződéses kapcsolatokban vállalt, és az egyes vagyonbiztosítások fizikai biztonsággal összefüggő követelményeit és gondoskodni azok végrehajtásáról.

A fentiekben megfogalmazott elvárások keretében a fizikai biztonsági kontrollok tekintetében (is) a védendő információs vagyon értékével arányos, kockázatelemzésen alapuló megoldások implementálása jellemző, azonban a szabványnak még számos, további explicit és implicit követelményét szükséges ezen a területen is kielégíteni, úgy, mint az életvédelem figyelembevétele, a kapacitásmenedzsment, az erőforrások prediktív felügyelete, a folyamatos fejlesztés, fejlődés fenntartása, valamint a védelmi intézkedések folyamatossága. A fizikai biztonság tervezésénél is értelmezhető a jól ismert „defense in depth", avagy a mélységi védelem, és szintén érvényes alapelv a „need to know" és a „need to do", amelyet úgy is fordíthatnánk, hogy a fizikai kontrollok kialakításával, módosításával, felügyeletével kapcsolatos jogosultságok a lehető legszűkebb részre korlátozódjanak, illetve az információfeldolgozó, információhordozó eszközökhöz, az azoknak helyet adó területekhez a hozzáférést a lehető legszükségesebb mértékre csökkentsük.

[14] National Institute of Standards and Technology.

Hozzáférés-felügyelet

Műszaki intézkedések tervezése

A szabvány fizikai biztonsági intézkedéseinek talán legfontosabb funkciója, hogy az információhoz és az információfeldolgozó eszközökhöz történő jogosultalan hozzáférést korlátozza. A fizikai biztonsági rendszer ezen funkciójában – jellegéből adódóan – akkor lehet igazán hatékony, ha még a végleges alaprajzi elrendezés kialakítása előtt megismerjük és érvényesítjük a lényegesebb tervezési alapelveket, amelyek közül a legfontosabbak:

- Az információbiztonság szempontjából kulcsfontosságú eszközöket és azok működését biztosító technológiákat befoglaló helyiségeket (géptermek, irattár, UPS, aggregátor helyiség stb.) úgy kell elhelyezni a létesítményen belül, hogy csökkentse az illetéktelen hozzáférés lehetőségét, nyújtson védelmet a telepítési környezetre jellemző (technológiai vagy környezeti katasztrófák), továbbá az épületüzemeltetésből és használatból származó kockázatok ellen (vízbetörés, szándékolatlan villamos leválasztás, tűzveszélyes technológia stb.).[15] A kültéren elhelyezett berendezések telepítésénél (például klíma kültéri egységek, aggregátor stb.) szintén törekedni kell a helyszín adottságaiból származó, lehető legvédettebb elhelyezésre.
- Biztosítani kell, hogy a kockázatértékelés alapján meghatározott, különböző biztonsági szintű területek (védelmi zónák) megfelelően el legyenek választva egymástól, az üzletmenet-folytonosság szempontjából fontos rendszer vagy technológia, továbbá a zárt területen elhelyezett számítóközpont nem érintkezhet nyílt területtel vagy közterülettel,[16] az eltérő védelmi zónák bejárata csak egy kategóriával alacsonyabb zónából nyílhat. Célszerű megoldás, ha azonos védelmi osztályba sorolt helyiségek egy védelmi zónában vannak.[17] A megoldás előnye, hogy a védelemhez szükséges eszköz és rendszerigény a lehető legkisebbre csökken, egyszerűsödik a beléptetőrendszerek jogosultsági csoportjainak tervezése, elkerülhetők a zónák közti szükségtelen átjárások.
- A menekülésre, mentésre vonatkozó szabályok betartásával a munkavállalói, vendég és beszállítói forgalmat, belépéseket a lehető legkevesebb pontra tervezzük, úgy, hogy lehetőségünk legyen meggyőződni a belépés jogosságáról, a szükséges ellenőrzések elvégzéséről.
- A szállítási és tárolási területeket úgy tervezzük, hogy a szállítmányokat le lehessen rakni anélkül, hogy a szállító személyzet hozzá tudjon férni az épület más részeihez.[18]

[15] Tervezés az IT biztonság szempontjából (2008) 23.
[16] Tervezés az IT biztonság szempontjából (2008) 23.
[17] Vasvári (2006) 45–47.
[18] MSZ ISO/IEC 27002 *Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve.* 51.

- A vendégeket lehetőség szerint ne az irodákban, hanem erre dedikált tárgyalóban fogadjuk, ahol közvetve sem lehetnek fültanúi üzleti vagy egyéb megbeszélésnek, prezentációknak. A tárgyaló(k) és a hozzájuk tartozó szociális helyiségek elhelyezését úgy szükséges tervezni, hogy a szervezethez érkezőknek lehetőség szerint csak az épület számukra lehető legszükségesebb részein kelljen tartózkodniuk. A fizikai elhelyezéssel korlátozni kell azon helyszínek hozzáférését, ahol szenzitív információkról rendszeresen tárgyalhatnak.
- A papíralapú információk védett elhelyezésének biztosítására alakítsanak ki irattárakat, az irodaterekben a napi szintű felhasználáshoz szükséges irathanyagok zárt tárolásához szükséges helykövetelményeket vegyék figyelembe.
- Az irodai funkciókat érdemes úgy tervezni, hogy a legkisebb ismeret elve alkalmazható legyen, lehetőleg az azonos munkakörben és hozzáférési engedélyekkel rendelkezők dolgozzanak egy területen. Az irodai információfeldolgozó eszközöket úgy kell elhelyezni, hogy az illetéktelen hozzáférés esélye minimálisra csökkenjen (például szomszédos épületből történő belátás).

Az elektronikus biztonságtechnikai rendszerelemek elhelyezésének tervezésénél a megfigyelés, behatolásjelzés szükségességét, továbbá az egyes eszközök technikai paramétereit a telepítési helyszín adottságaiból, használati módjából szükséges meghatározni, azonban e tekintetben is megfogalmazható néhány olyan tervezési alapelv, amelyet minden esetben célszerű figyelembe venni:

- A létesítmény ki- és belépési pontjai személyesen és/vagy elektronikusan felügyeltek legyenek.
- Az információt, információfeldolgozó vagy hálózati eszközöket, továbbá a folyamatos működésükhöz szükséges technológiát koncentráltan tartalmazó helyiségek elektronikus megfigyeléséről, behatolásjelzéséről gondoskodni szükséges. A szervertermek esetében minimálisan a hőmérsékletet, áramkimaradást és – ha a telepítési környezet indokolja – a vízbetörést felügyelni kell.
- A belépést, áthaladást korlátozó eszközök esetében a vészeseti kiürítéshez szükséges átbocsátó képességet és a nyithatóságot biztosítani szükséges, azonban a tűzjelző oldali vezérlések tervezésekor a vagyonvédelmi szempontokat szintén mérlegelni kell. A védett területek határán telepített beléptetőrendszer kétirányú azonosítással képes legyen a kényszerített nyitások jelzésére és úgynevezett antipassback funkció megvalósítására, támogassa a szükséges incidensmenedzsment-eljárásokat.
- A biztonságtechnikai rendszerek vezetékeinek elhelyezése illetéktelen fizikai hozzáférést gátló módon védőcsőben, kábeltálcán vagy műanyag csatornában történhet süllyesztett, illetve falon kívüli szereléssel. A rendszerelemek (vezérlő terminál, táp, központok) védett téren belül legyenek.

- A beléptetőrendszer jogosultsági csoportjainak és a behatolásjelző rendszerek partícióinak kialakításakor gondosan tervezni szükséges a jogosultságok idő és terület szerinti korlátozását, hogy a rendszerekben jogosult felhasználók is csak a számukra legszükségesebb területen, a szükséges időtartamig és időszakban tartózkodhassanak.
- A biztonságtechnikai rendszerek menedzseléséhez és kezeléséhez alkalmazott szoftverek minden kezelési ponton csak a szükséges beállítások elvégzését és funkciók használatát engedélyezzék, a rendszertervek bizalmas kezeléséről gondoskodni szükséges.

Azokra az esetekre, amikor folyamatszervezési okokból az információt tároló, feldolgozó, működésüket biztosító helyiséghez jogosulatlan személyek hozzáférése szükséges, és felügyeletük személyesen vagy elektronikus eszközökkel nem megoldható (takarítás, vészeseti beavatkozás stb.) kiegészítő kontrollokat szükséges biztosítani. Tiszta asztal politika keretében a távoli hozzáféréshez szükséges kivételek figyelembevételével tiltani kell az informatikai eszközök bekapcsolt állapotát, az iratanyagokat, mobil adathordozó eszközöket zárható tárolószekrényekben szükséges elhelyezni. Technikai oldalról gyakori intézkedés a munkaállomások merevlemezeinek titkosítása, továbbá úgynevezett Kensington-zárak alkalmazása. Azonos irodán belül dolgozó, azonban különböző jogosultságokkal rendelkező személyek hozzáférését az információfeldolgozó eszközök gondos elhelyezésével, és rálátást gátló képernyővédő (privacy filter) használatával lehet biztosítani.

A kiegészítő kontrollok alkalmazása szükséges azokban az esetekben is, amikor információfeldolgozó, vagy a szervezet információhoz távoli hozzáférést biztosító eszköz kikerül a vállalat fizikai biztonsági rendszerének felügyelete alól. Ilyen jellemző tevékenység a mobil eszközökkel végzett távmunka, amely során egy jól működő eszközmenedzsmenti (MDM) rendszer alkalmazása lopás vagy elvesztés esetére biztosítja a titkosított adattárolást, a távoli zárolási és törlési eljárásokat, kikényszeríti a céges szabályokat és segít az eszköz fizikai lokációjának felderítésében.

Információfeldolgozó eszközök meghibásodása esetén a szállítóhoz, karbantartóhoz történő kiszállítás előtt minden érzékeny információt el kell távolítani a berendezésből (hálózati eszközök memóriája, munkaállomások, szerverek, nyomtatók merevlemezei), továbbá érdemes már a beszerzésnél a garanciális követelmények közt a merevlemezekre visszatartási opciót megfogalmazni.

Az érzékeny információt tartalmazó papíralapú hulladékot elszállítás előtt iratmegsemmisítő berendezésekkel tegyük használhatatlanná. Amennyiben az iratkezelés kialakítása a papírhulladék átmeneti tárolását szükségessé teszi, alkalmazzunk zárt, plombálható gyűjtődobozokat. Abban az esetben, ha a gyűjtődobozok megsemmisítését külső szállítóra bízzuk, az csak a tárolóeszközök megbontása nélkül, jegyzőkönyv felvétele mellett történhet.

Üzletmenet-folytonossági szempontok gyakorta indokolják, hogy a szervezet gondoskodjon az informatikai rendszerek mentéseinek telephelyen kívüli, (offsite)

elhelyezéséről. A mentéseket tartalmazó eszközök szállítása és külső helyszínen történő tárolása esetén is biztosítani kell a fizikai védelmi intézkedések folytonosságát, a szervezeti információk partnernek, alvállalkozónak történő átadása esetén pedig szerződéses feltételként szükséges megkövetelni a fizikai biztonsági kontrollok kialakítását és üzemeltetését.

Technológiai kompatibilitás, megfelelőség

A fizikai biztonság, 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.

Ha a szervezetnél a bekövetkezett rendkívüli események kezelésére, az incidensmenedzsment támogatására SIEM[19]-rendszert alkalmaznak, szükséges annak előzetes megállapítása, van-e igény az elektronikus biztonsági eszközök SIEM-rendszerbe történő integrációjára. Az integrációs igény meghatározza többek közt azt, 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 jelszókomplexitásra vagy titkosítást biztosító adatátviteli protokollok használatára. A különböző információbiztonsági szempontú technológiai megszorítások, különösen a felhőalapú 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 adatbáziskezelő rendszerek, mentési eljárások).

Amennyiben igényként merül fel, hogy a munkavállalók okoseszközeiket (telefon, tablet stb.) az elektronikus beléptetőrendszerekben történő azonosításához használhassák, úgy a technológia kiválasztásánál figyelembe kell venni az alkalmazott készülékek operációs rendszereit, az azonosításhoz felhasználható adatkapcsolati lehetőségeit (BLE, NFC), továbbá a tervezett használat módját, az eszközök elhelyezésének lehetőségeit. A kontrollokat úgy tervezzük, hogy minden esetben elkerüljük a téves, nem szándékolt nyitásból származó kockázatokat (például: HID twist and go rendszerének használata).[20] Ha az elektronikus beléptetőrendszerek funkcióit dokumentumkontroll-

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

[20] Magas(abb) kockázatú területen a mobiltelefonos azonosítás nem javasolt. A nyilvánvaló biztonsági kockázatokon túl a beléptető kártya vizuális azonosíthatóságot (is) biztosít, amely segítséget nyújt a területen dolgozóknak az illetéktelen személyek benntartózkodásának kiszűrésében.

ra is alkalmazni kívánják – legjellemzőbben hálózati nyomtatók proximity kártyával történő integrációjában –, akkor olyan kártyaszabványt válasszunk, amelyet az alkalmazott nyomtatógyártó technológiája támogat, egyedi kódolást alkalmazó rendszerek esetében elképzelhető, hogy az nem, vagy csak nagy költséggel integrálható külső gyártók rendszereivel.

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 megfigyelőrendszerek esetében szükséges biztosítani, hogy képesek legyenek a személyes adatokat a meghatározott ideig tárolni, azokon az előre beállított paraméterek alapján végrehajtani a szükséges adattörlési műveleteket és műszakilag támogatni az érintettek megismeréshez és adathordozhatósághoz való jogát.

Kapacitástervezés szempontjából gondoljuk végig a szervezet közép- és hosszú távú növekedési terveit és lehetőségeit akár létszám, akár feladat, akár erőforrás tekintetében, ennek megfelelően tervezzük a rendszerek műszaki paramétereit (zónaszám, rögzítési kapacitás, átbocsátóképesség, integrálhatóság stb.). Ha a szervezet a biztonságtechnikai rendszereket egyéb szabványi követelmények kielégítésére is kívánja felhasználni, legjellemzőbben a különböző környezeti monitorozó rendszerek jelzéseit (230 V tápellátás, hőmérséklet felügyelet) a behatolásjelző rendszer szabad zónáin keresztül fogadni és továbbítani tervezzük annak műszaki megvalósításához szükséges eszközöket és képességeket.

Üzletmenet-folytonosság támogatása, a védelmi intézkedések folyamatossága

Az üzleti információk bizalmasságának garantálása mellett a fizikai biztonsági kontrolloknak fontos szerepük van az információ és információfeldolgozó eszközök, berendezések rendelkezésre állásának biztosításában is, így az előző fejezetben bemutatott védett elhelyezésen túl a fizikai biztonsági elemeknek a feltárt kockázatok és a józan műszaki, gazdasági megfontolások figyelembevételével ellenállóságot szükséges biztosítani a rendkívüli események hatásaival kapcsolatban.

E tekintetben a legrelevánsabb, szinte minden szervezetet érintő kockázat a tűzkockázat. Ennek csökkentése érdekében a telepítési helyszíntől függetlenül javasolt minimálisan az információfeldolgozó és informatikai hálózati eszközöket koncentráltan tartalmazó helyiségeket (például szerverterem), továbbá az üzletmenet-folytonosság szempontjából kritikus energiaellátó és egyéb működtető rendszerek, berendezéseknek elhelyezésére szolgáló helyiségeket legalább a befogadó épület mértékadó kockázati besorolásának megfelelő tűzgátló építményszerkezetekkel határolni és a telepítési

környezetnek megfelelő tűzjelző rendszerrel ellátni.[21] A kiemelt helyiségek védelmén túl javasolt a teljes munka-üzemi terület bevonása automatikus tűzjelző rendszer védelme alá.

Igen fontos annak tervezése is, hogy maguk a fizikai biztonsági intézkedések ne okozzanak a működés folytonosságában, az információhoz, az információfeldolgozó eszközökhöz történő hozzáférésben, használatában problémákat. Amennyiben a vonatkozó működésfolytonossági követelmények alapján a helyiségekbe automatikus oltórendszert is telepítenek, azt úgy szükséges megválasztani, hogy a technológia ne jelentsen járulékos kockázatot az informatikai eszközök és a munkát végző kollégák számára. Nem javasolt a nagynyomású vízködös oltórendszer, valamint az aeroszolos, illetve egyéb visszamaradó anyaggal oltó rendszer használata.[22] A gázzal oltó rendszereket, azok közül is az egészségre nem ártalmas megoldások alkalmazását (például INERGEN) érdemes előnyben részesíteni, amellyel az egészségkárosító kockázatok elkerülése mellett lehetőség adódik a helyiségekben az elsődleges emberi beavatkozások haladéktalan elvégzésére,[23] 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, a 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 újrainduljon.

A használatot esetlegesen akadályozó, nehezítő vagy járulékos kockázatokat okozó lehetőségeket egyéb eszközök tekintetében is végig kell gondolni. A beléptetőrendszereknél, különösen a biometrikus (vagy bizonyos kockázati szint fölött a többfaktoros) azonosítást alkalmazó megoldások esetében igen fontos figyelembe venni e tekintetben a megbízható működés két lényeges mérőszámát, a FAR-t (False Acceptance Rate,

---

[21] A tűzgátlás folyamatosságát biztosítva a helyiségen átvezetett villamos vagy gépészeti vezetékek, rendszerek átvezetési helyein, a vezeték és a rendszerelem, valamint az építményszerkezet közötti résben, nyílásban a tűz átterjedését az átvezetéssel érintett építményszerkezetre előírt tűzállóságiteljesítmény-követelmény időtartamáig meg kell gátolni. [54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról]

[22] Tervezés az IT biztonság szempontjából (2008) 36.

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

téves elfogadási arány) és az FRR-t (False Rejection Rate, téves elutasítási arány).[24] Az információbiztonság 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 sarkallhatja 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.[25]

A beléptetőrendszerek tekintetében érdemes megismerkedni még a fail safe és a fail secure üzemmódok jelentésével, és hatásukkal az információbiztonságra. Fail safe az áthaladást szabályozó eszköz működése, ha meghibásodás vagy a normáltól eltérő, úgynevezett vészeseti működés során az életvédelmi szempontokat helyezi előtérbe.[26] 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.[27] Ezen két üzemmód alkalmazása minden esetben egyedi, alapos megfontolásokat és gondos tervezést kíván, hogy sem az információhoz történő illetéktelen hozzáférés, sem a létesítményben tartózkodó személyek egészségének szempontjából ne jelentsen többletkockázatot.[28]

A normál szervezeti működéstől eltérő kedvezőtlen helyzetekben, például egy katasztrófa esetén is biztosítanunk kell a fizikai biztonsági intézkedések folytonosságát. Azoknak szükséges beépülni a vészhelyzeti (tűzriadó, bombariadó stb.) és üzletmenetfolytonossági tervezésbe, hogy a szervezet értékteremtő tevékenységének folyamatosságát biztosító alternatív üzleti folyamatokban is érvényesítsük az információvédelmi követelményeket. A fizikai biztonsággal összefüggő igényeket az alternatív folyamatokon túl az alternatív munkavégzési helyszínek tervezése és használata során is érvé-

---

[24] 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 (2011) 22–35.

[25] Tóth A. (megjelenés alatt)

[26] Erre példa, ha tápkimaradás esetén (amely lehet műszaki okból, vagy a tűzjelző rendszer vezérlő jelének hatására) az eszköz állapota nyitottá, átjárhatóvá válik. Bunyitai (2011) 22–35.

[27] Bunyitai (2011) 22–35.

[28] Ahol lehet, műszaki intézkedésekkel csökkentsük annak az esélyét, hogy a *fail secure*-ként működő rendszerek *single point of failure*-ként képesek legyenek megakadályozni a használatot. Táphiba esetén a tartalék áramforrást a várható legnagyobb áthidalási időnek megfelelően tervezzük, a beléptető terminál saját EEPROM memóriával, vagy más egyenértékű megoldással biztosítsa, hogy a szerverrel történő hálózati kapcsolat kiesése esetére a már felvett belépési jogosultságok alapján az áteresztés folyamatos legyen.

nyesíteni kell. Különösen igaz ez a szabvány balesetek elleni védelmi követelményeire, a hatályos magyar szabályzás nem tesz különbséget a munkavállalók és a tevékenység hatókörében tartózkodók biztonsága tekintetében aközött, hogy normál munkavégzés során, a munkaszerződésben megjelölt állandó munkavégzési helyszínen vagy az alternatív folyamatok során igénybe vett ideiglenes munkahelyeken végzik-e tevékenységüket. A biztonságért felelős szervezetnek az üzletmenet-folytonossági tervekben minden esetben vizsgálni kell, hogy az alternatív üzleti és az informatikai eszközök visszaállításának folyamataiban meghatározták-e a biztonsággal kapcsolatos minimális követelményeket, ha szükséges, az egyenértékűséget biztosító helyettesítési megoldásokat. Ritkán, de előfordulhat, hogy az üzleti hatáselemzés során a biztonság és a biztonsági intézkedéseket támogató rendszereket is üzletkritikus folyamatként, rendszerként azonosítják (gondoljunk itt egy nagy költségvetéssel működtetett kutatás-fejlesztési részleg támogatására), így magára a biztonsági folyamat folytonosságára, az elektronikus eszközök visszaállítására szintén akcióterveket kell készíteni, fenntartani és időszakosan tesztelni.

Incidensmenedzsment

A szabvány alapján incidensként szükséges kezelnünk minden olyan eseményt, amely nagy valószínűséggel veszélyezteti az üzleti tevékenységet, fenyegeti az információbiztonságot, továbbá megfelelő incidensjelző metódusokat és beavatkozásokat kell tervezni, implementálni a meghatározott információbiztonsági incidensekre való válaszként.[29]

A fizikai biztonsági rendszerek több szempont alapján is érintettek az incidensmenedzsmentben. Egyrészt, a fizikai biztonság megsértése önmagában is kiemelt incidenskategória, és mint ilyen, érvényes rá a szabvány azon követelménye, amely ezen kategóriákra részletes kezelési eljárásrendek, akciótervek kidolgozását követeli meg.[30] Másrészt, az alkalmazott elektronikus biztonságtechnikai rendszereknek kiemelt szerepe van az incidensek monitorozásában, kiértékelésében, vizsgálatában, adott esetben bizonyításában. A rendszereknek alapvető funkciójuk bizonyos incidensek jelzése (a behatolásjelző vagy a beléptető rendszer riasztásjelzései, a telepített kamerák élőképei), amelyek az azonnali beavatkozást támogatják. Az incidensek utólagos vizsgálatát segíti elő a különböző kameraképek ellenőrzése, vagy a beléptetőrendszerekben keletkezett mozgási adatok elemzése.[31] 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,[32] illetve a kezelési (hozzáférési), a bizonyíték-

[29] MSZ ISO/IEC 27002 *Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve.*

[30] A tervben foglaltakat megfelelően tesztelni, és annak aktualitását időszakos felülvizsgálatokkal biztosítani szükséges.

[31] Ezt az elemzést, ellenőrzést nemcsak incidens esetén, hanem folyamatosan, megelőző jelleggel el kell végezni.

[32] Például a kamerarendszer képes legyen digitális vízjellel ellátni vagy olyan fájlformátumban exportálni a rögzített felvételeket, amely kizárja az utólagos manipuláció lehetőségét.

gyűjtési 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, azon milyen műveleteket végzett, végezhetett. Magukban a fizikai biztonsági eszközökben bekövetkező incidensek jelzésére, vizsgálatára pedig hasznos lehet a már említett SIEM-integráció, továbbá az elvégzett felhasználói műveletek lokális naplózása. Alapvető és ismert követelmény, de fontossága miatt megemlítendő, hogy a rendszerek helyi és távoli riasztása, továbbá a jelzésére történő élőerős és szakértői reagálás minden napszakban, folyamatosan biztosított kell legyen.

Az incidensmenedzsment feladatok szempontjából speciális, ám nem egyedi helyzet, amikor a vállalkozás több bérlős ingatlanokban (jellemzően irodaházakban) kap helyet, ahol a létesítmény üzemeltetője működteti a szervezet fizikai védelmének részét képező biztonságtechnikai rendszereket, legtöbbször kamerákat, beléptetőket, de a szervezet által bérelt területen a tűzjelző rendszer is jellemzően integrált része az épület tűzjelzőhálózatának. Ez a gyakorlat számos kockázatot rejthet magában, egyrész az által, hogy harmadik fél kezeli a szervezet munkavállalóinak, ügyfeleinek személyes adatát. Másrészt a GDPR elvárásainak való nehezebb megfelelésen túl a hatékony incidenskezelést is hátráltatja, hogy formalizált eljárásokon keresztül, külső szervezettől szükséges igényelni a vizsgálathoz nélkülözhetetlen logokat, képeket, incidensriportokat, amelyek esetleg meg sem felelnek saját szervezetünk vonatkozó szabályainak, előállításuk, kezelésük, feldolgozásuk nem ellenőrzött körülmények közt történik. Az üzemeltető a területhez történő hozzáférési jogosultságokat saját hatáskörben, akár a szervezet tudta nélkül is biztosíthatja maga számára, az üzemeltetési modellből következően pedig a vészeseti beavatkozást például egy tűzjelzés esetén is ő, vagy az általa biztosított őrszolgálat végzi (akár tűzkulcsokat is igényelve ehhez a szervezettől), és megfelelő kiegészítő intézkedések nélkül[33] a vállalkozás nem fog értesülni a használatában lévő ingatlanrészekre történő külső belépésről.

Ezeket a szempontokat minden esetben szükséges mérlegelni, amikor a biztonságtechnikai rendszerek üzemeltetőjének személyéről döntünk, de amennyiben arra lehetőség van, javasolt, hogy minden rendszerelem a szervezet saját tulajdonában/üzemeltetésben legyen.

[33] Érdemes olyan megoldást választani ebben az esetben, hogy az üzemeltető ne ismerhesse meg a vállalkozás munkavállalóinak személyes adatait. Ennek egyik módszere lehet a nem perszonalizált, azonban a szükséges jogosultságokat tartalmazó azonosítók igénylése, ahol a személyhez rendelést a vállalkozás saját hatáskörben biztosítja. A bérleti szerződésekben rögzíteni szükséges, hogy incidens esetén hogyan, milyen formában, időszakon belül kerülnek átadásra a vizsgálathoz szükséges, biztonságtechnikai rendszerben kezelt információk, rögzíteni kell továbbá az általános ellenőrzéshez szükséges riportok gyakoriságát és formáját. Vállalható és költséghatékony lehet az a kompromisszum is, amikor a bérelt területek határán az üzemeltető, a bérelt területeken belül az információbiztonság szempontjából kiemelt helyiségekben a vállalkozás maga üzemelteti a fizikai biztonsági rendszereit.

Szabályzás és ellenőrzés

Az eddig ismertetett, fizikai biztonsággal összefüggő követelmények végrehajtását és hatékonyságát adminisztratív és ellenőrzési oldalról is támogatni szükséges. A feladatok részletes meghatározásának és számonkérhetőségének alapja, hogy legyen olyan érvényes szervezetszabályzó eszköz, amely a védendő vállalati értékkel kapcsolatos fizikai biztonsági szabályokat tartalmazza.

A szabályzat tartalmának megfelelő kialakításához a szervezet mérjen fel és dokumentáljon minden olyan követelményt (jogszabály, szerződés, biztosítás), amely az érdekelt felek elvárásainak kielégítéséhez szükséges. A fizikai biztonsággal kapcsolatos felelősségi körök és feladatok részletesen szabályozottak legyenek, és legyenek igazoltan elfogadva, például a szervezet munkavállalóinak munkaköri leírásaiban vagy speciális esetben kinevezési okiratokban.

A szabályzat céljával összhangban határozzák meg azokat a területeket (helyiségeket, helyiségcsoportokat, épületrészeket, szabad tereket), amelyek védettnek minősülnek. A védett területek, azok kategóriájának és a kategórián belül alkalmazott intézkedések meghatározása részletes, dokumentált kockázatfelmérésen alapuljon, amely kockázatértékelés a teljesség igénye nélkül legalább az alábbi szempontokra terjedjen ki:

- a tárolt, kezelt (védendő) vállalati érték jellege,[34] értéke, érzékenysége;
- a jogszabályi követelményeknek való megfelelőség vizsgálata;
- a létesítményt veszélyeztető külső tényezők felmérése;
- a létesítmény belső veszélyeztető tényezőinek felmérése;
- tulajdonosi és használói információk;
- a meglévő épületszerkezetek, vagyonvédelmi és tűzvédelmi rendszerek kiépítettségének és állapotának felmérése;
- azon helyzetek figyelembevétele, amelynek bekövetkezte esetén a területek védelme a rendszeresített eszközökkel nem biztosítható.

Az így azonosított védett területek tekintetében jelöljék ki a felelős személyeket, akik feladata a területre érvényes biztonsági szabályok érvényesítése, felügyelete, a jogosultak és a jogosultsági szintek meghatározása. A szabályzat részeként határozzanak meg előírásokat a hozzáférés kontrollálására rendelt azonosítók, belépést és benntartózkodást lehetővé tevő egyéb eszközök kezelésére, kiadására, visszavonására, továbbá a területen tartózkodás alapvető szabályainak meghatározására (folyamatos felügyelet követelménye, adatrögzítésre alkalmas eszközök tilalma, papíralapú dokumentációk kezelés, tárolása stb.).

A szabályzat részeként ki kell térni a biztonságtechnikai rendszerek beszerzésének, üzemeltetésének szabályaira, különös tekintettel a GDPR érintetti jogokra vonatkozó követelményeinek érvényesítésére, a jogosultságok kiadásának, visszavonásának,

[34] A szabályzásban részletesen szükséges meghatározni, mit kell védeni fizikai biztonsági intézkedésekkel (elektronikus és papíralapú információk, titkosítást biztosító kulcsok, információfeldolgozó eszközök stb.).

felülvizsgálatának szabályaira, a karbantartásra, a jelzések fogadásának és kezelésének módjára, továbbá egyéb, az incidensmenedzsment hatékonyságát támogató intézkedésekre. A szabályzat legyen összhangban más szakterületi szabályzó eszközökkel, amelyek céljukból adódóan szintén fogalmazhatnak meg fizikai biztonsággal kapcsolatos feladatokat, követelményeket (például tűzvédelmi szabályzat, backup policy stb.).

A fizikai biztonság és annak követelményei ne csak papíron, hanem a mindennapi működésben, kiemelten a menedzsmentfolyamatokban is „láthatók legyenek." A felelős területet minden esetben szükséges bevonni a szervezeti változáskezelési eljárásokba, az adatkezelési folyamatok megtervezésébe. Rendszeres auditokkal szükséges meggyőződni a fizikai biztonsági követelmények megvalósulásáról, továbbá releváns mérőszámok, úgynevezett KPI-k (Key Performance Indikátor, kulcs teljesítménymutató) meghatározásával és alakulásuk nyomon követésével felügyelni a bevezetett intézkedések célnak megfelelő, hatékony működését.

A belső szabályzók tartalmát, a szükséges védelmi feladatokat minden érintett számára oktatni kell, a munkavállalók és a külső foglalkoztatottak fizikai biztonsággal kapcsolatos feladataikról belépéskor és utána rendszeres időközönként részesüljenek képzésben, oktatásban. Sokan közülük nincsenek tisztában az általuk kezelt információ értékével, az esetleges támadások típusával, megvalósítási módjaival, így a tréningek során kiemelt figyelmet kell fordítani azokra a legyakoribb viselkedésbeli szabályokra, hiányosságokra, amelyeknek kihasználásával a potenciális elkövetők aránylag kis erőfeszítéssel és ráfordítással képesek megkerülni a fizikai biztonsági kontrollokat, továbbá, amelyek nem szándékosan (hanyag kezelésből, gondatlanságból eredően) az információk bizalmasságának, rendelkezésre állásának vagy integritásának sérüléséhez vezethetnek. A különböző munkakörök különböző kockázatokkal bírnak, akár elkövetővé, akár áldozattá válás szempontjából, így javasolt a munkakörök biztonsági jellegű profilozása, és az oktatási, ellenőrzési feladatok ezen biztonsági sajátosságokhoz történő igazítása.

Az oktatásokon túl adminisztratív módon is támogatni szükséges, hogy a felhasználók végrehajtsák az elvárt feladatokat. Ennek keretében az érintettek (fizikai) biztonsággal kapcsolatos kötelességeiket igazoltan vegyék tudomásul, mint ahogy azt is, hogy a munkáltató tevékenységüket a meghatározott módon és formában ellenőrzi. Alkalmazzanak formális fegyelmi eljárásokat a fizikai biztonság megsértőivel szemben, szigorú eljárásokkal szabályozzák a munkavállalók kilépési folyamatát, továbbá rendszeres belső ellenőrzésekkel, amennyiben indokolt, social engineering tesztekkel ellenőrizzék a bevezetett intézkedések hatékonyságát.

IRODALOMJEGYZÉK

Bunyitai Ákos (2011): A ma és a holnap beléptető rendszereinek automatikus személyazonosító eljárásai biztonságtechnikai szempontból. *Hadmérnök,* 6. évf. 1. sz. 22–35.

Hutter, David (2016): *Physical Security and Why It Is Important.* The SANS Institute.

Tóth Attila (megjelenés alatt): Tűzjelző rendszerek, beléptető rendszerek. In Christián László – Major László – Szabó Csaba szerk.: *Biztonsági vezető kézikönyv.* Budapest, Nemzeti Közszolgálati Egyetem.

Tóth Levente (2018): A komplex objektumvédelem kihívásai napjainkban. *Bolyai Szemle*, 27. évf. 1. sz. 35–44. Forrás: https://folyoiratok.uni-nke.hu/document/nkeszolgaltato-uni-nke-hu/Bolyai_Szemle_2018_01.pdf (2019. 07. 01.)

Vasvári György (2006): *CISM: Bankbiztonság.* Budapest, Információs Társadalomért Alapítvány.

Internetes források

https://hu.wikipedia.org/wiki/Kifigyelés (2019. 08. 22.)

ISO/IEC 27001:2013 *Information technology – Security techniques – Information security management systems – Requirements.* 2nd edition. Forrás: www.iso.org/standard/54534.html (2019. 07. 01.)

MSZ ISO/IEC 27002 *Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve.* Forrás: www.mszt.hu/web/guest/webaruhaz;jsessionid=F7619FB3BE8FF2BCDF45CBC8DB528A-BA?p_p_id=msztwebshop_WAR_MsztWAportlet&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_msztwebshop_WAR_MsztWAportlet_ref=152658&_msztwebshop_WAR_MsztWAportlet_javax.portlet.action=search (2019. 07. 01.)

Tervezés az IT biztonság szempontjából (2008). Miniszterelnöki Hivatal. Forrás: https://docplayer.hu/1848351-Tervezes-az-it-biztonsag-szempontjabol.html (2019. 07. 01.)

Jogforrások

2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól

2009. évi CLV. törvény a minősített adat védelméről

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

42/2015. (III. 12.) Korm. rendelet

54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról

ABSTRACT

The Practice of Designing and Applying Physical Security Controls in the Light of the Requirements Set in the International Standard ISO/IEC 27001

TISZOLCZI Balázs

Adequate protection of information and information systems requires careful planning and implementation of a large number of controls by businesses. In many cases, they do it by applying an information security framework, most often the international standard ISO/IEC 27001. There are instructions in the standard which deal with developing the physical security of information systems. This study discusses design and operational considerations that may help security professionals to develop physical security systems that meet the standard requirements.

Keywords: *physical security, standard 27001, design*