HADMÉRNÖK
BIZTONSÁGTECHNIKA

19. évfolyam (2024) 2. szám 5–15.
DOI: 10.32567/hm.2024.2.1

Gubics Frigyes[1]

SOC kialakítása projektmenedzsment segítségével és az üzemeltetés alapjai

Designing SOC with the Help of Project Management and the Basics of Operation

Absztrakt

A különböző típusú objektumok védelme más-más megközelítést igényel, függően attól, hogy milyen jellegű tevékenység folyik a védendő területen belül, illetve mekkora kockázatokkal dolgozunk, és esetleges bekövetkezés esetén milyen károkat szenvedhetünk el. Azok a szervezetek, amelyeknél van kultúrája az objektumvédelemnek és a biztonsági intézkedéseknek, egymással jól együttműködő, strukturált és egymást kiegészítő biztonsági rendszereket építenek ki, amelyek működését egy központi helyről koordinálják, ez a biztonsági központ. Ennek az objektumrésznek fontos szerepe van a megfelelő biztonsági szint fenntartásában, egyúttal támogatást biztosít a területen dolgozó operatív egységek részére. Prioritást élvez a biztonsági központ védelme, amelynek tervezése során felkészülünk a lehetséges támadásokra, illetve haváriahelyzetekre.

Kulcsszavak: objektumvédelem, biztonsági központ, tervezés, biztonság, fizikai védelem

Abstract

Different facilities require different approach of protection that depends on the profile and risk we need to handle, and also need to recognise what kind of risks we face and what are the possible effects. Organisations that have established a culture of facility protection and security measures, have a well-coordinated, structured and complementary security systems that are coordinated from a central location, which is the security centre (SOC).

[1] Biztonsági igazgató, Lenovo Manufacturing Kft., e-mail: easytwofly@gmail.com

The SOC is part of the facility infrastructure and has the main rule to keep security level high enough and also supports operative activity in the areas. Protecting the SOC effectively is a high priority, and it plays an important role in ensuring an appropriate level of security and provides support to the operational unit in preparing for possible attacks or incidents.

Keywords: facility protection, SOC, planning, security, project management, CCTV

Bevezetés

Az objektumok védelmének célja alapvetően a vagyon elleni cselekmények megelőzése, megakadályozása és az emberi élet védelme. Passzív védelmi eszközök segítségével az objektum területére történő behatolást kívánjuk késleltetni, illetve bizonyos esetekben megakadályozni. Ugyanakkor gondoskodni kell a cselekmény detektálásáról is. Az időben történő észlelés alkalmat ad a késlekedés nélküli válaszreakció megtételére, amelyben jelentős szerep hárul a biztonsági központra.

Az objektumok védelmét több, különféle védelmi eszköz egymástól függetlenül is működő, ugyanakkor egymásra épülő, illetve kiegészítő működtetésével biztosítjuk. Ezeknek az elemeknek a működőképességét, üzembiztosságát biztosítani kell, hiszen a megbízható működés a hatékony védelem alapja.

Az objektumok azok a dolgok, amelyekre az őrzési feladat, védelmi kötelezettség, megbízás kiterjed. Az objektum nem feltétlenül kell hogy fizikailag elhatárolt legyen a környezetétől, habár a hatékony védelemhez kívánatos. Az objektumnak van fizikai kiterjedése, tehát a védelmet is fizikai formában, több lépcsőben építjük fel.

Horváth Tamás szerint[2] nagyvállalatok esetében, ahol a működés holdingszerű, az anyavállalat alkotja meg a biztonsági rendszer kereteit, amelyet az egyes leányvállalatok telephelyein implementál. Ezek a minimumelvárások mintegy belső szabványokként funkcionálnak. Tapasztalatom szerint egy az egyben nem mindig lehetséges ezek használata, szükséges a testreszabásuk a helyi viszonyoknak megfelelően, elsősorban azokban az esetekben, amikor a telephely másik országban van, hiszen ebben a helyi törvényeknek is megfelelően kell eljárnunk és működtetni a rendszereinket. Például a GDPR, mint európai uniós irányelv, a személyes adatok kezelése tekintetében eltérő szabályokat tartalmaz az USA jogszabályi kereteihez képest, így tehát egy amerikai anyavállalat sztenderdjeit módosítani szükséges az európai viszonyokhoz, hogy megfeleljünk a törvényi előírásoknak.

A biztonsági központ

A biztonsági központ sérülékenységét, meghibásodási kockázatait minimálisra kell csökkenteni. Az objektum tervezése során erre fokozott figyelemmel kell lenni. Rendelkezésünkre állnak azon eszközök, amelyeket az egész objektum védelmi rendszerének kiépítése során is alkalmazunk. A védelmi szintet meg kell határozzuk a teljes objektumra és az azon belül elhelyezkedő egyes területekre. Ehhez a kockázatelemzést

[2] Horváth 2018.

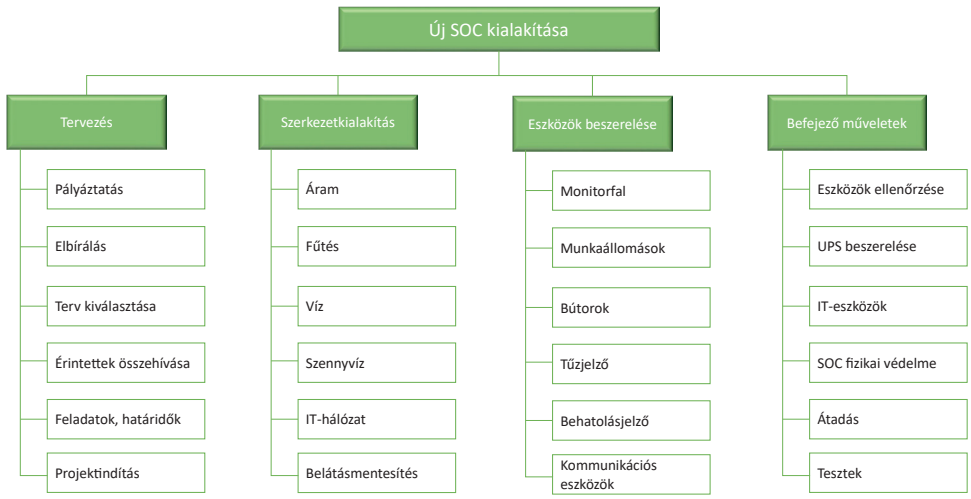
használjuk, amelynek segítségével reális képet kapunk a fennálló kockázatokról és a veszélyeztetettség mértékéről, amelyekhez a védelem szintjét igazítjuk. A biztonsági központ szenzitív, fokozottan védendő területnek számít, mert működésének kiesése esetén a biztonsági szolgálat létfontosságú információktól esik el, hiszen oda futnak be az általa felügyelt objektum őrzésére vonatkozó információk, ezzel együtt kiesése esetén a központ nem képes ellátni vészhelyzeti (például az objektum kiürítésével járó események) irányító funkcióját sem. Ezek részleges vagy teljes kiesése esetén a biztonsági szint csökken, amit azonban egyéb intézkedések bevezetésével bizonyos fokig kompenzálhatunk. Például a behatolásjelző rendszer meghibásodása esetén a vagyonőri létszám növelésével, őrpozíciók megerősítésével vagy újak nyitásával átmenetileg, amíg a hibát kijavítják. A biztonsági központ használhatatlanná válására fel kell készülnünk mint lehetséges kockázatra, amire az ERP[3] külön kitér. Megoldást jelenthet redundáns[4] rendszerek kialakítása: alternatív biztonsági központot hozunk létre egy eltérő helyszínen, lehetőleg nem ugyanazon az objektumon belül, így nem lesz érintve haváriahelyzet[5] esetén mindkét egység. Ez növeli a beruházási költségeket, ebben az esetben is a kockázatok elemzése segít meghozni a döntést, hogy megéri-e egy extra beruházást eszközölni. Piaci gazdasági társaságok esetén a menedzsment szempontjából a fő kérdés, hogy mennyi anyagi ráfordítás kell ahhoz, hogy a szükséges és elégséges védelmi szintet elérjem, és fenn tudjam tartani a kockázatok minimalizálása mellett.

Projektmenedzsment a biztonsági központ kialakítása során

A biztonsági központ kialakítása új épület tervezésekor része a projektnek. Amikor utólagosan, már meglévő, működő objektumba tervezünk SOC[6]-t, akkor a központ kialakítását tekintjük projektnek. Az érdekeltek *(stakeholder)*[7] bevonása fontos, hiszen az SOC létrehozása sok más terület képviselőjének munkáját is befolyásolhatja, segítheti. Például a tűzjelző központ telepítése, amely alapvetően az EHS[8] érdekkörébe tartozik, de észszerű, hogy annak felügyelete és kezelése a biztonsági szolgálat feladata, hiszen a nap 24 órájában, az év minden napján jelen vannak a telephelyen. A munka pályáztatásához meg kell fogalmazni az elvárásokat, amelyeket kiküldünk a pályázó cégek részére. A tender nyertese konzultáció útján pontosítja az igényeket. Ezután történik a költségvetés jóváhagyása. Amikor az anyagi források rendelkezésre állnak, a végleges terveket a pályázatot nyert cég készíti el a biztonsági vezető elvárásai és a szakma követelményei alapján. A tervek jóváhagyása a menedzsment, épületüzemeltetés és EHS osztály vezetőinek bevonásával történik. Az 1. ábra a projektkivitelezés folyamatát mutatja be. Garcia szerint[9] biztonságtechnikai mérnök

[3] ERP: emergency response plan (vészhelyzeti terv).
[4] Redundáns: párhuzamos, egymást helyettesítő rendszerek.
[5] Természeti csapás vagy emberi tevékenység során előállt vészhelyzet.
[6] SOC: surveillance operations center (felügyeleti műveleti központ).
[7] Stakeholder: érdekelt fél.
[8] EHS: environment, health, and safety (környezetvédelem, egészségvédelem, munkabiztonság).
[9] Garcia 2008.

alkalmazása elengedhetetlen, hiszen ő felügyeli a rendszerek integrációját, emellett a projektcsapat vezetőjének tapasztalattal kell rendelkeznie a biztonsági rendszerek kialakítása területén. Ez utóbbi állítást annyiban árnyalnám, hogy amennyiben nem a biztonsági szakterületről érkezik a vezető, fontos, hogy meghallja, megértse és érvényre is juttassa a szakág által támasztott igényeket a projekt valamennyi szakaszában.



1. ábra: Biztonsági központ létrehozása projekt
Forrás: a szerző szerkesztése

A megvalósítás alapkérdései:

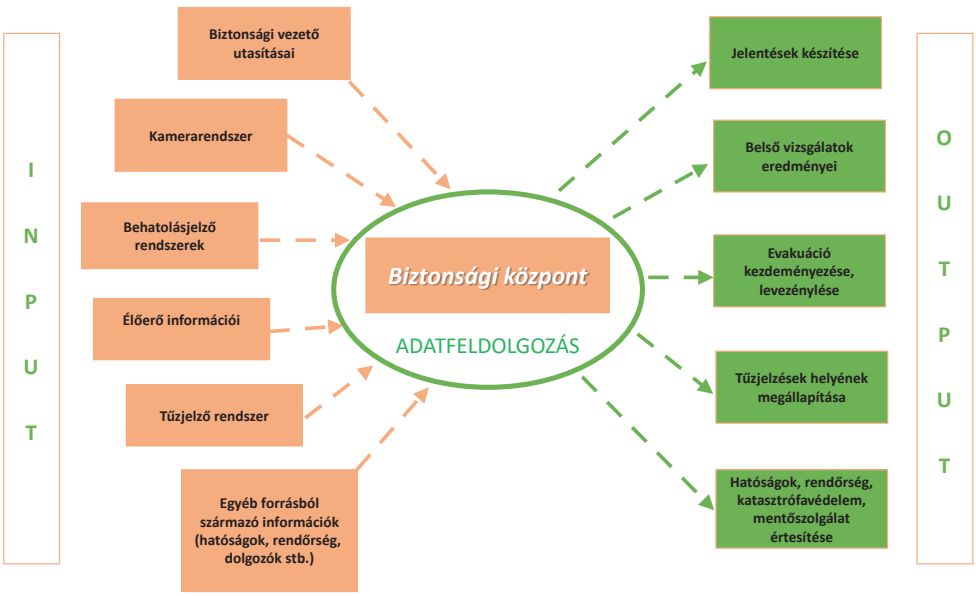
- A kivitelezési terv és az ahhoz használatos anyagok pontossága.
- A tervekben meghatározott és elfogadott elvárások megvalósításának fokozott ellenőrzése.
- Minőségi és garanciakérdések (a felhasznált anyagok és a kivitelezési munka minőségének garantálása a kivitelező által).
- Engedélyezési folyamatok (a létesítmény működéséhez szükséges hatósági engedélyek teljes körű beszerzése, illetve időszakos felülvizsgálatának intézése).[10]

Funkciók

A biztonsági központ létrehozása a biztonsági szolgáltatás, tevékenység keretbe foglalása, az adatok feldolgozásának központosítását is célozza. A bejövő információk jól detektálhatók, az egyes csatornákon érkező adatok fizikailag egy helyre érkeznek és összekapcsolhatók, összefüggéseikben értelmezhetők, kiértékelésük után pedig a válaszreakciók időben és adekvátan képződnek.

[10] Christián 2014b.

Az SOC az objektum védelmének központi eleme, amely működhet önállóan, de összekapcsolható, illetve egyfajta hierarchikus rendszerbe is állítható más biztonsági központtal vagy központokkal. A biztonsági központ földrajzi elhelyezkedése függ az üzemeltető telephelyi adottságaitól, a ráfordított anyagi erőforrásoktól, illetve szakmai döntésektől is.



2. ábra: A biztonsági központ információáramlása
Forrás: a szerző szerkesztése

A 2. ábra szemlélteti az információk gyűjtésének lehetséges forrásait, majd feldolgozás utáni „továbbküldését" intézkedések formájában, vagy akár az információ visszaküldését a forráshoz újabb adatigény megfogalmazásával, amennyiben döntés meghozatalához, illetve intézkedés kezdeményezéséhez az elsődleges információ kevésnek bizonyul.

Rendkívüli helyzetek

A napi operációval összefüggő biztonsági tevékenységen túlmenően adódhatnak rendkívüli helyzetek, amelyek eltérő reakciókat várnak az SOC személyzetétől. Tekintettel arra, hogy a biztonsági központban a nap 24 órájában szolgálatot látnak el, kézenfekvő, hogy a különböző váratlan helyzetek kezelésének is ez a központja, de legalábbis kulcsszerepet játszik azok megoldásában. A vállalat által megalkotott úgynevezett vészhelyzeti terv (ERP) rendelkezik az egyes feladatokról, szerepkörökről rendkívüli helyzetek esetén.

A stratégiai döntések nem az SOC-ban születnek meg, hanem az ilyen helyzetekben összeülő CMT[11] hozza meg azokat, amely a vállalatvezetés ide delegált tagjaiból tevődik össze, akik az általuk vezetett, a rendkívüli helyzetek kezelésében kulcsfontosságú területekért felelnek. A CMT elsődleges feladata az emberek, azon túlmenően pedig a vagyontárgyak mentése, ezek után pedig gondoskodni a helyreállításról és a termelés minél gyorsabb újraindításáról.

A biztonsági incidensek lehetnek ember által generáltak, illetve természeti eredetűek, jellegűek, amelyek bekövetkezésének esetén a detektálás és reagálás elsődlegesen a biztonsági központ feladata.

Váratlan helyezetek, amelyek kezelésében az SOC személyzetének kulcsszerepe van:

- időjárás okozta károk, meghibásodások kezelése,
- terrortámadás,
- bombafenyegetés,
- közlekedési katasztrófa,
- külső támadás,
- áramszünet,
- vízbetörés,
- epidéma, pandémia,
- földrengés,
- tűzeset.

A felmerülő kockázatokat figyelembe kell venni, majd ennek megfelelően kidolgozni az egyes esettípusokhoz kötődő lehetséges forgatókönyveket és folyamatokat. A felkészülés és a reagálási tervek kidolgozása a múltban bekövetkezett eseményeken alapul, de a vállalat alaptevékenységéhez kapcsolódó tipikus eseményekre is felkészülünk, kockázatelemzés segítségével. Az eseményspecifikus reagáláson túl szükség van eljárási rendre, amely tartalmazza az információs láncot, és definiálni kell döntési szinteket és jogosultságokat is. Az információs csatornák kijelölése a döntések és utasítások eljuttatásához a végrehajtó állományhoz elengedhetetlenek. A kommunikációs csatornákra van szükség a CMT, az SOC és az ERT[12] között. Az ERT a CMT által meghozott döntések végrehajtásában működik közre, és tagjait a CMT-tagok delegálják. Gondoskodni kell a helyettesítés rendjéről a CMT és ERT esetében. Az SOC-nak rendelkeznie kell személyzeti adatokkal, amelyek segítségével az evakuáció során meggyőződnek arról, hogy mindenki elhagyta az objektumot. A dolgozók legközelebbi hozzátartozói listájával is rendelkezni kell, hogy vészhelyzet esetén a családtagokkal fel tudjuk venni a kapcsolatot. Az adatok naprakészen tartása a kijelölt biztonsági személyzet/vezető feladata, felelőssége. Ennek érdekében folyamatos kapcsolattartás szükséges a Személyzeti Osztállyal.

[11] CMT: crisis management team (válságkezelő csapat).
[12] ERT: emergency response team (vészhelyzeti reagáló csapat).

Sérülékenységvizsgálat és a biztonsági központ fizikai pozicionálása

A megfelelő tervezés során a sérülékenységek a minimálisra csökkenthetők. Az olyan esetekben, amikor már meglévő objektumba telepítünk biztonsági központot, kénytelenek vagyunk az adottságainak megfelelő kompromisszumokat kötni. Közvetlenül, a dolgozók által frekventáltan használt területekről (például nagy forgalmú folyosó) ne legyen megközelíthető az SOC.

További tervezési szempontok

A biztonsági központot védő, megelőző infrastrukturális követelmények:

- a falazat és plafon kellően ellenálló kell legyen ipari baleset bekövetkezése és külső behatolás esetén is;
- a helyiségbe be- és kilépő kábelezés védelme;
- az informatikai rendszerek függetlenek az egyéb IT-rendszerektől;
- internetcsatlakozás nem lehetséges a használt eszközökön;
- vizesblokk ne legyen a közelben, illetve a hozzátartozó csővezeték ne menjen át a helyiségen, vízbetörés-védelem szükséges;
- friss levegő biztosítása;
- eszközök hűtésének biztosítása.

Mechanikai védelmi intézkedések:

- ellenálló falazat (például gipszkarton fal nem elfogadható) és plafon;
- megfelelő ellenállású ajtó;
- zárszerkezet az ajtóban;
- nincs ablak a helyiségen;
- ablakkal ellátott helyiségben gondoskodni kell a belátás korlátozásáról (fóliázás és függöny);
- a helyiségbe be- és kilépő kábelezés védelme.

Elektronikai védelmi intézkedések:

- beléptetővel ellátott ajtó;
- behatolásjelző rendszerbe integrálás;
- pánikgomb;
- interkom;
- UPS;[13]
- redundancia[14] biztosítása;
- elektromos ellátás;
- adatrögzítés (CCTV,[15] CAS,[16] intruder alarm[17]).

[13] UPS: uninterrupted power system (szünetmentes áramkör).
[14] Redundancia: erőforrások duplikálása a nagyobb rendelkezésre állás érdekében.
[15] CCTV: closed circuit television (zárt láncú kamerarendszer).
[16] CAS: centralized access system (beléptetőrendszer).
[17] Intruder alarm: behatolásjelző.

Kommunikáció:
- internet tiltva;
- független rádiókommunikáció, alternatív frekvenciával;
- mobiltelefon;
- vonalas telefon;
- közvetlen kommunikációs kapcsolat a rendőrséggel, katasztrófavédelemmel;
- privát kommunikációs eszközök és adathordozók bevitelének tiltása.

Rezsimintézkedések:
- belépések korlátozása;
- a belépési jogosultsággal rendelkezők körének rendszeres felülvizsgálata;
- sikertelen bejutások (fals kártyahúzások) rendszeres ellenőrzése és kivizsgálása;
- személyzet kiképzése, továbbképzése.

Humán faktor:
- személyzet kiválasztása;
- bizalmasság kérdése;
- titoktartási nyilatkozat;
- területismeret;
- képzés és továbbképzés;
- helyspecifikus ismeretek.

A biztonsági központ személyzetének és az IT-eszközöknek a védelme:
- az ipari tevékenység során esetlegesen felszabaduló, levegőben terjedő ártalmas gázoktól, részecskéktől és terjedésük irányától távol legyen;
- egyéni védelmi eszközök elhelyezése a helyiségben;
- önálló, megfelelő légcsere biztosítása;
- megfelelő hőmérséklet biztosítása.

A fenti szempontok szerinti megvalósítás mellett is fel kell készülnünk a biztonsági központ feladatainak ellátására alternatív megoldásokkal, amennyiben az elsődlegesen használt SOC-ból ez lehetetlenné válik. Célszerű létrehozni egy alternatív irányítási központot. Az alternatív központ biztosítására másik lehetőség, ha egy olyan központ veszi át a feladatok ellátását, amely a vállalatcsoporton belül egy másik objektum védelmében vesz részt. Ebben az esetben a tartalék központnak plusz személyzetre és eszközökre van szüksége úgy, hogy a megfelelő területismeret mellett az eszközök is alkalmasak legyenek a teljes értékű feladatellátásra. Az alternatív központ alkalmazásának akkor van realitása, ha egy vállalat egynél több telephellyel rendelkezik, amelyekből legalább kettő rendelkezik biztonsági központtal. A költség-haszon elv is szerepet játszik alternatív központ létrehozásában vagy már meglévő egység alkalmassá tételében a feladatok ellátására. Külföldön elhelyezkedő központban tevékenykedő személyzettől nem várható teljes értékű helyismeret, ugyanakkor ismerniük kell a helyi vészhelyzeti intézkedési terveket. Fontos, hogy közvetlen kapcsolatban legyenek a helyben szolgálatot teljesítő biztonsági személyzettel, illetve hogy szükség esetén a biztonsági központ legfontosabb funkcióit vegyék át, mint például a behatolásjelző

rendszer, a tűzjelző rendszer és CCTV-rendszer felügyelete. A kommunikáció a külföldi biztonsági központ személyzetével, a szükséges nyelvismeret szintén követelmény a biztonsági személyzet részére.

Jártasság biztosítása

A jártasság megszerzése, illetve fenntartása komoly erőfeszítést jelent az élőerős őrzést biztosító vagyonvédelmi cég oldaláról. Annak érdekében, hogy a biztonsági központ hatékonyan tudja ellátni feladatait az objektumvédelemben, illetve elsődleges irányító funkcióját betöltse, a technikai felszereltség mellett a személyzetnek rendelkeznie kell azzal a speciális tudással, amely biztosítja a működést az elvárt színvonalon. Az SOC-személyzet képzése iskolarendszeren belül és kívül sem megoldott, a szükséges ismereteket személyre, illetve telephelyre szabott formában kapják meg jelenleg a vagyonőrök. A biztonsági központban történő feladatellátás jóval több technikai jellegű kvalitást és alapvető IT-ismereteket igényel, mint amelyek a vagyonőri tevékenységhez szükségesek általában. Az ismeretek elsajátítása, illetve egy minimumszint meghatározása elengedhetetlen az SOC személyzete részére. Az SOC-ban a vagyonvédelmet szolgáló rendszereken kívül a tűzjelző rendszer központja is helyet kap, ezért szükséges a személyzet speciális, a beérkező tűzjelzésekhez kapcsolódó képzése, illetve az eljárásrend leoktatása rendkívüli, illetve vészhelyzetek eseteire. A személyzet létszámának meghatározása a feladatok jellegétől és mennyiségétől függ, de befolyásolja például a telephelyen telepített kamerák száma, milyen mennyiségűek a napi operáció során az élő időben követendő események, illetve a kivizsgálandó ügyek. Az éberség és a jártasság fenntartása érdekében a vészhelyzeti reagálást megfelelő időközönként gyakoroltatni kell, illetve nem szabad elfeledkeznünk az újonnan érkező személyzet képzéséről, valamint a meglévők továbbképzéséről sem. Fennelly szerint[18] a személyzetnek rendelkeznie kell az alábbiakban felsorolt készségekkel ahhoz, hogy hatékonyan tudja elvégezni a rábízott feladatot:

- biztonsági szabályzatok és eljárások ismerete,
- professzionalizmus,
- biztonsági tiszt jogosultsága,
- kapcsolatok a rendvédelmi szervekkel,
- járőrözési eljárások,
- megfigyelési technikák,
- kihívó technikák,
- vizsgálatok,
- jelentésírás,
- sürgősségi orvosi segítségnyújtás, elsősegélynyújtás,
- munkahelyi erőszak kezelése,
- biztonsági berendezések üzemeltetése.

[18] Fennelly 2013.

A fentieken túl azonban fontos, hogy a helyspecifikus szabályokat, eljárásokat tudják, illetve adaptálni legyenek képesek a megszerzett tudással a helyszíni adottságokhoz.

Összefoglalás

Az objektumvédelem során a védelmet ellátó biztonsági rendszerek központjának tervezése és kivitelezése létfontosságú. Az SOC esetében a rendelkezésre álló eszközök mind technikai, mind pedig élőerős oldalról hasonlók, mint amiket a teljes objektum védelméhez használunk. Az objektumvédelem célja nem kizárólagosan a periméter megóvása, hanem megfelelően kategorizálva és elhatárolva azokat, külön kisebb biztonsági zónák létrehozása és védelmi szintjük definiálása a kockázatelemzés eredményétől függően, hozzájuk rendelve a biztonsági rendszerelemeket. Ezeknek, az úgynevezett biztonsági zónán belüli szenzitív területeknek a felügyeletét is a biztonsági központba célszerű integrálnunk. Az SOC a szerepét akkor képes teljeskörűen betölteni, ha ott területismerettel, a biztonsági szabályokkal, az objektumon belüli munkafolyamatokkal, a technikai rendszerek kezelésével és megfelelő szakmai tudással rendelkező személyzet végzi a munkát, és képesek lekövetni az objektumon belüli folyamatváltozásokat is. A biztonsági központra úgy kell gondolnunk, mint a vállalatbiztonság agyközpontjára, ahol a bejövő információk feldolgozása zajlik, a megfelelő reagálás érdekében. Az SOC kialakításakor figyelembe vett környezeti adottságok, annak védelmi rendszere szavatolja a szolgáltatás folyamatosságának biztonságát. Az átgondolt kivitelezés, az érdekeltek bevonása a tervezéstől a megvalósulásig képesek garantálni azt, hogy olyan biztonsági központot alakítsunk ki, amely megfelel az előzetesen megfogalmazott feltételeknek, emellett alkalmasnak kell lennie arra is, hogy a későbbiekben – az igények esetleges változásához igazodva – képesek legyünk azt továbbfejleszteni. Az objektumvédelem kulcsfontosságú része az SOC, amelynek felépítése összehangolt munkát jelent több szakterület képviselőitől. Helye a komplex biztonsági rendszeren belül átgondolt koncepció eredménye. A biztonsági rendszeren belüli változásokat, fejlesztéseket képes lekövetni, illetve önálló egységként is továbbfejleszthető. A biztonságtechnika és az IT-terület fejlődése szorosan összefüggenek, az analóg rendszerek helyét egyre inkább átveszik a digitális megoldások, amelyekhez elengedhetetlen az IT-infrastruktúra fejlesztése. A rendszerek működéséhez szükséges személyzet tudását fejleszteni kell a megfelelő felkészültségi szint eléréséhez. A speciális tudás megszerzésére nem áll rendelkezésre iskolarendszerű vagy azon kívüli képzés, amelynek segítségével megfelelő alapokat kapnának az SOC-személyzet leendő tagjai. Az ismereteket munka közben, tapasztaltabb kollégáktól kapják meg, amihez hozzájárul még az objektumspecifikusan kidolgozott tréningtematika, amelyet a vagyonvédelmi vállalkozás vagy a megbízó vállalat biztonsági szakemberei dolgoznak ki. A vállalatbiztonsági kultúrával rendelkező cégek esetében a biztonsági folyamatok keretrendszere jobbára már adott, szerves része az átgondoltan megtervezett SOC.

Felhasznált irodalom

Christián László (2014a): *A magánbiztonság elméleti alapjai.* Budapest: NKE RTK.
Christián László szerk. (2014b): *Létesítményvédelem.* Budapest: Nemzeti Közszolgálati Egyetem.
Fennelly, Lawrence J. (2013): *Effective Physical Security.* Butterworth–Heinemann.
Garcia, Mary Lynn (2008): *The Design and Evaluation of Physical Security Systems.* Butterworth–Heinemann.
Horváth Tamás (2018): *Elektronikus megfigyelő- és ellenőrző rendszerek objektumorientált kialakítása különös tekintettel a biztonsági kockázatok rendszére.* Budapest: Óbudai Egyetem Biztonságtudományi Doktori Iskola.