HADMÉRNÖK

VI. Évfolyam 3. szám - 2011. szeptember

Lasz György
georgelasz@gmail.com

A BIZTONSÁGTECHNIKA ALAPJAINAK MEGJELENÉSE AZ OBJEKTUMVÉDELEM GYAKORLATÁBAN

Absztrakt

A rendezvénybiztosítás mellett az objektumvédelem a legnagyobb felségterülete a magánbiztonsági szolgálatoknak. A biztonságtechnika tudományos alapjainak ismerete nélkül azonban hosszabb távon nem létezhet magas szintű (objektum)védelem, nem lehet professzionális szolgáltatás, de facto: nem lehetnek elégedett ügyfelek.
Az információtechnológia mellett a védelmi szolgáltatások során használt eszközök és technikák fejlődése is jelentős, amelyek sokszor nem megfizethetőek a magánbiztonsági piacon, sokan kizárólag az állandó élőerős őrzés elkötelezettjei, noha a távfelügyeleti szolgáltatások rejtette protokollok - amelyek egyszerre tartalmazzák az elektronikus jelzőrendszerek kiszámíthatóságát és az élőerős védelem garantálta jelenlétet - többre érdemesek.

Besides the event security, the biggest area of private security services is the physical security. But high-level (physical)security cannot exists through a long term without knowledge of the scientific basis of security technology, it can't be a professional service, de facto clients can't be satisfied.
Besides the information technology, also the development of techniques and appliances used in protection services is important, whiches are often not affordable in the private security market, many people are committed to the permanent, manpower guarding, though protocols in distance surveillance - whiches include both computability of the electronic indicator systems and attendance ensured by manpower protection - are more worthy.

Kulcsszavak: *biztonságtechnika, objektumvédelem, magánbiztonság ~ security technology, physical security, private security*

BIZTONSÁG ÉS TUDOMÁNY

A biztonságtudomány nem régi keletű fogalom, így elemeinek meghatározása, cizellálása minden, ezzel foglalkozó kutató számára izgalmas kérdés. Publikációm bevezetőjében a második Biztonságtudományi Világkonferencián elhangzott elméleti koncepciókból és gyakorlati megismerősekből egyaránt merítettem. A biztonság nélkülözhetetlen eleme életünk minden részének, prioritás: bolygónk biztonságától, családunk, személyes biztonságunkon át lakóhelyünk nyugalmáig. Ebből is következik, hogy a biztonságtudomány az élet minden területét átfogja s tanulmányozza a rendszerek, közöttük a termelési rendszerek változásainak alapjait. Fejlődése cáfolja, hogy a biztonság a termelési rendszertől függ, s fejlődése a technológiai fejlődés mögé kényszerülne.[1] A biztonságtudomány célja a rendszerek biztonsági funkció központú elemzése, a rendszerbiztonság tervezése, részletes kidolgozása.

Ezekből fakadóan a biztonságtudomány az egészségmegőrzés egyik eszköze és az objektív valóság létező állapotának egyik aspektusa is egyben. A biztonság iránti igény, akár a biztonsággal kapcsolatos problémák az emberi gondolkodással egyidős. A megismerés a kisebbtől a nagyobb felé, vagyis a kevésbé ismerttől a bonyolultabb megismerése felé halad, amelyben több kutató szakaszokat azonosít (ártatlanság, felfedezés, rendszer biztonság, biztonságtudomány). A biztonságtudomány rendszere horizontálisan a filozófia mellett a biztonság és biztonságtechnikai tudományra figyel, vertikális rendszerében a biztonsági filozófia és az egyes horizontális elemek helyezkednek el. Ismernünk kell azonban a biztonság tervezésére vonatkozó két legfontosabb törvényt: teljes biztonságra törekedni kötelező, azt megvalósítani azonban nem lehet,[2] s minden biztonsági tevékenység eltérő hatékonysággal bír.

A biztonságtudomány számos vizsgálati módszerrel rendelkezik (HAZOP - hazard and operatibility studies, azaz veszély és működőképesség vizsgálat; ETA - event tree analisy, eseményfa elemzés; AEA - activity error analysis; TA - task analyis, feladat aanalízis; IEA - intital event analysis, kezdeti eseményelemzés; stb.) - ám ezek közül, munkám gyakorlatára figyelemmel hármat veszek nagyító alá. Az objektumvédelmet megelőző kezdeti eseményelemzésről, a feladat, valamint a végesemény elemzésről szólok.

Kezdeti eseményanalízis (IEA - inital event analysis), feladat- (TA - task analysis) és végesemény elemzés (PFA - post factum analysis) az objektumvédelemben[3]

A kezdeti eseményanalízis minden vállalást megelőző feladat. Ennek során összevetjük, hogy a rendelkezésre álló vagy elérhető erő, humán és infrastruktúra alkalmas-e a feladat végrehajtására, a megbízói igény teljesíthető-e? Ennél az eljárásnál a rendszert elemenként vizsgáljuk. Nézzük a jogi környezetet, a helyi normákat, ezek akklimatizálhatóságát, a lehetséges kockázati tényezőket. Szükséges ehhez minden dokumentáció, tervrajzok, biztonsági útvonalak, az objektum teljes műszaki és egyéb dokumentációja. Figyelnünk kell a számítógépes, felügyeleti rendszerekre, ezek programjaira, javítási és karbantartási utasításokra, korábbi veszélyhelyzetekre.

A feladat elemzés[4] megkerülhetetlen módszer, gyakorta használjuk a távfelügyeleti rendszerekben is, hiszen az emberi, felügyelői hibák elemzését nagyban segíti. A legelső lépés

---

[1] KISS Sándor: Biztonságtechnika alapjai. Főiskolai jegyzet, Budapest, 2004. Zrínyi Miklós Nemzetvédelmi Egyetem, Bolyai János Katonai Műszaki Főiskolai kar.

[2] A tételek innen: Hans A. Merz és Hans Bohnenblust megállapításai itt: Cost/Effectiveness Analyses and Evaluation of Risk Reduction Measures, 2-nd World Congress on safety Science Budapest, 1994.

[3] SOUKAS, Iuko: On the reliability and validity of safety analysis (Espoo, 1989). Innen: Kiss Sándor im. 20. p. A terminológiát Gál Csaba használja először, lásd ugyanitt

[4] McCLAY, R. E.: Using Task Analysis to Estimate the Risk of Human Error (2-nd WCOSS Budapest, 1994)

hogy egy hasonló, optimálisan és biztonságosan működő rendszer modelljét az új objektum védelmére átültetjük, vagy ha nincs ilyen, kidolgozzuk az optimális működési feltételeket, vagyis az általunk, az In-Kal-nál az úgynevezett szuper biztonsági protokollt. Minden részfeladatot is alaptevékenységekre bontunk, ugyanezt tesszük a lehetséges veszélyekkel. Tesszük mindezt azért, hogy a felmerülhető, potenciális hibák beazonosíthatóvá váljanak. Alapegységnek azt a legkisebb azonosítható és célszerű elemet választjuk, amely már megjeleníti az emberi tevékenységet, az érintett munkafeladattal és az ahhoz vezető folyamattal együtt.

A végesemény elemzést ezeket követően dolgozzuk ki, immáron a vállalás tudatában. A tipikus munkafolyamatok áttekintése és megtervezése mellett a krízishelyzetek modellezését, a rendszerelemek csoportosítását is optimalizáljuk, s a hierachia és értesítési, kommunikációs rendszert is fel kell állítanunk. Munkacsoportban dolgozunk, az esetleges eltérő véleményeket rendszeresen modellezzük, átnézzük a korábbi ellenőrzések, viszgálatok tapasztalatait is. Komplett rendszerleíró védelmi dokumentáció készül.

BIZTONSÁGELEMZÉS, KOCKÁZATFELFOGÁS

Minden biztonsági tevékenységet a feladat sajátosságaitól függően tervezhető kockázat kísér. A technikai eszközök jelentősen segítik az adott objektumvédelmi biztosítási feladatatokat, ám meghibásodásukat nem mindig lehet kizárni, ezért azok működtetése újabb kockázat lehet. Ekként tehát a kockázat az objektumvédelem során lehet:

- tervezhető, kiszámítható feladatkockázat;
- kiszámítható (azonnal pótolható) vagy váratlan (nem azonnal korrigálható) technikai kockázat;
- személyi kockázat.

Noha minden megbízás során a kockázat minimalizálására kell törekedni, e fentieket nem szabad figyelmen kívül hagyni. A biztonsági elemzés során megrajzolódnak a kockázatok összetevői, ezek természete és összefüggéseik, ekként nyílik lehetőség azok csökkentésére. Az elemzések során mindenképpen meg kell válaszolni:

- optimális humán és infrastruktúra elosztást feltételezve azt, hogyan található meg az optimális kockázatcsökkentési stratégia - harmóniában a megbízással és a tevékenység jellegével;
- a kockázati szintek meghatározását követően mekkora kockázatcsökkentés szükséges, milyen kritériumok vállalhatók, de facto: mi a kiszámítható kockázat?!

A kockázati tényező egy olyan számérték[5] amely egy meghatározott helyi értékű skálán megmutatja, hogy az adott kockázatra vetített számérték hol helyezkedik el. Ebből a kockázatvállalás mértékére is következtetünk, amelyet a környezet, a felszereltség, s a végrehajtásban részt vevők személye határoz meg. A kockázat mértéke fordítottan arányos a megbízhatósággal, vagyis minél inkább kiszámítható egy rendszer működése és felügyelete annál inkább csökkenthető a kockázat. Ehhez azonban tennék egy megkötést. Minden rendszer üzemeltetésénél fontos, hogy ne alakuljanak ki egészségtelen automatizmusok, amelyek növelik a kockázatot. A humánerőforrások cseréjével, képzésével ezt magabiztosan ki lehet szűrni.

A kockázati tényező meghatározásánál figyelembe kell venni annak valószínűségét, hogy az valóban bekövetkezik-e, erre SWOT elemzéssel is törekszünk. E tényező értékét a technikai, felügyeleti eszközök minden, legkisebb elemére is meg kell határozni. A kockázati határérték azt fejezi ki, hogy az adott közeg (egyén vagy környezet) milyen mértékben képes

[5] KISS Sándor i.m. 47. p.

tolerálni egy kockázat vagyis egy rendszerzavar bekövetkezését. A határ ott húzódik, ahol az adott közeg (már) hajlandó szellemi, és anyagi erőfeszítéseket tenni a kockázat elkerülése érdekében.

AZ OBJEKTUMVÉDELEM SZINTJEI – ÁLTALÁBAN

Az objektumvédelem azon tevékenységeket jelöli, amelyeket az épületek, ingatlanok és más vagyontárgyak betolakodók elleni védelme érdekében tehetünk. A védelmi rendszer megtervezésekor a három védendő szint a külső és a belső terület valamint a belső tér. Ha két vagy inkább három biztonsági formát tudunk létrehozni mindegyik szinten, több mint valószínű, hogy rendszerünk optimalizált, vagyis: hatékony objektumvédelmi rendszerrel rendelkezünk. William Deutsch ennek kapcsán három szintről ír.[6]

Az ingatlan külső területét a határai jelölik ki. Ezen terület védelmében célunk annak ellenőrzése, ki közelít belépési szándékkal. A védelem egyik legextrémebb formája a magas fal, zsilipes kapu, szögesdrótkerítés fegyveres őrrel védett kapuval. Más esetekben egy egyszerű sövény is elegendő. Annak eldöntésekor, hogy milyen biztonsági formát hozzunk létre, mérlegelni kell egy betolakodó belépésének kockázatát és az elérhető biztonsági intézkedések költségét. Két biztonsági elgondolást jelent a terület védelmében a Természetes Belépést Ellenőrzés (Natural Access Control) és a Területi Megerősítés (Territorial Reinforcement). Más és más teendőink vannak üzleti objektumok vagy magánlakóingatlan(ok) esetében.

A Natural Access Control[7] egyike a CPTED (Crime Prevention Through Environmental Design - bűnmegelőzés az épített környezet tervezése által) négy alapelvének. Az alapelvek az elkövetők gondolatainak előrelátásán és egy, a véghezvitelt elriasztó környezeti klíma létrehozásán alapulnak. Amikor a CPTED-et a gyakorlatba ültetik át - hívja fel a figyelmet többek között Deutsch -, olyan környezetet eredményez -magában foglalva az épületét és az azt körülvevő területet-, amely akadályozza a kriminális viselkedést, és ugyanakkor ösztönzi a polgárokat, hogy szemfülesek legyenek. Bár ezen elveket az új épületek terveihez, konstrukcióihoz fejlesztették, a koncepció alkalmazható a már meglévőknél is.

Az első megfontolandó dolog a Natural Access Control esetében a terület megközelítése. Be tudnak-e hajtani a járművek észrevétel nélkül a területre? Ha igen, fontolóra kell venni kapuk, sorompók és járdaszegélyek, irányító táblák, természetes épített környezeti tárgyak használatát, melyek irányítják a járműforgalmat az egyes ellenőrzött területekhez. Fontos, hogy ezek áttekinthetőek legyenek, és ne teremtsenek lehetőséget elrejtőzésre! Ezen ellenőrzött bejáratok biztonsági személyzethez vezessenek! Amikor a jármű belép a területre, a vezetőt a jól körülhatárolt parkolóhoz kell irányítani. Vizsgálnunk kell a gyalogosforgalmat. Ha illetéktelenek be tudnak jönni az épületbe, akkor nyilvános kaput kell felállítani. Ideális esetben ez a kapu az őrséghez vagy a recepcióhoz vezet, ahol fogadják a látogatókat. A tető a másik problémás terület. Koncentráljunk arra, hogy minden bejutást innen is korlátozzunk, megakadályozzunk. Ha a tető menekülési útvonal, helikopter leszállópálya is, akkor felügyelnünk kell a forgalmat.

Az elkövetők az észrevétel nélküli bejövetelnél még inkább igyekeznek gyorsan eltűnni. Azonban a kijáratok korlátozása még nehezebb, mint a bejáratoké az élet biztonságának fontossága miatt. A tűzvédelmi előírások nem mindenütt engedik bezárni az épület kijáratait, még ha ezen kijáratok a raktárépület távoli területén vannak is. A problémát ellensúlyozhatjuk, ha a kijáratok körülötti területeket nyitottá és láthatóvá tesszük, amennyire csak lehet. Amíg nem kerül alkalmazásra a rendszer (Natural Access Control), késleltető kijárati hardware-t szerelhetünk a vészkijáratokhoz. Ez a hardware riaszt és kb. 15

[6] http://bizsecurity.about.com/od/physicalsecurity/a/What_is_physical_security.htm
[7] Uo.

másodpercig zárva tartja az ajtót azután, hogy valaki megnyomja azt a kinyitás érdekében. A hang figyelmeztet arra, hogy valaki megpróbál észrevétel nélkül kijutni, illetve ad egy rövid időt a reagálásra. A késleltetett kijárati ajtókat egyértelműen jelezni kell, hogy bárki tudja, az ajtó kinyitásának megkísérlése esetén a riasztó riasztani fog. Ahogy a bejáratoknál, itt is ideális, ha a kijáratok a gyalogosokat és a járműveket az őrséghez vagy a recepcióhoz vezetik.

A fegyveres őr kérdése gyakorta vitatott kérdés. A külön tanulmányt megérő pro és kontra állításokat jelen alkalommal nem részletezem, ám a honi gyakorlat szerint erre leginkább csak jelentős pénzforgalmú, vagy kiemelt kockázatú objektumok esetén alakult ki gyakorlat. Noha az ügyfél kérése és igénye e szempontban is meghatározó, a fegyveres őr alkalmazása nagyon gondos megfontolást, körültekintő felmérést igényel, s persze a költségek emelkedését is feltételezi.

A Territorial Reinforcement célja az illetéktelen belépés és kilépés megelőzése, és a magán- és köztulajdon közötti világos különbségtétel. Ez a különbségtétel két okból fontos: a jogos tulajdonosnak a tulajdonlás érzése és az általa a nem oda tartozók figyelmeztetése miatt, másrészről, hogy a betolakodók nehézségekbe ütközzenek a bejutásnál. A Territorial Reinforcement nem ugyanaz, mint a területi védelem, de a célja mindkettőnek ugyanaz: a betolakodók távoltarása az ingatlantól.

A CPTED négy alapelve:

- Természetes felügyelet
- Natural Access Control
- Territorial Reinforcement
- Karbantartás.

Egyértelmű különbséget tehetünk a köz- és magánterületek között természetes és mesterséges módon is. Élő sövények és a terep adottságai hatékony módjai lehetnek az ingatlan határvonalainak meghúzásához. A derékig érő kerítéseket ugyan könnyű átmászni, de ezek hatékonyak a határok létrehozásában. Az ingatlan határainak megszabásánál a kerítéseket és tereptárgyakat kellően alacsonyan kell tartani, minthogy ezek láthatóan tarják az oldalvonalakat nem engedve teret a rejtett területeknek. Riasztó vagy kamerarendszer alkalmazása esetén táblák és ablak matricák hozzá tudnak járulni az előbbiek elriasztó erejéhez. Ezen jelek feltűnő helyeken való kirakása figyelmezteti a lehetséges elkövetőket, hogy a kriminális tevékenységet rögzítik, illetve reagálnak arra.

A belső terület az épület nyílászárói és falait által határolt terület. Erre legalább olyan figyelemmel kell lennünk, mint a külső területekre. A belső terület védelmét általában zárakkal, kapukkal, zsiliprendszerrel, kamerával és riasztó rendszerekkel valósítjuk meg. A zárak és kulcsok használatának célja a betolakodók kívül tartása. Egy elektronikus belépést felügyelő rendszer szintén hasznos eszköze a belső terület felé irányuló forgalom ellenőrzésének. Végül, a riasztó rendszer figyelmeztet, amikor a területet megsértették.

A kamera fontos kontroll lehet, események esetén pedig bizonyíték erejű. Ha illetéktelenek a tulajdonos tudomása nélkül tudnak másolatot készíteni a kulcsokról, az a biztonság komoly gyengeségét jelenti.

A belső tér a biztonság utolsó szintje, amely az épület belső terét foglalja magában. A biztonsági kamerák hatékony eszközei a belső tér ellenőrzésének, melyek felvételei bizonyítékai lehetnek a későbbi nyomozásnak. Védhető a belső tér mozgásérzékelőkkel, melyek érzékelik a betolakodók, őrök jelenlétét. Elektronikus belépést ellenőrző rendszer szintén alkalmas a forgalom ellenőrzésére és az illetéktelenek védett területre való belépésének megelőzésére.

ÚTMUTATÓ AZ OBJEKTUMVÉDELMÉHEZ

Szögezzük le: megkerülhetetlen védelem nincs, de a kockázat minimalizálható akkor, ha követünk egy elfogadott sémát. Javaslataim az alábbiak:

- Professzionális magánbiztonsági szolgáltatót válasszunk, referenciával, gyakorlattal!
- Alkalmazzunk zsiliprendszeres beléptetést, különösen az üzleti objektumoknál!
- Kizárólag biztonsági ajtókat és reteszzárakat alkalmazzunk!
- Használjunk kulcs-felügyeleti stratégiát! Abban az esetben, ha nem tudjuk, kinél vannak kulcsaink, vagy akiknél találhatóak, lemásolhatják-e azokat a beleegyezésünk nélkül, komoly rés van a biztonsági tervben. Elsőként fizikailag védeni kell az ajtókat, majd biztonságban tartani a kulcsokat egy felügyeleti stratégia kialakításával.
- Építsünk ki rendőrségre, vagy a biztonsági felügyeleti céghez bekötött riasztórendszert!
- Egy ellenőrzött riasztórendszer két alapvető célt szolgál: beindítja a szirénát, mely a betolakodót elijeszti, másodszorra riasztja a rendvédelmi szakembereket, akik reagálni tudnak a betörésre.
- A hivatkozott W. Deutsch ajánlása: "Floor Marshall" kijelölése.
- Erre leginkább akkor kerülhet sor, ha nem használunk biztonsági szolgálatot. A Floor Marshall egy olyan önkéntes a szervezetben, akinek feladata az ismeretlen látogatók megközelítése és az arról való meggyőződés, hogy legális céljuk van-e a területen tartózkodásra. Illetve ugyanő más alkalmazottak részére olyan személyeket biztosít, akik jelentik a gyanús egyéneket. Ez társasházaknál is megszervezhető.
- Elektronikus belépést ellenőrző rendszert telepítsünk!
- Ez az üzleti objektumoknál ma már megkerülhetetlen. A mechanikus zárak "nem hazudnak". Az ajtózárak elektronikus belépést ellenőrző rendszerrel való javításával azonban rögzíthetjük azt, aki kinyitja, vagy megpróbálja kinyitni az ajtót. Ez az információ hatalmas segítség, ha nyomozásra van szükség a biztonság megsértése miatt. Emellett a rendszer lehetővé teszi elektronikus kulcsok azonnali hozzáadását vagy elvételét. Ez kiküszöböli az elvesztett vagy ellopott kulcsok miatti védtelen állapotot, és megengedi az időn, dátumon vagy jogosultsági szinten alapuló testre szabott belépési privilégiumok kijelölését.
- Videófelügyelet használata.
- Nem csak a terület ellenőrzésének képességét javítják a kamerarendszerek, hanem hasznos bizonyítékot és információt szolgáltatnak, ha nyomozásra van szükség egy balesetnél, támadásnál vagy lopásnál. Az alkalmazottaknak titokban kell tartaniuk a felügyeleti rendszerek alkalmazását.
- Ismeretek szerzése a bűncselkemények megelőzéséről.

KIEGÉSZÍTÉSÜL

Amíg a terület és a belső rész védelmében vannak átfedések (pl. őrök és kamerák, melyek meg tudják védeni a kettőt), ezen három szintnek, és mindegyik szinten két vagy három objektumvédelmi intézkedés létrehozásának jegyében való gondolkodás segít végrehajtani az alkalmas objektumvédelmi intézkedéseket.

Az angol irodalomban a Crime Prevention Through Environmental Design (CPTED) a bűncselekmények végrehajtását bátortalanító gátló elvek sora. A koncepció egyszerű: Az épületeket és ingatlanokat a természet erőinek és a természeti csapások károsító hatásának

megelőzésére tervezték; a bűn megelőzésére is megtervezettnek kell lenniük. Ezen elveket használhatjuk az otthoni irodák, és felhőkarcolók esetében is. A megelőző felmérés, tanácsadás cégünk szolgáltatásai között is elérhető, s keresett.

A Natural Access Control rendszer olyan elemeket használ, mint a járdasziget, járda vagy ajtók, melyek a gyalogos- és a járműforgalmat irányítják az ingatlanunkon. A rendszer célja a kockázat észlelésének előidézése a lehetséges elkövetők gondolataiban az ellenőrzés érzésének kiiktatásával.

A Territorial reinforcement szándéka nem annak megelőzése, hogy valaki területünkre belépjen, a betolakodók kívül tartásához őrökre, kapukra, szögesdrót-kerítésekre és hasonló dolgokra van szükség. Ennek célja inkább a lehetséges elkövetők számára annak az üzenete, hogy az adott terület máshoz tartozik. A CPTED más elveinek kombinálásával hatékony lehet a kriminálprevencióban.

Felhasznált irodalom

[1] KISS Sándor: Biztonságtechnika alapjai. Főiskolai jegyzet, Budapest, 2004. Zrínyi Miklós Nemzetvédelmi Egyetem, Bolyai János Katonai Műszaki Főiskolai kar

[2] MERZ, Hans A. és BOHNENBLUST, Hans megállapításai itt: Cost/Effectiveness Analyses and Evaluation of Risk Reduction Measures, 2-nd World Congress on safety Science Budapest, 1994.

[3] SOUKAS, Iuko: On the reliability and validity of safety analysis (Espoo, 1989). Innen: Kiss Sándor im. 20. p. A terminológiát Gál Csaba használja először, lásd ugyanitt

[4] McCLAY, R. E.: Using Task Analysis to Estimate the Risk of Human Error (2-nd WCOSS Budapest, 1994)

[5] http://bizsecurity.about.com/od/physicalsecurity/a/What_is_physical_security.htm

[6] TRUMP, Kenneth S. – a Nemzeti Iskolai Biztonság és Biztonsági Szolgáltatások, Cleveland-i, nemzeti konzultációs, iskolai biztonságra és vészhelyzetekre felkészítő tréningre és konzultációra specializálódott cég elnöke in: American school Board journal/February 2007, p. 26-29.

[7] http://www.counterterrorbusiness.com/features/93-event-security/481-bringing-home-the-gold-in-event-security

[8] JACOBS, Jerome, ©27-01-2009.
Forrás:
http://www.iacpo.org/index.php?option=com_k2&view=itemlist&layout=category&task=category&id=5&Itemid=130