DOI: https://doi.org/10.12700/btsz.2026.8.1.53

APPLYING LAYERED PHYSICAL SECURITY FOR THE PROTECTION OF CRITICAL ORGANIZATIONS

TÖBBRÉTEGŰ FIZIKAI VÉDELEM ALKALMAZÁSA A KRITIKUS SZERVEZETEK VÉDELMÉBEN

NAGY Gergely[1]

Abstract

Recent developments in the fields of security and security policy have once again drawn attention to the decisive role of physical protection for critical infrastructures and institutions essential to the functioning of society. The European and Hungarian regulatory environment, as well as legislation adopted in the course of legal harmonisation and certification requirements imposed on certain organisations, prescribe concrete physical and environmental protection measures. The study presents an easily adaptable, multilayered framework based on the principles of defence in depth. Through the structured logic of interconnected security zones, it provides transparency regarding areas of responsibility and the designation of necessary controls. The model applies a risk-proportionate approach, defining protective measures on the basis of relevant threats, exposures, and critical dependencies, thereby supporting business continuity. The proposed framework serves both as a practical planning guideline for strengthening physical security and as a compliance framework for meeting applicable legal and standards-based requirements.

Keywords

layered defense, defense in depth, hybrid warfare, industrial security

Absztrakt

Az elmúlt időszak biztonsági és biztonságpolitikai fejleményei ismét ráirányították a figyelmet a kritikus infrastruktúrák és a társadalom működése szempontjából jelentős intézmények fizikai védelmének meghatározó szerepére. Az európai és hazai szabályozási környezet, valamint a jogharmonizáció során megalkotott előírások és tanúsítványi követelmények konkrét fizikai és környezeti védelmi intézkedéseket is megfogalmaznak. A tanulmány egy könnyen adaptálható, többrétegű védelemre épülő keretrendszert mutat be a mélységi védelem elveinek alkalmazásával, amely biztonsági zónák egymásra épülő logikáján keresztül teszi átláthatóvá a felelősségi területeket és a szükséges kontrollok kijelölését. A modell kockázatarányos megközelítést érvényesít: a védelmi intézkedéseket a releváns fenyegetettségek, kitettségek és kritikus függőségek ismeretében határozza meg, támogatva az üzletmenet-folytonosság fenntartását. A bemutatott modell egyszerre szolgál gyakorlati tervezési alapelvként a fizikai biztonság megerősítéséhez, valamint megfelelési keretként a vonatkozó jogszabályi és szabványi elvárások teljesítéséhez.

Kulcsszavak

többrétegű védelem, mélységi védelem, hibrid hadviselés, létesítmény biztonság

[1] gergely.nagy777@gmail.com | ORCID: 0009-0004-2590-2120 | information security expert |információbiztonsági szakértő, We-Know Zrt.

BEVEZETÉS

A 2025-ös év egyik meghatározó biztonsági és biztonságpolitikai trendje a fizikai biztonság felértékelődése volt. A globális digitalizáció folyamata továbbra sem tört meg, és ezzel párhuzamosan a kiberbiztonság jelentősége is tovább növekedett, számos olyan esemény történt Magyarországon, valamint közvetlen és tágabb környezetünkben, amelyek ismét ráirányították a figyelmet a fizikai térben megvalósuló védelem megkerülhetetlen szerepére. A kritikus infrastruktúrák, pénzintézetek, közintézmények és katonai létesítmények őrzés-védelme továbbra is kulcsfontosságú, nem kiváltható biztonsági tényező.

Az elmúlt év során több, nagy visszhangot kiváltó esemény is rávilágított a társadalom működése szempontjából fontos intézmények fizikai védelmének sérülékenységeire. Az év végén történt az elmúlt évtizedek egyik legnagyobb bankrablása, valamint a Louvre ékszerrablása, Magyarországon pedig több alkalommal is felfedező kedvű fiatalok jutottak be kritikus infrastruktúra-létesítményekbe. Ezek az esetek, bár részben haszonszerzésből vagy kalandvágyból elkövetett cselekmények sok esetben súlyos rendszerszintű hiányosságokra mutatnak rá.

A fenti incidenseknél lényegesen komolyabb kihívást jelent Oroszország fokozódó hibrid hadviselési tevékenysége, melynek keretében 2022 óta szisztematikus, nem hagyományos hadviselési kampányt folytat Európa ellen, amelynek központi eleme a kritikus infrastruktúrák elleni szabotázs, vandalizmus és kémkedés. A cél elsősorban nem az azonnali fizikai rombolás vagy tömeges emberáldozatok okozása, hanem az európai társadalmak destabilizálása, az Ukrajna támogatásával összefüggő politikai és társadalmi költségek növelése, valamint a NATO és az Európai Unió kollektív reagálóképességének gyengítése.

Európa kritikus infrastruktúrája különösen sérülékeny a hosszú évtizedeken át halogatott beruházások, az elöregedett rendszerek, valamint az egymásra utalt hálózatok miatt. Oroszország ezt a helyzetet tudatosan használja ki, célpontjai között szerepel az energiaellátás, a közlekedés, a kommunikáció, a vízellátás, az egészségügy, valamint a katonai és logisztikai infrastruktúra. [1, p. 2]

A biztonsági fenyegetések mellett az európai és magyarországi vállalatoknak, valamint közigazgatási szerveknek egyre összetettebb jogszabályi megfelelési kötelezettségeknek is eleget kell tenniük. A NIS2 és a CER irányelvek[7] [8], valamint az ezekhez kapcsolódó hazai jogharmonizáció során megalkotott jogszabályok[2] [3] és végrehajtási rendeletek [4] [5] már konkrét fizikai védelmi intézkedések bevezetését is előírják a több mint 3000 érintett hazai szervezet számára. A vonatkozó hazai jogszabály a 2-es ellenálló képességi szintbe tartozó szervezetek számára konkrétan előírja „a kritikus infrastruktúrák területén a biztonság több rétegű kialakítását, amely késlelteti a legnagyobb védelmet igénylő területek elérését.”[4 2.2]

Ezzel párhuzamosan egyre több nagyvállalat követeli meg beszállítóitól olyan információbiztonsági tanúsítványok (pl.: ISO/IEC 27001, TISAX) megszerzését, amelyek nemcsak logikai, hanem fizikai biztonsági kontrollokat is előírnak, ideértve a fizikai hozzáférés korlátozását, a létesítmények védelmét (behatolás, tűz, betekintésvédelem stb.), valamint az eszközök és adatok fizikai biztonságának fenntartását.

A tanulmány célja, hogy egy könnyen adaptálható keretrendszert és gyakorlati segítséget nyújtson az érintett szervezetek számára: egyrészt a jogszabályi és beszállítói megfelelési követelmények teljesítésében, másrészt saját fizikai és szervezeti rezilienciájuk mérhető és fenntartható növelésében.

MÉLYSÉGI VÉDELEM

A mélységi védelem (Defense in Depth) koncepciója a katonai stratégiai tervezésből ered, ahol célja olyan akadályok komplex rendszerének kialakítása volt, amelyek lassítják és feltartóztatják a támadó felet céljai elérésében, miközben lehetőséget biztosítanak tevékenysége folyamatos nyomon követésére, valamint a megfelelő válaszlépések kidolgozására és végrehajtására a támadás elhárítása érdekében.

A koncepciót viszonylag régóta alkalmazzák a nukleárisipar területén is, ahol a balesetek hatásainak elszigetelése érdekében három egymástól független, egymást követő védelmi gát kerül kialakításra, ami alacsony szintre csökkenti annak valószínűségét, hogy egy baleset a létesítményen kívül is hatást gyakoroljon. Az alapelv szerint, minden biztonsági berendezést eleve sérülékenynek kell tekinteni, ezért azt egy további védelmi eszközzel kell védeni. [9, p. 9]

A kiberbiztonsági megközelítésben a mélységi védelem olyan megelőző és észlelő intézkedések összességét jelenti, amelyek akadályozzák a támadó előrehaladását, miközben lehetővé teszik a behatolás időben történő felismerését és a reagálást, a biztonsági incidens következményeinek csökkentése érdekében.

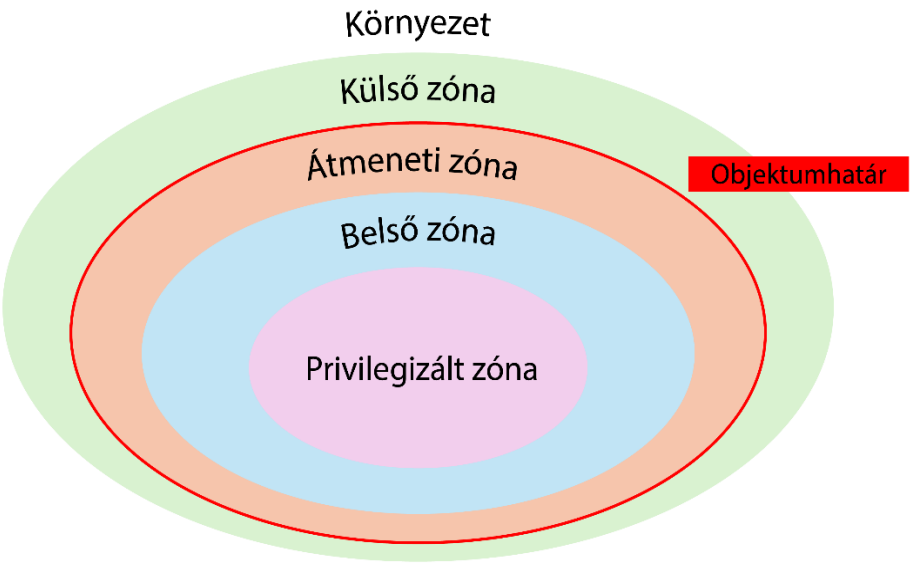
A mélységi védelem nem egy az egyben történő megfeleltetésen alapul, vagyis egy-egy konkrét kockázatra nem egyetlen megoldással, válaszlépéssel válaszol. Ezzel szemben holisztikus megközelítést alkalmaz, amely a szervezet valamennyi eszközének védelmét célozza, figyelembe véve azok kapcsolatait és egymásrautaltságát. A rendelkezésre álló erőforrások felhasználásával olyan, egymásra épülő megfigyelési és védelmi rétegek kerülnek kialakításra, amelyek a szervezet tényleges kitettségéhez és üzleti kockázataihoz igazodnak, ezáltal hatékony és kockázatarányos védelmet biztosítva. [10, p. 2]

A védelmi intézkedések alkalmazása tehát nem – lehet – öncélú, hanem szorosan kell kapcsolódnia a szervezet alapvető működési céljaihoz. Elsődleges rendeltetése a szervezet üzletmenet-folytonosságának fenntartása, valamint a kritikus folyamatok és erőforrások védelme. Ennek megfelelően a többrétegű védelmi intézkedések kiválasztása és kialakítása során a kockázatarányosság elvét kell érvényesíteni és a bevezetett kontrolloknak kizárólag olyan mértékben szabad korlátozniuk a szervezet mindennapi működését, amennyire a fenyegetések kezeléséhez feltétlenül szükséges.

A túlzottan szigorú vagy nem megfelelően illesztett védelmi intézkedések önmagukban is kockázatot jelenthetnek, mivel felesleges többletköltséget jelentenek, akadályozhatják az üzleti folyamatokat és hosszútávon a szabályok megkerülésére ösztönözhetik a felhasználókat. Ez adott esetben azt is jelentheti, hogy egy belsőbb védelmi zónában „enyhébb" védelmi intézkedések is elfogadhatóak. A mélységi védelem sikeres alkalmazása csak akkor valósulhat meg, ha a kontrollok kiegyensúlyozott, a működéshez illeszkedő rendszerként kerülnek kialakításra.

TÖBBRÉTEGŰ VÉDELMI MODELL

A mellékelt védelmi modell nem új szemléletet vezet be, hanem a jelenleg hatályos hazai jogszabályi környezet, valamint a vonatkozó nemzetközi szabványok és bevált jógyakorlatok rendszerbe foglalt alkalmazására épül. Emellett a szervezetek meglévő üzletmenet, működési-folyamati és infrastrukturális sajátosságaihoz illeszthető.



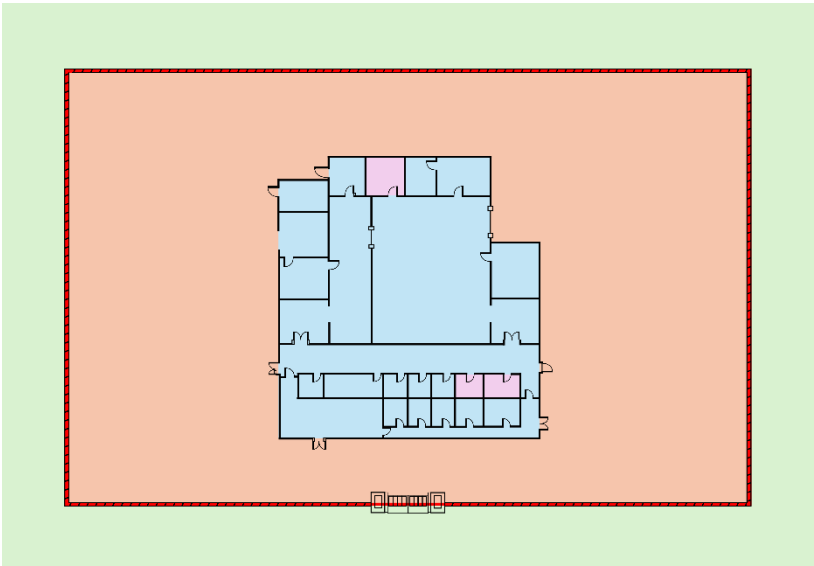
1. ábra – Védelmi zónák rétegrendje. Forrás: saját szerkesztés.

A modell célja a felelősségi területek, illetve az egyes területeken alkalmazandó védelmi intézkedések egyértelmű kijelölésének és kiválasztásának megkönnyítése. A modell strukturált keretet biztosít a fizikai biztonsági intézkedések tervezéséhez és értékeléséhez, elősegítve a következetes és kockázatarányos védelem kialakítását.

Fontos hangsúlyozni, hogy egy szervezet a gyakorlatban nem kizárólag egy-egy zónával rendelkezhet: a működés jellegétől, méretétől és kockázati kitettségétől függően az egyes zónákból több is kijelölhető, akár párhuzamosan, akár egymástól elkülönülően. Ugyanakkor a zónák egymásra épülő rétegrendjének – az ábrán meghatározott logika szerinti – megtartása a modell működőképességének alapfeltétele.

A zónák sorrendje nem felcserélhető, minden belsőbb védelmi szint csak az azt megelőző rétegek működése mellett képes megfelelően ellátni funkcióját. Ez a felépítés biztosítja, hogy az egyes védelmi intézkedések ne önálló, elszigetelt elemekként jelenjenek meg, hanem a mélységi védelem alapelvének megfelelően, egymást erősítő, koherens rendszerként támogassák a szervezet biztonságát. Amennyiben nem megoldható, hogy az adott zónát az alacsonyabb védelmi szintű zóna fizikailag is teljesen körbevegye, úgy a rétegrendet legalább a megközelítési útvonal tekintetében kell alkalmazni.

Egyes kritikus rendszerelemek esetében indokolt lehet a védelmi modell nem kizárólag síkbeli, hanem térbeli értelmezése is. Elsősorban a pilóta nélküli légieszközök, drónok elterjedése miatt, lehetőség szerint a fizikai biztonsági rétegek a fizikai tér teljes spektrumában értelmezendők. Ennek megfelelően a modell alaplogikája nemcsak a horizontális elrendezésben, hanem adott esetben a megközelítési irányok teljes halmazára kiterjedően is alkalmazható lehet.



2. ábra – Minta kialakítás: ipari létesítmény alaprajza, a zónák jelölése az 1. ábrán alkalmazottal megegyezik. A felső privilégizált zóna esetében csak a megközelítési útvonalak, az alsó két privilégizált zóna esetében teljes spektrumban alklmazott védelmi rétegekkel. Forrás: saját szerkesztés.

VÉDELMI ZÓNÁK

Környezet

A környezet a szervezet működésének tágabb fizikai és nem fizikai, így különösen jogi, gazdasági, társadalmi és biztonságpolitikai elemeit és összefüggéseit foglalja magába. Ebbe a dimenzióba tartoznak mindazon külső tényezők, amelyek a szervezet működésére hatással lehetnek, ugyanakkor többnyire közvetlen befolyásolási körén kívül esnek, vagy csak rendkívül korlátozott mértékben befolyásolhatók.

A szervezettel kapcsolatos kockázatok jelentős része ebben a külső térben gyökerezik: a geopolitikai folyamatok, a jogszabályi környezet változásai, a gazdasági helyzet, a társadalmi feszültségek, valamint az általános biztonsági környezet mind olyan tényezők, amelyek közvetlenül vagy közvetve hatással vannak a szervezet fenyegetettségi szintjére.

A környezethez kapcsolódó kontrollintézkedések célja nem a közvetlen fizikai védelem, hanem a szervezet működését érintő külső kockázatok korai felismerése, értelmezése és kezelhetővé tétele. A külső környezet változásainak értelmezése nélkül nem alakítható ki reális kép a fenyegetettségekről és nem határozhatók meg megalapozottan a szervezet fizikai biztonsági intézkedései. A külső környezeti tényezők vizsgálata így a mélységi védelem kiindulópontja, amely meghatározza a további zónákban alkalmazandó védelmi szinteket és kontrollokat.

Elsődleges védelmi intézkedésként a szervezet részéről egy átfogó, dokumentált és folyamatosan működtetett kockázatmenedzsment-keretrendszer kialakítása és fenntartása szükséges és sok esetben jogszabályi kötelezettség is. [3, 6. § (1)] A szervezetek mindennapi működésük során folyamatosan kockázatokat kezelnek üzleti-működési céljaik elérése érdekében, ideértve többek között a kiberbiztonsági, az ellátási láncok megszakadásából,

vagy a munkavállalók biztonságát érintő kockázatokat. Ennek érdekében olyan folyamatokat kell kialakítaniuk, amelyek lehetővé teszik a működésükkel összefüggő kockázatok értékelését és a kezelésükre vonatkozó döntések meghozatalát a szervezeti prioritások, valamint a belső és külső korlátok figyelembevételével. A kockázatmenedzsment tehát nem lehet egyszeri tevékenység, hanem a mindennapi működésbe ágyazott, folyamatos és iteratív folyamat kell, hogy legyen.[12, p. 44] A kockázatelemzés szerves része a minőség-, környezeti- és információbiztonsági irányítási rendszereknek is, melyek kialakítása egyes szervezetek esetében szintén jogszabályi kötelezettség. [4, 2.2]

A zónához kapcsolódó védelmi intézkedések tehát jellemzően adminisztratív jellegű kontrollok, amelyek a szervezet stratégiai szintű felkészültségét és döntéstámogatását szolgálják. Ide tartozik mindenekelőtt a rendszeres és dokumentált kockázatelemzés, az ellenálló képességi tervek és mátrixok.

Kulcsfontosságú a kritikus függőségek azonosítása, különös tekintettel azokra a külső erőforrásokra és szolgáltatásokra (pl.: közműellátásra, adatkapcsolatokra), beszállítókra amelyek kiesése vagy sérülése aránytalan hatással lehet a szervezet működésére és biztonságára. A környezethez kapcsolódó kontrollintézkedések keretében a szervezet köteles biztosítani a hatóságokkal történő együttműködés és információcsere kialakítását és fenntartását. Célravezető lehet továbbá a nyílt forrású információk (OSINT) monitorozása a szervezetet érintő eseményekről.

Külső zóna

A külső zóna a szervezet közvetlen fizikai környezetét jelenti, amely az objektumhatáron kívül elhelyezkedő területeket foglalja magába, és közvetlen kapcsolatban áll a tágabb környezettel. Ez a zóna képezi a szervezet és a külvilág közötti első érintkezési felületet, ahol a fenyegetések legkorábban megjelenhetnek, ugyanakkor a szervezet befolyása ezen a területen jellemzően továbbra is korlátozott.

Ebbe a zónába tartozhatnak többek között: a közterületek, parkolók és várakozóhelyek, megközelítési útvonalak, a bejáratokhoz, kapukhoz vezető utak, az objektum környezetében található nyílt területek, szomszédos épületek, létesítmények.

Sajátossága, hogy nem kizárólag a szervezet által használt vagy ellenőrzött területeket foglalja magába, mégis jelentős hatással van az objektum biztonságára. A környezeti adottságok, a forgalom jellege, a közvilágítás, a beláthatóság, valamint a szomszédos funkciók mind befolyásolják a későbbi zónákban alkalmazandó védelmi intézkedések kialakítását.

A külső zóna esetében a szervezet elsősorban nem korlátozó, hanem megfigyelő, értékelő és megelőző jellegű tevékenységeket végezhet. A cél nem a teljes kontroll, hanem a fenyegetések korai felismerése, valamint a belsőbb védelmi rétegek megalapozása.

A zónában tipikusan az alábbi tevékenységek végezhetők és szükségesek: a környezeti és biztonsági tényezők folyamatos figyelemmel kísérése (forgalom, események, rendészeti helyzet), amennyiben lehetséges a terület védelmi szempontok szerinti optimalizálása (pl.: kerítés vonalában lévő növénytakaró ritkítása)[4, 2.1], megfigyelési és „elrettentési” eszközök alkalmazása (pl.: közvilágítás, látható kamerák, figyelmeztető jelzések), a megközelítési útvonalak és bejáratok láthatóságának biztosítása, a szomszédos létesítményekből vagy területekről eredő kockázatok azonosítása.

A külső zóna és korlátozottabb mértékig a környezeti zóna esetében a szervezet legnagyobb ráhatása a biztonságra a tervezési szakaszban érvényesül. A beruházási, illetve kivitelezési döntések meghozatala előtt, különösen zöldmezős beruházások esetén kiemelt jelentőségű a létesítmény telepítési helyének megválasztása. [5, 12.49.]

Ebben a fázisban szükséges elvégezni az első, magas szintű kockázatelemzést, amely feltárja a területre jellemző természeti, infrastrukturális, környezeti és biztonsági kockázatokat, és amelynek eredményei alapján kiválasztható az üzletmenet és a biztonság szempontjából leginkább megfelelő helyszín. A nem megfelelő telepítési döntések hosszú távon olyan kockázatokat konzerválhatnak, amik később kizárólag jelentős költségek vagy kompromisszumok árán, bizonyos esetekben pedig még így sem kezelhetők.

Redundáns telephelyek kialakítása esetén a külső zónához kapcsolódó kockázatelemzésnek regionális biztonsági-biztonságpolitikai és akár geológiai szempontokra is ki kell terjednie (pl.: földrengési zónák, tektonikus lemezek elhelyezkedése, időjárási mintázatok).[5, 12.43.]

A külső zónában végzett tevékenységek eredményei közvetlen bemenetet jelentenek a kockázatmenedzsment és a mélységi védelem további szintjei számára, meghatározva az objektumhatáron és azon belül alkalmazandó védelmi intézkedések jellegét és mértékét.

Kiemelt kockázati tényezőt jelentenek az objektum működéséhez szükséges közműellátottsághoz kapcsolódó kritikus függőségek és azok belépési pontjainak védelme [4, 2.2] és esetleges redundanciák kialakításának lehetősége.[4, 2.2] Az energiaellátás, a vízés csatornahálózat, a gázszolgáltatás, valamint a távközlési és adatátviteli infrastruktúra jellemzően az objektumhatáron kívülről érkezik, így azok sérülékenysége, elérhetősége és védelmi szintje a szervezet közvetlen ellenőrzésén kívül esik. E függőségek megszakadása, történjen akár szándékos beavatkozás, akár műszaki hiba vagy természeti esemény következtében, jelentős működési zavarokat és kaszkádhatásokat idézhet elő, amelyek a belső és privilegizált zónák biztonságát és működését is közvetlenül érintik.

Objektumhatár

Az objektumhatár a szervezet által védett terület fizikai és jogi elválasztási vonala, amely kijelöli a külső, jellemzően nem ellenőrzött környezet és az objektum belső, már szervezeti felelősség alá tartozó területek közötti határt. Az objektumhatár a mélységi védelem egyik kulcseleme, mivel többnyire itt történik meg a nyílt környezetből az ellenőrzött térbe való belépés első szintű szabályozása.

Megjelenési formája a létesítmény jellegétől és kockázati besorolásától függően eltérő lehet. Ide tartozhatnak többek között: a kerítések, falak, kapuk és sorompók, természetes akadályokkal (pl.: vízfelület, terepadottságok) megerősített határvonalak. Abban az esetben amikor a fizikai elválasztás korlátozott mértékben valósítható meg jelölések, táblák és egyéb figyelemfelhívó elemek elhelyezése, egyéb építészeti-tájépítészeti megoldások vagy egyes esetekben akár útfelfestések is hatásosak lehetnek. [11, p. 182]

A zóna elsődleges funkciója nem feltétlenül a behatolás teljes megakadályozása, hanem a fenyegetések észlelésének, az elrettentésnek és a behatolási kísérletek késleltetésének biztosítása. A megfelelően kialakított objektumhatár időt nyer a szervezet számára a reagálásra, és lehetőséget teremt a belső védelmi rétegek aktiválására.

Az alkalmazott védelmi intézkedések kiválasztása során is a kockázatarányosság elvét kell érvényesíteni, figyelembe véve az objektum funkcióját, a fenyegetettségi környezetet és a működési sajátosságokat és jogszabályi előírásokat. [4, 1. mellékelt]

Ennek megfelelően az objektumhatáron tipikusan az alábbi eszközök és megoldások jelennek meg: mechanikai védelmi elemek (kerítések, kapuk, zárak), elektronikus jelző- és érzékelőrendszerek (pl.: kerítésvédelem, mozgásérzékelés), kamerás megfigyelőrendszerek, beléptetési pontok és forgalomszabályozó megoldások, őrzés-védelmi és járőrtevékenységek.

Az objektumhatár nem önálló védelmi elem, hanem a mélységi védelem logikai rendszerébe illeszkedő átmeneti pont a külső zóna és az átmeneti zóna között. Hatékony működése feltételezi a külső zónában végzett megfigyelési és kockázatelemzési tevékenységek eredményeinek eredményes felhasználását, valamint a belsőbb zónákban alkalmazott kontrollokkal való összehangolt működést.

Megfelelő kialakítása és üzemeltetése biztosítja, hogy a belsőbb zónákon belül alkalmazott védelmi intézkedések ne legyenek indokolatlanul túlterhelve, miközben hozzájárul a szervezet fizikai biztonságának, üzletmenet-folytonosságának és rezilienciájának fenntartásához.

Átmeneti zóna

Az átmeneti zóna az objektumhatáron belül elhelyezkedő, de még nem teljes mértékben védett terület, amely átmenetet képez a külső, jellemzően nyilvános vagy korlátozottan ellenőrizhető környezet és a szervezet belső, védett működési területei között. Funkcióját tekintve ez a zóna szolgálja a forgalom szétválasztását, az előzetes ellenőrzést, valamint a belsőbb védelmi rétegek tehermentesítését.

Sajátossága, hogy itt különböző jogosultsági szintű személyek tartózkodhatnak egyidejűleg. Ide tartozhatnak például: látogatók és ügyfelek, beszállítók és alvállalkozók, áruszállítást végző személyek, olyan munkavállalók, akiknek nincs jogosultságuk a belső vagy privilegizált zónákba történő belépésre.

Tipikus átmeneti zónák a recepciók, előterek, várók, egyes tárgyalók, rakodóterületek, árufogadó helyek, közintézmények nyilvánosan hozzáférhető belső és látogatóterei.

A zónában alkalmazott védelmi intézkedéseknek is kiegyensúlyozott módon kell biztosítaniuk a biztonságot és a működés folyamatosságát. Ezért jellemzően csak korlátozott ellenőrzési intézkedések alkalmazhatók, a belépés még nem feltétlenül egyéni jogosultsághoz kötött és a hangsúly a megfigyelésen és elkülönítésen van. A túlzottan szigorú kontrollok itt is akadályozhatják az üzletmenetet (pl.: be- és kiszállítást) vagy a szolgáltatások igénybevételét, míg a nem megfelelő védelem közvetlen kockázatot jelenthet a belsőbb zónákra nézve.

Indokolt lehet a látogatók és külső személyek regisztrációja, előzetes azonosítása, forgalomirányítás és mozgási útvonalak kijelölése, vizuális megfigyelés (pl.: kamerarendszerek, személyzet jelenléte), belépési jogosultságok előkészítése a belső zónák irányába, fizikai elválasztás biztosítása a belsőbb területektől (pl.: ajtók, beléptetőpontok), áruszállítás és logisztikai folyamatok ellenőrzött lebonyolítása.

Az átmeneti zóna hatékony működése kulcsszerepet játszik abban, hogy az illetéktelen személyek ne juthassanak tovább a belső védelmi rétegekbe, miközben a szervezet alaptevékenysége zavartalanul folytatható marad.

Az itt alkalmazott intézkedések célja nem a teljes kizárás, hanem a kockázatok elkülönítése, csökkentése és kezelhető szintre hozása, mielőtt azok a belső vagy privilegizált zónákat érintenék.

Belső zóna

A belső zóna az objektum azon területeit foglalja magában, ahol a szervezet alaptevékenysége ténylegesen megvalósul. Ezek a terek nem nyilvánosak, és kizárólag a megfelelő jogosultsággal rendelkező személyek számára hozzáférhetőek. A belső zóna elválasztása az átmeneti zónától a mélységi védelem egyik meghatározó eleme, mivel a zónában üzletmenetkritikus folyamatok is zajlanak.

A zónába tipikusan az alábbi területek tartoznak: irodák, gyártási és termelési területek, raktárak, laboratóriumok, műhelyek, belső kiszolgáló és adminisztratív helyiségek, tárgyalók és olyan zárt terek, ahol üzleti, technológiai vagy személyes adatok kezelése történik.

Az itt alkalmazott védelmi intézkedések célja már nem csupán az elrettentés vagy az észlelés, hanem a jogosulatlan hozzáférés tényleges, fizikai megakadályozása, valamint a szervezet működésének és erőforrásainak védelme. Ennek megfelelően a belépés ebbe a zónába szabályozott és dokumentált, jellemzően egyéni jogosultságokhoz kötött kell hogy legyen. A zónában található munkaterületek további jogosultság alapú elkülönítése is indokolt lehet.[13, p. 6]

A védelem kialakítását ezért jogosultságon alapuló hozzáférés („need to access” elv), a munkakörhöz és feladatokhoz igazított hozzáférési szintek, a fizikai és szervezeti kontrollok összehangolt alkalmazása kell hogy meghatározza.

A mélységi védelem rendszerében a belső zóna a védelmi intézkedések súlypontját jelenti. Míg a külső és átmeneti zónák célja a fenyegetések kiszűrése és csökkentése, addig a belső zóna biztosítja, hogy az objektumba jutott személyek és eszközök csak a szükséges mértékben és ellenőrzött körülmények között férhessenek hozzá a szervezet erőforrásaihoz, valamint előkészíti a legmagasabb védelmi szintet képviselő privilegizált zóna elkülönítését.

Privilegizált zóna

A privilegizált zóna a szervezet objektumán belül kialakított legmagasabb védelmi szintű terület, amely azokat a helyiségeket és funkcionális egységeket foglalja magába, ahol a szervezet működése szempontjából kiemelten érzékeny erőforrások, információk vagy személyek találhatók. A zóna védelme alapvetően meghatározza a szervezet ellenálló képességét, mivel az itt bekövetkező biztonsági incidensek aránytalanul nagy hatással lehetnek az üzletmenetre, a jogszabályi megfelelésre és reputációra.

A zónába tartozhatnak többek között a felsővezetői irodák és tárgyalók, szerverszobák, adatközponti helyiségek, biztonsági szobák, kritikus irattárak, ipari és kritikus infrastruktúra esetén vezérlőtermek, irányítóközpontok.

Az ebben a zónában alkalmazott védelmi intézkedések célja nem csupán a jogosulatlan hozzáférés megakadályozása, hanem a belső fenyegetések minimalizálása, valamint az egyes események gyors és pontos visszakövethetőségének biztosítása. Ennek megfelelően a belépés kizárólag szigorúan szabályozott, személyre szabott és dokumentált jogosultságok alapján történhet, valamint a legkisebb jogosultság elvének (least privilege)[4, 2.1] is érvényesülnie kell.

A zónában alkalmazott intézkedések jellemzően: többtényezős fizikai azonosítás (pl.: belépőkártya + kód), belépések és jelenlét részletes naplózása, folyamatos vagy eseményvezérelt kamerás megfigyelés, kísérési kötelezettség külső vagy ideiglenes jogosultságú személyek esetén, négyszem-elv alkalmazása, rendszeres jogosultság-felülvizsgálat és audit, környezeti paraméterek (pl.: hőmérsékelt, páratartalom) folyamatos monitorozása valamint a rendkívüli eseményekre vonatkozó speciális eljárások (pl.: vészhelyzeti belépés). Ezen intézkedések célja nem kizárólag a külső támadások kivédése, hanem a belső visszaélések, emberi és műszaki hibák és szándékos károkozás kockázatának csökkentése is.

Minta kialakítás

Zóna	Elhelyezkedés	Tipikus szereplők	Fő cél	Egy-egy a zónára jellemző védelmi intézkedés
Környezet	Objektumhatáron kívül, tágabb környezet	Lakosság, közlekedők, külső szereplők	Fenyegetések azonosítása, kontextus megértése	A kritikus szervezet kockázatértékelése: „felméri és dokumentálja a kritikus szervezet és a kritikus infrastruktúra fenyegetettségét, fenyegetést jelentő kockázatait, amelyek rendkívüli eseményhez vezethetnek, meghatározza az azonosított fenyegetések káros hatásait és azok mértékét, a fenyegetések káros hatásainak és azok bekövetkezésének valószínűségét, és a kitettség mértékét” [4, 15. § (1)]
Külső zóna	Objektumhatáron kívül, közvetlen környezet	Belépő és külső személyek	Korai észlelés, elrettentés	Létesítmény elhelyezkedése: „Figyelembe veszi a fizikai és környezeti veszélyeket az EIR-nek helyet adó létesítmény megtervezésekor. A meglévő létesítményeknél figyelembe veszi a szervezeti kockázatmenedzsment stratégiában szereplő fizikai és környezeti veszélyeket.” [5, 12.49.]
Objektumhatár	Objektumhatáron	Belépő személyek	Elválasztás, késleltetés, ellenőrzés	„a létesítmény belépési pontjain biztosítja a személyek és járművek biztonsági (átvilágítás, átvizsgálás, tiltott tárgyak kutatása) ellenőrzését” [4, 2.2. -9]

Zóna	Elhelyezkedés	Tipikus szereplők	Fő cél	Egy-egy a zónára jellemző védelmi intézkedés
Átmeneti zóna	Objektumhatáron belül	Látogatók, beszállítók, korlátozott jogosultságú dolgozók	Szűrés, forgalomszabályozás	Belátás- és rálátásvédelem: minden olyan területen biztosítani kell, ahol járműveket vagy formatervezés szempontjából releváns alkatrészeket/komponenseket dolgoznak fel vagy tárolnak. Ez magában foglalja az épületek vonatkozó üvegfelületeit, valamint azokat a védelmi intézkedéseket, amelyek megakadályozzák a belátást nyitott ajtókon, kapukon vagy ablakokon keresztül. [13 p. 5]
Belső zóna	Objektum belseje	Munkavállalók	Jogosulatlan hozzáférés megakadályozása	A fizikai hozzáférések felügyelete: „Ellenőrzi a fizikai hozzáféréseket az elektronikus információs rendszereket tartalmazó létesítményekben, hogy észlelje a fizikai biztonsági eseményeket és reagáljon rájuk.” [5, 12.17.]
Privilegizált zóna	Objektum legvédettebb részei (vezetői irodák, szerverszobák)	Korlátozott számú (privilégizált) jogosult	Kritikus erőforrások védelme	Környezeti védelmi intézkedések: „Meghatározott biztonságos szinten tartja a hőmérsékletet, a páratartalmat, a légnyomást és a sugárzást az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben (például: adatközpont, szerver szoba, központi gépterem).” [5, 12.37.]

1. táblázat. Megjegyzés: a környezet nem védelmi zóna szűk értelemben, de a kockázatmenedzsment-alapját képezi. A felsorolt egy-egy védelmi intézkedés példa jellegű és a tanulmányban említett jogszabályokból és szabványokból került kiválasztásra.

ÖSSZEFOGLALÁS

A bemutatott többrétegű modell a mélységi védelem elveire építve olyan strukturált, kockázatalapú megközelítést kínál, amely egyszerre támogatja a szervezetek zárt, teljes körű, folytonos és a kockázatokkal arányos védelemének kialakítását, üzletmenet-folytonosságának fenntartását és jogszabályi megfelelését. A modell nem új követelményeket vezet be, hanem a jelenleg hatályos hazai és európai szabályozási környezet – különösen a NIS2 és a CER irányelvek és a jogharmonizáció során megalkotott hazai jogszabályok – által megfogalmazott elvárásokat ülteti át a fizikai térben értelmezhető, gyakorlati struktúrába.

A zónák egymásra épülő kialakítása lehetővé teszi a kockázatarányos védelem megvalósítását: a szervezet nem egységesen, hanem a tényleges fenyegetettségek alapján alkalmaz eltérő szintű intézkedéseket. Ez összhangban áll a nemzetközi szabványok, így az ISO/IEC 27001, a TISAX, valamint a NIST-alapú kockázatmenedzsment-keretrendszerek alapelveivel is, amelyek a kockázatok azonosítását, értékelését és arányos kezelését helyezik előtérbe.

A modell alkalmazása egyúttal hozzájárul a szervezeti reziliencia növeléséhez, mivel a fizikai, szervezeti és humán kontrollok egységes rendszerben jelennek meg, csökkentve az egyedi hibákból vagy incidensekből fakadó kaszkádhatások kialakulásának esélyét. A mélységi, zónás szemlélet így nem pusztán megfelelési eszköz, hanem egy hosszútávon fenntartható, ellenálló és átlátható fizikai biztonsági architektúra alapja.

IRODALOMJEGYZÉK

[1] Charlie Edwards, Senior Adviser, Strategy and National Security; Nate Seidenstein, Research Assistant (2025 augusztus) The International Institute for Strategic Studies, The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure Forrás: https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/

[2] 2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről és

[3] 2024. évi LXIX. törvény Magyarország kiberbiztonságáról

[4] 474/2024. (XII. 31.) Korm. rendelet Kritikus szervezetek ellenálló képességéről szóló törvény végrehajtásáról

[5] 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

[6] 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról

[7] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)

[8] Az Európai Parlament és a Tanács (EU) 2022/2557irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről (CER irányelv)

[9] Premier ministre; Secrétariat général de la défense nationale Direction centrale de la sécurité des systèmes d'information Sous-direction des opérations Bureau conseil La défense en profondeur appliquée aux systèmes d'information, La défense en profondeur appliquée aux systèmes d'information - Mémento Forrás: https://messervices.cyber.gouv.fr/documents-guides/mementodep-v1-1.pdf

[10] Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies Industrial Control Systems Cyber Emergency Response Team September 2016 Forrás: https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[11] National Institute of Standards and Technology Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology Joint Task Force NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations Forrás: https://doi.org/10.6028/NIST.SP.800-53r5

[12] Stouffer K, Pease M, Tang CY, Zimmerman T, Pillitteri V, Lightman S, Hahn A, Saravia S, Sherule A, Thompson M (2023) Title. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-82r3. Forrás: https://doi.org/10.6028/NIST.SP.800-82r3

[13] Verband der Automobilindustrie Minimum requirements for prototype protection in the German automotive industry Version: 3.0 Date: November 07, 2018 Forrás: https://www.vda.de/dam/jcr:855b28fe-fc1b-4819-bd49-f282f2ff754b/20181107_VDA_Minimum_Requirements_for_Prototype_Protection_Version3.pdf?mode=view