DOI: 10.38146/BSZ-AJIA.2025.v73.i1.pp113-126

Ipari nagyberuházások biztonsági kockázatainak sajátosságai és kezelési elveik

Characteristics of security risks of large industrial investments and their management principles

Gubics Frigyes
biztonsági igazgató
Lenovo Manufacturing Kft.
fgubics@lenovo.com

Absztrakt

Cél: A jelentős ipari beruházási projektek biztonságának fontos szerepe van a sikeres megvalósításban. Jelen tudományos cikk célja, hogy átfogó elemzést nyújtson a nagy ipari beruházások biztonsága és végrehajtása közötti kapcsolatról. A biztonságot befolyásoló tényezők vizsgálata, amelyek befolyással vannak a megvalósítás sikerére, kockázatok feltárása és azok mérséklése, illetve az érintettek érdekeinek védelme adják a biztonsági rendszer kialakításnak létjogosultságát. A biztonságos környezet megteremtése alapvetés az elvárt végeredmény és a vagyonvesztés megelőzése szempontjából.

Módszertan: A szerző kvalitatív kutatást végezve, szekunder adatokat felhasználva dokumentumelemzést végzett annak érdekében, hogy átfogó képet adjon a jelentős ipari beruházások biztonsággal kapcsolatos összefüggéseiről. Empirikus úton szerzett tapasztalatok is segítették a munkát, lévén a szerző maga is részt vett kiemelt ipari beruházás projektmenedzsmentjében mint biztonsági vezető.

Megállapítások: A kiemelt ipari beruházások sikerességét jelentősen befolyásolja azok biztonsági szintje. A hatékony biztonsági tevékenység több szervezet aktív közreműködését igényli. A transzparencia, a szálra csiszolt biztonsági folyamatok és módszerek egyfajta garanciát jelentenek a stabil keretek biztosításához a tervezés, kivitelezés, majd pedig az üzemszerű működés szakaszaiban.

Érték: Az ipari beruházások előkészítése során felmerülő biztonsági kockázatok hangsúlyozása, az érdekelt szervezetek bevonása a biztonsági teendőkbe,

A szerző a kéziratot magyar nyelven nyújtotta be. Benyújtás: 2024. 04. 08. Átdolgozás: 2024. 06. 05. Elfogadás: 2024. 06. 07.

egyfajta preventív biztonsági tevékenység a vagyonvesztés megelőzése és a projekt sikereségének segítése érdekében.

Kulcsszavak: ipari beruházás, kockázatelemzés, vagyonbiztonság, adatvédelem

Abstract

Aim: Major construction and investment security is important if order to be done successfully. The aim of this article is to describe and analyse security relations of these kind of projects. Analysing several part of security they affect the result of construction activities, risk assessment and risk mitigation, and of course to protect stake holders interests are the main directions of security activity. Secured environment also a base of achieve the expected results and activity of loss protection. Transparency, finalized workflows and tactics also can guarantee of a stable background during planning, implementation and later on final operation.
Methodology: The author carried out qualitative research, using secondary data, and conducted a document analysis in order to provide a comprehensive picture of the security-related connections of major industrial investments. Empirical experience also helped the work, as the author himself participated in the management of a priority industrial investment project as a security manager.
Findings: The success of priority industrial investments is significantly influenced by its level of security. Effective security activities require the active cooperation of several organizations. Transparency, meticulous security processes and methods are a kind of guarantee for ensuring a stable framework in the phases of planning, implementation and then operation.
Value: Emphasizing the security risks arising during the preparation of industrial investments, involving interested organizations in the security activity, a kind of preventive security activity in order to prevent the loss of property and help the success of the project.

Keywords: Industrial investment, risk assessment, asset security, data protection

Bevezetés

Az ipari nagyberuházási projektek kulcsfontosságúak a gazdasági növekedés, a technológiai fejlődés és az infrastruktúra fejlesztése szempontjából. Azonban ezek kapcsán számos biztonsági kihívással nézünk szembe, amelyek veszélyeztethetik sikerességüket. Ez a cikk a jelentősebb ipari beruházások biztonsági

vonatkozásaival foglalkozik, illetve keretbe helyezi az egyes elemeket. A különféle biztonsági kockázatok kezelése, a hatékony stratégiák és innovatív technológiák hozzáadnak a projekt sikeréhez, a befektetői bizalomhoz és a fenntartható fejlődéshez. Az érdekeltek közötti együttműködés, a nemzetközi biztonsági szabványok betartása és a múltbeli tapasztalatokból történő folyamatos tanulás kulcsfontosságú a biztonsági kockázatok kezeléséhez. Ezek a projektek számos más ágazattal együttműködnek és szoros egymásra utaltságban vannak, mint például az energiaszolgáltatók, a szállítmányozás, az alapanyag-beszerzés és -gyártás, így ezen szakterületek kapcsolata jelentős gazdasági haszonnal járhat mind a helyi, mind a globális közösségek számára. Ezzel együtt számos kihívást is hordoznak magukban, melyekből egyik legfontosabb a biztonság kérdése, hiszen ezen is állhat vagy bukhat egy beruházás sikere. Az azonosított kockázatok megfelelő kezelése kritikus, mely megalapozza az ipari beruházások megfelelő védelmi kialakítását.

A biztonság elemei

Több kulcsfontosságú tényező is szerepet játszik a nagyobb ipari beruházási projektek tervezésekor. Ezek megértése a hatékonyan működő biztonsági rendszer kiépítésének alapja. A politikai stabilitás és a kiszámítható jogszabályi keret alapvető szempontok akkor, amikor egy piaci vállalat úgy dönt, hogy beruházást eszközöl egy adott országban. Ez biztosít kedvező környezetet a befektetésekhez, csökkentve a kormányzatokhoz és a jogszabályi háttérhez kapcsolódó kockázatokat, amelyek megzavarhatják vagy ellehetetleníthetik a projektet. A pénzügyi kockázatok felmérése és kezelése, mint például a megfelelő finanszírozás biztosítása, a költségtúllépések minimalizálása és a bevételek biztosítása. A kiberbiztonság és az adatvédelem is fontos szempont a mai digitalizálódó világban. Mivel az ipari projektek egyre inkább digitális rendszerekre és adatvezérelt folyamatokra támaszkodnak, a kiberfenyegetésekkel szembeni védelem egyre fontosabbá válik. Az adatszivárgás, az illetéktelen hozzáférés és a rendszer sebezhetőségei elleni védelem elengedhetetlen a működés integritásának megőrzéséhez és a szenzitív információk védelméhez. Tiszolczi Balázs Gergely (2019) szerint az információk biztonságának megőrzéséhez egyre több és más jellegű technikai ismeretre van szükség, ilyenek a hálózatok, az alapvető informatikai ismeretek, illetve az információbiztonság.

A fizikai biztonság a projekt helyszíneinek, felszereléseinek és infrastruktúrájának védelme az eltulajdonítás, a vandalizmus és a jogosulatlan hozzáférés elleni intézkedéseket foglalja magában. Az átgondoltan megalkotott biztonsági

intézkedések, például a felügyeleti rendszerek, a hozzáférés-ellenőrzés és a fizikai/mechanikai/elektronikai eszközök implementálása segít csökkenteni a lehetséges kockázatokat.

Ezek a projektek gyakran összetett ellátási láncok igénybevételével működnek, melyekben a részt vevő beszállítók száma magas. Különösen jellemző ez a multinacionális cégek esetében, ahol a világ minden tájáról érkezhetnek be anyagok. Az ellátási lánc integritásának és megbízhatóságának biztosítása (szállítás, logisztika, beszerzés) segít csökkenteni az olyan rizikókat, mint a csalás, a termékek manipulálása, valamint az anyagokhoz és szolgáltatásokhoz kapcsolódó anomáliák, késések.

A fenntartható fejlődés biztosítása, a környezetvédelmi előírások betartása és a helyi közösségekkel való felelősségteljes együttműködés az ökoszisztémákra és közösségekre gyakorolt negatív hatások mérséklése érdekében fontos. Ezek elmulasztása nemcsak a vállalat jó hírnevében tesz kárt, hanem jogi és hatósági eljárásokat vonhat maga után, amely a projekt késedelméhez vezethet.

Fontos szót ejtenünk a beruházással kapcsolatos biztonsági vezetői feladatok ellátásáról, mely jelentős pozíció az eredményességet tekintve. Ahogy azt Christián, Major és Szabó (2019) hangsúlyozza, ideálisan az első számú döntéshozóhoz van becsatornázva, mely új projekt esetében annak vezetője, illetve a vállalatvezető. A pozicionálás jelentősége az érdekérvényesítés hatékonyságában van, hiszen több szinttel lentebb, középvezetőként az információk a management szűrőin mennek keresztül mire a döntéshozókig elérnek, ez rontja a hatékonyságot és befolyásolóképességet, és a biztonsági szint csökkenéséhez is vezethet. A biztonsági vezetőnek úgynevezett showstopper[1] jogot érdemes adni, ennek segítségével súlyos biztonsági hiányosságok esetén megállíthat bizonyos folyamatokat, melyek a javító intézkedések után indíthatóak újra, megelőzve ezzel a vagyonvesztést.

Politikai stabilitás és jogszabályi keretrendszer

A politikai háttér és a jogi keretrendszer országonként eltérő, melyek jelentősen befolyásolják a beruházási kedvet, illetve segíthetik meghozni a döntést, hogy adott térségbe telepítse-e az adott vállalat az ipari kapacitását vagy annak egy részét. Ma már elmondhatjuk, hogy a multinacionális cégek termelésüket igyekeznek diverzifikálni, és földrajzilag ott megtermelni az adott termékkört, ahol azt értékesítik. A politikai stabilitás olyan környezetet biztosít, amely elősegíti

1 Shwostopper: akadálya a további fejlesztésnek, fejlődésnek.

a projektek hosszú távra történő tervezését és a végrehajtást. A helyszín kiválasztása geopolitikai szempontból kulcsfontosságú, hiszen ez is növelheti a befektetők bizalmát. A kiszámítható politikai környezet kedvező befektetési légkört teremt, mind a hazai, mind pedig a külföldi tőkét vonzza.

Fentieken túlmenően a stabil, világos és átlátható jogszabályi keret egyértelmű viszonyokat teremt, hiszen a kiszámíthatóság és tervezhetőség fontos a befektetés megtérülése szempontjából. Védi az összes érintett fél (stakeholders)[2] érdekeit, növeli a bizalmat és az elszámoltathatóságban is segít. A környezetvédelemre, az egészségügyi és munkavédelmi előírásokra, a munkajogokra és a pénzügyi tevékenységre vonatkozóan adja meg a kereteket.

A rendszeres párbeszéd, konzultáció és koordináció segít abban, hogy a politika is igazodjon az ipar igényeihez, elősegíti a gazdasági növekedést és védi az stakeholderek érdekeit, mindezek mellett a sikeres projekt végrehajtása alapköve a fenntartható fejlődés elősegítésének az adott térségben.

Gazdasági stabilitás és pénzügyi kockázatok

A gazdasági környezet, amelyben a projektek működnek, jelentősen befolyásolhatja életképességüket és sikerüket. A makrogazdasági mutatók, például a GDP[3]-növekedés, az inflációs ráták és a kamatlábak ingadozása kihívásokat és bizonytalanságokat jelenthet a projekttervezés és -végrehajtás szempontjából, és nehezíti a pénzügyi tervezhetőséget.

A pénzügyi kockázatok, beleértve a finanszírozási korlátokat, a költségtúllépéseket és a bevétel bizonytalanságait, a nagy ipari projektek velejárói, kockázatai. A megfelelő finanszírozási források biztosítása és a cash flow[4] hatékony kezelésére is figyelmet kell fordítani.

A hatékony és eredményes pénzgazdálkodás, a szigorú költségvetés-tervezés, a pontos költségbecslés és a körültekintő pénzügyi tervezés elengedhetetlen a pénzügyi kockázatok mérsékléséhez. Alapos, mindenre kiterjedő pénzügyi megvalósíthatósági tanulmányok készítése és különféle forgatókönyvek átgondolása segíthet azonosítani a lehetséges kockázatokat, és megkönnyítheti az azokra való felkészülést és az előzetes tervek elkészítését. Érdemes pénzügyi szakembereket bevonni a tervezési fázisban is.

2 Stakeholders: érdekelt felek.

3 GDP (Gross Domestic Product): A bruttó hazai termék, a közgazdaságtanban egy bizonyos terület – többnyire egy ország – adott idő alatti gazdasági termelésének a mérőszáma. Méri a nemzeti jövedelmet és teljesítményt.

4 Cash flow: pénzforgalom.

Kiberbiztonság és adatvédelem

Digitalizálódó világunkban a kiberbiztonság és az adatvédelem kritikus biztonsági tényezővé váltak a nagy ipari beruházások esetében is. Ezek a projektek nagymértékben támaszkodnak egymással összekapcsolt rendszerekre, digitális technológiákra és adatvezérelt folyamatokra, így sebezhetővé válhatnak a kiberfenyegetésekkel és az információs, ezen belül is a személyes adatokkal történő visszaélésekkel szemben.

A körültekintően kimunkált kiberbiztonsági intézkedések bevezetése rendkívül fontos az infrastruktúra, az érzékeny adatok és a szellemi tulajdon védelme érdekében. Erős tűzfalak, behatolásérzékelő rendszerek és titkosítási protokollok alkalmazása segíthet a jogosulatlan hozzáférés és az adatszivárgás elleni védelemben. Sérülékenység vizsgálatok[5] és penetrációs tesztek[6] segítenek azonosítani a potenciális gyengeségeket és sebezhetőségeket, lehetővé téve az időben történő reagálást.

Az adatvédelem ugyanilyen fontos, mivel a projektek gyakran nagy mennyiségű érzékeny és védett információval dolgoznak. A biztonságos adattárolás, a hozzáférés-szabályozás és az adattitkosítás alkalmazása segít megelőzni az érzékeny adatok jogosulatlan kezelését, nyilvánosságra hozatalát vagy ellopását. Az adatvédelmi előírásoknak, például a GDPR[7]-nek, illetve Magyarországon az Info törvénynek[8] történő megfelelés biztosítja a személyes adatok védelmét.

Az alkalmazottak részére szervezett képzések fontos szerepet játszanak a kiberbiztonság és az adatvédelem fenntartásában. A személyzet felvilágosítása a lehetséges kockázatokról, a jelszavak gyakori cseréje, a gyanús tevékenységek bejelentésének és fontosságának hangsúlyozása az átfogó kiberbiztonsági stratégia alapvető elemei.

Kiberbiztonsági szakértők, szakcégek bevonása a tevékenységbe tovább csökkenti a kiberbiztonsági kockázatokat. Az iparági partnerekkel, kormányzati szervekkel és kiberbiztonsági szervezetekkel történő együttműködés megkönnyítheti a bevált gyakorlatok alkalmazását és az újonnan felmerülő fenyegetésekkel és sebezhetőségekkel kapcsolatos információmegosztást.

---

5 A sérülékenység vizsgálat egy fejlesztés alatt álló vagy elkészült termék (honlap, alkalmazás, szoftver, hálózat) tesztelése. A teszt során az etikus hackerek olyan bugokat (hibákat) keresnek, amivel egy rosszindulatú támadó vissza tud élni (XSS, RCE, LFI, SQLi).

6 Penetrációs teszt: olyan biztonsági gyakorlat, amelyben egy kiberbiztonsági szakértő megpróbálja megtalálni és kihasználni a számítógépes rendszer sérülékenységeit.

7 GDPR (General Data Protection Regulation): az Európai Parlament és Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 96/45/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet).

8 Info törvény: 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

Fizikai biztonság és vagyonvédelem

A projektek gyakran értékes eszközöket, például berendezéseket, infrastruktúrát és alapanyagokat kezelnek, amelyeket meg kell védeni a lopás, szabotázs és illetéktelen hozzáférés ellen.

A komplex fizikai biztonsági intézkedések végrehajtása elengedhetetlen a projekt telephelyeinek és eszközeinek védelme érdekében. Ez magában foglalja a biztonsági személyzetet, a felügyeleti rendszerek kiépítését, valamint a beléptetési és kiléptetési pontok létrehozását. Az olyan eszközök, mint a CCTV[9] kamerák, mozgásérzékelők és riasztórendszerek alkalmazása javítja a potenciális biztonsági fenyegetések hatékony detektálását és a válaszreakciókat.

A közvetlen projektterület biztosítása mellett az anyagok és berendezések szállításának körülményeit is át kell gondolni. Az ellátási láncok biztonságossá tétele, valamint a megfelelő nyomon követés és felügyelet segíthet megelőzni a lopást és a szállítás közbeni manipulációt.

Berek Tamás és Bodrácska Gyula (2010) szerint a helyi bűnüldöző szervekkel és biztonsági szakemberekkel való együttműködés értékes információkkal szolgálhat a lokális biztonsági helyzetről és kockázatokról, ezzel segíthet a személyre szabott biztonsági stratégia kidolgozásában. Álláspontom szerint azonban figyelembe kell venni a majdani elkészült objektumban tervezett tevékenységet, vagyis a vállalati profilt, mivel a védelem kialakításához ez kockázati elemként jelentkezik, melyet kezelni szükséges.

Az ellátási lánc biztonsága

Az ellátási lánc biztonságának egyik elsődleges szempontja a megfelelő minőségű és mennyiségű anyagok, alkatrészek, termékek rendelkezésre állása. A szigorú minőségellenőrzési rendszer, az előzetes beszállítói auditok elvégzése és a nyomon követhetőség fenntartása a teljes ellátási láncon segít minimalizálni annak kockázatát, hogy nem megfelelő minőségű és mennyiségű anyagok kerüljenek a projektbe. A rendszeres auditok és vizsgálatok igazolhatják a minőségi szabványoknak és a szerződéses követelményeknek való megfelelést.

Az ellátási lánc megszakadásai jelentős kockázatot jelentenek a projektek ütemezésére és költségeire nézve. A természeti katasztrófák, a geopolitikai események, a sztrájkok vagy a közlekedési zavarok mind befolyásolhatják az anyagok és szolgáltatások időben történő szállítását. A készenléti tervek létrehozása,

9 CCTV (Closed-Circuit Television): zárt láncú kamerarendszer.

a beszállítók diverzifikálása és az átlátható kommunikációs csatornák fenntartása az ellátási lánc kulcsfontosságú partnereivel segíthet csökkenteni ezeket a kockázatokat, és biztosíthatja az alternatív lehetőségek elérhetőségét.

A biztonsággal kapcsolatos információk, például a lehetséges fenyegetésekkel kapcsolatban, vagy a best practices[10] megosztása segít a potenciális sebezhetőségek azonosításában és kezelésében. A beszállítókkal és vállalkozókkal szemben támasztott egyértelmű elvárások és követelmények a biztonsági protokollokkal és szabványokkal kapcsolatban biztosítják az ellátási lánc biztonságának következetes és egységes megközelítését.

A technológiai fejlesztések, mint például a blokklánc[11] technológia és az IoT[12] segítenek, hogy átlátható és naprakész, pontos nyilvántartással rendelkezzünk a tranzakciókról és a termékek mozgásáról.

Környezeti és társadalmi kockázatok

A környezeti kockázatok közé tartozik a szennyezés, az élőhelyek pusztulása, az erdőirtás és a természeti erőforrások kimerülése. A nagy ipari projekteknek meg kell felelniük a környezetvédelmi előírásoknak, alapos környezeti hatásvizsgálatot kell végezni, és megelőző intézkedéseket kell tenniük a környezetszennyezés megelőzése érdekében. A megújuló energiaforrások alkalmazása és a hulladéktermelés minimalizálása segít a környezeti kockázatok mérséklésében és a projekt ökológiai lábnyomának csökkentésében.

Társadalmi kockázatok a helyi közösségek esetleges zavarásából, a földterületekkel kapcsolatos konfliktusokból és a kulturális örökségre gyakorolt negatív hatásokból fakadnak. A társadalmi aggodalmak megértéséhez és kezeléséhez az érdekelt felek, köztük a helyi közösségek bevonása szükséges. Helyi megélhetési programok (munkahelyek teremtése), a kulturális örökség tiszteletben tartása és a helyi fejlesztési kezdeményezések támogatása hozzájárul a társadalmi kockázatok minimalizálásához és a projekt pozitív társadalmi megítélését is segítheti.

10 Best practies: A jó/legjobb (bevált) gyakorlat egy olyan működési mód, modell, megoldás, amely főbb részleteiben megismerhető, megtanulható és tapasztalatait felhasználva máshol is alkalmazható. Általában egy széles körben elismert, ideális folyamat, racionalizált modell vagy megoldás, amely egy adott szervezet számára adaptálható azonos vagy legalább hasonló környezeti feltételek, külső adottságok megléte esetén.

11 Blokklánc (block chain): egy adatbázis, mely abban különbözik a hagyományos adatbázisoktól, hogy az információk nem egy centralizált hálózaton, azaz egy központi szerveren, hanem egy elosztott hálózaton vannak tárolva.

12 IoT (Internet of Things): olyan különböző, egyértelműen azonosítható elektronikai eszközöket jelent, amelyek képesek felismerni valamilyen lényegi információt, és azt egy internetalapú hálózaton egy másik eszközzel kommunikálni.

Az emberi jogi megfontolások a környezeti és társadalmi kockázatok kezelésének is szerves részét képezik. A munkajogok tiszteletben tartása, a méltányos fizetés biztosítása, a biztonságos munkakörülmények elengedhetetlenek az etikus működés fenntartásához. A nemzetközileg elismert emberi jogi normák és iránymutatások betartása segítenek ebben.

Továbbá a környezeti és társadalmi hatások rendszeres nyomon követése és értékelése folyamatos fejlesztést és alkalmazkodást tesz lehetővé. A független auditok objektív betekintést nyújthatnak abba, hogy a projekt megfelel-e a környezetvédelmi és társadalmi normáknak, biztosítva az elszámoltathatóságot és átláthatóságot.

A biztonsági kockázatok csökkentése

A nagy ipari beruházási projektek biztonsági kockázatainak csökkentése átfogó és proaktív megközelítést igényel.

Bizonyos eszközök használatával képesek lehetünk növelni az ipari beruházási projektek általános biztonságát, minimalizálhatjuk a kockázatokat. A proaktív intézkedések, az együttműködés és a folyamatos értékelés, ellenőrzés hozzájárul e projektek rezisztenciájához és hosszú távú sikeréhez az állandóan változó biztonsági környezetben.

Lawrence J. Fennelly (2013) szerint a biztonságos környezet megteremtése körültekintő tervezéssel már a projekt előkészítési szakaszában megfontolást igényel, és az olyan egyszerűnek tűnő megoldások, mint a megfelelő világítás, akadálymentes rálátás az objektumokra, vagy kapcsolat a környező épületekkel, közúti infrastruktúrával előnyt jelenthetnek a komplex biztonsági rendszer megtervezésénél.

Kockázatértékelés és -kezelés

Horváth Tamás (2018) szerint a kockázatelemzés eredménye alapján határozható meg, hogy a telepítendő biztonságtechnikai rendszerek megfelelő választ adjanak a lehetséges kockázatokra. Meglátásom szerint ezen túlmenően fontos, hogy a technikai megoldások mellett el kell helyeznünk az élőerős őrzést is a „sakktáblán”, a kellően átgondolt rezsim intézkedésekkel együtt. A hatékony kockázatértékelés és -kezelés kulcsfontosságú eleme az ipari beruházási projektek biztonságának. Az átfogó kockázatértékelések segítségével azonosítjuk azokat a potenciális fenyegetéseket, sebezhetőségeket és problémás területeket, amelyek

hatással lehetnek a projekt biztonságára. A kockázatértékelés első lépése a lehetséges kockázatok azonosítása és elemzése különböző szempontok szerint, beleértve a politikai, gazdasági, kiberbiztonsági, fizikai és környezeti tényezőket. Ez magában foglalja a projekt környezetének, az érdekelt felek érdekeinek és a lehetséges hatások alapos értékelésének elvégzését. Szakértők, például kockázati tanácsadók vagy biztonsági szakemberek bevonása értékes segítséget jelenthet.

A kockázatok azonosítása után rangsorolni kell őket a valószínűségük és a lehetséges hatásuk alapján. Ez lehetővé teszi, hogy megfelelő erőforrásokat allokáljunk, és célzott stratégiákat dolgozzunk ki. A kockázatkezelési terveknek konkrét intézkedéseket kell tartalmazniuk az azonosított kockázatok csökkentésére.

Charles Sennewald (2011) a kockázatok elemzése után a már meglévő kockázatcsökkentő intézkedések felülvizsgálatát, majd pedig a szükség szerinti módosításokat javasolja annak fényében. Ehhez a teljes biztonsági rendszer időnkénti áttekintése szükséges, akár külsős szakértő, cég bevonásával. Ez alátámasztja, hogy a kockázatelemzés a folyamatok szükségszerű változásával párhuzamosan folyamatosan zajlik annak érdekében, hogy időben képesek legyenek reagálni a megváltozott körülményekre, ezzel csökkentve a lehetséges veszteségeket és alacsonyan tartva a rizikót.

A rendszeres nyomon követés és értékelés elengedhetetlen annak biztosításához, hogy a kockázatkezelési stratégiák hatékonyak és naprakészek maradjanak. Ez magában foglalja a lehetséges fenyegetések folyamatos monitorozását, a projekt környezetében bekövetkezett változások nyomon követését és a kockázatok újraértékelését a projekt előrehaladtával. A kockázatkezelési terveket szükség szerint módosítani kell a felmerülő új kockázatok vagy a változó körülmények lekövetésével, a naprakészen tartás érdekében.

A biztonsági incidensek előrejelzése lehetővé teszi, hogy tervet dolgozzunk ki, kommunikációs protokollokat hozzunk létre, és biztosítsuk az üzletmenet folytonosságát. Ezeket a terveket szimulációkkal és gyakorlatokkal kell tesztelni a hatékonyságuk értékelése és a szükséges fejlesztések elvégzése érdekében.

Mélységi védelem

A mélységi védelem kiépítése segítséget nyújt a fellépő incidensek hatékony kezelésében. Ez magában foglalja a rezsim intézkedéseket, a technikai megoldásokat mely lehet mechanikai vagy elektronikus, illetve a rendszer fontos része az élőerő alkalmazása is. Garcia Mary Lynn (2007) szerint egy jól tervezett biztonsági rendszer mélységi és kiegyensúlyozott védelmet biztosít, minimalizálva a rendszerelemek meghibásodásának következményeit. Álláspontom

szerint a klasszikusnak tekinthető, úgynevezett periméter védelemtől el kell mozdulnunk, és a jól felépített külső héj védelmén túlmenően a biztonsági folyamatokat kell implementálnunk az egyes szervezeti egységek munkafolyamataiba, illetve a biztonsági szervezet operatív tevékenysége is több szinten, mélységben kell történjen. Ilyen például a biztonsági ellenőrzési pontok létrehozása, vagy érzékeny, nagy kockázatú területek fokozott védelme.

Együttműködés és információmegosztás

Az érintettek, a projekttulajdonosok, a kormányzati szervek, a biztonsági szakemberek és a helyi közösségek közötti együttműködés elősegítésével közös erőfeszítéseket tehetünk a biztonsági kockázatok hatékony azonosítására és kezelésére.

Az együttműködés megkönnyíti az információk és a helyes eljárások megosztását, lehetővé téve, hogy tanuljunk egymás tapasztalataiból, és részesüljünk a kollektív bölcsességből. A különböző nézőpontok és meglátások használatával átfogóbb és stabilabb biztonsági stratégia alakítható ki. Ez az együttműködésen alapuló megközelítés segít azonosítani a lehetséges vakfoltokat, létrehozni innovatív megoldásokat, és holisztikusan kezelni a biztonsági kihívásokat.

Az együttműködés és információmegosztás különféle formákban testesülhet meg, például rendszeres megbeszélések, workshopok, konferenciák és közös szimulációs gyakorlatok. Ezek elősegítik a nyílt párbeszédet, erősítik a kapcsolatokat, és bizalmat építenek az érdekelt felek között. Ezenkívül a külső szervezetekkel, például biztonsági szervezetekkel, kutatóintézetekkel vagy iparági szövetségekkel kötött partnerségek hozzáférést biztosíthatnak speciális tudáshoz és erőforrásokhoz. A kormányzati szervek szintén fontos szerepet játszanak az együttműködés és az információmegosztás elősegítésében.

Az érdekelt felek bevonása és közösségi kapcsolatok

Az érintettek bevonása magában foglalja a különböző csoportok aggodalmainak, szükségleteinek és törekvéseinek aktív meghallgatását. Lehetőséget biztosít a potenciális biztonsági kockázatok kezelésére, betekintést nyerhet a helyi dinamikába, és olyan stratégiák kidolgozását segítheti, amelyek összhangban állnak az összes érdekelt elképzelésével. Ez az együttműködésen alapuló megközelítés növeli a projektek elfogadottságát, és csökkenti a biztonságot veszélyeztető konfliktusok vagy a helyiek ellenállásának valószínűségét.

Az erős közösségi kapcsolatok kialakítása elengedhetetlen a pozitív projektkörnyezet kialakításához. A bizalom megteremtésével és a nyitott kommunikáció fenntartásával képesek lehetünk kezelni a helyi közösség aggályait, mérsékelhetjük a lehetséges társadalmi kockázatokat, és biztosíthatjuk, hogy a projekt kézzelfogható előnyökkel járjon a helyi lakosság számára is. A párbeszédben való részvétel, a rendszeres közösségi találkozók és a projekt biztonsági intézkedéseiről való tájékoztatás segíti a kapcsolatépítést és a partnerséget.

Képzés és készségfejlesztés

A projektben részt vevők tudásába és készségeinek fejlesztésébe történő befektetéssel erősíthetjük szervezetünk képességét a biztonsági kockázatok azonosítására és a hatékony reagálásra.

A biztonságtudatosság (alertness)[13] kialakítása, a gyanús tevékenységek bejelentési eljárásainak oktatása és végrehajtása hozzájárul a biztonságos projektkörnyezet megteremtéséhez. A rendszeres biztonsági auditok segítenek azonosítani a fizikai biztonsági intézkedések hiányosságait vagy gyengeségeit, lehetővé téve az időben történő változtatásokat és fejlesztéseket. Átfogó képzési programokat kell kidolgozni annak érdekében, hogy az alkalmazottakat a biztonsági protokollokról, eljárásokról és a legjobb gyakorlatokról oktassuk. Potenciális fenyegetések, például a számítógépes támadások, fizikai incidensek vagy környezeti veszélyek ismeretének átadását, valamint útmutatást e kockázatok megelőzésére és kezelésére is oktatni kell. A képzésnek a biztonság széles skáláját kell lefednie, így a kockázattudatosságot, a vészhelyzeti reagálást, a válságkezelést és az események jelentését.

A képzési programoknak hangsúlyozniuk kell a biztonságtudatosság kultúrájának fontosságát. Az éberség, az elszámoltathatóság és a felelősség érzésének kialakulása a biztonságra összpontosító kollektív gondolkodásmódot hoz létre. Az alkalmazottak ösztönzése, hogy jelentsenek minden gyanús tevékenységet vagy potenciális biztonsági kockázatot, elősegíti a projektbiztonság fenntartásának proaktív megközelítését. Rendszeres frissítő képzéseket kell biztosítanunk annak érdekében, hogy a dolgozók naprakészek maradjanak a változó biztonsági környezet ellenére is.

13 Alertness: éberség, készenlét.

Összefoglalás

A jelentős ipari beruházások biztonsága összetett és sokrétű. A különféle biztonsági tényezők hatékony stratégiák és innovatív technológiák révén történő kezelése elengedhetetlen a projekt sikeréhez, a befektetői bizalomhoz és a fenntartható fejlődéshez. Az érdekeltek közötti együttműködés, a nemzetközi biztonsági szabványok betartása és a múltbeli tapasztalatokból történő folyamatos tanulás kulcsfontosságú a biztonsági kockázatok kezeléséhez, valamint a beruházás biztonságos környezetének megteremtéséhez. Globalizálódó világunkban hazánkban is jelen vannak multinacionális vállalatok, melyek elemi érdeke olyan kapcsolatrendszereket létrehozni és fenntartani, melyek segítségével hosszú távú, a biztonság minden aspektusát figyelembe vevő együttműködés alakulhat ki a helyi közösségekkel, mely közös érdekeken alapszik. A biztonságos projektmegvalósításhoz támogatás szükséges, mely nem merül ki az állami hatóságokkal való jó kapcsolatban, és folyamatos kommunikációt igényel. A biztonságot helyi összefüggéseiben kell szemléljük, hiszen a globális biztonsági folyamatok kevéssé vannak hatással közvetlenül a mikroközösségekre, ezért elsősorban a helyi sajátosságok figyelembevételével kell kialakítanunk a biztonsági rendszert. Ennek felépítése, struktúrája szorosan kell kövesse a projekt egyes fázisait, és megfelelően, időben kell reagáljon rájuk, mintegy lekövetve a projekt fejlődését. A kockázatok változásának lekövetése szintén fontos része a hatékony biztonsági rendszer felépítésének és működtetésének.

Felhasznált irodalom

Berek T. & Bodrácska G. (2010). Az élőerős őrzés az objektumvédelem építőipari ágazatában. *Hadmérnök,* V. évfolyam 4. szám.

Christián L., Major L., & Szabó C. (2019). *Biztonsági vezetői kézikönyv.* Dialóg Campus.

Garcia, M. L. (2007). *Design and Evaluation of Physical Protection Systems.* Elsevier Science. https://doi.org/10.1016/B978-0-08-055428-0.50005-1

Horváth T. (2018). Elektronikus megfigyelő-, és ellenőrző rendszerek objektumorientált kialakítása különös tekintettel a biztonsági kockázatok rendszere. Budapest: Óbudai Egyetem Biztonságtudományi Doktori Iskola.

Lawrence, J. F. (2013). *Effective Physical Security.* Butterworth-Heinemann.

Sennewald, C. A. (2011). *Effective Security Management.* Elsevier: Butterworth-Heinemann. https://doi.org/10.1016/B978-0-12-382012-9.00021-6

Tiszolczi B. G. (2019). Fizikai biztonsági kontrollok tervezésének és alkalmazásának gyakorlata az ISO/IEC 27001 szabvány elvárásainak tükrében. *Magyar Rendészet,* 2–3, 233–249. https://doi.org/10.32577/mr.2019.2-3.12

Alkalmazott jogszabályok

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről

A cikk APA szabály szerinti hivatkozása

Gubics F. (2025). Ipari nagyberuházások biztonsági kockázatainak sajátosságai és kezelési elveik. *Belügyi Szemle*, *73*(1), 113–126. https://doi.org/10.38146/BSZ-AJIA.2024.v73.i1.pp113-126

Nyilatkozatok

Összeférhetetlenség

A szerző nem jelentett összeférhetetlenséget.

Finanszírozás

A szerző nem kapott pénzügyi támogatást a kutatáshoz, a szerzőséghez és/vagy a cikk publikálásához.

Etikai nyilatkozat

Jelen cikkhez nem kapcsolódik adatkészlet.

Levelező szerző

A cikk levelező szerzője Gubics Frigyes, aki a fgubics@lenovo.com e-mail címen érhető el.