DOI: 10.38146/BSZ.2024.1.6

A veszélyes üzemek információbiztonsági képességeinek fejlesztési lehetőségei napjaink kihívásainak tükrében

Opportunities for developing the information security capability at hazardous plants given current challenges

Vásárhelyi Örs
információbiztonsági szakértő
Alverad Technology Focus Kft.
vasarhelyi.ors@gmail.com

Absztrakt

Cél: Napjaink egyik, ha nem a legnagyobb kihívásai közé tartozik a kibertér-támadásokkal szembeni eredményes és hatékony védelmi képesség kialakítása. Ez mára már nemcsak állami szinten elvárás, hanem vállalati és magánfelhasználói szinten is jelentkező valós igény. Jelen tanulmányban a szerző elsősorban a 21. század új típusú fenyegetésének globális trendjeire, a leginkább veszélyeztetett szektorokra kívánja felhívni a figyelmet, valamint a hazai veszélyes üzemek kiberbiztonsági képességeinek fejlesztési lehetőségeit veszi számba.

Módszertan: A szerző elsődlegesen kvalitatív kutatási módszer által, szekunder adatok segítségével végzett kutatást, valamint dokumentumelemzést annak érdekében, hogy globális és regionális szinten is meghatározza a kibertér fenyegetéseinek aktuális trendjeit, támadási vektorjait. Emellett empirikus kutatást is végzett primer adatok felhasználásával a veszélyes anyagokkal foglalkozó üzemek irányítási/biztonsági irányítási rendszereinek fejlesztési lehetőségei meghatározása érdekében, valamint hogy ezen üzemek elektronikus információs rendszerei korunk fenyegetéseivel szembeni rezilienciáját a későbbiekben kialakíthassa.

Megállapítások: A kibertérből érkező támadások száma folyamatos növekedést mutat az elmúlt évtizedekben, az ipari szereplők kiemelt célpontjai ezeknek az új típusú támadásoknak. Annak érdekében, hogy hazánk hatékony védelmi képességet alakítson ki, különösen az ipari szereplők esetén, fontos

a katasztrófavédelem iparbiztonsági hatóság felügyelete alá tartozó, veszélyes anyagokkal foglalkozó üzemek kibervédelmi képességének létrehozása.
Érték: A hazai veszélyes anyagokkal foglalkozó üzemek biztonsági irányítási rendszerének 21. századi fenyegetésekkel szembeni védelmi képesség kialakítási lehetőségeinek számbavétele. Az irányítási rendszer információbiztonsági szempontokkal történő kiegészítéséről és megvalósíthatóságáról e tudományos munka részletesebb tájékoztatást kíván adni.

Kulcsszavak: globális, kibertámadás, információbiztonság, ipari vezérlőrendszer

Abstract

Aim: One of the biggest challenges people face today is the development of an effective and efficient defence capability against cyber attacks. Nowadays, this is not only an expectation at the public level, but also a real need at the corporate and private user level. In this study, the author primarily wishes to draw attention to the global trends of new types of threats in the 21st century, the most vulnerable sectors, as well as to the development possibilities of the cyber security capabilities of domestic hazardous plants.
Methodology: The author has conducted a qualitative research method using primary and secondary data to identify current trends and attack vectors of threats in cyberspace at global and regional levels. In addition, the author has also conducted empirical research using primary data to determine the development possibilities of the management/safety management systems of plants dealing with hazardous substances, as well as to build the resilience of the electronic information systems of these plants against cyber threats.
Findings: The number of cyber-attacks have continued to grow over the last few decades, and industrial companies have become the main targets of these new types of attacks. In order for Hungary to develop an effective defence capability, especially in the case of industrial actors, it is important to create the cyber defence capability of plants dealing with hazardous materials under the supervision of the disaster management, industrial safety authority.
Value: Taking stock of the possibilities of developing the security management system of domestic hazardous materials plants to protect against 21st century threats. This scientific work intends to provide more detailed information on the addition and feasibility of the management system with information security aspects.

Keywords: globalism, cyberattack, information security, industrial control system

Bevezetés

A ma működő társadalmak szerves részét képezi a kommunikációs eszközöktől, hálózatoktól való függés. Mai információs társadalmunkban már a legnagyobb politikai, gazdasági és kulturális felhajtóerő az információk naprakész, pontos, helyes ismerete és feldolgozásának hatékonysága. Ennek a közgazdasági megfelelője a tudásgazdaság, vagyis a tudás gazdasági hasznosítása által érték jöhet létre.

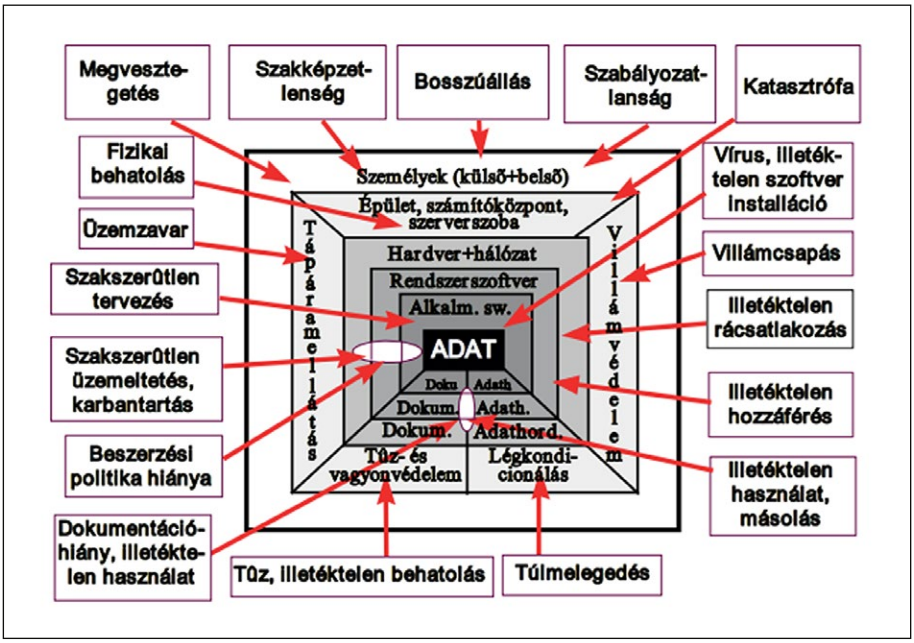
Az információtól való függőségünk egészen az államigazgatás szintjéig terjed, így érthető módon az információ hiányát bármely szinten, minden szereplő megérzi, káros következményekkel járhat, ha a megfelelő információ nem áll rendelkezésre. Ugyanúgy káros következménye lehet annak, ha az információ túl nagy mennyiségben áll rendelkezésre, bármiféle rendszerezés nélkül. További problémákat okoz, ha bizalmas információk harmadik fél kezébe kerülnek (ami akár jelentheti azt is, hogy nyilvánosságra hozzák őket és a társadalom valamennyi szereplője számára megismerhetővé válik). A fent felsorolt esetek, valamint társadalmunk információs rendszereket ért támadások esetén való kitettsége miatt szükséges volt az információbiztonságot megalkotni, alkalmazni.

Információbiztonság alapjai

Az információ szó hallatán sokan szigorúan az informatikát értik, pedig ez ennél egy sokkal tágabb fogalom. Az információbiztonság olyan folyamatok és intézkedések összessége, amelyek célja az adatok védelme. Az információbiztonság kiterjed a számítógépes rendszerekre, az elektronikus kommunikációra, a hálózatokra, valamint az információkat tartalmazó papíralapú dokumentumokra, valamint egyéb adathordozókra is. Más értelmezésben: „*Az információbiztonság a szóban, rajzban, írásban, a kommunikációs, informatikai és más elektronikus rendszerekben, vagy bármilyen más módon kezelt információk védelmére vonatkozik*.” (Muha & Krasznay, 2014).

A hazai jogszabályok elsődlegesen az elektronikus információs rendszerek védelmét kívánják biztosítani. E tudományos munka is elsődlegesen az elektronikus információs rendszerekben kezelt adatok védelmével kíván foglalkozni.

1. számú ábra
Az elektronikus információs rendszerek védelmi modellje



Forrás: Muha & Krasznay, 2014.

Fontos megemlíteni, hogy az információbiztonság egyik alapelve az úgynevezett CIA elv, vagy magyarul BSR elv, ami a következő szavakat foglalja magába: bizalmasság, sértetlenség és rendelkezésre állás. E három kulcsfontosságú fogalom, ami az adatokat hivatottak védeni. A 2013. évi L. törvény értelmében az adat a sértetlenségéből fakadóan két további komponenst tartalmaz: hitelességet és letagadhatatlanságot.

Az adatok védelme érdekében megalkotott CIA modell ellen a támadói oldal is létrehozta a maga hármasát a sikeres támadások végrehajtásának alapelveként, ezt szokás DAD (disclosure, alteration, denial) modellnek nevezni.

Disclosure (leleplezés): Az érintett rendszer bizalmasságának sérülésével jár, akkor valósul meg a leleplezés, ha egy jogosulatlan személy vagy felhasználó illetéktelenül fér hozzá bizalmas adatokhoz.

Alteration (módosítás): Ebben az esetben az érintett szervezet információs rendszereiben tárolt, feldolgozott vagy továbbított adatok sértetlensége kompromittálódik. A módosítást kétféle kategóriába szokás sorolni, az egyik a szándékos módosítás, a másik a véletlenül történő módosítás.

Denial (akadályozás): Akadályozás akkor valósul meg, amikor a jogosultsággal rendelkező felhasználók valamilyen okból kifolyólag nem férnek hozzá az elektronikus információs rendszerhez, vagy a benne kezelt, tárolt adatokhoz. Ez lehet például elektromosáram-szolgáltatás pillanatnyi kiesése miatt, vagy célzott támadás által kiváltott szolgáltatás megtagadásos (DoS) támadás (Gyurák, 2015).

Annak érdekében, hogy a fent ismertetésre kerülő sikeres támadási tulajdonságok ne tudjanak megvalósulni, védelmi intézkedéseket szükséges megvalósítani preventív, preventív-detektív, valamint gyors elhárító képességek formájában. A hazai jogszabályok által a védelmi intézkedések három nagy kategóriában kerültek besorolásra, melyek a következők: adminisztratív, fizikai és logikai védelmi intézkedés. Fontos megjegyezni, hogy a hazai jogszabályok elsődlegesen az állami szervekre vonatkoznak, és hatályuk nem terjed ki a magánszemélyekre vagy a magánvállalatokra.

Az adminisztratív védelmi intézkedéseket lehet úgy jellemezni, mint kapocs a fizikai és logikai védelmi intézkedések között. Elsősorban itt a szervezet által szabályzati szinten kerülnek meghatározásra különböző védelmi intézkedések, szabályok, követelmények. A szervezetnek tartania kell magát a dokumentumokban meghatározottakhoz. Emellett megemlíthető, hogy az adminisztratív védelemhez tartozik a különböző felhasználói biztonságtudatosság képzések összeállítása, megszervezése és végrehajtása.

Fizikai védelem fogalmába tartozik az elektronikus információs rendszerek hardver elemeinek, valamint az azok működését biztosító infrastruktúra elemeknek a védelme. A fizikai biztonság elsődleges feladata, hogy a jogosulatlan fizikai hozzáférést megakadályozza az érintett elektronikus információs rendszer(ek)hez, valamint azok helyét biztosító helyiségekhez. A másik fontos aspektusa, hogy a védeni kívánt rendszerek működési állapotát biztosító infrastrukturális elemek kompromittálódását (például elektromos hálózat zavarása, megsemmisítése) megelőzze, amennyiben szükséges hatékonyan és gyorsan elhárítsa (például redundancia biztosításával). A fizikai védelem eszközei közé sorolhatók a különböző behatolásjelzők, tűz- és füstjelző megoldások stb.

Logikai védelemhez tartoznak mindazon szoftverkomponensek, amelyek az elektronikus rendszer védelme során felhasználhatók. A szervezet által kikényszerített jelszókezelési szabályok, jogosultságkezelés megvalósítása, a szervezet naplózási tevékenységei, a kriptográfiai megoldások, amik biztosítják az adatok titkosságát és hitelességét úgy, hogy a védtelen közegben elhelyezkedő adatokat titkosítják, illetve a védtelen közegen keresztüli kommunikációt biztosítják. A logikai védelmi pillér alapeszközei közé tartoznak: a szimmetrikus kulcsú és nyilvános kulcsú rejtjelezők, kriptográfiai hash függvények. Ide tartoznak

a határvédelmi megoldások, például tűzfalak. Gyakorlatilag ezt a pillért meg lehet feleltetni az informatikai védelem fogalmával (Gyurák, 2015).

Az információbiztonság jelentősége az információs technológia fejlődésével párhuzamosan napról napra nő. Az adatvédelmi, valamint elektronikus információs rendszereket értinő biztonsági incidensek, például a hackerek támadásai, malware-ek, a rosszindulatú programok és az infokommunikációs rendszereket körbe vevő fizikai környezeti tényezők (például tűz, árvíz) elleni védelem kiemelten fontos az információk védelme érdekében.

Az első jelentős kibertámadásokat csak az 1990-es években tapasztalta meg a világ, amikor az internet elterjedése és a számítógépes hálózatok növekedése lehetővé tette, hogy szélesebb tömegekhez és szervezetekhez is bevezetésre kerüljön, aminek köszönhetően már az emberiség nagyobb mértékben függött a technológiától. Elég csak az 1990-es évek második felében zajló Moonlight Maze fedőnevet viselő támadás sorozatra gondolni, amit vélhetően orosz hackerek hajtottak végre az amerikai kormány és katonai szervezetek számítógépes rendszerein, ezres nagyságrendben tulajdonítottak el jogosulatlanul titkos katonai dokumentumokat. Amikor a számítógépes kémkedés jelei nyilvánvalóvá kezdtek válni, akkor már a támadók közel két éve figyelték belülről a rendszert (Haig & Kovács, 2008). Ez a támadás az APT-támadások[1] egyik korai példája volt, és világszinten felhívta a figyelmet az ilyen típusú fenyegetések komolyságára és veszélyeire, valamint arra, hogy a kormányzati és katonai szervek elektronikus információs rendszerei a kibertámadások potenciális célpontjaivá válhatnak.

A kibertámadások hátterében húzódó célok a következők lehetnek:

- pénzügyi haszonszerzés,
- információ jogosulatlan megszerzése vagy azokban károkozás,
- politikai célok elérése,
- az adatok manipulálása/módosítása vagy megsemmisítése,
- a piaci versenytársakkal szembeni előny megszerzése, például azok információs rendszereinek meggyengítésével,
- alapvető, kritikus infrastruktúrák elektronikus információs rendszereinek működésképtelenné tétele (terrorizmus). A kibertámadások áldozatai egyaránt lehetnek kormányok, vállalatok, szervezetek és egyének, a támadások módszerei, kiterjedtségük, hatásuk különbözőek lehetnek a céloktól, képességektől és az érintett rendszer védelmétől függően.

1 APT-támadás (Advanced Persistent Threat). Az APT-támadás célja alapvetően nem a rongálás útján való károkozás, hanem az adatlopás. A támadó fejlett technikákkal és eszközökkel behatol egy célzottan kiválasztott hálózatba, ahol hosszabb időn keresztül észrevétlenül bent marad, és ezalatt értékes információkat szerez meg.

A következő részben ismertetésre kerülnek napjaink kibertámadásainak legelterjedtebb formái, technikái és a támadásoknak leginkább kitett szektorok, régiók.

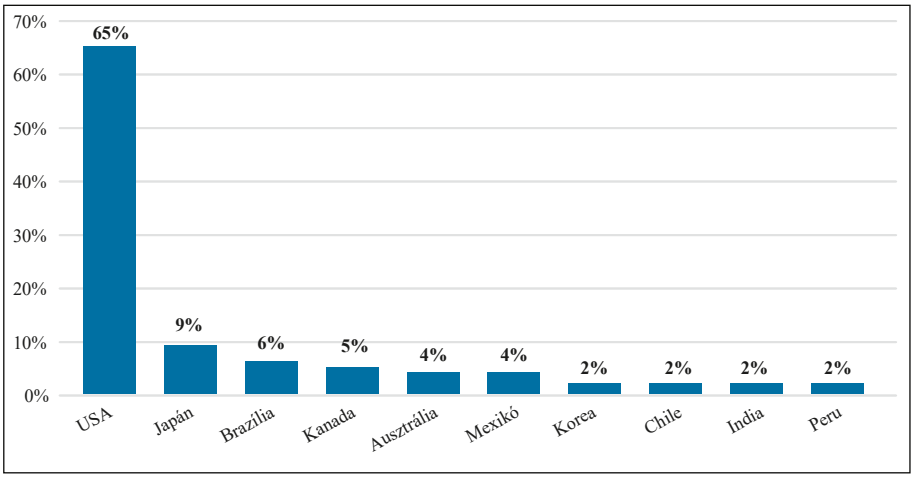
Kiberbiztonsági mutatók, trendek

Jelen tanulmányban ismert IT-biztonsággal foglalkozó cégek friss biztonsági jelentéseit kívánom elemezni, azokból következtetéseket levonni globális szinten. Ennek érdekében, valamint az empirikus kutatása alátámasztása miatt kvalitatív megközelítést alkalmaztam. Ezzel az eljárással mélyebb összefüggések megfigyelését kívánom elvégezni. Igyekeztem olyan dokumentumok tartalomelemzését elvégezni, melyek megbízható forrásoknak tekinthetők, és az azokban található számadatok, statiszták dekódolását és összevetését követően reprezentatív mintának minősülnek.

A kanadai székhelyű BlackBerry vállalat az elmúlt években már főként kiberbiztonsági megoldásokban érdekelt, és leginkább Észak-Amerikában népszerűek a szolgálatásai. 2022 negyedik negyedévéről készítettek átfogó biztonsági jelentést, melyben szereplő adatokat a saját ügyfeleik biztonsági eseményeinek információiból állítottak össze.

A jelentés szerint 2022 utolsó negyedévében a kibertámadásoknak leginkább kitett országok tízes rangsora a következőképpen alakult.

2. számú ábra
Top tíz legtöbbet támadott országok listája (BlackBerry)

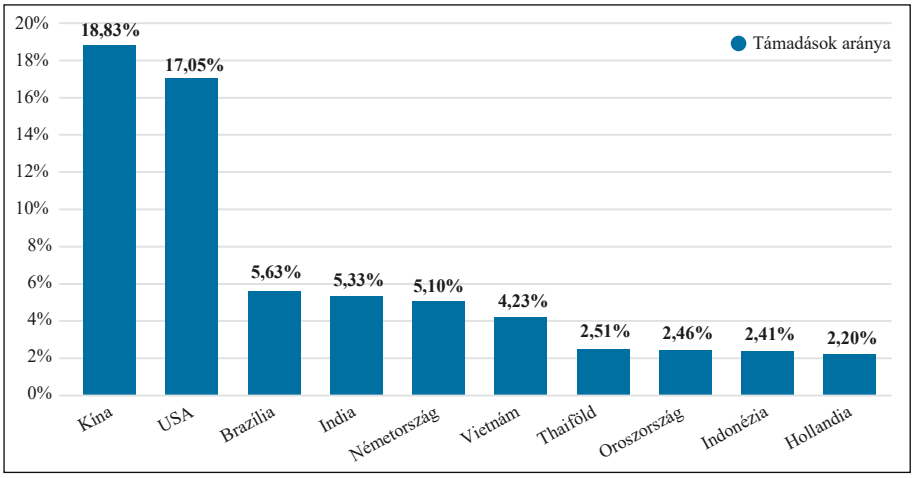


Forrás: BlackBerry Cybersecurity, 2023.

Ezt a felmérést nem lehet reprezentatív felmérésként értékelni, mert minden ilyen jellegű vállalat, jelentésük összeállításakor a saját ügyfeleik adataiból dolgozik, s mivel a BlackBerry egy észak-amerikai székhellyel rendelkező cég, az ügyfelei többsége is ebben a régióban található.

A 2022-ben megjelenő, izraeli székhelyű CyberProof kiberbiztonsági szolgáltatásokra specializálódott vállalat által végzett kutatás felhasznált saját adatokat, valamint nyílt forrású adatokat annak érdekében, hogy meg tudja állapítani a 2021-es év tíz leginkább (kibertérből) támadott országát. Az általuk felállított sorrendet a következő grafikon szemlélteti (DavidPur, 2022).

3. számú ábra
Kibertámadásoknak leginkább kitett országok (2021)



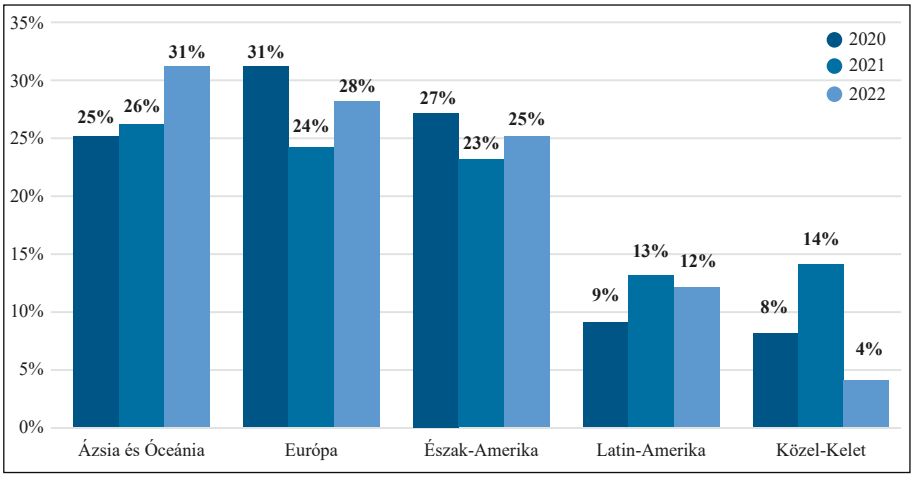
Forrás: DavidPur, 2022.

Európa kitettsége az új típusú fenyegetéssel szemben

Európában 2022 márciusától, közvetlenül azután, hogy Oroszország megtámadta Ukrajnát, jelentősen megnőtt a hátsóajtók (backdoor) telepítése. Ezzel a módszerrel a támadók illetéktelen hozzáférést hoznak létre az elektronikus információs eszközhöz és/vagy rendszerhez, amelyen keresztül képesek ellopni a felhasználói adatokat, vagy megfigyelni a felhasználói tevékenységeket. A régióban a hátsóajtók telepítése az esetek 21%-át, míg a ransomware támadások 11%-át tette ki. Az X-Force által lereagált esetek 10%-ában távoli elérésre szolgáló eszközöket azonosítottak. Az IBM ügyfeleket érő negatív hatások tekintetében az Európában megfigyelt X-Force esetek 38%-a zsarolással kapcsolatos,

17%-a adatlopásra, 14%-a pedig hitelesítő adatgyűjtésre utalt. Európát sújtották leginkább a zsarolásos támadási módszerek; az X-Force által megfigyelt összes zsarolási eset 44%-a ebben a régióban történt. A publikus alkalmazások kihasználása volt az európai szervezetekkel szemben alkalmazott leggyakoribb fertőzési vektor (a fertőzés terjesztésének átvitelére alkalmazott csatorna), amely az X-Force által a régióban kezelt összes incidens 32%-át tette ki, és ezek közül több ransomware fertőzéshez vezetett. Az érvényes helyi fiókokkal való visszaélés 18%-kal a második helyre került, a célzott adathalász linkek pedig 14%-kal a harmadik helyre szorultak vissza a 2021-es 42%-hoz képest, mivel ez az érték jelentősen csökkent. A célzott adathalász linkek számának csökkenése a jobb felhasználói tudatosságnak, az erősebb e-mail biztonsági védelemnek köszönhetően alakulhatott ki. Európában a második leginkább támadott ágazat az ipari gyártás volt az esetek 12%-ával, lemaradva az üzleti szolgáltatási szektor mögött. A harmadik helyezett pedig az energia és az egészségügy ágazat lett 10–10%-kal. Az Egyesült Királyság volt a legtöbbet támadott ország Európában, az esetek 43%-a itt történt, Németország 14%-kal a második, míg a harmadik helyen Portugália végzett 9%-kal (IBM Security, 2023).

4. számú ábra
Régiónkénti incidensek mértéke 2020–2022



Forrás: IBM Security, 2023 nyomán készítette a szerző.

Fókuszban az ipar

A BlackBerry jelentése a klasszikus ipari szereplők közül elsődlegesen az autóiparral foglalkozik behatóbban. Az autógyártással foglalkozó létesítmények az európai szabályzásnak, valamint annak a hazai jogrendbe történő átültetésének köszönhetően (SEVESO III. Irányelv) veszélyes anyagokkal foglalkozó üzemeknek minősülnek, az ott tárolt és gyártás során felhasznált veszélyes anyag mennyiségek miatt. Ez az alig százéves múltra visszatekintő ipari ágazat hatalmas technológiai forradalom és paradigmaváltás alatt áll jelenleg, elég csak az új típusú vezetéstámogató rendszerekre (ADAS) és a még nem végleges fázisban járó önvezetésre gondolnunk. Ez a digitális átalakulása a közlekedés és közlekedők szempontjából számos előnnyel jár, viszont a kiberbiztonság tekintetében fokozottan megnő a fenyegetettség kockázata azzal, hogy a járművek egyre inkább összekapcsoltabbakká válnak, mind egymással, mind a közlekedési infrastruktúra egyes elemeivel, valamint egyre autonómabbak lesznek.

Ami még fontosabb, hogy a gyártástechnológiában bekövetkezett fejlődés számos pozitív hozadéka mellett veszélyt is rejt magában, többek között a kibertérből érkező támadásokkal szembeni kitettséget. Az új típusú támadások nemcsak az autóipart vették célba, hanem az egész gyártásipart is, a gyártási műveletek megzavarása, érzékeny adatok ellopása és az ellátási láncok kompromittálása céljából. A BlackBerry 2022-ben növekedést figyelt meg az autóipart célba vevő rosszindulatú entitások számában, és az általuk okozott kiesések, incidensek mértékében. Az autóipar hatalmas ellátási lánccal rendelkezik, több körös beszállítói láncok vannak és ezek potenciálisan mind kitettek a célzott támadásokkal szemben.

A cég jelentése alapján az autóipar ellen alkalmazásra kerülő legelterjedtebb támadások 2022 utolsó negyedévében a következők.

Letöltőprogram (Downloader)

A megtévesztő támadás szereplői a művelet első részeként ráveszik az áldozatokat, hogy telepítsék a letöltőprogramot. A kérés végrehajtása után a letöltőprogramok további rosszindulatú kódokat és hasznos adatokat telepítenek, ezáltal szélesebb körű kibertámadásokat képesek végrehajtani.

A GuLoader kiváló példája egy olyan letöltőprogramnak, amely ebben a jelentési időszakban az autóipart célozta meg. A rosszindulatú programot először 2019-ben azonosították, ez idő alatt folyamatosan fejlődött. A GuLoader gyakran legitim digitális dokumentumokként vagy futtatható fájlokként jelenik meg, mielőtt letöltene más kártevőket tartalmazó szoftvereket.

Adattolvaj (Infostealer)

Az adattolvaj egy olyan típusú kártékony szoftver (malware), amelynek célja az érzékeny információk eltulajdonítása a fertőzött eszközökről/ rendszerből. A gyakorlatban az adatlopást úgy hajtják végre, hogy megkeresik és illegálisan kiszűrik az áldozat rendszeréből az adatokat, amelyeket aztán pénzügyi és/vagy taktikai célok támogatására használnak fel. Az adattolvajok olyan RAT-okkal (Remote Access Trojan) együtt használhatók, mint a Remcos, ami az egyik legalapvetőbb rosszindulatú program, s amelyet gyakran szolgáltatásként adnak el más fenyegető szereplők számára, hogy hozzáférést és irányítást szerezzenek az áldozatrendszerek felett. (A RAT-ok általában titokban települnek az áldozat számítógépére, és lehetővé teszik a támadó számára a számítógép teljes irányítását anélkül, hogy a felhasználó észre venné.)

Ransomware (Zsarolóvírus)

A ransomware minden biztonsági csapat rémálma. Az ipari ellátási láncokat megcélzó ransomware-ek pusztító hatásúak lehetnek. Az autóiparban egy ransomware támadás az ellátási lánc bármely szakaszában leállíthatja a termelést vagy a forgalmazást, ami elsődlegesen bevétel- és hírnévveszteséget okozhat az iparág ökoszisztémáiban.

A BlackCat ransomware-t 2022-ben figyelték meg néhány hírhedtebb ransomware támadásban. A gyakran kis- és középvállalkozásokat zsaroló kiberbűnözői csoportok, akik ezt a RaaS-t használják, döntően haszonszerzés céljából és nagyrészt a gyártást célozzák meg. A BlackCat ransomware behatol egy környezetbe, kiszűri az értékes adatokat, majd titkosítja a csatlakoztatott rendszereket (BlackBerry Cybersecurity, 2023). A RaaS jelentése: Ransomware as Sevice – vagyis a ransomeware programokat és vezérlő infrastruktúrájukat mint szolgáltatást meg lehet venni azok fejlesztőitől, így számos kiberbűnöző felhasználhatja, amenynyiben a „szolgáltatótól" megvásárolja. Számos üzleti modell létezik a ransomware-ek értékesítésével kapcsolatban, a legelterjedtebb formulák a következők:

1. Egyszeri ransomware vásárlás.
2. Havi előfizetés.
3. Jutalék a váltságdíj százalékában.
4. Egyes RaaS-szolgáltatók több fizetési módot kombinálnak, például előfizetési díjat és a váltságdíj egy részét (általában százalékban).

A RaaS szolgáltatások kínálói általában a dark weben keresztül érhetők el, a szolgáltatás növekvő népszerűsége miatt a zsarolóvírusok terjedése egyre inkább

széles körűvé válik, és mind a vállalkozások, mind az egyének számára súlyos biztonsági kockázatot jelentenek (Kaspersky, 2023).

Kettős felhasználású eszközök (Dual-Use Tools)

A kettős felhasználású eszközök általában legitim eszközök és szoftverek, amelyek olyan funkciókat kínálnak, amelyekkel a támadók akár visszaélhetnek. A „living off the land" (LotL), mely kifejezés a rendszerek által nyújtott eszközök kiaknázására utal, a gyakorlatban azt jelenti, hogy a támadók olyan eszközöket, funkciókat vagy technológiákat használnak fel, amelyek már megtalálhatóak a célrendszerben, így minimalizálják az észlelés kockázatát és nehezebbé teszik a védekezést. A kibertámadások elkövetésére leginkább alkalmazott kettős felhasználású eszközök közé tartoznak a penetrációs tesztek (penetration testing) eszközei és szoftverei. Ezeket eredetileg arra tervezték, hogy teszteljék és ellenőrizzék a szervezetek informatikai rendszereinek biztonságát, de a kiberbűnözők is alkalmazzák ezeket támadásaik végrehajtására és a sebezhető rendszerek megtalálására. Ennek köszönhetően a támadók egy-egy rendszer sérülékenységét automatizált módon, könnyedén detektálhatják (BlackBerry Cybersecurity, 2023).

A támadók a rosszindulatú kódok helyett egyre inkább kettős felhasználású eszközökre hagyatkoznak a célrendszerbe való bejutáshoz, az értékes adatok kiszivárgásához vagy akár a rosszindulatú programok „engedélyezett" eszközként történő telepítéséhez. A rendszergazdáknak el kell távolítaniuk minden olyan kettős felhasználású eszközt, amelyre nincs érvényes használati eset (use case) vagy üzleti indok.

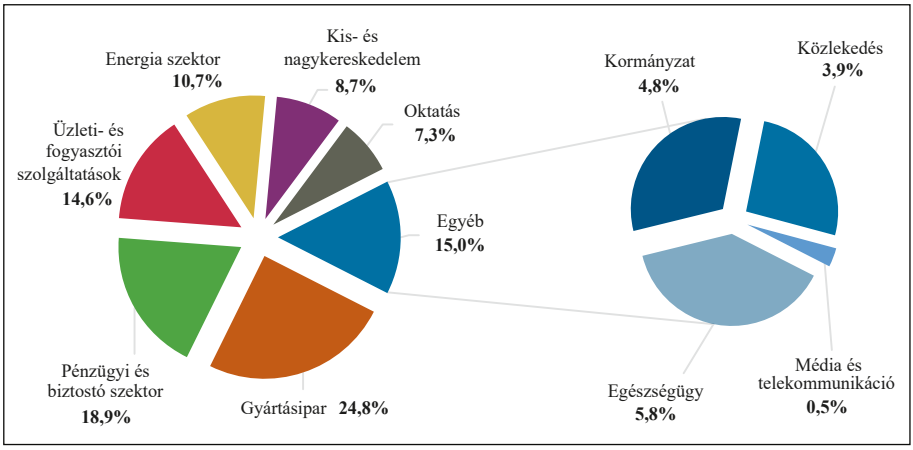
A CISCO 2022-es évértékelő jelentésében ismerteti a három, kiberbűnözők által leginkább használt kettős felhasználású eszközt, melyek a következők: Cobalt Strike, Brute Ratel és a Silver. Nem meglepő módon ezek mind red team eszközök, azaz támadások szimulálására használják a kiberbiztonsági szakemberek. Ezeknek az eszközöknek a detektálása nem egyszerű feladat, és a jelentés arra is kitér, hogy ha sikerül is, a támadók kilétét szinte lehetetlen azonosítani a későbbiekben. A CISCO vizsgálata alapján a kettős felhasználású eszközök APT-, ransomware vagy más támadások elfedésére, azok kiegészítésére is kiválóan alkalmas (CISCO Talos, 2023).

Az IBM X-Force legfrissebb jelentését vizsgálva részletesebb kimutatásokra bukkanhatunk. Az X-Force évente közzéteszi a világ kiberbiztonsági helyzetét összefoglaló jelentését, amely az aktuális trendeket és a jövőbeli fenyegetéseket ismerteti, emellett ajánlásokat tartalmaz a védelmi intézkedések, megoldások javítására és fejlesztésére. Az IBM ügyfelei számára az X-Force biztosítja

a megfelelő információkat és megoldásokat ahhoz, hogy védelmet alakítsanak ki a kiberbiztonsági kockázatokkal szemben.

Az IBM X-Force Threat Intelligence Index 2023-as jelentése az egyes iparágakat összehasonlítva arra a következtetésre jutott, hogy 2022-ben a támadásoknak leginkább kitett iparág a gyártásipar volt, s ami még említésre méltó, hogy az energetikai szektor is kiemelt célpontja a támadóknak.

5. számú ábra
A 2022-es év leginkább támadott ágazatai



Forrás: IBM Security, 2023 nyomán készítette a szerző.

A különböző kiberbiztonsági megoldásokat nyújtó vállalatok tapasztalatai alapján kijelenthető, hogy az üzemek, beleértve a veszélyes anyagokkal foglalkozó üzemeket is, potenciális célpontjai lehetnek egy-egy esetleges kibertérből érkező támadásnak.

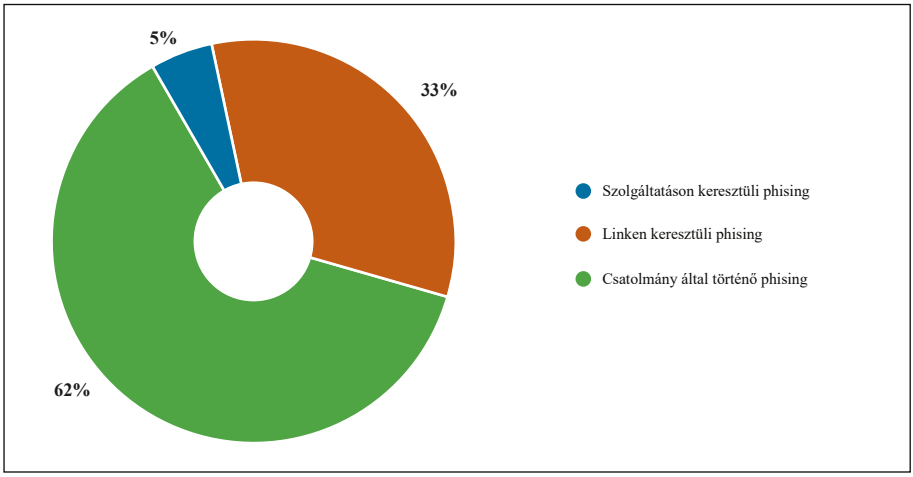
A támadási vektorok ismertetése előtt szükséges tisztázni a fogalmat: a támadási vektor egy olyan útvonal vagy módszer, amelyen keresztül egy támadó eléri vagy befolyásolja a rendszert vagy hálózatot, és kárt okozhat benne.

Az ArticWolf kiberbiztonsági vállalat szerint az öt leginkább elterjed támadási vektor:

1. Phishing (adathalászat).
2. Sebezhetőség kihasználása (Log4J).
3. Biztonsági szempontból hibás konfiguráció.
4. Kompromittálódott hitelesítő adatok.
5. Ellátási lánc beszállítóin keresztüli bejutás a célpont vállalatrendszerébe (Artic Wolf, 2022).

A célzott adathalász támadásokat az IBM X-Force jelentése alapján a következő technikai komponensekre lehet tovább-bontani: szolgáltatáson keresztüli adathalász tevékenység, weboldal linkjével történő adathalászat, jellemzően e-mail csatolmány letöltésével egy rosszindulatú kód futtatása által történő adathalász tevékenység. Ezek 2022-es megoszlását a 6. számú ábrán láthatjuk.

6. számú ábra
Célzott adathalász technikák megoszlása



Forrás: IBM Security, 2023.

Az X-Force Incident Response adatai szerint 2022-ben a hátsóajtók telepítése volt a leggyakoribb célintézkedés. Ez az összes jelentett incidens közül 21%-ot tett ki. Ezt követően a második legnépszerű támadások a ransomware támadások voltak, melyek az esetek 17%-ban voltak felelősek a támadók céljai elérésének segítésében. Az esetek 6%-ában az üzleti e-mail kompromittálása érdekében tett intézkedések állnak. Rosszindulatú dokumentumok (maldocs), spam kampányok, távoli elérési eszközök kihasználása és a célpont szervereihez való hozzáférés az összes jelentett incidensek 5–5%-ában voltak felfedezhetők (IBM Security, 2023).

Véleményem szerint a rendszeres időközönként megtartásra kerülő, felhasználóknak szóló, szerepköralapú biztonságtudatossági képzések nagy mértében hozzájárulnak az adathalász támadások és ransomware támadások hatékonyságának csökkentéséhez.

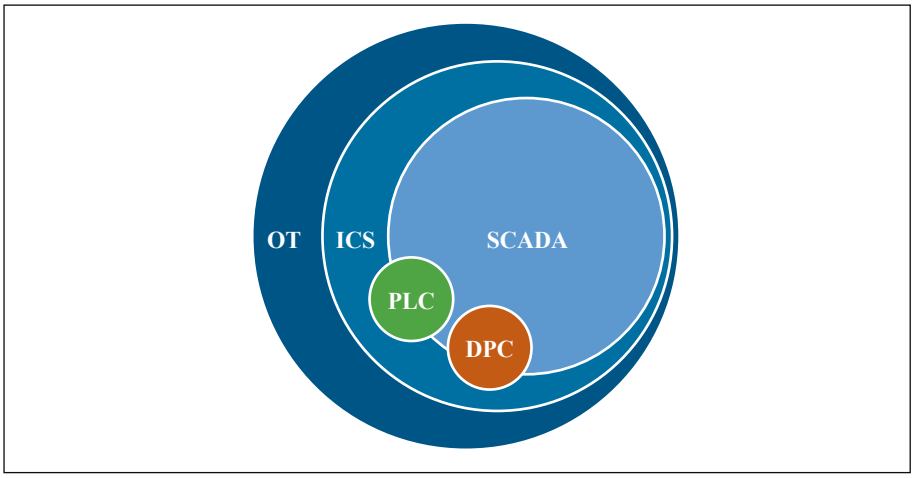
Az OT-rendszerek kitettsége

Az IT-rendszereken kívül, melyek elsődlegesen számítástechnikai infrastruktúrára és az abban kezelt adatokra fókuszál, az OT (operációs technológia) a gyártási folyamatok és az ipari rendszerek irányításához szükséges technológiákat foglalja magában. Amennyiben ipari üzemekről beszélünk, megkerülhetetlen fogalom az OT és az abban lévő ipari vezérlőrendszerek (ICS – Industrial Control System) biztonságának kérdésköre.

Ezeknek az eszközöknek a megbízhatósága és biztonsága kulcsfontosságú az ipari vállalatok számára, hiszen egy esetleges hiba vagy támadás akár súlyos következményekkel is járhat. A veszélyes üzemek esetében az OT biztonságának kérdésköre még nagyobb jelentőséggel bír. Ezekben az üzemekben olyan veszélyes anyagokkal dolgoznak, amelyek súlyos egészségkárosodást vagy akár halált is okozhatnak. Az ilyen üzemeknél kiemelt fontosságú a megbízható és biztonságos működés, hiszen egy súlyos ipari baleset következményei akár hatalmas mértékű pusztítással járhatnak az emberi életre, egészségre és a természeti és épített környezetre nézve egyaránt. Az ICS biztonsága az ipari folyamatok működését veszélyeztető fenyegetések elleni védelemmel foglalkozik. Ezek a fenyegetések lehetnek külső támadások, például hackerek által elkövetett kibertámadások, vagy belső fenyegetések, például hibák vagy rosszindulatú szándékkal elkövetett események. Az ICS biztonságában a kulcsfontosságú elemek közé tartozik az eszközök és szoftverek megbízhatósága és sebezhetőségének minimalizálása, a hálózatbiztonság, a hozzáférési jogosultságok kezelése, valamint az események és a működési adatok monitorozása és elemzése.

Az OT-biztonság azonban ennél is tágabb területet ölel fel, amely a gyártási folyamatok minden aspektusára kiterjed. Az OT biztonsága az ICS biztonságát is magába foglalja, de figyelmet fordít az üzemeltető személyzet tudatosságára, az alkalmazottak képzésére, a rendszeres karbantartásra és a működési folyamatok optimalizálására is.

7. számú ábra
OT-rendszerelemek kapcsolatai egymáshoz viszonyítva



Forrás: Gast, 2020.

Korábban az ipari üzemek hálózata zártkörű volt, izoláltan működtek a világhálótól és más rendszerektől, azonban a 2010-es években létrejött az ipar negyedik forradalma, az Ipar 4.0. Ez egy jelentős paradigmaváltást hordozott magában, aminek fő célkitűzése, hogy a hatékonyabb termelés növelése érdekében új dimenzióra emelje a digitalizációs és automatizációs folyamatokat az ipari termelésben. Emellett a másik érdemi célja az volt, hogy az ipari termelést rugalmasabbá tegye az ügyfelek elvárásainak megfelelően.

Az Ipar 4.0 kommunikációs csatornái, eszközei közé tartozik az internet, IoT környezet és a mesterséges intelligencia, gépi mélytanulás, mely révén az ipari vállalatok hatékonyabban képesek feldolgozni a rendelkezésre álló adatokat.

Az Ipar 4.0 terjedése a vállalatoknál jelentős előnyökkel jár, hiszen a termelést végző eszközök, ipari vezérlőrendszerek – jellemzően IoT környezet segítségével – képesek egymással kommunikálni humán beavatkozás nélkül. Ezzel költséghatékonyabban és pontosabban kerülnek végrehajtásra az egyes munkafázisok (Ászity & Dömötör, 2019).

Az IBM X-Force 2023-as jelentése kitér az OT-hálózatok ellen elkövetett rosszindulatú kezdeti jogosultság szerzési vektorok első helyezettjeire a 2022-es év tekintetében. A célzott adathalász technikák végeztek az első helyen, mivel az esetek 38%-ában valamilyen adathalász módszerrel próbáltak a támadók kezdeti jogosultságokat szerzeni a célpontjuk OT-hálózatába való bejutáshoz. A második helyen a nyilvánosan elérhető alkalmazások rosszindulatú kihasználása

állt 24%-kal. A jogosultságok megszerzése érdekében az egyes rendszerek, szoftverek hátsóajtóinak azonosítása és kihasználása is kiemelkedő szerepet játszik, az esetek 20%-ában ezt a módszert alkalmazták a támadók. Végezetül pedig a ransomware típusú támadások segítségével megszerzett hozzáférések az ipari rendszereknél továbbra is népszerű technikának számítanak, az esetek 19%-ában feleltek a jogosultságok megszerzéséért.

A támadások hatásait vizsgálva a zsarolás továbbra is vezető pozícióban van az esetek 29%-ával, az adatlopások pedig a második helyen állnak 24%-os eredménnyel (IBM Security, 2023).

Az OT-rendszerek esetén kiemelt biztonsági probléma, valamint sérülékenységet okozó jellegzetesség, hogy nem kerül az IT- és OT-hálózat egymástól szegmentálásra. Amennyiben az OT-környezet a világhálótól elszigetelten üzemel, de az IT-hálózattól nem került „hermetikusan elválasztásra", és vannak olyan például monitorozó rendszerek, melyek az OT-környezetből nyerik az adatokat (SQL – relációs adatbázis), az OT-környezet sebezhetővé válik az IT-oldal miatt. A hálózat ezen részeinek megfelelő szegmentálása és a rajtuk keresztüli kommunikáció szoros figyelemmel kísérése megőrizheti az eszközök biztonságát (Gast, 2020).

A Honeywell által publikált jelentés az USB portokhoz csatlakoztatható hordozható adattárolók fenyegetéséről számolt be. Ezek a hordozható eszközök malware-rel fertőzöttek. A fenyegetések 52%-át cserélhető adathordozókra tervezték. A Honeywell által tapasztalt fenyegetések közül továbbra is a trójaiak domináltak, az észlelt kártevők 76%-át tették ki. A távelérést vagy távvezérlést biztosító rosszindulatú programok aránya 51% volt. Az elkövetők szándékosan használnak USB cserélhető adathordozókat kezdeti támadási vektorként, ennek segítségével távoli kapcsolatot képesek létesíteni további payloads-ok (a kártékony kódok azon része, ami rosszindulatú műveletet hajt végre) letöltéséhez, adatok kiszűréséhez, valamint az irányítás megszerzéséhez. Hordozható adathordozókat használnak a támadók, hogy ipari vállalatok légrés (air-gapped) környezetébe – ezek a környezetek általában le vannak választva a világhálótól és más hálózatoktól – könnyedén be tudjanak hatolni, és kártékony tevékenységeket hajtsanak végre (Honeywell Forge, 2022). A CISCO által közzétett 2022-es évi kiberbiztonsági jelentés arról számol be, hogy 2022. január óta a CTIR (a CISCO biztonsági incidenskezelő csoportja) növekvő számú beavatkozásra reagált olyan esetekben, amelyekben a szervezeteket károsító programokkal fertőzött eltávolítható USB hordozható adattárolók szerepeltek. Több, USB-n keresztül terjedő kártevőcsaládot is megfigyeltek, beleértve a Windows rendszereket célzó Sality és PlugX programokat. Ez a régi támadási módszer hatékonyan alkalmazható az izolált környezetben működő elavult, biztonsági javításokkal nem rendelkező, örökség rendszerek ellen (CISCO Talos, 2023).

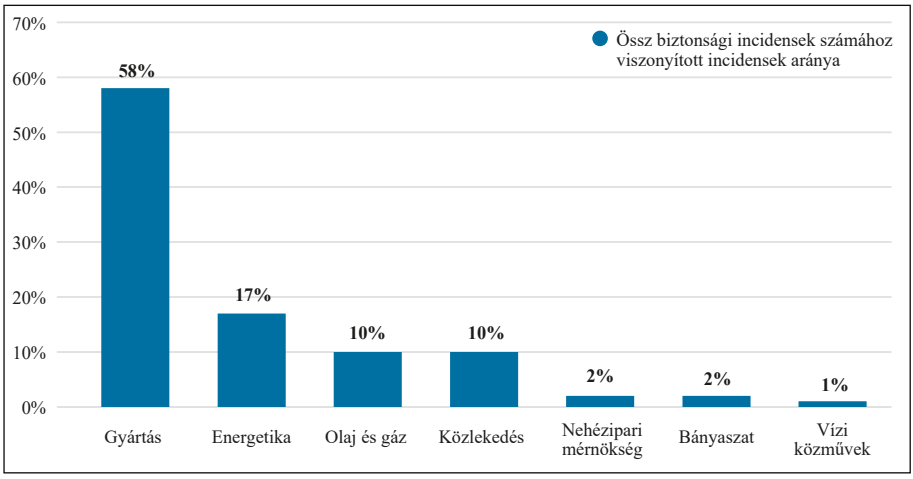
Általában az USB-n keresztüli rosszindulatú programokat az ipari célpontok elleni nagyobb kibertámadási kampányok részeként használják fel. Azért alkalmazzák ezeket az eszközöket, mert képesek megkerülni a hálózati védelmet és a légréseket, amelyeken számos ipari létesítmény védelme múlik.

Természetesen mint mindennek, az ipari vállaltok digitalizációjának is számos hátránya van, a legnagyobb, hogy ezzel kiemelt célponttá válnak a kibertérből érkező támadásokkal szemben. Egy veszélyes anyagokkal foglalkozó üzemmel szembeni esetleges rosszindulatú hacker támadás közvetetten komoly, akár súlyos ipari balesetet is elő tud idézni. Véleményem szerint, melyet kutatási adataim is alátámasztanak, a hazai üzemek OT-rendszereinek biztonsága sok esetben nincs teljeskörűen, a kockázatokkal arányos módon megvalósítva. A közeljövőben számos hazai üzem biztonsági stratégiájában kiemelt hangsúlyt kell fektetni a hálózatvédelmi képességének fejlesztésére.

Az IBM X-Force biztonsági jelentésében összeállításra került a 2022-es évben leginkább támadott OT-hálózatok iparágak szerinti megoszlása.

8. számú ábra

Leginkább támadott OT-rendszerek, iparágak szerinti bontásban (2022)



Forrás: IBM Security, 2023.

Hazánk veszélyes üzemeinek biztonsági kérdésköre

Magyarországon a veszélyes anyagokkal foglalkozó üzemek biztonságos működését számos jogszabály, hatósági felügyelet és ellenőrzés, valamint az üzemeltető biztonságos üzemeltetés melletti elköteleződése révén létrejövő védelmi szabályok, intézkedések biztosítják.

A 219/2011. (X. 20.) Korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről egyértelműen rendelkezik a veszélyes anyagokkal foglalkozó üzemek besorolásáról, az üzemeltetésre háruló biztonsági dokumentációk elkészítéséről. A jogszabály legfrissebb kiegészítése a SEVESO III. irányelv hazai jogrendbe ültetésének eredményeképpen született meg. A veszélyes üzemek Magyarországon három kategóriába sorolódnak az üzem területén található veszélyes anyagok mennyisége alapján. A három kategória a következő: (1) küszöbérték alatti veszélyes üzemek; (2) alsó küszöbértékű veszélyes üzemek és (3) felső küszöbértékű veszélyes üzemek. Ezeken a kategóriákon kívül a jogszabály hatálya alá tartoznak a kiemelten kezelendő létesítményeket.

A veszélyes üzemek biztonságos üzemeltetése és a hatósági megfelelés érdekében számos biztonsági dokumentációt kell elkészítenie az üzemeltetőknek, ideértve a küszöbérték alatti és alsó küszöbértékű üzemek irányítási rendszerének dokumentációját, valamint a felső küszöbértékű üzemek esetén biztonsági irányítási rendszert (BIR) szükséges működtetni. Alsó küszöbértékű és küszöbérték alatti veszélyes anyagokkal foglalkozó üzemek esetén működtetett irányítási rendszer, amely a súlyos balesetek kialakulásának kockázatát csökkenti, ellenben a felső küszöbértékű üzemtől eltérően ezt nem szükséges egységes biztonsági irányítási rendszer keretébe foglalni, természetesen a jogszabály által előírt tartalmi követelmények megegyeznek a BIR-ével.

Ezek az irányítási rendszerek a veszélyes anyagokkal kapcsolatos súlyos balesetek megelőzését és elhárítását biztosítják. Az üzemeltető a biztonsági irányítási rendszert beépíti a veszélyes anyagokkal foglalkozó üzem általános vezetési rendszerébe.

A hatóság által megkövetelt biztonsági irányítási rendszer (BIR) szerkezeti felépítését tekintve hasonlóságot mutat az ISO nemzetközi szabványcsalád ISO/IEC 9001:2015 Minőségirányítási Rendszerrel (MIR), ISO/IEC 14001:2015 Környezetirányítási Rendszerrel (KIR) és az ISO/IEC 45001:2018 Munkahelyi Egészségvédelmi és Biztonsági Irányítási Rendszerrel (MEBIR) (Vass, Mesics , & Kovács, 2016).

Ezen irányítási rendszerek is átvették más nemzetközi szabvány által előirányzott irányítási rendszerek alapvető működési mechanizmusát, a PDCA ciklust.

Ennek köszönhetően a biztonsági teljesítményértékelési és a nyomonkövetési rendszer kialakítása, amihez szükséges az üzemspecifikus biztonsági teljesítménymutatók meghatározása is, megvalósítható. Ez végül egy folyamatosan fejlődő, biztonságos üzemeltetést eredményezhet.

Magyarországon a veszélyes anyagokkal foglalkozó üzemek jelentős része nem rendelkezik független tanúsító szervezet által tanúsított információbiztonsági irányítási rendszerrel (ISO/IEC 27001:2013 – ISO/IEC 27001:2022), s amennyiben nem minősül nemzeti létfontosságú rendszerelemnek, abban az esetben a 41/2015 BM rendeletben foglaltak sem érvényesíthetők rajtuk kötelező jelleggel.

Mivel a kibertérből érkező támadások száma évről évre nő, az üzemek és végsősoron hazánk biztonságáért szükséges lenne a jövőben az iparbiztonsági hatóság által az üzemekben megvalósított információbiztonsági intézkedéseket, valamint a kibertérből érkező támadások elleni védelmi képességet ellenőrizni. A 219/2011. (X. 20.) Korm. rendeletben foglalt irányítási, valamint biztonsági irányítási rendszer információbiztonsági szempontokkal történő fejlesztési lehetőségei tekintetében jelenleg is kutatást folytat a szerző. Számos nemzetközi ajánlás, szabvány létezik a témában, valamint a hazai jogszabályok között is fellelhetőek azok a komponensek, melyek segítségével megalkotható lenne egy keretrendszer, mely az IT- és OT-rendszerek alapvető biztonsági feltételeit lennének hivatottak biztosítani.

Ennek a keretrendszernek a megvalósításán túl a másik probléma a katasztrófavédelmi hatóság információbiztonsági kompetenciájának kialakítása, valamint az ellenőrzések időbeli korlátai miatt kialakuló nehézségek leküzdése. A biztonsági irányítási rendszerek ellenőrzési nehézségeire már korábban több hazai szerző is felhívta a figyelmet. Míg egy adott irányítási rendszer auditálására specializálódott auditori csapatnak az időmenedzsmentje megenged több napos auditálási tevékenységet, addig a hatóságnak ez csak egy részfeladat, számos egyéb, fontos feladat mellett. Ebből következően nem tudnak néhány óránál többet fordítani egy-egy veszélyes üzem BIR-jének auditjára (Mesics, 2015).

Megoldási lehetőségek

Azon veszélyes üzemeknek az elektronikus információs rendszerei védettebbek, melyek a 2012. évi CLXVI. törvény hatálya alá tartoznak, és nemzeti létfontosságú rendszerelemnek minősülnek. Ez köszönhető annak, hogy a 2013. évi L. törvény 2 § (2) bekezdés c) pontja kijelenti, hogy e törvény rendelkezéseit kell alkalmazni az európai, valamint nemzeti létfontosságú rendszerelemek

elektronikus információs rendszereivel kapcsolatban. Ezen elektronikus információs rendszerek védelmi képességének követelményeit a 41/2015. (VII. 15.) BM rendelet biztosítja, ami tekinthető a 2013. évi L. törvény végrehajtási rendeletének is. Mivel hazánkban azon veszélyes anyagokkal foglalkozó üzemek száma, melyek egyben nemzeti vagy európai létfontosságú rendszerelemnek minősülnek meglehetősen kevés, ezért ebből kifolyólag a veszélyes üzemek többségére a 2013. évi L. törvény, valamint a 41/2015. (VII. 15.) BM rendelet hatálya nem terjed ki. Ezen üzemek üzemeltetői nincsenek hatósági felügyelet mellett kötelezve az elektronikus információs rendszerük védelmének jogszabályok szerinti kialakítására. Ebből kifolyólag a védendő rendszerek adott biztonsági osztályba történő besorolása, valamint a szervezet biztonsági szintjének meghatározása, és az azokhoz tartozó biztonsági követelmények megvalósítása sem történik meg.

Jelen tudományos munka nem állítja, hogy nincsenek védelmi intézkedések és megoldások alkalmazásban egyetlen egy üzem elektronikus információs rendszere esetén sem. Minden bizonnyal vannak, viszont ezek a védelmi megoldások nincsenek egységesen kezelve, átláthatatlanok. Nem biztosított, hogy a védelmi intézkedések és megoldások az információbiztonsági kockázatokkal arányosan kerültek kialakításra.

Kutatásom során egy olyan információbiztonsági keretrendszert tervezek összeállítani, aminek hatására a veszélyes üzemek IT-hálózata biztonságosabbá tehető, valamint az ellenőrző hatóság is, mélyebb informatikai és információbiztonsági ismeretek nélkül, képes leellenőrizni és objektíven értékelni azt. Ez a keretrendszer bekerülne a veszélyes üzemek irányítási rendszerébe, valamint a felső küszöbértékű üzemek esetén a biztonsági irányítási rendszer szerves részét képezné. Ezen információbiztonsági kontrollok összeállítása elsődlegesen a jelenleg hatályos hazai jogszabályokból, a nemzetközi szabványokból, mint az ISO/IEC 27001:2022, valamint más szervezetek útmutatóiból (például az amerikai NIST 800-53 rev. 5) kerülnek a jövőben megvalósításra. Az OT-biztonság is részét képezi a biztonsági irányítási rendszerek fejlesztésének. Ez esetben az összeállításra kerülő kontrollszett főként az iparági jó gyakorlatokból és az amerikai NIST 800-82 ipari vezérlőrendszerek (ICS) védelmének kialakítását segítő útmutatóból kerül kialakításra. A keretrendszerek kialakításában kiemelt szerepet kap az érthetőség, hogy minden fél ugyanazt értse az egyes kontrollok alatt, valamint az átláthatóság, hatósági vizsgálati rész felépítése. A hatóságnak az üzem más jellegű vizsgálatai miatt limitált ideje jut az irányítási rendszerek vizsgálatára, ezért szükséges egy checklist összeállítása, így az ellenőrzések célirányosan lefolytathatók a lehető legkisebb időveszteség mellett.

Információbiztonsági keretrendszer implementálási kötelezettsége alól mentességet élvezhetnének azon üzemeltetők, akik rendelkeznek információbiztonsági irányítási rendszerrel (IBIR). A menetességet csak azok az üzemek kaphatnák meg, melyek IBIR-jének működési minőségét igazoló tanúsítványa független, akkreditált tanúsító szervezet által került kiállításra. Ekkor a katasztrófavédelmi hatóság a bemutatott tanúsítvány és jegyzőkönyv átvizsgálását követően rendelkezhetne az implementálási kötelezettség alóli mentességről.

A katasztrófavédelmi bírságolás a fent megfogalmazottak nem megfelelő megvalósításáért, vagy annak teljes elmulasztásáért egy olyan kérdéskör, mellyel jelen tanulmány keretei között nem kívánok behatóbban foglalkozni. A jelenleg is hatályos katasztrófavédelmi bírságolás szabályait és tételeit tartalmazó jogszabályba[2] könnyedén implementálható lehet az információbiztonsági szempontok mellőzése, vagy nem teljes körű megfelelősége, mint BIR nem megfelelőség.

A veszélyes anyagokkal foglalkozó üzemek irányítási, illetve biztonságirányítási rendszerének információbiztonsági és ICS biztonsági szempontokkal történő fejlesztési lehetősége a magyar veszélyes anyagokkal foglalkozó üzemek biztonságát növelné egy jelentős 21. századi kihívással szemben, ami végső soron az ország biztonságára is kedvezően hatna.

Összefoglalás

A kibertámadások száma évről évre növekvő értékeket mutat. Tanulmányomban igyekeztem bemutatni az elmúlt évben leginkább alkalmazott támadási fajtákat, módszereket és technikákat. Ismert kiberbiztonsági profillal rendelkező vállalatok éves áttekintő beszámolói kerültek elemzésre, melyek alapján megállapíthatóvá vált a trendek folyamatos átalakulása. A régebbi módszerek új formában történő alkalmazása széles körben elterjedté vált a támadói oldalon (például USB meghajtók általi támadások, vagy a ransomware mint szolgáltatás térhódítása stb.). A jelentésekből jól kivehető, hogy az új típusú támadások kiemelt célpontjai az ipari tevékenységet folytató vállalatok. A téma aktualitása indokolttá teszi, hogy kutatást végezzek a hazai veszélyes üzemek kibervédelmi képességének fejlesztési lehetőségeivel kapcsolatban. Véleményem szerint a veszélyes üzemek irányítási rendszereibe implementálhatók az IT- és OT-biztonság kialakítását biztosító védelmi intézkedések. A veszélyes anyagokkal foglalkozó üzemek az Országos Iparbiztonsági Főfelügyelőség felügyelete alá

2 208/2011. (X. 12.) Korm. rendelet a katasztrófavédelmi bírság részletes szabályairól, a katasztrófavédelmi hozzájárulás befizetéséről és visszatérítéséről.

tartoznak, így kézenfekvő törekvés, hogy a hatóság a rendszeres időközönként végrehajtott ellenőrzéseinek keretein belül az üzem kibervédelmi képességeit is vizsgálja. A későbbiekben részletes IT- és OT-biztonsági szempontokat tartalmazó keretrendszert és hatósági ellenőrzéseket segítő módszertant kívánok kidolgozni, azonban ehhez további kutatások elvégzése szükséges.

Felhasznált irodalom

Artic Wolf. (2022). *The Top 5 Cyber Attack Vectors*. https://arcticwolf.com/resources/blog/top-five-cyberattack-vectors/

Ászity S. & Dömötör F. (2019). *IPAR 4.0.* Akadémiai Kiadó. https://doi.org/10.1556/9789634542759

BlackBerry Cybersecurity. (2023). *Global Threat Intelligence Report.*

CISCO Talos. (2023). *2022 Year in Review.* CISCO.

Davidpur, N. (2022). *Which Countries are Most Dangerous? Cyber Attack Origin – by Country*. (CyberProof). https://blog.cyberproof.com/blog/which-countries-are-most-dangerous

Gast, K. (2020). *What is ICS Security? How to Defend Against Attacks*. https://securityboulevard.com/2020/12/what-is-ics-security-how-to-defend-against-attacks/

Gyurák G. (2015). *Informatikabiztonság I.* Pollack Press.

Haig Zs. & Kovács L. (2008). Fenyegetések a cybertérből. *Védelempolitika*, *1*(5), 61–69.

Honeywell Forge. (2022). *Industrial cybersecurity USB threat report 2022.* Honeywell.

IBM Security. (2023). *X-Force Threat Intelligence Index 2023.*

Kaspersky. (2023). *Ransomware-as-a-service (RaaS)*. https://encyclopedia.kaspersky.com/glossary/ransomware-as-a-service-raas/

Mesics Z. (2015). Biztonsági irányítási rendszer értékelése. *Hadmérnök, 10*(1), 108–118.

Muha L. & Krasznay C. (2014). *Az elektronikus információs rendszerek biztonságának menedzselése.* Nemzeti Közszolgálati Egyetem.

Vass G., Mesics Z. & Kovács B. (2016). *Útmutató a biztonsági irányítási rendszerekkel kapcsolatban a SEVESO III. irányelv hazai bevezetésével módosuló jogszabályi előírások végrehajtásához.* Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság Országos Iparbiztonsági Főfelügyelőség Veszélyes Üzemek Főosztály.

A cikk APA szabály szerinti hivatkozása

Vásárhelyi Ö. (2024). A veszélyes üzemek információbiztonsági képességeinek fejlesztési lehetőségei napjaink kihívásainak tükrében. *Belügyi Szemle*, *72*(1), 89–111. https://doi.org/10.38146/BSZ.2024.1.6