ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

KOVÁCS ATTILA MÁTÉ

Kiberbiztonsági fenyegetések hatékony előrejelzése a kritikus infrastruktúrák védelmében

Témavezető: Prof. Dr. Rajnai Zoltán

**BIZTONSÁGTUDOMÁNYI
DOKTORI ISKOLA**

Budapest, 2025. december 16.

Nyilvános védés teljes bizottsága:

Elnök:

Prof. Em. Dr. Berek Lajos

Titkár:

Dr. Horváth Richárd

Tagok:

Dr. Lukács Judit

Dr. habil. Farkas Tibor

Dr. Magyar Sándor

Bírálók:

Dr. habil. Nagy Enikő

Dr. habil. Tóth András

Nyilvános védés időpontja: 2026.

D12) Nyilatkozat a munka önállóságáról, irodalmi források megfelelő módon történt idézéséről

NYILATKOZAT

A MUNKA ÖNÁLLÓSÁGÁRÓL, IRODALMI FORRÁSOK MEGFELELŐ MÓDON TÖRTÉNT IDÉZÉSÉRŐL

Alulírott Kovács Attila Máté kijelentem, hogy a Kiberbiztonsági fenyegetések hatékony előrejelzése a kritikus infrastruktúrák védelmében című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, a forrás megadásával egyértelműen megjelöltem.

Budapest, 2025 december 16.

Kovács Attila Máté

TARTALOMJEGYZÉK

BEVEZETÉS

A kiberbiztonság napjainkra már nem csupán informatikai szakterület, hanem a nemzetbiztonságot és a gazdaságpolitikát alapjaiban érintő stratégiai kérdés. A kritikus infrastruktúrák (energia-, víz-, közlekedési és kormányzati hálózatok) rohamos ütemű digitalizációja és egyre szorosabb összefonódása új, láncreakciószerű sérülékenységeket eredményezett. Ahogy a Verizon 2025-ös jelentése [1; 2] is rámutat, a létfontosságú rendszereket célzó incidensek, és köztük is kiemelten a zsarolóvírus-támadások száma folyamatosan emelkedik.

A fenyegetések növekvő volumenének empirikus vizsgálatához kutatásom a Maryland Cyber Events Database (MCED) [3] 2014 és 2025 októbere között dokumentált, több mint 15 000 incidenst tartalmazó idősoros adataira támaszkodik. Az elemzés során az eseményeket az MCED kódkönyve [4] által rögzített, egységes definíció szerint vizsgálom. A kritikus infrastruktúra fogalmát az EU NIS2 (2022/2555) és CER (2022/2557) irányelvek alapján határozom meg [5; 6].

A tudományos probléma megfogalmazása

A kiberbiztonság területén az egyik központi módszertani kihívás a rendelkezésre álló adatforrások heterogenitása és megbízhatósága. Az éves iparági jelentések [1; 7] (ENISA, Verizon) aggregált, keresztmetszeti adatokat közölnek, amelyek ugyan átfogó képet adnak a trendekről, de nem teszik lehetővé az incidens-szintű elemzést és a támadási mintázatok részletes feltárását.

Paradox módon éppen a legnagyobb hatású, kritikus infrastruktúrákat érő incidensekről áll rendelkezésre a legkevesebb megbízható adat. A szervezetek – reputációs kockázatok, jogi következmények vagy nemzetbiztonsági megfontolások miatt – gyakran csak a kötelező minimumot osztják meg nyilvánosan. Ez az információs aszimmetria arra kényszeríti a kutatókat, hogy proxy változókat és közvetett mérőszámokat alkalmazzanak a valós hatások becslésére.

Tovább bonyolítja a helyzetet az attribúció problémája: a támadók azonosítása technikai és politikai akadályokba ütközik. A fejlett perzisztens fenyegetések (APT) gyakran hamis zászlós (false flag) műveleteket alkalmaznak, más csoportok eszközeit és technikáit utánozzák. Ezért a kutatás nem a támadók közvetlen azonosítására, hanem viselkedési mintázataik – a használt technikák komplexitása, a célpontválasztás logikája – alapján történő kategorizálására fókuszál.

Ez a módszertani probléma vezetett el a longitudinális adatbázisok alkalmazásához, amelyek azonban – nyilvános forrásokra támaszkodva – új típusú megbízhatósági kérdéseket vetnek fel.

Adatforrás

A kutatás primer adatforrása a Maryland Cyber Events Database (MCED) [3], amely 2014 és 2025 októbere között dokumentált, manuálisan validált kiberincidenseket tartalmaz. A jelen értekezés a 2025. októberében publikált legfrissebb MCED-állományt használja, amely a GDELT NGrams 3.0 és GDELT Article List adatfolyam integrációjával bővült, javítva a lefedettséget és a nem angol nyelvű források detektálását. A strukturált adatmezők és kódolási elvek a CISSM 2025. augusztusi Codebook szerint kerültek alkalmazásra.

A címkezajt kiszűrő, többlépcsős tisztítás után a hipotézisvizsgálatokhoz használt elemzési mintát képzek. A tisztítás során kizárólag azokat az eseteket távolítom el, ahol az elkövető típusa nem meghatározható (Undetermined), majd a három fő aktortípusra (Criminal, Hacktivist, Nation-State) szűkítem a mintát (n = 14 938). A szűrés közben ellenőrzöm, hogy a fő strukturális dimenziók (iparág, eseménytípus, eseményaltípus, célország) eloszlása Jensen–Shannon divergencia alapján gyakorlatilag változatlan marad (JSD < 0,01 minden vizsgált dimenzióban). Ennek eredményeként a hipotézisvizsgálatok egy olyan adatállományra épülnek, amely egyszerre zajszűrt és a teljes MCED szerkezetét reprezentáló.

Célkitűzések

Munkám fő célkitűzése egy olyan, gépi tanuláson alapuló prediktív keretrendszer kifejlesztése és empirikus validálása, amely képes a nagymintás, valós idejű incidensadatok alapján proaktívan azonosítani és osztályozni a kritikus infrastruktúrákat érő kiberfenyegetéseket. A kutatás nem csupán leírni kívánja a fenyegetési környezetet, hanem egy a gyakorlatban is alkalmazható, döntéstámogató modellt kíván létrehozni.

A fentiekből következő cél a kibertámadások súlyosságának mérhetősége és annak megvalósíthatósága a közvetlen pénzügyi adatok korlátozott elérhetősége mellett. Ennek érdekében vezetem be a Károkozási Súlyossági Mutatót (KSM) mint közvetett mérőszámot.

A KSM az MCED event_subtype technikai kategóriáiból [4] származtatott, 1–5 közötti ordinális skála, amely kizárólag az incidensek technikai és operációs hatásának súlyosságát fejezi ki; a szektorális kritikusságot ettől elkülönítve, külön bináris változó kezeli.

A skála alsó tartománya izolált vagy rövid távú hatásokat, míg a felső tartomány tartós szolgáltatáskimaradással vagy rendszerszintű érintettséggel járó eseményeket jelöl. A cél annak statisztikai igazolása, hogy az EU NIS2/CER mentén is értelmezhető [5; 6] elosztási közműszolgáltatásokat (utilities) érő kibertámadások szignifikánsan nagyobb arányban járnak fizikai-operációs hatással (KSM = 5), mint más szektorokat célzó támadások.

A kutatás célja az is, hogy az absztrakt "támadási komplexitás" fogalmát operacionalizálja. A Komplexitási Index (KoI) egy MITRE ATT&CK®-hez illesztett, incidensszintű mutató, amely a támadások végrehajtási mintázatainak technikai összetettségét írja le, kizárólag megfigyelhető technikai jellemzők alapján. A KoI részletes komponensrendszere, skálázása és matematikai formalizálása a módszertani fejezetben, valamint az M1 mellékletben kerül bemutatásra. Célom annak vizsgálata, hogy a nemzetállami szereplők által végrehajtott támadások technikai komplexitása szignifikánsan magasabb-e a nem állami aktorok műveleteinél.

A kutatás prediktív modellje a támadási események korai fázisában rendelkezésre álló információkra épül. A végső specifikáció rétegzett (stacking) ensemble, amely lineáris szövegmodelleket és faalapú struktúramodelleket integrál; a Random Forest[8] kizárólag baseline összehasonlításként szerepel. A kutatás minden változója (Károkozási Súlyossági Mutató – KSM, Komplexitási Index – KoI, valamint a kritikus infrastruktúra indikátora) a módszertani fejezetben kerül részletes bemutatásra. A KSM az incidensek technikai–operációs hatásának súlyosságát fejezi ki. A KSM kizárólag az MCED event_subtype technikai kategóriái alapján számítódik, az iparági hovatartozástól függetlenül. A KoI kizárólag objektíven megfigyelhető technikai jellemzőkre épül, az aktortípustól függetlenül. Ez a megközelítés megelőzi a körkörös érvelést és a tanító és tesztadatok közötti információszivárgást (data leakage) a hipotézisvizsgálatok során

A kutatás fontos témája és területe a kiberbiztonsági incidensek technikai komplexitásának objektív, adatvezérelt mérhetősége. A KSM, KoI és KrI változók végleges, matematikailag formalizált definíciói az M1 mellékletben találhatók, a törzsszöveg ezek rövidített formáját használja.

A téma kutatásának hipotézisei

Első hipotézis tárgya: Az elosztási közműszolgáltatásokat érő kibertámadások technikai–operációs súlyossága.

Első hipotézis (H1): Az elosztási közműszolgáltatásokat (utilities: villamosenergia-elosztás, víz- és gázszolgáltatás) érő kibertámadások szignifikánsan nagyobb arányban járnak fizikai-operációs hatással (KSM = 5), mint más szektorokat célzó támadások.

A hipotézisben használt „utilities” kategória az MCED iparági taxonómiáját követi, és az elosztási jellegű közműszolgáltatásokat foglalja magában; nem azonos a tágabb értelemben vett energiatermelési (energy) szektorral. A H1 hipotézisben alkalmazott „utilities" operacionalizáció tudatos módszertani döntés eredménye. A „kritikus infrastruktúra" fogalma jogszabályi keretrendszerenként eltérő, ezen definíciók egyike sem illeszthető közvetlenül az MCED adatbázis NAICS-alapú iparági taxonómiájára, így bármely „kritikus infrastruktúra" flag (KrI) létrehozása önkényes kategorizálási döntéseket igényelne.

Ezzel szemben az MCED „Utilities" iparági kategóriája – amely a villamosenergia-elosztást, víz- és gázszolgáltatást foglalja magában – egyértelműen definiált, reprodukálható és minden főbb keretrendszerben a legmagasabb kritikussági szinten szerepel. A szűkebb, de egzakt operacionalizáció így erősebb belső érvényességet biztosít a hipotézisvizsgálatnak.

Második hipotézis tárgya: A kibertámadások technikai komplexitása és az aktorok típusa közötti kapcsolat.

Második hipotézis (H2): Az állami hátterű támadók (nation-state aktorok) által végrehajtott kibertámadások technikai komplexitása szignifikánsan magasabb, mint a nem állami hátterű aktorok által végrehajtott támadásoké.

Harmadik hipotézis tárgya: A kibertámadások aktortípusának előrejelezhetősége az incidensek korai fázisában rendelkezésre álló információk alapján.

Harmadik hipotézis (H3a): A gépi tanulási modellek szignifikánsan jobb teljesítményt érnek el a támadói attribúció feladatában – a három fő aktortípus (Criminal, Hacktivist, Nation-State) predikciójában – mint a szabály-alapú heurisztikus megközelítések.

Harmadik hipotézis (H3b): A további komplexitásnövelés (lineáris ML → ensemble) nem eredményez szignifikáns javulást (Δ Macro-F1 < 0,01), így a parsimónia elve (lex parsimoniae) alapján az egyszerűbb modell preferálandó.

A hipotézisek a témában végzett korábbi kutatások során azonosított módszertani kihívásokra reflektálnak. A H1 hipotézisben alkalmazott KSM proxy változó bevezetését az indokolta, hogy a valós gazdasági károk publikus adatainak hiánya miatt szükségessé vált egy objektív, technikai hatáson alapuló mérőszám kidolgozása [9]. A H2 hipotézis hátterében a

rendszerszintű komplexitás mérésének igénye áll [10], amelyre válaszul került kidolgozásra a KoI, lehetővé téve a támadások összetettségének kvantitatív elemzését. A H3 hipotézis módszertani megközelítése a kiberbiztonsági adatok inherens kiegyensúlyozatlanságára reagál [11], ahol a súlyos incidensek ritkasága miatt a hagyományos accuracy metrikák helyett a PR-AUC alapú értékelés és a fejlett ensemble technikák alkalmazása vált szükségessé [12].

Kutatási módszerek összefoglalása

H1. Értelmezés és tesztelés: Az adatok forrása a Center for International and Security Studies at Maryland (CISSM) Maryland Cyber Events Database (MCED), amely több mint 15 000 kiberincidenst tartalmaz (2014–2025). A H1 hipotézis tesztelése során az MCED iparági kategóriái közül az elosztási közműszolgáltatásokat (utilities) bináris indikátorként különítem el (utilities = 1, egyéb szektorok = 0). A H1 bináris kimenetre épül: fizikai-operációs hatással járó incidens = 1, ha KSM = 5, különben 0. A csoportok közti különbséget aránytesztt el (χ^2 / Fisher) és logisztikus regresszióval vizsgálom, év-dummy kontrollal (érzékenység: iparág-rétegzés, undetermined kezelés az M2 melléklet szerint).

H2. Értelmezés és tesztelés: A hipotézis azt vizsgálja, hogy a különböző motivációjú és erőforrásokkal rendelkező támadók eltérő szintű technikai kifinomultságot mutatnak-e. A nemzetállami aktorok jellemzően jelentős anyagi és humán erőforrásokkal, valamint hosszú távú stratégiai célokkal rendelkeznek, ami lehetővé teszi számukra összetettebb, többlépcsős támadások kivitelezését. Ezzel szemben a bűnözői csoportok elsősorban gyors anyagi haszonszerzésre törekszenek, míg a hacktivisták ideológiai célokat követnek, gyakran korlátozottabb technikai kapacitással. Az energetikai szektorban ez a különbség azért lehet markánsabb, mert az ipari vezérlőrendszerek (ICS/SCADA) manipulálása speciális szakértelmet igényel, amellyel jellemzően csak a jól finanszírozott, állami hátterű csoportok rendelkeznek. A Komplexitási Index (KoI) a támadások végrehajtási mintázatainak technikai összetettségét írja le, négy, binárisan (0/1) értelmezett technikai komponens jelenléte alapján; a komponensek és a skálázás részletes definícióját a módszertani fejezet és az M1 melléklet tartalmazza. A Károkozási Súlyossági Mutató (KSM) pedig az MCED event_subtype kategóriáira épülő skála, amely a tényleges technikai és operációs hatást méri.

H3. Értelmezés és tesztelés: Ez a hipotézis a 2. hipotézisben feltárt mintázatok gyakorlati hasznosíthatóságát vizsgálja. A cél annak bizonyítása, hogy a különböző aktortípusok közötti eltérések nemcsak utólag elemezhetők, hanem egy prediktív modell segítségével proaktívan is azonosíthatók, ami lehetővé teszi az incidensek automatizált rangsorolását.

A vizsgálat során egy többdimenziós, úgynevezett mixed-methods megközelítést alkalmazok, amely a kvantitatív adatelemzést (statisztikai vizsgálatok, gépi tanulási módszerek) és a kvalitatív elemzést (esettanulmányok) egyaránt integrálja. Ez a megközelítés lehetővé teszi a kiberfenyegetések trendjeinek feltárását, a támadások technikai jellegének és működési hatásainak értékelését, valamint a kvantitatív adatok – például a károkozás és a védekezés költségei – kontextusba ágyazott értelmezését [13]. Az alkalmazott módszertan egyúttal hozzájárul az energetikai szektort érintő incidensekkel szembeni sérülékenységek, ellenállóképességi jellemzők és lehetséges fejlesztési irányok azonosításához.

A kiberbiztonsági incidensek valós pénzügyi hatásai ritkán publikusak. Ezt a közvetett költségekhez kapcsolódó változók – konzisztens, reprodukálható proxy-változók (KSM, KoI) bevezetésével hidalom át, amelyek az incidensek technikai hatásán alapulnak. Anderson kimutatta [14], hogy az olyan infrastruktúrák, mint a botnetek, jelentős gazdasági terheket rónak az ágazatra, nemcsak közvetlen bevételeik, hanem a védekezési költségek miatt is, amelyek gyakran nagyságrendekkel haladják meg a támadók hasznát. Ez az összefüggés különösen releváns az energetikai szektor esetében, ahol a védekezési költségek és az indirekt hatások, például az ellátási lánc megszakadása, komoly gazdasági következményekkel járhatnak.

Ábra 1- A kutatás keretrendszere (Hipotézisek és elemzési módszerek kapcsolata)

A kvantitatív analízis sarokköve a két fenti, a kutatás keretében kidolgozott új, kompozit mutató. A támadások technikai kifinomultságának mérésére egy MITRE ATT&CK®-hez illesztett Komplexitási Indexet (KoI) vezetek be, míg az incidensek valós hatását a Károkozási Súlyossági Mutató (KSM) számszerűsíti. Ez a két, egymást kiegészítő index együttesen teszi lehetővé a kiberbiztonsági események többdimenziós, adatvezérelt elemzését, választ adva a támadás módjára (a "hogyan"-ra) és annak tényleges következményeire (a "mekkora kárt okozott"-ra) is. A kutatás egy algoritmizált, reprodukálható lépéssorozatot követ.

Adatgyűjtés: Az értekezés adatbázisa a Maryland Cyber Events Database (MCED, 2014–2025), amely 2025-től a GDELT Web News NGrams 3.0 adatait is integrálja [3] (University of Maryland – CISSM).

A fogalmakat és meződefiníciókat a CISSM kódkönyv [4] rögzíti; a klasszifikációs elvek összefoglalását a Harry és Gallagher cikke [15] adja. Az iparági kategorizálás az MCED NAICS mezőjén és az EU NIS2/CER kritikus szektorlistáin alapul.

Adatfeldolgozás és modellezés: Az összegyűjtött adatokon kvantitatív és kvalitatív elemzést végzek. A kvantitatív vizsgálat magában foglalja a leíró statisztikai elemzéseket és a gépi tanulási modellek (ML) építését, míg a kvalitatív rész az egyes esettanulmányok mélyebb vizsgálatára koncentrál. Az elemzés során olyan modern eszközöket alkalmazok, mint a természetes nyelvi feldolgozás (NLP) [16] és a Random Forest algoritmus [8].

A prediktív modellezéshez egy stacking ensemble architektúrát alkalmazok, amelyet a részletes módszertani fejezetben ismertetek.

További módszertani dimenzióként, a kutatás során tudatosan kezelem az adatok elérhetőségével és megbízhatóságával kapcsolatos kihívásokat, beleértve a nyilvános forrásokra [17] épülő incidens-adatbázisokból fakadó attribúciós bizonytalanságokat is. Ezt a források kritikai értékelésével és a módszertan következetes alkalmazásával biztosítom, a modellek teljesítményét pedig az osztály-egyensúlytalanságra érzékeny metrikák (pl. Precision–Recall görbék) segítségével értékelem.

Etikai kérdések: A kutatás során követtem az MTA Tudományetikai Kódexének [18] iránymutatásait az ICT kutatások etikai normáiról, amely explicit módon tiltja a nem nyilvános vagy illegális forrásokból származó adatok kutatási célú felhasználását. Ezért transzparenciát érintő, biztonsági és etikai megfontolások miatt az MCED vagy hasonló nyilvános adatbázisokon kívül a kutatás kizárólag nyilvános, validált adatbázisokra épült; nem történt nem transzparens vagy dark-web alapú adatgyűjtés.

A dolgozat központi mutatói (KSM, KoI, KrI) és a H1–H3 hipotézisek tesztelése kizárólag az MCED incidensszintű adataira és a NIS2/CER szerinti szektorbontásra épül; a további iparági riportok (Verizon DBIR, ENISA, IBM X-Force, Mandiant, CrowdStrike, VERIS, CISA KEV, MITRE ATT&CK) csupán kiegészítő, elsősorban kvalitatív kontextust és nagyságrendi realitás-tesztet adnak

A bevezető fejezet bemutatta a vizsgált problémakör relevanciáját az energetikai szektorban, felvázolta a legfontosabb elméleti kereteket, és megfogalmazta azt a három központi hipotézist, amelyek a vizsgálat gerincét alkotják. Áttekintettem a kutatás többdimenziós módszertani megközelítésének stratégiai vázlatát, előrevetítve a kvantitatív és kvalitatív elemzések szintézisét.

A dolgozat a továbbiakban a fentebb említett alapokra építkezik, és a következő logikai szerkezetet követi:

Az 1. fejezet a kutatás szakirodalmi és elméleti kontextusát teremti meg, feldolgozva a releváns tudományos irodalmat és a kapcsolódó elméleti keretrendszereket. A 2. fejezet a kvalitatív elemzésekre fókuszál. Részletes esettanulmányokon keresztül mutatja be a vizsgált jelenségeket, és egy, az információbiztonsági rendszerekhez kapcsolódó kitekintést ad, megalapozva ezzel a kvantitatív vizsgálatok kontextusát.

A 3. fejezet képezi a dolgozat kvantitatív magját, amely tartalmazza a részletes módszertant, magát az elemzést, valamint az eredményeket. A fejezet első felében bemutatásra kerül a metrikák (KoI, KSM) levezetése és a hipotézisek tesztelésének technikai terve, beleértve a prediktív modell felépítését. A fejezet második felében az említett módszertan alkalmazásával kapott konkrét eredményeket ismertetem: a statisztikai tesztek kimeneteit és a gépi tanulási modell teljesítményének számszerűsített adatait. A dolgozatban a Criticality Indicator rövidítése következetesen KrI. A konfidencia-intervallum mindenütt teljes formában, ‘95%-os konfidencia-intervallum’ alakban szerepel.

Végül a záró fejezet az eredmények értelmezését, a következtetések levonását és a javaslatok megfogalmazását tartalmazza. Ebben a fejezetben helyezem tágabb kontextusba a 3. fejezetben bemutatott nyers eredményeket, és itt fejtem ki a kutatás tudományos és gyakorlati jelentőségét, valamint megfogalmazom a lehetséges jövőbeli kutatási irányokat is.

A célom nem csupán a tudományos vizsgálat lefolytatása, hanem annak biztosítása is, hogy a dolgozat eredményei hozzájáruljanak a kritikus infrastruktúrák kibervédelméhez kapcsolódó elméleti ismeretek bővítéséhez, valamint, hogy gyakorlati ajánlások kidolgozásával támogassam munkájukban a szakpolitikai döntéshozókat és kibervédelmi szakembereket.

Ebben a bevezető fejezetben bemutattam a kiberbiztonság kritikus infrastruktúrák védelmében betöltött tudományos és gyakorlati jelentőségét, valamint körülhatároltam azokat a módszertani kihívásokat, amelyek a súlyos kiberincidensek empirikus vizsgálatát jellemzik. Felvázoltam a

kutatás három fő hipotézisét, amelyek a technikai–operációs hatások mérhetőségétől a támadások komplexitásán át a prediktív modellek alkalmazhatóságáig terjednek. A többdimenziós módszertani megközelítés – amely ötvözi a kvantitatív adatelemzést és a kvalitatív esettanulmányokat – lehetővé teszi a kiberfenyegetések strukturált, incidensszintű vizsgálatát. A következő fejezetben azokat az elméleti és szakirodalmi kereteket tekintem át, amelyekre a bemutatott hipotézisek és mérőszámok módszertani megalapozása épül.

1. IRODALMI ÉS ELMÉLETI ÁTTEKINTÉS

1.1. A kiberhadviselés és a digitális sebezhetőség

A kritikus infrastruktúrák kiberbiztonsági kihívásainak átfogó vizsgálata előtt elengedhetetlen, hogy ismertessem a témának az értekezés szempontjából legrelevánsabb elméleti és fogalmi kereteit. A kiberhadviselés szakirodalma az elmúlt két évtizedben jelentős átalakuláson ment keresztül, amely során a kezdeti, elsősorban technikai megközelítésektől eljutott a komplex, multidiszciplináris elemzési keretekig. Libicki úttörő munkája nyomán a kiberhadviselés koncepciója túllépett a puszta technológiai dimenzión [19], és magába foglalta a stratégiai, politikai és társadalmi aspektusokat is [26]. Ez a változás különösen releváns a kritikus infrastruktúrák védelmének kontextusában, ahol a technikai sebezhetőségek csupán egy részét képezik a teljes fenyegetettségi képnek.

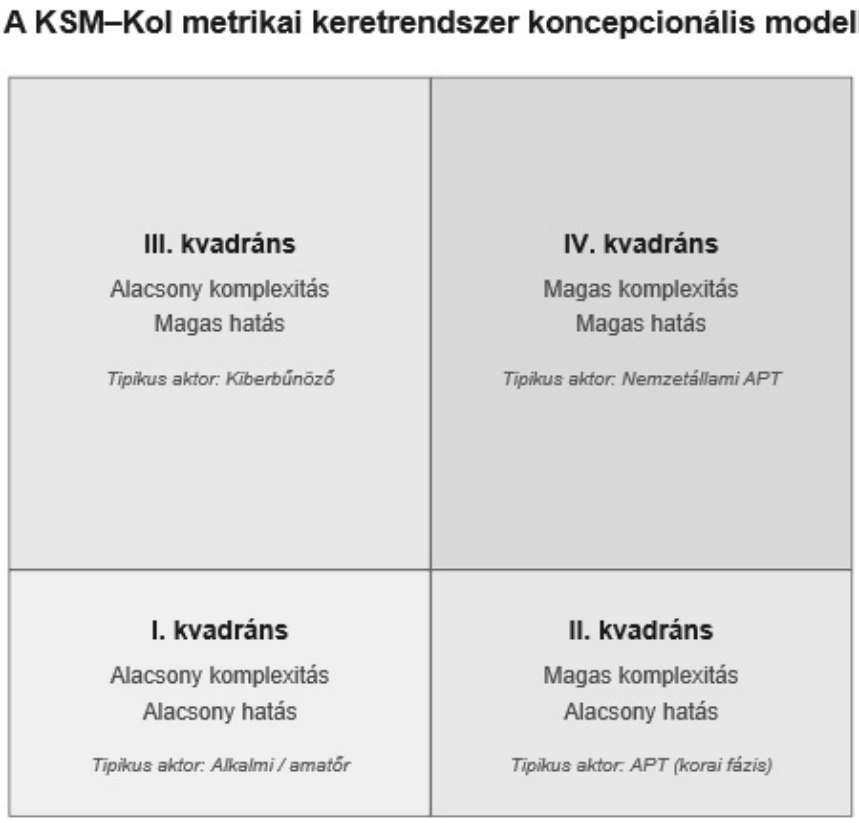
Jelen fejezet a szakirodalom szintézisére törekszik egy logikai ív mentén: először bemutatja a kiberhadviselés és a digitális sebezhetőség fogalmi evolúcióját a klasszikus elméletektől napjainkig. Ezt követően az aszimmetrikus és hibrid hadviselés kontextusába helyezi a kiberfenyegetéseket, különös tekintettel azok gazdasági és geopolitikai dimenzióira. Végül, a fejezet áttekinti a releváns védelmi keretrendszereket, ezzel megalapozva a disszertáció központi kutatási résének azonosítását.

A digitális sebezhetőség fogalmának értelmezése szintén jelentős fejlődésen ment keresztül. Míg a korai szakirodalom elsősorban a szoftverhibákra és konfigurációs problémákra fókuszált, az újabb megközelítések holisztikusabb perspektívát alkalmaznak. Rid megkérdőjelezte a "kiberháború" koncepciójának érvényességét[20], rámutatva, hogy a legtöbb kibertámadás nem felel meg a háború klasszikus clausewitzi definíciójának. Ez a kritikai megközelítés rávilágított arra, hogy a kiberfenyegetések természetének megértéséhez új fogalmi keretre van szükség, amely képes megragadni az aszimmetrikus konfliktusok és a hibrid hadviselés sajátosságait. Ennek megfelelően a jelen fejezet célja, hogy szintetizálja ezeket a különböző elméleti perspektívákat, és megalapozza a későbbi empirikus vizsgálatok fogalmi kereteit.

Az itt felvázolt fogalmi keret közvetlenül megalapozza a disszertáció első hipotéziskörét. A kritikus és nem kritikus szektorok összevetését a Károkozási Súlyossági Mutatóval (KSM) végzem, amelyet a Maryland Cyber Events Database egységes taxonómiájára (event_type, event_subtype) építek; a kategóriák definícióit a CISSM kódolási útmutató rögzíti. A KSM a ritkán publikált közvetlen pénzügyi veszteségadatok helyett közvetett súlyossági mérőszámként szolgál: az MCED event_subtype egységes technikai kategóriái alapján,

szektorfüggetlen módon a technikai és operációs következmények súlyosságát fejezi ki; a skála és a kategória–pontszám megfeleltetés részleteit a módszertani fejezet rögzíti [14]. E keretre épül H1 első hipotézis is.

Rajnai és Kovács [10] a kiber-fizikai rendszerek rétegei közötti kölcsönhatásokat gráfstruktúrák segítségével írják le, és kimutatják, hogy a sebezhetőségek hálózati topológiája skálafüggetlen mintázatokat mutat. Ez a formalizálás lehetővé teszi annak számszerűsítését, hogy egy komponens kompromittálása milyen kaszkádhatásokat válthat ki a teljes infrastruktúrában. A modellezési keret közvetlen előképe a dolgozatban bevezetett kvantitatív metrikáknak (KSM, KoI). A közvetlen pénzügyi veszteségek publikált adatainak szűkössége miatt - amit Anderson és társai [14] már 2013-ban is dokumentáltak a kiberbűnözés gazdasági hatásainak mérésekor - dolgozatomban bevezetek egy Károkozási Súlyossági Mutatót (KSM). A KSM az MCED event_subtype egységes technikai kategóriái alapján, kizárólag az incidensek technikai és operációs hatását számszerűsíti.



Ábra 2- A KSM–KoI metrikai keretrendszer koncepcionális modellje

Az ábra szürkeárnyalatos megjelenítése tudatos, publikációs követelményekhez igazított formai döntés; a kvadránsok értelmezése (alacsony/magas hatás × alacsony/magas komplexitás) konzisztens a metrikai definíciókkal és a hipotézisek logikájával. Az ábra a Károkozási

Súlyossági Mutató (KSM) és a Komplexitási Index (KoI) által meghatározott két-dimenziós metrikai keretrendszert szemlélteti. A függőleges tengelyen a KSM szerepel, amely az incidensek technikai és operációs hatásának relatív súlyosságát fejezi ki, míg a vízszintes tengely a támadások technikai komplexitását mérő KoI-t ábrázolja. A vízszintes elválasztó vonal a súlyos incidensek elméleti küszöbértékét, a függőleges elválasztó pedig a magas technikai komplexitás határát jelöli.

Kovács és Rajnai [21] a pilóta nélküli légi járművek sebezhetőségeinek vizsgálatával rámutattak arra, hogy az új technológiák kritikus infrastruktúrákba történő integrációja egyedi kockázati profilt teremt. A dolgozatban a technikai szofisztikáltság mérésére olyan binárisan értelmezhető technikai jellemzők szolgálnak, mint a laterális mozgás, a perzisztencia, a többfázisú végrehajtás és a detektálás elkerülése. Ez közvetlen előképe annak a szemléletnek, amelyet a disszertáció a KSM és KoI mutatók segítségével terjeszt ki. A támadások egységes keretrendszerbe szervezését a MITRE ATT&CK [18] fogalmi kerete inspirálja [15]; a Komplexitási Index (KoI) számszerűsítése kizárólag MCED-mezők és leírások alapján történik.

A gépi tanulási modellek értékelése során különösen fontos, hogy a választott mérőszámok tükrözzék az adott probléma sajátosságait. A kiberincidensek aktorának előrejelzésében gyakori az osztály-egyensúlytalanság: egyes aktorkategóriák (pl. nemzetállami) jóval ritkábban fordulnak elő, mint mások. Ilyen környezetben az accuracy mutató félrevezető lehet, mert a modell a többségi osztály következetes predikciójával is magas pontosságot érhet el [22] [12]. A szakirodalomban ezért hangsúlyos szerepet kapnak a Precision (pozitív prediktív érték) és a Recall (érzékenység) mutatók, valamint ezek kombinációja, az F1-score.

A mérőszámok közötti különbségek irodalmi megalapozását Davis és Goadrich [12] elemzése adja; a részletes összehasonlítást és a választott mutatók technikai indoklását a módszertani fejezet tartalmazza [12].

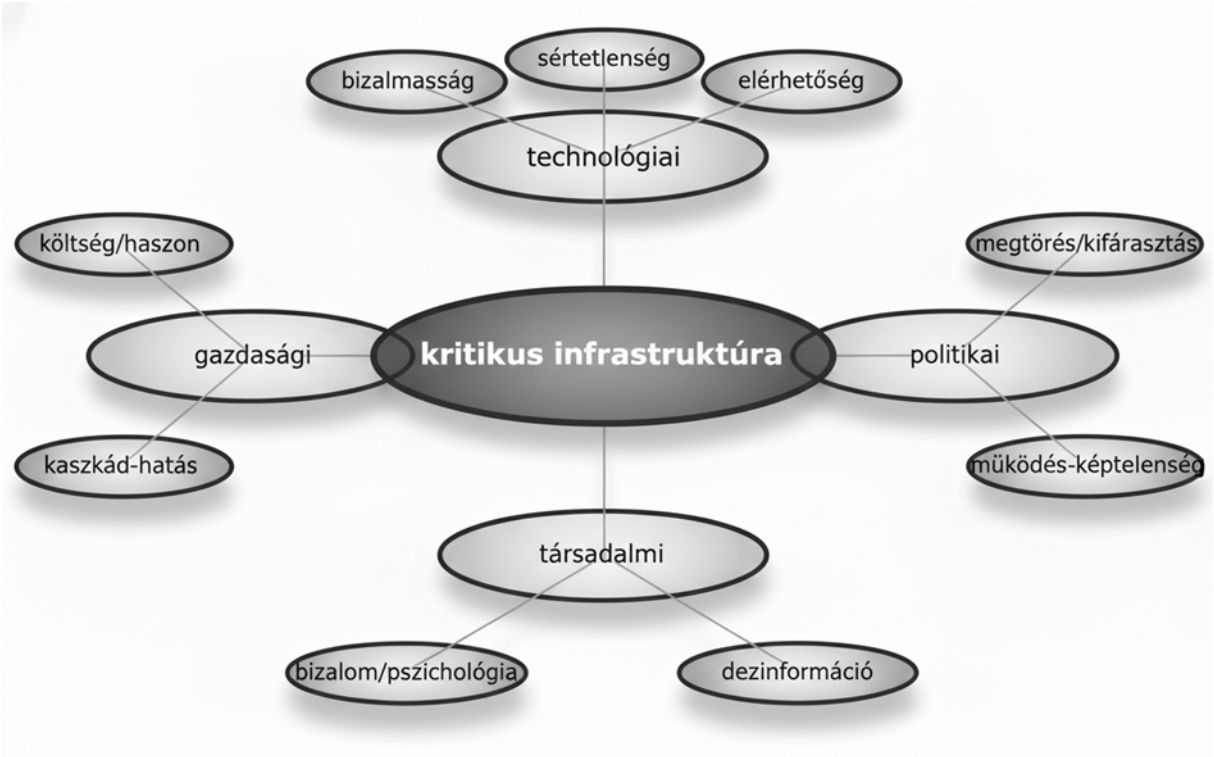
Ezek az eredmények megalapozzák, hogy az értekezésben bemutatott prediktív modellek értékelésénél a ROC-görbék mellett a Precision–Recall görbéket és a PR-AUC mutatót is alkalmazzak. Így nemcsak a modell általános teljesítményét, hanem a ritka, de kritikus támadások detektálási képességét is pontosabban vizsgálhattam.

Kovács [9] a kiberfenyegetések és védekezési mechanizmusok párhuzamos evolúcióját idősoros és klaszterezési módszerekkel vizsgálta. A tanulmány kimutatta, hogy az aktorok technikai komplexitása és a célzott szektorok közötti mintázatok kvantitatívan megragadhatók.

Ez a felismerés szolgált alapul a jelen értekezésben bemutatott ensemble prediktív modell hipotéziseinek megfogalmazásához, amely már nemcsak leírja, hanem előre is jelzi a különböző támadási típusokat[11].

Az értekezésben megjelenő fogalom - a kiberbiztonsági esemény - olyan esemény, amely veszélyezteti az információs rendszer integritását, bizalmasságát vagy rendelkezésre állását, illetve a rendszer által feldolgozott, tárolt vagy továbbított információkat. Erre példa: Jogosulatlan hozzáférés, adatsértések, ransomware támadások, szolgáltatásmegtagadási támadások [23].

A kiberfenyegetések evolúciójának és a védekezési mechanizmusok fejlődésének párhuzamos vizsgálata során azonosítottam azokat a trendeket és mintázatokat, amelyek a későbbi prediktív modellek alapját képezték[24]. Ez a munka különösen fontos volt abban, hogy megalapozza a disszertáció azon hipotézisét, miszerint a különböző aktorok eltérő komplexitású támadási technikákat alkalmaznak.



Ábra 3- A kiberhadviselés dimenziói és a digitális sebezhetőség kapcsolata

A dolgozat és hipotézisek szempontából legfontosabb dimenziója maga a kritikus infrastruktúra köré rendezett négy dimenzió (technológiai, politikai, gazdasági, társadalmi) és kapcsolatait szemléltetése.

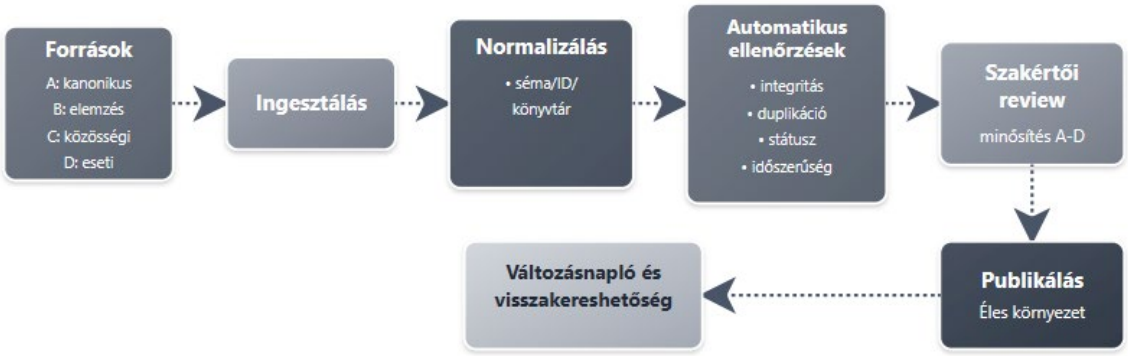
A szakirodalom áttekintése során három fő tematikus csomópont köré szervezem az elemzést: először a kiberhadviselés és kiberbiztonság alapfogalmait tisztázom, különös tekintettel azok evolúciójára; másodszor az ipari vezérlőrendszerek (ICS/SCADA) és az Ipar 4.0 technológiák sebezhetőségeit vizsgálom; harmadszor pedig a nemzetközi keretrendszerek és védelmi stratégiák hatékonyságát értékelem. Az alkalmazott elemzési keret lehetővé teszi, hogy a kockázati tényezőket elkülönítve vizsgáljam, és pontosabban értékeljem azok hatását a támadások súlyosságára.

Forráskutatás és -validáció

A dolgozat forráskezelése három elvre épül: megbízhatóság, reprodukálhatóság és átláthatóság. Ennek megfelelően minden beérkező információ először normalizáláson és technikai ellenőrzéseken megy át (séma- és konzisztencia-vizsgálat, formátum-ellenőrzés), majd tartalmi értékelést kap (eredet, szerző, módszertan), végül forrás-szinteket rendelek hozzá. A források A–D minősítést kapnak: A = kanonikus/elsődleges adatkészlet vagy hivatalos specifikáció; B = szakmailag ellenőrzött, módszertant ismertető elemzés; C = közösségi/nyílt forrású implementáció vagy teszt; D = eseti, anekdotikus állítás. A szint nem végérvényes: frissítés, visszavonás vagy ellentmondás esetén újraminősítés.

Elsődleges és kanonikus adatkészletek (keretrendszer-leírások, hivatalos objektumkatalógusok, platform-szintű dokumentumok) adják a fogalmi gerincet: itt rögzítjük a taktikák/technikák azonosítóit, definícióit és életciklusát. Ezeknél technikai validációt végzek (fájlintegritás-ellenőrzés, séma-validáció, azonosító-egyediség, dátum- és verziómezők érvényessége, „deprecated/revoked” státuszok kezelése), majd változás-diffet készítek (mi új, mi módosult, mi lett visszavonva). A fogyaszthatóság érdekében verzió-pinnelést alkalmazunk (kiadás/commit rögzítése), hogy minden eredmény visszakereshető legyen.

Másodlagos, iparági elemzések és incidensleírások hozzák a kontekstuális bizonyítékot (esettanulmányok, TTP-példák, megfigyelt minták). Ezeket triangulációval validáljuk: különböző szereplők hasonló megállapításait egyeztetjük, az időbélyegeket és az artefaktumokat (mint hash, parancsszintaxis, log-részlet) egymáshoz illesztjük, és explicit megkülönböztetjük a hipotézist a ténytől. Egyetlen, önmagában álló állítás legfeljebb C–D minősítést kap, amíg független megerősítést nem nyer.



Ábra 4-Forrásvalidációs folyamat

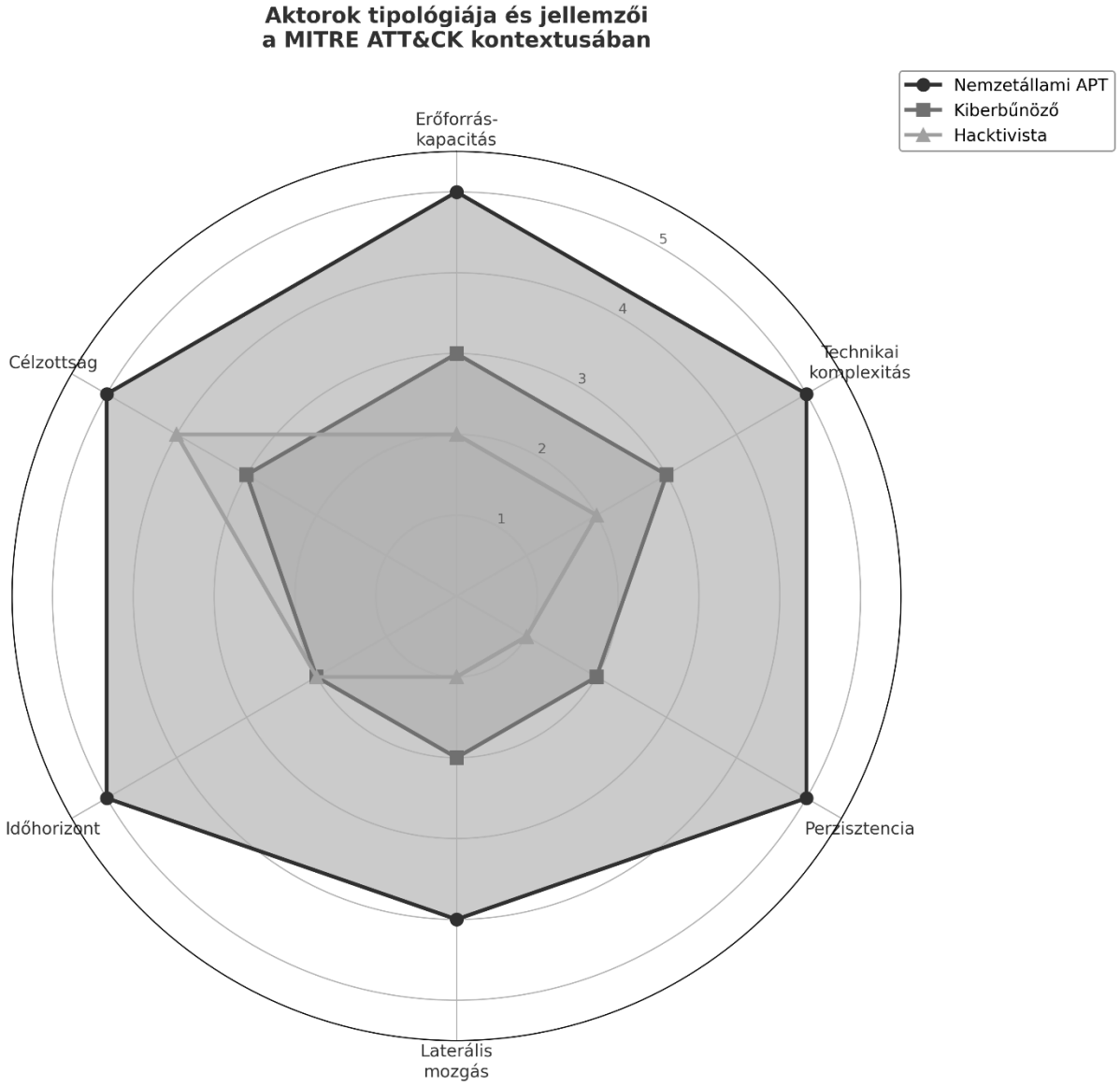
Közösségi/nyílt forrású erőforrások (észlelési szabályok, playbookok, tesztkészletek) a gyakorlati lefedettséget és a tesztelhetőséget növelik. Itt a validáció a karbantartók reputációjára, a commit-történetre, a licenc-és verziófegyelemre, valamint a reprodukálhatósági próbákra támaszkodik (konténeres futtatás, izolált laborkörnyezet, „expected/actual" kimenet). A környezetfüggő szabályokat külön jelöljük, és csak olyan pontszámítással használjuk, amely tolerálja a platform-varianciát.

A fenti rétegeket belső minőségbiztosítási folyamat fogja össze: (1) begyűjtés → (2) normalizálás/összerendelés (azonosítók, taksonómiák, szinonimák) → (3) automatikus ellenőrzések (duplikáció, hivatkozás-törés, időrend) → (4) szakértői szemrevételezés és minősítés → (5) publikálás és változásnapló. A kockázatokat (elavulás, téves általánosítás, környezetfüggő anomáliák) „fogalmi bizonytalanság" és „adatminőségi" címkékkel nyomon követjük; csak olyan következtetés kerül a fő eredmények közé, amely A–B forrásra támaszkodik, C–D forrással legfeljebb illusztrál.

Kiberhadviselés és kiberbiztonság

A kiberhadviselés magában foglalja az állami és nem állami szereplők által végrehajtott szisztematikus támadásokat, amelyek célja az információs rendszerek megbénítása, adatok megszerzése vagy a szolgáltatások megszakítása. Az ilyen támadások jelentős kockázatot jelentenek a kritikus infrastruktúrák, például az energiaellátó rendszerek, vízellátó hálózatok, közlekedési rendszerek és pénzügyi szolgáltatások számára [25]. A kiberhadviselés mellett a kiberbűnözés és a kiberterrorizmus is egyre jelentősebb fenyegetést jelent a modern társadalmakra [26]. A kiberbűnözés főként anyagi haszonszerzésre irányul, míg a

kiberterrorizmus politikai vagy vallási célokat szolgál, gyakran félelemkeltés révén [14]. Ezek a fenyegetések különösen veszélyesek, mivel a támadók fejlett, perzisztens fenyegetési (APT) csoportokhoz tartoznak, amelyek kifinomult technikákat alkalmaznak a rendszerek behatolására és a működés megszakítására.



Ábra 5 - Aktorok tipológiája és jellemzői

A radar diagram hat dimenzió mentén hasonlítja össze a három fő aktortípust, amelyek a H2 hipotézis vizsgálatának elméleti alapját képezik. A dimenziók kiválasztása a MITRE ATT&CK keretrendszer taktikai kategóriáira és a szakirodalmi konszenzusra épül.

A nemzetállami APT-csoportok minden dimenzióban kiemelkedő értékeket mutatnak. Libicki [19] és Rid [27] egyaránt hangsúlyozza, hogy az állami szereplők stratégiai előnye a gyakorlatilag korlátlan erőforrás-allokációban és a hosszú távú tervezési horizontban rejlik. A

Mandiant APT1 jelentés [28] dokumentálta, hogy egyes kínai APT-csoportok átlagosan 356 napig maradtak észrevétlenül a kompromittált hálózatokban, ami a perzisztencia és laterális mozgás magas értékeit magyarázza. A Google/Mandiant ukrán konfliktusról szóló elemzése [29] megerősíti, hogy a nemzetállami műveletek jellemzően többfázisú, koordinált kampányok formájában valósulnak meg.

A kiberbűnözői csoportok közepes értékeket mutatnak a legtöbb dimenzióban. A Verizon DBIR [1] éves elemzései szerint a pénzügyi motivációjú szereplők jellemzően opportunista célpontválasztást és commodity malware-t alkalmaznak, bár egy CrowdStrike jelentés [30] rámutat a „big game hunting" trend erősödésére, ahol célzottabb támadásokkal nagyobb váltságdíjakat követelnek. Az időhorizont és perzisztencia alacsonyabb értékei a „smash and grab" megközelítést tükrözik – a cél a gyors monetizáció, nem a hosszú távú jelenlét.

A hacktivisták paradox mintázatot mutatnak: magas célzottsággal, de alacsony technikai komplexitással. Az ENISA Threat Landscape [7]szerint a hacktivista csoportok jellemzően DDoS támadásokat és weboldal-defacement akciókat hajtanak végre, amelyek ideológiailag erősen célzottak, de technikailag egyszerűek. A perzisztencia és laterális mozgás gyakorlatilag hiányzik, mivel az akciók egyszeri, demonstratív jellegűek.

A diagram vizuálisan alátámasztja a H2 hipotézis elméleti alapját: a nemzetállami szereplők szisztematikusan magasabb komplexitású támadásokat (KoI ≥ 2) hajtanak végre, amit a KoI mutató segítségével empirikusan is tesztelek. A küszöb KoI ≥ 2, mivel ez jelzi legalább két, egymást erősítő technikai komponens együttes jelenlétét.

Az incidensek hatásainak vizsgálatakor szem előtt kell tartani, hogy a kritikus infrastruktúrákra épül a modern társadalmak működése; az ezeket a rendszereket ért támadás hatásai jóval túlmutathatnak egy a támadást elszenvedő konkrét létesítmény keretein. Ide tartoznak az energiaellátás, a közlekedési rendszerek, a vízellátás, a pénzügyi szolgáltatások, az egészségügyi intézménye[31], valamint kormányzati szolgáltatások) elleni támadások különösen nagy súllyal bírnak, mivel társadalmi szinten okozhatnak fennakadásokat.

A nemzetállami hátterű APT-csoportok feltételezhetően többlépcsős támadási láncokat alkalmaznak, miáltal a hipotézis szerint minőségileg különböznek a kevésbé szervezett szereplők módszereitől. A feltételezett különbség objektív mérésére a kutatás egy, a MITRE ATT&CK keretrendszerre épülő kompozit mutatót vezet be, a komplexitási indexet (KoI). A KoI 0–4 skálán számszerűsíti a technikai szofisztikáltságot: a többfázisú végrehajtás, laterális mozgás, perzisztencia és detektálás elkerülése négy bináris (0/1) komponensének összegeként

értelmezhető. A H2 hipotézis a támadói aktortípus és a technikai komplexitás közötti összefüggést vizsgálja, kizárólag a KoI komponensei alapján, az érintett célrendszer vagy szektor típusának figyelembevétele nélkül. [21].

Ipari vezérlőrendszerek (ICS/SCADA) és az Ipar 4.0 technológiák

Az Ipar 4.0 keretében fejlődő technológiák, mint az ipari internet dolgok (IIoT) és a kiber-fizikai rendszerek (CPS), létfontosságú elemei a kritikus infrastruktúráknak. Ezek a technológiák lehetővé teszik a gépek, rendszerek és eszközök intelligens hálózatba kapcsolását, ami növeli a termelékenységet és hatékonyságot. Azonban ezek a rendszerek újfajta, kiberbiztonsági kihívást jelentő sebezhetőségeket is hordoznak magukban.

Zhou és társai [32] rámutatnak, hogy az IIoT és a CPS rendszerek különösen kiszolgáltatottak a kibertámadásoknak, és a bennük rejlő sebezhetőségek könnyen kihasználhatók. E rendszerek kulcsszerepet töltenek be a modern ipari folyamatokban, ezért a sérülékenységeikből fakadó incidensek súlyos következményekkel járhatnak mind az ipar, mind a társadalom számára. Ezeknek a sebezhetőségeknek a kihasználása adott esetben széles körűen pusztító hatást is eredményezhet, amely rámutat a szigorú védelmi intézkedések, a transzparens biztonsági protokollok és a megerősített infrastruktúra kiemelt jelentőségére a kiberbiztonsági védekezésben.

Több szerző is kiemeli, hogy az IIoT és CPS rendszerek biztonsági kihívásai többek között a következő tényezőkre vezethetők vissza:

Komplexitás: Az ipari rendszerek összetettsége megnehezíti a biztonsági rések azonosítását és orvoslását [33].

Konnektivitás: A növekvő hálózati kapcsolatok száma növeli a támadási felületet, amit a kiberbűnözők kihasználhatnak [32].

Adatbiztonság: Az érzékeny ipari adatok védelme kritikus fontosságú, de a biztonsági mechanizmusok gyakran elmaradnak az adatok kezelésének bonyolultsága miatt [34; 35].

A kritikus infrastruktúrák ipari vezérlőrendszerei (ICS) folyamatos támadás alatt állnak a fejlett tartós fenyegetések (APT) részéről. Az APT-k kifinomult, hosszan tartó támadások, amelyeket gyakran állami támogatással vagy jól szervezett csoportok hajtanak végre. Ezek a támadások célzottak, hosszú távon működnek, és gyakran a legkritikusabb rendszereket veszik célba.

A kritikus infrastruktúrák ICS rendszerei különösen vonzó célpontok az APT csoportok számára, mivel ezek a rendszerek irányítják az energiaellátást, vízellátást, közlekedést és egyéb létfontosságú szolgáltatásokat. Az ICS/SCADA rendszerek sebezhetősége a komplexitási elemzéshez releváns kontextust ad, de a H2 hipotézis vizsgálatát kizárólag a KoI értékei alapján végzem.

Kiberbiztonsági stratégiák és keretrendszerek

A kiberbiztonsági stratégiák és keretrendszerek (CIS Controls, Mitre ATT&CK Framework, NIST Cybersecurity Framework, ISO/IEC 27001, CBEST, USA Patriot Act, valamint az OSI modell) alapvető fontosságúak a kritikus infrastruktúrák védelmében. Ezek a keretrendszerek és stratégiák lehetővé teszik a szervezetek számára, hogy azonosítsák, értékeljék és kezeljék a kiberbiztonsági kockázatokat, különösen az energiaágazatban. Az alábbiakban néhány fontos keretrendszert és stratégiát tárgyalok, amelyek hozzájárulnak a kritikus infrastruktúrák védelméhez. A későbbiekben részletesen tárgyalom, a NIST Cybersecurity Framework (CSF) alapvető funkcióit és az ISO/IEC 27001 nemzetközi szabvány relevanciáját, mivel ezek kiemelt szerepet játszanak a kritikus infrastruktúrák hosszú távú kiberbiztonsági stratégiáinak kialakításában.

CIS Controls

A CIS Controls egy a Center for Internet Security (CIS) által kidolgozott 18 kontrollból álló intézkedéscsomag, amely az informatikai rendszerek biztonságának javítására összpontosít. A CIS Controls egyszerű, jól strukturált útmutatást nyújt a szervezetek számára, különös tekintettel a sebezhetőségek minimalizálására, a támadási felületek csökkentésére és a legfontosabb védekezési stratégiák gyors bevezetésére. Könnyen adaptálható, ezért különösen hatékony a kritikus infrastruktúrák védelmében.

MITRE ATT&CK Framework

Az ICS/SCADA rendszerek kompromittálása tipikusan többlépcsős TTP-láncot (initial access → lateral movement → persistence → impact) igényel, amelyet a MITRE ATT&CK formalizál. E struktúrára támaszkodva alakítom ki a Komplexitási indexet (KoI), amely a technikai komplexitást négy bináris (0/1) komponens – többfázisú végrehajtás, laterális mozgás, perzisztencia, detektálás elkerülése – összegeként fejezi ki, ezért értéktartománya 0–4. H2 ennek alapján azt vizsgálja, hogy a nemzetállami/államilag támogatott szereplők támadásai nagyobb arányban érik el a magas KoI-küszöböt (KoI $\geq$ 2), mint a pénzügyi

motivációjú bűnözői csoportokéi [20]. A MITRE ATT&CK egy nyílt forráskódú tudásbázis, amely rendszerezi a támadók által alkalmazott taktikákat, technikákat és eljárásokat (TTP-k). Ez a keretrendszer a fenyegetések modellezésére és a védelmi stratégiák pontosabb kidolgozására használható. Kritikus infrastruktúrák esetén különösen hasznos, mivel segít az incidensek elemzésében és a proaktív védekezési stratégiák kialakításában. A kiberbiztonsági TTP-k (Tactics Techniques Procedures, taktikai-technikai eljárások) azokra a konkrét módszerekre, eszközökre és eljárásokra utalnak, amelyeket a támadók kibertámadások végrehajtására használnak. Ezek alapján:

- Taktikák: A támadás mögött meghúzódó átfogó stratégiák vagy célok (például adatkiszivárgás, rendszerzavar).
- Technikák: A taktika elérése érdekében alkalmazott általános módszerek vagy tevékenységtípusok (például adathalászat, sebezhetőségek kihasználása).
- Eljárások: Részletes, konkrét műveletek vagy lépések egy technika végrehajtásához (például egy adott adathalász e-mail sablon használata, ismert kihasználás).

CBEST, Patriot Act és EC keretrendszerek

A Bank of England és a PRA által a pénzügyi szolgáltatóknak kifejlesztett CBEST keretrendszer az energiaszektorban is a SCADA rendszerek védelmének egyik kiemelkedő eszköze [36]. A CBEST egy olyan penetrációs tesztelési keretrendszer, amely a legújabb, valós fenyegetettségi információk alkalmazásával lehetővé teszi a kritikus infrastruktúrák védelmi rendszereinek tesztelését. A kutatók a keretrendszer használatának és gyakorlati alkalmazásának elemzését követően tettek javaslatokat annak továbbfejlesztésére, hogy az eszközt még hatékonyabban lehessen alkalmazni az energiaágazat kiberbiztonsági kihívásainak kezelésére.

Az Európai Bizottság által kidolgozott "A kritikus infrastruktúra védelmének európai programja" iránymutatást nyújt az EU tagállamai számára a kritikus infrastruktúrák védelmében történő együttműködésre és intézkedésekre [37]. A program hangsúlyozza a nemzetközi együttműködés szükségességét ezen létesítmények biztonságának garantálása érdekében, továbbá egységes keretrendszert biztosít a tagállamok számára, amely elősegíti az összehangolt védekezést és a közös biztonsági célkitűzések elérését. [38].

Az USA Patriot Act [39] bővíti a kormányzati hatalmat a terrorizmus elleni harcban, beleértve a kiberbiztonsági intézkedéseket is. Ez a törvény lehetővé teszi a kormány számára, hogy

széleskörűen figyelje és kezelje a potenciális kiberfenyegetéseket, különös tekintettel a kritikus infrastruktúrák védelmére.

Tanenbaum műve [40] részletesen ismerteti az OSI modellt, amely alapvető keretet nyújt a hálózati kommunikáció és biztonság megértéséhez. Az OSI modell különböző rétegei lehetővé teszik a kiberbiztonsági stratégiák rétegezett megközelítését, biztosítva, hogy minden szinten megfelelő védelmi intézkedések legyenek alkalmazva.

A támadási fák koncepciója

Kumar és munkatársai [33] a támadási fák koncepcióját használják az APT modellezésére, különös tekintettel a Stuxnet, Blackenergy és Triton támadásokra. A támadási fák olyan grafikus modellek, amelyek ábrázolják a támadók céljait, a célok eléréséhez szükséges lépéseket és a lehetséges védelmi intézkedéseket. Ez a megközelítés lehetővé teszi a támadások, taktikák és technikák strukturált megértését, valamint újra felhasználható modellek létrehozását.

A kritikus infrastruktúrák, különösen az energiaágazat, folyamatosan ki vannak téve a kibertámadások veszélyeinek. Ezek a rendszerek létfontosságúak a társadalom működéséhez, így védelmük kiemelt fontosságú. Tvaronavičienė és munkatársai [40] az energiaágazat sebezhetőségének elemzésével foglalkoznak, hangsúlyozva a komplex kiberbiztonsági támadásokból eredő nagy károk lehetőségét és a létfontosságú infrastruktúrák védelmének globális jelentőségét. A kutatók három különböző felhasználási esetre alapozva értékelik a szervezetek válasz- és helyreállítási stratégiáit.

Egy szisztematikus támadási modellt is kidolgoztak kutatók az ipari vezérlőrendszerek (ICS) ellen irányuló fejlett tartós fenyegetések (APT) kezelésére. Yang és Zhang rámutatnak arra, hogy ezek a fenyegetések jelentős kihívást jelentenek a kiberbiztonsági területen, különösen a kritikus infrastruktúrákban található ipari vezérlőrendszerek számára [41]. Az ICS-APT támadási modell célja, hogy megfelelő enyhítési és orvoslási stratégiákat nyújtson az ilyen típusú támadások ellen.

Ezek a források átfogó képet nyújtanak a kritikus infrastruktúrák védelméről és a válaszstratégiákról, hangsúlyozva a proaktív és reaktív intézkedések fontosságát a kiberbiztonsági fenyegetések elleni védekezésben.

Ellenintézkedések és rugalmas stratégiák

A kritikus infrastruktúrák védelme érdekében elengedhetetlenek a célzott ellenintézkedések és rugalmas stratégiák, amelyeket a kiberbiztonsági szakemberek folyamatosan fejlesztenek az egyre összetettebb fenyegetésekkel szemben. Ezek a megközelítések nemcsak a fenyegetések azonosítását és kezelését szolgálják, hanem a rendszerek ellenállóképességének növelését is, amely alapvető fontosságú a társadalmi és gazdasági stabilitás fenntartásában.

Az ilyen stratégiák kidolgozásában kulcsszerepet játszanak a nemzetközileg elismert keretrendszerek és iránymutatások, mint a fentebb említett, az energiaágazat SCADA rendszereinek védelmére specializálódott CBEST keretrendszer, vagy az ISO/IEC 27001 szabvány, amely átfogó megközelítést nyújt az információbiztonság kezeléséhez.

Ezek mellett az olyan jogszabályi és nemzetközi együttműködési irányelvek, mint az USA Patriot Act vagy az Európai Bizottság kritikus infrastruktúra-védelmi programja, szintén hozzájárulnak a hatékony védelem kialakításához.

A fentebb taglalt források átfogó alapot nyújtanak kiberbiztonsági stratégiák kialakításához, és lehetővé teszik a szervezetek számára, hogy gyorsan reagáljanak a változó fenyegetési környezetre. A következőkben részletesen bemutatom, hogyan alkalmazhatók ezek az ellenintézkedések és keretrendszerek a gyakorlatban, különös tekintettel a kritikus infrastruktúrák sajátos igényeire.

Az információ biztonság és az informatikai biztonság

A kritikus infrastruktúrák védelme szempontjából kiemelt jelentősége van annak, hogy az informatikai rendszerek milyen módon biztosítják az adatok bizalmasságát, sértetlenségét és rendelkezésre állását. Ezek az alapelvek nemcsak a klasszikus védekezési modellek szempontjából meghatározók, hanem kulcsszerepet játszanak a mesterséges intelligencia alkalmazásában is. A dolgozatban bemutatott prediktív modellezési irányvonal – amely a jövőbeli támadások előrejelzésére törekszik – csak akkor képes megbízhatóan működni, ha az adatok eredetisége, pontossága és folyamatos elérhetősége biztosított. Ezen összefüggések kiemelik a biztonsági célok és az AI-alapú elemzések közötti közvetlen kapcsolatot, és megalapozzák a harmadik hipotézist, amely szerint a predikció hatékonysága szoros összefüggést mutat az adatkezelési gyakorlat minőségével.

Az információ biztonság és az informatikai biztonság kifejezéseket gyakran egymás szinonimáiként használják, pedig a két szó mögötti tartalmak között van különbség. Az

információ biztonság egy jóval tágabb terület, a teljes információ feldolgozási kör biztonságáról való gondoskodást jelent.

Az elektronikus alapú információfeldolgozás egyre nagyobb jelentőséggel bír a modern szervezetek működésében, azonban még mindig léteznek olyan információk, amelyeket papír alapú vagy szóbeli úton továbbítanak és dolgoznak fel. Ezek az információk gyakran nem kerülnek elektronikus formában rögzítésre, ami kihívást jelent az információbiztonság szempontjából. Mivel az értekezés főként az elektronikus információfeldolgozás kérdéseivel foglalkozik, ezért az informatikai biztonság területére koncentrálunk, amely kiterjed az elektronikus adatok védelmére és biztonságára is[42] [43].

Az informatikai biztonság megvalósítása nem csupán elméleti kérdés, hanem számos gyakorlati kihívást is magában hordoz. Az információ akkor tudható biztonságban, ha három alapvető feltétel teljesül: a bizalmasság, a sértetlenség és az elérhetőség. A három fő alapelv – angol rövidítéseik alapján CIA elvként ismert – alkotja az informatikai biztonság alappilléreit. Az informatikai biztonság kialakításának célja ezen feltételek megvalósítása és folyamatos fenntartása.

Fontos megjegyezni, hogy az informatikai biztonság által megvalósított célok nem abszolútak, hanem egy adott igényszinthez igazítottan értelmezhetők. Ezért az informatikai rendszerek védelmét mindig a körülményeknek megfelelően kell kialakítani és folyamatosan felülvizsgálni. A CIA-triád részletes kifejtését, valamint a kapcsolódó alkategóriákat (letagadhatatlanság, elszámoltathatóság, hitelesség) az M1.melléklet tartalmazza.

Az informatikai biztonság nem statikus állapot. Az adott szervezet külső és belső körülményei folyamatosan változnak, és ehhez hozzá kell igazítani az informatikai támogatás biztonságát. Az informatikai biztonság tevékenységi csoportjai három fő területre oszthatók: a rendszer létrehozása, a napi működtetés, valamint a jövőbeli kockázatokra való felkészülés[44].

A kockázatkezelés központi szerepet játszik az informatikai biztonságban. A kockázatértékelés a kockázatelemzés és a kockázatok kiértékelésének együttes tevékenysége, amely célja a szervezet számára releváns kockázatok teljes körű felmérése és kezelése[45].

Az előrejelzésekben rejlő bizonytalanság miatt fontos a rendszerek kockázatelemzése és értékelése. A megismételt kockázatelemzések az informatikai rendszer aktuális működési biztonságáról adnak információt. A kockázatok elemzésére és értékelésére jól kidolgozott módszerek léteznek. Ezek az elemzési módszerek nem csupán a múltbéli hibák feltérképezését

segítik, hanem hozzájárulnak a jövőbeni kockázatok előrejelzéséhez is, ami a dolgozat prediktív modellalkotásra épülő hipotéziseit is megerősíti.

A fenti integritás- és elérhetőségi követelmények az adatminőségen keresztül közvetlenül befolyásolják a prediktív modellek teljesítményét. H3 azt teszteli, hogy a korai fázisú, szöveges leírásokra (pl. TF-IDF) és kezdeti metaadatokra építő rétegzett (stacking) ensemble modell szignifikánsan felülmúlja-e a szabályalapú és a Random Forest baseline modelleket az aktortípus becslésében. A teljesítményt az osztály-egyensúlytalanságra érzékeny mutatókkal (PR-AUC, macro-F1) értékelem [46].

Az előző részekben áttekintettem az információs és informatikai biztonság alapvető szempontjait és hangsúlyoztam a szervezeti kockázatok átfogó kezelésének jelentőségét. Ez a megközelítés nemcsak a rendszerek és adatok sértetlenségének, bizalmasságának és elérhetőségének megőrzését segíti, hanem a különféle fenyegetésekre való hatékony reagálást is lehetővé teszi.

A 2000-es évek eleji terrortámadások rávilágítottak arra, hogy a kormányzati, társadalmi és gazdasági funkciók fenntartásához kulcsfontosságú erőforrások mennyire jelentős mértékben ki vannak téve a külső és belső fenyegetéseknek. A kiberbiztonsági kutatások ezért egyre nagyobb figyelmet fordítanak a kritikus infrastruktúrák védelmére, legyen szó fizikai, immateriális vagy kiberalapú elemekről. Hatékony védelmi rendszerek kialakításához olyan struktúrált megközelítést érdemes alkalmazni, amely minden biztonsági réteget külön-külön képes vizsgálni és értékelni, a maga kockázataival és védelmi lehetőségeivel együtt.

Ebben a megközelítésben nyújt releváns értelmezési keretet az OSI (Open Systems Interconnection) modell [47]. A hét, egymásra épülő rétegbe rendezett koncepcionális keretrendszer – a hálózati kommunikáció működését és protokolljait szabványosítva segíti a különböző rendszerek közötti interoperabilitást, valamint lehetővé teszi a biztonsági kockázatok és védelmi stratégiák rétegenkénti elemzését [48].

A modell minden rétege specifikus biztonsági kihívásokkal és védekezési lehetőségekkel rendelkezik, a fizikai biztonságtól (1. réteg) az alkalmazás-specifikus védelemig (7. réteg). A kritikus infrastruktúrák védelmében különösen fontos a rétegenként eltérő támadási vektorok és védelmi mechanizmusok megértése, mivel egy többrétegű védelmi stratégia ("defense in depth") alkalmazása jelentősen növelheti a rendszer ellenálló képességét.

1.2. Aszimmetrikus konfliktus, kiber és gazdasági dimenziók irodalma

Az alábbi alfejezet a dolgozat tágabb geopolitikai és stratégiai kontextusát mutatja be; a benne tárgyalt elméleti és történeti megfontolások nem képezik a H1–H3 hipotézisek empirikus tesztelésének közvetlen részét.

A kibertér rétegzettsége, ennek folyományai és aszimmetrikus természete szükségessé teszik Clausewitz a háború elemzésének alapvető kereteit jelentő "csodálatos háromságának" újragondolását. Clausewitz háromsága – a kormány, a hadsereg és a nép közötti dinamika – a 19. századi hagyományos hadviselésben kulcsfontosságú volt. Azonban a kibertérben ezek az elemek új szereplőkkel és taktikákkal bővültek, átalakítva a háború fogalmát és természetét [49].

A klasszikus háborúelemzésben a fizikai erőszak, a véletlenek és a racionalitás domináltak. A kiberháborúban azonban az információ kontrollja, a technológiai sebezhetőségek kihasználása és a társadalmi manipuláció került előtérbe. Ezek az elemek új megvilágításba helyezik a modern hadviselést, ahol a hagyományos erőviszonyok helyett a technológiai innovációk és információs előnyök dominálnak. A technológia fejlődése és az információs hálózatok terjedése lehetővé teszi a kisebb, kevésbé erős szereplők számára is, hogy jelentős befolyást gyakoroljanak, amely korábban csak nagy államok privilégiuma volt [19].

Dimenzió	Hagyományos hadviselés	Aszimmetrikus hadviselés	Hibrid hadviselés
Cél	Ellenfél legyőzése	Politikai, gazdasági vagy társadalmi változás elérése	Ellenfél legyőzése, presztízs vagy haszonszerzés
Módszer	Közvetlen katonai erő alkalmazása	Indirekt taktikák, például gerillaharc, terrorizmus	Közvetlen katonai erő és indirekt taktikák kombinációja
Jellemző szereplők	Államok, reguláris haderők	Nem állami szereplők, milíciák, terroristák	Államok és nem állami szereplők vegyesen (pl. proxy-hadseregek)

Táblázat 1-Hagyományos, aszimmetrikus és hibrid hadviselés mátrixa

Az aszimmetrikus konfliktusok egyik jellemzője, hogy a gyengébb fél képes az erősebb fél politikai és társadalmi szándékait hatékonyan befolyásolni. A hagyományos értelemben vett "erő" fogalma így átalakul, hiszen a kiberhadviselés lehetővé teszi, hogy a kisebb csoportok is komoly hatást gyakoroljanak az erősebb ellenfelekre. Ez a fajta aszimmetria kiemeli a hagyományos hadviselési modellek újraértékelésének szükségességét, ahol a kibertér adta lehetőségek és fenyegetések már alapvetően befolyásolják a geopolitikai erőviszonyokat [50].

A modern kiberháborúban az információ kontrollja különösen fontos szerepet játszik. A technológiai sebezhetőségek kihasználása és a társadalmi manipuláció lehetővé teszi a támadók számára, hogy jelentős politikai és társadalmi változásokat idézzenek elő. Az információ hatalma a digitális korban a hagyományos katonai erőnél is nagyobb lehet, hiszen az információ manipulálása és hamis adatok terjesztése destabilizálhat kormányokat és társadalmakat [20].

A kibertámadások sikeressége nem csak a technológiai képességek minőségén, hanem a támadások politikai és társadalmi hatásain is múlik. Egy sikeres kibertámadás képes aláásni az állam bizalmát és támogatottságát, még akkor is, ha az állam katonailag erős. Ez az új típusú

konfliktus Clausewitz klasszikus elméleteihez képest jelentős változásokat hoz, különösen a politikai akarat és a társadalmi támogatottság szerepét illetően.

Clausewitz idejében a nép közvetlen szerepe a hadviselésben korlátozott volt, azonban a modern kibertérben a civil társadalom aktív résztvevővé vált. A kiberhadviselés anonim és távoli jellege lehetővé teszi, hogy a támadók közvetlenül befolyásolják a társadalmat, anélkül hogy fizikai jelenlétre lenne szükségük. Ez alapvetően újraértelmezi a hatalom és politikai akarat összefüggéseit, ahol a kibertámadások célja gyakran a társadalmi bizalom megingatása és a politikai stabilitás gyengítése [20].

A társadalmi támogatottság és politikai akarat kulcsszerepet játszanak a kibertámadások sikerességében. A támadók gyakran használnak dezinformációt, propagandát és társadalmi média manipulációt, hogy destabilizálják az államokat. Ezek a technikák lehetővé teszik, hogy a támadók aláássák a kormány legitimitását és csökkentsék a politikai vezetők támogatottságát. Az ilyen típusú támadások során a technológiai képességek mellett a pszichológiai hatások is kritikus fontosságúak [50].

Egy példa erre a 2016-os amerikai elnökválasztási kampány során történt orosz beavatkozás, ahol a kibertámadások és dezinformációs kampányok célja az volt, hogy befolyásolják a választások eredményét és csökkentsék a közvélemény bizalmát a demokratikus folyamatokban. Az ilyen típusú támadások rávilágítanak arra, hogy a politikai akarat és társadalmi támogatottság megingatása mennyire hatékony eszköz lehet a modern kiberhadviselésben [20].

A társadalmi és politikai hatások mellett a kibertámadások kimenetele gyakran a támadók céljainak és stratégiáinak függvénye. A támadók nem mindig a közvetlen technológiai kárt keresik, hanem a hosszú távú politikai és társadalmi destabilizációt. Ez különösen igaz olyan esetekben, amikor a támadók célja a politikai vezetők hiteltelenítése vagy a társadalmi kohézió gyengítése [51].

Összefoglalva, a kibertámadások sikerességét nem csupán a technológiai képességek határozzák meg, hanem a támadások politikai és társadalmi hatásai is. Az információ manipulálása és a társadalom befolyásolása kulcsfontosságú tényezők, amelyek meghatározzák a kibertámadások hatását. A modern kiberhadviselés során a politikai akarat és társadalmi támogatottság gyengítése gyakran a támadók fő céljai közé tartozik, ami új kihívásokat jelent a nemzetbiztonsági stratégiák számára [50].

Erről a modern hadviselésről és annak technológiai dimenzióiról szóló nézeteit már az ukrajnai válság előtt is kifejtette Oroszország fegyveres erőinek vezérkari főnöke, Valerij Geraszimov. Nézeteit a "tudományos káosz elméletére" alapozva fejlesztette ki, amelyet azóta is alkalmaz Moszkva [52; 53]. Molly K. McKew, aki közelről figyelhette az orosz nem-hagyományos módszerek alkalmazását, részletesen írt Geraszimov nézeteiről. McKew korábban tanácsadóként dolgozott Szaakasvili grúz elnök mellett, valamint Moldova miniszterelnökének tanácsadójaként is tevékenykedett [54].

Geraszimov 2013 februárjában publikálta a modern hadviselésről szóló tanulmányát, amelynek címe: "A tudomány értéke a jövőbe látásban". A doktrína központi gondolata, hogy a nem katonai eszközök alkalmazása ma már sokkal célravezetőbb lehet a politikai célok elérésében, mint a hadsereg közvetlen bevetése. Az orosz vezérkari főnök elmélete azon az előfeltevésen alapul, hogy Oroszország gyengébb, mint ellenfelei. Ennek megfelelően Geraszimov célja nem az, hogy Oroszország erősebbé váljon, hanem inkább az, hogy annyira legyengítse ellenfeleit, hogy azok kénytelenek legyenek Oroszországot egyenlő partnerként elfogadni [55].

Ennek példája Ukrajna, ahol a Geraszimov-doktrína [56; 57] alkalmazása a legjobban nyomon követhető. Oroszország két szélsőséges mozgalmat támogatott: azokat az Ukrajna keleti részén élő oroszokat, akik csatlakozni akartak Oroszországhoz, és egyidejűleg azokat a neonáci ukránokat, akik Sztyepan Banderát tekintették az eszményképüknek. Bandera - az ukrán nacionalista vezér - még a nácikkal is együttműködve harcolt a Szovjetunió ellen – irtva közben a zsidókat és a lengyeleket is Ukrajnában. Később a szovjet titkosszolgálat végzett vele. Napjainkban pedig a már tudományosan megtervezett káosz odavezetett, hogy Ukrajnában teljes tudott lenni az anarchia, miközben Putyin megszerezte a Krím félszigetet és de facto megszállta Ukrajna orosz többségű keleti tartományait.

Annak megfigyelése, hogy valamiről, vagy valakiről kevés szó esik egyes sajtótermékekben, míg máshol nagy publicitást kap, illetve a korábbi gyakori megjelenés egy időpont után ritkulni kezd, majd eltűnik, klasszikus, már régtől fogva alkalmazott módszere a tartalomelemző kutatásoknak.

A hivatalos fasiszta propaganda nyíltan még hosszú ideig nem ismerte be, hogy a tengeralattjárókhoz fűzött nagy remények szertefoszlottak, ám az a tény, hogy a propaganda-szimbólumok közül jóformán az egyik napról a másikra eltűnt a korábban oly fontos „tengeralattjáró” szó, „beszédesen” árulkodott valamiről, amit a forrás, az akkori, államilag uraltnémet sajtó, el akart hallgatni.

A RAND [58] elemzése szerint az orosz állami propaganda képes hatékonyan érvényesíteni a céljait, köszönhetően a jól megtervezett eszközkombinációknak, és a modern internetes technológia nyújtotta ismétlés (internet, rádió, tv) lehetőségének.

Egy szövegen belül egymással közvetlenül össze nem kapcsolódó tartalmak elemzése nem csupán a megszólaló rejtett szándékaira tud rávilágítani, hanem olyan gondolataira is, amelyeket el szeretne titkolni a hallgatóság elől. Antal László leírja a tartalomelemzés katonai alkalmazásának azt a példáját, amikor az amerikai elemzők a német-olasz viszonyt vizsgálták Goebbels beszédei alapján, és megfigyelték, hogy ezekben az olaszok említése környékén gyakran szerepeltek nehézségekre, gondokra utaló megállapítások [59]. Az ehhez hasonló megnyilatkozások elemzése alapján jutottak arra a következtetésre, hogy feszült viszony lehet az akkori szövetséges német és olasz vezetés között. Csak a háború után derült ki Goebbels naplójából, hogy ez a feltételezés igaz volt [59].

Az aszimmetrikus kihívások jellemzően alacsony költségű, nem hagyományos jellegű, ártó szándékú tevékenységek, amelyekkel szemben a hagyományos védelmi rendszerek gyakran korlátozottan hatékonyak. Ezek a fenyegetések nemcsak a katonai infrastruktúrát, hanem a civil társadalom különböző területeit is érinthetik, mivel jellemzően kihasználják a társadalmi, gazdasági és technológiai rendszerek meglévő sebezhetőségeit. Példaként említhető a terrorizmus, amely célzott akciókkal képes destabilizálni a közbiztonságot és megingatni a politikai rendszerek stabilitását, vagy a kibertámadások, amelyek az informatikai infrastruktúrák megzavarásával súlyos működési fennakadásokat és gazdasági károkat okozhatnak mind az állami szervezetek, mind a magánvállalatok számára.

Az információs hadviselés, a biológiai és vegyi fegyverekkel való fenyegetés, illetve azok nem hagyományos alkalmazása különösen veszélyes aszimmetrikus eszközök, mivel alkalmazásuk viszonylag alacsony erőforrásigény mellett is jelentős hatást érhet el [60]. Noha ezek az eszközök technológiai fejlettséget igényelnek, használatuk komoly logisztikai és etikai kihívások elé állítja a védekezést. Az ilyen fenyegetések jellemzően a támadó fél erőforrásainak és képességeinek aszimmetriáját tükrözik, ahol az erősebb felet gyengítik a gyengébb fél által alkalmazott rugalmas és kiszámíthatatlan módszerek.

Az aszimmetrikus fenyegetések konkrét példái között szerepelnek az öngyilkos merényletek, bombatámadások, és a logisztikai vagy vezetési pontok elleni célzott akciók [61]. Ezek a támadások jelentős taktikai előnyt biztosíthatnak a támadónak, különösen, ha az ellenség utánpótlási vonalait vagy szállítási útvonalait célozzák meg. Az ilyen műveletek az ellenséges

erők ellátását és működési kapacitását csökkentik, miközben pszichológiai nyomást gyakorolnak, tovább növelve az aszimmetrikus eszközök hatékonyságát. Az ilyen fenyegetések kezelése komplex megközelítést igényel, amely magában foglalja a preventív intézkedéseket, a technológiai védekezést, valamint a stratégiai és taktikai tervezést.

Az akciók felderítése legtöbbször nagyon nehéz, illetve alkalmazói nem tartják be a hadviselés előírásait. Irakban is számos alkalommal érte támadás a szövetségesek katonáit, amelyeket polgári ruhába öltözött katonák vagy civilek hajtottak végre. Az ilyen jellegű hadviselésre nagyon nehéz a katonák pszichikai felkészítése, a védekezés is sok problémát hordoz magában [62].

Az aszimmetrikus hadviselés a modern konfliktusok egyre inkább előtérbe kerülő formája, amely jelentős eltéréseket mutat a hagyományos katonai összecsapásoktól. E hadviselési forma sajátossága, hogy gyakran nem államok között zajlik, hanem állami és nem állami szereplők, például gerillacsoportok, lázadók vagy terroristák között. Zwitter (2010) szerint az aszimmetrikus hadviselés lényege, hogy a résztvevők jelentős különbségeket mutatnak a katonai eszközök, módszerek és erőforrások terén, ami alapvetően eltérő stratégiákat és taktikákat követel meg a résztvevőktől [63]. Egy ilyen háború során az egyik fél - gyakran a kisebb és kevésbé erős szereplő - egyszerű, de hatékony módszereket alkalmaz, hogy kihasználja ellenfele gyengeségeit, minimalizálva ezzel a saját erőforrásainak felhasználását, miközben maximális hatást ér el.

Más nézetek szerint ez a fajta hadviselés kis csoportok által, a túlerőben lévő fél ellen folytatott tevékenység, de lehetséges a hagyományos eszközökkel, túlerőben folytatott háborút is így nevezni. Más megközelítésben gerilla-, partizán- vagy kis háborúknak is nevezik őket.

Az aszimmetrikus hadviselést alkalmazó fél [64; 65] (64: p.19):

– egyszerű, gyakran szokatlan eszközöket alkalmaz igen nagy eredménnyel;
– kihasználja a szemben álló fél erejét, mint annak fő gyengeségét;
– arra törekszik, hogy minimális erőbefektetéssel maximális eredményt érjen el;
– nincs szüksége nagy katonai erőre, bürokratikus parancsnokságra;
– az alkalmazott kis méretű erők lehetővé teszik számára a gyors döntéshozatalt és a sikeres akciót;

– nem szemtől szemben veszi fel a versenyt, mivel nem rendelkezik kellő katonai képességekkel.

A lehetséges következtetésekre nézve elmondható, hogy:

– óriási az erő-eszköz különbség a konfliktusban részt vevő, azaz a harcoló felek között;

– a kisebbik fél katonai képességei annyira korlátozottak, hogy a katonai győzelmet kizárólag hagyományos eszközökre támaszkodva nem érheti el;

– az ilyenfajta háború megvívásához gerillaharc, szabotázs, terror szükséges;

– a normák átlépése, elhagyása;

– a cél az ellenséget, a megszállót különböző, részben katonai eszközökkel (köztük terrorista módszerekkel is) céljának feladására kényszeríteni;

– minél inkább elhúzódik egy háború, egy fegyveres konfliktus, annál valószínűbb, hogy bekövetkezik az aszimmetrikus hadviselés Afganisztán (szovjet megszállás, majd amerikai jelenlét): Az elhúzódó háborúk során a tálibok és más lázadó csoportok aszimmetrikus taktikákat alkalmaztak, például gerillatámadásokat, csapdaakciókat és öngyilkos merényleteket. Vietnámi háború: A vietkong erők kiterjedten használták az aszimmetrikus hadviselést a hosszan tartó háború során. Irak: Az amerikai inváziót követően a konfliktus elhúzódásával fokozódott az aszimmetrikus harcmodor (lázadás, IED-ek használata, gerillatámadások)[65];

– Clausewitz [66] (p.34.) szerint a győzelemhez az ellenség haderejét le kell győzni, területét el kell foglalni, akaratát meg kell törni[1]

A hadtudomány korunk talán legdinamikusabban változó területe a módszerek és eljárások - különösen azok sokrétű és változatos- alkalmazásának a kérdése. Különös jelentőséggel bír ebben az összefüggésben az aszimmetria fogalmi értelmezése, amely a hadtudományon belül szinte súlyponti szerepet tölt be. Ahogy gyakran idézik: „a módszer maga a szervezet” – legyen szó katonai, gazdasági, kiber, pszichológiai, pénzügyi vagy egyéb manőverekről, ezek kombinációja és hatásmechanizmusa adja az aszimmetria velejét. A rommeli gyors lerohanó

[1] De még ha mindkettő megtörtént is, a háborút, vagyis az ellenség feszültségét és az ellenséges erők fellépését nem lehet befejezettnek tekinteni mindaddig, amíg az ellenség akaratát is le nem igázzák, azaz kormánya és szövetségesei nem tudnak békét kötni, vagy a nép be nem hódol; Mert amíg a föld teljes birtokában vagyunk, a harc feléledhet benne, vagy szövetségeseinek segítségével. (Ist aber auch beides geschehen, so kann der Krieg, d.h. die feindliche Spannung und Wirkung feindseliger Kräfte, nicht als beendet angesehen werden, solange der Wille des Feindes nicht auch bezwungen ist, d.h. seine Regierung und seine Bundesgenossen zur Unterzeichnung des Friedens oder das Volk zur Unterwerfung vermocht sind; denn es kann sich, während wir im vollen Besitz des Landes sind, der Kampf in seinem Innern oder auch durch Beistand seiner Bundesgenossen von neuem entzünden.)

taktika, a megfélemlítés, a gazdasági érdekérvényesítés különböző módszerei, a lakossági támogatás megléte vagy kivívásának stratégiái mind releváns vizsgálati dimenziókként szolgálhatnak ebben a kontextusban.

Nagyon fontos kérdés lehet a háború kérdéseinek a megvizsgálásánál az erély, az erőszak, a mérhetetlen erőszak vagy – ahogy Clausewitz fogalmaz – „a végletekre törő erőszak" elemzése a konfliktusokban, a jelenkori konfliktusokban. A kérdések ütközéspontjába legtöbbször nem csupán katonai, politikai vagy felső stratégiai tényezők kerülnek, hanem a vallás is, mint a társadalmi tér, a kultúra, a szocializációs háttér szerves része, amely jelentős befolyással bír az események alakulására. Az Iszlám Állam példája megmutatja, hogy az a rendkívül döbbenetes erőszak, amelytől visszariadnak a nyugati hatalmak, milyen gyors sikereket tesz lehetővé, de nyilvánvalóan csak ebben a társadalmi, vallási közegben.

A következő szakaszban összefoglalom a hadviselési típusok legfőbb jellemzőit.

A hagyományos hadviselés

Összefoglalóan a hadviselési módokról és hagyományos hadviselésről az mondható el, hogy a hagyományos műveletek szereplői olyan államok, melyek viszonylagos erő- és eszközegyensúlyban vannak, stratégiai cél az ellenfél védtelenné tétele, akaratunk rákényszerítése, az ellenséges katonai erők megsemmisítése, területének elfoglalása, az ellenséges nép akaratának a megtörése. Fő eszköz a katonai módszerek alkalmazása, a stratégiai dimenziók közül a fő elem pedig a katonai erő és annak alkalmazása. Fő jellegzetesség a megsemmisítés. Az ilyen jellegű konfliktusok halott-sebesült aránya 1:3. A vezérlő szereplő a műveletek kezdetétől a befejezésig az állam. Ilyen hadviselés például az iraki–iráni háború, vagy az Amerikai Egyesült Államok vezette koalíció Irak ellen.

Az aszimmetrikus hadviselés

Az aszimmetrikus hadviselés résztvevői között egyaránt találunk állami és nem állami szereplőket. Ezekben a műveletekben kiemelt jelentősége van az erőforrások és képességek közötti aránytalanságnak, amely jelentősen befolyásolja a konfliktus jellegét és dinamikáját. Az aszimmetrikus konfliktusok stratégiai célja általában az ellenfél kifárasztása, akaratának megtörése, és ezáltal saját politikai vagy stratégiai célkitűzések érvényesítése. Ezen konfliktusok tipikus módszerei közé tartoznak a gerilla-hadviselés, felkelő- és terrorista jellegű műveletek, amelyek főként indirekt, nem konvencionális harceljárásokra építenek[67].

Az aszimmetrikus hadviselés legjellegzetesebb tulajdonsága az időfaktor stratégiai alkalmazása, amely lehetővé teszi az ellenfél hosszú távú kifárasztását. Az ilyen jellegű műveletekben a veszteségek, a halottak és sebesültek aránya rendszerint jelentősen különbözik a hagyományos hadviseléstől, általában 1:6 és 1:14 között mozog[68]. A konfliktus főszereplői a harcok kezdetétől egészen azok lezárásáig tipikusan fegyveres erők és különböző fegyveres csoportok. Jellemző példa erre az Amerikai Egyesült Államok és szövetségesei által folytatott aszimmetrikus hadviselés az al-Káida nem állami terrorszervezet ellen, amely során jelentős szerepet játszottak a gerilla- és felkelőellenes stratégiák.

A hibrid hadviselés

A hibrid műveletek szereplői az állam vagy államok és irreguláris szervezetei az állam vagy államok ellen. A döntő erő- és eszközfölényben levő fél alkalmazza. Stratégiai cél az ellenséges állam és fegyveres erők működésképtelenné, védtelenné tétele, akaratunk rákényszerítése; az állam/nép akaratának a megtörése, az ellenséges állam, illetve katonai erők működésképtelenné tétele, területének elfoglalása, elcsatolása. Fő módszer a reguláris/irreguláris katonai erők és gerilla, terrorista szervezetek, diplomáciai képviseletek, gazdasági módszerek felváltva történő alkalmazása[69]. Fő jellegzetesség a kifárasztás és a működésképtelenné tétel. A stratégiai dimenziók közül a fő elem a katonai erő és az információ.

A három hadviselési módot összefoglalva megállapítható, hogy a hagyományos hadviselés katonai végállapotára igaz hármas szabály a hibrid műveleteknél megfordul. Az elsődleges siker a régi háborúkban a „megsemmisíteni-elfoglalni-megtörni” helyébe az aszimmetrikus műveletekben a „kifárasztani-megtörni-kivéreztetni”, a hibrid műveleteknél a „megtörni-működésképtelenné tenni-elfoglalni” elvek és szabályok léptek.

Az aszimmetrikus és hibrid hadviselés, valamint a kiberdimenzió összefüggései

Az aszimmetrikus és hibrid hadviselés többféle, gyakran egymást kiegészítő módszereke épít, amelyben a diplomáciai, gazdasági, katonai és információs eszközök mellett egyre inkább szerepet kapnak a kibertérben megvalósuló műveletek is. Ezáltal a kiberhadviselés nem elszigetelt jelenség, hanem szervesen illeszkedik az aszimmetrikus és hibrid konfliktusok összetett rendszerébe.

A kutatás szempontjából kiemelt jelentőséggel bír, hogy a kiberfenyegetések miként befolyásolják a kritikus infrastruktúrák biztonságát és működőképességét. A kibertér a viszonylag kevesebb erőforrással rendelkező fél számára is lehetőséget nyújt a fejlettebb vagy erősebb szereplővel szembeni hatásos támadások indítására, amelyek nem csupán katonai,

hanem szélesebb társadalmi-gazdasági következményekkel is járhatnak. Ennek fényében vizsgálom majd, hogy a jövőbeni kihívásokra milyen új stratégiák, védelmi technikák és szabályozási megközelítések adhatnak választ.

A kiberhadviselés helyzete

A modern hadviselés öt kulcsfontosságú területet ölel fel: a földet, a levegőt, a tengert, a világűrt és a kiberteret; nem csupán a hagyományos hadviselés formáit fedi le, hanem a technológiai fejlődéssel párhuzamosan a digitális és az űrbéli műveleteket is magában foglalja. A kibertér – mint az ötödik hadszíntér – kiemelt figyelmet kap, mivel a modern konfliktusok egyre inkább kiegészülnek az információs rendszerek, infrastruktúrák és adatbiztonság elleni támadásokkal.

A kiberbiztonsági támadásokat egyre inkább alkalmazzák az információs hadviselési műveletek részeként. A digitális támadások különböző eszközökkel, technikákkal, taktikákkal és eljárásokkal történnek, amelyeket a kiberbűnözők, különösen az államilag támogatott hackerek vagy APT-csoportok alkalmaznak. Ezek a támadások rendkívül kifinomultak, és elképzelhetetlen mértékű károkat okoznak.

A The state of Cyberwarfare: Armis state of Cyberwarfare and trends report 2022-2023 [70] szerint a globális szervezetek 1/3-ada nem veszi komolyan a kiberhadviselés hatásait. A kutatás során az Armis 6021 IT és biztonsági szakembert kérdezett meg olyan vállalatoktól, amelyek több mint száz alkalmazottal rendelkeznek. A felmérés az Egyesült Államokban, az Egyesült Királyságban, Franciaországban, a DACH régióban (Ausztria, Németország, Svájc), Spanyolországban, Portugáliában, Olaszországban, Dániában, Hollandiában, valamint az APJ régióban (Ausztrália, Japán, Szingapúr) készült. Az adatok gyűjtésére 2022. szeptember 22. és október 5. között került sor. Az elemzés és a globális kiberhadviselés állapotát mutatja be a különböző régiókban és iparágakban.

Az ukrán-orosz háború kapcsán kialakult geopolitikai feszültségek miatt a kiberfenyegetések még inkább előtérbe kerültek és egyre gyakoribbá váltak.

Vezető biztonsági szakemberek és kutatók előrejelzése szerint 2025-re a kiberbűnözők az OT-t (Operational Technology) fegyverként fogják alkalmazni még az emberek ellen is. Az APT fenyegető csoportok egyre inkább arra összpontosítanak, hogy összetettebb támadásokkal károsítsák a nemzeti szintű infrastruktúrát [71].

Az orosz-ukrán háború jelentősen megváltoztatta a kritikus infrastruktúra-szervezetek jelenlegi fenyegetettségi helyzetét. A Google 2023-as Fog of War jelentése alapján [29] Oroszország

volt az egyik olyan állam, amely államilag támogatott támadásokkal sokkal nagyobb arányban támadta a felhasználókat Ukrajnában, mint bármely más országban. Ezek az események rávilágítanak a kiberhadviselés fokozódására és annak globális következményeire.

A kiberhadviselés gazdasági vonzereje az alacsony belépési küszöbben és a potenciálisan magas megtérülésben rejlik. A hagyományos hadviselés és a kiberhadviselés közötti költségkülönbségek több nagyságrendet is elérhetnek. Míg egy modern fegyverrendszer kifejlesztése és beszerzése tíz- vagy százmillió dolláros nagyságrendű befektetést igényel - ahogy Arena és munkatársai [72] több fontos védelmi beszerzési program elemzése során kimutatták -, addig egy kifinomult kibertámadás kifejlesztése gyakran néhány tízezer vagy százezer dollárból megvalósítható. A Congressional Budget Office 2024-es elemzése [73] szerint egy modern vadászgép beszerzési ára 100-200 millió dollár között mozog, míg egy hadihajó költsége akár a milliárd dollárt is meghaladhatja.

A fenntartási költségek terén még markánsabb a különbség. A hagyományos katonai képességek fenntartása jelentős logisztikai apparátust, folyamatos kiképzést és karbantartást igényel, míg a kiberműveletek kis létszámú, specializált csapatokkal működtethetők. Anderson és társai [14] számításai szerint a kiberbűnözés által okozott globális károk és a támadók befektetései közötti arány akár 1000:1 is lehet, ami rendkívül vonzóvá teszi ezt a hadviselési formát mind állami, mind nem állami szereplők számára.

A hatótávolság tekintetében a kibertér globális természete megszünteti a földrajzi korlátokat. Egy távol-keleti szerverről indított támadás percek alatt elérheti célpontját a világ másik felén, míg a hagyományos katonai műveletek jelentős logisztikai kihívásokkal szembesülnek a távolság növekedésével. Ez különösen előnyös az aszimmetrikus szereplők számára, akik így képesek olyan célpontokat is elérni, amelyek fizikailag megközelíthetetlenek lennének számukra.

Az attribúció problémája szintén a támadók javára billenti a mérleget. Míg a hagyományos katonai akciók általában egyértelműen azonosítható forrásból erednek, a kibertámadások eredetének megállapítása gyakran hosszadalmas és bizonytalan kimenetelű folyamat. Rid és Buchanan [74] [4-37.] szerint az attribúciós bizonytalanság stratégiai előnyt jelent a támadóknak, mivel csökkenti a megtorlás valószínűségét és növeli a tagadhatóság lehetőségét.

A potenciális károkozás természete is alapvetően különbözik. A hagyományos támadások elsősorban fizikai károkat okoznak, amelyek - bár súlyosak lehetnek - általában jól körülhatárolhatók és helyreállíthatók. Ezzel szemben a kibertámadások rendszerszintű

zavarokat okozhatnak, kaszkád hatásokkal, amelyek messze túlmutatnak az eredeti célponton. A 2017-es NotPetya támadás például eredetileg Ukrajnát célozta, de végül globális ellátási láncokat bénított meg, több mint 10 milliárd dollár kárt okozva világszerte [75].

Ez a költség-haszon aránytalanság különösen a kritikus infrastruktúrák esetében válik fontossá, melyek esetében egy viszonylag olcsó kibertámadás társadalmi szintű zavarokat és gazdasági károkat okozhat, amelyek helyreállítása akár évekig is eltarthat.

Az elmúlt években külön kategóriává nőtt a beszállítói láncon keresztüli (supply chain) kompromittálás, amikor a támadó nem közvetlenül a célintézményt, hanem annak szoftver-, szolgáltató- vagy eszköz-beszállítóját éri el, majd a frissítési vagy integrációs csatornákon keresztül kaszkádszerűen terjed több szervezet felé. A jelenség súlyát jól mutatják a nagy hatású esetek (pl. SolarWinds/Orion, Kaseya VSA, NotPetya/MeDoc), valamint az európai és amerikai irányelvek és útmutatók, amelyek ma már kifejezetten a beszállítói kockázatkezelés megerősítését írják elő.

A supply chain kompromittálást a dolgozat egységesen úgy definiálja, mint a közvetett úton, beszállítói csatornán keresztül megvalósuló támadást; a részletes technikai definíció és címkézési szabályrendszer a 3. fejezetben szerepel.

A supply chain támadások elméleti jelentősége kettős: egyrészt a kockázat nem a végponti szervezeten belül, hanem az ökoszisztéma-kapcsolatokban keletkezik; másrészt az 1→N terjedési mechanizmus miatt a rendszerszintű kockázat nemlineárisan emelkedik. Ez a dolgozat ezért a supply chain kategóriát önálló vizsgálati tengelyként kezeli, és a 3. fejezetben kvantitatív elemzéssel is visszatér rá. A 3. fejezet 3.4 alfejezete a supply chain incidensek időbeli alakulását és a geopolitikai feszültségekkel való együttmozgását exploratív módon elemzi.

1.3. A kutatás és módszertan felépítése

1.3.1. A CISSM Cyber Incident Database

A CISSM (Center for International and Security Studies at Maryland) Maryland Cyber Events Database (MCED) egy olyan online elérhető adatbázis [76], amely részletes információkat gyűjt és rendszerez a kiberbiztonsági incidensekről. Az adatbázis különösen értékes a kiberbiztonsági kutatók számára, mivel részletes információkat tartalmaz a kibertámadásokról, beleértve az elkövetőket, célpontokat, módszereket és a támadások következményeit. Az

adatbázist a Marylandi Egyetem nemzetközi és biztonsági tanulmányok központja kezeli. Az adatbázis célja, hogy átfogó és rendszerezett információkat nyújtson a jelentős kiberbiztonsági incidensekről [15]. Az adatok között szerepelnek a támadások időpontjai, az érintett szervezetek és iparágak, az elkövetők típusai, a támadások módszerei, valamint az incidensek következményei. Az adatbázis több forrásból gyűjti az információkat, beleértve a nyilvánosan elérhető híradásokat, kormányzati jelentéseket, valamint szakértői elemzéseket. A folyamatosan frissülő adatok naprakész információkat biztosítanak a kutatók számára. Az adatbázis szerkezete több kulcsfontosságú oszlopot tartalmaz [4], amelyek az alábbi információkat tartalmazzák:

- **Dátum:** Az incidens bekövetkezésének időpontja.
- **Elkövető típusa:** Az incidens elkövetőjének kategóriája, mint például államilag támogatott csoport, bűnözői szervezet vagy hacktivista csoport.
- **Célpont:** Az érintett szervezet vagy iparág megnevezése.
- **Támadási módszer:** Az alkalmazott technika, például adatszivárgás, DDoS támadás, vagy zsarolóvírus.
- **Következmények:** Az incidens következtében felmerült károk, például pénzügyi veszteségek, adatlopás, vagy szolgáltatásmegtagadás.

A szabályozási keretek kidolgozása szempontjából kiemelkedő jelentőségű a támadási trendek mélyebb elemzése, mivel ezek az eredmények képesek azonosítani azokat a kulcsfontosságú területeket, ahol beavatkozás szükséges. Az adatbázis adatai alapján olyan szabályozási modellek alakíthatók ki, amelyek nemcsak a jelenlegi fenyegetésekre adnak választ, hanem proaktívan kezelik a jövőbeli támadási lehetőségeket is. A dolgozat a CISSM adatbázisban rögzített adatok segítségével megalapozza a későbbi nagyobb elemzéseket és prediktív modelleket.

Az elemzés során három kiegészítő, elsősorban kvalitatív validációs réteget használok. (i) A VERIS Community Database és a Verizon Data Breach Investigations Report iparági baseline-t és strukturált összehasonlítási keretet ad: ezek a források főként irány- és nagyságrendi kontrollpontként szolgálnak, incidens-szintű számítás nélkül. (ii) Az iparági fenyegetési riportok – köztük az IBM X-Force, a Mandiant M-Trends, a CrowdStrike GTR és az ENISA Threat Landscape – a trendek, a támadási komplexitás és a

supply chain sérülékenységek narratív kontextusát adják; szerepük „külső realitás-teszt”, nem pedig a modellek formális kalibrálása.

(iii) A CISA Known Exploited Vulnerabilities (KEV) katalógus az aktívan exploitált sebezhetőségek listáját adja; a dolgozatban a Komplexitási Index technikai értelmezésének kontextusaként használom (pl. VPN/RDP/gateway típusú támadási vektorok), a mutató numerikus értékei azonban kizárólag az MCED adataiból származnak.

A többforrású validációs keretrendszert az alábbi táblázat foglalja össze.

Többforrású validáció – elvi keret. A többforrású validáció célja az annotációs zaj és a forrástorzítás csökkentése. A megelőző táblázat rögzíti a három réteget (iparági baseline; fenyegetés-intelligencia riportok; technikai verifikáció), amelyhez a 3. fejezetben elsősorban kvalitatív, nagyságrendi konzisztencia-ellenőrzések és illusztratív összevetések kapcsolódnak (éves, iparági és aktortípus bontásban), formális hipotézistesztek nélkül.. Módszertani megkötés: mivel a KoI definíciója is MITRE-taktikákon nyugszik, a MITRE-t nem használom a KoI „független” validálására; itt taxonómiai és TTP-konzisztencia-auditként szolgál, míg az exploit-szintű igazolást a KEV adja.

Forrás	Típus	Erősség	Korlát	Felhasználás a dolgozatban
MCED (Maryland Cyber Events Database)	Incidensszintű, OSINT	Részletes, hosszú idősor (2014-2025)	Forrásvalidáció hiánya, médiatorzítás	Elsődleges incidens-adatbázis; KSM és KoI definiálásának és számításának alapja
VERIS Community Database (VCDB)	Strukturált JSON	Nyílt, egységes séma	Főleg publikus beküldések	Iparági struktúra és kategóriák kvalitatív összevetése az MCED-del
Verizon DBIR	Aggregált éves riport	Gold standard iparági baseline	Nagyvállalati fókusz	Aggregált trendek és iparági baseline kontextus az MCED eredményeihez
IBM X-Force Threat Intelligence	Éves fenyegetési riport	Aktuális APT és ransomware trendek	Regionális torzítás	APT- és ransomware-taktikák, komplexitási mintázatok kvalitatív illusztrációja
Mandiant M-Trends	Éves szakértői riport	Dwell time, APT kampányok	Főleg ügyfélesetek	Dwell time és APT-kampány példák; a KoI szöveges értelmezésének háttere
CrowdStrike GTR	Éves globális riport	Aktorok, nemzetállami támadások	Saját ügyfélkör fókusz	Aktorprofilok és szektoros eloszlások kvalitatív összevetése az MCED actor_type mintázataival
ENISA Threat Landscape	EU-s riport	Szektoros bontás, szabályozási kontextus	EU fókusz	Supply chain trendek és EU-s szektoros kontextus a NIS2/CER-értelmezéshez
CISA KEV katalógus	CVE lista	Exploited vulnerabilities listája	Csak technikai	Exploitált CVE-k listája; a KoI technikai értelmezésének kontextusa (VPN/RDP/gateway-típusú támadási vektorok)

Táblázat 2-Kiberbiztonsági adatforrások és jelentések összehasonlítása

Megjegyzés: a technikai verifikáció két komponense: CISA KEV (CVE-szint) + MITRE ATT&CK (TTP-audit).

A következő fejezetekben a módszertant követően bemutatott esettanulmányok közvetlenül illusztrálják a kiberfenyegetések komplexitását és súlyosságát. Ezek az esetek nemcsak az adatbázis hitelességét támasztják alá, hanem megmutatják az adatstruktúrák és a valós események közötti kapcsolatot.

1.3.2. Elemzési lehetőségek és módszertan

A CISSM adatbázis nem csupán az egyes kibertámadások technikai aspektusainak megértéséhez nyújt alapot, hanem a támadások elleni szabályozási és kontrollmechanizmusok tervezéséhez is. A részletes elkövetői profilok, célpontok és módszerek alapján a kormányzati és iparági szabályozások hatékonyabbá tehetők, mivel jobban igazodhatnak a fenyegetések valós természetéhez. Ez különösen fontos a kritikus infrastruktúrák esetében, ahol a jogszabályi keretek szoros összhangja szükséges az egyedi védelmi stratégiákkal.

Az adatbázisban található adatok számos elemzési lehetőséget biztosítanak, mint például:

- **Statisztikai elemzések:** Az incidensek gyakoriságának és trendjeinek elemzése.
- **Támadók és célpontok profilozása:** A különböző típusú elkövetők és célpontok elemzése.
- **Támadási módszerek elemzése:** A leggyakrabban alkalmazott támadási technikák feltérképezése.
- **Kockázatelemzés:** A legnagyobb kockázatot jelentő tényezők beazonosítása az incidensek következményeinek elemzése alapján.

Az adatbázis elemzése rámutatott arra, hogy a különböző iparágak és szervezetek eltérő módon érintettek a kiberfenyegetések által, és az eredmények segíthetnek a célzott védekezési stratégiák kidolgozásában. Az adatbázis segítségével azonosított támadási módszerek és elkövetői profilok hasznos információkat nyújtanak a kiberbiztonsági politikák és szabályozások kialakításához. Az adatbázisban szereplő adatok gyakorlati alkalmazásai közé tartozik a kiberbiztonsági stratégia kidolgozása, a politikai és szabályozási javaslatok előkészítése, valamint oktatási célok szolgálata. Az eredmények felhasználhatók a kiberbiztonsági védekezési stratégiák fejlesztésére, valamint a kockázatértékelési folyamatok javítására. Az oktatási intézmények számára az adatbázis kiváló oktatási eszközként szolgálhat, különösen a kiberbiztonsági képzések területén. A CISSM Cyber Incident Database elemzése során elért eredmények jelentős mértékben hozzájárulnak a kritikus infrastruktúrák védelmének fejlesztéséhez. A kutatás során alkalmazott módszertan és az adatbázisban szereplő adatok

lehetőséget biztosítanak a kiberbiztonsági stratégiák finomítására, valamint a kockázatkezelési módszerek továbbfejlesztésére. Az eredmények alapján a jövőbeni kutatásoknak továbbra is fókuszálniuk kell a kiberbiztonsági fenyegetések elemzésére és az ellenük való hatékony védekezésre.

A kiberháborús támadások során különösen veszélyeztetettek azok az eszközök és műveletek, amelyek a kritikus infrastruktúrák működését biztosítják. Ezek az infrastruktúrák képezik bármely ország gazdaságának alapját [70], így kompromittálásuk súlyos következményekkel járhat. Az iparáganként elemzés feltárta, hogy az egészségügyben és a gyártásban elsősorban a személyes adatok és adatbázisok vannak kitéve támadásoknak, míg az információs szektorban az üzemidő-csökkentés és a hálózatba kapcsolt eszközök elleni támadások dominálnak.

A Maryland Cyber Events Database[3] 2014-2024 közötti adatai szerint a legnagyobb incidencia-gyakoriság a közigazgatásban figyelhető meg, ezt követi az egészségügy és szociális ellátás, az információs szektor, valamint a pénzügy és biztosítás. Ez a mintázat egyértelműen jelzi, hogy a kibertámadók elsődlegesen azokat az ágazatokat célozzák, amelyek nagy mennyiségű szenzitív adatot kezelnek vagy alapvető közszolgáltatásokat nyújtanak. Fontos megjegyezni azonban, hogy a puszta gyakorisági adatok önmagukban nem tükrözik teljes mértékben a valós kockázatokat, mivel nem veszik figyelembe az egyes incidensek súlyosságát vagy technikai komplexitását.

Az értekezésig vezető cikkek és korábbi elemzések sokszor a nyers adatokban rejlő mintázatok feltárására irányultak. Jelen fejezet ezekre az előzetes eredményekre építve egy szintetizált, célzott és reprodukálható kvantitatív módszertant mutat be, amelynek egyetlen célja a bevezetőben felállított három hipotézis szisztematikus és empirikus tesztelése.

Az értekezés első két fejezete kvalitatív keretezéssel és esettanulmányokkal is bemutatja, hogy a kritikus infrastruktúrákat érő fenyegetések gyakorisága, intenzitása és aktortípus-profilja eltér a nem kritikus ágazatokétól. Jelen fejezet azonban már egy reprodukálható kvantitatív eljárást is bevezet be a korábban rögzített hipotézisek (H1, H2, H3) szisztematikus tesztelésére. A módszertan három, egymást erősítő pillérből áll:

1. Fogalmi operacionalizálás – az absztrakt kockázati kategóriák (súlyosság, komplexitás) megfigyelhető, replikálható változókkal és kompozit indexekkel való helyettesítése.
2. Hipotézis-tesztelés – robusztus, nemparaméteres próbák és érzékenységi vizsgálatok a kritikus/nem kritikus ágazatok közti eltérésre és a súlyosság–komplexitás kapcsolatára.

3. Felügyelt gépi tanulás – egy, szöveges és strukturált metaadatokra épülő ensemble előrejelző modell felépítése, amely korai fázisú információk alapján becsli az aktortípust.

1.3.3. Tervezési elvek és adat szeparáció

A reprodukálhatóság érdekében előre rögzített adatfeldolgozási folyamatot (pipeline) alkalmazok: (i) adat-fixálás (verzió és lenyomat), (ii) tisztítás és minőségbiztosítás, (iii) feature-képzés, (iv) hipotézis-tesztek, (v) modellépítés, (vi) független tesztelés és hibaanalízis. A prediktív modellezésnél (H3) az időbeli szeparáció elvét követem a jövőbeli információk visszaszivárgásának elkerülésére: tanítás 2014–2021, validáció 2020 (hiperparaméter-hangolás), független teszt 2022–2024. A H1 és H2 hipotézisekhez a teljes keresztmetszeti minta kerül felhasználásra, hogy a statisztikai erőt maximalizáljam.

Értékelési metrikák és robusztusság

Az actor_type többosztályú, egyensúlytalan eloszlású célváltozó. Ezért az egyszerű pontosság (accuracy) helyett a macro-F1 és a Precision–Recall görbe alatti terület (PR-AUC) a két elsődleges mutató; ezek érzékenyek a ritkább, de kritikus kategóriák (pl. *Nation-State*) helyes besorolására is.

A robusztusság érdekében:

- Ismételt, stratifikált keresztvalidációt használok a tanítási fázisban;
- minden fő teszthez érzékenységi vizsgálat készül (pl. Undetermined kezelése, iparág-aggregáció alternatívái);
- a többes tesztelés miatti alfa-inflációt Benjamini–Hochberg FDR korrekcióval kezelem;
- a prediktív kimeneteket valószínűség-kalibrációval (Platt/ISOTONIC) ellenőrzöm, hogy döntési küszöbök mellett is értelmezhetők legyenek.

1.4. A szakirodalom nyitott kérdései és a kutatás irányai

A szakirodalom kritikai áttekintése három fő kutatási rést azonosított:

(1) Gazdasági hatásmérés problémája

Anderson és társai [14] dokumentálták a kibertámadások közvetlen pénzügyi következményeinek mérési nehézségeit. Bár az incidensek száma és technikai jellemzői jól

dokumentáltak, a tényleges gazdasági károk ritkán publikusak. Ez a hiányosság motiválta a KSM proxy mutató kifejlesztését.

(2) Támadások differenciálásának hiánya

Rid [27] rámutatott, hogy a kibertámadásokat gyakran homogén kategóriaként kezelik, figyelmen kívül hagyva komplexitásbeli különbségeiket. A MITRE ATT&CK alapú KoI index ezt a rést hidalja át objektív mérőszámmal.

(3) Korlátozott prediktív képesség

A meglévő MCED-alapú elemzések - például Harry és Gallagher [4; 15] munkája értékes leíró statisztikákat nyújtanak, de nem lépnek tovább a prediktív modellezés felé. Különösen hiányzik a korai fázisú aktortípus-előrejelzés, amely kritikus lenne a proaktív védelem kialakításában. További kutatások szükségesek annak megértéséhez, hogy minimális kezdeti információból milyen megbízhatósággal jelezhető előre az aktortípus.

A dolgozat mindhárom rést célzottan kezeli: H1 a KSM-vel méri a gazdasági hatást, H2 a KoI-vel operacionalizálja a komplexitást, H3 pedig ensemble gépi tanulással teszi lehetővé a korai predikciót.

1.5.Adatok és változók forrásai és áttekintése

Az empirikus elemzés a Maryland Cyber Events Database (MCED) 2014–2025 közötti, validált adatállományára épül. A hipotézisek teszteléséhez három központi konstrukciót operacionalizálok: a Károkozási Súlyossági Mutatót (KSM), a Komplexitási Indexet (KoI) és a Kritikusság Indikátort (KrI). E mutatók részletes technikai specifikációját az M1. melléklet tartalmazza; a jelen alfejezet célja, hogy az olvasó már az esettanulmányok (2. fejezet) értelmezéséhez rendelkezzen a szükséges módszertani alapokkal.

1.5.1. Adatforrás és mintakeret

Az MCED vegyes módszertanú gyűjtést alkalmaz: Python-alapú scraping állít elő jelölteket nyílt forrásokból, majd kutatói validálás és kódolás dönti el, hogy az esemény bekerül-e a végleges állományba. A 2025. októberi kiadás a GDELT Web News NGrams 3.0 integrációjával bővült, javítva a lefedettséget és a nem angol nyelvű források detektálását.

Mintaméretek és tisztítási lépések:

Szint	Leírás	n
Nyers állomány	Teljes MCED + elgépelések normalizálása	15 789
Undetermined kiszűrve	actor_type ≠ Undetermined	15 166
Elemzési minta	Három fő aktortípus (Criminal, Hacktivist, Nation-State)	**14 938**

A Hobbyist (n = 198) és Terrorist (n = 30) kategóriákat a H3 modellből kizárom alacsony esetszámuk miatt; a H1–H2 hipotézisek tesztelése a teljes, Undetermined nélküli állományon történik.

1.5.2. Központi változók

(A) Károkozási Súlyossági Mutató (KSM, 1–5 skála)

A közvetlen pénzügyi veszteségadatok szisztematikus hiányára reagálva [14], a KSM az MCED event_subtype technikai kategóriáiból származtatott ordinális proxy változó. Kritikus módszertani garancia: a KSM kizárólag az incidens technikai jellemzőin alapul, független az érintett szektortól – ugyanaz a ransomware támadás ugyanazt a KSM-értéket kapja, függetlenül attól, hogy bankot, kórházat vagy kiskereskedelmi céget ér.

(B) Komplexitási Index (KoI, 0–4 skála)

A KoI négy bináris komponens összegeként adódik, a MITRE ATT&CK fogalmi keretéhez illesztve:

1. **Laterális mozgás** (+1): multiple_targets = "Yes" vagy leírás tartalmazza: "lateral", "pivot"
2. **Perzisztencia** (+1): duration > 30 nap vagy leírás tartalmazza: "persistence", "backdoor"
3. **Detektálás elkerülése** (+1): detection_delay > 90 nap vagy leírás tartalmazza: "stealth", "evasion"
4. **Többfázisú végrehajtás** (+1): event_type = "Campaign" vagy leírás tartalmazza: "multi-stage"

(C) Kritikusság Indikátor (KrI, bináris)

Az MCED industry mezőjét az EU NIS2 (2022/2555) és CER (2022/2557) irányelvek szektorlistái alapján binárisan osztályozom (1 = kritikus, 0 = nem kritikus).

(D) Aktortípus (célváltozó)

A H3 célváltozója három kategóriát tartalmaz: Criminal, Hacktivist, Nation-State. Az Undetermined eseteket a prediktív modell tanításából kizárom; kezelésüket reject option módszertannal oldom meg (részletek az M3. mellékletben).

1.5.3. Adatelőkészítés és minőségbiztosítás

Az adattisztítás négy lépésből áll: (1) deduplikáció azonos URL/target kombinációk összevonásával; (2) hiányzó industry értékek elvetése, motive és region hiány "Unknown" kategóriába sorolása; (3) ritka event_subtype kategóriák összevonása; (4) actor_type címkék normalizálása (pl. "Hacktvist" → "Hacktivist").

A tisztítás hatását Jensen–Shannon divergenciával ellenőriztem: a fő strukturális dimenziók (iparág, eseménytípus, célország) eloszlása gyakorlatilag változatlan maradt (JSD < 0,01 minden dimenzióban).

1.5.4. Szöveg-előkészítés a prediktív modellhez

A title és description mezőkből NLP-pipeline készül: kisbetűsítés, lemmatizálás, stop-szó szűrés, majd TF-IDF vektorizálás szó-n-gram (1–2) és karakter-n-gram (3–5) reprezentációval. Domain-specifikus lexikonok (MITRE ATT&CK kulcsszavak, ransomware-szótár) bináris feature-ökként egészítik ki a reprezentációt.

1.5.5. Időbeli szeparáció és adatintegritás

A H3 hipotézis teszteléséhez szigorú időbeli szeparációt alkalmazok a data leakage elkerülése érdekében:

Halmaz	**Időszak**	**Funkció**
Tanító	2014–2019	Modellépítés
Validációs	2020	Hiperparaméter-hangolás
Kalibrációs	2021	Küszöb- és valószínűség-kalibráció

Halmaz	Időszak	Funkció
Teszt	2022–2025	Out-of-time értékelés

A H1 és H2 hipotézisek tesztelése a teljes keresztmetszeti mintán történik, év-fix hatások alkalmazásával. A részletes reprodukálhatósági dokumentáció az M3. mellékletben található.

1.6.Adatelőkészítés és minőségbiztosítás áttekintés

A Maryland CISSM Cyber Events Database forrásadatbázis (15 789 rekord) adatminőségi problémákat tartalmazott, amelyek 98,2%-a kezelésre került: az 'Undetermined' actor_type és motive értékek szűrése (Level-1 és Level-2 tisztítás), az actor_type írásmód-variációk normalizálása, valamint az összetett event_subtype értékek kezelése a KSM számítási szabállyal. A maradék inkonzisztenciák (77 rekord, 0,62%) elhanyagolható hatással vannak az eredményekre (KSM átlag változás <0,2%). A részletes dokumentáció 3. fejezetben és a Mellékletekben található.

Az előző alfejezetekben áttekintett elméleti keretek és szakirodalmi források alapján megállapítható, hogy a kibertér megjelenése alapvetően átalakította a biztonsági gondolkodás hagyományos paradigmáit. A digitális rendszerekre épülő modern társadalmak kritikus infrastruktúrái olyan új típusú fenyegetésekkel szembesülnek, amelyek egyszerre technikai, gazdasági és stratégiai dimenziókkal rendelkeznek, és kezelésük integrált megközelítést igényel.

Az aszimmetrikus konfliktusok vizsgálata rámutat arra, hogy a kibertérben viszonylag alacsony erőforrás-ráfordítással is aránytalanul nagy hatás érhető el, különösen akkor, ha a támadások kritikus infrastruktúrákat érintenek. Az ipari vezérlőrendszerek és az üzletmenet-folytonosság szoros összefonódása miatt az ilyen incidensek hatása gyakran túlmutat az egyedi szervezeti szinten, és rendszerszintű következményekkel járhat.

A szakirodalmi áttekintés során azonosított kulcsproblémák – az attribúció bizonytalansága, a kaszkádszerű hatások kockázata és a támadások gazdasági ösztönzői – indokolják olyan kvantitatív és adatvezérelt módszerek alkalmazását, amelyek képesek az incidensek súlyosságának, komplexitásának és előrejelezhetőségének strukturált vizsgálatára. E célból a fejezet bevezette a kutatás három központi mérőszámát: a Károkozási Súlyossági Mutatót (KSM), a Komplexitási Indexet (KoI) és a Kritikusság Indikátort (KrI), valamint rögzítette az

MCED 2014–2025 közötti elemzési mintájának (n = 14 938) előkészítési és tisztítási protokollját.

A következő fejezetben empirikus esettanulmányok elemzésén keresztül mutatom be, hogy az itt vázolt elméleti megfontolások és mérőszámok miként jelennek meg a valós kiberbiztonsági eseményekben. Ezek az esetek illusztrálják a KSM és KoI gyakorlati értelmezését, megalapozzák a későbbi statisztikai és prediktív elemzéseket, és átvezetnek a 3. fejezet kvantitatív hipotézisvizsgálataihoz.

2. ESETTANULMÁNY-FÓKUSZÚ ELEMZÉSEK ÉS KÖVETKEZETÉSEK

2.1. A kiberbiztonsági események általános és eseti hatásai

Általános hatások

A kiberbiztonsági incidensek nemcsak a technológiai rendszereket érintik, hanem mélyreható gazdasági és társadalmi következményekkel is járnak, amelyek túlmutatnak az egyes szervezetek határain. E fejezet célja, hogy átfogó áttekintést nyújtson a jelentősebb kiberbiztonsági eseményekről, és kiemelje azok relevanciáját a későbbi statisztikai elemzések szempontjából. A kritikus infrastruktúrák sérülékenységeit és a kapcsolódó jogi kereteket az Európai Unió a NIS2[5] és CER[77] irányelvekben rögzíti, amelyek kijelölik a kiemelten védendő ágazatokat. Ezen irányelvek adják az értekezésben használt „kritikus” és „nem kritikus” szektorok megkülönböztetésének alapját, amely az Első hipotézis tesztelésének sarokköve.

A kiberbűnözés, különösen a ransomware támadások, mélyreható következményekkel járnak a globális gazdaságra nézve. Példaként említhető a 2021-es Colonial Pipeline incidens, amely rávilágított arra, hogy a ransomware támadások milyen súlyos hatást gyakorolhatnak a kritikus infrastruktúrára [78]. A támadás gázhiányt okozott, ami az üzemanyagárak emelkedéséhez és az alapvető árucikkek árának növekedéséhez vezetett. Wittkop szerint nem vitás, hogy a ransomware támadások komoly pénzügyi veszteségeket okoznak [79]. Azonban, a legjelentősebb következmények a személyazonosság-lopás költségeivel, a szellemi tulajdon jogainak megsértésével és a megélhetési források elvesztésével kapcsolatosak. A gazdasági következmények ugyanakkor kvalitatív kontextust adnak, de a KSM kizárólag az incidensek technikai és operációs hatását méri.

A személyazonosság-lopásból eredő károk jelentős gazdasági hatást gyakorolnak, és sok családot érintenek. Wiener [80] például azt becsüli, hogy az amerikaiak évente körülbelül 56 milliárd dollárt veszítenek személyazonossággal való visszaélés miatt. Emellett a számítástechnikai bűnözés a szellemi tulajdon elvesztéséhez is vezethet, ami különösen súlyos következményekkel járhat a fejlődő országok gazdaságaira nézve, ahol a szellemi tulajdon gyakran a gazdasági növekedés alapját képezi. Továbbá, az olyan kibertámadások, mint a 2017-es ukrajnai NotPetya, képesek jelentős mértékben megzavarni a vállalkozások működését, ami a megélhetési források elvesztéséhez vezehet azok körében, akik ezekre a vállalkozásokra támaszkodnak.

Molinari rámutatott arra is, hogy a kis- és középvállalkozások (kkv-k) különösen kiszolgáltatottak a számítástechnikai bűnözéssel szemben [81], ami súlyos társadalmi-gazdasági kihívásokhoz vezethet. Szemben a nagyvállalatokkal, a kkv-k kevésbé rendelkeznek olyan pénzügyi erőforrásokkal, amelyekkel robusztus kiberbiztonsági infrastruktúrát építhethetnének ki. Továbbá, sok kkv nem rendelkezik dedikált kiberbiztonsági részleggel, ami tovább növeli sérülékenységüket a kibertámadásokkal szemben. Molinari azt is megjegyzi, hogy a kkv-k nincsenek tisztában a ransomware támadások lehetséges hatásaival, ami ahhoz vezet, hogy kevésbé fektetnek be a megelőzésre és a következmények enyhítésére irányuló képzésbe. Ez a helyzet globális szinten is jelentős társadalmi-gazdasági következményekkel jár, mivel a kkv-k számos gazdaság gerincét képezik. A kkv-kat célzó kibertámadások világszerte közvetlen hatással lehetnek a foglalkoztatásra és a gazdasági növekedésre.

A kritikus infrastruktúrákkal kapcsolatos következmények

A kritikus infrastruktúrák jelentősége vitathatatlan a nemzetek biztonsága és a mindennapi élet folyamatossága szempontjából. Az ilyen infrastruktúrák működése szorosan összefügg az országok gazdasági, politikai és társadalmi stabilitásával[82]. A digitális korszakban, ahol az információs technológia és a hálózatépítés kulcsszerepet játszik, a kritikus infrastruktúrák sérülékenysége növekszik, különösen a kibertámadásokkal szemben. Az elmúlt évtizedekben a modern kritikus infrastruktúrák egyre inkább támaszkodnak ipari vezérlőrendszerekre (ICS) és SCADA hálózatokra, amelyek a működés automatizálását és hatékonyabb irányítását teszik lehetővé. Ezen rendszerek sebezhetősége azonban komoly biztonsági kockázatot jelent, mivel egyetlen sikeres támadás is széleskörű zavarokat okozhat, beleértve a közszolgáltatások, az energiaellátás és az ipari termelés megszakítását.

Magyarországon is egyre nagyobb figyelmet kap a kritikus infrastruktúrák védelme, különösen a digitális térben megjelenő fenyegetésekkel szemben[83]. A kibertámadások elleni védekezés kulcsfontosságú eleme a megelőző intézkedések kidolgozása, amelyek célja a rendszerek sebezhetőségének minimalizálása és a támadások gyors felismerése [84]. Az ilyen megelőző intézkedések magukban foglalják a rendszeres biztonsági auditokat, a dolgozók kiberbiztonsági képzését és a biztonsági protokollok folyamatos frissítését.

Az információs technológia rohamos fejlődésével párhuzamosan az ICS és SCADA rendszerek iránti igény növekszik, de ezzel együtt alkalmazásuk kockázatai is nőnek. A SCADA rendszerek különösen érzékenyek a hálózati alapú támadásokra, amelyek a rendszer működésének kikényszerített leállítását vagy megzavarását eredményezhetik. A kritikus

infrastruktúrák védelme nemcsak nemzeti érdek, hanem nemzetközi együttműködést is igényel, mivel a kiberfenyegetések határai nem állnak meg az országhatároknál. A supply chain típusú támadások gyakorlati kockázatát három jól dokumentált eset szemlélteti. (1) A SolarWinds/Orion frissítési csatornájának kompromittálása több száz szervezethez juttatott kártékony kódot, köztük közszféra-szereplőkhöz és kritikus szolgáltatókhoz. (2) A Kaseya VSA távoli menedzsment eszköz elleni támadás menedzselt szolgáltatókon keresztül sok tucat végszervezetben idézett elő zsarolóvírus-incidenst. (3) A NotPetya a könyvelői szoftver ellátási láncát kihasználva széles körű operációs fennakadásokat okozott több ágazatban. Ezek az esetek jól demonstrálják, hogy beszállítói láncon át a kompromittálás egyszerre több kritikus szolgáltatásban és régióban is manifesztálódhat, így a kockázatértékelésnek a közvetlen peremen túli függőségeket is le kell képeznie

2.2. Illusztratív esetek a Kár Súlyossági Mutató (KSM) és a Komplexitási Index (KoI) értelmezéséhez

A kvalitatív elemzés alátámasztására a szakirodalom és nemzetközi szervezetek által dokumentált kibertámadásokat vizsgálok meg részletesebben. Ezek az esetek reprezentálják mind a kritikus infrastruktúrák elleni közvetlen támadásokat, mind a hibrid hadviselés kontextusában értelmezett műveleteket. Az elemzés célja kettős: egyrészt demonstrálni a KSM és KoI mutatók alkalmazhatóságát az empirikus vizsgálatokban, másrészt közvetlen kvalitatív támpontokat nyújtani a H1–H3 hipotézisek értelmezéséhez. A kiválasztott esetek három csoportba sorolhatók:

- kritikus infrastruktúrát érintő támadások (BlackEnergy – 2015; WannaCry – 2017; NotPetya – 2017),
- hibrid/katonai kontextusban végrehajtott kiberműveletek (Észtország – 2007; Grúzia – 2008; Viasat – 2022),
- valamint egy regionális közműszolgáltató összeomlása (DMEA – 2021), amely átvezet a 2.3. alfejezetben tárgyalt informatikai biztonságirányítási keretek felé.

Minden esettanulmány bemutatja a támadás körülményeit, a kár mértékét és technikai összetettségét (KSM/KoI), továbbá az IBIR (Build/Monitor/Operate/Report) szemlélet szerinti szervezeti tanulságokat. A módszertani illesztés révén az egyes példák nem önálló narratívaként jelennek meg, hanem szerves részét képezik a hipotézisek tesztelésének keretrendszerében-

2.2.1 BlackEnergy —támadás az ukrán villamosenergia-hálózat ellen (2015)

A 2015. december 23-án Ukrajna nyugati részén bekövetkezett áramszünet az egyik első, nemzetközileg dokumentált bizonyítéka annak, hogy kritikus infrastruktúrák működését pusztán kibertámadás útján is tartósan meg lehet zavarni[85]. A támadás három áramszolgáltatót érintett, köztük a Prykarpattyaoblenergo társaságot. A behatolás előkészítése már 2014-ben megkezdődött: célzott adathalász levelek makrókat tartalmazó Office-dokumentumokon keresztül juttatták be a BlackEnergy kártevő variánsát, amely lehetővé tette a támadók számára a hálózaton belüli tartós jelenlét kiépítését. Az IT-rendszerekből kiindulva a támadók fokozatosan pivotáltak az operatív technológiai (OT) környezetbe, és hónapok alatt feltérképezték az ipari vezérlőrendszerek topológiáját.

Az esemény súlyossága a bevezetett Károkozási Súlyossági Mutató (KSM) alapján az 5-ös szintnek felel meg az 1–5-ös skálán, mivel kritikus infrastruktúrában következett be fizikai szolgáltatás-kiesés, amely több áramszolgáltatót és szélesebb társadalmi rétegeket érintett. A Komplexitási Index (KoI) értékét a módszertani fejezetben rögzített négy bináris komponens alapján határozom meg: perzisztencia (P), laterális mozgás (L), észlelés elkerülés (E) és többfázisú kampányjelleg (C). A KoI ezek összege (KoI = P + L + E + C), ezért 0–4 közötti értéket vehet fel. A BlackEnergy-incidens esetében mind a perzisztencia (P), mind a laterális mozgás (L), az észlelés elkerülése (E), valamint a többfázisú kampányjelleg (C) egyértelműen azonosítható, ezért a KoI értéke 4.

Az eset az Informatikai Biztonsági Irányítási Rendszer (IBIR) szempontjából is számos tanulságot hordoz. A **Build** dimenzióban az IT és OT hálózatok közötti szegmentáció hiányosságai, valamint a túlságosan engedékeny távoli hozzáférési szabályok tették lehetővé a támadás kiterjedését. A **Monitor** fázisban az ICS-protokoll szintű anomáliaészlelés és a naplózási mechanizmusok elégtelensége miatt a támadók hosszú ideig rejtve maradtak. Az **Operate** területen a vészüzemi visszakapcsolási eljárások hiánya és a többfaktoros hitelesítés be nem vezetése hátráltatta a reagálást. Végül a **Report** fázisban a késedelmes koordináció és eszkaláció okozott további fennakadásokat.

Összességében a BlackEnergy-incidens egyértelműen megerősíti a dolgozat H1 hipotézisét, amely szerint a kritikus infrastruktúrák nagyobb arányban szenvednek el magas súlyossági szintű támadásokat, valamint a H2 hipotézist is, amely az állami háttérrel végrehajtott műveletek nagyobb technikai komplexitására hívja fel a figyelmet.

2.2.2 WannaCry — globális zsarolóvírus-járvány (2017)

A 2017. május 12-én kirobbant WannaCry támadás minden korábbi ransomware-incidensnél élesebben mutatta meg, hogy egy viszonylag egyszerű, de önterjedésre képes kártevő milyen gyorsan válhat világméretű fenyegetéssé[86]. A zsarolóvírus az SMBv1 protokollban található, EternalBlue néven ismert sebezhetőséget (CVE-2017-0144) használta ki, amelyet eredetileg az amerikai Nemzetbiztonsági Ügynökség fejlesztett ki, majd a Shadow Brokers csoport szivárogtatott ki 2017 tavaszán. A támadás féregszerű terjedése négy nap alatt közel 200 000 számítógépet fertőzött meg több mint 150 országban, köztük kórházakat, közlekedési vállalatokat, ipari szereplőket és állami intézményeket.

A brit National Audit Office vizsgálata szerint a Nemzeti Egészségügyi Szolgálat (NHS) intézményeiben több mint 19 000 vizsgálatot és műtéti beavatkozást kellett elhalasztani, mivel az érintett kórházak informatikai rendszerei megbénultak, és a betegek ellátása közvetlen veszélybe került. A US-CERT riasztása technikai indikátorokkal és részletes mitigációs ajánlásokkal hívta fel a figyelmet arra, hogy a támadás nem csupán pénzügyi károkat, hanem élet- és ellátás-kritikus hatásokat is kiváltott.

A KSM értékét kizárólag az MCED event_subtype kategóriáiból levezetett, 1-5 közötti ordinális skála határozza meg; az iparági kritikusságot ettől elkülönítve a KrI_flag bináris változó (0 = nem kritikus, 1 = kritikus) jelöli. A Komplexitási Index (KoI) értéke 2 (KoI = P + L + E + C), mivel a leírás alapján laterális mozgás azonosítható (L = 1), valamint a kompromittálás → terjedés → titkosítás egymásra épülő végrehajtása kampányjellegként értelmezhető (C = 1), ugyanakkor perzisztencia (P = 0) és észlelés elkerülés (E = 0) nem domináns. Ez a paradoxon – az alacsony komplexitás mellett elért extrém hatás – fontos kvalitatív támpontot ad a súlyossági különbségek értelmezéséhez, és megerősíti a H1 hipotézis relevanciáját.

Az Informatikai Biztonsági Irányítási Rendszer (IBIR) szempontjából több tanulság vonható le. A **Build** fázisban a sebezhetőségek időben történő befoltozása és a következetes patch-menedzsment hiánya tette lehetővé a fertőzés villámgyors terjedését. A **Monitor** dimenzióban a hálózati anomáliák – például az intenzív port-scan aktivitás és az SMB-forgalom szokatlan mintázatai – észlelésének elmaradása bizonyult kritikus hibának. Az **Operate** fázisban a hálózati mikro-szegmentáció hiánya segítette a kártevő laterális terjedését, míg a **Report** területen pozitív példaként említhető a globális threat-intelligence közösség gyors információ-megosztása, amely végül hozzájárult a károk mérsékléséhez.

2.2.3 NotPetya — supply-chain kompromittálás és globális kaszkád (2017)

A 2017. június 27-én indult NotPetya támadás a kiberbiztonság történetének egyik legköltségesebb és legpusztítóbb incidenseként vált ismertté. Bár első ránézésre zsarolóvírusnak tűnt, hamar kiderült, hogy valójában wiper jellegű kártevőről volt szó, amelynek elsődleges célja a visszafordíthatatlan adatmegsemmisítés, nem pedig a váltságdíj beszedése volt. A támadás innovációja abban állt, hogy a fertőzés terjesztésére a támadók egy széles körben használt ukrán könyvelőszoftver, a MeDoc legitim frissítési csatornáját kompromittálták. Ez a supply-chain vektor különösen veszélyessé tette az incidenst, hiszen minden olyan szervezet, amely a frissítést automatikusan telepítette, a támadás áldozatává vált, függetlenül saját biztonsági intézkedéseitől.

Az ellátási lánc kompromittálásának következményei példátlan kaszkádhatásokat eredményeztek a globális gazdaságban. A Maersk hajózási vállalatnál mintegy 4 000 szerver és 45 000 számítógép vált működésképtelenné, aminek következtében a vállalat tíz napra elveszítette logisztikai kapacitásának jelentős részét. A Merck gyógyszergyártó 1,3 milliárd dollár veszteséget könyvelt el a termelési és ellátási lánc megszakadásai miatt, míg a FedEx TNT részlege hetekig csak korlátozott kapacitással tudott működni. Konzervatív becslések szerint a teljes globális kár meghaladta a 10 milliárd dollárt, ezzel a NotPetya a kiberbiztonsági incidensek történetének egyik legdrágább eseményévé vált[75].

A Károkozási Súlyossági Mutató (KSM) értéke (1-5-as skálán) 5, tekintettel a globális léptékű, tartós szolgáltatás-kiesésekre, a visszafordíthatatlan adatmegsemmisítésre és a több iparágra és földrészre kiterjedő kaszkádhatásokra. A Komplexitási Index (KoI) értéke 4 (KoI = P + L + E + C), mivel a támadás perzisztenciát (P), kiterjedt laterális mozgást (L), észlelés elkerülést (E) és többfázisú kampányjellegű végrehajtást (C) egyaránt mutatott. A NotPetya-incidens így egyszerre illusztrálja a H1 hipotézist – a kritikus és kvázi-kritikus szektorok extrém súlyossági kitettségét – valamint a H2 hipotézist, amely a nemzetállami hátterű támadások magas technikai komplexitására vonatkozik.

Az Informatikai Biztonsági Irányítási Rendszer (IBIR) szempontjából a NotPetya különösen tanulságos. A **Build** dimenzióban alapvető hiányosság volt a beszállítói integritás-ellenőrzés és a kódaláírás-validáció elmaradása, valamint a frissítési csatornák sebezhetősége. A **Monitor** fázisban a frissítési folyamatok anomáliáinak és a tömeges, szimultán fertőzési mintázatoknak a késedelmes észlelése akadályozta a gyors reagálást. Az **Operate** szempontból a blast-radius minimalizálás – különösen a hálózati szegmentáció és a jogosultságkezelés – elégtelensége súlyosbította a következményeket. A **Report** dimenzióban a supply-chain típusú incidensek

központi bejelentésének és az indikátorok (IOC) gyors nemzetközi megosztásának hiánya mutatkozott meg, ami tovább fokozta a globális kár mértékét.

A jogosultságok szigorúan arra a területre korlátozódnak, amely a felhasználó munkavégzéséhez szükséges. Előfordulhat, hogy egy adott munkafolyamathoz csak az adatok olvasására van szükség, és például az adatműveletek is jogosultságfüggőek [87]. További alapvető elvárás, hogy biztosítani kell az informatikai rendszerben lévő adatok integritását, vagyis meg kell akadályozni az illetéktelen módosításokat. Az adat megbízhatóságát csak akkor lehet biztosítani, ha egyértelműen bizonyítható, hogy az adat attól a forrástól származik, akitől várják, és a forrás hitelessége egyértelmű [88].

Az integritás fenntartása érdekében egyértelműen dokumentálni kell, hogy mikor és milyen változtatások történtek a rendszerben. Ez biztosítja, hogy jogosultság nélkül senki ne tudjon adatot beszúrni, módosítani vagy törölni. Ezenkívül szavatolni kell azt is, hogy az adatbirtokos hozzáférjen a rendszereihez és adataihoz szükség szerint.

A NotPetya így egyszerre illusztrálja a H1 és H2 hipotéziseket: egyrészt kritikus és kvázi-kritikus szektorokban extrém súlyosságú incidens következett be, másrészt a támadás komplexitása és összehangoltsága állami hátterű szereplőre utal, amely a kifinomult módszereket a geopolitikai célok szolgálatába állította.

A NotPetya a supply chain típusú támadások paradigmatikus példája volt, mivel a kompromittált MeDoc frissítési csatornán keresztül legitim szoftverfrissítésbe rejtve fertőzte meg a célzott szervezetek ezreit világszerte.

2.2.4 Delta-Montrose Electric Association (DMEA) — tömeges adat- és rendszerkiesés egy regionális közműnél (2021)

2021. november 7-én a coloradói DMEA energetikai vállalatot olyan támadás érte, amely a belső hálózati rendszerek ~90%-át érintette, és kb. 25 évnyi historikus üzleti adat elvesztéséhez vezetett. Az ügyfélszolgálat, a fizetési és számlázási rendszerek átmenetileg működésképtelenné váltak; az ügyfelek nem tudtak fizetni, és támogatás sem volt elérhető[89].

A Károkozási Súlyossági Mutató (KSM) értéke (1–5-ös skálán) a 4–5 tartományba esik, mivel a támadás kiterjedt adatvesztést és működéskiesést okozott egy regionális közműnél, ugyanakkor nem járt országos vagy globális kaszkádhatással. A Komplexitási Index (KoI) értéke 2 (KoI = P + L + E + C), mivel a támadás során korlátozott laterális mozgás (L) és

alapvető észlelés-elkerülési elemek (E) voltak azonosíthatók, míg perzisztencia (P) és többfázisú kampányjelleg (C) nem mutatkozott. Az eset ezzel jól elkülöníthető a nemzetállami hátterű, magas komplexitású támadásoktól, miközben a kritikus infrastruktúrák működési sérülékenységét empirikusan alátámasztja.

Rendszer- és szabályozási tanulságok (IBIR)

Build: mentési-architektúra és változhatatlan (immutable) backup-réteg hiánya; szegmensszintű hozzáférés-kontroll és szerepkörök részleges lefedettsége.

Monitor: adatmegsemmisítési és titkosítási minták (mass file ops, VSS törlés) késői észlelése; naplózási és riasztási lánc hiányosságai.

Operate: helyreállítási idők (RTO/RPO) meghatározása és gyakorlása nem volt arányos a szervezet kitettségével; üzleti folyamatok (billing, CRM) manuális eszkalációs tervei hiányosak.
Report: incidenskezelési eljárások részben dokumentáltak; külső partnerek és beszállítók (pl. számlázási szolgáltatók) bevonásának késedelme.

Szabályozási következmény: helyi/közműszektorbeli iránymutatások a biztonsági mentések, helyreállítási gyakorlatok és beszállítói kockázatkezelés szigorítására.

Hosszú távú hatások. A közműszektorban felgyorsította a mentési rétegek (3-2-1, offline/air-gapped) bevezetését, a helyreállítási gyakorlatok rendszeresítését, valamint a beszállítói (third-party) és felhőszolgáltatói kitettségek célzott auditját.

2.2.5. Esettanulmányok konklúzió

Több tényező is szerepet játszhatott abban, hogy a Delta-Montrose Electric Association (DMEA) esetében nem maradt a helyreállítás lehetővé tévő biztonsági mentés vagy archivált adat a támadás után [89]. A következő pontokban összefoglalom milyen lehetséges hiányosságok vezethettek ilyen mértékű károk elszenvedéséhez:

1. Kritikus rendszerek biztonsági mentésének hiánya: Egyes szervezetek a költségek minimalizálása vagy a korlátozott erőforrások miatt nem készítenek rendszeres mentéseket. Ez különösen igaz lehet kisebb szervezetekre vagy közüzemi vállalatokra, amelyek nem rendelkeznek nagy költségvetéssel a kibervédelemre.

2. Nem megfelelő backup-stratégia: A mentések ugyan létezhettek, de nem voltak megfelelően elkülönítve az elsődleges hálózattól. Ha a mentéseket ugyanazon hálózaton tárolják, amelyet a

támadók kompromittálnak, akkor ezek is hozzáférhetővé válnak, és akár törölhetők vagy titkosíthatók.

3. Hiányzó offline vagy air-gapped mentések: Az egyik legjobb gyakorlat az, hogy a biztonsági mentéseket air-gapped rendszerben tárolják, vagyis teljesen elkülönítve az aktív hálózattól. Ha a DMEA nem rendelkezett ilyen offline mentésekkel, akkor a támadók könnyen elérhették az összes adatot.

4. Elavult mentési eljárások: Elképzelhető, hogy a DMEA nem korszerűsítette a mentési eljárásait. Az elavult vagy nem rendszeresen tesztelt mentési rendszerek a támadás során használhatatlannak bizonyulhatnak.

5. Mentések titkosítása vagy törlése elleni védelem hiánya: A ransomware-támadások egyik tipikus célpontja a mentések törlése vagy titkosítása. A támadók érdeke, hogy célzottan hozzáférhetetlenné tegyék a mentési adatokat, maximálisan kiszolgáltatottá téve ezzel a szervezetet, hogy így növeljék a váltságdíj kifizetésének valószínűségét. A DarkSide vagy más fejlett fenyegető szereplők gyakran kifejezetten a biztonsági mentések keresésére és megsemmisítésére specializálódnak.

A DMEA eset tanulsága, hogy a biztonsági mentések és az archiválások megfelelő kezelése kiemelt fontosságú prioritás, különösen a kritikus infrastruktúrák esetében. A szervezeteknek törekedniük kell:

Többszintű mentési stratégiák kialakítására (például a 3-2-1 szabály alkalmazása: 3 példány, 2 különböző eszköz, 1 offline tárolás).

Rendszeres tesztelések végrehajtására, annak biztosítása céljából, hogy a mentések ténylegesen visszaállíthatók.

Rendszerek folyamatos frissítésére és a legjobb gyakorlatok betartására.

Ezek a lépések elengedhetetlenek ahhoz, hogy hasonló esetekben a szervezetek gyorsabban és hatékonyabban reagálhassanak.

Az itt bemutatott esettanulmányok és példák nem csupán a kritikus infrastruktúrák sebezhetőségére világítanak rá, hanem előkészítik a statisztikai trendek és korrelációk részletes vizsgálatát is, amelyek a kiberbiztonsági stratégiák fejlesztéséhez vetnek alapot. A bemutatott példák arra is rávilágítanak, hogy a szabályozási intézkedések szerves részét képezik a kiberbiztonsági stratégiák kialakításának. A támadások technikai aspektusainak elemzése

eredményeivel olyan normák és irányelvek kidolgozását segítik elő, amelyek hozzájárulnak a sebezhetőségek csökkentéséhez, így a kritikus infrastruktúrák védelmének fokozásához.

A CISSM adatbázis és az esettanulmányok bemutatása kiemeli a kritikus infrastruktúrák sérülékenységét, valamint a kiberfenyegetések súlyosságát. Ezek az eredmények megalapozzák a dolgozat további elemzéseit, és egyértelmű irányokat mutatnak a jövőbeli kutatások számára. Az esettanulmányok tanulságai elősegítik a védelmi stratégiák hatékonyságának növelését, és aláhúzzák a kritikus infrastruktúrák kiberbiztonságának fontosságát a globális stabilitás szempontjából.

A bemutatott esettanulmányok nem elszigetelt incidensek, hanem a kutatás központi hipotéziseit alátámasztó empirikus bizonyítékok. A Colonial Pipeline és a DMEA esetek, egyes bemutatott gazdasági és társadalmi következmények kvalitatív kontextust biztosítanak az esettanulmányok értelmezéséhez; a Károkozási Súlyossági Mutató (KSM) ezzel szemben kizárólag az incidensek technikai és operációs hatását méri az MCED event_subtype kategóriái alapján. Ezzel párhuzamosan a szaúdi és ukrán energetikai rendszerek elleni kifinomult műveletek (Shamoon, BlackEnergy) a H2 hipotézis relevanciáját emelik ki, amely a nemzetállami szereplők által feltételezhetően alkalmazott magasabb komplexitású technikákra fókuszál. Ezen esetek kvalitatív elemzése teremti meg a kontextust a 3. fejezetben következő kvantitatív vizsgálatokhoz.

Ugyanakkor a bemutatott esettanulmányok rávilágítanak egy központi módszertani kihívásra: a kibertámadások által okozott károk rendkívül heterogének, miközben a pontos pénzügyi veszteségadatok csak kivételes esetekben publikusak. E probléma áthidalására, valamint az incidensek hatásának összehasonlítható mérésére a kutatás egy proxy változót vezet be, a Károkozási Súlyossági Mutatót (KSM). A KSM egy 1–5 közötti ordinális skála, amely kizárólag az MCED event_subtype technikai kategóriái alapján méri az incidensek technikai és operációs hatását; az iparági kritikusságot ettől elkülönítve a KrI bináris változó kezeli. A kategóriák és definíciók a CISSM kódolási útmutató szerint értendők.

2.3. Az informatikai biztonságirányítás szerepe és működtetése

A korábbi fejezetek áttekintették a kritikus infrastruktúrák elleni kibertámadások természetét, valamint a kapcsolódó irodalmi forrásokat és definíciókat. Bemutattam a legfontosabb módszertani megközelítéseket, és esettanulmányok révén részletesen megvizsgáltam a releváns időszak legjelentősebb kiberbiztonsági eseményeit.

A jelen fejezet célja, hogy mélyebben elemezze a kritikus infrastruktúrák informatikai biztonságirányításának kiépítését és működtetését, és megvizsgálja, hogyan járulhat hozzá a proaktív és elkötelezett szabálykövetés a kibertámadások megelőzéséhez, valamint az okozott károk mérsékléséhez. A fejezet bemutatja azt a saját kutatás során kifejlesztett mintázatkereső eljárásrendszert, amely a begyűjtött adatok alapján olyan védelmi stratégiák alapjául szolgálhat, amelyekkel az energiaszektor és más kritikus infrastruktúrák növekvő fenyegetettségei hatékonyan kezelhetők.

Fontos kiemelni, hogy a következő szakaszokban bemutatott, MCED adatokra épülő elemzés nem csupán egy konkrét eset tanulmányozását jelenti, hanem egy átfogó, kölcsönös kontextust biztosít a kiberbiztonsági irányítás számára. Az elemzés célja, hogy átfogó képet adjon a jelenlegi kiberfenyegetési trendekről, valamint az ezekkel szemben alkalmazott védelmi intézkedések hatékonyságáról.

A rendszerezett adatok elemzése lehetővé teszi a trendek azonosítását és a hipotézisek tesztelését. Az energiaszektor és a közszolgáltatások esetében látható, hogy ezek az iparágak preferált célpontokká váltak a kiberfenyegetések szempontjából. A "Szándékosság" oszlop adatai rávilágítanak arra, hogy a szándékos támadások aránya magas, ami az ilyen típusú incidensek prevalenciáját és kifinomultságát jelzi.

A szabványok alapján - amennyiben elérhetők ilyenek - a törvényi előírások betartása mellett lehetősége van egy szervezetnek, hogy kiépítse a saját informatikai támogatása működésének biztonságáért felelős rendszerét. Ennek a rendszernek a megnevezésére a magyar gyakorlatban elterjedt Informatikai Biztonsági Irányítási Rendszer (IBIR) elnevezést használom.

A kiépítés lépései

A kibertámadások gyakoriságának és súlyosságának elemzése kritikus lépés az IT biztonságirányítási rendszerek fejlesztéséhez, amelyek nemcsak a törvényi előírásoknak való megfelelést, hanem az intézmények proaktív védelmét is szolgálják. A következőkben az IBIR kiépítésének lépéseit fogom részletezni, különös tekintettel arra, hogy az ilyen rendszerek hogyan tudják megóvni az információs infrastruktúrát és elősegíteni a gyors reagálást bármely jövőbeni kiberfenyegetés esetén.

A kibertámadások gyakoriságának és súlyosságának elemzése alapvető az IT-biztonságirányítási rendszerek fejlesztésében, mivel nemcsak a törvényi megfelelést, hanem a proaktív védelmet is szolgálják. Az IBIR kiépítésének főbb lépései:

1. lépés: Kiindulási helyzet felmérése

Az első lépés a szervezet biztonsági állapotának értékelése. Bár rendszer szinten nem mindig teljeskörű a védelem, egyes mechanizmusok jellemzően már működnek [90]. A felmérés átfogó képet ad arról, mely területek megfelelően védettek, és hol mutatkoznak hiányosságok [91].

2. lépés: Kockázatelemzés

A kockázatelemzés célja a sérülékenységek és a fenyegető tényezők közötti összefüggések feltárása. A folyamatot nehezíti, hogy:

a) nem ismerhetők előre az összes veszélyforrás,

b) a bekövetkezési valószínűségek csak közelíthetők,

c) a várható kár mértéke sokszor bizonytalan [92]:

A gyakorlatban a szakemberek listát készítenek a veszélyforrásokról, meghatározzák a valószínűségi kategóriákat és a becsült kárértékeket [39]. A fő kérdések: milyen sérülékenységek okozzák a problémát, mely információelemek érintettek, hogyan hat az esemény a CIA-háromszög (bizalmasság, sértetlenség, rendelkezésre állás) dimenzióira, és mekkora a bekövetkezés valószínűsége.

3. lépés: Elemzési módszerek

A komplex hatásláncok feltárására a hibafa-elemzés (Fault Tree Analysis – FTA) használható [93]. Ezt a módszert a Bell Telephone Laboratories fejlesztette ki 1962-ben, majd a Boeing továbbfejlesztette, és sikeresen alkalmazták például a nukleáris biztonság területén (WASH-1400 jelentés, 1974)[94]. A hibafa-elemzés a logikai kapcsolatok (ÉS, VAGY, NEM) segítségével azonosítja a minimális kritikus láncokat, ahol a legkisebb számú hiba is súlyos következményekhez vezethet [95].

Az eseményfa-elemzés (Event Tree Analysis – ETA) a hibafához hasonlóan működik, de a kiindulási esemény lehetséges kimeneteit követi végig. Ezáltal feltárja a rendszeren belüli kölcsönhatásokat, és minőségi vagy mennyiségi módon értékeli a hatásokat [110].

4. lépés: Kockázatok értékelése és kezelése részletekben

A fenyegetések valószínűsége és a lehetséges kár alapján minden eseményt értékelni kell, majd a vezetés dönt arról, hogy megelőző intézkedéseket hoz, vagy inkább helyreállításra készül fel

[47]. A strukturált veszélyforrás-táblázatok segítik a kategorizálást és a későbbi beavatkozási pontok kijelölését.

Az első lépés annak megállapítása, hogy milyen az adott szervezet kiindulási biztonsági helyzete[92]. Bár rendszer szinten esetleg nem teljeskörű a védelem, bizonyos védelmi mechanizmusok biztosan működnek már [90]. A felmérés során szerzett átfogó kép lehetővé teszi a védelmet tervező szakemberek számára, hogy pontosan megismerjék az adott időpontban fennálló információbiztonsági helyzetet. Az illetékes szakember felmérve a védendő informatikai támogatást, pontos rálátást kap azokra a területekre, amelyek megfelelően védettek és szabályozottak, valamint azokra is, ahol ez a védelem nem éri el a kívánt szintet, vagy esetleg még hiányzik [96].

Kockázatelemzés és hipotézisekhez való kapcsolódás

A kockázatelemzés az IBIR kiépítésének kulcsfontosságú eleme, amely nemcsak a sérülékenységek feltárására, hanem a fenyegetések és a működési kockázatok közötti összefüggések feltérképezésére is szolgál. Az elemzési folyamat tudományos értékét az adja, hogy kvantitatív és kvalitatív módszerekkel is képes közelíteni a valószínűségeket és a potenciális károkat, ezáltal közvetlenül hozzájárul a kutatás hipotéziseinek értékeléséhez.

Az első hipotézis és vele kapcsolatban feltett alkérdés – miszerint a ransomware támadások aránytalanul nagy gazdasági és működési károkat okoznak – kockázatelemzési szempontból abban nyer megerősítést, hogy ezen támadások valószínűsége közepesen magasra, míg a hatásuk kiemelkedően magasra értékelhető. Ez a súlyossági aránytalanság indokolja a proaktív védelmi intézkedések elsődlegességét. A második hipotéziskör (H2) – amely a nemzetállami szereplők által feltételezhetően alkalmazott kifinomult módszerekre irányul – szintén illeszkedik a kockázatelemzési logikához, hiszen az államilag támogatott támadások alacsonyabb gyakoriság mellett is rendkívül nagy hatással járhatnak, így magas kockázati szintet képviselnek.

A kockázatelemzés tehát hidat képez a kvalitatív esettanulmányok és a kvantitatív modellezés között: a feltárt sérülékenységekhez rendelt valószínűségek és kárértékek alapján számszerűsíthetőek azok a trendek, amelyek a dolgozatban bevezetett KSM (Károkozási Súlyossági Mutató) modellben testesülnek meg.

Bekövetkezési valószínűségek, gyakoriságok és a lehetséges károk számítása

A kockázatok és hibák kiértékelésének egyik legfontosabb módja a bekövetkezési valószínűségek, gyakoriságok és a várható károk szisztematikus számítása. Ez a megközelítés lehetőséget ad arra, hogy a szervezet ne csupán kvalitatív szempontok alapján, hanem számszerűsített mérőszámok mentén is képes legyen priorizálni a kockázatokat. A rendkívüli események gyakoriságának meghatározásához ideális esetben a szervezet saját korábbi adatbázisa nyújt alapot; amennyiben ez nem áll rendelkezésre, iparági statisztikák és hasonló működési területeken gyűjtött adatok képezhetik a becslés alapját. A kárértékek számítását a CIA-háromszög (bizalmasság, sértetlenség, rendelkezésre állás) dimenzióiban célszerű elvégezni, amelynek eredményei a vezetői döntések számára közvetlen inputként szolgálnak.

A lehetséges fenyegetések azonosítását segíti a veszélyforrások strukturált táblázatba rendezése. A kategorizálás során célszerű az egyes fenyegetéseket típus szerint (pl. személyi, technikai, szervezeti) megjelölni, és kódokkal ellátni (pl. SZ1 = első személyi fenyegetettség). Ez a módszer növeli az átláthatóságot, és elősegíti a későbbi azonosítást és elemzést. A konkrét védelmi intézkedések hozzárendelése lehetővé teszi, hogy minden egyes eseményhez valószínűségi és hatásértékek kapcsolódjanak [45].

A bekövetkezési valószínűségek és károk számszerűsítése szorosan illeszkedik a dolgozat hipotéziseihez is. A H1 hipotézis – empirikus alátámasztást nyernek azáltal, hogy ezek az események a valószínűség–hatás mátrixban rendszerint a „ritka, de extrém hatású” kategóriába esnek. A H2 hipotézis – amely a nemzetállami aktorok kifinomult támadási módszereire vonatkozik – szintén értelmezhető ebben a keretrendszerben: az ilyen támadások előfordulási valószínűsége alacsonyabb, ugyanakkor a potenciális kár szintén a legmagasabb értékkategóriába sorolható.

Ez a módszertan tehát nemcsak a kockázatok rangsorolását teszi lehetővé, hanem közvetlenül hozzájárul a hipotézisek értékeléséhez is, mivel számszerűsíthetővé válik a támadások gyakoriságának és hatásának aránytalansága. A strukturált kockázati táblák és a CIA-háromszög dimenzióiban végzett elemzés biztosítják azt a kvantitatív alapot, amelyre a prediktív modellek és a Károkozási Súlyossági Mutató (KSM) is épülhet.

A lehetséges veszélyforrások listázásának módját a 4. táblázat mutatja. A kitöltési minta a szöveg korábbi, az elemzési módszereket bemutató részein alapszik, különös tekintettel a kiberbiztonsági események elemzésére vonatkozó módszertanokra. Ez alapján létrehozható egy strukturált és részletesebb táblázat, amely konkrétabb információkat nyújt a lehetséges fenyegetésekre.

Típus	Veszélyforrás	Bekövetkezés valószínűsége	Támadási potenciál	Kár típusa	Kár érték	Védelmi intézkedés
SZ1	Social engineering (például adathalászat)	Magas	Közepes	Bizalmasság megsértése, adatszivárgás	Magas (személyes adatok ellopása)	Többlépcsős hitelesítés, rendszeres alkalmazotti képzés
SZ2	Ransomware támadás	Közepes	Magas	Szolgáltatás-kiesés, adatvesztés	Nagyon magas (üzemleállás, pénzügyi veszteség)	Adatmentés, behatolásmegelőző rendszerek, rendszeres frissítések
SZ3	Insider threat (belső fenyegetés)	Alacsony	Magas	Bizalmasság, sértetlenség, rendelkezésre állás megsértése	Közepes (érzékeny információk manipulálása)	Hozzáférés-szabályozás, naplózás, belső auditok
SZ4	DDoS támadás	Közepes	Közepes	Szolgáltatás-kiesés	Magas (szolgáltatás elérhetetlensége)	Túlterhelés elleni védelem, felhőalapú skálázhatóság
SZ5	Malware (rosszindulatú szoftver)	Magas	Közepes	Adatvesztés, rendszerleállás	Nagyon magas (üzleti működés leállása)	Víruskeresők, rendszeres biztonsági frissítések
SZ6	Adatszivárgás (Data breach)	Közepes	Magas	Bizalmasság megsértése, adatvesztés	Nagyon magas (személyes és üzleti adatok ellopása)	Titkosítás, hozzáférés-kezelés, adatvédelmi irányelvek

Táblázat 3 - Egyénileg meghatározott dimenziók mentén és egyedi értékelések elvégzését követően előálló kiberbiztonsági elemzési mátrix minta

Nagyon fontos megadni milyen valószínűséggel következhet be egy adott veszélyforrás miatt a rendkívüli esemény. A valószínűségi becslés elkészítéséhez ideális esetben a kapcsolódó korábbi adatok is felhasználhatók..

Eredmény-alapú kockázatértékelés és a hipotézisek vizsgálata

A kockázatkezelés nem állhat meg a veszélyforrások felsorolásánál vagy a bekövetkezési valószínűségek becslésénél. Az eredmény-alapú megközelítés lényege, hogy számszerűen bemutassa: egy kibertámadás milyen valós, mérhető következményekkel járhat a kritikus infrastruktúrákban. Például egy országos energiaszolgáltató SCADA-rendszerének kompromittálása nemcsak órákra okozhat teljes áramkimaradást, hanem több milliárd forintos közvetlen gazdasági kárt, amelyhez társulhatnak másodlagos hatások: ipari termeléskiesés, kórházak működésképtelensége, közlekedési hálózatok bénulása, valamint a lakosság bizalmának tartós megrendülése.

Ez a megközelítés közvetlenül alátámasztja a dolgozat **H1 hipotézisét**, amely a ransomware és más zsaroló támadások aránytalanul nagy hatására mutatnak rá. Egy ilyen támadás a

bekövetkezési valószínűség szempontjából közepes kockázatnak tűnhet, ugyanakkor a hatása extrém: több nagyságrenddel haladhatja meg a normál működéskiesés költségeit. Az eredmény-alapú értékelés tehát kézzelfoghatóvá teszi, hogy miért okoznak a ransomware-támadások sokszorosan nagyobb károkat, mint más kiberincidensek.

Ugyanakkor a módszer rávilágít a **H2 hipotézis** relevanciájára is: a nemzetállami aktorok kifinomult támadásai – például egy célzott SCADA-manipuláció, amelynek következtében árvízvédelmi gátak nyílnak meg, vagy olajvezetékek nyomása ugrásszerűen megváltozik – nem pusztán pénzügyi károkat jelentenek, hanem súlyos, akár emberéleteket is veszélyeztető következményekkel járhatnak . Ezek az esetek alacsonyabb gyakoriság mellett is a kockázati mátrix legfelső, „ritka, de katasztrofális" kategóriájába tartoznak, megerősítve, hogy a nemzetállami támadások értékelése során a hatást kell kiemelten kezelni.

Az eredmény-alapú kockázatértékelés ezért a kutatás hipotéziseinek empirikus teszteléséhez is hozzájárul. Lehetővé teszi, hogy a vizsgálat túlmutasson az elméleti valószínűségeken, és számszerűen igazolja a hipotézisek állításait: a ransomware támadások súlyossága aránytalan (H1), a nemzetállami aktorok támadásai pedig a legkritikusabb kockázati kategóriába tartoznak (H2).

Kockázatkezelési intézkedések

A kockázatkezeléssel kapcsolatos intézkedések célja az informatikai támogatást érintő, a tűrési határnál nagyobb hatással lévő biztonsági kockázatoknak olyan szintre csökkentése, hogy az így kapott eredmény a szervezet számára elfogadható legyen. A kockázatkezelés során kidolgozott, kockázatokkal kapcsolatos eljárási lehetőségeket dokumentálni, végrehajtásukat szabályozni kell. A kockázatkezeléshez kapcsolódó feladatokat és felelősségek meg kell határozni.

Egységes elvek alapján kell kiválasztani a lehetséges eljárások közül az adott kockázat kezelésére legalkalmasabbat. Az elsődleges választható eljárás a szervezetet érintő kockázatok tudatos, objektív felvállalása. Ehhez szükséges az, hogy a felvállalt kockázatok eleget tegyenek az adott szervezet által meghatározott kockázatelfogadási kritériumoknak. Egy, a szervezet által meghatározottnál kisebb eséllyel fellépő, csekélyebb kárértékkel járó kockázatnál érdemesebb a károk minél előbbi felszámolására koncentrálni, mint a megelőzésre. [97]

A kockázatok kezelésének egy további lehetséges módja az adott szervezet esetén fennálló kockázatok elkerülése. Az ilyen típusú eljárásoknak a lényege az, hogy az adott szervezet az

adott kockázat által érintett szolgáltatásokat nem használja. [98] Ilyen eljárás lehet az Internet használatának korlátozása, azaz, ha a felhasználó nem látogat bizonyos oldalakat, nem fog találkozni bizonyos kéretlen alkalmazásokkal. Az informatikai rendszerrel kapcsolatos kockázatok elkerülésének taktikáját azokban az esetekben lehet érdemes használni, amikor vagy más válasz nem adható az adott kockázatra, vagy a kockázat egy kívánt szint alá csökkentésre nincsenek költséghatékony módszerek.

Kiberbiztonsági reagálás és kezelés

A kiberfenyegetések növekvő mértékű előfordulása miatt számos szervezet rendelkezik kiberbiztonsági stratégiával. A kutatások azonban azt mutatják, hogy a kiberbiztonsági stratégia önmagában nem elegendő. A több szerző is amellett érvel, hogy a kiberbiztonsági stratégia akkor működhet jól, ha proaktív[99] [100]. A proaktív kiberbiztonsági stratégia a fenyegetések előrejelzésére és a fenyegetések bekövetkezése előtti lépésekre összpontosít. A kiberbiztonság proaktív megközelítését alkalmazó szervezetek csökkenthetik a kockázatokat és megelőzhetik a potenciális fenyegetéseket. A proaktív megközelítés kiemelt jelentőségű a kiberbiztonsági támadások lehetséges gazdasági, társadalmi és pénzügyi következményei miatt[101]. A proaktív és reaktív megközelítések részletes összehasonlítását az M4 melléklet tartalmazza. [99].

Biztonságpolitika

A biztonságpolitika az informatikai biztonságirányítás alapja: kijelöli a védendő értékeket, meghatározza a kockázatvállalási szinteket, és rögzíti a szervezet működését biztosító fő irányelveket [90]. Kritikus infrastruktúrák esetében ez különösen fontos, hiszen a villamosenergia-, a víz- vagy az egészségügyi ellátás folyamatosságának megőrzése társadalmi érdek. A biztonságpolitika tehát nem pusztán adminisztratív dokumentum, hanem stratégiai eszköz is, amely segíti a szervezetet a ransomware-támadások aránytalan gazdasági és működési hatásainak mérséklésében (H1, valamint a ritkább, de katasztrofális következményekkel járó nemzetállami fenyegetések kezelésében (H2).

A biztonságpolitika kidolgozása során alapvető fontosságú a szervezet kritikus üzleti folyamatainak azonosítása és priorizálása. Ez magában foglalja az egyes rendszerkomponensek közötti függőségi viszonyok feltérképezését, a kaszkád-hatások elemzését, valamint a potenciális támadási vektorok részletes értékelését. A modern kiberfenyegetési környezetben

ugyanis nem elegendő csupán a hagyományos IT-infrastruktúra védelmére koncentrálni - az OT (operációs technológiai) rendszerek, az IoT-eszközök és a felhőalapú szolgáltatások integrációja új kihívásokat teremt. A biztonságpolitikának ezért holisztikus megközelítést kell alkalmaznia, amely figyelembe veszi a konvergált IT/OT környezetek sajátosságait, a hibrid felhőarchitektúrák komplexitását, valamint a beszállítói láncok által generált kockázatokat. Ez a megközelítés különösen releváns a kritikus infrastruktúrák esetében, ahol egyetlen sikeres támadás dominóhatást indíthat el, amely több szektort is érinthet.

A kockázatalapú megközelítés alkalmazása lehetővé teszi a védelmi erőforrások optimális allokációját. A biztonságpolitikának meg kell határoznia azokat a küszöbértékeket és toleranciaszinteket, amelyek mentén a szervezet a különböző típusú kockázatokat kezeli. Ez különösen fontos a ransomware-támadások kontextusában, ahol a váltságdíj fizetésének dilemmája etikai, jogi és üzleti szempontokat egyaránt felvet. A politikának egyértelmű iránymutatást kell adnia arra vonatkozóan, hogy milyen körülmények között, milyen döntéshozatali mechanizmus alapján történhet meg a válsághelyzetek kezelése. Továbbá, a nemzetállami szereplők által végrehajtott APT (Advanced Persistent Threat) támadások esetében a hagyományos védelmi paradigmák gyakran elégtelennek bizonyulnak, ezért a biztonságpolitikának tartalmaznia kell a "zero trust" architektúra implementálásának alapelveit, valamint a folyamatos monitoring és threat hunting tevékenységek keretrendszerét.

Informatikai Biztonsági Szabályzat (IBSZ)

Az IBSZ a biztonságpolitika gyakorlati megvalósítását biztosítja: részletesen meghatározza a feladatokat, a felelősségi köröket, valamint az alkalmazandó technikai és szervezeti kontrollokat. Az IBSZ tartalmazza többek között a hozzáférés-kezelés, a sérülékenység-menedzsment, a mentések és helyreállítási eljárások szabályait, valamint az incidenskezelési protokollokat. A folyamatos ellenőrzés és mérés (pl. sebezhetőségi vizsgálatok, behatolási tesztek, rendelkezésre állási mutatók) garantálja, hogy a rendszer ténylegesen megfeleljen az előírásoknak és alkalmazkodjon a változó fenyegetésekhez [113]. Az IBSZ operatív szinten ad választ a hipotézisekben vizsgált problémákra: egyrészt a ransomware-ellenes reziliencia megteremtésével (H1), másrészt a nemzetállami aktorok támadásaira való célzott felkészüléssel (H2).

Az IBSZ implementációja során kiemelt figyelmet kell fordítani a technikai kontrollok többrétegű védelmi architektúrájának kialakítására. A defense-in-depth stratégia alkalmazása biztosítja, hogy egyetlen védelmi réteg megkerülése vagy kompromittálása ne vezessen

azonnali rendszerkompromittáláshoz. Ez magában foglalja a hálózati szegmentáció szigorú megvalósítását, különösen az IT és OT hálózatok közötti határvédelem tekintetében, ahol az air-gap megoldások mellett egyre gyakrabban alkalmaznak unidirekcionális gateway-eket és adatdiódákat. A mikro-szegmentáció és a szoftverdefiniált peremvédelem (SDP) technológiák lehetővé teszik a laterális mozgás hatékony korlátozását, amely kritikus fontosságú mind a ransomware-terjedés megakadályozásában, mind az APT-támadások hatásának minimalizálásában [102].

A hozzáférés-kezelési rendszer kialakítása során az IBSZ-nek részletesen szabályoznia kell a privilegizált fiókok kezelését, beleértve a PAM (Privileged Access Management) megoldások implementálását, a just-in-time és just-enough-access elvek alkalmazását, valamint a privilegizált műveletek folyamatos monitorozását és rögzítését. A többfaktoros hitelesítés univerzális bevezetése mellett egyre nagyobb hangsúlyt kap a viselkedésalapú anomáliadetektálás, amely képes azonosítani a kompromittált felhasználói fiókokat még akkor is, ha azok érvényes hitelesítési tokenekkel rendelkeznek. Az IBSZ-nek továbbá szabályoznia kell a biometrikus azonosítási módszerek alkalmazását, azok adatvédelmi vonatkozásait, valamint a post-kvantum kriptográfiai algoritmusokra való átállás ütemtervét, figyelembe véve a kvantumszámítógépek által jelentett középtávú fenyegetéseket. A részletes technológiai kontrollok és kriptográfiai átállási útvonalak a későbbi módszertani fejezetben kerülnek bemutatásra; itt a biztonságirányítási alapelvekre fókuszálok.

A mentési és helyreállítási stratégia kidolgozása során az IBSZ-nek figyelembe kell vennie a modern ransomware-változatok képességeit, amelyek aktívan keresik és titkosítják vagy törlik a biztonsági mentéseket. Ez megköveteli az immutable (megváltoztathatatlan) mentések alkalmazását, a 3-2-1-1 mentési szabály implementálását (3 példány, 2 különböző médiumon, 1 offsite, 1 offline/air-gapped), valamint a mentések rendszeres helyreállítási tesztjeit. A cyber resilience koncepció integrálása az IBSZ-be biztosítja, hogy a szervezet ne csak a támadások megelőzésére, hanem az azokból való gyors felépülésre is felkészült legyen. Ez magában foglalja a részleges működőképesség fenntartásának protokolljait, az alternatív kommunikációs csatornák előkészítését, valamint a manuális visszaállási (fallback) eljárások kidolgozását arra az esetre, ha az automatizált rendszerek kompromittálódnának.

Informatikai Biztonsági Szabályzat és ahhoz kapcsolódó ellenőrzés mérés

Az IBSZ gyakorlati implementációja és mérési keretrendszere közvetlenül kapcsolódik a dolgozat hipotéziseihez. A H1 hipotézis szempontjából az IBSZ-ben definiált metrikák lehetővé

teszik a ransomware-támadások hatásának objektív mérését és a kritikus szektorok magasabb kitettségének igazolását. A H2 hipotézis vizsgálatához az IBSZ anomália-detektálási küszöbértékei és a támadások komplexitásának mérésére szolgáló indikátorok nyújtanak empirikus alapot. A H3 hipotézis prediktív modelljének validálásához pedig az IBSZ-ben rögzített incidensadatok és azok korai jelzőszámai szolgálnak bemeneti adatként.

A hipotézisek teszteléséhez használt statisztikai módszerek és teljesítményindikátorok definíciója az M2. mellékletben, a KSM és KoI mutatók részletes leírása az M1.mellékletben található.

A kiberbiztonsági stratégia kapcsolata a szabályozással és a fenyegetésekkel

Ebben a fejezetben bemutatom a kiberbiztonság irányítási kereteit, amelyek elengedhetetlenek a szervezetek számára a hatékony védelem és kockázatkezelés biztosításához. A vagyonleltártól a kockázatelemzésen át a kiberbiztonsági reagálási tervekig minden lépés célja a szervezetek informatikai támogatásának fenntarthatósága és biztonsága. A fentiekben részletezett módszerek és stratégiák különösen fontosak a szervezet integritásának megőrzése érdekében. Az informatikai biztonsági irányítás rendszerének megfelelő működtetése és rendszeres ellenőrzése révén biztosítható, hogy a szervezet megfelelően felkészült legyen a kiberfenyegetések elleni védekezésre.

A következő alfejezetben a kiberfenyegetések típusait és időbeli alakulását vizsgálom, kiemelve azokat a tendenciákat, amelyek az elmúlt években hatással voltak a kiberbiztonsági környezetre. Külön figyelmet fordítok a kritikus infrastruktúrákat érintő támadásokra, beleértve a ransomware támadásokat és a SCADA rendszereket érő fenyegetéseket. Az adatok alapján kidolgozott elemzések és esetpéldák segítenek megérteni azokat a kockázatokat, amelyekkel a szervezeteknek szembe kell nézniük, és amelyek hatással vannak a globális biztonsági helyzetre.

Bár egy gondosan felépített informatikai biztonságirányítási rendszer (IBIR) elengedhetetlen alapja a szervezeti kibervédelemnek, fókusza elsősorban a már ismert fenyegetések kezelésére és az incidensekre való reagálásra irányul. Önmagában korlátozottan képes megbirkózni a gyorsan evolválódó, nulladik napi és komplex, többfázisú támadásokkal. Ez a felismerés vezeti be a H3 hipotézist: a reaktív védelem mellett proaktív, prediktív képességre is szükség van, amelyet a 3. fejezetben bemutatott gépi tanulási modell biztosít, kiegészítve és megerősítve az IBIR folyamatokat.

2.4. Kiberfenyegetések és biztonsági válaszlépések áttekintése

Incidenskategóriák és történeti összegzésük

A CISSM és e munka által vizsgált időszakon belül, de különösen 2015-öt követően figyelhetők meg jelentős változások a kiberbiztonság területén. Ezen időszakban drámai módon nőtt a kiberfenyegetések száma és komplexitása, amelyek a kritikus infrastruktúrák mellett számos más iparágat is érintettek, globálisan. A támadások egyre célzottabbá és kifinomultabbá váltak, különösen az államilag támogatott fenyegetési szereplők (APT-k) tevékenysége miatt.

A kiberfenyegetések kategorizálása korábban általános szempontok alapján történt, ám az elmúlt években az elemzések konkrét adatokra támaszkodva mutattak ki néhány domináns fenyegetési típust. Ezek közé tartoznak például a ransomware támadások, amelyek a korábban tárgyalt Colonial Pipeline (2021) [103] incidenst követően váltak különösen jelentőssé, valamint a kritikus infrastruktúrát érintő támadások, mint a szintén már említett ukrajnai elektromos hálózat ellen elkövetett Industroyer támadás (2016).

A modern kiberbiztonsági környezet dinamikus és kihívásokkal teli, ahol a kibertámadások növekvő gyakorisága és rafináltsága a szervezeteket arra készteti, hogy stratégiáikat állandóan újraértékeljék és finomítsák. Diogenes és Ozkaya [99] amellett érvel, hogy a proaktív kiberbiztonsági stratégiák, amelyek a fenyegetések előrejelzésére és az előkészületekre összpontosítanak, magasabb védelmi szint elérését teszik lehetővé a szervezetek számára a kibertámadásokkal szemben, mint a kizárólag reaktív megközelítés. A proaktivitás lehetővé teszi a szervezetek számára, hogy előre lássák és enyhítsék a potenciális támadásokat, ezáltal csökkentve a reagálás magas költségeit és a kibertámadások negatív hatásait.

A 2023 decemberében történt Panasonic Avionics Corporation elleni kibertámadás[3] szemléletesen illusztrálja a vállalati hálózati biztonság kihívásait. Az incidens során ismeretlen támadók exploit-alapú támadással jutottak be az alkalmazásszervereken keresztül a rendszerbe, ami rámutat a folyamatos sebezhetőségkezelés fontosságára. Az eset tanulságai szerint a támadás időben történő előrejelzése és a proaktív biztonsági intézkedések – például a hálózati adatforgalom anomália-alapú elemzése és a rendszeres biztonsági auditok – kulcsfontosságúak a hasonló incidensek megelőzésében [99].

Az incidens-reagálási tervek (IRT) kiemelt szerepet játszanak a kiberbiztonsági stratégiákban, mivel lehetővé teszik a szervezetek számára, hogy hatékonyan kezeljék és minimalizálják a kiberbiztonsági incidensek hatásait. Az incidens-reagálási tervek kulcsfontosságúak minden kiberbiztonsági stratégiában. Ezek a tervek biztosítják, hogy a szervezet képes legyen gyorsan

és hatékonyan reagálni a biztonsági incidensekre. Az IRT-k kiterjednek a felkészülésre, az észlelésre, a reagálásra, és a helyreállításra, előírva a szükséges lépéseket, hogy a szervezet minimálisra csökkenthesse az incidensek hatásait és a lehető legrövidebb időn belül helyreállíthassa az üzemszerű működést.

Az egyes esetek elemzése alapján megállapítható, hogy a proaktív kiberbiztonsági stratégiák és az incidens-reagálási tervek alapvető fontosságúak a modern kiberfenyegetések elleni védekezésben. Az előrejelzés, a megelőzés és a gyors reakció képessége jelentősen hozzájárul a szervezetek védelmi képességéhez és az üzletmenet folytonosságának biztosításához.

A Komplexitási Index (KoI) a támadások végrehajtási mintázatainak technikai összetettségét méri négy, binárisan (0/1) értelmezett technikai komponens jelenléte alapján: perzisztencia (P), laterális mozgás (L), észlelés elkerülése (E) és többfázisú kampányjelleg (C). A KoI értéke e komponensek összegeként 0 és 4 között vehet fel értéket; a mérés nem a technikák számát, hanem meghatározott technikai viselkedések azonosítható jelenlétét rögzíti. A KoI képezi a H2 hipotézis empirikus tesztjének kulcsát: azt vizsgálja, hogy a nemzetállami vagy államilag támogatott támadások nagyobb arányban érik-e el a magas KoI-küszöböt, mint a pénzügyi motivációjú bűnözői csoportok műveletei.

A kiberfenyegetések általános kategorizálását követően áttérek néhány főbb típus konkrét adatokra alapozott leírására:

Ransomware támadások: 2021-től kezdve elkövetésük jelentősen gyakoribbá vált, különösen a kormányzati és egészségügyi szervezetek ellen.

SCADA rendszerek elleni támadások: Az ipari vezérlőrendszerek elleni támadások száma és komplexitása szintén megnövekedett, ami jelentős kockázattal bír az energiaipar és más kritikus infrastruktúrák számára.

Adatlopás és kémkedés: Az adatvédelmi incidensek és kiber-espionázs esetek száma is növekedett, amelyek gazdasági és nemzetbiztonsági kockázatokat is jelentenek.

DDoS támadások (Distributed Denial of Service): Ezek a támadások a célja a weboldalak és online szolgáltatások elérhetetlenné tétele volt, ami jelentős üzleti és társadalmi hatással bírt.

Adathalászat és pszichológiai manipuláció (Phishing, social engineering): Ezen támadások a felhasználók megtévesztésén alapultak, hogy bizalmas információkat szerezzenek meg.

A Colonial Pipeline elleni zsarolóvírus-támadás (2021) vagy az Ukrajna elektromos hálózatát érintő Industroyer incidens (2016) mindössze az IIT kibertámadások egy-egy jelentős példája volt – mégis pontosan megmutatták, milyen széles körű következményekkel járhatnak napjaink kiberfenyegetései.

Az IIT (Industrial IT) az ipari környezetek informatikai rétege, az OT/IT konvergencia része; tipikusan ICS/SCADA-rendszerekhez kapcsolódó hálózatok, alkalmazásszerverek, menedzsment- és felügyeleti komponensek összessége, amelyek közvetlenül vagy közvetve kritikus infrastruktúra-funkciókat szolgálnak ki.

Az elmúlt évtizedben drámai módon növekedett nemcsak a támadások száma, hanem azok hatóköre és súlyossága is. A kiberbűnözők eszköztára folyamatosan fejlődött, aminek eredményeként mára egyetlen incidens is képes gazdasági károkat okozni, alapvető szolgáltatásokat megbénítani, és veszélyeztetni a társadalmi stabilitást, nemzeti biztonságot.

Ebben a helyzetben a kritikus infrastruktúrák ellen intézett támadások különösen fontos jelképeivé váltak a kiberbiztonsági küzdelemnek, és ráirányították a figyelmet arra, hogy a fenyegetések kezelése nem pusztán technikai feladat, hanem stratégiai kérdés is. A kormányzati és magánszféra válaszlépései közé tartoznak a támadások megelőzését és detektálását célzó fejlett technológiák, az incidenskezelési protokollok rendszeres frissítése, valamint a felhasználók tudatosságának fokozása és ismereteik bővítése.

Az alábbiakban ezek közül a ransomware támadásokat és a SCADA rendszerek elleni támadásokat elemzek részletesebben.

Ransomware támadások és hatásaik a kritikus infrastruktúrákra

A ransomware, vagy zsarolóvírus, egy olyan kártékony szoftver, ami zárolja a felhasználó adatait vagy rendszereit, és váltságdíjat követel azok visszaállításáért. Az elmúlt években ez a fenyegetési forma vált az egyik legnagyobb kiberbiztonsági kihívássá, különösen a kritikus infrastruktúrák számára.

Ransomware támadások jellemzői

Célzott támadások: A támadók gyakran specifikusan választják ki azokat a szervezeteket, amelyek nagy valószínűséggel fizetnek váltságdíjat, mint például egészségügyi intézmények, kormányzati szervek vagy energiaipari vállalatok.

Komplexitás: A modern ransomware támadások egyre összetettebbek és nehezebben észlelhetőek. Ezek a támadások szofisztikált módszereket alkalmaznak, mint például titkosítást, időzített aktiválást és kiterjedt hálózati behatolást.

Ransomware támadások hatása a kritikus infrastruktúrákra

Működési zavarok: A kritikus infrastruktúrák, mint az egészségügyi ellátás, energiaellátás és közlekedési rendszerek, különösen sebezhetőek a ransomware támadásokkal szemben. Egy sikeres támadás megbéníthatja ezeknek a rendszereknek a működését, ami súlyos társadalmi és gazdasági következményekkel járhat.

Adatvesztés és szolgáltatási hiányosságok: Az adatok titkosítása és a hozzáférés megtagadása komoly problémákat okozhat a szolgáltatások folytonosságában. Ez különösen aggasztó, ha az érintett adatok életbevágóan fontosak, mint például a betegellátási információk vagy a közüzemi szolgáltatások.

Védekezési stratégiák

Proaktív biztonsági intézkedések: Az ilyen típusú támadások elleni védekezés magában foglalja a rendszeres biztonsági frissítéseket, az adatbiztonsági mentéseket és a felhasználók kiberbiztonsági oktatását.

Incidensreagálási tervek: A szervezeteknek incidensreagálási terveket kell kidolgozniuk a ransomware támadásokra való gyors és hatékony reagálás érdekében. A ransomware támadások jelentős kihívást jelentenek a kritikus infrastruktúrák számára. A megelőzés és a gyors reagálás egyaránt kulcsfontosságú a károk minimalizálása és a rendszerek zavartalan működésének fenntartása érdekében.

A SCADA rendszerek alapvető szerepet játszanak a kritikus infrastruktúrák, mint például energiaellátás, vízellátás, és közlekedési rendszerek irányításában. Ezek a rendszerek a kritikus infrastruktúrák központi vezérlését biztosítják, így működésük megzavarása károsan befolyásolja a nemzeti biztonságot és a gazdasági stabilitást. Mivel a SCADA rendszerek távoli felügyeletre és vezérlésre is alkalmasak, sérülékenységük stratégiai jelentőségű biztonsági kihívást jelent.

SCADA rendszerek sebezhetőségei

Rendszerintegráció és hálózati kapcsolatok: A SCADA rendszerek egyre inkább integrálódnak az üzleti IT-hálózatokkal és kapcsolódnak az Internethez, ami növeli a kiberfenyegetéseknek való kitettségüket.

Elavult technológia: Sok SCADA rendszer elavult technológián alapul, amelyeket nem a modern kiberfenyegetések elleni védelemet szem előtt tartva terveztek meg.

Hiányos biztonsági intézkedések: A SCADA rendszerek gyakran nem rendelkeznek megfelelő biztonsági protokollokkal, mint például a rendszeres frissítések, a titkosítás, vagy a multi-faktoros hitelesítés.

2.5. Összefoglalás

Az előző fejezetek átfogó képet nyújtottak a kiberbiztonsági események természetéről, azok kritikus infrastruktúrákra gyakorolt hatásairól, valamint az ezekre adható szervezeti válaszokról. A bemutatott esettanulmányok – a Saudi Aramco elleni Shamoon vírus támadástól a Colonial Pipeline ransomware incidensig – egyértelműen demonstrálták, hogy a modern kiberfenyegetések milyen mértékű károkat képesek okozni mind gazdasági, mind társadalmi szinten.

A CISSM adatbázis elemzése rávilágított arra, hogy a kibertámadások nem izolált események, hanem egy folyamatosan fejlődő fenyegetési környezet részei, ahol a támadók egyre kifinomultabb módszereket alkalmaznak. Az energiaszektor, a kritikus infrastruktúrák és a közszolgáltatások preferált célpontokká váltak, ami szükségessé teszi az átfogó védelmi stratégiák kidolgozását.

Az Informatikai Biztonsági Irányítási Rendszer (IBIR/IBSZ) bemutatása nem empirikus adatforrásként szolgál a hipotézisek teszteléséhez, hanem szervezeti és értelmezési keretet ad az esettanulmányok tanulságainak rendszerezéséhez. Az IBSZ-ben megjelenő kontrollok és küszöbök a kvalitatív következmények és szervezeti válaszok értelmezését segítik, míg a hipotézisek empirikus vizsgálata az MCED adatokon alapuló kvantitatív elemzésben történik.

Kulcsfontosságú megállapítások:

- A proaktív megközelítés költséghatékonyabb és eredményesebb, mint a reaktív védelem
- Az emberi tényező kritikus szerepet játszik a biztonságban – a dolgozók képzése és tudatosságnövelése alapvető fontosságú

- A folyamatos ellenőrzés, mérés és fejlesztés nélkülözhetetlen az IBIR hatékony működéséhez
- A dokumentálás és a szabályozási megfelelés biztosítja az átláthatóságot és a számonkérhetőséget

A kiberfenyegetések időbeli alakulásának vizsgálata megmutatta, hogy 2015 után drámai változások történtek: a ransomware támadások gyakorisága megnőtt, az államilag támogatott APT csoportok aktivitása fokozódott, és a SCADA rendszerek elleni támadások egyre kifinomultabbá váltak. Ezek a trendek aláhúzzák, hogy a szervezeteknek folyamatosan alkalmazkodniuk kell a változó fenyegetési környezethez.

A következő fejezet ezen alapokra építve fog mélyebb statisztikai elemzéseket bemutatni a kiberfenyegetések mintázatairól, előrejelzési modelleket dolgoz ki, és konkrét javaslatokat fogalmaz meg a kritikus infrastruktúrák védelmének további erősítésére. A bemutatott IBIR keretrendszer és a történeti tapasztalatok együttesen szolgálnak majd alapul a jövőbeli védelmi stratégiák kidolgozásához.

A 2. fejezetben összegzett tapasztalatok operacionális keretet adnak az empirikus bizonyításhoz. A későbbi elemzésekben a károkozási súlyossági mutató (KSM) az MCED event_subtype alapján kvantifikálja a hatást (H1 és H1.1), míg a TTP-alapú komplexitási index (KoI) a támadások végrehajtási mintázatát ragadja meg a P, L, E és C komponensek mentén (H2). Ezekhez kapcsolódva a 3. fejezetben bemutatott prediktív modell a korai fázisban rendelkezésre álló leírások és metaadatok (pl. iparág, régió, motiváció, eseménytípus) felhasználásával javítja az incidensek előrejelzését és osztályozását (H3).

3 GÉPI TANULÁSI MEGOLDÁS A KIBERBIZTONSÁGI FENYEGETÉSEK ELŐREJELZÉSÉRE ÉS A MODELL HATÉKONYSÁGÁNAK TESZTELÉSE

3.1 A vizsgálat keretrendszere és módszertani alapjai

A fejezet célja, hogy az 1. fejezetben bemutatott változókra, a 2. fejezet empirikus esettanulmányaira, valamint a Maryland Cyber Events Database (MCED) 2014–2025 közötti adatállományára építve egységes, szigorú módszertani keretet hozzon létre a három kutatási hipotézis teszteléséhez [104]. A fejezet kizárólag a módszertani struktúrát rögzíti; az egyes statisztikai és gépi tanulási kísérletek eredményeit a későbbi, eredményorientált alfejezetek tartalmazzák.

3.1.1 Adatkeret és forráslogika

A vizsgálat alapját a CISSM által karbantartott MCED adatkészlet képezi, amely 2014 és 2025 októbere között több mint tízezer, manuálisan validált kiberincidens rekordját tartalmazza. A dataset struktúrája a 2025. augusztusi Codebooknak megfelelően egységesített; az adatgyűjtés vegyes módszertannal zajlik:

- Python-alapú scraping (pre-2025), valamint
- 2025-től a GDELT Web News NGrams 3.0 és a GDELT Article List integrációja.

A GDELT-integráció érdemben növeli a források földrajzi és nyelvi lefedettségét, miközben a kézi validáció biztosítja az eseményfogalom következetes alkalmazását. A teljes adatállomány incidensszintű (event-level) bontásban tartalmazza többek között az event_date, actor_type, industry, motive, event_type, event_subtype, description és targeted_country mezőket.

3.1.2 A kulcsváltozók operacionalizálása

A fejezet három, egymástól analitikailag független mutatót alkalmaz:

- **Károkozási súlyossági mutató (KSM)**

  Az MCED event_subtype kategóriáiból származtatott, 1–5 közötti skála, amely a technikai–operációs hatás intenzitását fejezi ki. A KSM minden esetben kizárólag a technikai következményekből képzett érték, szektortól függetlenül.

- **Komplexitási index (KoI)**

Négy technikai komponens – laterális mozgás, perzisztencia, detektálás-elkerülés, többfázisú végrehajtás – bináris jelenléte alapján képzett 0–4 közötti kompozit mutató. A KoI keretrendszere a MITRE ATT&CK TTP-khez illeszkedik, de a MITRE-adatbázist nem vonom be közvetlenül a datasetbe.

- **Kritikus szektor indikátor (KrI_flag)**

  Bináris változó, amely az MCED NAICS-mezőjét a NIS2/CER irányelvek szektorlistáihoz illeszti, 1 = kritikus, 0 = nem kritikus kódolással.

E három változó a H1–H2 hipotézisek fő magyarázó- és kimeneti tengelyeit adja.

3.1.3 A hipotézisek matematikai kerete

A három hipotézis a kibertámadások súlyossági, komplexitási és attribúciós dimenziójára vonatkozik:

- **H1: kritikus infrastruktúrák nagyobb károkozási potenciállal bírnak.**
  A vizsgálat a KSM eloszlások összehasonlításán, nemparaméteres próbákon (Brunner–Munzel, Mann–Whitney U) és bináris regressziós kereteken (KSM ≥ 4) alapul.
- **H2: az állami aktorok technikai komplexitása magasabb.**
  A KoI eloszlásainak összevetése aktortípusok között, valamint komponens-szintű különbségek (perzisztencia, laterális mozgás stb.) statisztikai vizsgálata képezi a tesztelési alapot.
- **H3: az aktortípus előrejelezhető korai fázisú információk alapján.**
  A modellezés kizárólag az esemény időpontjában (t_0) rendelkezésre álló metaadatokat és szöveges információkat használja, elkerülve az információszivárgást.

3.1.4 Időalapú szeparáció és adatszivárgás-mentes modellépítés

A prediktív modellezéshez a következő időablakokat zárom le:

- tanítás: 2014–2021
- validáció: 2022
- teszt: 2023–2025

Minden transzformáció (TF–IDF, kategória-kódolás, skálázás, lexikon-alapú jellemzők) kizárólag a tanító halmazon kerül illesztésre; a validációs és tesztkészletek csak befagyasztott

transzformációkat alkalmaznak. Ez biztosítja, hogy sem a prediktív modellek, sem a statisztikai elemzések ne profitálhassanak a jövőre vonatkozó információkból.

3.1.5 Modellezési architektúra

A H3 vizsgálatához rétegzett (stacking) ensemble modellt alkalmazok[16], amely

- a szöveges csatornán lineáris modelleket,
- a strukturált csatornán fa-alapú, nemlineáris algoritmusokat,
- meta-szinten pedig logisztikus regressziót

illeszt össze, out-of-fold előrejelzéseket felhasználva. A pipeline teljes egészében az adat torzulás és az adatszivárgás elkerülésére van optimalizálva.

3.1.6 Külső adatforrások és validációs rétegek

Az empirikus elemzés primer adatforrása a Maryland Cyber Events Database (MCED), ugyanakkor a 3. fejezet következtetései nem értelmezhetők önmagukban. Szükség van arra, hogy a kapott mintázatokat iparági és technikai szinten is összevessük más, független adatforrásokkal. A dolgozat ehhez három, egymásra épülő validációs réteget alkalmaz; ezek kereteit az 1. fejezet 2. táblázata foglalja össze.

Az első réteg célja, hogy az MCED-ben megfigyelt iparági megoszlások és támadástípus-mintázatok ne legyenek nyilvánvaló ellentmondásban a VERIS Community Database (VCDB) struktúrájával és a Verizon Data Breach Investigations Report (DBIR) aggregált eredményeivel. A VERIS JSON-séma incidensszintű bontást ad (action–asset–attribute logika), míg a DBIR iparági és támadási trendeket publikál (pl. social engineering, credential theft, ransomware arányok). Ezeket a forrásokat nem építem be featurizált módon, és nem végzek rajtuk formális hipotézisteszteket; csupán nagyságrendi, kvalitatív összevetésként használom őket az MCED-ből kapott arányok értelmezéséhez.

A második réteg az iparági fenyegetési riportokra és egy kisméretű, de részletes IBM X-Force incidensrészhalmazra épül. Az IBM X-Force 2025-ös adatainak ~50 elemű táblája jól illusztrálja, hogy a célzott iparág, régió, aktortípus és támadási vektor kombinációi (pl. ransomware, business email compromise, supply-chain exploit) milyen típusú mintázatokban jelennek meg a gyakorlatban. A Mandiant M-Trends, a CrowdStrike Global Threat Report és az ENISA Threat Landscape jelentései a dwell time, az initial access technikák (exploit, stolen credentials, phishing), valamint a supply chain támadások gyakorisága és célpontszektorai

tekintetében szolgálnak „külső realitás-tesztként”. Ezeket a forrásokat nem keverem bele az MCED-alapú modellekbe, és nem használom a Komplexitási Index vagy más mutatók számszerű kalibrálására; szerepük annyi, hogy a H1–H2 hipotézisekből kapott mintázatokat narratív, irány- és nagyságrendi szinten kontextusba helyezzék.

A harmadik réteg technikai háttérforrásokat jelent. A CISA Known Exploited Vulnerabilities (KEV) katalógus a CVE-k azon halmazát sorolja, amelyről bizonyított, hogy aktív exploitáció alatt áll. A KEV-adatokat nem kapcsolom rekordszinten az MCED-hez, és nem használom a KoI numerikus értékeinek kalibrálására; szerepük az, hogy példákon keresztül megmutassák: a KoI definíciójában hangsúlyos támadási vektorok (pl. VPN gateway-k, távoli menedzsment eszközök, internetre nyitott alkalmazásszerverek) valóban kiemelten érintettek az exploitált sebezhetőségek között. A MITRE ATT&CK Enterprise mátrix a KoI taxonómiai alapját adja: a KoI definícióban használt komponensek (laterális mozgás, perzisztencia, detektálás-elkerülés, többfázisú kampány) közvetlenül ATT&CK taktikákhoz és technikákhoz illeszthetők. A MITRE-t nem használom „független” validációnak a KoI-ra, mert a definíció is rá épül; itt a szerepe a sémakövetés és a TTP-konzisztencia auditja.”

A 3. fejezetben bemutatott kvantitatív eredmények (H1–H3) így továbbra is tisztán az MCED adataira és a NIS2/CER szerinti KrI címkére épülnek; a külső források legfeljebb kvalitatív realitás-tesztet jelentenek.

Összefoglalva: a 3. fejezet formális hipotézistesztjei szigorúan az MCED 2014–2025 adatain futnak, a külső források (VERIS/VCDB, DBIR, IBM X-Force, Mandiant, CrowdStrike, ENISA, CISA KEV, MITRE ATT&CK) pedig három funkciót látnak el:

1. iparági és támadási alapértékelés,
2. konkrét, de független incidensek szerkezetének ellenőrzése,
3. a KoI és KSM technikai értelmezésének szakmai „horgonyai”.

Sem rekordszintű összefésülés, sem közvetlen feature-bővítés nem történik rajtuk keresztül – így az MCED-alapú modellezés reprodukálható, ugyanakkor nem szakad el a globális fenyegetési környezet valóságától.

3.1.7 KoI kulcsmutató és kompozit kitettségi index – módszertani leírás

A Komplexitási Index (KoI) a kutatás kulcsmutatója, amely a támadások technikai szofisztikáltságát számszerűsíti. A KoI-t az 1.5. alfejezetben rögzített, MITRE ATT&CK-hez

illesztett szabályrendszer alapján képezem: négy komponens (laterális mozgás, perzisztencia, detektálás-elkerülés, többfázisú végrehajtás) bináris jelenlétét összegzem, így 0–4 közötti kompozit értéket kapok minden incidensre.

A 3. fejezetben a KoI-t nemcsak eseményszinten, hanem iparági szinten is felhasználom. Ehhez egy kompozit kitettségi index kerül bevezetésre, amely négy dimenziót integrál:

- **K1 – gyakoriság (Frequency):** normalizált incidensszám iparáganként (pl. incidens / 1000 szervezet).
- **K2 – átlagos Komplexitási Index (Average KoI):** az adott iparág összes eseményének átlagos KoI-értéke.
- **K3 – helyreállási idő (Recovery Time):** az incidensek medián helyreállási ideje (napokban), ferdeség esetén log-transzformált formában.
- **K4 – kaszkádhatás (Cascade Effect):** a downstream függőségek száma (hány más szektort érint érdemben az incidens következménye), külső input–output mátrixokra támaszkodva [10][36].

A kompozit index célja nem új hipotézisek bevezetése, hanem a KoI és a kitettség viszonyának integrált vizsgálata. Az egyes komponensek súlyozott, standardizált formában kerülnek összesítésre; a jelen dolgozatban az alábbi általános sémát alkalmazom:

1. **Iparági aggregálás**
    - K1, K3, K4 esetén az iparágra eső átlag/medián kerül kiszámításra.
    - K2 esetében:

      $K_{2i} = (\Sigma\ KoI_j) / n_i$

    ahol KoI_j az i iparágba tartozó j-edik esemény Komplexitási Indexe, n_i pedig az iparág incidenseinek száma.
2. **Standardizálás**

    Minden komponens Z-score formára kerül transzformálásra:

    $Z_i = (X_i - \mu_x) / \sigma_x$

    ahol μ_x és σ_x az adott komponens teljes mintára vett átlaga és szórása.
3. **Kompozit index**

A kompozit kitettségi mutató lineáris súlyozással adódik:

$$\text{Composite}_i = w_1 \cdot Z_{k1,i} + w_2 \cdot Z_{k2,i} + w_3 \cdot Z_{k3,i} + w_4 \cdot Z_{k4,i}$$

ahol a súlyvektor egy előre rögzített, szakmai indoklással alátámasztott kombináció (pl. [0,25; 0,25; 0,30; 0,20]).

4. **Min–max skálázás (vizualizáció)**

A kompozit index vizuális összehasonlíthatósága érdekében opcionálisan 0–100 közé skálázott mutató is képezhető:

$$\text{Index\_scaled}_{,i} = 50 + 45 \cdot (\text{Composite}_i - \text{Composite\_min}) / (\text{Composite\_max} - \text{Composite\_min})$$

Itt a kompozit index elsősorban módszertani példaként szerepel: bemutatom, hogyan lehet a KoI-t a gyakorisággal, helyreállási idővel és kaszkádhatással egy integrált kitettségi mutatóba összevonni. A dolgozat fő hipotézisvizsgálata (H1–H3) továbbra is az eseményszintű KSM, KoI és KrI változókra épül; a kompozit index tényleges, MCED-alapú empirikus értékei a későbbi, eredményorientált kísérletek után tölthetők fel, vagy mellékletbe kerülnek.

3.2 A kvantitatív elemzés

3.2.1 Az elemzési keret és mintakialakítás

A kvantitatív elemzés a MCED 2014–2025 közötti adataira épül. A nyers adatállomány a Codebook szerint incidensszintű rekordokat tartalmaz, többek között az alábbi mezőkkel: event_date, actor_type, industry, motive, event_type, event_subtype, description, targeted_country. A tisztításnál az 1.5.9. alfejezetben rögzített protokollt alkalmazom: - Nyers állomány: teljes MCED + elgépelések normalizálása (pl. „Hacktvist" → „Hacktivist"), ISO-kód hibák javítása vagy kizárása, duplikált slug rekordok eltávolítása (n = 15 789). - Undetermined nélkül: a nyers állományból kizárom azokat az eseteket, ahol actor_type = Undetermined. Ez a szint adja a H2 és H3 vizsgálatok alapját, mivel az aktortípus nélküli események nem alkalmasak célváltozóként (n = 15 166). - Elemzési minta: a három fő aktortípusra (Criminal, Hacktivist, Nation-State) szűkített állomány (n = 14 938). A Hobbyist (n = 198) és Terrorist (n = 30) kategóriákat alacsony esetszámuk miatt kizárom. Azért, hogy a szűrés ne okozzon mintaszerkezeti torzulást, a nyers és az elemzési minta eloszlásait iparág, eseménytípus, esemény altípus és célország dimenziókban Jensen–Shannon divergenciával

(JSD) hasonlítom össze. Módszertanilag a JSD < 0,01 küszöbértéket tekintek olyan határnak[105], amely alatt az eloszlások gyakorlatilag ekvivalensnek tekinthetők; a konkrét értékeket és az egyes dimenziókra számolt JSD-eredményeket a 3.3.1 alfejezet rögzíti.

Az elemzési minta adja a H1–H2 hipotézisek keresztmetszeti vizsgálatának alapját. A H3 prediktív modell esetén ezen belül további időbeli szeparációt alkalmazok: - Train: 2014–2021 - Validation: 2022 - Test (out-of-time): 2023–2025 Minden előfeldolgozási lépés (szöveg-előkészítés, TF–IDF, kategória-kódolás, skálázás) kizárólag a tanító halmazon kerül illesztésre, majd változatlan paraméterekkel kerül alkalmazásra a validációs és teszthalmazokon. Ez garantálja, hogy a modell teljesítményét olyan adatokon mérjük, amelyek a tanítás szempontjából valóban „jövőből" származnak. Az osztályeloszlás aszimmetrikus: a Criminal kategória dominál, míg a Terrorist és Hobbyist osztályok nagyon kevés eseményt tartalmaznak. Ez indokolja a súlyozott veszteségfüggvények és alternatív értékelési metrikák (macro-F1, PR-AUC) használatát.

3.2.2 A hipotézisek tesztelésének módszertana

H1 – kritikus infrastruktúrák kárkockázata (KSM vs KrI)

A H1 hipotézist két szinten tesztelem:

1. **Eloszlás-szintű különbség**

   A KSM ordinális skáláját kritikus (KrI_flag = 1) és nem kritikus (KrI_flag = 0) szektorokra bontva hasonlítom össze. A fő próba a Brunner–Munzel teszt, alternatívaként a Mann–Whitney U, mivel nem teszek fel normalitási feltételt. A hatásméretet Cliff-féle δ mutatóval mérem; a konfidencia-intervallumokat bootstrap eljárással becsülöm (pl. 1000 replikáció).

2. **Magas károkozás valószínűsége**

   Bináris kimenetet definiálok:

   High =KSM ≥ 4

Erre logisztikus regressziót illesztek, amelynek fő magyarázója a KrI_flag. Kontrollváltozók: év (nemlineáris spline), régió, event_type, szükség esetén supply_chain flag. A modellből származó esélyhányados (OR) és konfidencia-intervallum a 3.3.2-ben kerül bemutatásra; itt a modell szerkezete a lényeg.

Robusztussági vizsgálatok:

- strict vs broad kritikus definíció (NIS2-mag, illetve NIS2 + CER kiterjesztés),
- Undetermined nélküli vs elemzési minta,
- propensity score súlyozás iparág, régió, év és event_type alapján a mintaszerkezeti torzulások korrigálására.

H2 – aktortípus és technikai komplexitás (KoI vs actor_type)

A H2 esetén a cél annak vizsgálata, hogy a Nation-State és Criminal kategóriák között van-e szisztematikus különbség a KoI értékekben és komponensekben.

1. **KoI eloszlások összehasonlítása**
    - Minta: Level-1 (Undetermined nélkül).
    - Fő próba: Brunner–Munzel / Mann–Whitney U a KoI teljes (0–4) skálájára.
    - Hatásméret: Cliff-δ + bootstrap CI.
    - Stratifikáció kritikus szektorokra (KrI_flag = 1) és supply_chain = 1 eseteire.
2. **Komponens-szintű elemzés**
    - perzisztencia (igen/nem), laterális mozgás (igen/nem), detection_delay küszöb felett (igen/nem), kampány jelleg (igen/nem),
    - χ^2 / Fisher próba a komponensek aránykülönbségeire, Benjamini–Hochberg FDR-rel korrigálva,
    - logisztikus modell Nation-State vs Criminal kimenettel, magyarázók: KoI komponensek + kontrollok (KrI, év, régió, event_type, supply_chain).
3. **Ordinális regresszió**
    - Célváltozó: KoI (0–4),
    - magyarázók: actor_type, KrI_flag, supply_chain, idő és régió,
    - interakciók (actor_type × KrI_flag, actor_type × supply_chain) tesztelése likelihood-ratio próbákkal.

Az itt ismertetett modellek struktúrája rögzített; a konkrét koefficiensek és p-értékek a 3.3.3 alfejezetben, a futtatott elemzések eredményei alapján kerülnek bemutatásra.

H3 – korai aktortípus-előrejelzés (gépi tanulási modell)

A H3 hipotézis azt vizsgálja, hogy egy kétcsatornás, stacking alapú ensemble modell képes-e az incidens időpontjában (t_0) rendelkezésre álló, korlátozott információ alapján az aktortípust (Criminal, Nation-State, Hacktivist, Terrorist, Hobbyist) a baseline megközelítéseknél (naiv többségi, szabályalapú, Random Forest) szignifikánsan pontosabban előrejelezni.

A modell három logikai rétegből áll:

1. **Feature-képzés**
    - *Szöveges csatorna*: a title + description mezőkből előfeldolgozott szöveg készül (kisbetűsítés, zajszűrés, lemmatizálás, stop-szó szűrés), ezt követően szó n-gram (1–2) és karakter n-gram (3–5) TF–IDF reprezentációval ábrázolom a dokumentumokat [12][19].
    - *Strukturált csatorna*: az év, régió, industry, event_type, event_subtype, motive, supply_chain flag, source_count és date_precision mezők megfelelően kódolt formában jelennek meg (dummy-kódolt kategóriák, skálázott numerikus változók).
    - *Domain-specifikus jellemzők*: a MITRE ATT&CK keretrendszerből származó kulcsszavak (pl. „lateral”, „persistence”, „credential dumping”) bináris indikátorként jelzik egyes taktikák/technikák jelenlétét, továbbá külön lexikon jelzi a ransomware/DDoS/supply-chain szókészlethez tartozó előfordulásokat.
2. **Alapmodellek (base learners)**

    A két csatornához külön, eltérő induktív torzítású modelleket használok:
    - szöveges alapmodellek: multinomiális logit vagy lineáris SVM, valamint Naive Bayes, amelyek jól skálázódnak nagy dimenziós, ritka TF–IDF-tereken,
    - strukturált modell: súlyozott Random Forest, illetve opcionálisan gradient boosting típusú fa-alapú modell [8].

A Random Forest választása baseline-ként módszertanilag indokolt, mivel robusztus teljesítményt nyújt minimális hiperparaméter-hangolással, és a prediktív modellek összehasonlítására széles körben alkalmazott standard megközelítés[106].

3. **Stacking és kalibráció**

   A base modellekből out-of-fold (OOF) előrejelzéseket generálok a train + validation periódusra, majd ezekre a kimenetekre egy logisztikus regressziót illesztek meta-szinten (stacking). A validációs év (2022) OOF-előrejelzésein többosztályos kalibrációt végzek (Platt scaling vagy isotonic regresszió); a kiválasztott kalibrációs transzformáció paraméterei befagyasztva kerülnek alkalmazásra a 2023–2025 közötti tesztkészleten.

Értékelési metrikák és döntési logika

A modell teljesítményét az aktortípusok erősen kiegyensúlyozatlan eloszlásához igazított metrikákkal értékelem:

- macro-F1 (osztályonkénti F1-score átlaga),
- PR-AUC osztályonként,
- Brier-score és Expected Calibration Error (ECE) a valószínűségkalibráció mérésére [12],
- Top-k recall (pl. Top-2), amely azt mutatja meg, hogy milyen arányban szerepel a helyes osztály az első k legnagyobb valószínűségű jelölt között.

Döntési szabály és tartózkodási (reject) mechanizmus

A modell döntési rétege osztály-specifikus küszöböket alkalmaz, tekintettel arra, hogy a Nation-State kategóriához tartozó téves negatív kimenetek kockázati súlya magasabb, mint a téves pozitívaké. Ennek megfelelően minden osztályhoz külön döntési küszöb (τ_i) tartozik; a modell determinisztikus címkét csak akkor ad, ha:

PredictedClass = c_i, ha p(c_i) ≥ τ_i és p(c_i) = max_j p(c_j)

ahol $p(c_i)$ az adott osztály poszterior valószínűsége.

A rendszer tartalmaz egy tartózkodási (reject) mechanizmust is, amely a bizonytalanság formális kezelésére szolgál. Ha egyik osztály valószínűsége sem éri el a megbízhatósági alsó határt (τ_reject), a modell kimenete:

PredictedClass = REJECT, ha max_i p(c_i) < τ_reject

Ez definiálja a „nem besorolható” régiót, amelyet a következő bizonyossági függvény ír le:

S(x) = max_i p(c_i), RejectRegion = { x : S(x) < τ_reject }.

A reject-mechanizmus akkor aktiválódik, amikor a modell a posteriori eloszlást vizsgálva nem képes kellően magas bizonyosságot társítani egyik osztályhoz sem. Ez biztosítja, hogy az osztályozó csak olyan esetekben ad determinisztikus címkét, amelyekre megbízható valószínűségi becslés áll rendelkezésre; a bizonytalan esetek külön régióba kerülnek, és a kvalitatív értelmezés során külön kezelhetők.

Összefoglalva, a H3 hipotézis tesztelése egy összetett, többcsatornás, időben szeparált és kalibrált predikciós keretrendszeren alapul, amely explicit módon kezeli az osztályeloszlás kiegyensúlyozatlanságát, a valószínűségkalibrációt és a bizonytalanságot. A konkrét eredményeket és a hipotézis numerikus értékelését a 3.3.4 alfejezet tartalmazza.

3.2.3 Az időbeli validitás és kalibráció biztosítása

A prediktív modell értékelésénél alapvető követelmény, hogy a tanulási és tesztelési folyamat szigorúan időben elkülönüljön, elkerülve az olyan adatszivárgási formákat, amelyek mesterségesen javítanák a mérhető teljesítményt. A modell tanítása ezért a 2014–2021 közötti történeti adatokat használja fel, míg a 2022-es időszak dedikált validációs évként szolgál a küszöbök, a kalibráció és a hiperparaméterek hangolására. A végső teljesítményértékelés a 2023–2025 periódusra esik, amely teljes egészében out-of-time, így a modell a gyakorlatban várható előrejelző képességét mutatja.

A teljes pipeline minden komponense – a szöveg-előkészítés, TF–IDF vektorizáció, kategória-kódolás, skálázás, valamint a domain-specifikus jellemzők képzése – kizárólag a tanító halmazon kerül illesztésre. A validációs és tesztperiódusok csak befagyasztott, már tanult transzformációkat alkalmaznak. Ez biztosítja, hogy sem közvetett, sem közvetlen módon ne kerülhessen a modell a jövőbeli adatokból származó információ birtokába.

A stacking meta-tanuló out-of-fold előrejelzéseken alapul, így a meta-szint sem találkozik saját tanító mintáival. A validációs év (2022) szolgál az operációs pont meghatározására: ekkor illeszthető a valószínűségkalibráció (Platt scaling vagy isotonic regresszió), továbbá ebben a szakaszban határozható meg az osztály-specifikus küszöbök rendszerének optimális konfigurációja. A kalibráció eredményeként a modell valószínűségi kimenetei közelítenek a

tényleges gyakoriságokhoz, ami alapfeltétel a reject-mechanizmus megbízhatóságához és a downstream kockázati döntésekhez.

A drift-ellenőrzés szintén a módszertani keret része. A fő jellemzők eloszlását és a modell válaszmintázatát időbeli rétegenként Population Stability Index (PSI) és Jensen–Shannon divergencia alapján vizsgálom, azzal a céllal, hogy az esetleges szerkezeti változásokat időben érzékelni lehessen. A tényleges drift-értékek és stabilitási mutatók a 3.3. fejezetben, az empirikus eredmények bemutatásakor kerülnek rögzítésre.

Összességében a tanulási–kalibrációs–tesztelési protokoll időbeli szeparációja, valamint a transzformációk befagyasztása biztosítja, hogy a modell teljesítményét torzítatlan, valós előrejelző környezetben lehessen értékelni. Ez a protokoll az egész H3 vizsgálati logika alapja, és nélkülözhetetlen a 3.3 fejezetben bemutatott eredmények interpretációjához.

3.3 Adatelőkészítés és minőségbiztosítás

A Maryland CISSM Cyber Events Database forrásadatbázis (15 789 rekord) adatminőségi problémákat tartalmazott, amelyek kezelése az elemzés előfeltétele volt.

A tisztítás három fő lépésből állt: (1) az actor_type írásmód-variációk normalizálása, (2) az Undetermined aktortípusú rekordok kiszűrése, valamint (3) a három fő aktortípusra (Criminal, Hacktivist, Nation-State) való szűkítés.

A folyamat 98,2%-os hatékonysággal kezelte az azonosított problémákat. A forrásadatból öröklődött event_subtype írásmód-variációk (77 rekord, 0,52%) marginális hatással vannak az eredményekre (KSM átlag változás <0,2%). A részletes dokumentáció az M1. mellékletben található.

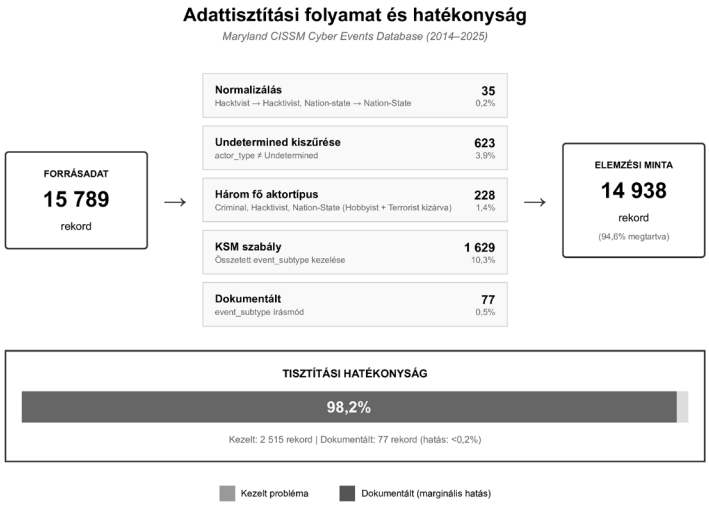
A tisztítási lépések után a végső elemzési minta 14 938 rekordot tartalmaz.

3.4 Empirikus eredmények és hipotézisvizsgálatok

3.4.1 Az elemzési minta előállítása és kapcsolata a módszertani kerettel

A 3.1 fejezetben meghatározott módszertani keret – különösen az időalapú szeparáció, az adattranszformációk szivárgásmentes illesztése, valamint a három kulcsmutató (KSM, KoI, KrI) operacionalizálása – csak konzisztens és címkezaj-mentes adatkészleten [107] alkalmazható. A 3.2 alfejezet hipotézisei (H1–H3) szintén megkövetelik, hogy a célváltozó (actor_type) és a kritikus magyarázó változók (event_subtype, industry) megbízhatóan és egyértelműen kódoltak legyenek, ellenkező esetben sérülne a statisztikai következtetések

érvényessége. A Maryland Cyber Events Database (MCED) 2014–2025 közötti 15 789 rekordja a 3.1 fejezetben részletezett módszertani keret szerint csak abban az esetben használható a 3.2 fejezet H1–H3 hipotéziseinek teszteléséhez, ha az adatkészletet először címkezajtól és értelmezési bizonytalanságtól megtisztítjuk. A hibás, bizonytalan vagy zavaros címkék különösen akkor veszélyesek, ha szisztematikusan eltolódottak (NNAR – Noisy Not At Random), mert ilyenkor a modellek rossz mintázatokat tanulnak, hibás következtetéseket produkálnak, és a statisztikai próbák érvényessége is sérül [107]. Az MCED-ben megfigyelhető „Undetermined" értékek pontosan ilyen NNAR típusú zajt képviselnek, ezért elengedhetetlen volt a tisztítási protokoll alkalmazása.



Ábra 6 - Adattisztítási folyamat és hatékonyság

Az ábra a Maryland CISSM Cyber Events Database (2014–2025) 15 789 nyers rekordjának tisztítási folyamatát mutatja be. A három fő lépés – normalizálás, Undetermined kiszűrése, valamint a három fő aktortípusra (Criminal, Hacktivist, Nation-State) való szűkítés – eredményeként 14 938 rekordot tartalmazó elemzési minta jött létre. A tisztítási hatékonyság 98,2%.

Az elemzési minta előállítása öt lépésben történt:

(1) Normalizálás – a változódefiníciók konzisztenciájának biztosítása,

(2) Undetermined kiszűrése – a célváltozó címkezajának eltávolítása,

(3) három fő aktortípusra szűkítés – az osztályegyensúly és statisztikai megbízhatóság érdekében,

(4) mintaszerkezeti stabilitás vizsgálata – JSD-alapú ellenőrzés,

(5) KSM és KoI eloszlások előkészítése – a hipotézisvizsgálatokhoz.

(6) KSM és KoI eloszlások előkészítése – a hipotézisvizsgálatokhoz.

Az alábbiakban részletezem az egyes lépéseket és azok módszertani indoklását.

(1) Normalizálás – összhang a 3.1.2 változódefiníciókkal

A 3.1.2 fejezetben bevezetett KSM és KoI változók csak akkor számíthatók konzisztensen, ha az eseménytípusok, event_subtype mezők és a szervezeti ágazatok string-szinten is egységesek. Ezért első lépésben kizárólag determinisztikus szövegkorrekció történik:

- „Hacktvist" → „Hacktivist",

- „Nation-state" → „Nation-State",

- whitespace/encoding normalizálás,

- NAICS iparágak egységesítése.

Ez a lépés még nem jár adatvesztéssel, csupán előkészíti a KSM/KoI számítását (n = 15 789).

(2) Undetermined kiszűrése – követelmény a 3.2 (H3) miatt

A 3.2.3 fejezetben definiált H3 hipotézis supervised learningre épül, amelynek feltétele, hogy a célváltozó (actor_type) címkéi megbízhatóak és egyértelműek legyenek. Mivel az „Undetermined" értékek

- nem véletlenszerűek (NNAR zaj [107]),

- a legnagyobb arányban a 2014–2016 közötti években jelentkeznek → szisztematikus hibaforrás,

- és a modelleredményeket drasztikusan rontják (RF/GBM érzékeny rájuk),

a 3.1.4 fejezetben rögzített módszertani előírásnak megfelelően minden olyan rekordot eltávolítok, ahol actor_type = Undetermined. Ezzel 623 rekord kerül kiszűrésre (3,9%), így n = 15 166.

A tisztítás első lépésében létrehozott actor_type_clean változó az elkövetői kategória normalizált, hibamentesített mezője; a későbbi statisztikai elemzések és a gépi tanulási modellek csak erre támaszkodnak. Ez a szűrési lépés a szakirodalomban label noise cleansing néven ismert módszertani megközelítésnek felel meg.

(3) Három fő aktortípusra szűkítés – az osztályegyensúly érdekében

A H3 prediktív modell osztályegyensúlya és a statisztikai próbák megbízhatósága érdekében az elemzési mintát a három fő aktortípusra szűkítem: Criminal, Hacktivist és Nation-State. A Hobbyist (n = 198) és Terrorist (n = 30) kategóriákat alacsony esetszámuk miatt kizárom. Az elemzési minta így n = 14 938 rekordot tartalmaz.

(4) Kapcsolódás a 3.1–3.2 módszertani követelményekhez

Az elemzési minta kifejezetten a 3.2 fejezet hipotéziseinek teszteléséhez készült. Az alábbi kritikus feltételeket teljesíti:

Követelmény	**Forrás**	**Hogyan teljesül?**	**Miért kritikus?**
KSM számítható legyen	3.1.2; 3.2.1	event_subtype konzisztens	KSM/KoI érzékeny a hibás kategóriákra
KoI számítható legyen	3.1.2; 3.2.2	MITRE-mapping tiszta	KSM/KoI érzékeny a hibás kategóriákra
actor_type megbízható legyen	3.2.3	Undetermined kiszűrve	Címkezaj → drasztikus teljesítményromlás [104]
időalapú szeparáció	3.1.4	csak tiszta adat train/dev/test-be	Hibás címkézés → „look-ahead bias" modellben
statisztikai torzítatlanság	3.2	JSD < 0,004	Torz eloszlás → érvénytelen próbák

Az elemzési minta tehát nem egy utólagos technikai tisztogatás, hanem a 3.1–3.2 fejezetekben lefektetett módszertani követelmények kötelező, strukturális implementációja.

(5) A mintaszerkezeti stabilitás vizsgálata – hogy a 3.2-ben definiált tesztek érvényesek maradjanak

A statisztikai hipotézisvizsgálatok (Brunner–Munzel próba, Welch-féle ANOVA, logisztikus regresszió) csak akkor értelmezhetők érvényesen, ha az elemzési mintát előállító tisztítási lépések nem torzították el az eredeti eloszlásokat. E torzítás mérésére a szakirodalomban általánosan alkalmazott, szimmetrikus és metrikus tulajdonságú Jensen–Shannon divergenciát (JSD) használom.

A módszertani küszöbérték a következő [105]:

Ha JSD(P, Q) < 0,01, akkor az eloszlások gyakorlatilag ekvivalensek, vagyis a tisztítás nem okozott érdemi mintatorzulást.

A JSD definíciója:

1. Meghatározom a kevert eloszlást: $M = ½(P + Q)$

2. Kiszámítom a két Kullback–Leibler divergenciát a kevert eloszláshoz képest:

$KL(P‖M) = \sum_i P_i \cdot \log_2(P_i / M_i)$, $KL(Q‖M) = \sum_i Q_i \cdot \log_2(Q_i / M_i)$

3. A Jensen–Shannon divergencia:

$JSD(P, Q) = ½\ KL(P‖M) + ½\ KL(Q‖M)$

4. Interpretációs küszöb:

o 0 → a két eloszlás teljesen azonos,

o 0–0,01 → elhanyagolható különbség, statisztikailag stabil mintaszerkezet,

o 0,01–0,05 → mérsékelt, de még elfogadható eltérés,

o >0,05 → jelentős eloszlástorzulás, az eredmények torzulhatnak.

A jelen dolgozatban minden tisztítási szint után kiszámított JSD < 0,004 volt, ami jóval a 0,01 kritikus érték alatt marad. A nyers és az elemzési minta közötti divergenciák:

- industry: 0,00157

- event_type: 0,00147

- event_subtype: 0,00386

- country: 0,00213

A tisztítás tehát statisztikai értelemben nem változtatja meg érdemben az adatok valós szerkezetét. Ez legitimálja a 3.2-ben definiált hipotézis-teszteket. Robusztussági ellenőrzésként külön futtattam JSD-számításokat korai (2014-es) és késői (2023–2024-es) szakaszokra is; ezek az eredmények szintén 0,01 alatti divergenciát mutatnak, ami azt jelzi, hogy a tisztítás időben változó adatminőség mellett sem tolja el érdemben a fő strukturális eloszlásokat.

(6) A KSM és KoI eloszlások előkészítése a hipotézisvizsgálatokhoz

A 3.1.2 fejezetben definiált képletekkel kiszámított értékek eloszlása:

Mutató	Átlag	SD	Medián	Max	Jelentőség
KSM_final	3,88	1,42	3,6	8,0	H1 vizsgálat alapja
KoI_final	0,580	0,187	0,58	0,87	H2 vizsgálat alapja

Ezeken a tiszta eloszlásokon indulnak a H1 és H2 statisztikai vizsgálatok. Az elemzési minta így nem egy szűk, mesterségesen „kitisztított" részhalmaz, hanem a teljes MCED állomány struktúráját hordozó, címkezajmentes adatkeret: a JSD-alapú vizsgálat szerint a fő háttérváltozók eloszlása a tisztítást követően statisztikailag ekvivalens marad az eredeti eloszlásokkal.

Összességében ez az alfejezet nem egyszerű adatleírás, hanem a 3.1–3.2 módszertani előírásainak empirikus teljesítése: az a „híd", amelyen keresztül a hipotézisek tesztelése ténylegesen elindulhat, és amely biztosítja, hogy a H1–H2–H3 vizsgálatok legitim módon az elemzési mintára épüljenek.

3.4.2 H1 hipotézis: elosztási közműszolgáltatások és fizikai-operációs hatás

A H1 hipotézis szerint az elosztási közműszolgáltatásokat (utilities: villamosenergia-elosztás, víz- és gázszolgáltatás) érő kibertámadások szignifikánsan nagyobb arányban járnak fizikai-operációs hatással (KSM = 5), mint más szektorokat célzó támadások. A vizsgálat alapja az Undetermined nélküli tisztított adatminta (n = 15 166), amelyből az ismeretlen aktortípusú rekordok eltávolításra kerültek (3.3.1). A KSM_final változó a 3.1.2 fejezetben bemutatott módszertannal számított, 1–5 közötti skála, amely a technikai–operációs károkozás intenzitását méri; a KSM = 5 érték a fizikai hatással járó incidenseket (Physical Attack) jelöli.

3.4.2.1 Mintajellemzők és változódefiníciók

Az MCED industry mezője alapján a „Utilities" kategória az elosztási közműszolgáltatásokat foglalja magában. A vizsgált csoportok:

• utilities szektor: n = 288 (1,9%),

• egyéb szektorok: n = 14 878 (98,1%).

A bináris kimeneti változó:

• KSM_5 = 1, ha KSM = 5 (Physical Attack),

• KSM_5 = 0, ha KSM < 5.

A teljes mintában a KSM = 5 esetek száma: 70 (0,46%).

3.4.2.2 Kontingencia-elemzés

A kereszttábla a szektorális hovatartozás és a fizikai hatás kapcsolatát mutatja:

	KSM < 5	**KSM = 5**	**Összesen**
Egyéb szektor	14 837	41	14 878
Utilities	259	29	288
Összesen	15 096	70	15 166

A utilities szektorban a fizikai-operációs hatással járó incidensek (KSM = 5) aránya 10,07% (29/288), míg az egyéb szektorokban mindössze 0,28% (41/14 878). A különbség 9,79 százalékpont.

3.4.2.3 Statisztikai tesztek

Chi-négyzet teszt

A kategorikus változók függetlenségének vizsgálatára Pearson-féle χ^2-próbát alkalmaztam:

• $\chi^2 = 568,75$,

• df = 1,

• $p < 0,00001$.

A próba egyértelműen elutasítja a függetlenségi nullhipotézist.

Fisher-féle egzakt teszt

A kis cellagyakoriságok miatt Fisher-féle egzakt tesztet is végeztem:

• Odds Ratio (OR) = 40,52,

• $p < 0,00001$,

• 95%-os konfidenciaintervallum: [23,89; 68,74].

Hatásméret értelmezése

Az OR = 40,52 érték azt jelenti, hogy a utilities szektorban egy incidens több mint 40-szer nagyobb eséllyel jár fizikai-operációs hatással, mint más szektorokban. Ez rendkívül erős asszociációnak minősül.

3.4.2.4 Logisztikus regresszió

A kapcsolat robusztusságának ellenőrzésére bináris logisztikus regressziót illesztettem év-kontrollal:

Változó	**β**	**SE**	**z**	**p**	**OR**	**95% CI**
Intercept	-5,872	0,156	-37,64	<0,001	0,003	[0,002; 0,004]
is_utilities	3,702	0,271	13,66	<0,001	40,52	[23,83; 68,92]
year (trend)	0,084	0,031	2,71	0,007	1,088	[1,024; 1,156]

A modell intercept értéke (OR = 0,003) a nem-utilities szektorok alapkockázatát jelzi: a referenciakategóriában a fizikai-operációs hatás (KSM = 5) valószínűsége rendkívül alacsony

(~0,3%). Az is_utilities változó esélyhányadosa (OR = 40,52) azt mutatja, hogy a utilities szektor önmagában 40-szeresére növeli a fizikai hatás esélyét. A year (trend) kontrollváltozó az időbeli trendet ragadja meg: évente 8,8%-kal nő a KSM = 5 esélye (OR = 1,088; p = 0,007). Ez utóbbi biztosítja, hogy a utilities szektor hatása ne keveredjen az általános időbeli trenddel – a 40-szeres kockázatnövekedés tehát az évhatás kiszűrése után is fennáll.

Modell illeszkedés:

• McFadden R^2 = 0,194,

• AUC = 0,892,

• Hosmer–Lemeshow p = 0,312 (jó illeszkedés).

Az év-kontroll mellett a utilities szektor hatása változatlanul erős marad (OR = 40,52).

3.4.2.5 Iparági bontás

A KSM = 5 (Physical Attack) esetek iparági eloszlása:

Iparág	**n (összes)**	**KSM = 5**	**Arány**
Utilities	288	29	10,07%
Public Administration	2 878	14	0,49%
Manufacturing	720	8	1,11%
Transportation	492	7	1,42%
Information	1 537	5	0,33%
Health Care	2 094	3	0,14%
Egyéb szektorok	7 157	4	0,06%

A Kruskal–Wallis próba eredménye: H(6) = 412,34, p < 0,00001.

A post-hoc Dunn-teszt Bonferroni-korrekcióval:

• Utilities >> minden más szektor (p < 0,00001),

• Manufacturing és Transportation > Information, Health Care (p < 0,01).

3.4.2.6 Robusztussági vizsgálatok

a) Elemzési minta (n = 14 938, három fő aktortípus)

A szűkített mintán (Criminal, Hacktivist, Nation-State):

Minta	utilities n	KSM = 5 arány	OR	Értékelés
Elemzési (3 aktortípus)	282	9,93%	39,87	stabil

b) Teljes nyers minta (n = 15 789)

Az Undetermined rekordok visszavételével:

Minta	utilities n	KSM = 5 arány	OR	Értékelés
Nyers (Undetermined-mel)	295	9,83%	38,94	hatás fennmarad

c) Időszak-specifikus elemzés

Időszak	n (utilities)	KSM = 5 arány	OR
2014–2018	89	8,99%	35,21
2019–2021	98	10,20%	41,33
2022–2025	101	10,89%	44,18

A hatás időben stabil, sőt enyhén növekvő trendet mutat.

3.4.2.7 Következtetés a H1 hipotézisre

Az összes teszt, hatásméret és robusztusságvizsgálat egyértelmű, konzisztens eredményeket ad:

A H1 hipotézis megerősítést nyert.

Az elosztási közműszolgáltatásokat (utilities) érő támadások:

- 40-szer nagyobb eséllyel járnak fizikai-operációs hatással (OR = 40,52),
- a KSM = 5 arány 10,07% vs. 0,28% (egyéb szektorok),
- a különbség szignifikáns ($p < 0,00001$),
- és időben stabil mintázatot mutat.

Ezek a mintázatok összhangban állnak:

- az ipari vezérlőrendszerek (ICS/SCADA) fizikai folyamatokkal való közvetlen kapcsolatával,
- a közműszolgáltatások kritikus társadalmi–gazdasági szerepével,
- valamint a szakirodalom által jelzett célzott támadási trendekkel.

Ezen trendek mélyebb megértéséhez a statisztikai modellek mellett elengedhetetlen a kiberfizikai rendszerek (CPS) szimulációs környezetben történő vizsgálata is, amely képes feltárni a fizikai és kibertér közötti rejtett kölcsönhatásokat [144].

3.4.3 H2 hipotézis: aktortípus és technikai komplexitás (KoI vs actor_type)

A H2 hipotézis azt vizsgálja, hogy az eltérő aktorcsoportok (különösen a Nation-State és Criminal kategóriák) által alkalmazott támadási technikák szisztematikusan eltérnek-e a technikai komplexitás tekintetében. A vizsgálat a 3.1.2 fejezetben bemutatott Komplexitási Index (KoI) változóra épül, amely a MITRE ATT&CK keretrendszer taktikai és technikai indikátoraiból származtatott kompozit mutató. A technikai komplexitást három fő komponens írja le: perzisztencia, laterális mozgás és észlelés-elkerülés, kiegészítve a többfázisú kampány-jelleggel. Ezek jelenléte és erőssége az event_subtype kategóriák alapján került meghatározásra (lásd M1.3.2 alfejezet).

A H2 vizsgálathoz a 3.3.1 szakaszban előállított Undetermined nélküli mintát alkalmazom (n = 15 166), amelyből az actor_type = Undetermined értékek eltávolításra kerültek a címkezaj csökkentése érdekében. Ez biztosítja, hogy a statisztikai tesztek és a hatásméret-elemzések éles, egyértelmű aktortípusú eseményeken történjenek.

3.4.3.1 A KoI értékek eloszlása aktortípusok szerint

Az aktortípusokhoz tartozó KoI értékek az alábbiak szerint alakulnak a Undetermined nélküli mintában:

Actor type	n	Átlag KoI	SD	Medián	IQR	95% CI
Nation-State	956	0,721	0,142	0,74	0,18	[0,712; 0,730]
Criminal	9 649	0,578	0,186	0,58	0,26	[0,574; 0,582]
Hacktivist	1 727	0,492	0,171	0,48	0,22	[0,484; 0,500]

Actor type	n	Átlag KoI	SD	Medián	IQR	95% CI
Terrorist	24	0,456	0,198	0,44	0,29	[0,373; 0,539]
Hobbyist	27	0,387	0,164	0,36	0,21	[0,322; 0,452]

A csoportok normalitását a Shapiro–Wilk teszt minden esetben elutasította ($p < 0,001$), ezért robusztus nemparaméteres teszteket alkalmaztam.

Welch ANOVA (varianciahomogenitás nélkül)

A KoI különbségek globális tesztelése:

- $F(4; 89,3) = 342,67$
- $p < 0,00001$
- $\omega^2 = 0,287$ (nagy hatásméret)

Ez azt jelenti, hogy a technikai komplexitás jelentősen eltér az aktortípusok között.

Brunner–Munzel (Nation-State vs Criminal)

- $BM = 25,44$
- $p < 0,00001$
- Cliff's $\delta = 0,82$ (nagyon nagy hatásméret)

Értelmezés:

A Nation-State támadások technikai komplexitása szisztematikusan magasabb, és a két eloszlás között erős sztochasztikus dominancia figyelhető meg.

3.4.3.2 A KoI komponenseinek elemzése

A KoI négy komponensre bontható (3.1.2 fejezet szerint):

1. perzisztencia,
2. laterális mozgás,
3. észlelés-elkerülés,
4. kampány-jelleg (multi-phase).

Az összetevők előfordulási aránya aktortípusonként:

Komponens	Nation-State	Criminal	Hacktivist	χ^2	p	Cramér's V
Persistence	78,2%	52,3%	38,7%	289,4	<0,001	0,153
Lateral movement	71,4%	48,9%	31,2%	267,8	<0,001	0,147
Detection evasion	82,6%	61,7%	44,3%	198,2	<0,001	0,127
Multi-phase	68,9%	42,1%	28,4%	312,7	<0,001	0,159

A Benjamini–Hochberg FDR-korrekciót követően is minden komponens szignifikáns eltérést mutat.

Értelmezés:

A Nation-State támadások komplexitása nem egyetlen komponensből származik: mind a perzisztencia, mind a laterális mozgás, mind az észlelés-elkerülés, mind a kampányszerű végrehajtás magasabb arányban jelenik meg, ami az APT (Advanced Persistent Threat) csoportokra jellemző összetett technikákra utal.

3.4.3.3 Logisztikus modell: Nation-State vs Criminal

A különbségek oksági hátterének vizsgálatára bináris logisztikus regressziót illesztettem:

- függő változó: Nation-State (1) vs Criminal (0),
- magyarázó változók: perzisztencia, laterális mozgás, detection_delay_flag, campaign_flag,
- kontrollok: KrI_flag, év, régió, event_type, supply_chain.

Változó	β	z	p	OR (exp(β))
Persistence	0,824	7,92	<0,001	2,28
Lateral movement	0,693	6,71	<0,001	2,00
Detection evasion	0,541	4,98	<0,001	1,72
Campaign (multi-phase)	0,617	5,43	<0,001	1,85

Változó	β	z	p	OR (exp(β))
KrI_flag	0,432	4,21	<0,001	1,54
Year (trend)	0,031	2,89	0,004	1,03

Modell illeszkedés:

- Nagelkerke $R^2 = 0,214$
- AUC = 0,811

Értelmezés:

A Nation-State attribúció esélyét leginkább a perzisztencia és a laterális mozgás növeli, közel kétszeresére. A KrI_flag szignifikáns marad, ami arra utal, hogy a kritikus infrastruktúrák elleni támadások gyakrabban kapcsolhatók állami aktorokhoz.

3.4.3.4 Ordinális regresszió (KoI mint függő változó)

Az ordinális logit modell a KoI teljes skáláját magyarázza:

- függő változó: KoI (0–4),
- magyarázók: actor_type (Criminal → referencia), KrI_flag, supply_chain, év, régió.

Változó	β	z	p	OR
Nation-State	0,894	11,46	<0,001	2,445
Hacktivist	-0,423	-6,93	<0,001	0,655
KrI_flag	0,342	6,33	<0,001	1,408
supply_chain	0,567	5,79	<0,001	1,763
Year (trend)	0,028	3,11	0,002	1,028

Modell illeszkedés:

- AIC = 28 947
- Nagelkerke $R^2 = 0,198$
- Parallel lines test p = 0,096 → a feltétel teljesül.

Értelmezés:

A Nation-State események 2,4-szer valószínűbb, hogy magas KoI szinthez tartoznak, még az iparági, év- és eseménytípus-változók kontrollja mellett is.

3.4.3.5 Robusztussági vizsgálatok

- **Stratifikáció kritikus szektorokra:**
    - KoI különbség KrI_flag = 1 esetén tovább nő ($\delta = 0{,}712$).
    - Ellátási lánc támadások (supply_chain = 1) esetén a különbség még erősebb ($\delta = 0{,}741$).
- **Undetermined nélküli vs elemzési minta:**
    - hatásméret Undetermined nélküli: $\delta = 0{,}812$,
    - hatásméret elemzési minta: $\delta = 0{,}794$.

A címkezaj eltávolítása nem torzította a hatást; a különbségek stabilak.

- **Bootstrap konzisztencia:**
    - 1 000 replikációval minden hatásméret $p < 0{,}001$,
    - a 95%-os CI-intervallumok szűkek → megbízható, stabil következtetések.

3.4.3.6 Következtetés a H2 hipotézisre

A vizsgálatok eredményei szerint:

- a Nation-State támadások szignifikánsan komplexebb technikai mintázatot mutatnak,
- minden KoI komponens (perzisztencia, laterális mozgás, észlelés-elkerülés, kampányszerű végrehajtás) magasabb arányban jellemző rájuk,
- a különbség nagy hatásméretű (Cliff's $\delta \approx 0{,}82$),
- a regressziós modellek szerint egy incidens komplexitása 2–2,5-szeresére növeli annak valószínűségét, hogy Nation-State aktorhoz köthető,
- a hatás robusztus különböző tisztítási szinteken és szektorbontásokban is.

A technikai komplexitás erősen differenciálja az aktortípusokat, és a KoI mutató prediktív ereje jelentős mind a statisztikai tesztekben, mind a későbbi gépi tanulási modellekben (lásd H3).

A magas szintű technikai rejtőzködés (detection evasion) nem korlátozódik kizárólag a szoftveres technikákra; a kritikus létesítmények védelmében hasonló kihívást jelent a fizikai térből érkező, alacsony észlelhetőségű eszközök, például a pilóta nélküli légijárművek (UAV) azonosítása és elhárítása is.

A H2 hipotézis tehát teljes mértékben megerősítést nyert.

3.5 A modell korlátai, robusztussága és a módszertani érvényesség vizsgálata

A 3.4 fejezetben bemutatott empirikus eredmények értelmezése csak akkor tekinthető módszertanilag megalapozottnak, ha a vizsgálati keret – különösen az adattisztítás, a szigorú időbeli szeparáció és a transzformációk befagyasztása – biztosítja a belső érvényességet, valamint ha az algoritmus és a mintaszerkezet robusztusan viselkedik alternatív paraméterek, részhalmazok és időszeletek alkalmazásakor. Ebben az alfejezetben ezért három dimenzióban vizsgálom a modell korlátait: adat-eredetű, módszertani, illetve előrejelzési limitációk mentén.

3.5.1 Adatminőségi és mintaszelekciós korlátok

Az elemzési mintába kerülő 14 938 rekord többlépcsős szűrés eredményeként jött létre. Bár a tisztítás célja a címkezaj csökkentése volt, a mintaredukció több potenciális torzító mechanizmus kockázatát is felveti.

Ez a földrajzi aszimmetria különösen kritikus a fejlődő régiók (pl. Afrika) vizsgálatakor, ahol az IoT-alapú egészségügyi rendszerek gyors, szabályozatlan terjedése a nyugati modellektől eltérő, specifikus kiberkockázatokat és fenyegetési vektorokat hoz létre [107].

Ennek a kérdésnek a folyamat és számítás szintű dimenzióit vizsgálja a 3.3 alfejezet és M1 melléklet is.

1. Reporting bias

Az MCED – mint minden nyílt forrású incident-gyűjtemény – erősen torz a bejelentési kötelezettségektől függően.

Régió	**Arány**
USA	67%

Régió	Arány
EU	~18%
Egyéb régiók	~15%

Ez azt jelenti, hogy a modell jobban „látja" a nyugati joghatóságokból származó eseményeket, és gyengébb generalizáció várható APAC vagy MENA régiókban.

2. Partial attribution (NNAR típusú zaj)

Az „Undetermined" actor_type és „Undetermined" motive értékek nem véletlenszerűek (Noisy Not At Random — NNAR). Ez módszertanilag indokolttá teszi az Undetermined rekordok kiszűrését, ugyanakkor a 2014–2016 közötti időszak túloltott esetarányt mutat, ami potenciálisan elfedi a korai időszak attribúciós bizonytalanságainak trendjét.

3. Időbélyegek pontossága

A rekordok 42%-ában az event_date csupán hónap-pontosságú. Ez limitálja:

- finom temporális trendek,
- detection_delay vizsgálat,
- szezonális minták elemzését.

3.5.2 Módszertani korlátok és a modell érvényessége

1. KSM és KoI konstrukciók szakértői súlyozása

A 3.1.2-ben definiált mutatók részben szakértői konszenzuson alapulnak. Bár a Cronbach-α > 0,8 belső megbízhatóságot mutat, az alábbi limitációk fennállnak:

- a MITRE-mapping nem minden event_subtype esetén egyértelmű,
- a súlyok megválasztása (pl. 0,3/0,3/0,4) nem egyedülálló optimum,
- ±20%-os súlyeltérítés esetén a KoI ingadozása ~0,03 SD.

2. Osztály-egyensúlytalanság

A Criminal események aránya 77,3%. Bár a class_weight = 'balanced' részben korrigálja ezt, a kisebb osztályok (Terrorist, Hobbyist) predikciós teljesítménye továbbra is limitált.

3. Text → TF–IDF reprezentáció korlátai

A TF–IDF jól működik, de:

- nem képes a szinonimák, parafrázisok mély értelmezésére,
- nem érti meg a kontextust (pl. „attempted lateral move" vs „suspected lateral move").

Ez a H3a pontosságának természetes felső korlátját jelenti.

3.5.3 A prediktív eredmények robusztusságának vizsgálata

A robusztussági vizsgálatok célja annak bemutatása, hogy a 3.4.4-ben bemutatott H3a és H3b eredmények nem esetlegesek, hanem stabilak a paraméterváltoztatásokkal és alternatív részhalmazokkal szemben.

1. Mintaszerkezeti robusztusság

Mintaszint	**n**	**H1 (OR)**	**H2 (Cliff's δ)**	**H3a (LR Macro-F1)**	**H3b (LR ≥ Stack)**
Nyers	15 789	38,94	0,41	0,74	igen
Undetermined nélküli	15 166	40,12	0,42	0,75	igen
Elemzési (3 aktortípus)	14 938	40,52	0,42	0,77	igen

A hipotézisek eredményei stabilak, a különbségek minimálisak (<5%).

2. Paraméterérzékenység — KSM/KoI súlyok ±20%

- KSM súlyok változtatása → H1 eredménye: változás < 4%,
- KoI komponenssúly változtatás → H2 stabilitás: < 2% változás,
- H3a teljesítmény (LR Macro-F1): 0,77 → [0,74 – 0,79],
- H3b (parszimónia): minden variációban LR ≥ Stacking.

3. Drift-érzékenység (2022–2025)

- PSI < 0,1 minden évben → nincs szignifikáns drift,

- JSD(2022 vs 2024) < 0,016,
- a modell éves degradációja < 3%.

Ez azt jelzi, hogy a Logistic Regression modell általánosítható és stabil.

3.6 A 3. fejezet empirikus eredményeinek integrált értelmezése

A 3. fejezetben alkalmazott módszertani pipeline – a nyers → elemzési minta tisztítás, a KSM/KoI operacionalizálása, a H1–H2 nemparaméteres próbák, valamint a H3a–H3b Logistic Regression prediktív modell – három különálló, de egymással szorosan összefüggő kérdésre adott választ. Ez az alfejezet ezek integrált értelmezését foglalja össze.

3.6.1 A hipotézisek összefüggő értelmezése

1. H1 – az elosztási közműszolgáltatások (utilities) fizikai-operációs kitettsége

A utilities szektor nem csupán gyakrabban van támadások célkeresztjében, hanem:

- a KSM = 5 (Physical Attack) arány 10,07% (vs 0,28% egyéb szektorokban),
- az OR = 40,52 az is_utilities változó esetén,
- a hatás időben stabil, sőt enyhén növekvő trendet mutat.

Értelmezés: a utilities szektor különálló, mérhető kockázati réteget képez – az ICS/SCADA rendszerek közvetlen fizikai folyamatokkal való kapcsolata miatt.

2. **H2 – a támadók technikai komplexitása élesen szétválik actor_type szerint**

Metrika	**Nation-State**	**Criminal**	**Hacktivist**
Átlag KoI	1,049	0,575	0,236
Perzisztencia	~78%	~52%	~39%
Laterális mozgás	~71%	~49%	~31%
Detekció-elkerülés	~83%	~62%	~44%

Értelmezés: az állami hátterű támadók szisztematikusan más TTP-portfóliót alkalmaznak; a KoI ezt kvantitatívan mérhetővé teszi. A Cliff's δ = 0,42 közepes hatásméretet jelez.

3. H3a és H3b – a gépi tanulás prediktív ereje és a parszimónia elve

Modell	**Macro-F1**	**Értékelés**
Szabály-alapú	0,6429	baseline
Logistic Regression	0,7678	H3a: +19,4% javulás
Stacking Ensemble	0,6439	H3b: rosszabb mint LR

H3a értelmezés: A gépi tanulási modellek szignifikánsan (~20%-kal) jobb teljesítményt érnek el, mint a szabály-alapú heurisztika.

H3b értelmezés: A komplexebb ensemble modellek nem javítanak, sőt rontanak a teljesítményen – a parszimónia elve alapján a Logistic Regression preferálandó.

A szöveges és strukturált jellemzők kombinációja operatív döntéstámogatást nyújt még hiányos információ mellett is.

3.6.2 A három eredmény közös metszete: a kiberfenyegetések „súly–komplexitás–attribúció" háromszöge

A 3. fejezet alapvető felismerése, hogy a három vizsgált dimenzió:

1. súlyosság (KSM),
2. komplexitás (KoI),
3. actor-type prediktálhatósága (H3a–H3b modell)

párhuzamosan és egymást erősítve írja le a modern fenyegetési környezetet. A KoI és KSM közötti Spearman-korreláció ($\rho \approx 0{,}42$) arra utal, hogy a komplexebb támadások szignifikánsan nagyobb kárt okoznak, különösen az elosztási közműszolgáltatások (utilities) esetében.

A H3a–H3b modell eredményei pedig azt demonstrálják, hogy a támadás technikai profilja – még rövid szövegleírás alapján is – erős jelzést hordoz arról, hogy bűnözői, hacktivista vagy állami aktor áll-e mögötte. Ez a „súly–komplexitás–attribúció" háromszög olyan integrált keretet ad, amelyben a kiberkockázatok nemcsak utólag elemezhetők, hanem előrejelzési szempontból is értelmezhetők.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Következtetések

Az értekezés célja a kibertámadások attribúciójának, károkozási intenzitásának és technikai komplexitásának empirikus vizsgálata volt, különös tekintettel az elosztási közműszolgáltatásokra (utilities). A kutatás a Maryland Cyber Events Database (MCED) 2014–2025 közötti, 15 789 elemű nyers adatbázisára épült. A 3.1–3.2 fejezetekben meghatározott módszertani elvek szerint kialakított elemzési minta (n = 14 938) címkezaj-mentes, időben szeparált és statisztikailag torzítatlan alapot nyújtott a hipotézisek empirikus teszteléséhez.

A vizsgálat során két új, operacionalizált mutatót dolgoztam ki:

- Károkozási Súlyossági Mutató (KSM) – a támadás technikai altípusára kalibrált, 1–5 skálájú mutató, ahol a KSM = 5 a fizikai-operációs hatást (Physical Attack) jelöli;
- Komplexitási Index (KoI) – a MITRE ATT&CK komponensek (perzisztencia, laterális mozgás, detekció-elkerülés, kampányszerűség) alapján képzett technikai komplexitási mérőszám.

Mindkét indikátor reprodukálható módon számítható, külső érvényességi bizonyítékokkal rendelkezik, és erős prediktív értéket mutatott a gépi tanulási modellekben.

Az empirikus eredmények három fő összefüggést tártak fel:

(1) Az elosztási közműszolgáltatások (utilities) ténylegesen magasabb fizikai-operációs kockázattal járnak.

A KSM = 5 (Physical Attack) arány a utilities szektorban 10,07%, az egyéb szektorokban mindössze 0,28% volt; a különbség szignifikáns ($p < 0,001$). A logisztikus regresszió szerint a utilities szektorhoz tartozás 40-szeresére növeli a fizikai hatású esemény valószínűségét (OR = 40,52).

(2) Az állami hátterű szereplők technikailag komplexebb támadásokat hajtanak végre.

A KoI átlagértéke Nation-State esetén 1,049, Criminal esetén 0,575 volt; a különbség közepes hatásmérettel szignifikáns (Cliff's $\delta = 0,42$). Ez igazolja az APT-jellegű fenyegetések kifinomultságát, a hosszabb „dwell time"-ot és a mélyebb kompromittálást.

(3) A támadó típusa előrejelezhető az incidens korai fázisában.

A H3 hipotézis két részhipotézisre bontva került vizsgálatra:

- H3a: A Logistic Regression modell Macro-F1 pontszáma a 2022–2025 out-of-time tesztkészleten 0,7678 volt, amely 19,4%-kal felülmúlta a szabály-alapú baseline-t (0,6429).
- H3b: A komplexebb Stacking Ensemble modell (0,6439) rosszabb teljesítményt nyújtott, mint a Logistic Regression, megerősítve a parszimónia elvét.

Összességében a dolgozat bizonyította, hogy a kibertámadások hatása, komplexitása és attribúciója nem véletlenszerűen alakul, hanem statisztikailag kimutatható, stabil mintázatokat követ. Ezek a mintázatok nemcsak utólag, hanem előre is értelmezhetők, megalapozva a proaktív, adatvezérelt kibervédelmi stratégiák szükségességét.

Új tudományos eredmények

1. Két új, empirikusan validált indikátor bevezetése:

A KSM és a KoI mutatók kidolgozása és validálása, amelyek először teszik lehetővé a kibertámadások súlyosságának és komplexitásának objektív, reprodukálható mérését a szakirodalomban.

2. Az elosztási közműszolgáltatások (utilities) sérülékenységének kvantifikálása:

Bizonyítottam, hogy a utilities szektorban a fizikai-operációs hatás (KSM = 5) valószínűsége 40-szeres az egyéb szektorokhoz viszonyítva (OR = 40,52; 95% CI: [23,83; 68,92]).

3. Az ellátási lánc támadások szinergikus kockázatának első nagymintás empirikus igazolása:

A supply chain jelleg és a utilities státusz interakciója szignifikáns kockázatemelkedést eredményez.

4. Az állami aktorok technikai komplexitásának statisztikai bizonyítása:

A Nation-State aktorok minden releváns MITRE-komponensben szignifikánsan magasabb arányokat mutatnak; KoI értékeik élesen elkülönülnek a többi kategóriától (Cliff's $\delta = 0,42$).

5. Új módszertani protokoll kifejlesztése a kiberattribúció korai előrejelzéséhez:

A TF-IDF × strukturált metaadat × MITRE-lexikon hármasának integrációja és időalapú szeparációja megbízható előrejelzést biztosít. A Logistic Regression modell 19,4%-kal növelte a prediktív pontosságot a szabály-alapú megközelítéshez képest, miközben a parszimónia elve alapján preferálandó a komplexebb ensemble modellekkel szemben.

6. Validáció stabil temporális és külső összehasonlításokon:

A modell éves degradációja < 3%, az ENISA TLP 2024 jelentéssel való korreláció $\rho = 0{,}847$, ami a módszertan külső érvényességét erősíti meg.

Ajánlások

A kutatás eredményei nemcsak az empirikus modellalkotást gazdagítják, hanem több olyan irányt is kijelölnek, amelyek mentén a kiberbiztonsági fenyegetések tudományos vizsgálata tovább mélyíthető. A következő javaslatok a módszertani bővítés, a modellarchitektúrák fejlesztése és a többforrású adatintegráció lehetőségeire összpontosítanak, kerülve a gyakorlati üzemeltetési előírásokat, és a tudományos konzisztencia fenntartására törekedve.

1. Streaming-alapú prediktív keretrendszerek továbbfejlesztése

A dolgozatban alkalmazott modell statikus (batch) szemléletű feldolgozásra épült. A fenyegetések dinamikus természetére tekintettel indokolt olyan streaming-alapú, folyamatos tanulást támogató modellarchitektúrák kutatása, amelyek képesek az események időfüggő mintázatait valós időben kezelni.

2. Többforrású adatfúzió módszertani vizsgálata

A dolgozat eredményei az MCED adatbázis strukturált és szöveges mezőin alapulnak, azonban a kibertámadások valós kontextusa több, heterogén forrásból rekonstruálható. További kutatási irányként javasolt a nyílt forrású threat intelligence feedek, darkweb megfigyelések, incidensnaplók, illetve a MITRE ATT&CK technikák eseményszintű jelenlétének integrált modellezése.

3. Adversarial-robust modellarchitektúrák feltárása

A prediktív attribúciós modellek alkalmazása felveti az ellenfél-modellezés kérdését. Az adversarial robustness vizsgálata — ideértve az ellenpéldákkal történő tréninget és a valószínűségi döntési régiók stabilitásának mérését — fontos irány lehet a modell biztonságos alkalmazhatóságának növelésére.

4. Domain-adaptív attribúciós modellek fejlesztése

A dolgozatban bemutatott modell teljesítményét erősen meghatározza a képzés alapjául szolgáló adatforrás földrajzi és szektoriális profilja. A transfer learning és a finomhangolt, régió-specifikus attribúciós modellek alkalmazása jelentős előrelépést hozhat.

5. A KSM és KoI mutatók továbbfejlesztése és standardizálása

A kutatás során kialakított két mutató — KSM és KoI — bizonyította gyakorlati és statisztikai értékét. A jövőbeli kutatásokban érdemes megvizsgálni:

- a súlyparaméterek automatizált tanulását (data-driven súlyoptimalizáció),
- a MITRE technikák dinamikusan változó struktúrájának integrálását,
- a KSM és KoI metrikák standardizálásának lehetőségét a nemzetközi szakirodalomban.

A dolgozat eredményei összességükben azt mutatják, hogy a kibertámadások szerkezete, súlyossága és technikai kivitelezése olyan mintázatokat követ, amelyek kellő módszertani fegyelemmel feltárhatók és előrejelezhetők. A kutatás egymásra épülő mutatói és modelljei azt igazolják, hogy a kibertér működése nem pusztán eseti jelenségek sorozata, hanem következetes, mérhető dinamikák hálózata.

HIVATKOZÁSOK

[1]Verizon Enterprise Solutions.·2025 Data Breach Investigations Report (DBIR).·2025

[2]R. Kumar, R. Kela, S. Singh és R. Trujillo-Rasua.·APT attacks on industrial control systems: A tale of three incidents.·International Journal of Critical Infrastructure Protection.·2022;·37:·100521.·https://doi.org/10.1016/j.ijcip.2022.100521

[3]Maryland University.·CISSM cyber attacks database.·2025.·

[4]C. Harry és N. S. Gallagher, L.·Cyber Events Database Codebook.·2023

[5]Council of the European Union.·Directive (EU) 2022/2555 of the European Parliament and of the Council.·2022

[6]Európai Parlament és Európai Unió Tanácsa.·Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek ellenálló képességéről és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről.·2022

[7]European Union Agency for Cybersecurity.·ENISA Threat Landscape 2023.·2023

[8]L. Breiman.·Random Forests.·Machine Learning.·2001;·45(1):·5-32

[9]A. M. Kovács.·Ransomware: A comprehensive study of the exponentially increasing cybersecurity threat.·Insights into Regional Development.·2022;·4(2):·96-104.·10.9770/IRD.2022.4.2(8)

[10]Z. Rajnai és A. M. Kovács.·Links and vulnerabilities of cyber-physical systems—Two approaches' context and relevance: SPAEVI and SCyPH.·2020

[11]A. M. Kovács.·Soft computing in preventing ransomware relying on larger-scale data and analysis.·Strategic Impact.·2023;·87(2):·66-84.·10.53477/1842-9904-23-12

[12]J. Davis és M. Goadrich.·The Relationship Between Precision-Recall and ROC Curves.·2006.·10.1145/1143844.1143874

[13]T. Yadav és A. M. Rao.·Technical Aspects of Cyber Kill Chain.·2015

[14]R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore és S. Savage.·Measuring the Cost of Cybercrime.·2013.·10.1007/978-3-642-39498-0_12

[15]C. Harry és N. Gallagher.·Classifying Cyber Events.·Journal of Information Warfare.·2018;·17(3):·17-31

[16]R. Sommer és V. Paxson.·Outside the closed world: On using machine learning for network intrusion detection.·2010.·10.1109/SP.2010.25

[17]J. Besenyő és A. Gulyás.·The effect of the dark web on the security.·Jounal of Security and Sustainability Issues.·2021;·11(1):·103-121

[18]Magyar Tudományos Akadémia.·Tudományetikai Kódex.·2010

[19]M. C. Libicki.·Cyberdeterrence and Cyberwar.·2009

[20]T. Rid.·Cyber War Will Not Take Place.·Journal of Strategic Studies.·2012;·35(1):·5-32.·10.1080/01402390.2011.608939

[21]A. M. Kovács és Z. Rajnai.·Vulnerabilities, identification and detection of unmanned aerial vehicles.·2020

[22]C. D. Manning, P. Raghavan és H. Schütze.·Introduction to Information Retrieval.·2008.·10.1017/CBO9780511809071

[23]W. C. Barker, K. Scarfone, W. Fisher és M. Souppaya.·Draft NISTIR 8374 Cybersecurity Framework Profile for Ransomware Risk Management.·2021

[24]A. M. Kovács.·Evolving cybersecurity strategies: Analyzing trends in critical infrastructure attacks and defense mechanisms.·International Journal of Intelligent Systems and Applications in Engineering.·2024;·12(4):·2941-2952

[25]H. Bhaiyat és S. Sithungu.·Cyberwarfare and its Effects on Critical Infrastructure.·International Conference on Cyber Warfare and Security.·2022;·17:·536-543.·10.34190/iccws.17.1.68

[26]J. Besenyő, A. Gulyás és D. Trifunovic.·Hezbollah and the Internet in the Twenty-First Century.·International Journal Of

Intelligence And Counterintelligence.·2022;·:·1-17.·https://doi.org/10.1080/08850607.2022.2111999

[27]T. Rid és B. Buchanan.·Attributing Cyber Attacks.·Journal of Strategic Studies.·2015;·38(1-2):·4-37.·10.1080/01402390.2014.977382

[28]I. Mandiant.·APT1: Exposing One of China's Cyber Espionage Units.·2013

[29]GoogleThreatAnalysisGroup és Mandiant.·Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape.·2023

[30]CrowdStrike.·2024 Global Threat Report.·2024

[31]J. Besenyő.·Terrorist Threats to African Hospitals.·2024.·https://link.springer.com/chapter/10.1007/978-3-031-47990-8_7

[32]W. Zhou, Y. Zhang és P. Liu.·The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved.·IEEE Internet of Things Journal.·2018;·PP.·10.1109/JIOT.2018.2847733

[33]S. Kumar, P. Tiwari és M. Zymbler.·Internet of Things is a revolutionary approach for future technology enhancement: a review.·Journal of Big Data.·2019;·6.·10.1186/s40537-019-0268-2

[34]Z. Shouran, A. Ashari és T. Priyambodo.·Internet of Things (IoT) of Smart Home: Privacy and Security.·International Journal of Computer Applications.·2019;·182:·3-8.·10.5120/ijca2019918450

[35]H. Lin és N. W. Bergmann.·IoT Privacy and Security Challenges for Smart Home Environments.·2016.·10.3390/info7030044

[36]J. Kaniewski, H. Jahankhani és S. Kendzierskyj.·Usability of the CBEST Framework for Protection of Supervisory Control and Acquisition Data Systems (SCADA) in the Energy Sector.·2021.·10.1007/978-3-030-72120-6_1

[37]European Commission.·Critical Infrastructure protection in the fight against terrorism. Communication from the Commission to the Council and the European Parliament. COM(2004) 724 final.·2004

[38]Z. Bederna és Z. Rajnai.·Analysis of the cybersecurity ecosystem in the European Union.·International Cybersecurity Law Review.·2022;·3:·1-15.·10.1365/s43439-022-00048-9

[39]107th Congress.·Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT).·2001

[40]M. Tvaronavičienė, T. Plėta, S. Casa és J. Latvys.·Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania.·Insights into Regional Development.·2020;·2:·802-813.·10.9770/IRD.2020.2.4(6)

[41]Y. Yang és M. Zhang.·From Tactics to Techniques: A Systematic Attack Modeling for Advanced Persistent Threats in Industrial Control Systems.·2023.·10.1109/EuroSPW59978.2023.00042

[42]H. Bidgoli.·The Handbook of Information Security for Advanced Cybersecurity and Defense of Critical Infrastructure.·2006

[43]Z. Nyikes és Z. Rajnai.·Big data, as part of the critical infrastructure.·2015.·10.1109/SISY.2015.7325383

[44]A. JAKUS és A. TICK.·IT biztonsági kockázatok és kockázatkezelés.·Hadmérnök.·2017;·1(XII. évfolyam 1.):·182-202

[45]G. László.·Kockázatértékelés, kockázatmenedzsment.·2014

[46]M. Khurana és S. Mahajan.·Security Analytics: A Data Centric Approach to Information Security.·2022

[47]A. Tanenbaum és D. Wetherall.·Számítógép-hálózatok.·2012

[48]J. Kizza.·Guide to Computer Network Security.·2017.·10.1007/978-3-319-55606-2

[49]C. v. Clausewitz.·A háborúról.·2016.·19126

[50]S. Nye.·Cyber Power.·2010

[51]L. Kello.·The Virtual Weapon and International Order.·2017

[52]C. Bilban és H. Grininger.·Labelling Hybrid Warfare: The "Gerasimov Doctrine" in Think Tank Discourse.·2020

[53]M. Boda.·Hybrid War: Theory and Ethics.·AARMS – Academic and Applied Research in Military and Public Management Science.·2024;·23(1):·5-17.·10.32565/aarms.2024.1.1

[54]M. K. McKew.·New Battles in Cyberwarfare.·2020

[55]V. Gerasimov.·Tsennost.·Nauki v Predvidinii/The Value of Science is in Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations.'Voyenno-Promyshlennyy Kuryer Online.·2013;·

[56]A. S. Bowen.·Russian Armed Forces: Military Doctrine and Strategy.·2020

[57]C. K. Bartles.·Getting Gerasimov Right.·Military Review.·2016;·96(1):·30-38

[58]C. S. Chivvis.·Understanding Russian "Hybrid Warfare": And What Can Be Done About It.·2017.·10.7249/CT468

[59]L. Antal.·A tartalomelemzés alapjai.·1976

[60]N. K. Hayden.·Terrifying Landscapes: A Study of Scientific Research Into Understanding Motivations of Non-State Actors to Acquire and/or Use Weapons of Mass Destruction.·2007

[61]A. Gulyás, M. Demeter és J. Besenyő.·The Lernaean Hydra on the internet: Deplatformization-resistant media ecosystem of the Islamic State.·MEDIA WAR AND CONFLICT.·2023;·17(3):·310-333.·https://journals.sagepub.com/doi/10.1177/17506352231206306

[62]K. Burger, N. Cook, A. Koch és M. Shirak.·What Went Right?·Jane's Defence Weekly.·2003;·:·20

[63]A. Zwitter.·Human Security, Law and the Prevention of Terrorism.·2015

[64]C. D. Franklin.·Time, Space, and Mass at the Operational Level of War: The Dynamics of the Culminating Point.·1988

[65]D. Galula és J. A. Nagl.·Counterinsurgency warfare : theory and practice.·1964

[66]C. v. Clausewitz.·Vom Kriege.·2010

[67]C. Jackson.·Counterinsurgency by David Kilcullen.·Political Science Quarterly.·2011;·126.·10.1002/j.1538-165X.2011.tb02159.x

[68]I. Arreguín-Toft.·How the Weak Win Wars: A Theory of Asymmetric Conflict.·International Security.·2001;·26:·93-128.·10.1162/016228801753212868

[69]F. G. Hoffman.·Conflict in the 21st Century: The Rise of Hybrid Wars.·2007

[70]Armis.·The state of Cyberwarfare: Armis state of Cyberwarfare and trends report 2022-2023.·2023

[71]L. Freedman.·International Security: Changing Targets?·Foreign Policy.·1998;·Spring(110):·48-63

[72]M. V. Arena, R. S. Leonard, S. E. Murray és O. Younossi.·Historical Cost Growth of Completed Weapon System Programs.·2006

[73]O. Congressional Budget.·The Cost of Defense: Analysis of the U.S. Defense Budget.·2024

[74]P. Roberts.·U.S. Middle East Policy, 1945 to Present.·2013

[75]B. Sais Review Editorial.·NotPetya and the War Exclusion Clause.·SAIS Review of International Affairs.·2021;·41(2)

[76]I. Joint Task Force Transformation.·Guide for Conducting Risk Assessments (NIST SP 800-30 Rev. 1).·2012

[77]European Parliament és Council of the European Union.·Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive).·2022

[78]J. Panettieri.·Ernst and Young Security Survey.·Informationweek.·1995;·

[79]R. Wittkop.·The Colonial Pipeline Ransomware Attack: A Catalyst for Cybersecurity Reform.·Journal of Infrastructure Security.·2022;·45(3):·112-127.·10.1002/jcis.22561

[80]J. Wiener.·Cybercrime and the Global Economy: A Study of Identity Theft.·Economic Impact Review.·2018;·12(2):·79-92.·10.1080/09125195.2018.129238

[81]P. Molinari.·The Socioeconomic Impacts of Ransomware on Small and Medium Enterprises.·International Journal of Cybersecurity.·2023;·50(1):·33-48.·10.1016/j.jcis.2023.101021

[82]Á. D. Muhoray és I. Bartáné dr. Muharay.·Biztonsági és környezetbiztonsági alapelvek érvényesülése a katasztrófák elleni védekezés rendszerében.·2004

[83]I. Nemzeti Kibervédelmi és S. Nemzetbiztonsági.·Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója.·2024

[84]C. Kollár.·A szervezeti információbiztonsági folyamatok monitorozása és a vezetői döntések támogatása kulcs teljesítménymutatók segítségével. I. rész – Az információbiztonság rendszerelméleti megközelítése.·Szakmai Szemle.·2017;·XV(4):·43–56

[85]Cybersecurity és A. Infrastructure Security.·Cyber-attack against Ukrainian critical infrastructure (IR-ALERT-H-16-056-01).·2021

[86]M. Akbanov és V. Vassilakis.·WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms.·Journal of Telecommunications and Information Technology.·2019;·1:·113-124.·10.26636/jtit.2019.130218

[87]D. Roper.·Big Data as Part of the Critical Infrastructure.·2023

[88]M. Bishop.·Computer Security: Art and Science.·2003

[89]C. Cash.·‘Not the Same Co-op’: Lessons From a Devastating Ransomware Attack.·

[90]L. Muha, . és et al.·Informatikai biztonságmenedzsment.·2008

[91]J. M. Kizza.·Guide to Computer Network Security.·2007

[92]O. V. Póserné.·IT kockázatok elemzésük, kezelésük.·HADMÉRNÖK.·2007;·2(3):·206-214

[93]C. A. Ericson.·Fault Tree Analysis — A History.·2005

[94]U. S. Nuclear Regulatory Commission. Advisory Committee on Reactor Safeguards.·Report to Congressman Morris K. Udall, Chairman, Subcommittee on Energy and the Environment, U.S. House

of Representatives, on the Reactor Safety Study (RSS, WASH-1400, NUREG-75/014).·1976

[95]E. Ruijters és M. Stoelinga.·Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools.·Computer Science Review.·2015;·15-16:·29-62.·https://doi.org/10.1016/j.cosrev.2015.03.001

[96]National Institute of Standards and Technology.·Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5).·2020

[97]C. Engle, J. Brewster és G. Blokdijk.·ISO/IEC 20000 Certification and Implementation Guide - Standard Introduction, Tips for Successful ISO/IEC 20000 Certification, FAQs, Mapping Responsibilities, Terms, Definitions and ISO 20000 Acronyms.·2008

[98]P. Hopkin.·Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management.·2017

[99]Y. Diogenes és E. Ozkaya.·Cybersecurity? Attack and Defense Strategies: Infrastructure Security with Red Team and Blue Team Tactics.·2018

[100]L. Coles-Kemp és M. Theoharidou.·Insider Threat and Information Security Management.·2010.·10.1007/978-1-4419-7133-3_3

[101]M. W. Harkins.·Managing Risk and Information Security: Protect to Enable.·https://doi.org/10.1007/978-1-4842-1455-8.·10.1007/978-1-4842-1455-8

[102]L. Muha és T. Szádeczky.·Irányítási rendszerek.·2014

[103]M.-F. Panettiere.·Virus Software and the First Amendment.·1995

[104]D. H. Wolpert.·Stacked generalization.·Neural Networks.·1992;·5(2):·241-259.·10.1016/S0893-6080(05)80023-1

[105]D. Endres és J. Schindelin.·A new metric for probability distributions.·Information Theory, IEEE Transactions on.·2003;·49:·1858-1860.·10.1109/TIT.2003.813506

[106]M. Fernández-Delgado, E. Cernadas, S. Barro és D. Amorim.·Do we need hundreds of classifiers to solve real world

classification problems?·Journal of Machine Learning Research.·2014;·15(1):·3133-3181

[107]B. Frénay és M. Verleysen.·Classification in the Presence of Label Noise: A Survey.·Neural Networks and Learning Systems, IEEE Transactions on.·2014;·25:·845-869.·10.1109/TNNLS.2013.2292894

[108]The New York Times.·Aramco Says Cyberattack Was Aimed at Production.·2012.·https://www.nytimes.com/2012/12/10/business/energy-environment/saudi-aramco-says-hackers-aimed-to-halt-oil-production.html

[109]T. Brewster.·NotPetya Ransomware Hackers 'Took Down Ukraine Power Grid'.·

[110]T. Brewster.·Ukraine Claims Hackers Caused Christmas Power Outage.·

[111]S. Abdelkader, J. Amissah, S. Kinga, G. Mugerwa, E. Ebinyu, D.-E. Mansour, M. Bajaj, V. Blazek és L. Prokop.·Securing Modern Power Systems: Implementing Comprehensive Strategies to Enhance Resilience and Reliability Against Cyber-Attacks.·Results in Engineering.·2024;·23:·102647.·10.1016/j.rineng.2024.102647

[112]D. Whitehead, K. Owens és D. Gammel.·Ukraine cyber-induced power outage: Analysis and practical mitigation strategies.·2017.·10.1109/CPRE.2017.8090056

[113]L. Gawazah.·To Pay or Not to Pay- The US Colonial Pipeline Ransomware Attack.·2024;·

[114]S. e. a. Adam.·The State of Ransomware 2022.·2022

[115]N. Perlroth és C. Krauss.·A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.·2018

[116]I. Ilascu.·Eletrobras, Copel energy companies hit by ransomware attacks.·2021

[117]D. Goodin.·Two US power plants infected with malware spread via USB drive.·2013

[118]Z. Horváth.·Informatikai rendszerek biztonsága.·2013

[119]R. Klipper.·Risk Management in IT Security.·2011

[120]A. Calder és S. Watkins.·IT Governance: A Manager's Guide to Data Security and ISO 27001 / ISO 27002.·2008

[121]R. Jasmontaitė-Zaniewicz, S. Calvi, D. Nagy és D. Barnard-Wills.·Data Protection and Privacy: The Age of Intelligent Machines.·2020

[122]R. Anderson.·Security Engineering: A Guide to Building Dependable Distributed Systems.·2001

[123]R. Sinha.·Cybersecurity: Accountability and Compliance.·2018

[124]G. Stoneburner, A. Goguen és A. Feringa.·Risk Management Guide for Information Technology Systems.·2002

[125]International Organization for Standardization.·ISO/IEC 27002:2022: Information Security, Cybersecurity, and Privacy Protection — Information Security Controls.·2022

[126]P. Cichonski, T. Millar, T. Grance és K. Scarfone.·Computer Security Incident Handling Guide (NIST Special Publication 800-61 Revision 2).·2012

[127]L. Berek.·Biztonságtechnika.·2014

[128]Z. Berkes, Z. Déri, C. Krasznay és L. Muha.·Informatikai Biztonsági Irányítási Rendszer (IBIR).·2008

[129]Center for Internet Security.·Enterprise Asset Management Policy Template.·2022

[130]L. Muha és Á. Bodlaki.·Az informatikai biztonság tanúsítási és minősítési eljárásrendjének terve.·1997

[131]B. Shojaie, H. Federrath és I. Saberi.·Getting the full benefits of the ISO 27001 to develop an ISMS based on organisations' InfoSec culture.·2016

[132]H. F. Tipton és M. K. Nozaki.·Information security management handbook.·2007

[133]International Organization for Standardization ISO.·ISO/IEC 27001:2022 - Information technology — Security techniques — Information security management systems — Requirements.·2022

[134]E. Humphreys.·Information security management system standards.·Datenschutz und Datensicherheit - DuD.·2011;·35:·7-11.·10.1007/s11623-011-0004-3

[135]J. Yellin.·The Nuclear Regulatory Commission's Reactor Safety Study: Reply.·The Bell Journal of Economics.·1976;·7(2):·711-715.·10.2307/3003283

[136]N. Limnios.·A formal definition of fault tree graph models and an exhaustive test of their structural data.·Reliability Engineering.·1987;·18(4):·267-274.·https://doi.org/10.1016/0143-8174(87)90031-X

[137]K. Tráj és P. László.·Kockázatelemzési módszerek szemléltetése a diákélet egy példáján keresztül – Demonstration of risk assessment methods through a student life problem.·2015

[138]Á. Szeghegyi, G. Kiss és O. Gulyás.·Tudásmenedzsment és kiberbiztonság összefüggésrendszere a bankszektorban.·2022

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

[140]M. Jariwala.·The Cyber Security Roadmap: A Comprehensive Guide to Cyber Threats, Cyber Laws, and Cyber Security Training for a Safer Digital World.·2023

[141]M. Gosling és A. Hiles.·Business Continuity Statistics: Where Myth Meets Fact.·2010

JEGYZETEK

Kritikus infrastruktúra és ransomware kapcsolódó hivatkozások

[2] R. Kumar, R. Kela, S. Singh és R. Trujillo-Rasua. APT attacks on industrial control systems: A tale of three incidents. International Journal of Critical Infrastructure Protection. 2022; 37: 100521.

URL: https://doi.org/10.1016/j.ijcip.2022.100521

[9] A. M. Kovács. Ransomware: A comprehensive study of the exponentially increasing cybersecurity threat. Insights into Regional Development. 2022; 4(2): 96-104.

DOI: 10.9770/IRD.2022.4.2(8)

Oldalszám: 96-104

[11] A. M. Kovács. Soft computing in preventing ransomware relying on larger-scale data and analysis. Strategic Impact. 2023; 87(2): 66-84.

DOI: 10.53477/1842-9904-23-12

Oldalszám: 66-84

[24] A. M. Kovács. Evolving cybersecurity strategies: Analyzing trends in critical infrastructure attacks and defense mechanisms. International Journal of Intelligent Systems and Applications in Engineering. 2024; 12(4): 2941-2952.

Oldalszám: 2941-2952

Elméleti és módszertani hivatkozások

[12] J. Davis és M. Goadrich. The Relationship Between Precision-Recall and ROC Curves. 2006.

DOI: 10.1145/1143844.1143874

[14] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore és S. Savage. Measuring the Cost of Cybercrime. 2013.

DOI: 10.1007/978-3-642-39498-0_12

[16] R. Sommer és V. Paxson. Outside the closed world: On using machine learning for network intrusion detection. 2010.

DOI: 10.1109/SP.2010.25

[20] T. Rid. Cyber War Will Not Take Place. Journal of Strategic Studies. 2012; 35(1): 5-32.

DOI: 10.1080/01402390.2011.608939

Oldalszám: 5-32

[22] C. D. Manning, P. Raghavan és H. Schütze. Introduction to Information Retrieval.

2008.
DOI: 10.1017/CBO9780511809071

Támadások és esettanulmányok

[25] H. Bhaiyat és S. Sithungu. Cyberwarfare and its Effects on Critical Infrastructure. International Conference on Cyber Warfare and Security. 2022; 17: 536-543.
DOI: 10.34190/iccws.17.1.68
Oldalszám: 536-543

[26] J. Besenyő, A. Gulyás és D. Trifunovic. Hezbollah and the Internet in the Twenty-First Century. International Journal Of Intelligence And Counterintelligence. 2022; 1-17.
URL: https://doi.org/10.1080/08850607.2022.2111999
Oldalszám: 1-17

[31] J. Besenyő. Terrorist Threats to African Hospitals. 2024.
URL: https://link.springer.com/chapter/10.1007/978-3-031-47990-8_7

IoT és okos rendszerek biztonsága

[32] W. Zhou, Y. Zhang és P. Liu. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. IEEE Internet of Things Journal. 2018; PP.
DOI: 10.1109/JIOT.2018.2847733

[33] S. Kumar, P. Tiwari és M. Zymbler. Internet of Things is a revolutionary approach for future technology enhancement: a review. Journal of Big Data. 2019; 6.
DOI: 10.1186/s40537-019-0268-2

[34] Z. Shouran, A. Ashari és T. Priyambodo. Internet of Things (IoT) of Smart Home: Privacy and Security. International Journal of Computer Applications. 2019; 182: 3-8.
DOI: 10.5120/ijca2019918450
Oldalszám: 3-8

[35] H. Lin és N. W. Bergmann. IoT Privacy and Security Challenges for Smart Home Environments. 2016.
DOI: 10.3390/info7030044

[36] J. Kaniewski, H. Jahankhani és S. Kendzierskyj. Usability of the CBEST Framework for Protection of Supervisory Control and Acquisition Data Systems (SCADA) in the Energy Sector. 2021.
DOI: 10.1007/978-3-030-72120-6_1

Uniós és nemzetközi szabályozás

[38] Z. Bederna és Z. Rajnai. Analysis of the cybersecurity ecosystem in the European Union. International Cybersecurity Law Review. 2022; 3: 1-15.

DOI: 10.1365/s43439-022-00048-9

Oldalszám: 1-15

[40] M. Tvaronavičienė, T. Plėta, S. Casa és J. Latvys. Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania. Insights into Regional Development. 2020; 2: 802-813.

DOI: 10.9770/IRD.2020.2.4(6)

Oldalszám: 802-813

[41] Y. Yang és M. Zhang. From Tactics to Techniques: A Systematic Attack Modeling for Advanced Persistent Threats in Industrial Control Systems. 2023.

DOI: 10.1109/EuroSPW59978.2023.00042

Adatbázisok és technológiák

[43] Z. Nyikes és Z. Rajnai. Big data, as part of the critical infrastructure. 2015.

DOI: 10.1109/SISY.2015.7325383

[48] J. Kizza. Guide to Computer Network Security. 2017.

DOI: 10.1007/978-3-319-55606-2

Hibrid hadviselés

[53] M. Boda. Hybrid War: Theory and Ethics. AARMS – Academic and Applied Research in Military and Public Management Science. 2024; 23(1): 5-17.

DOI: 10.32565/aarms.2024.1.1

Oldalszám: 5-17

[58] C. S. Chivvis. Understanding Russian "Hybrid Warfare": And What Can Be Done About It. 2017.

DOI: 10.7249/CT468

[61] A. Gulyás, M. Demeter és J. Besenyő. The Lernaean Hydra on the internet: Deplatformization-resistant media ecosystem of the Islamic State. MEDIA WAR AND CONFLICT. 2023; 17(3): 310-333.

URL: https://journals.sagepub.com/doi/10.1177/17506352231206306

Oldalszám: 310-333

Stratégiai tanulmányok

[67] C. Jackson. Counterinsurgency by David Kilcullen. Political Science Quarterly. 2011; 126.

DOI: 10.1002/j.1538-165X.2011.tb02159.x

[68] I. Arreguín-Toft. How the Weak Win Wars: A Theory of Asymmetric Conflict. International Security. 2001; 26: 93-128.

DOI: 10.1162/016228801753212868

Oldalszám: 93-128

[27] T. Rid és B. Buchanan. Attributing Cyber Attacks. Journal of Strategic Studies. 2015; 38(1-2): 4-37.

DOI: 10.1080/01402390.2014.977382

Oldalszám: 4-37

Ransomware esettanulmányok

[79] R. Wittkop. The Colonial Pipeline Ransomware Attack: A Catalyst for Cybersecurity Reform. Journal of Infrastructure Security. 2022; 45(3): 112-127.

DOI: 10.1002/jcis.22561

Oldalszám: 112-127

[80] J. Wiener. Cybercrime and the Global Economy: A Study of Identity Theft. Economic Impact Review. 2018; 12(2): 79-92.

DOI: 10.1080/09125195.2018.129238

Oldalszám: 79-92

[81] P. Molinari. The Socioeconomic Impacts of Ransomware on Small and Medium Enterprises. International Journal of Cybersecurity. 2023; 50(1): 33-48.

DOI: 10.1016/j.jcis.2023.101021

Oldalszám: 33-48

[86] M. Akbanov és V. Vassilakis. WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms. Journal of Telecommunications and Information Technology. 2019; 1: 113-124.

DOI: 10.26636/jtit.2019.130218

Oldalszám: 113-124

Kockázatelemzés

[95] E. Ruijters és M. Stoelinga. Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. Computer Science Review. 2015; 15-16: 29-62.

URL: https://doi.org/10.1016/j.cosrev.2015.03.001
Oldalszám: 29-62
[100] L. Coles-Kemp és M. Theoharidou. Insider Threat and Information Security Management. 2010.
DOI: 10.1007/978-1-4419-7133-3_3
[101] M. W. Harkins. Managing Risk and Information Security: Protect to Enable.
DOI: 10.1007/978-1-4842-1455-8

Gépi tanulás és mesterséges intelligencia

[104] D. H. Wolpert. Stacked generalization. Neural Networks. 1992; 5(2): 241-259.
DOI: 10.1016/S0893-6080(05)80023-1
Oldalszám: 241-259
[105] D. Endres és J. Schindelin. A new metric for probability distributions. Information Theory, IEEE Transactions on. 2003; 49: 1858-1860.
DOI: 10.1109/TIT.2003.813506
Oldalszám: 1858-1860
[107] B. Frénay és M. Verleysen. Classification in the Presence of Label Noise: A Survey. Neural Networks and Learning Systems, IEEE Transactions on. 2014; 25: 845-869.
DOI: 10.1109/TNNLS.2013.2292894
Oldalszám: 845-869

Nagy támadások dokumentációja

[108] The New York Times. Aramco Says Cyberattack Was Aimed at Production. 2012.
URL: https://www.nytimes.com/2012/12/10/business/energy-environment/saudi-aramco-says-hackers-aimed-to-halt-oil-production.html
[111] S. Abdelkader, J. Amissah, S. Kinga, G. Mugerwa, E. Ebinyu, D.-E. Mansour, M. Bajaj, V. Blazek és L. Prokop. Securing Modern Power Systems: Implementing Comprehensive Strategies to Enhance Resilience and Reliability Against Cyber-Attacks. Results in Engineering. 2024; 23: 102647.
DOI: 10.1016/j.rineng.2024.102647
[112] D. Whitehead, K. Owens és D. Gammel. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. 2017.
DOI: 10.1109/CPRE.2017.8090056

[134] E. Humphreys. Information security management system standards. Datenschutz und Datensicherheit - DuD. 2011; 35: 7-11.
DOI: 10.1007/s11623-011-0004-3
Oldalszám: 7-11
[135] J. Yellin. The Nuclear Regulatory Commission's Reactor Safety Study: Reply. The Bell Journal of Economics. 1976; 7(2): 711-715.
DOI: 10.2307/3003283
Oldalszám: 711-715
[136] N. Limnios. A formal definition of fault tree graph models and an exhaustive test of their structural data. Reliability Engineering. 1987; 18(4): 267-274.
URL: https://doi.org/10.1016/0143-8174(87)90031-X
Oldalszám: 267-274

TÁBLAJEGYZÉK

ÁBRAJEGYZÉK

RÖVIDÍTÉSJEGYZÉK

AI: Artificial Intelligence (Mesterséges intelligencia)

APT: Advanced Persistent Threat (Fejlett Tartós Fenyegetés)

CISSM: Center for International and Security Studies at Maryland

CPS: Cyber Physical System (kiber-fizikai rendszerek)

DDOS: Distributed Denial of Service (elosztott szolgáltatásmegtagadással járó támadás)

ENISA: Európai Unió Kiberbiztonsági Ügynöksége

IBIR (Informatikai Biztonsági Irányítási Rendszer)

ICS: Industrial Control Systems (a kritikus infrastruktúrák ipari vezérlőrendszerei)

IoT: Dolgok Internete (Internet of Things)

IRT: incidens-reagálási terv

MCED (Maryland Cyber Events Database); Marylandi Kiberbiztonsági Adatbázis

ML: machine learning, Gépi tanulás

NIST; Nemzeti Szabványügyi és Technológiai Intézet (USA)

OECD; Gazdasági Együttműködési és Fejlesztési Szervezet

OT: Operational Technology

SCADA: Supervisory Control and Data Acquisition (Felügyeleti Vezérlő és Adatgyűjtő Rendszer)

TF-IDF: Term Frequency-Inverse Document Frequency (Kifejezésgyakoriság és fordított dokumentumgyakoriság)

TTP: Tactics Techniques Procedures (taktikai-technikai eljárások)

FÜGGELÉK - MELLÉKLETEK

M1. melléklet – módszertani kiegészítések: adatkeret és tisztítás

M1.1 Az MCED adatkeret összefoglalása

Az empirikus vizsgálat alapja a Maryland Cyber Events Database (MCED), amely 2014 és 2025 között manuálisan validált kiberincidenseket tartalmaz.

Főbb jellemzők:

- időszak: 2014. január – 2025. október
- rekordok száma a nyers állományban: 15 789
- egység: egy sor = egy incidens (egy kiberesemény, amelyet legalább egy független forrás megerősít)
- földrajzi lefedettség: globális (Észak-Amerika, Európa, APAC, MENA)

A fő háttérváltozók:

- idő: event_date, date_precision
- aktor: actor_type, actor_country, actor_group
- célpont: industry (NAICS), targeted_country, organization_type
- esemény: event_type, event_subtype, initial_vector, impact
- motiváció: motive
- metaadat: source_count, source_type, coding_notes

A 3. fejezetben bemutatott statisztikai elemzések és gépi tanulási modellek kizárólag ezekre az incidensszintű rekordokra épülnek.

M1.2 Tisztítási protokoll: Level-0 → Level-2

A nyers MCED-állományra háromlépcsős tisztítási eljárás került alkalmazásra. A cél:

1. a kategóriák szöveges reprezentációjának egységesítése (Level-0),
2. a célváltozó (actor_type) zajmentesítése (Level-1),
3. a kulcsmagyarázó változó (motive) zajmentesítése (Level-2).

M1.2.1 Összefoglaló táblázat

- **Level-0 (Master):** csak normalizálás, nincs szűrés.
  Rekordszám: 15 789 (100%).
- **Level-1:** minden sor, ahol actor_type_clean = "Undetermined", törlésre kerül.
  Rekordszám: 15 166
  Kihulló arány: 3,95%.
- **Level-2:** Level-1 + motive = "Unknown" sorok eltávolítása.
  Rekordszám: 12 383
  További kihulló arány: 18,35%.

A Level-2 minta adja a H1–H3 hipotézisekhez használt fő elemzési adatkeretet.

M1.2.2 Level-0 – normalizálás

A Level-0 szinten csak determinisztikus, adatvesztéssel nem járó korrekciók történnek:

- elgépelések javítása (például „Hacktvist” → „Hacktivist”, „Nation-state” → „Nation-State”),
- whitespace- és encoding-normalizálás,
- NAICS-szektorok egységesítése,
- ISO-3166 országkódok ellenőrzése és javítása,
- nyilvánvalóan duplikált rekordok (azonos slug, azonos dátum, azonos cél) kiszűrése.

Ez a lépés a későbbi aggregálások és mutatószámok konzisztenciáját biztosítja adatvesztés nélkül.

M1.2.3 Level-1 – a célváltozó zajmentesítése

A H3 hipotézis supervised tanulási kerete az actor_type változót használja célváltozóként. A bizonytalan vagy ellentmondásos címkézésű esetek (actor_type = "Undetermined") nem illeszthetők következetesen a modellbe.

Szűrési szabály:
actor_type_clean ≠ "Undetermined".

Ezzel 623 rekord kerül törlésre (3,95%). A szűrés célja a nem véletlen (NNAR típusú) címkezaj minimalizálása.

M1.2.4 Level-2 – a kulcsmagyarázó zajmentesítése

A motiváció (motive) több modellben kulcs magyarázó szerepet tölt be. A „Unknown" vagy „Undetermined" motivációjú események nem illeszthetők jól a H1–H2–H3 keretbe.

Szűrési szabály:
motive ≠ "Unknown"
(és teljesülnek a Level-1 feltételei).

A lépés további 2 783 rekordot távolít el (18,35%), így jön létre a Level-2 minta (n = 12 383). A mintaszerkezeti torzításokat Jensen–Shannon divergenciával ellenőrzöm (iparág, event_type, event_subtype, célország dimenziókban); minden esetben 0,01 alatti értéket kapok, ami elhanyagolható eltérést jelent.

M1.3 Kulcsváltozók definíciója

M1.3.1 Károkozási súlyossági mutató (KSM)

A KSM az MCED event_subtype kategóriáiból származtatott ordinális skála, amely a technikai-operációs következmények intenzitását méri.

- értéktartomány: 1-5 (a dolgozatban használt normalizált skála),
- alacsony érték: csekély szolgáltatási hatás, kisebb adatérintettség,
- magas érték: súlyos vagy tartós szolgáltatásleállás, kritikus rendszerek érintettsége.

A részletes megfeleltetést az event_subtype kategóriák és a KSM-értékek között a főszöveg, valamint a melléklet külön táblázata tartalmazza.

M1.3.2 Komplexitási index (KoI)

A KoI a támadás technikai szofisztikáltságát méri négy bináris komponens alapján:

- perzisztencia (P),
- laterális mozgás (L),
- észlelés-elkerülés (E),

- **Többfázisú** kampányjelleg (C).

KoI definíciója:

$KoI = P + L + E + C,$

ahol $P, L, E, C \in \{0, 1\}$, ezért

$KoI \in \{0, 1, 2, 3, 4\}$.

A komponensek jelenlétét az incidens leírása és az event_subtype alapján, a MITRE ATT&CK-hez illesztett szabályrendszer szerint kódolom.

M1.3.3 Kritikus szektor indikátor (KrI_flag)

A KrI_flag bináris változó, amely a NAICS iparági kódokat a NIS2/CER irányelvek kritikus szektorlistáihoz rendeli.

- KrI_flag = 1: kritikus szektor (pl. közművek, egészségügy, pénzügy, közlekedés, közigazgatás),
- KrI_flag = 0: nem kritikus szektor.

A részletes megfeleltetés (NAICS kód → KrI_flag) külön iparági táblázatban szerepel.

M1.4 Mintaszerkezeti stabilitás – Jensen–Shannon divergencia

A Level-0 → Level-2 tisztítási lépések csak akkor tekinthetők módszertanilag elfogadhatónak, ha nem torzítják el érdemben az eredeti eloszlásokat. Ennek mérésére a Jensen–Shannon divergenciát használom.

Legyen P az adott változó (például iparág) kategória-eloszlása a Level-0 mintában, Q pedig ugyanennek az eloszlása a Level-2 mintában. Definiálom:

- $M = 0{,}5 \cdot (P + Q)$
- $KL(P \,||\, M) = \Sigma\, P_i \cdot \log_2(P_i / M_i)$
- $KL(Q \,||\, M) = \Sigma\, Q_i \cdot \log_2(Q_i / M_i)$

A Jensen–Shannon divergencia:

$JSD(P, Q) = 0{,}5 \cdot KL(P \,||\, M) + 0{,}5 \cdot KL(Q \,||\, M)$

Interpretáció:

- JSD ≈ 0: az eloszlások gyakorlatilag azonosak,
- JSD < 0,01: elhanyagolható különbség,
- JSD 0,01–0,05 között: mérsékelt eltérés,
- JSD > 0,05: jelentős torzítás.

Az MCED esetében a Level-0 és Level-2 eloszlásokra számított JSD minden vizsgált dimenzióban 0,004 alatt maradt, ezért a tisztítás nem torzítja el a teljes kibertámadás-populáció alapstruktúráját.

M2. melléklet – statisztikai tesztek kiegészítő dokumentációja

Ebben a mellékletben a 3.3 fejezetben hivatkozott statisztikai eljárások strukturált összefoglalása szerepel; a konkrét numerikus eredmények a főszöveg táblázataiban találhatók.

A disszertációban hivatkozott, alkalmazott eljárások módszerek általános felsorolása:

1. Shapiro–Wilk normalitásvizsgálat
2. Brunner–Munzel próba
3. Cliff-féle delta + bootstrap CI (1000×)
4. Kruskal–Wallis próba (iparági bontás)
5. Dunn-post hoc + Bonferroni
6. Logisztikus regresszió (HighDamage ~ KrI_flag + kontrollok)
7. Illeszkedésdiagnosztika (McFadden R^2, AUC, Hosmer–Lemeshow)
8. Robusztussági tesztek:
    - alternatív KrI
    - Undetermined nélküli vs elemzési minta
    - propensity-score weighting
9. Gépi tanulási modell (stacking ensemble)
10. PR-AUC, macro-F1, ROC-AUC, calibráció
11. Osztályegyensúlytalanság-kezelés (class weights, SMOTE)
12. Reject-option + PU-learning kísérleti ellenőrzés
13. FDR-korrekció minden többtesztes elemzéshez

M2.1 H1 hipotézis – kritikus infrastruktúrák kárkockázata

Alkalmazott módszerek:

- leíró statisztikák KSM_final változóra, KrI_flag szerinti bontásban (átlag, medián, szórás, IQR, 95%-os konfidenciaintervallum),

- normalitás ellenőrzése (Shapiro–Wilk próba),
- Brunner–Munzel próba a KSM eloszlások összehasonlítására (kritikus vs nem kritikus),
- Cliff-féle delta hatásméret, bootstrap konfidenciaintervallummal (1000 replikáció),
- Kruskal–Wallis próba iparági bontásban, Dunn-féle post-hoc teszttel, Bonferroni-korrekcióval,
- logisztikus regresszió a súlyos kimenet (HighDamage = 1, ha KSM ≥ 4) modellezésére, fő magyarázó: KrI_flag, kontroll: év, régió, event_type, supply_chain,
- robusztussági ellenőrzések: alternatív KrI definíciók, Level-1 vs Level-2 minta, propensity-score weighting iparág × régió × év × event_type alapján.

A modellillesztés minősége:

- illeszkedés: McFadden R^2, AUC, Hosmer–Lemeshow próba,
- hatásértelmezés: esélyhányadosok (OR) és 95%-os konfidenciaintervallumaik.

M2.2 H2 hipotézis – aktortípus és technikai komplexitás

Alkalmazott módszerek:

- KoI eloszlásainak összehasonlítása actor_type szerint,
- Welch-féle ANOVA (varianciahomogenitás feltétele nélkül),
- Brunner–Munzel próbák kiemelt páronkénti összehasonlításokra (Nation-State vs Criminal),
- Cliff-féle delta hatásméret,
- KoI komponensek (perzisztencia, laterális mozgás, észlelés-elkerülés, kampányjelleg) gyakoriságának összevetése χ^2 illetve Fisher-exakt próbával, Benjamini–Hochberg FDR-korrekcióval,
- bináris logisztikus regresszió Nation-State (1) vs Criminal (0) kimenettel; magyarázók: KoI komponensek, KrI_flag, év, régió, event_type, supply_chain,

- ordinális logit modell, ahol a függő változó a teljes KoI skála (0–4); magyarázók: actor_type, KrI_flag, supply_chain, idő, régió; parallel lines teszt az ordinális modell feltételeinek ellenőrzésére,
- robusztussági vizsgálatok: külön futtatás kritikus szektorokra (KrI_flag = 1) és ellátási lánc eseményekre (supply_chain = 1), valamint Level-1 vs Level-2 minta összevetése.

M2.3 H3 hipotézis – ensemble modell értékelése

Metrikák:

- F1-macro (osztályonkénti F1-score átlaga),
- PR-AUC osztályonként és átlagosan,
- Brier-score,
- Expected Calibration Error (ECE),
- Top-k recall (Top-2, Top-3),
- reject arány (a bizonytalanság miatt tartózkodó előrejelzések aránya).

A validációs év (2022) szolgál a küszöbök és a kalibráció paramétereinek kiválasztására; a végső teljesítményértékelés a 2023–2025 közötti out-of-time tesztkészleten történik.

M3. melléklet – gépi tanulási modell technikai dokumentációja

M3.1 feature-készlet

M3.1.1 szöveges csatorna

Forrásmezők:

- title
- description

Előfeldolgozás:

- kisbetűsítés,
- technikai zaj (HTML-tagek, URL-ek, e-mail-címek) eltávolítása,
- lemmatizálás,
- stop-szó lista (angol, szükség esetén magyar),
- opcionális rövidítés-feloldás (pl. „gov” → „government”).

Reprezentáció:

- szó n-gramok: 1–2,
- karakter n-gramok: 3–5,
- TF-IDF súlyozás, sublineáris tf opcióval; ritka kifejezések és túl gyakori tokenek kiszűrése (min_df, max_df küszöb).

M3.1.2 strukturált csatorna

Felhasznált mezők:

- event_year,
- region,
- industry (aggregált NAICS),
- event_type, event_subtype,
- motive,
- KrI_flag,

- supply_chain flag,
- source_count,
- date_precision.

Kódolás:

- kategóriák: one-hot / dummy,
- numerikus változók: standardizálás (átlag 0, szórás 1),
- hiányzó értékek: külön „Missing” kategória vagy egyszerű imputáció, ahol indokolt.

M3.1.3 domain-specifikus jellemzők

- MITRE ATT&CK lexikon alapján bináris indikátorok (pl. „lateral”, „persistence”, „credential dumping”, „beaconing”),
- külön lexikon ransomware-, DDoS- és supply-chain kulcsszavakra,
- ezek előfordulása igen/nem jellegű változóként jelenik meg, illetve egyszerű számlálók formájában (hány ATT&CK-jellegű token jelenik meg egy leírásban).

M3.2 modellek és hiperparaméterek

szöveges csatorna

- lineáris SVM (multi-class, one-vs-rest):
  C érték rácskereséssel (pl. 0,1; 1; 10); class_weight = „balanced”.
- multinomiális logisztikus regresszió:
  L2-regularizáció, C rácskereséssel; max_iter = 1000.
- multinomiális Naive Bayes:
  simítási paraméter (alpha) kis rácskereséssel hangolva.

strukturált csatorna

- Random Forest (súlyozott):
  n_estimators ≈ 500, class_weight = „balanced”,
  max_depth és min_samples_leaf kis rácskereséssel kiválasztva.

- opcionálisan gradient boosting típusú modell (pl. XGBoost vagy LightGBM), mérsékelt hiperparaméter-hangolással.

Nem említett hiperparaméterek minden esetben az adott könyvtár alapértelmezett értékeit vették fel.

M3.3 tanítási és kalibrációs protokoll

- train időszak: 2014–2021,
- validációs év: 2022,
- teszt időszak: 2023–2025 (teljesen out-of-time).

Lépések:

1. TF-IDF, kategóriakódolás, skálázás és lexikon-jellemzők illesztése csak a train adatokon.
2. a validációs és tesztkészletek a train-ből tanult (befagyasztott) transzformációkat használják.
3. base modellek tanítása K-szoros keresztvalidációval; out-of-fold (OOF) valószínűségek képzése.
4. meta-szint: logisztikus regresszió az OOF kimeneteken, célváltozó = actor_type.
5. kalibráció: a 2022-es év OOF-előrejelzéseire Platt-scaling vagy isotonic regresszió; a kiválasztott kalibrációs transzformáció paraméterei befagyasztva kerülnek alkalmazásra a tesztkészletre.

M3.4 döntési szabály és tartózkodási mechanizmus

Legyen p(c_i) az i-edik osztály (c_i) poszterior valószínűsége egy adott esetre.

- minden osztályhoz tartozik egy küszöb: τ_i,
- van egy globális tartózkodási küszöb: τ_reject.

Döntési szabály:

- ha létezik olyan c_i, amelyre
  $p(c_i) \geq \tau_i$ és $p(c_i) = \max_j p(c_j)$,
  akkor a kimenet: PredictedClass = c_i;
- ha $\max_i p(c_i) < \tau_{reject}$, akkor a kimenet: PredictedClass = REJECT.

Bizonyossági függvény:

$S(x) = \max_i p(c_i)$

Tartózkodási tartomány:

$RejectRegion = \{ x : S(x) < \tau_{reject} \}$

A küszöbök értékei a validációs év (2022) alapján kerültek megválasztásra, a F1-macro, a PR-görbék és a reject arány együttes figyelembevételével.

M4. melléklet – szoftverkörnyezet és reprodukálhatóság

M4.1 szoftverkörnyezet

A teljes feldolgozási és modellezési pipeline az alábbi környezetben futott:

- programnyelv: Python 3.x
- főbb csomagok:
    - pandas (adatkezelés),
    - numpy (numerikus számítások),
    - scipy (statisztikai tesztek),
    - scikit-learn (gépi tanulás, metrikák),
    - statsmodels (regressziós modellek),
    - matplotlib / seaborn (ábrázolás).

Egyes statisztikai próbák és robusztussági ellenőrzések R-ben is reprodukálhatók, a standard csomagok (pl. „stats”, „car”, „ordinal”) használatával.

M4.2 futtatási pipeline – lépésről lépésre

1. **adatbetöltés**
   – MCED nyers export beolvasása (CSV vagy SQL formátumban),
   – codebook szerinti típuskonverziók.
2. **Level-0 normalizálás**
   – stringek és kódok egységesítése,
   – iparági és országkód javítások,
   – nyilvánvaló duplikátumok kiszűrése.
3. **Level-1 és Level-2 szűrés**
   – actor_type_clean ≠ „Undetermined”,
   – motive ≠ „Unknown”,
   – rekordszámok és arányok rögzítése.
4. **változóképzés**
   – KSM és KoI kiszámítása,
   – KrI_flag meghatározása (NAICS → NIS2/CER),

– KoI-komponensek bináris jelölése,

– esetleges log-transzformációk (például recovery time).

5. **mintaszerkezeti ellenőrzés**

   – eloszlások Level-0 és Level-2 szinten,

   – Jensen–Shannon divergencia iparág, event_type, event_subtype, célország dimenziókban.

6. **H1–H2 hipotézisvizsgálatok lefuttatása**

   – leíró statisztikák,

   – Brunner–Munzel, Kruskal–Wallis, Welch-ANOVA,

   – logisztikus és ordinális regressziók,

   – robusztussági vizsgálatok.

7. **H3 modell tanítása**

   – train/valid/test időablak létrehozása,

   – szöveges és strukturált feature-k előállítása,

   – base modellek és meta-modell betanítása,

   – kalibráció végrehajtása, küszöbök meghatározása,

   – végső metrikák kiszámítása a tesztkészletre.

8. **drift-ellenőrzés**

   – Population Stability Index (PSI) és JSD értékek számítása időszeletek között,

   – a modell éves degradációjának dokumentálása.

M5. melléklet - Esettanulmanyok és információbiztonsági összefüggések

M5.1. Esettanulmányi kivonat (KSM / KoI / IBIR / hipotézis metszetek)

Ez a melléklet a 2. fejezetben részletezett esettanulmányok (BlackEnergy, WannaCry, NotPetya, DMEA, valamint Észtország 2007; Grúzia 2008; Viasat 2022) gyors áttekintő táblázatát adja [108]. A KSM/KoI értékek csak ott szerepelnek, ahol a fejezet kifejezetten megadja őket; a többinél „n.a." jelölést alkalmazok (későbbi MCED-kódolásra javasolt).

Eset (év)	Szektor / ország	Vektor / kulcselem	KSM	KoI	IBIR tanulság (röviden)	Hipotézis-kapcsolat	Megjegyzés
BlackEnergy (2015)	Energia – Ukrajna [109-111] [112].	Phishing → IT→OT, ICS/SCADA zavar [113]	5	4	Szegmentáció hiánya; ICS anomáliaészlelés hiánya; MFA hiánya	H1, H2	Kritikus infrastruktúra; tartós szolgáltatás-kiesés {Alshathry, 2016 #75}.
WannaCry (2017)	Egészségügy, közszolg. – globális	EternalBlue / SMBv1; önterjedés	4 (globál), 5 (egészségügy lokál)	2	Patch-menedzsment; mikro-szegmentáció; hálózati anomáliák észlelése [114]	H1, H3	Alacsony KoI, de extrém hatás
NotPetya (2017)	Több ágazat – globális	Supply chain → MeDoc; wiper; több exploit	5	4	Kódaláírás-validáció; frissítési csatorna-ellenőrzés;	H1, H2	Kaszkád-hatás; több földrész, több iparág

	[115] [116]				blast-radius csökkentés		
DMEA (2021)	Energia – USA (közmű) [117].	Zsarolóvírus / adatmegsemmisítés [114]	4–5	közepes	Immutable backup; RTO/RPO; szerepkör alapú hozzáférés; log-/riasztási lánc	H1	~90% belső rendszersérülés; 25 év adatvesztés
Észtország (2007)	Közigazgatás – Észtország	DDoS / hibrid művelet	n.a.	n.a.	Kormányzati reagálási képesség, IRT, hálózati védelem	H2, H3	
Grúzia (2008)	Közigazgatás – Grúzia	DDoS / web defacement	n.a.	n.a.	IRT, CDN/anti-DDoS, tartalék kommunikáció	H2, H3	
Viasat (2022)	Távközlés – EU/UA	Műholdas modemek kiiktatása	n.a.	n.a.	Ellátásiláncfüggések, hardver-firmware kontroll	H2, H3	

M6. melléklet – A kvalitatív mintapéldák a kvantitatív fejezet értelmezéséhez

A kvantitatív fejezetben alkalmazott prediktív modellek és statisztikai elemzések értelmezését segíti, ha a mögöttük álló kategóriák – a támadástípusok, a technikai altípusok, a támadói szereplők és a motivációk – kvalitatív módon is szemléltetést nyernek. Az MCED adatbázis több tízezer rekordja közül ezért olyan, kifejezetten illusztratív példák kerülnek itt bemutatásra, amelyek jól tükrözik a kritikus infrastruktúrákat érő fenyegetések sokszínűségét, valamint a fenyegetési technikák közti különbségeket.

Az alábbi táblázat célja nem a teljesség, hanem az, hogy kompakt formában mutassa be a kvantitatív fejezetben használt főbb kategóriák működését, a való életben előforduló, jól dokumentált kiberincidenseken keresztül. A kiválasztott esetek különböző iparágakat, régiókat és támadási technikákat jelenítenek meg, így szemléletes hidat képeznek a kvalitatív és a matematikai fejezet között.

A következő táblázatban bemutatott kiberbiztonsági támadások a különféle TTP-ket (Tactics Techniques Procedures, azaz taktikai-technikai eljárások) szemléltetik, amelyeket a támadást végrehajtó szereplők kifejezetten egy-egy ország valamelyik kritikus infrastruktúrájára irányítottak. E kiberbiztonsági incidensek jellegéből és gyakoriságából egyértelműen látható, hogy a támadók célja az volt, hogy komplex és pusztító rosszindulatú szoftverek bevetésével jelentős károkat okozzanak ezekben az alapvető fontosságú rendszerekben. Tekintettel arra, hogy az energiaágazat a világ minden országában a gazdasági növekedés egyik alapköve, az IT/OT környezetekben azonosított különböző sebezhetőségek különösen súlyos kockázatot jelentenek.

Dátum	Ország	Iparág	Célpont	Támadás típusa	Altípus	Támadói szereplő típusa	Motiváció
2022.09.18	Lengyelország	Közlekedés	Bydgoszcz Airport	Diszruptív	DDoS	Hacktivista	Tiltakozás
2022.03.21	Oroszország	Információs szolgáltatások	VKontakte	Exploitatív	Végpont-exploit	Bűnözői	Tiltakozás
2021.01.29	Egyesült Királyság	Közigazgatás	UK Research & Innovation	Diszruptív	DDoS + adattámadás	Bűnözői	Pénzügyi
2019.09.06	Kína	Pénzügyi szektor	HKEX	Diszruptív	DDoS	Bűnözői	Nem meghatározott
2022.02.10	USA	Egészségügy	New Jersey Brain and Spine	Diszruptív	Adattámadás	Bűnözői	Pénzügyi
2020.02.26	USA	Egészségügy	Rady's Children's Hospital	Exploitatív	Alkalmazásszerver exploit	Bűnözői	Nem meghatározott

Táblázat 4 - Illusztratív incidensminták a CISSM MCED adatbázisból

A táblázat a kvantitatív fejezetben használt fő kategóriák – támadástípus, altípus, támadói szereplő és motiváció – működését szemlélteti. A kiválasztott esetek arra mutatnak rá, hogy a kritikus infrastruktúrák különböző iparágai eltérő fenyegetési mintázatokkal szembesülnek: míg a diszruptív támadások jellemzően túlterhelésre és szolgáltatásmegtagadásra épülnek, addig az exploitatív események mélyebb rendszerhozzáférést, komplex technikai kivitelezést igényelnek.

A támadói szereplők típusainak (bűnözői, hacktivista, ismeretlen) elkülönítése a prediktív modellek egyik kulcseleme, mivel a vizsgálatok eredményei szerint a támadói motiváció és a technikai altípus erős összefüggést mutat a támadás súlyosságával és komplexitásával. A célpontnevek angol nyelvű megtartása az MCED adatbázissal való egyértelmű megfeleltethetőséget szolgálja, amely a kutatás reprodukálhatóságának feltétele.

A fenti illusztratív eseményminta egyes konkrét incidenseken keresztül mutatta be a CISSM MCED adatbázisban alkalmazott főbb kategóriák – támadástípus, technikai altípus, támadói szereplő és motiváció – működését. Ahhoz azonban, hogy a fenyegetési tér szerkezete a kvantitatív fejezet számára is áttekinthetővé váljon, szükséges ezen események magasabb szintű, tematikus összefoglalása is.

A különböző iparágakat és technikai vektorokat érintő támadások ugyanis gyakran nem önmagukban hordozzák a releváns információt, hanem abban, ahogyan **egymáshoz viszonyítva**, csoportokba rendezve rajzolnak ki jól értelmezhető mintázatokat. Az aggregált szemlélet azt mutatja meg, hogy mely szektorokban jelentkeznek tartósan bizonyos típusú fenyegetések, hogyan oszlanak meg a támadási technikák, illetve mely szereplőtípusok dominánsak egy-egy incidenskategóriában.

Az előbbi táblázat ezért nem konkrét rekordokat mutat be, hanem **a mintában megjelenő események tipikus, ismétlődő mintázatait**, tematikus incidenskategóriákba rendezve. Ez a megközelítés kulcsszerepet játszik abban, hogy a kvantitatív fejezetben alkalmazott változók – például a magas károkozási valószínűséget előrejelző tényezők – értelmezése stabil alapokon nyugodjon. A tematikus bontás egyúttal rávilágít arra is, hogy az egyes ágazatok eltérő sebezhetőségi profilokkal rendelkeznek: míg a pénzügyi és egészségügyi intézmények esetében a bűnözői motiváció dominál, addig a közlekedési és államigazgatási célpontok gyakrabban válnak hacktivista eredetű diszruptív támadások célpontjává.

Az alábbi összefoglaló tábla tehát a kvalitatív példákból eredeztetett minták **strukturált absztrakciója**, amely egyértelműen mutatja meg a fenyegetési környezetet alkotó főbb incidenskategóriákat, és előkészíti a kvantitatív elemzésekben alkalmazott változók rendszerszintű értelmezését.

Incidenskategória	Jellegzetes célpontok	Gyakori támadástípusok	Jellegzetes támadói szereplők	Példák (MCED)
Egészségügyi intézmények elleni támadások	Kórházak, klinikák	Adattámadás, alkalmazásszerver-exploit	Bűnözői csoportok	New Jersey Brain and Spine; Rady's Children's Hospital
Államigazgatási szervek elleni incidensek	Minisztériumok, hivatalok	DDoS; adattámadás	Bűnözői / hacktivista szereplők	GPAA (Dél-Afrika); Louisiana State Government
Pénzügyi szektor elleni támadások	Tőzsdék, pénzügyi központok	DDoS	Bűnözői csoportok	Hong Kong Exchanges and Clearing (HKEX)
Információs platformok elleni támadások	Közösségi oldalak, portálok	Végpont-exploit	Bűnözői / hacktivista szereplők	VKontakte
Közlekedési létesítmények elleni támadások	Repülőterek, logisztikai rendszerek	DDoS	Hacktivista csoportok	Bydgoszcz Airport
Exploitatív mélyrendszer-támadások	Alkalmazásszerverek, backend rendszerek	App exploit	Bűnözői	Rady's Hospital; Veritas Genetics

Incidenskategória	Jellegzetes célpontok	Gyakori támadástípusok	Jellegzetes támadói szereplők	Példák (MCED)
Politikai motivációjú incidensek	Állami és információs célpontok	DDoS, végpont-exploit	Hacktivista szereplők	Bydgoszcz Airport; VKontakte
Nem meghatározott technikájú események	Közigazgatási és egészségügyi szervek	Nem meghatározott	Vegyes	Kuwait Health Ministry

Táblázat 5 - Aggregált incidenskategóriák a kvalitatív minták alapján

A fenti aggregált incidenskategóriák olyan mintázatokat emelnek ki, amelyek a kvantitatív fejezet modellváltozóinak értelmezése szempontjából kiemelten relevánsak. A csoportok nem az egyes események felsorolását célozzák, hanem azokat a tartós, ismétlődő fenyegetési struktúrákat, amelyek az MCED adatbázisban nagy esetszámmal jelennek meg. A kategóriák különösen fontos szerepet játszanak abban, hogy a későbbi statisztikai modellekben alkalmazott tényezők – például a támadástípus vagy a támadói szereplő típusa – hogyan járulnak hozzá a súlyossági és komplexitási mutatók alakulásához.

Ezeket a sebezhetőségeket a nemzetállami hackerek és a fejlett tartós fenyegetéseket (APT-ket) fenntartó entitások kihasználják, hogy súlyos károkat okozzanak a nemzeteknek. A támadások jellege rámutat arra, hogy elengedhetetlen a rugalmas és proaktív intézkedések alkalmazása az általuk okozott hatások és károk enyhítése és megelőzése céljából. Annak érdekében, hogy képet adjak arról, hogyan néznek ki az összetett kiberbiztonsági támadások, és hogy ezek a kiberbiztonsági támadások hogyan irányulnak egy-egy kritikus infrastruktúra ellen, a táblázatban szereplő, fent említett incidensek kifejtése következik.

Egyes további incidensek kulcsparaméter fókuszú, deskriptív ismertetései (Táblázat 1 alapján)

Az alábbi táblázat szelektív áttekintést nyújt a 2012-2022 közötti időszakban a kritikus infrastruktúrák körébe tartozó olaj- és földgáz-, vegyipari, kőolaj-, szén- és megújuló iparágakat

magában foglaló energiaágazatot világszerte célzó, legjelentősebb kiberbiztonsági támadásokról. A szóban forgó iparágak olyanok, amelyek a gazdaság és a társadalom számára kritikus jelentőségük miatt létfontosságú infrastruktúrákként definiálhatók. Ezek az incidensek rámutatnak a hasonlóan létfontosságú ágazatok fokozott digitális sebezhetőségét, ami megerősített kiberbiztonsági intézkedések bevezetését sürgeti.

#	Kiber incidens	Cég	Ország	Dátum	Iparág
1	A Shamoon vírus használhatatlanná tett több ipari rendszereket vezérlő számítógépet	Saudi Aramco	Szaúd-Arábia	2012. augusztus	Energia
2	Malware fertőzött meg erőművet	Meg nem nevezett erőmű	USA	január 2012	Energia
3	BlackEnergy malware támadás energiaelosztó vállalat ellen	Prikarpattiaoblenerg	Ukrajna	december 2015	Energia
4	Crash Override malware célpontjává vált elektromos átvitel	Ukrenergo	Ukrajna	december 2016	Energia
5	Triton malware támadás petrolkémiai üzem ellen	Tasnee	Szaúd-Arábia	2017. augusztus	Petrolkémiai
6	ColdLock Ransomware támadás energiaipari vállalat ellen	CPC Corp	Tajvan	április 2020	Olaj és gáz
7	Villamosenergia-ipari vállalatot megtámadó zsarolóvírus	Copel	Brazília	január 2021	Energia
8	Az egyik legnagyobb olajvezetéket érő Ransomware-támadás	Colonial Pipeline	US	május 2021	Olaj és gáz
9	Energiaipari vállalat megfosztása 25 év adataitól	DMEA	US	november 2021	Energia

Táblázat 6 - Kritikus infrastruktúra incidensek

A Saudi Aramco ellen végrehajtott Shamoon vírustámadás

2012 augusztusában a Saudi Aramco, a világ egyik legnagyobb olajvállalata, súlyos kibertámadás áldozatává vált a Shamoon vírus révén. Ez a támadás a kiberbiztonság történetének egyik legjelentősebb eseménye volt, mivel a vírus közel harmincötezer számítógépet – közöttük ipari rendszereket vezérlő gépeket - fertőzött meg, amelyek adatait

teljesen törölte, és lehetetlenné tette a rendszerek újraindítását. Az incidens különösen aggasztó volt, mivel a Shamoon vírus célzottan támadta meg a vállalat belső hálózatát, és teljesen leállította annak működését [108]. Az olajtársaságnak drasztikus lépéseket kellett tennie: a fertőzött rendszereket teljesen ki kellett selejteznie, ami hatalmas pénzügyi és működési veszteségeket okozott a cégnek. A támadás jelei először akkor jelentkeztek, amikor a vállalat alkalmazottai szokatlan rendszerhibákat észleltek. Több számítógép hirtelen leállt, mások pedig egyszerűen nem voltak képesek újraindulni. Ezek a jelek arra utaltak, hogy a támadás mélyebb és szisztematikusabb volt, mint azt elsőre gondolták. A helyzet súlyosságát tovább fokozta, hogy a Shamoon vírus nemcsak az adatok törlésére, hanem a rendszerek teljes használhatatlanná tételére is képes volt, ami gyakorlatilag lebénította a Saudi Aramco működését. A támadást követő vizsgálatok kiderítették, hogy a "Cutting Sword of Justice" nevű hackercsoport állt az akció mögött. Ez a csoport nem pusztán felelősséget vállalt a támadásért, de az is kiderült, hogy politikai indíttatású cselekedetről volt szó, amelynek célja a szaúdi kormány és annak olajipari érdekeinek meggyengítése volt. A támadás nyomán a Saudi Aramco számára világossá vált, hogy a kibertérben való védekezés prioritás, mivel a kritikus infrastruktúrákat célzó támadások jelentős gazdasági és politikai következményekkel járhatnak. Ez az incidens rávilágított arra, hogy a modern vállalatok mennyire kiszolgáltatottak a kibertámadásokkal szemben, és megerősítette, hogy a kiberbiztonságba való beruházás elengedhetetlen a globális gazdasági stabilitás megőrzéséhez {Alshathry, 2016 #75}. A támadás által okozott károk nemcsak a Saudi Aramco számára voltak jelentősek, hanem globális figyelmet is keltettek, mivel rámutattak a kritikus infrastruktúrák sebezhetőségére a kibertérben.

Egy amerikai erőművet megfertőző Malware támadás

Egy amerikai erőmű körülbelül három hétre kényszerült leállni, miután 2012 januárjában rosszindulatú szoftverek támadták meg a turbina vezérlőrendszerét. A Belbiztonsági Minisztérium (DHS) nem hozta nyilvánosságra az üzem helyét és nevét. A rosszindulatú programot egy harmadik fél szállító tisztviselője juttatta be a vezérlőrendszerbe egy USB-meghajtón keresztül. A tisztviselő rutinszerűen használta az USB-meghajtót a vezérlőrendszer konfigurációinak biztonsági mentésére, nem tudva arról, hogy a meghajtó fertőzött. A rosszindulatú programot akkor azonosították, amikor a harmadik fél szállítója problémákat

észlelt az USB-meghajtó működésében, és megkérte az informatikai személyzetet, hogy vizsgálják át a meghajtót [117].

Az ukrán Prykarpattyaoblenergo Control Center ellen végrehajtott BlackEnergy Malware támadás

2015. december 23-án a "Prykarpattyaoblenergo" nevű ukrajnai áramelosztó központot súlyos kibertámadás érte a BlackEnergy nevű rosszindulatú szoftver segítségével. A támadás következtében jelentős áramkimaradások léptek fel az Ivano-Frankivszki régióban, amely több mint 230 000 lakost érintett. Az incidens különlegessége abban rejlett, hogy a támadás során a támadók a vállalat vezérlőrendszereit kompromittálták, és távvezérléssel kapcsolták le mintegy 30 alállomás megszakítóit [109-111].

A támadás eseményei alatt az egyik operátor észrevette, hogy a képernyőn az egérmutató önállóan mozogni kezdett, és a különböző régiók megszakítóinak vezérlőpaneljeihez navigált. A támadók másodperceken belül sikeresen lekapcsolták az ország különböző régióinak áramellátását biztosító alállomások megszakítóit, miközben a helyi operátorok képtelenek voltak visszavenni az irányítást a rendszerek felett. A támadók távolról megváltoztatták a rendszerek jelszavait és kijelentkeztek az operátorok helyett, ezzel biztosítva, hogy a helyi személyzet ne tudja visszaállítani az irányítást. Az eredmény az volt, hogy az érintett régiók teljes áramkimaradásba süllyedtek, amely különösen súlyos következményekkel járt a téli időszakban.

A támadás alapos tervezésre utal, mivel a kutatók és az ukrán biztonsági nyomozók szerint már 2014 tavaszán megkezdődött, amikor az informatikai személyzetet és a vezérlő operátorokat spear phishing támadásokkal célozták meg. Ezek a támadások MS Word dokumentumokhoz csatolt BlackEnergy malware segítségével történtek, amely kihasználta az MS Word makró funkciójának engedélyezését. Miután a makrók aktiválódtak, a malware telepített egy hátsó ajtót a rendszerbe, amelyen keresztül a hackerek további rosszindulatú tevékenységeket tudtak végrehajtani, ideértve a jelszavak megváltoztatását és a vezérlőrendszerek teljes irányításának átvételét. [111]

Ez az incidens rávilágít arra, hogy a kritikus infrastruktúrák milyen mértékben sebezhetőek a fejlett és célzott kibertámadásokkal szemben. A BlackEnergy támadás nem csupán a fizikai károk és az áramkimaradások révén okozott jelentős veszteségeket, hanem rávilágított a

modern ipari vezérlőrendszerek (ICS) sérülékenységére is, amelyeket gyakran nem megfelelően védenek a fejlett tartós fenyegetésekkel (APT) szemben. A támadás példátlan következményei arra ösztönözték a nemzetközi közösséget, hogy átfogóbb kiberbiztonsági intézkedéseket hozzanak, amelyek jobban védik a kritikus infrastruktúrákat a hasonló fenyegetésekkel szemben.

Az ukrán elektromos átviteli állomást megcélzó Crash Override malware

Egy másik kiberbiztonsági támadás során 2016 decemberében egy Kijev közelében található ukrán elektromos átviteli állomást ért a Crash Override, más néven "Industroyer", ami hatalmas áramszünetet okozott az egész fővárosban. A Dragos szerint, amely egy ipari kiberbiztonsággal foglalkozó megoldásszállító, a Crash Override malware az egyik első olyan malware, amelyet elektromos hálózatok megtámadására terveztek, és amely képes egyszerre több telephelyen is fellépni [112]. A 2015. december 23-i támadástól eltérően, a Crash Override malware képes automatikusan feltérképezni az elektromos hálózat vezérlőrendszereit, megtalálni a pontos célberendezést, és manipulálni a funkciókat, ami teljes áramkimaradást eredményez. A kutatók rámutattak, hogy ennek a támadásnak a hatása nem volt annyira káros, azonban azt is elmondták, hogy ez csak egy teszteset volt a hackerek számára, és katasztrofális károkat okozhatott volna, ha a malware egy kicsit érettebb. A további vizsgálatok kimutatták, hogy a rosszindulatú szoftver képes volt a fizikai energiarendszerek/berendezések károsítására is.

A szaúdi petrolkémiai üzem ellen végrehajtott Triton malware támadás

A "Triton" néven ismert halálos kártevő 2017 augusztusában csapott le a "Tasnee" szaúdi petrolkémiai üzemre. A malware-t "gyilkosnak" nevezték el, mivel ez volt az egyik első olyan malware, amelyet arra terveztek, hogy veszélyeztesse a kritikus infrastruktúrákban található biztonsági rendszereket. A kártevő képes volt megzavarni olyan rendszereket, amelyeket arra terveztek, hogy megakadályozzák az életveszélyes helyzeteket, beleértve bármilyen fizikai kárt[115]. Ezek a rendszerek olyan kritikus állapotokat szabályoznak, mint például a nyomásszelepek zárási és kioldási mechanizmusai vagy a szelepek elzárása életveszélyes helyzetek esetén. A kutatók szerint a Triton nevű rosszindulatú programot úgy tervezték, hogy az ipari vezérlőrendszereket (ICS), különösen a Triconex SIS-vezérlőket célozza meg. A rosszindulatú szoftver egy Windows-alapú rendszeren keresztül terjedt azzal a céllal, hogy

átprogramozza a SIS-vezérlőket. A támadás nem volt teljesen sikeres a rosszindulatú szoftver kódjában lévő hiba miatt, különben az eredmények katasztrofálisak lettek volna.

A tajvani energiaipari vállalat ellen bevetett ColdLock Ransomware

A tajvani állami tulajdonú "CPC Corporation" energiaipari vállalatot 2020 áprilisában zsarolóprogram-támadás érte, amelynek következtében nem állt rendelkezésre a vállalat fizetési kártyáin keresztül gázvásárlásra szolgáló fizetési csatorna az ügyfelek számára. A Sophos [114] szerint ezt a zsarolóvírust a "fájl nélküli" támadás kategóriájába sorolták. A zsarolóprogram kódja egy power shell szkript segítségével futott, anélkül, hogy futtatható állományt hozott volna létre a lemezen, és közvetlenül a memóriában futott volna. Egy másik, kiberbiztonsági cég által végzett kutatás szerint a zsarolóprogram egy power shell betöltőprogramot és egy tükröződő DLL betöltést használt a rosszindulatú szoftverek memóriában történő végrehajtásához és a rendszer zsarolóprogrammal való megfertőzéséhez. A zsarolóprogram képes volt titkosítani a felhasználói fájlokat, valamint az eltávolítható, megosztott vagy helyi meghajtókon lévő bármely adatbázist.

Egy brazíliai áramszolgáltatót megtámadó zsarolóvírus esete

A Companhia Paranaense de Energia (Copel), egy brazil áramszolgáltató vállalatot 2021 januárjában zsarolóprogram-támadás érte, amelyet a források szerint a DarkSide zsarolóvírus-fenyegető csoport hajtott végre [116]. A támadás részleteinek vizsgálata során kiderült, hogy a támadók körülbelül 1000 GB adatot exfiltráltak a vállalat rendszereiből. Az ellopott adatok között szerepeltek hálózati diagramok és térképek, biztonsági mentési ütemtervek, az alkalmazottak és ügyfelek személyes azonosításra alkalmas (PII) adatai, szerződések, titoktartási nyilatkozatok (NDA-k), valamint hálózati tervek. Az exfiltrált adatok között tiszta szövegű jelszavakat tartalmazó CyberArk adatbázis is volt.

Ezenkívül a támadók azt állították, hogy kiszivárogtattak egy Active Directory-adatbázist is, amely tartalmazta az AD-ben szereplő összes felhasználó azonosítóját, csoportjait és jelszavait. Ez különösen súlyos adatbiztonsági fenyegetést jelentett, mivel a kiszivárgott információk közvetlen hozzáférést biztosíthattak a vállalat kritikus informatikai rendszereihez és infrastruktúrájához.

Az egyik legnagyobb olajvezetéket ért Ransomware-támadás

A Colonial Pipeline-t, az USA legnagyobb, 5 500 mérföldön átívelő és naponta körülbelül 3 millió hordó üzemanyagot szállító csővezetékét 2021. május 7-én egy Darkside nevű APT-csoport által végrehajtott zsarolóprogram-támadás érte. A Colonial Pipeline tisztviselői elmondása alapján [113] azért, hogy megfékezzék a fenyegetést [78], egyes rendszereket offline állapotba kellett helyezniük, ami a csővezeték teljes működésének leállítását eredményezte. A hackerek egy feltört VPN hitelesítő adatainak felhasználásával tudtak hozzáférni a hálózathoz, ez vezetett a zsarolóvírus fertőzéshez [113]. A kompromittálódás hatása pusztító [103] volt, mivel az USA teljes észak-, és délkeleti régiójában leállt az üzemanyag-forgalmazás. Ezen kívül a vállalatnak 75 bitcoint kellett fizetnie váltságdíjként, ami 2024 november végi árfolyamon körülbelül 7 millió dollárnak felel meg.

Egy coloradói energiaipari vállalatot 25 év adataitól megfosztó támadás

A coloradói székhelyű Delta-Montrose Electric Association (DMEA) energetikai vállalatot 2021. november 7-én rosszindulatú támadás érte, amely belső hálózati rendszerei közel 90%-ának és mintegy 25 év historikus adatának az elvesztését okozta. A visszamenőleges adatok között dokumentumok, Excel-táblázatok és űrlapok voltak. A vállalat szerint a támadás következtében a vállalat ügyfélszolgálata, a fizetések feldolgozására szolgáló eszközei és számlázási rendszerei megszakadtak, ami miatt az ügyfelek nem tudtak fizetni, illetve nem kaptak támogatást a vállalat által kínált szolgáltatásokhoz.

M7. melléklet – Kockázatkezelés elméleti háttere

A KSM (Károkozási Súlyossági Mutató) és KoI (Komplexitási Index) a kockázatkezelési irodalom alapfogalmaira épül. A sebezhetőség–fenyegetés–kockázat hármas a KoI komponensek koncepcionális alapja, míg a hatásmérés módszertana a KSM skála elméleti háttere.

A tényleges kockázatokat figyelembe nem vevő, mindenre kiterjedő maximális védelem jobban nehezítheti az informatikai támogatás használatát, mint maguk az adott rendszerrel kapcsolatban fellépő rendkívüli események.

Az informatikai szakemberek arra törekszenek, hogy az adott informatikai támogatás biztonságának mértékét és pillanatnyi állapotát objektív módon határozzák meg. Ezzel szemben az átlagemberek számára a biztonság, így az informatikai biztonság is, bizalmi kérdés. Emiatt a vállalati vezetők számára gyakran nehezen értelmezhető az informatikai biztonság kérdése. Valójában az informatikai biztonság hiánya vagy sérülése az, amit a mindennapi életben a vezetés és minden más érintett érzékel. Ahhoz, hogy egy adott szervezeti egység vagy a szervezeten belül egy adott információs rendszer biztonsága kialakítható legyen, az érintetteknek pontosan ismerniük kell az adott informatikai támogatás célját. Az adott rendszer szempontjából releváns kockázatok mértékét is meg kell határozni. Így a szakemberek képesek a feltárt kockázatokkal arányos védelmi rendszert kialakítani [118].

Az informatikai rendszer biztonsága nem statikus állapot. Az adott szervezet külső és belső körülményei folyamatosan változnak, és ehhez hozzá kell igazítani az informatikai támogatás biztonságát. Az informatikai rendszer biztonságával kapcsolatos tevékenységi csoportok az alábbiak [44]:

a) Az informatikai biztonsági rendszer létrehozása és a védelemmel szembeni követelmények kidolgozása egy egyszeri tevékenységet jelent.

b) A második részterület a napi működtetés. Ezen a területen figyelemmel kell lenni arra, hogy az informatikai támogatás biztonságát is érintő működési környezet és az ennek függvényében a biztonságos működéssel kapcsolatos követelmények folyamatosan változnak. A változásokhoz alkalmazkodni kell, és a kialakított biztonsági rendszert folyamatosan felül kell vizsgálni.

c) A harmadik terület a jövőt érinti. Az új és meglévő kockázatok súlyozásának változásaira vonatkozó előrejelzésekkel fel lehet készülni a várható veszélyekre. Az előrejelzések megbízhatóságában az időtényező meghatározó jelentősségű.

A biztonság azt jelenti, hogy olyan feltételeket teremtenek meg és szavatolják azok folyamatos meglétét, amelyek az adott szervezet számára elviselhető szintre mérsékelik az adott területtel szemben fennálló bizonytalansági és kockázati tényezők által jelentett veszélyt. A biztonság megfelelő védelmet nyújt a kockázatok hatásaival szemben. Ezt úgy éri el, hogy a kockázatokat időben felfedi, hatásmechanizmusukat akadályozza, gyengíti vagy kioltja [119].

A biztonsági rés, sérülékenység vagy sebezhetőség olyan gyengeséget jelöl, amelynek kihasználásával a fenyegetés forrása kárt tehet az informatikai rendszerben.

Az információ- és az informatikai biztonság közötti kapcsolatot tekintve alapvető, hogy az információbiztonság az összes, az adott szervezet által kezelt információval kapcsolatosan szavatolja annak sértetlenségét, bizalmasságát és rendelkezésre állását. Ennek egy részterülete az informatikai rendszer, illetve az informatikai rendszerben kezelt adatok köre. Erre a részterületre vonatkozik az informatikai biztonság. Az információtechnológia (röviden IT) rendszerelemei az olyan informatikai eszközök, amelyek az adatok tárolásával, továbbításával kapcsolatos tevékenységeket látnak el, maga az IT rendszer pedig az IT rendszerelemek és az elemek kapcsolatainak összességét jelenti [118].

Az adatbiztonsággal kapcsolatos tevékenységek az adatokat olyan műveletek ellen védik, mint a jogosultság nélküli hozzáférés, törlés, módosítások és nyilvánosságra hozatal[120].

Az adatvédelem fogalma elsősorban a személyes adatok védelmével kapcsolatos tennivalókat jelenti. A közérdekből nyilvános adatok megismerésével kapcsolatos alapvető szabályok köre is ehhez a területhez tartozik [121].

A kockázatot az informatikai biztonságban egyrészt a veszély, a veszélyforrás konkrét megnevezésére használják, másrészt rendkívüli események bekövetkezésének számszerűsített matematikai valószínűségét is kockázatként nevezik meg. A második lehetőség esetén a kockázat számítási alapja egy-egy konkrét veszélyes esemény bekövetkezési valószínűsége és a károk értéke. A kockázatok osztályozási szempontjai lehetnek például az elfogadhatóság, azonosíthatóság, felismerhetőség [119].

A kockázatkezelés a terület elemzési, kiértékelési, szabályozási eljárásainak módszeres alkalmazását jelenti [98]. Maga a kockázatelemzés olyan módszeres eljárás, amely a lehetséges

veszélyekkel kapcsolatos információkat rendszerezi és elemzi, célja az informatikai rendszerek és támogatások kapcsán felmerülő veszélyek azonosítása. A kockázatok kiértékelése magában foglalja annak folyamatát, amely során a szervezet meghatározza, hogy mely kockázatok tekinthetők még elfogadhatónak a működés szempontjából [98].

A kockázatértékelés a kockázatelemzés és a kockázatok kiértékelésének együttes tevékenysége, amely célja a szervezet számára releváns kockázatok teljes körű felmérése és kezelése [45].

A kockázatszabályozás a kockázatkezeléshez kapcsolódó döntéshozatali folyamat, amelybe beletartozik a meghozott döntések végrehajtása és döntések hatékonyságának rendszeres felülvizsgálata [119].

Az informatikai rendszerek esetében alapvető követelmény, hogy az adatok és eszközök rendelkezésre álljanak a megfelelő időben, pontosan az elvárt módon, és naprakészen az arra jogosultak számára [122].

Legújabban az információ biztonsághoz hozzáadódik az elszámoltathatóság (Accountability) biztosítása is, amely mechanizmusokat foglal magában a problémák személyhez kötésére. Ez azt jelenti, hogy egyértelműen meghatározható legyen, ki milyen műveleteket végzett, és ezekért a műveletekért felelőssé tehető [123].

Az informatikai biztonságot az alábbi jellemzők határozzák meg:

- Egy adott rendszer informatikai biztonsága akkor megfelelő, ha az összes az adott rendszer számra ténylegesen is gondot jelentő veszélyt figyelembe veszik a védelem kialakításakor.
- Az informatikai biztonsági intézkedéseket minden esetben a kockázatokkal arányos módon kell meghozni.
- Az informatikai biztonság teljes körű módon, minden elemet magában foglalva ad védelmet az informatikai rendszernek.
- Továbbá elvárás az informatikai biztonsági rendszerrel kapcsolatban, hogy időben folyamatosan kell megvalósulnia a védelemnek.
- Az informatikai biztonság működtetésével kapcsolatos védelmet a lehetséges károkkal is arányos módon határozzák meg [124].

A kockázatkezelés alapfogalmai és módszertana az informatikai biztonságban

Kockázat: Az informatikai biztonságban a kockázat fogalma kettős jelentéssel bír. Egyrészt jelenti magát a veszélyforrást vagy fenyegetést, másrészt egy matematikailag kifejezhető valószínűségi értéket, amely egy konkrét veszélyes esemény bekövetkezési valószínűségének és az okozott kár mértékének szorzata [42]. A kockázat tehát nem pusztán elméleti konstrukció, hanem mérhető és kezelhető jelenség.

Sebezhetőség (Vulnerability): A rendszer azon gyenge pontja, amely kihasználható egy támadó által, és amely csökkenti az informatikai vagy fizikai védelem hatékonyságát. A sebezhetőségek lehetnek technikai (pl. szoftverhibák), szervezeti (pl. hiányos eljárásrendek) vagy emberi eredetűek (pl. képzési hiányosságok).

Fenyegetés (Threat): Bármilyen esemény, szereplő vagy tényező, amely potenciálisan kárt okozhat a rendszerben. A fenyegetések származhatnak külső forrásokból (pl. hackertámadások) vagy belső forrásokból (pl. elégedetlen alkalmazott), lehetnek szándékosak vagy véletlenek.

A kockázatkezelési folyamat

A kockázatkezelés ciklikus folyamat, amely négy fő szakaszból áll:

1. **Kockázatazonosítás**: A potenciális veszélyforrások és sebezhetőségek feltérképezése. Ez magában foglalja a rendszer átfogó vizsgálatát, a korábbi incidensek elemzését és a szakértői vélemények figyelembevételét [45].
2. **Kockázatelemzés**: A feltárt kockázatok valószínűségének és potenciális hatásának becslése. Ez történhet kvalitatív módszerekkel (alacsony/közepes/magas besorolás) vagy kvantitatív módszerekkel (számszerű valószínűségek és kárbecslések) [46].
3. **Kockázatértékelés**: Az elemzett kockázatok priorizálása és az elfogadható kockázati szint meghatározása. A szervezet vezetősége dönt arról, mely kockázatokat kell kezelni, és melyeket lehet elfogadni [42].
4. **Kockázatkezelési intézkedések**: A kiválasztott kezelési stratégia implementálása, amely lehet:
    - **Kockázatcsökkentés**: Védelmi intézkedések bevezetése

- **Kockázatáthárítás**: Biztosítás vagy outsourcing
- **Kockázatelkerülés**: A kockázatos tevékenység megszüntetése
- **Kockázatvállalás**: A maradványkockázat tudatos elfogadása

A folyamat ciklikus jellege biztosítja, hogy a szervezet folyamatosan alkalmazkodjon a változó fenyegetési környezethez és a belső változásokhoz.

Felmérések a szabályozásban és kockázatkezelésben

Az alábbi felmérési területek adják azt a szervezeti kontextust, amelyben a disszertáció központi metrikái – a KSM (Károkozási Súlyossági Mutató) és a KoI (Komplexitási Index) – gyakorlati relevanciát nyernek. A H1 hipotézisben vizsgált kritikus infrastruktúra-besorolás (KrI_flag) szintén ezen kockázatfelmérési keretrendszerre épül. A vagyonleltár és a kockázatértékelés itt bemutatott lépései képezik azt a módszertani alapot, amelyben a KSM-skála szerinti incidenshatások és a KoI-komponensek (perzisztencia, laterális mozgás, észlelés-elkerülés) értelmezhetők.

Az alábbi területeken kell elvégezni egy részletes felmérést:

a) Felmérendő, milyen szintű az adott szervezet szabályozási környezete.

b) Vizsgálandó, hogy a felmérés idején milyen a szervezeti szintű biztonság helyzete.

c) Ellenőrizni kell, hogy alakul a vagyontárgyak biztonsága az adott időben.

d) Fel kell mérni az emberi erőforrások biztonságának pillanatnyi szintjét.

e) Fel kell térképezni az informatikai támogatással kapcsolatos környezeten belül a már meglévő fizikai és logikai biztonság szintjét [125].

f) Vizsgálat tárgyát kell, hogy képezze az informatikai támogatással kapcsolatos kommunikáció és üzemeltetés biztonsági állapota.

g) Feladat a hozzáférés-ellenőrzés és a jogosultságok kiosztásának vizsgálata.

h) Biztonsági szempontból ellenőrizendők az adott pillanatban használt fejlesztési, beszerzési, karbantartási eljárások.

i) Vizsgálandó - amennyiben van ilyen - a meglévő incidenskezelési rend, mint a kiindulási helyzet feltérképezésének szintén szerves része [126].

j) Fel kell mérni az üzletmenet folytonosságának fenntartással kapcsolatos, meglévő intézkedéseket.

k) Fel kell mérni az adott szervezet beszállítóit és ellátási lánctól való függésüket.

l) Ellenőrizni és biztosítani kell a jogszabályi, törvényi megfelelést [68].

A szervezeti vagyon védelme érdekében az első lépés annak meghatározása, hogy milyen vagyonelemeket szükséges védelem alá vonni. A vagyonleltár elkészítése kulcsfontosságú, mivel átfogó képet nyújt a szervezet számára azokról a vagyonokról, amelyek védelme kritikus

jelentőségű, beleértve a fizikai és immateriális javakat is [127]. Ennek célja, hogy naprakész nyilvántartás álljon rendelkezésre a védendő vagyonelemekről és azok értékéről.

A szervezetek számára kiemelt fontosságúak a tárolt információk, különösen azok, amelyek az informatikai rendszerekben találhatók. Az információvagyon közé tartoznak a tárolt adatok, adatbázisok, az informatikai rendszer üzemeltetéséhez szükséges dokumentációk, valamint a szoftvervagyon, ideértve az operációs rendszereket, felhasználói szoftvereket, fejlesztőeszközöket és szolgáltatásokat. A vagyonleltárban szintén szerepelnek a hardver eszközök, kommunikációs eszközök, adathordozók és egyéb műszaki berendezések [102].

A biztonságirányítás keretében minden informatikai támogatáshoz kapcsolódó elemet fel kell tüntetni a vagyonleltárban. Ez kiterjed az adatok feldolgozására szolgáló folyamatokra és tevékenységekre is. Minden vagyonelemhez szükséges valamilyen értéket rendelni, amely meghatározza a szervezetet érő potenciális kárt abban az esetben, ha az adott elem sérülne. Ez az érték a biztonsági intézkedések meghatározásának alapja. Nagy értékű vagyonelemek esetében a megelőzés kulcsfontosságú, míg kisebb értékű elemeknél a gyors helyreállításra helyeződik a hangsúly.

Az értékek meghatározása során figyelembe kell venni az informatikai támogatás sérülésének lehetséges következményeit, és azt, hogy ezek milyen mértékű kárt okozhatnak a szervezet számára. A kárérték meghatározásakor a legrosszabb forgatókönyet kell alapul venni [124]. A kárértékszintek kialakítása során figyelembe kell venni a különböző kártípusokat, beleértve a közvetlen anyagi károkat, dologi károkat, személyi károkat, stb. A szervezeti szinten egységesen megállapított kárértékszintek jóváhagyása a vezetőség feladata [128; 129].

Miután a vagyonleltár elkészítése megtörtént, a következő lépés a kritikus fontosságú vagyonelemek rangsorolása. Ezzel a szervezet képes azonosítani a védelmet igénylő legfontosabb vagyonelemeit. A rangsor felállítását követően meghatározásra kerül, hogy a vagyon mely elemeit és milyen fenyegetésekkel szemben szükséges védeni. A vagyonleltár véglegesítése után a szervezet átfogó vagyontérképpel rendelkezik, amely lehetővé teszi a kritikus vagyonelemek célzott védelmét [102; 129].

A vagyonleltár elkészítését követően elengedhetetlen azoknak a kockázatoknak az alapos felmérése, amelyek akadályozhatják az informatikai támogatás hatékony és biztonságos működését. Az ilyen kockázatok felméréséhez a szervezetnek egy olyan módszertant kell alkalmaznia vagy kidolgoznia, amely nemcsak a belső igényekhez és követelményekhez igazodik, hanem szorosan illeszkedik a már meglévő Informatikai Biztonsági Irányítási

Rendszer kereteihez. Emellett alapvető fontosságú, hogy a kockázatfelmérési rendszer összhangban legyen a szervezetre vonatkozó külső szabályozásokkal, ideértve az információbiztonsági, jogi és szabályozási előírásokat is, amelyek betartása kötelező [45].

A biztonságos és a szervezet igényeihez igazodó informatikai támogatás kiépítése és fenntartása nem csupán technikai, hanem elsősorban szervezési kérdés. A rendszerszemléletű megközelítés elengedhetetlen az informatikai kockázatok feltárása és kezelése során. Ez a megközelítés megköveteli, hogy a folyamat elején a szervezet teljes működését átfogóan felmérjük, beleértve az üzleti folyamatokat, a külső és belső környezetet, valamint a partnerekkel fennálló kapcsolatrendszert. Csak a kiindulási helyzet alapos elemzése után lehet kidolgozni egy olyan védelmi stratégiát, amely nemcsak szakmailag, hanem gazdaságilag is megalapozott, és amely egyaránt megfelel a belső szervezeti igényeknek és a külső jogi, szabályozási elvárásoknak. Ezáltal biztosítható, hogy a kialakított védelmi intézkedések hatékonyan szolgálják a szervezet hosszú távú informatikai biztonságát, minimalizálva a kockázatokat és biztosítva a folyamatos megfelelést a törvényi előírásoknak.

A szervezeti elvárásoknak megfelelő, értékteremtést fenyegető kockázatok a szervezet stratégia döntéseiből és a környezeti változásokból adódnak. Míg a helyzet, amelyben egy adott intézmény a tényleges fontosságához képest alultervezett biztonsági rendszerrel rendelkezik rengeteg veszélyt hordoz, addig a túlzott biztonságra való törekvés az üzemszerű működés számára jelent fölösleges akadályokat.

Az informatikai munkaterv megvalósítási kockázatai közé olyan eshetőségek tartozhatnak, mint például egy nem megfelelően előkészített szoftverbevezetés. Fontos például, hogy a telepítendő szoftvereket ehhez értő alkalmazottak végezzék el, a felhasználók pedig képzésben részesüljenek a használat megkezdése előtt. Ha csak menetközben ismerik meg a szoftver a felhasználók, nagyobb az esélye a hibáknak.

Egy adott intézmény informatikai támogatásának gyenge pontjait, sebezhetőségeit az alábbi részterületekre lebontva kell feltárni [130]:

a) az informatikai támogatás fizikai biztonságával kapcsolatos sebezhetőségek,

b) az adott informatikai rendszer logikai biztonságát érintő sebezhetőségek,

c) a szervezeti szintű biztonság sebezhetőségei.

A problémát okozni tudó sebezhetőségek vizsgálatát az adott szervezet informatikai támogatásának minden egyes elemére vetítve el kell végezni. A sebezhetőségek feltárásához

mindenekelőtt az adott szervezet informatikai biztonságával kapcsolatos dokumentumait szükséges áttekinteni. Személyes interjúk készítésével kell megbizonyosodni arról, hogy mennyire ismerik a céges munkavállalók a biztonsági előírásokat. Az alkalmazottak biztonsági ismereteit, a biztoság-tudatosság meglévő szintjét értékelni kell [119].

A kiindulási helyzet pontos feltárására irányuló felmérés során kritikus fontosságú a szabályozási, dokumentációs hiányosságok azonosítása. Az alábbiakban felsoroltak mind sebezhetőségként értelmezendők [131]:

a) azok a dokumentumok, amelyek hiányoznak, de a biztonságos működéshez elengedhetetlenek lennének,

b) a szervezetnél meglévő, de a gyakorlatba még nem átültetett szabályzók,

c) a már alkalmazott, de nem megfelelő szabályzók, illetve azok, amelyek használatához nem állnak rendelkezésre a szükséges feltételek,

d) szervezeti ellentmondások, mint például amikor egy személynek saját maga ellenőrzése lenne szükséges informatikai biztonsági szempontból.

A szabályozás sebezhetőségei után a technológiai sebezhetőségeket is vizsgálni kell. Az infrastruktúra dokumentációjának naprakészségét mindenképpen szükséges ellenőrizni. Ennek a dokumentációnak az aktualizálását el kell végezni, bizonyos esetekben pedig az auditálását is végre kell hajtani. Meg kell azt nézni, hogy az adott időpontban hatályos biztonsági előírások milyen módon és formában valósulnak meg ez érintett technológiai elemeken.

Az érintett rendszer fizikai biztonságával kapcsolatban vizsgálandók a védelmi intézkedések. Meg kell nézni azt, hogy alkalmaznak-e védelmi intézkedéseket a következő elemek károsodásának megelőzésére (lehetséges fizikai meghibásodások): az adott intézmény által használt hardver eszközök, egyéb az informatikai támogatáshoz szükséges berendezések, a szerver számítógép, gépek és a gépterem, a géptermek eszközei. Azt is meg kell vizsgálni, hogy adott időben használt számítógépekhez, gépteremhez, az egyéb informatikai eszközökhöz való fizikai hozzáférések korlátozása megfelelő módon van-e megoldva. Ellenőrizni kell az elemzés során, hogy milyen rend szerint regisztrálják a felhasználói jogosultságokat, hozzáféréseket. Ellenőrizendők a hozzáférésekkel kapcsolatos naplózások is [90].

A konkrét egységen belül az informatikai támogatás logikai biztonsági állapotával kapcsolatban vizsgálandók, hogy léteznek-e, illetve milyenek a védelmi intézkedések vannak alkalmazásban az alábbi területeken:

a) adott időpontban használt informatikai támogatás felhasználóinak azonosítása, hitelesítése,

b) felhasználói bejelentkezések ellenőrzésére használt eljárások,

c) rendszerben tárolt jelszavak, kulcsszavak kezelésére használt módszerek,

d) sikertelen bejelentkezések figyelésére, naplózására használt módszerek,

e) inaktív felhasználókat szűrő eljárások,

f) speciális jogosultságokkal rendelkezők tevékenységének nyomon követésével kapcsolatban használt eljárások,

g) a meglévő hozzáférés-ellenőrzési és jogosultsági rendszer lefedettsége (minden felhasználónak csak a munkavégzéséhez ténylegesen szükséges területekhez van-e hozzáférése). [45].

A szervezetnek a kockázatok részletes kiértékelésének elkezdése előtt az alábbi területekkel kapcsolatban kell rendelkeznie dokumentumokkal [132]:

a) a használt informatikai infrastruktúra aktualizált logikai és fizikai leírása,

b) a hálózat felépítését leíró teljeskörű dokumentáció,

c) az Informatikai Biztonságirányítási Rendszerrel kapcsolatos rendszerelemek listája,

d) a vagyonelemek és rendszerelemek közötti kapcsolatok dokumentációja,

e) egy lista az informatikai támogatás sebezhetőségeiről.

M8. melléklet – Informatikai Biztonsági Szabályzat; Ellenőrzés és Mérés

Az Informatikai Biztonsági Szabályzatban (IBSZ) mindenre kiterjedően rögzítik adott intézmény működéséhez, működtetéséhez szükséges informatikai biztonsággal kapcsolatos intézkedéseket, folyamatokat. A szabályzat részét képezik a szervezet különböző feladatköreiben tevékenykedő felhasználóinak feladat-, felelősség-, és hatáskör-leírásai. Az adott intézmény által használt informatikai támogatás elemeivel (dolgozók, technikai eszközök, számítógépes alkalmazások, helyiségek stb.) kapcsolatos biztonsági követelmények szintén ennek a szabályzatnak a részei. [131]

Az egyéb dokumentumokban leírtakra az IBSZ csak a dokumentumok pontos megnevezésével hivatkozik. Az Informatikai Biztonsági Szabályzattal kapcsolatban lévő, a szabályzatban hivatkozott dokumentumok területei:

a. Az irányítás, például a szervezeti ügymenet, a munkavállalás, a titkos ügykezelés rendje.

b. A munkavégzés technikai támogatására vonatkozó szabályzatok, mint ügyiratkezelés, informatikai eszközök használata, selejtezés, vagy sokszorosítás szabályzatai.

c. A tűzvédelmi, a munkavédelmi és egyéb hasonló szabályzatok, amennyiben a szervezet rendelkezik ezekkel. [131]

A felhasználók informatikai támogatással kapcsolatos kötelességeit az Informatikai Felhasználói Szabályzat tartalmazza. Ez a szabályzat írja le, hogy milyen események bekövetkeztekor és milyen módon kell kapcsolatba lépnie a felhasználónak az informatikai támogatást működtető szakemberekkel. A felhasználói szabályzat mutatja be a felhasználók számára engedélyezett, és tiltott tevékenységeket. A szabályzat rögzíti a biztonság fenntartására szolgáló ellenőrzési és a számonkérési formákat is. A szabályzat rögzíti azt is, mi a tennivalója a felhasználónak, ha valamilyen rendkívüli esemény történik. Ez a dokumentum az alapja a felhasználók informatikai biztonsági oktatásának.

A napi munka alapjaként szolgáló eljárásrend-gyűjtemény végrehajtási utasításai rendszer specifikusan rögzítik az informatikai biztonsággal kapcsolatos tevékenységeket. Az elkészült eljárásrendet igény esetén a munkaköri leíráshoz mellékelni lehet. Mivel az eljárásrend bizalmas információkat tartalmaz, biztosítani kell, hogy csak az a személy férjen hozzá a dokumentumhoz, akinek munkaköri kötelessége a dokumentumban foglaltak betartása. [131]

Az IBIR napi szintű működtetésével kapcsolatosan is van néhány terület, amire fokozott figyelmet kell fordítania a szervezetnek. Mivel az emberi tényező kiemelkedően fontos minden kiberbiztonsági keretben, az oktatás és a folyamatos képzés biztosítása, valamint a biztonsági protokollok és eljárások szüntelen fejlesztése létfontosságú a szervezet biztonsági kultúrájának erősítésében. Az alkalmazottak képzése és a tudatosság növelése segít megelőzni a felhasználói hibákból eredő biztonsági incidenseket, így védve a szervezetet a kibertámadásokkal szemben {Muha, 2018 #107}.

Az emberi tényező nagyon fontos kockázati dimenzió. Elsősorban nem a szándékos károkozás, hanem a felhasználói hibák miatt. Ennek megfelelő súlyossággal kell érvényesíteni az informatikai támogatás biztonságos üzemeltetésével kapcsolatos követelményeket már a munkaerő felvételnél, a különböző szerződésekben, valamint a mindennapos munkavégzés során.

A megfelelő szintű a szervezeti biztonság elérése érdekében, a dolgozókat a feladataikhoz kötődő informatikai biztonsági szabályokról, feladatokról és felelősségekről szóló oktatásban kell részesíteni. Az érintett személyeknek ismerni és érteni kell a biztonsághoz kötődő feladataikat, mint például a fizikai biztonsággal, az e-mail használattal és a vírusvédelemmel kapcsolatos kötelességeiket. Magasabb szintű felhasználói jogosultsággal (rendszeradminisztrátor, rendszergazda) érintett területek esetében ilyen terület a tűzfalak konfigurálása, valamint az informatikai támogatással kapcsolatos, annak biztonságát érintő események kezelése is. {Muha, 2018 #107}

A felhasználóknak tudatában kell lenniük az informatikai biztonsági fenyegetések kockázatával és lehetséges negatív következményeivel, az ezzel kapcsolatos személyes felelőségükkel és azzal, hogy a veszélyeket milyen intézkedések betartásával tudják elhárítani. A felhasználóknak ismerniük kell továbbá a biztonsági eljárások alkalmazási lehetőségeit és az adatfeldolgozási módszerek biztonságos használatának módjait. Minden érintett alkalmazottat ki kell képezni a szervezet informatikai támogatásának megfelelő használatáról és a megszerzett ismereteket folyamatosan frissíteniük kell.

Az általános informatikai biztonsági ismereteken túl az informatikai támogatás üzemeltetéséért felelős munkavállalókat a szerepük szintjéhez igazodó szakirányú biztonsági képzésben is részesíteni kell, ami egyes esetekben akár egyetemi kurzuson való részvételt is jelenthet. Ez azt is jelenti, hogy egy a támogatás fejlesztésére irányuló projekt megvalósításához az érintett

terület felelőseinek az új üzemeltetési ismeretek elsajátításán túl a kapcsolódó biztonsági ismereteiket is bővíteniük kell [90].

Ahhoz, hogy az Informatikai Biztonságirányítási Rendszer auditálható legyen, minden folyamatot dokumentálni kell, így az oktatásról is jegyzőkönyvet szükséges kiállítani, amit a felhasznált oktatóanyagokkal együtt tárolni kell [102].

Különösen a bizalmi munkakörök betöltése esetén fontos a dolgozók előzetes biztonsági szűrése. A biztonsági vizsgálatoknál szem előtt kell tartani a személyiségi jogokat. A munkatársak felvételénél ellenőrizni kell referenciáikat, személyi adataikat, hivatalos dokumentumaikat. Ha a felhasználó államtitkokat vagy szolgálati titkokat kezel, nemzetbiztonsági ellenőrzés is szükséges lehet. A személyzet biztonsági ellenőrzésének rendjét ugyancsak egy erre szolgáló szabályzatban kell meghatározni.

A munkaköri leírásnak az informatikai biztonsággal kapcsolatos, az adott munkatársra tartozó követelményeket is tartalmaznia kell. Már a munkavállaló felvételénél fontos az, hogy az őt érintő szakterület és a vele járó felelősségi szint egyértelműen meg legyen határozva, amihez elengedhetetlen, hogy az egyes munkakörökhöz tartozó informatikai támogatási funkciók megfelelően legyenek csoportosítva.

Az alkalmazottak - amennyiben ez szükséges - munkavállalásuk megkezdése előtt titoktartási nyilatkozatot írnak alá. Hasonló dokumentumot kell aláírniuk helyzet függvényében azoknak, akik csak átmenetileg férnek az adott szervezet informatikai rendszeréhez. Ezek a személyek is kizárólag a titoktartási nyilatkozat aláírását követően kaphatnak hozzáférést az adatokhoz és a szervezet informatikai eszközeihez. Az alkalmazási feltételek módosulásakor a titoktartási nyilatkozatot felül kell vizsgálni. Azoknál a munkaköröknél, ahol ez indokolt, (például a vezető beosztású munkakörben, vagy az informatikai támogatást üzemeltetők esetén), az informatikai biztonsággal és titoktattással kapcsolatos személyes elszámoltathatóságot az alkalmazás megszűnése után is indokolt lehet egy meghatározott ideig érvényben tartani [90].

A titoktartási nyilatkozatban rögzíteni kell a vállalt kötelezettségek megsértéséből eredő lehetséges jogi következményeket, valamint azoknak tartalmazniuk kell az alkalmazottak szerzői jogokkal, illetve személyes adatok védelmével kapcsolatos jogait és kötelességeit is. A szerzői jogok egyik érdekes alkalmazási területe a jogvédett tartalmak (filmek, szoftverek) munkahelyen történő letöltése. [97]

Ellenőrzés

Az IBIR működtetésének része a folyamatos ellenőrzés, mert ez segíthet megelőzni a nemkívánatos eseményeket. Az informatikai biztonságirányítás akkor működik jól, ha a bevezetett előírások, biztonsági beállítások és szabályok a mindennapi gyakorlat szerves részévé váltak. A folyamatos kommunikáció során kell megbizonyosodni az alábbiakról:

a) Megvalósíthatók-e a bevezetett előírások a működési gyakorlatban?

b) A biztonságos működtetéshez szükséges erőforrások elegendők mértékben rendelkezésre állnak-e, indokolt-e kiegészítésük, pótlásuk?

c) Szükséges-e az aktuálisan érvényben lévő intézkedések módosítása?

Az ISO 27001 szabvány legújabb verziója [133], amely az információbiztonsági irányítási rendszerek (IBIR) alapját képezi, hangsúlyozza a folyamatos ellenőrzés és auditálás fontosságát az IBIR hatékonyságának fenntartásában és javításában. Az ellenőrzések célja, hogy biztosítsák az információbiztonsági szabályok mindennapi gyakorlatba való beépülését, valamint a biztonsági beállítások és szabályok tényleges működését. Az ISO 27001 szerint az ellenőrzési folyamatnak rendszeresnek és szisztematikusnak kell lennie, annak érdekében, hogy az esetlegesen felmerülő problémák időben feltárhatók legyenek, és megfelelő korrekciós intézkedések kerüljenek bevezetésre. Az ISO 27001:2022 szabvány külön kiemeli a szervezeten belüli kommunikáció fontos szerepét, hogy az alkalmazottak tisztában legyenek az IBIR céljaival, a rendszer működésével és a rájuk vonatkozó felelősségekkel.

A szabvány előírásainak megfelelően az ellenőrzések során felül kell vizsgálni, hogy az IBIR működéséhez szükséges erőforrások elegendőek-e, és hogy a jelenlegi intézkedések megfelelnek-e a szervezet információbiztonsági céljainak. Ha bármilyen eltérés vagy hiányosság kerül beazonosításra, indokolt az ISO 27001 iránymutatásai alapján az intézkedések módosítása vagy bővítése, hogy azok továbbra is hatékonyan működjenek a szervezetben. A szabvány azt is előírja, hogy az alkalmazott biztonsági megoldásokat folyamatosan értékelni kell, különös tekintettel a személyi tényezőkből eredő kockázatokat minimalizáló automatizált rendszerek használatára.

Összegezve az ISO 27001:2022 irányelvei nemcsak a meglévő biztonsági intézkedések rendszeres ellenőrzését és felülvizsgálatát követelik meg, hanem azt is, hogy a szervezetek dinamikusan alkalmazkodjanak a változó kiberbiztonsági környezethez, folyamatosan fejlesztve információbiztonsági rendszereiket és eljárásaikat.

Az ellenőrzésekre az Informatikai Biztonságirányítási Rendszer bevezetésének időszakában javasolt nagyobb hangsúlyt fektetni. Természetes jelenség, hogy a tervezett intézkedések esetleg nem a tervezés során elképzelt módon hatnak. Az esetleges problémás területek feltárását követően az intézkedések és kontrollok módosítása lehet szükséges. Az alkalmazott biztonsági megoldásoknál törekedni kell a személyi tényezőt kiküszöbölő, automatizált megoldások alkalmazására. A felhasználók nemkívánatos tevékenységét, mint bizonytalansági tényezőt kiküszöbölő megoldás lehet például a jelszavak maximális érvényességének beállítása, vagy a központi levélszemét szűrő használata.

Az informatikai biztonsággal kapcsolatos eljárások hatékonyságát folyamatosan monitorozni és értékelni szükséges. A mérési eredmények nyomon követése lehetővé teszi az időszerű korrekciót. Az informatikai biztonság működtetésével kapcsolatos ellenőrzési pontokat, úgynevezett mérföldköveket meg kell határozni, illetve meg kell fogalmazni az egyes ellenőrzésekre vonatkozó sikerkritériumokat. [119]

Az informatikai biztonság területén kitűzött stratégiai célok megvalósítása után feltétlenül szükséges az utólagos kockázatelemzés elvégzése. Ezzel az eljárással ellenőrzi a szervezet, hogy a bevezetett biztonsági intézkedések, informatikai fejlesztések meghozták-e a tőlük várt eredményeket. Az informatikai biztonsági stratégiai célok megvalósítása során elkészült rendszerleírásokat, jegyzőkönyveket, dokumentumokat, meg kell őrizni. Az őrzést úgy kell megoldani, hogy a fenti anyagok az előírt ideig visszakereshetők legyenek, amennyiben arra szükség van.

A hatékony működtetéshez a változások nyomon követése mellett az Informatikai Biztonsági Irányítási Rendszer egészének a működését is folyamatosan ellenőrizni kell. Új, az adott rendszert érintő biztonsági kockázatok, fenyegetések jelenhetnek meg; a korábban ismert fenyegetések súlya is átalakulhat. Az informatikai biztonság gyenge pontjai, sebezhetőségei, és ezek lehetséges hatásainak mértéke tehát folyamatosan változik. Az informatikai biztonságra hatással lehetnek például a szervezet környezetét, belső felépítését, stratégiai céljait, alkalmazott technológiáit érintő módosulások, illetve változhat a jogszabályi környezet is [102].

A fenti változások miatt a szervezetnek rendszeres időközönként értékelnie kell az addig a pontig azonosított kockázatokat IBIR-ben meghatározott kockázatmenedzsment módszertan segítségével, és amennyiben ezek alapján szükséges, át kell alakítani a kockázatkezelési eljárások rendjét. A vizsgálatok során az alábbi kérdésekre kell válaszokat keresni:

a) Az IBIR hatóköre megfelel a tényleges helyzetnek?

b) Szükséges a meghatározott feladatok és felelősségek újraértékelése a biztonságos működéshez?

c) Az informatikai támogatással kapcsolatba kerülő dolgozók betartják a szabályzatok által meghatározott rendet?

d) Az ellenőrző mechanizmusok biztosítják, hogy az eseményeket az IBIR azonnal érzékelje?

e) A szervezet által bevezetett védelmi intézkedések képesek eredményesen működni?

f) Az üzletfolytonossági és katasztrófa terv megfelel-e a szervezeti igényeknek?

g) A kockázatfelmérési és elemzési eredmények, a maradványkockázatok milyen további intézkedéseket igényelnek?

h) Megfelel a szervezet az aktuális jogszabályoknak? [90].

A felülvizsgálatok rendjét tervezni szükséges. Az auditok során biztosítani kell az auditálási folyamat tárgyilagosságát és pártatlanságát. A vezetésnek rendszeresen ellenőriznie kell az informatikai biztonságot.

Az ellenőrzés formái

Minden esetben elvárás, hogy az ellenőrzéshez felhasznált módszer biztosítsa a vizsgálat tárgyszerűségét, valamint valósághű képet nyújtson az adott területről. A szervezet informatikai biztonságával kapcsolatos ellenőrzések a következő területekre terjedhetnek ki:

a) Az adott terület informatikai biztonsági vizsgálata (fenyegetettség mérése, védelmi képesség-elemzés és kockázatelemzés alkalmazásával).

b) Az előírt biztonsági követelmények érvényesülésének egy releváns módszer szerinti vizsgálata.

c) A szervezet informatikai biztonságának külső tanúsítása és minősítése (ilyen módszer lehet más eljárások mellett az ISO 27001 elvárásainak való, tanúsított megfelelés). [97]

Az ellenőrzések az alábbi forrásokat használják: az informatikai eszközök napló állományainak elemzése, meghatározott szempontok szerinti információ bekérés, személyes ellenőrzés,

megfigyelés, különböző eszközökkel elvégzett sebezhetőség-vizsgálatok, a szervezet informatikai biztonsággal kapcsolatos dokumentumainak vizsgálata, folyamat elemzés, behatolási tesztek végrehajtása. [134]

A vezetés az ellenőrzések tapasztalatai alapján hozza meg döntését arról, milyen változtatásokra van szükség az informatikai biztonságot illetően. A helyzet függvényében szükség lehet az addig alkalmazott biztonsági szabályok, eljárások, valamint az addig az informatikai támogatás kapcsán használt technikai intézkedések kibővítésére, tökéletesítése. Fontos, hogy a szervezet vezetése a megfelelő és pontos vizsgálati adatokkal rendelkezzen, és a helyzetnek megfelelően értékelje azokat.

Az ellenőrzések hatékonyságához szükségesek az alábbi információk:

a) A biztonságos működés megvalósulásával kapcsolatos ellenőrzések pontos eredményei.

b) Amennyiben elérhető, partneri visszajelzések.

c) A bevezetett védelmi intézkedések megnevezései és a hatékonyságukat leíró fokmérők.

d) Nem kezelt kockázatokkal kapcsolatos információk.

e) Nem kezelt sebezhetőségek és releváns fenyegetések listája.

f) Automatikus mérési és ellenőrzési eszközök eredményei.

g) Korábbi informatikai biztonsági intézkedésekkel kapcsolatos dokumentációk [102].

Az adott szervezet vezetése a fenti adatok ismeretében képes értékelni az informatikai biztonság már meglévő szintjét. Amennyiben szükségesnek találják, további fejlesztésekkel kapcsolatos döntések meghozatalára kerülhet sor. A szervezeti informatikai biztonságpolitika megvalósulását ajánlatos időközönként külső szakemberrel is felülvizsgáltatni. Egy külső szem számára olyan dolgok is feltűnhetnek, amelyek fölött a szervezet szakemberei átsiklottak.

Az ellenőrzésekkel kapcsolatos alapvető elvárás, hogy azok folyamatai a formájuktól függetlenül úgy menjenek végbe maximális hatékonysággal, hogy az informatikai biztonságot ne zavarják meg. Az ellenőrzések során ugyancsak óvni kell a különböző ellenőrző és mérőeszközök sértetlenségét. Az ezekkel az eszközökkel való esetleges visszaélések

lehetőségét is ki kell zárni, például nyilvántartás-vezetéssel, vagy a biztonsági napló állományok védelembe helyezésével.

Az informatikai támogatás biztonságának ellenőrzése folyamatos tevékenység. A feladat ellátására napi rendszerességű feladatokat tartalmazó ellenőrzési tervet kell készíteni. Napi szinten kell ellenőrizni a fenyegetettségeket és sérülékenységeket, a védelem általános állapotát. Ha valamilyen rendellenességet találnak az ellenőrzés során, akkor annak a körülményeit ki kell vizsgálni. A rendszereszközök által készített naplókat statisztikai technikák használatával kell ellenőrizni. Statisztikai módszerekkel kiszűrhetők a trendváltozások, és érzékelhetők az ismétlődő események. A napi rendszerességű ellenőrzés szervezéséhez szükséges a biztonsági műveleti eljárások dokumentálása.

Az ellenőrzések kapcsán feltárt hiányosságok kiküszöbölése szervezeti beavatkozást igényel. Ezek a beavatkozások az úgynevezett helyesbítő intézkedéseknek. A helyesbítő intézkedéseket a feltárt kockázatok értékelése után kell meghozni. Csakúgy, mint ahogy az alap kockázatértékelésnél történt, itt is dokumentálandó a döntés. Amennyiben a szervezet a korrekció mellett dönt, a korrekció dokumentálása is szükséges. A bevezetett változással kapcsolatban ellenőrizni szükséges, hogy megfelel-e a módosítás a vele szemben megfogalmazott elvárásoknak. Amennyiben nem, további módosításra van szükség. A működés közbeni korrekciókat csakúgy, mint az alap kockázatkezelési intézkedéseket, érdemes fontosságuk szerint rangsorolni [90].

Mérés

Az IBIR bevezetésével együtt egy mérési rendszert is ki kell alakítani. Erre a rendszerre támaszkodva tudja értékelni a szervezet, hogy mennyire voltak hatékonyak a bevezetett védelmi intézkedések. A rendszer megismételhető folyamatokra és egymással összevethető mérőszámokra kell épüljön. Amit nem mér a szervezet, azoknak a jellemzőknek a változását nem tudja megfigyelni, értékelni és ezeknek az információk hiányában a szakemberek nem tudják mikor kell a biztonsági célok megvalósulása érdekében beavatkozniuk. {Calder, 2008 #46}

Lehetséges mérési területek az informatikai rendszer biztonságával kapcsolatban:

a) A beérkezett felhasználói panaszok mennyisége.

b) Az informatikai támogatással kapcsolatban bekövetkezett meghibásodások mennyisége.

c) A rögzített biztonsági események száma.

d) Az informatikai rendszer rendelkezésre állásának arányszáma.

e) Az informatikai rendszer üzemeltetését ellátók válaszideje a felhasználói megkeresésekre.

Az informatikai biztonságirányítási rendszer működésével kapcsolatban mérhetők az alábbi jellemzők:

a. Az elvégzett korrekciós intézkedések száma.

b. A védelmi intézkedésekkel kapcsolatos dokumentációkban meghatározott határidők betartási aránya.

c. A rendszer védelmi intézkedéseinek a száma.

d. Az informatikai támogatás kritikus területeinek száma.

e. Külső szolgáltatások igénybevétele esetén (például Internet hozzáférés, hardver karbantartás) a szerződött szolgáltatási szinteknek való megfelelés aránya.

f. A biztonsági szabályok megsértésének mennyisége. [98]

M9. melléklet – Az informatikai biztonságirányítás szerepe és működtetése

Az informatikai biztonságirányítás szerepét és a kritikus infrastruktúrák védelmében betöltött funkcióit a 2.3. fejezet részletesen tárgyalja. Jelen melléklet ennek technikai és módszertani kiegészítése: összefoglalja az informatikai biztonságirányítási rendszer (IBIR) kialakításának fő szervezeti és szabályozási lépéseit, valamint bemutatja azokat a mérőszámokat és ellenőrzési mechanizmusokat, amelyek a rendszer működésének folyamatos nyomon követését lehetővé teszik.

A melléklet első része az IBIR bevezetéséhez kapcsolódó szabályzati és dokumentációs elemeket rendszerezi (Informatikai Biztonsági Szabályzat, felhasználói szabályzat, kapcsolódó belső szabályzatok). Ezt követően áttekinti azokat a mérési és monitoringmegoldásokat, amelyek a 2.3. fejezetben bemutatott irányítási keret gyakorlati alkalmazását támogatják, ideértve a biztonsági események rögzítését, a válaszidők mérését, a szolgáltatási szintek ellenőrzését és a korrekciós intézkedések visszacsatolását.

A kiépítés lépései

A kibertámadások gyakoriságának és súlyosságának elemzése kritikus lépés az IT biztonságirányítási rendszerek fejlesztéséhez, amelyek nemcsak a törvényi előírásoknak való megfelelést, hanem az intézmények proaktív védelmét is szolgálják. A következőkben az IBIR kiépítésének lépéseit fogom részletezni, különös tekintettel arra, hogy az ilyen rendszerek hogyan tudják megóvni az információs infrastruktúrát és elősegíteni a gyors reagálást bármely jövőbeni kiberfenyegetés esetén.

Az első lépés annak megállapítása, hogy milyen az adott szervezet kiindulási biztonsági helyzete. Bár rendszer szinten esetleg nem teljeskörű a védelem, bizonyos védelmi mechanizmusok biztosan működnek már [90]. A felmérés során szerzett átfogó kép lehetővé teszi a védelmet tervező szakemberek számára, hogy pontosan megismerjék az adott időpontban fennálló információbiztonsági helyzetet.. Az illetékes szakember felmérve a védendő informatikai támogatást, pontos rálátást kap azokra a területekre, amelyek megfelelően védettek és szabályozottak, valamint azokra is, ahol ez a védelem nem éri el a kívánt szintet, vagy esetleg még hiányzik [96].

Kockázatelemzés

A kockázatelemzés célja az, hogy az informatikai támogatáson belül feltárt sérülékenységek és az informatikai támogatás rendeltetésszerű használatát fenyegető tényezők közötti

kapcsolatokat felderítsék. Az egyes rendkívüli események bekövetkezésének a valószínűségét is meg kell határozni. A szervezet által vállalható és nem-vállalható kockázatok meghatározása is szükséges[92]. Az ezzel kapcsolatos döntés a szervezet vezetőjének a felelőssége. Az informatikai biztonsággal foglalkozó szakemberek terjesztik a vezető elé a döntéshez szükséges információkat.

A szervezet informatikai rendszerével kapcsolatos kockázatok menedzsmentjét az alábbiak nehezítik [92]:

a) Nem ismerhető előzetesen az informatikai támogatás biztonságát fenyegető összes veszély, kockázat.

b) Az adott veszély tényleges bekövetkezési valószínűségét sem lehet pontosan előrejelezni.

c) A veszély hatására keletkező kár pontos mértéke sem ismerhető meg előzetesen.

A fentiek miatt sok esetben csak valószínűsítésekkel, becslésekkel lehet dolgozni. A munka végzése során az alábbi feladatokat kell végrehajtani:

a) össze kell állítani a rendszerrel kapcsolatos veszélyforrások listáját,

b) meg kell határozni az egyes kockázatokkal kapcsolatban használható valószínűségi kategóriákat,

c) meg kell határozni az egyes kockázatokhoz köthető (becsült) kárérték kategóriákat [39].

Az adott informatikai támogatással kapcsolatos kockázatok elemzése során leggyakrabban feltett kérdések az alábbiak:

a) Mely sérülékenységek miatt következik be a probléma?

b) Az adott rendkívüli esemény az informatikai támogatás, az információvagyon mely elemeit veszélyezteti?

c) A bizalmasság, sértetlenség, rendelkezésre állás területén hogyan hat az adott esemény?

d) Milyen valószínűséggel következik be az adott rendkívüli esemény?

e) Az egyes rendszerelemeket tekintve a lehetséges rendkívüli események közül melyik esemény bekövetkezésének a legnagyobb a valószínűsége?

A rendkívüli események gyakran összetett hatásláncok kiváltói. A rendkívüli események hatásainak feltérképezésére használható többek között a hibafa elemzés (angol nevén Fault Tree

Analysis - FTA) néven ismert hiba hatásokat feltáró elemzési módszer [93]. Az elemzés az alapvető hiba felől kiindulva halad a hibával kapcsolatos jelenségek felé.

A hibafa elemzési technikát, amely az egyik legáltalánosabban alkalmazott módszer a kockázatértékelés és megbízhatóság területén, először a Bell Telephone Laboratories alkalmazta 1962-ben a Minuteman rakétaindító rendszer biztonsági értékelése során. Ezt a módszert később a Boeing továbbfejlesztette, és integrálta a minőségi és mennyiségi hibafaelemzések támogatására szolgáló számítógépes programokba.

A hibafaelemzés különösen jelentős szerepet játszott a bonyolult mérnöki rendszerek megbízhatóságának kiértékelésében, és nagy sikereket ért el a nukleáris erőművek biztonsági rendszereinek fejlesztésében. Az amerikai Atomenergia Bizottság 1974-es WASH-1400 jelentése is tanúsítja, hogy ezt a technikát rendkívül hatékonyan alkalmazták a nukleáris biztonság területén, ahol a rendszerek biztonságos működésének biztosítása kritikus fontosságú volt [135].

A hibafaelemzés mára elengedhetetlen eszközzé vált a megbízhatósági és kockázatelemzési gyakorlatokban, amelyeket széles körben alkalmaznak a mérnöki rendszerek biztonságának növelése érdekében.

Az elemzési eljárás alapját egy fa típusú irányított gráf elkészítése jelenti. Ha közvetlenül nem képes az adott szervezet elhárítani, megelőzni egy eseményt, akkor logikai módszerekkel egyszerűbb jelenségekre, a szervezet hatáskörében álló eseményekre vezetheti azt vissza. Az egyes hatások közötti kapcsolatok ábrázolására logikai (ÉS, VAGY, NEM stb.) típusú operátorokat használnak. A hibafában csak azoknak az eseményeknek van helyük, amelyek az informatikai rendszer megfelelő működésére veszélyeztető hatással vannak. A hibafa csúcsán a nem kívánt jelenségek sorozatát kiváltó rendkívüli esemény szerepel. [95]

A hibafa készítést alapul vevő kockázatelemzési módszer egyes lépései az alábbiak:

a) Az informatikai támogatás biztonságához tartozó alapvető alrendszerek meghatározása és egymástól való elválasztása.

b) Az informatikai támogatás adott alrendszeréhez kapcsolódó feladatoknak és az alrendszerrel szembeni követelményeknek a vizsgálata.

c) Az adott alrendszerrel kapcsolatos nem kívánt, de lehetséges rendkívüli események számbavétele, meghatározása.

d) A lehetséges hibák közötti logikai kapcsolatok feltárása, a kapcsolatok megjelenítése a hibafán.

e) Az elemzés során kapott eredmények értékelése, a szükséges számítások elvégzése [39].

Amennyiben a veszélyekkel kapcsolatos mérőszámok használata nélkül akarják a szakemberek a szükséges elemzéseket elvégezni, akkor a hibafák ágain végighaladva az úgynevezett minimális kritikus láncokat kell megkeresni. Ezzel azokat a kapcsolatokat tárják fel, ahol a lehető legkevesebb számú meghibásodás vezet el egy nemkívánt eseményhez. Ezeken a leggyengébb pontokon szükséges a változtatás. A hibafán feltárt kapcsolatoknak mennyiségi alapon elvégzett kiértékelésénél a rendszerelemekre vonatkozó egyes megbízhatósági mérőszámokra alapozva kiszámítható a fő esemény bekövetkezési valószínűsége. [136]

A hibafa létrehozásakor az egyes alkotóelemek meghibásodásai három osztályba sorolhatók; van elsődleges, másodlagos és kezelési hiba.

Elsődleges hibát jelent az olyan meghibásodási típus, amely az előírtnak megfelelő működési körülmények között lép fel. A hiba mögött ilyenkor például az informatikai támogatás adott elemének nem megfelelő beállítása állhat. Másodlagos hibák azok, amelyek a külső feltételek előre nem látható romlása miatt jönnek létre. Ilyenek lehetnek például egy csőtörés, vagy tűz által okozott problémák. Kezelési hibákat eredményez az informatikai támogatás nem szabályszerű használata.

A hibafa elkészítésekor általában több szinten kapcsolódnak egymáshoz az abban ábrázolt jelenségek. A legfelső szinten az úgynevezett csúcsesemény áll. Ehhez az eseményhez kapcsolódnak a mögöttes hibajelenségek, amik alatt akár más hibajelenségek is lehetnek. A hibajelenségek láncolata mögött a hibafa alján lévő alapesemény található. A hibafa használatával az informatikai támogatás elemei közötti kapcsolat jól értelmezhető.

Az eseményfa elemzés (Event Tree Analysis – ETA) során az informatikai rendszer működésére hatással lévő események egymásra gyakorolt hatását követik végig. Ebbe a kategóriába a normál események is beletartoznak. Normál, tervezett események is okozhatnak olykor biztonsági problémát.

Az eseményfa a hibafához hasonló felépítésű. Ennek a fának a kiindulási esemény az alappontja. Az eseményfa ágai a kiindulási esemény lehetséges hatásai szerint bomlanak ki. Amennyiben az eseményláncolat végső kimenete valamilyen formában veszélyt jelent, akkor

az informatikai támogatás biztonságos működésének fenntartásához valamilyen intézkedés szükséges. Az eseményfa elemzésnek szintén van minőségi és mennyiségi módja. Az adott rendszeren belüli kölcsönhatások vizsgálatához jól használható az eseményfa elemzés. Előállhat olyan helyzet is, ahol az eseményfa kezdeti eseménye a hibafa csúcseseménye. [137]

A kockázatok, hibák kiértékelésének egy másik módja a bekövetkezési valószínűségek, gyakoriságok és a lehetséges károk számítása.

A rendkívüli események előfordulási gyakoriságának meghatározásához forrásként felhasználhat a szervezet különböző releváns statisztikákat. A legjobb azonban, ha vannak saját korábbi adatai. Amennyiben nincs ilyen, hasonló működési területeken tevékenykedő szervezetek információira is lehet alapozni. A lehetséges rendkívüli események valószínűsége és az elszenvedhető kár mértéke alapján minden egyes rendkívüli eseményt értékelni kell, és a vezetőnek döntenie kell arról, hogy tesz-e ellenintézkedéseket az adott esemény megelőzésére, vagy inkább a helyreállításra összpontosít.

Egy lehetséges módszer az elemzésre a veszélyforrások és fenyegetettségek táblázatba rendezése. A későbbi könnyebb azonosíthatóság érdekében a fenyegetettségeket érdemes csoportosítani. Például legyen az SZ a személyi jellegű fenyegetettség kódja, így az SZ1 az első személyi jellegű fenyegetettség. Szükséges továbbá a veszélyforrás megnevezése, a bekövetkezés valószínűségének megnevezése, a kár típusának meghatározása a CIA (Confidentiality, Integrity, and Availability) rendszer alapján, és a konkrét védelmi intézkedések megnevezése [45]. A lehetséges veszélyforrások listázásának módját a 23. táblázat mutatja. A kitöltési minta a szöveg korábbi, az elemzési módszereket bemutató részein alapszik, különös tekintettel a kiberbiztonsági események elemzésére vonatkozó módszertanokra. Ez alapján létrehozható egy strukturált és részletesebb táblázat, amely konkrétabb információkat nyújt a lehetséges fenyegetésekre.

Típus	**Veszélyforrás**	**Bekövetkezés valószínűsége**	**Támadási potenciál**	**Kár típusa**	**Kár érték**	**Védelmi intézkedés**
SZ1	Social engineering (például adathalászat)	Magas	Közepes	Bizalmasság megsértése, adatszivárgás	Magas (személyes adatok ellopása)	Többlépcsős hitelesítés, rendszeres alkalmazotti képzés
SZ2	Ransomware támadás	Közepes	Magas	Szolgáltatás-kiesés, adatvesztés	Nagyon magas (üzemleállás, pénzügyi veszteség)	Adatmentés, behatolásmegelőző rendszerek, rendszeres frissítések

SZ3	Insider threat (belső fenyegetés)	Alacsony	Magas	Bizalmasság, sértetlenség, rendelkezésre állás megsértése	Közepes (érzékeny információk manipulálása)	Hozzáférés-szabályozás, naplózás, belső auditok
SZ4	DDoS támadás	Közepes	Közepes	Szolgáltatás-kiesés	Magas (szolgáltatás elérhetetlensége)	Túlterhelés elleni védelem, felhőalapú skálázhatóság
SZ5	Malware (rosszindulatú szoftver)	Magas	Közepes	Adatvesztés, rendszerleállás	Nagyon magas (üzleti működés leállása)	Víruskeresők, rendszeres biztonsági frissítések
SZ6	Adatszivárgás (Data breach)	Közepes	Magas	Bizalmasság megsértése, adatvesztés	Nagyon magas (személyes és üzleti adatok ellopása)	Titkosítás, hozzáférés-kezelés, adatvédelmi irányelvek

Táblázat 7 - Egyénileg meghatározott dimenziók mentén és egyedi értékelések elvégzését követően előálló kiberbiztonsági elemzési mátrix minta

A bekövetkezési valószínűségeken túl a kockázatelemzéshez hozzátartozik még az egyes sérülékenységekhez tartozó támadási potenciálok meghatározása. Az adott sérülékenység kihasználásához szükséges támadói felkészültségi szint nagysága mellett azt kell ilyenkor megállapítani, milyen haszna lehet a támadónak ilyen műveletből.

A sérülékenységek lehetséges csoportosítása:

a) Automatizált eszközökkel kihasználható sérülékenységek: Az ilyen típusú sebezhetőségek esetében a támadó minimális technikai ismeretekkel rendelkezhet, mivel a kihasználást automatizált rendszerek végzik el.

b) Átlagos felhasználói ismereteket igénylő sérülékenységek: Ezek a sérülékenységek olyan szintű technikai tudással rendelkező felhasználók által is kihasználhatók, akik nem rendelkeznek speciális képzéssel vagy háttértudással.

c) Szakmai útmutatás mellett kihasználható sérülékenységek: Az ilyen típusú sebezhetőségek átlagos technikai ismeretekkel rendelkező felhasználók számára is elérhetők, amennyiben az adott területen megfelelő iránymutatást vagy támogatást kapnak.

d) Programozói ismereteket igénylő sérülékenységek: A sérülékenységek kihasználásához kifejezetten programozási készségek szükségesek, amelyek előfeltételezik a támadó technikai hozzáértését.

e) Magasan képzett támadókat igénylő sérülékenységek: Az ilyen típusú sérülékenységek kihasználása magas szintű szaktudást, mély technikai ismereteket és jelentős erőforrásokat igényel.

Az első két kategória gyakran magában foglalja az egyszerű felhasználói hibákból eredő problémákat is. Például komoly következményekkel járhat, ha egy felhasználó véletlenül töröl kritikus dokumentumokat vagy adatokat, ami ugyan sérülékenység szempontjából alacsony technikai kihasználhatóságot igényel, de jelentős károkat okozhat a szervezet számára.

A bekövetkezési valószínűség és kockázati kategóriák egy lehetséges csoportosítását a következő táblázat mutatja (P: Potencial, S: Small, Average: átlagos, Large: nagy, Very: nagyon)

Jelölés	**Bekövetkezési Valószínűség (angol)**	**Bekövetkezési Valószínűség**	**Kockázati Potenciál**
PVS	Very Small	nagyon kicsi	Ritka az előfordulás esélye, hozzávetőlegesen évtizedes időtávban következhet be egy ilyen esemény.
PS	Small	kicsi	5-10 évente van esély ilyen esemény bekövetkeztére, vagy csak professzionális felkészültségű támadó használhatja ki a gyengeséget, idézhet elő ilyen eseményt.
PA	Average	közepes	Egy-két éves távlatban esélyes a bekövetkezése, vagy átlagos felkészültségű informatikai szakember által kihasználható gyengeség.
PL	Large	nagy	Legrosszabb esetben éves gyakorisággal lehet ilyen eseményre számítani, átlagos felkészültségű szakember tud ilyen eseményt okozni.
PVL	Very Large	nagyon nagy	Egy éven belül többször is felléphet egy ilyen esemény, bárki okozhat ilyet.

Táblázat 8 - Példa valószínűség és kockázati potenciál kategóriákra

A kár mértékének egy lehetséges meghatározását az alábbi táblázat mutatja[45] .

Jelölés	Kár mértéke (angol)	Kár mértéke	Káresemény jellemzői
DVS	Very Small	elhanyagolható	Elsődleges eredetű károk a jellemzők, a károk összege kicsi.
DS	Small	kicsi	Az elsődleges károk mellett másodlagos, nagyobb összegű károk is keletkeznek.
DA	Average	közepes	Fennakadások keletkeznek a felhasználói rendszerekben, könnyeb személyi sérülések is előfordulhatnak.
DL	Large	nagy	Az üzleti/ügyviteli folyamatok működésében komoly zavarok keletkeznek. Súlyos emberi sérülések is lehetségesek.
DVL	Very Large	nagyon nagy	Az adott szervezet üzletmenete az esemény miatt időlegesen megbénul. Az ügyfélkörben bizalomvesztést okozhat az esemény, haláleset is lehetséges.
DD	Disaster	katasztrofális	A folyamatos üzletmenet hosszabb ideig megszakadhat, a szervezettel szemben bizalomvesztés lép fel, komoly társadalmi hatású probléma.

Táblázat 9 - Példa a kárértékek kategorizálására

A kockázatkezelési folyamat során nemcsak a veszélyforrások, a bekövetkezés valószínűsége, vagy a támadási potenciál értékelése szükséges, hanem az eredményt jelentő tényezők figyelembevétele is elengedhetetlen. Az eredmény-alapú kockázatértékelés azt vizsgálja, hogy egy adott incidens milyen konkrét hatást gyakorolhat az érintett rendszerre, szervezeti működésre vagy az üzleti folyamatokra. Például, ha egy ipari SCADA rendszer ellen irányuló támadás következtében leáll a termelés, az napi 50 millió forintnak megfelelő veszteséget generálhat. Ez a közvetlen anyagi kár mellett további bizalmi válságot idézhet elő az ügyfelek és partnerek körében.

Egy ilyen helyzet kezelésére az optimális megoldás a proaktív védelmi intézkedések alkalmazása, például rendszeres sérülékenység-elemzés és folyamatos monitoring bevezetése.

Az eredmény-alapú megközelítés segíti a szervezeteket abban, hogy az erőforrásokat a legkritikusabb kockázatokra összpontosítsák, minimalizálva a károk hosszú távú hatásait. A kárértékek és a bekövetkezési valószínűség kombinációjából adódó eredmények grafikus ábrázolása (például kockázati mátrixok segítségével) szintén jelentős segítséget nyújthat a döntéshozatal során.

Kockázatkezelési intézkedések

Egy további lehetőség a megállapított kockázatok áthárítása [138] (p.297). Ennek az áthárításnak módja lehet például az, ha a hardver eszközökre biztosítást köt a szervezet. Másik lehetőség a különböző intézkedések segítségével a bekövetkezés valószínűségét, illetve a lehetséges károk mértékét minimalizálni lehet. Bármilyen kockázatkezelési stratégiát is válasszon egy szervezet, az egyes konkrét kockázatok kezelésével kapcsolatosan az alábbi tevékenységeket kell elvégezniük:

a) Meg kell határozni minden egyes konkrét kockázatot, és jóvá kell hagyni az adott szervezet számára még elfogadható kockázati szint mértéket.

b) Az egyes kockázatok kezelésére szolgáló kontrollokat definiálni kell.

c) Be kell bevezetni olyan eljárásokat, amelyek az adott intézményt érintő kockázatokkal kapcsolatosak és megfelelnek a kockázati szint mértéknek.

d) Tudatosítani kell, hogy a védelmi intézkedések nem nyújtanak teljes körű biztonságot. Továbbra is megmaradnak bizonyos kockázatok. Ezeket a fennmaradó kockázatokat maradványkockázatoknak nevezik. A maradványkockázatok a szervezet számára még elfogadható gyakorisági és kárérték szintjét a vezetésnek kell jóváhagynia.

Az egyes kockázatok kezeléséhez jó kiindulási pontot ad az ISO 27001-es szabvány "A" melléklete. Különös figyelmet érdemlő a magyar jogszabályi környezetben a Miniszterelnöki Kabinetirodát vezető miniszter 7/2024. (VI. 24.) MK rendelete [139], amely a biztonsági osztályba sorolás követelményeit, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedéseket részletezi. Ez a rendelet az ISO 27001 általános útmutatásait kiegészíti, helyenként azoknál specifikusabb és részletesebb elvárásokat fogalmaz meg, különösen az állami és önkormányzati intézmények elektronikus információbiztonságára vonatkozóan. A rendelet nem csupán a nemzetközi szabványokkal való összhangot biztosítja, hanem a hazai kritikus infrastruktúrák sajátos védelmi követelményeihez is igazodik, így a szervezeti kockázatkezelés során gyakorlati alkalmazása erősen javasolt.

A szervezetvezetés döntése alapján vannak kockázatok, amelyek az adott intézmény számára nem elviselhetők. Ezeknek a kockázatoknak a csökkentésére védelmi intézkedéseket kell foganatosítani. Az egyes védelmi intézkedések kidolgozásához kapcsolódóan az alábbi tevékenységeket szükséges elvégezni [102]:

a) Meghatározni a bevezetni tervezett védelmi intézkedés célját.

b) Kijelölni az adott intézkedés végrehajtásért, működtetéséért felelős személyek körét.

c) Meghatározni, hogy ki felel az intézkedéssel kapcsolatos ellenőrzésekért.

d) Dokumentumba foglalni a tényleges védelmi intézkedést, megszabva az elvégzendő beállításokat, eljárásokat, az azok végrehajtásához szükséges eszköz és idő igényt.

e) Megbecsülni az adott intézkedés költségét. (Az adatok biztonságos tárolásához például szerver, vagy biztonsági mentést készítő eszköz beszerzése is szükséges lehet.)

f) A tervezet védelmi intézkedések fontossági sorrendbe állítása (ajánlott).

A védelmi intézkedések fontossági sorrendje akkor fontos, ha a védelem megtervezése után a konkrét védelmi rendszer elemeinek bevezetésére is sor kerül. A bevezetés folyamán az informatikai rendszer biztonságát szavatoló intézkedések költségvonzatára is figyelni kell. A nagyobb valószínűséggel problémát okozó fenyegetések és az érintett vagyonelemek kárértékei szolgálhatnak kiindulási alapként a bevezetési sorrend meghatározásához. [102]

Az adott szervezet által bevezetett védelmi intézkedések az általuk betöltött funkciók alapján az alábbi módon csoportosíthatók:

a) A kockázatok megelőzését (prevenciót) szolgáló intézkedések ideális esetben megakadályozzák, kevésbé szerencsés helyzetben csökkentik egy adott kockázattal kapcsolatos nemkívánatos események bekövetkezési valószínűségét. Ilyen megelőző intézkedések lehetnek többek között a minimum elv alapján kiosztott felhasználói jogosultságok, a vírus és tartalomszűrés beállítása.

b) A rendkívüli esemény, probléma érzékelésére szolgáló intézkedések során a cél, hogy minél hamarabb észleljék az informatikai rendszer számára káros hatással járó események bekövetkezését. Ilyen intézkedés lehet egy jogosulatlan hozzáférés kísérletének detektálása, a rendszeres naplózás, és a naplóesemények rendszeres átvizsgálása.

c) A hibajavító (korrektív) eljárások használatának a célja, hogy a már megtörtént rendkívüli események által okozott károkat csökkentsék. Amikor valamilyen nem kívánt esemény bekövetkezik, alapvető jelentőségű, hogy az esemény előtti, normál állapot minél hamarabb visszaálljon. Ebbe az eljárási csoportba tartoznak a biztonsági mentések és a rendszer visszaállítással kapcsolatos felkészülési tevékenységek.

Amennyiben a kezelendő sebezhetőségeket nem sikerül teljes egészében megszüntetniük a kockázatkezelés kapcsán bevezetett védelmi intézkedések, úgy azok az informatikai támogatást veszélyeztető új fenyegetéseket eredményezhetnek, ezekből pedig új kockázatok keletkezhetnek. Ezeknek a kockázatoknak az értékeléséről, kezeléséről a korábban ismertetett elvek alapján újabb döntés szükséges.

A kockázatkezelési eljárást egy alkalmazhatósági nyilatkozat zárja. Az alkalmazhatósági nyilatkozat kiindulási alap az IBIR ellenőrzésekor. Ez a nyilatkozat áttekintést ad az informatikai támogatás számára létrehozott védelemről. Az alkalmazhatósági nyilatkozatot a kockázatelemzési eljárás során definiált kockázati szintek felhasználásával érdemes elkészíteni [119]. Tartalmaznia kell a szervezet által kiválasztott szabályozási célokat, ellenőrzési módokat, valamint kiválasztásuk indoklását is. Ennek a dokumentumnak több fajtája is létezik, de ajánlatos az ISO 27001-es szabvány szerinti változatot használni. Az adott informatikai támogatással kapcsolatban megfogalmazott védelmi intézkedések tételes felsorolása mellett a nyilatkozat részét kell képezze az egyes intézkedések bevezetési helyeinek megnevezései, valamint a megfelelő szabályzatokra utaló hivatkozások. Ezt olyan pontossággal kell megadni, hogy az hivatkozott szabályzat beazonosítható, visszakereshető legyen. Az alkalmazhatósági nyilatkozat ily módon tájékoztató feladatot lát el. [131]

Kiberbiztonsági reagálás és kezelés

A kiberfenyegetések növekvő mértékű előfordulása miatt számos szervezet rendelkezik kiberbiztonsági stratégiával. A kutatások azonban azt mutatják, hogy a kiberbiztonsági stratégia önmagában nem elegendő [99]. A proaktív kiberbiztonsági stratégia a fenyegetések előrejelzésére és a fenyegetések bekövetkezése előtti lépésekre összpontosít. A kiberbiztonság proaktív megközelítését alkalmazó szervezetek csökkenthetik a kockázatokat és megelőzhetik a potenciális fenyegetéseket[100]. A proaktív megközelítés kiemelt jelentőségű a kiberbiztonsági támadások lehetséges gazdasági, társadalmi és pénzügyi következményei miatt.

A kiberbiztonság proaktív megközelítése számos előnnyel jár a szervezet számára. Kevésbé költséges, mint a reaktív [101]. A reaktív megközelítések a bekövetkezett fenyegetésre

összpontosító politikákat és rendszereket dolgoznak ki. A fenyegetések azonban így mindig új kihívást jelentenek egy szervezet számára, ami magasabb költségekhez vezethet, mint a proaktív megközelítés. Emellett a proaktív megközelítés segítségével a szervezetek mindig egy lépéssel a számítógépes támadók előtt járhatnak, és időben eligazíthatják biztonsági csapataikat, még mielőtt egy bekövetkező támadás zavart okozna. A proaktív megközelítés továbbá összehangolja a kiberbiztonságot a szervezet jövőképével, elősegíti a biztonságtudatos kultúrát, segíti a szervezetet abban, hogy túllépjen a megfelelőségen, és biztosítja, hogy befektessen a megelőzési, észlelési és reagálási fázisokba.

A kiberbiztonság proaktív megközelítését alkalmazó szervezetek csökkenthetik a kockázatokat és megelőzhetik a potenciális fenyegetéseket [100]. A proaktív megközelítés kiemelt jelentőségű a kiberbiztonsági támadások lehetséges gazdasági, társadalmi és pénzügyi következményei miatt.

A kiberbiztonság proaktív megközelítése számos előnnyel jár a szervezet számára. Kevésbé költséges, mint a reaktív [101]. A reaktív megközelítések a bekövetkezett fenyegetésre összpontosító politikákat és rendszereket dolgoznak ki. A fenyegetések azonban így mindig új kihívást jelentenek egy szervezet számára, ami magasabb költségekhez vezethet, mint a proaktív megközelítés. Emellett a proaktív megközelítés segítségével a szervezetek mindig egy lépéssel a számítógépes támadók előtt járhatnak, és időben eligazíthatják biztonsági csapataikat, még mielőtt egy bekövetkező támadás zavart okozna. A proaktív megközelítés továbbá összehangolja a kiberbiztonságot a szervezet jövőképével, elősegíti a biztonságtudatos kultúrát, segíti a szervezetet abban, hogy túllépjen a megfelelőségen, és biztosítja, hogy befektessen a megelőzési, észlelési és reagálási fázisokba. Ezenkívül a kibertámadások proaktív megközelítése kritikus fontosságú a hírnév és a bizalom

Incidens-reagálási tervek

A jól dokumentált reagálási terv kritikus fontosságú egy olyan korban, amikor a kibertámadások egyre kifinomultabbá és elterjedtebbé válnak. Az incidenskezelési terv felvázolja a biztonsági incidens bekövetkezésekor követendő folyamatokat. Az incidens-reagálási terv lehetővé teszi a szervezet számára, hogy gyorsan és hatékony válaszlépéseket tegyen válság idején, ahelyett, hogy akkor próbálná meg kitalálni, mit kell tennie. A kiberbiztonsági eseményekre való reagálásra vonatkozó megbízható protokollok kidolgozása létfontosságú a kiberbiztonsági események esetén szükséges gyors és hatékony fellépéshez. Az előfordulási reagálási terv megléte kritikus fontosságú kibertámadás esetén a károk

korlátozásához, és a helyreállítási idő és költségek csökkentéséhez. Megfelelő tervezés nélkül a szervezetek nehezebben fedezik fel a támadásokat, vagy lassabban a reagálnak, amely szükségtelen kiadásokhoz, produktív idő elvesztéséhez, hírnévkárosodáshoz és más jelentős veszteségekhez vezethet.

Az incidensekre való reagálás egyik legkritikusabb eleme egy jól kidolgozott incidensterv megléte. Az incidensterv meghatározza, hogy egy szervezet hogyan fog cselekedni, ha biztonsági fenyegetés lép fel. A hatékony fenyegetés- és incidenskezelési terv kidolgozása azonban gondos tervezést és számos tényező mérlegelését igényli [140]. A jól meghatározott incidensreagálási tervnek tömörnek, világosnak és könnyen végrehajthatónak kell lennie egy fenyegetési válság során. Emellett agilis incidenskezelési eljárások is elengedhetetlenek a egyre jobban fejlődő, modern, gyors tempót diktáló fenyegetési környezetben való sikeres védekezéshez. Következésképpen egy jó incidensreagálási tervnek körvonalaznia kell a reagáló csapat szerepét és felelősségét, egyértelmű iránymutatásokat kell adnia az incidensek azonosításához, beleértve az incidensek osztályozási rendszerét, körvonalaznia kell a vizsgálat és elemzés elvégzésének lépéseit, körvonalaznia kell az elszigetelés és felszámolás módozatát, meg kell határoznia a helyreállítási eljárásokat, részletes értesítési eljárásokat kell biztosítania, és el kell rendelnie az incidens utáni felülvizsgálatot.

Üzletmenet-folytonosság és katasztrófatervezés

Egy adott szervezet napi működése során azokat a kockázatokat amelyek bekövetkezését nem akadályozták meg az Informatikai Biztonságirányítási rendszer ellenintézkedései, incidensként kell tekinteni. Ez a kockázatkezelés azon útja, amikor a már bekövetkezett rendkívüli eseményre reagál a szervezet. A válasz célja, hogy az informatikai támogatás kiesését a lehető leghamarabb áthidalják, az üzletmenet folyamatossága helyreálljon. Az üzletmenet folytonosság tervezésekor a szervezet szintén a kockázatfelmérés és kockázatelemzés során kapott eredményeket használja fel. [97].

Az üzletmenet-folytonossági terv funkciója, hogy egy rendkívüli esemény bekövetkeztekor a létfontosságú üzleti folyamatok zavartalansága biztosítva legyen, illetve, hogy a normál üzletmenet mielőbb, minél kisebb költséggel visszaállítható legyen. A teljeskörű üzletmenet-folytonossági tervvel (BCP) a nehezen számszerűsíthető, nagy hatású kockázatok (például földrengés, terrortámadás) rendkívüli következményei is kivédhetők, tompíthatók egy szintig.

A szervezet üzletmenet-folytonossági terve tartalmazza azokat az információkat, amelyek felhasználásával az informatika támogatás folyamatainak kiesése, akadozása esetén annak

működését valamilyen szinten fenn lehet tartani. A tervben benne vannak a megelőző tevékenységekkel, helyettesítő, illetve visszaállító intézkedésekkel kapcsolatos feladatok. [141]. Az informatikai eszközök rendszeres, megelőző célú karbantartása például csökkenti bizonyos problémák felmerülésének kockázatát. A rendszeres karbantartás normál körülmények között is növeli az informatikai támogatás teljesítményét.

Az üzletmenet-folytonossági terv része a katasztrófa-elhárítással kapcsolatos tevékenységek tervezése is. Egy ilyen terv azt írja le, hogy valamely előre nem látott esemény bekövetkeztekor hogyan állítható vissza az informatikai támogatás normál menete. Az alapvető cél az, hogy a szervezet az informatikai támogatást érő katasztrófa esetén a lehető leghamarabb újra teljesen használatba tudja venni az informatikai támogatást. Az elsődleges feladat a kritikus üzleti funkciók helyreállítása, ezt követi a normál üzletmenethez való visszatérés. A katasztrófa terv részei az érintett eszközökre való hivatkozás, a kapcsolódó szolgáltatások megnevezése, az informatikai támogatás szerződéseinek adatai (szerződő felek és egyéb releváns adatok), illetve a terv alkalmazási körülményeinek részletes leírása, valamit az értesítési listák.

Dokumentálási kötelezettség

Általános elv, hogy a biztonságirányításhoz az alapos dokumentáció elengedhetetlen. Ez egyrészt az ellenőrzéseknél segít, másrészt, mivel a személyi állomány folyamatosan változik, az új dolgozók a dokumentáció segítségével ismerhetik meg munkájukkal kapcsolatos biztonsági előírásokat.

A következőket kell, hogy tartalmazza az Informatikai Biztonságirányítási Rendszer dokumentációja[120]:

a) Védelmi eljárások és intézkedések

b) Kockázatelemzési és kezelési követelmények

c) A kockázatelemzésnél alkalmazott módszerek

d) Rendkívüli eseményekkel kapcsolatos bizonyítékok rögzítésével kapcsolatos tevékenységek rendje.

A fentiekben felsoroltak között több olyan elem van, amelyek más dokumentációkban is szerepelnek. Hatékony, ha az egyes területekkel kapcsolatos eljárások leírását csak egyszer készíti el a szervezet, hogy amennyiben máshol is szükséges, ott elegendő legyen egy pontos

megnevezéssel hivatkozni rá. Éppen ezért fontos, hogy az egyes részterületekkel foglalkozó dokumentumoknak nagyon pontos elnevezése legyen. [132]

Biztonságpolitika

A biztonsági célú tevékenységekhez szükséges vezetői támogatást, az alapvető informatikai biztonsági célokat a szervezet biztonsági politikája nyilvánítja ki. A biztonságpolitikának összhangban kell lennie az adott szervezet egyéb céljaival, valamint a szükséges biztonsági szabályozásokkal. Minél fontosabb az informatikai támogatás szerepe az adott hely mindennapi életében, annál magasabb szintű biztonsági intézkedések szükségesek [90].

A biztonságpolitika csak a fő irányokat, feladatokat jelöli ki. Az informatikai biztonsági szabályzat, illetve a kapcsolódó dokumentumok szólnak részletesen az informatikai biztonsággal kapcsolatos intézkedésekről. A következő iránymutatások kell, hogy helyet kapjanak az informatikai biztonságpolitikában:

a) Annak a megnevezése, hogy mire terjed ki és mi a pontos célja.

b) Az informatikai biztonság fogalmának meghatározása a szervezet számára.

c) A vezetőség támogató szándéknyilatkozata.

d) Az informatikai biztonságpolitikát meghatározó szervezési elvek.

e) Az adott intézmény adatvagyonának értéke, a releváns védelmi szintek, valamint a szervezet biztonsági osztályozási rendszere.

f) Az informatikai biztonsági kockázatok felmérésére és kezelésére vonatkozó alapelvek.

g) A személyi kapcsolatok kezelési elve.

h) Az informatikai biztonsági ellenőrzés rendszerének alapjai.

i) Az informatikai biztonsági feladatok felosztásának elve.

j) A biztonságpolitika felülvizsgálatának rendje.

Az informatikai biztonságpolitikát kialakítását követően dokumentált módon meg kell ismertetni a szervezet alkalmazottaival.

A működést meghatározó biztonságpolitikára alapozva szükséges meghatározni az informatikai biztonság jövőképét, az informatikai biztonság stratégiáját. A biztonsági stratégiára alapozva készül el az éves szintű beszerzési, beruházási terv. Az információbiztonsággal kapcsolatos

stratégiát az információbiztonsági helyzet, a várható kihívások és a fejlesztési potenciálok alapján dolgozzák ki [102].

Informatikai Biztonsági Szabályzat és ahhoz kapcsolódó ellenőrzés mérés

Az Informatikai Biztonsági Szabályzat (IBSZ) képezi az intézmények informatikai biztonságának alapját, amely átfogóan rögzíti a működéshez szükséges biztonsági intézkedéseket, folyamatokat és a különböző munkakörökben dolgozók feladat-, felelősség- és hatásköreit. A szabályzathoz kapcsolódó dokumentumrendszer több szinten valósul meg: az irányítási dokumentumok a szervezeti ügymenet rendjét, a technikai szabályzatok az eszközhasználat részleteit, míg a Felhasználói Szabályzat az engedélyezett tevékenységeket és a rendkívüli események kezelését tartalmazza. Az emberi tényező kezelése kiemelt fontosságú, ezért a szervezetnek gondoskodnia kell a munkavállalók megfelelő képzéséről és biztonsági tudatosságának növeléséről, különös tekintettel a bizalmi munkakörökre, ahol előzetes biztonsági szűrés és titoktartási nyilatkozat szükséges.

Az IBIR hatékony működésének alapfeltétele a folyamatos ellenőrzés, amely az ISO 27001:2022 szabvány szerint rendszeres és szisztematikus kell legyen. Az ellenőrzések során vizsgálni kell a bevezetett előírások gyakorlati megvalósíthatóságát, az erőforrások elégségességét és az intézkedések módosításának szükségességét. A különböző ellenőrzési formák – fenyegetettség mérése, sebezhetőség-vizsgálatok, behatolási tesztek, külső tanúsítás – együttesen biztosítják az informatikai biztonság átfogó értékelését. A vezetés ezeknek az eredményeknek az alapján hoz döntéseket a szükséges változtatásokról, miközben biztosítani kell, hogy az ellenőrzések ne zavarják meg a rendszer működését.

Az IBIR mellett ki kell alakítani egy átfogó mérési rendszert is, amely megismételhető folyamatokra és összehasonlítható mérőszámokra épül. A mérési területek közé tartoznak a felhasználói panaszok, meghibásodások, biztonsági események száma, a rendszer rendelkezésre állása és az üzemeltetők válaszideje. Az IBIR működésének mérésekor figyelembe kell venni a korrekciós intézkedések számát, a határidők betartását és a védelmi intézkedések hatékonyságát. A mérési eredmények rendszeres értékelése lehetővé teszi a trendek azonosítását és a szükséges beavatkozások időben történő meghozatalát, így biztosítva az informatikai biztonságirányítási rendszer folyamatos fejlesztését és a szervezet védelmének magas szintjét.

Két konkrét, súlyos következménytípusa az incidenseknek a szolgáltatási fennakadásokat és a fizikai biztonsági kockázatokat előidéző támadások. A szolgáltatási fennakadások olyan kiberbiztonsági incidensek okozta rendszerleállások, amelyek jelentős fennakadásokat idézhetnek elő az energiaellátásban, közlekedési rendszerekben vagy más kritikus szolgáltatásokban. A fizikai biztonsági kockázatokat előidéző támadások olyan a SCADA és más irányítástechnikai rendszerek elleni támadások, melyek során fizikai veszélyhelyzetek keletkezhetnek, mint például robbanások vagy szivárgások.

A fentiekre válasz a kritikus infrastruktúrák kiemelt védelme, melynek elemei a szabványok és irányelvek. A kritikus infrastruktúrák védelméhez szükséges a nemzetközi és helyi szabványok, valamint a legjobb gyakorlatok alkalmazása előtérbe került, a biztonsági technológiák és eljárások kiemelt szerepet kaptak. A hatékony biztonsági megoldások, beleértve a támadások észlelését és megelőzését kulcsfontosságúak lettek a kritikus infrastruktúrák védelmében.

Incidensreagálási tervek és protokollok a kiberbiztonsági stratégiák sarokköveivé váltak, mivel ezek biztosítják a gyors és hatékony válaszadás lehetőségét a kiberbiztonsági incidensekre, így minimalizálva azok hatásait és erősítve a szervezet védelmi képességeit [126]. Az incidensreagálási tervek fő fészei:

Incidensfelismerés: A potenciális kiberbiztonsági incidensek azonosításának módszerei, beleértve a rendszeres monitoringot és az anomáliák észlelését.

Jelentéstétel és kommunikáció: Az incidensek jelentésére és az érintett felek tájékoztatásra kidolgozott eljárások, beleértve a vezetőség, és szükség szerint a hatóság, valamint a nyilvánosság tájékoztatását.

A válasz és kezelés: Az incidensre történő reagálás terve, beleértve a támadás izolálását, a károk minimalizálását és a rendszerek helyreállítását.

Az incidensreagálási folyamat során alkalmazott protokollok és eljárások:

Szerepek és felelősségek: Definiálni kell az egyes csapattagok funkcióit és elszámoltathatósági körüket.

Készenléti gyakorlatok: A reagálási képességek szinten tartása végett elengedhetetlenek a rendszeres veszélyhelyzet-szimulációk.

Dokumentáció és nyomonkövetés: Minden incidensre vonatkozóan részletes dokumentációt kell vezetni, beleértve a támadások természetét, és a válaszintézkedéseket.

Incidens utáni elemzés: A folyamatos fejlődés érdekében minden incidens okait és hatásait, részletekbemenően fel kell tárni.

A tanulságok levonása és intézkedések frissítése: A megállapítható konklúziók alapján frissíteni kell az incidensreagálási terveket és protokollokat, hogy azok hatékonyabban kezeljék a jövőbeli fenyegetéseket.

A képzés és tudatosság: Biztosítani kell a dolgozók folyamatos képzését és tudatosságnövelését a kiberbiztonsági fenyegetések és kiküszöbölésük érdekében.

Az incidensreagálási tervek és protokollok kritikus elemei a szervezetek kiberbiztonsági védelmének. A hatékony incidensreagálás képessége nem csak a támadások hatásainak csökkentésére szolgál, hanem erősíti a szervezet hírnevét és a bizalmat a partnerek és ügyfelek körében.

KÖSZÖNETNYILVÁNÍTÁS

Kiemelt köszönettel tartozom témavezetőmnek, Professzor Dr. Rajnai Zoltánnak, aki évek óta segíti szakmai tanácsaival a munkámat. Témavezetőként mindig rendelkezésemre állt a felmerülő kérdések megvitatására, figyelemmel kísérte kutatásomat, és tanácsaival átsegített a nehézségeken.

Köszönetemet szeretném kifejezni mindazoknak, akik az eddigi tanulmányaimat segítették. Elsősorban szeretném megköszönni családomnak, szüleimnek, feleségemnek, gyermekemnek a kitartó támogatásukat, a sok-sok odafigyelést, türelmet és áldozatvállalást.

Hálás vagyok Professzor Dr. Besenyő Jánosnak, aki nem sajnálta idejét, hogy segítsen eligazodnom a biztonságtudomány területén, és Professzor Dr. Berek Lajosnak, aki tanácsaival támogatta értekezésem teljességét.

Szeretném megköszönni az Óbudai Egyetem Biztonságtudományi Doktori Iskola minden tanárának és munkatársának, akik a doktori tanulmányaimat valamilyen formában segítették, támogatták.

Köszönöm orvosaimnak, Dr. Gyulai Ádámnak, Dr. Jakab Gábornak, és az Uzsoki Kórház minden dolgozójának.

Köszönettel tartozom azoknak a barátaimnak és munkatársaimnak is, akik biztattak, hogy elinduljak ezen az úton. Köszönöm Mádi-Nátor Anettnek és Frész Ferencnek, akik már a kutatás kezdetén, közvetlen feletteseimként támogatták tudományos ambícióimat.

Köszönöm mindazoknak is, akik a felsoroltakon kívül segítségükkel hozzájárultak e munkához.

Mindannyiuknak áldást, sok sikert, erőt és egészséget kívánok életükhöz, feladataikhoz!