DOI-azonosító: https://doi.org/10.53304/RT.2025.2.02

BEZERÉDI IMRE

A felhasználói viselkedéselemzés szerepe a kibertámadások megelőzésében: rendészeti kihívások és lehetőségek a digitális korban

Absztrakt

A tanulmány a kiberbiztonság növekvő fontosságát vizsgálja a felhasználói viselkedéselemzés (User Behavior Analytics, UBA) kontextusában, fókuszálva a rendészeti kihívásokra. A digitális technológiák fejlődése új kockázatokat teremt, ahol a humán tényező kulcsfontosságúvá válik a védelmi rendszerekben. A kutatás feltárja a felhasználói viselkedés és kiberbiztonság összefüggéseit, elemzi a kibertámadások evolúcióját és a mesterséges intelligencia alkalmazási lehetőségeit. Megállapítja, hogy az emberi tényező a kiberbiztonság leggyengébb láncszeme, ugyanakkor a gépi tanulás és a mesterséges intelligencia jelentősen növelheti a fenyegetésdetektálás hatékonyságát. Kiemeli a rendszeres képzések, tudatosságnövelő programok és interdiszciplináris együttműködés fontosságát. Végkövetkeztetése, hogy a felhasználói viselkedéselemzés integrálása paradigmaváltást indíthat el a kiberbűnözés elleni védekezésben.

Kulcsszavak: kiberbiztonság, felhasználói viselkedéselemzés, rendészeti kihívások, mesterséges intelligencia

Abstract

The study examines the growing importance of cybersecurity through user behavior analysis (UBA), focusing on law enforcement challenges. The rapid development of digital technologies creates new risks where the human factor becomes crucial in defense systems. The research explores the relationships between user behavior and cybersecurity, analyzing cyber attack evolution and artificial intelligence application possibilities. It concludes

that the human element remains the weakest link in cybersecurity, while machine learning and Artifical Intelligence can significantly enhance threat detection efficiency. The study emphasizes the importance of regular training, awareness programs, and interdisciplinary cooperation. Its key conclusion suggests that integrating user behavior analysis can initiate a paradigm shift in combating cybercrime, offering a holistic approach to digital security challenges.

Keywords: cybersecurity, user behavior analysis, law enforcement challenges, artificial intelligence

Bevezetés

A rendészeti szférában régóta bevett gyakorlat az anekdotikus bölcsesség alkalmazása a bűncselekmények és más jogsértések szemléltetésére. Az egyik ilyen klasszikus körzeti megbízottaktól származó megállapítás szerint *„addig nincs baj, amíg nem lopnak mozdonyt, malomkövet vagy parazsat."* Míg ez a mondás a nem mindennapi, viszont egyszerű megítélésű és látható bűncselekményekre vonatkozott, a mai világban a fenyegetések egyre inkább láthatatlanok és szofisztikáltak. A technológiai fejlődés és a digitális világ térnyerésével a modern kor mozdonyai, malomkövei és a parázs már nem fizikai tárgyak, hanem adatok, informatikai rendszerek és digitális infrastruktúrák formájában jelennek meg.

A kibertámadások megelőzésének egyre nagyobb szerepe van mind az állami, mind a magánszektor védelmében, ahol a rendészeti eszközök és megközelítések új kihívásokkal néznek szembe. A bűncselekmények elkövetői egyre kifinomultabb technikákat alkalmaznak, gyakran kihasználva a felhasználói szokásokat és rendszeres viselkedési mintákat, nem pedig az anomáliákat. A támadók jellemzően a napi rutinra építenek, például olyan forrásokról küldenek adathalász e-maileket, amelyekről a felhasználók rendszeresen kapnak üzeneteket, így növelve a sikeres megtévesztés esé-

lyét. Ebben az új környezetben a felhasználói viselkedéselemzés (User Behavior Analytics, UBA) kiemelt fontosságúvá vált a rendészeti és kiberbiztonsági szférában egyaránt. A viselkedési minták alapos feltérképezése és a megszokottól való eltérések azonosítása kulcsfontosságúvá vált a digitális fenyegetések korai felismerésében és kezelésében.

A tanulmány célja, hogy áttekintést nyújtson a felhasználói viselkedéselemzés rendészeti alkalmazásáról a kibertámadások megelőzésében, különös tekintettel a belső fenyegetések felismerésére és a szociális manipuláció (social engineering) elleni védekezésre. Az információbiztonsági monitoring és az anomáliák detektálása kritikus eszköz lehet a rendőrség és más bűnüldöző szervek számára, amelyeknek egyre inkább szükségük van az új technológiák és eljárások bevezetésére a hatékony kiberbiztonsági feladataik ellátása érdekében. A bűnüldöző szervek számára különös nehézséget jelent, hogy lépést tartsanak a folyamatosan változó kibertérben megjelenő új fenyegetésekkel, ezért a kiberbiztonság területén alkalmazott innovatív megoldások és módszerek fontos szerepet képviselnek a hatékony védekezés szempontjából. Ahogy a támadások egyre inkább az emberi tényezőre, vagyis a felhasználói hibákra építenek, úgy válik egyre fontosabbá a felhasználói viselkedés elemzése a védekezési stratégiákban. A humán tényező és a kiberbűnözés közötti összefüggések mélyebb megértése nemcsak a megelőzés szempontjából fontos, hanem a bűnüldözés hatékonyságát is növelheti a digitális bűncselekmények elleni küzdelemben. A kutatás kitér a felhasználói viselkedési minták elemzésére, a technológiai és oktatási stratégiák szerepére, valamint a mesterséges intelligencia (MI) és a gépi tanulás (ML) lehetőségeire a kiberbiztonsági rendszerekben.

A kutatás célja

A kiberbiztonság egyre növekvő fontossága és a digitális infrastruktúrák folyamatos térnyerése révén a felhasználói viselkedés elemzése központi kérdés a kibertámadások megelőzésében. A digitális technológiák gyors fejlődése és azok széleskörű alkalmazása következtében a felhasználói sze-

rep kulcsfontosságúvá vált a kiberbiztonság fenntartásában. Ahogy a támadások egyre inkább célzottá válnak, a humán tényező, különösen a felhasználói viselkedés és az emberi döntéshozatal, döntő szerepet játszik a szervezetek és egyének kitettségében a kibertámadásokkal szemben.[1]

A gyakorlati tapasztalatok azt mutatják, hogy egyetlen figyelmen kívül hagyott biztonsági figyelmeztetés vagy egy gyanús e-mail megnyitása is elegendő lehet ahhoz, hogy egy szervezet teljes informatikai infrastruktúrája kompromittálódjon.[2] A kiberbiztonság területén az egyik legígéretesebb kutatási irányvonal a felhasználói viselkedéselemzés alkalmazása. Az UBA-rendszerek folyamatosan monitorozzák és elemzik a felhasználói tevékenységeket, képesek azonosítani a normál viselkedési mintákat, majd detektálni az azoktól való eltéréseket. Ez a megközelítés különösen hatékony a belső fenyegetések azonosításában, ahol a jogosult felhasználók tevékenysége jelenthet biztonsági kockázatot.[3]

A felhasználói tudatosság fejlesztése kulcsfontosságú eleme a hatékony kibervédelemnek.[4] A rendszeres és megfelelően strukturált képzések szignifikánsan növelik a szervezetek biztonsági szintjét. A digitalizáció térnyerésével és a globális hálózatok bővülésével a kibertámadások egyre szofisztikáltabbá válnak, ami növekvő fenyegetést jelent mind az állami, mind a magánszektor számára. Ez összhangban van a nemzetközi kutatási eredményekkel is, amelyek hangsúlyozzák a humán tényező jelentőségét a kiberbiztonságban.[5]

---

[1] Aldawood, Hussain – Skinner, Geoffrey: Reviewing cyber security social engineering training and awareness programs – Pitfalls and ongoing issues. Future internet, 2019, 11 (3), 73. sz.

[2] Verizon: 2023 Data Breach Investigations Report.
Forrás: https://www.verizon.com/business/resources/reports/dbir/ Letöltés ideje: 2024. 09. 28.

[3] Leitold Ferenc: A felhasználói viselkedés, mint információbiztonsági kockázat becslése. Konferencia-menedzselő rendszer, networkshop. 2019. Forrás: https://doi.org/10.31915/NWS.2019.24

[4] IBM: Cost of a Data Breach Report 2024. Forrás: https://www.ibm.com/reports/data-breach Letöltés ideje: 2024. 09. 12.

[5] Safa, Nader Sohrabi – Von Solms, Rossouw – Furnell, Steven: Information security policy compliance model in organizations. computers & security. 2016/56. szám. 70-82. o.

A viselkedéselemzésre és a tudatos felhasználói magatartásra oktatás, valamint a megfelelő szervezeti szabályrendszerek megalkotása kulcsfontosságúak lesznek a jövőbeni kiberbiztonsági rendszerekben, különösen egy olyan világban, ahol a felhasználói szokások és minták megfigyelése egyre gyakrabban válik támadások kiindulópontjává. Az olyan biztonsági kockázatok, mint a ChatGPT és más MI alapú eszközök vállalati használata sokszor tiltva vannak, mivel ezeken keresztül bizalmas adatok szivároghatnak ki, amikor a felhasználói tartalmak a szolgáltatás részévé válnak. A felhasználói viselkedés és a kiberbiztonsági kockázatok közötti összefüggések mélyebb megértése elengedhetetlen a hatékony védelmi mechanizmusok kialakításához. A felhasználói figyelmetlenség, a tudatosság hiánya és a rutinszerű viselkedésminták jelentős szerepet játszanak a kibertámadások sikerességében, különösen a szociális manipulációval és belső fenyegetésekkel szemben.[6] Az emberi tényező kiemelt fontosságú a modern kibertámadásokban, ahol a támadók gyakran pszichológiai manipulációt alkalmaznak céljaik elérése érdekében.[7]

Az UBA és az MI alkalmazása hozzájárulhat a kibertámadások proaktív felismeréséhez és megelőzéséhez. Ezek a technológiák lehetővé teszik a normál felhasználói viselkedéstől való eltérések automatikus detektálását, ami kulcsfontosságú a potenciális fenyegetések korai szakaszban történő azonosításában.[8] A felhasználói tudatosság fejlesztésére irányuló programok hatékonyságának növelése érdekében fontos a képzési módszerek fo-

[6] Bányász Péter – Bóta Bettina – Csaba Zágon: A social engineering jelentette veszélyek napjainkban. In: Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében. Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat. Budapest, 2019. 12-37. o.

[7] Hadnagy, Christopher: Social engineering: The science of human hacking. John Wiley & Sons. 2018.

[8] Kumaraguru, Ponnurangam – Sheng, Steve – Acquisti, Alessandro – Cranor, Lorrie Faith – Hong, Jason: Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology (TOIT), 2010, 10.2: 1-31. o.

lyamatos fejlesztése és személyre szabása. Az interaktív és gyakorlatorientált megközelítések különösen hatékonynak bizonyultak a kiberbiztonsági ismeretek átadásában és a helyes viselkedésminták kialakításában.[9]

A kutatásom célja mindezek alapján:

1. Feltárni a felhasználói viselkedés és a kiberbiztonság közötti komplex összefüggéseket, különös tekintettel arra, hogy az emberi tényező miként válik kulcsfontosságúvá a kibertámadások megelőzésében és a szervezetek biztonságának fenntartásában.
2. Tanulmányozni a kibertámadások evolúcióját és növekvő szofisztikáltságát a digitalizáció és a globális hálózatok bővülésének kontextusában, rávilágítva arra, hogy ez milyen kihívásokat jelent mind az állami, mind a magánszektor számára a jövő kiberbiztonsági rendszereinek fejlesztésében.
3. Elemezni a User Behavior Analytics (UBA) rendszerek és az MI alkalmazásának lehetőségeit a kibervédelemben, vizsgálva, hogy ezek a technológiák hogyan járulhatnak hozzá a normál felhasználói viselkedéstől való eltérések automatikus detektálásához és a potenciális fenyegetések korai felismeréséhez.
4. Megvizsgálni a felhasználói tudatosság fejlesztésére irányuló programok hatékonyságát, valamint feltárni azokat a komplex stratégiákat, amelyek a felhasználók viselkedésének tudatos formálását célozzák, figyelembe véve, hogy a technológiai megoldások önmagukban nem elegendőek a kiberbiztonság fenntartásához.

Ezen kutatási célok átfogó keretet adnak a tanulmány témáinak és kérdéseinek, lehetővé téve a kiberbiztonság és a felhasználói viselkedés elemzésének mélyebb megértését. A kutatás célja, hogy hozzájáruljon a kiberbiztonsági stratégiák fejlesztéséhez és a potenciális fenyegetések elleni védekezés erősítéséhez, figyelembe véve az emberi tényezőt és a technológiai

[9] Bada, Maria – Sasse, Angela M. – Nurse, Jason RC: Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672, 2019.

innovációt egyaránt. A kutatás nemcsak a kiberbiztonsági fenyegetésekre adott válaszok kidolgozásában, hanem a biztonsági kultúra és tudatosság fejlesztésében is fontos szerepet játszik. A javasolt intézkedések és stratégiák integrálása segíthet a kiberbűnözés elleni küzdelem hatékonyságának növelésében, hozzájárulva egy biztonságosabb digitális ökoszisztéma kialakításához.

Irodalmi áttekintés

A felhasználói viselkedés elemzésének elméleti alapjai

A felhasználói viselkedés elemzése (UBA) egy viszonylag új és innovatív megközelítés a kiberbiztonság területén, amely az emberi tényezőre helyezi a hangsúlyt a technológiai biztonsági intézkedések mellett. Ez a módszer jelentős paradigmaváltást jelent a hagyományos kiberbiztonsági szemlélethez képest, amely korábban elsősorban technikai jellegű kihívásként kezelte a problémát, és főként az infrastruktúra, valamint az információk védelmére koncentrált a rosszindulatú programok, hálózati támadások és egyéb technikai fenyegetések ellen.[10]

Az elmúlt évtizedekben azonban egyre nyilvánvalóbbá vált, hogy a technikai védelem önmagában nem elégséges a komplex kiberbiztonsági kihívások kezelésére. A felhasználók hibái, figyelmetlensége, vagy akár szándékos károkozása olyan jelentős kockázati tényezőket jelentenek, amelyeket a hagyományos technológiai megoldások nem képesek megfelelően kezelni.[11] Ez a felismerés vezetett a felhasználói viselkedés, mint potenciális biztonsági fenyegetésforrás intenzívebb vizsgálatához a kiberbiztonsági kutatásokban. A felhasználói viselkedés elemzésének elméleti alapja azon a feltételezésen nyugszik, hogy a felhasználók tevékenységei –

[10] Muha Lajos – Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése. Nemzeti Közszolgálati Egyetem. Budapest, 2018.
[11] Verizon: 2023 Data Breach Investigations Report. Forrás: https://www.verizon.com/business/resources/reports/dbir/ Letöltés ideje: 2024. 09. 28.

legyenek azok normálisak vagy a megszokottól eltérőek – értékes információkat szolgáltatnak a potenciális fenyegetésekről és biztonsági problémákról.[12] Ez az elmélet szorosan kapcsolódik a viselkedési mintázatok felismerésének és elemzésének koncepciójához, amely a pszichológia és a kognitív tudományok területéről származik.[13] Az UBA-rendszerek elsődleges célja, hogy folyamatosan monitorozzák és elemezzék a felhasználói tevékenységeket, azonosítva azokat a viselkedési mintákat, amelyek eltérnek a megszokottól, és potenciálisan egy kibertámadás vagy biztonsági incidens előjelei lehetnek. Ez a megközelítés lehetővé teszi a proaktív védekezést, szemben a hagyományos, reaktív biztonsági intézkedésekkel.

Az UBA-rendszerek működésének elméleti alapja a normál viselkedési minták meghatározása és az ezektől való eltérések detektálása. Ez a folyamat magában foglalja a nagy mennyiségű felhasználói adat gyűjtését, elemzését és értelmezését, amihez fejlett adatelemzési és ML-algoritmusokat alkalmaznak.[14] Az anomália-detekció során ezek a rendszerek képesek azonosítani olyan subtle, azaz árnyalatnyi eltéréseket is, amelyek emberi elemzők számára észrevétlenek maradnának.[15] A felhasználói viselkedés elemzésének egyik kulcsfontosságú elméleti aspektusa a kontextuális információk figyelembevétele. A rendszerek nem csak izolált eseményeket vizsgálnak, hanem figyelembe veszik a felhasználó szerepkörét, munkakörét, szokásos tevékenységi mintáit és az adott szervezeti környezetet is. Ez az

[12] Bányász Péter – Bóta Bettina – Csaba Zágon: A social engineering jelentette veszélyek napjainkban. In: Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében. Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat. Budapest, 2019. 12-37. o.

[13] Kovács László – Krasznay Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. Nemzet és Biztonság–Biztonságpolitikai Szemle 10.1. 2017. 3-16. o.

[14] Szádeczky Tamás: Big Data a közigazgatásban. In: Sasvári, Péter (szerk.): Informatikai rendszerek a közszolgálatban. Ludovika Egyetemi Kiadó. Budapest, 2020. 113-126. o.

[15] Bederna Zsolt – Váczi Dániel – Pollner Péter – Szádeczky Tamás: Támadás hálózatba szervezve. In: Auer, Ádám; Joó, Tamás (szerk.): Hálózatok a közszolgálatban. Dialóg Campus Kiadó. Budapest, 2019. 223-247. o.

átfogó megközelítés lehetővé teszi a fals pozitív riasztások számának csökkentését és a valódi fenyegetések pontosabb azonosítását. Az UBA-rendszerek elméleti alapjainak fontos része a folyamatos tanulás és adaptáció koncepciója.[16]

Mivel a felhasználói viselkedés és a kiberbiztonsági fenyegetések állandóan változnak, ezek a rendszerek folyamatosan frissítik és finomítják modelljeiket az új adatok és tapasztalatok alapján.[17] Ez a dinamikus megközelítés biztosítja, hogy az UBA-rendszerek hatékonyan alkalmazkodjanak az evolválódó fenyegetési környezethez. A felhasználói viselkedés elemzésének elméleti alapjai egy komplex, multidiszciplináris megközelítést tükröznek, amely integrálja a kiberbiztonsági ismereteket, a viselkedéstudományokat és a fejlett adatelemzési módszereket. Ez az innovatív megközelítés lehetővé teszi a szervezetek számára, hogy hatékonyabban azonosítsák és kezeljék a felhasználói viselkedésből eredő biztonsági kockázatokat, kiegészítve és megerősítve a hagyományos technológiai védelmi megoldásokat.[18]

A felhasználói viselkedés szerepe a kiberbiztonságban

A felhasználói viselkedés elemzése (UBA) egy viszonylag új megközelítés a kiberbiztonságban, amely az egyes felhasználók általános viselkedési mintáinak elemzésén alapul. Az UBA-rendszerek a felhasználók normális tevékenységét monitorozzák, majd ezeket az adatokat felhasználják az anomáliák és potenciális támadások azonosítására. Ez a technika különösen

[16] Leitold Ferenc: Practical approach for measuring the level of user behaviour. In: 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). IEEE, 2019. 1-2. o.

[17] Legárd Ildikó: Célpont vagy! -a közszolgálat felkészítése a kiberfenyegetésekre." Hadmérnök 15.1. 2020. 91-105. o.

[18] Homoliak, Ivan – Toffalini, Flavio – Guarnizo, Juan – Elovici, Yuval – Ochoa, Martina: Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. ACM Computing Surveys (CSUR), 52(2), 2019. 1-40. o.

hatékony a belső fenyegetések felismerésében, amikor a támadások a jogosult felhasználók fiókjain keresztül történnek.[19]

Az UBA-rendszerek különösen hatékonynak bizonyulnak a belső fenyegetések azonosításában, különösen akkor, amikor a támadások legitim felhasználói fiókokon keresztül történnek.[20] Az ML integrálása jelentős előrelépést hozott ezen a téren, mivel AI alapú rendszerek 85%-os pontossággal képesek előre jelezni a potenciális biztonsági incidenseket, meghaladva a hagyományos módszerek hatékonyságát.[21] Ez a megközelítés összhangban van a nemzetközi trendekkel, melyek az ML alkalmazásának növekvő jelentőségét hangsúlyozzák a kiberbiztonság területén.[22] A felhasználói tudatosság növelése kritikus tényező a hatékony kiberbiztonság megvalósításában, mivel a rendszeres képzések és szimulált támadási gyakorlatok akár 60%-kal is csökkenthetik a sikeres social engineering támadások arányát. Egy longitudinális vizsgálat szerint a szervezeti biztonsági kultúra kialakítása és fenntartása jelentős mértékben hozzájárul a kibertámadások megelőzéséhez.[23] A gyakorlati megoldások közé tartoznak a szimulált adathalász támadások is, amelyek lehetőséget biztosítanak a felhasználók számára, hogy kockázatmentes környezetben tanulják meg felismerni a potenciális fenyegetéseket. Ezek a képzések nemcsak az elméleti tudás átadását, hanem a valós életben alkalmazható készségek fejlesztését is célozzák,

[19] Hadarics Kálmán: Incidens-menedzsment gyakorlat. Nemzeti Közszolgálati Egyetem. Budapest, 2019.

[20] Arohan, Yash – Yadav, Ashwin – Pandey, Aakash – Churi, Shardul – Saxena, Manvi – Vaghani, Akshit: An introduction to context-aware security and User Entity Behavior Analytics. International Journal of Advance Research, Ideas and Innovations in Technology, 2020, 6.5: 27-33. o.

[21] Liu, Fucheng – Wen, Yu – Zhang, Dongxue – Jiang, Xihe – Xing, Xinyu – Meng, Dan: Log2vec: A heterogeneous graph embedding based approach for detecting cyber threats within enterprise. In: Proceedings of the 2019 ACM SIGSAC conference on computer and communications security. 2019. 1777-1794. o.

[22] Buczak, Anna L. – Guven, Erhan: A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications surveys & tutorials, 2015, 18.2: 1153-1176. o.

[23] Abawajy, Jemal: User preference of cyber security awareness delivery methods. Behaviour & information technology, 2014, 33.3: 237-248. o.

összhangban az adathalászat elleni képzések hosszú távú hatékonyságát vizsgáló nemzetközi kutatásokkal.[24] A felhasználói viselkedéselemzés lehetőséget nyújt a kockázatok előrejelzésére, miközben a felhasználók oktatása és tudatosságának növelése csökkentheti a támadások sikerességét. A jövőbeni kutatásoknak a felhasználói viselkedés finomabb elemzésére és az algoritmusok továbbfejlesztésére kell összpontosítaniuk, hogy a védekezési rendszerek még proaktívabbá váljanak. Egyes kutatások rámutatnak, hogy a felhasználók tevékenységeinek szisztematikus elemzése kulcsfontosságú információkat szolgáltat a potenciális fenyegetésekről, lehetővé téve a proaktív védekezést és a biztonsági incidensek korai felismerését.[25]

A felhasználói viselkedéselemző rendszerek elsődleges célja a normálistól eltérő viselkedési minták azonosítása, amelyek potenciálisan kibertámadások vagy biztonsági incidensek előjelei lehetnek. A szociális manipulációs technikák, mint például az adathalászat, azon az alapvető pszichológiai megfigyelésen alapulnak, hogy a felhasználók bizonyos körülmények között könnyen befolyásolhatók, és hajlamosak figyelmen kívül hagyni a biztonsági protokollokat, különösen, ha egy jól felépített megtévesztéssel találkoznak. Ez a jelenség összhangban van a social engineering támadások pszichológiai mechanizmusait részletesen vizsgáló kutatásokkal. A szervezeti kultúra és a személyes attitűdök kulcsfontosságú szerepet játszanak a biztonsági magatartás kialakításában. Magyarországon végzett kutatások szerint a szervezetek jelentős része nincs megfelelően felkészülve a modern kiberfenyegetések felismerésére és kezelésére, ami kritikus sebezhetőséget jelent a célzott támadásokkal szemben. A hazai vállalatok gyakran alábecsülik a kiberbiztonság jelentőségét, és nem fordítanak elegendő erőforrást a védelmi rendszerek fejlesztésére és a munkavállalók oktatására. A prob-

[24] Kumaraguru, Ponnurangam – Sheng, Steve – Acquisti, Alessandro – Cranor, Lorrie Faith – Hong, Jason: Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology (TOIT), 2010, 10.2. 1-31. o.
[25] Krasznay Csaba: A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban. Nemzet és Biztonság – Biztonságpolitikai Szemle 2017/3. szám. 38–53. o.

léma megoldása érdekében a rendszeres és gyakorlatorientált kiberbiztonsági képzések fontosságát hangsúlyozzák a szakértők.[26] Fontos megemlíteni, hogy Magyarországon több kijelölt szervezet is létezik, amelyek segítséget nyújthatnak a vállalatoknak ezen a területen, például az Alkotmányvédelmi Hivatal (AH), a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NKI) és más szakosított állami szervek. A probléma méretéhez képest azonban kevés szó esik arról, hogy a cégeknek lenne honnan segítséget kérni Magyarországon is.

Az interaktív, szimuláción alapuló képzések jelentősen hatékonyabbak a hagyományos, elméleti oktatásnál. A szerzők szerint ezek a gyakorlatok nem csak az elméleti tudást, hanem a valós helyzetekben alkalmazható készségeket is fejlesztik, ami kulcsfontosságú a gyorsan változó fenyegetési környezetben. A felhasználói viselkedéselemzés területén a jövőbeni kutatásoknak a viselkedési minták finomabb elemzésére és az algoritmusok továbbfejlesztésére kell összpontosítaniuk.[27] Érdemes lenne nagyobb hangsúlyt fektetni a biometrikus sajátosságok vizsgálatára is, mint például a kurzormozgás felismerése és annak egy adott felhasználóhoz rendelése, ami további azonosítási réteget biztosíthat a rendszerekben. Az ML-modellek és a big data analitika integrálása a viselkedéselemző rendszerekbe jelentősen növelheti a fenyegetések előrejelzésének pontosságát és a védelmi rendszerek proaktivitását.

A felhasználói viselkedés elemzése jelentős mértékben támaszkodik a viselkedési anomáliák felismerésére, amelyek egy adott felhasználó normál viselkedési mintáitól való eltérések lehetnek, például egy szokatlan bejelentkezési helyszín vagy egy nem megszokott időben történő tevékenység.[28] Ezek az anomáliák jelezhetik, hogy egy külső támadó hozzáférést

[26] Kiss Adrienn – Kollár Csaba: Az információbiztonság időszerű kérdései a magyarországi kkv-k körében. Scientia et Securitas, 4(2), 2024. 98-107. o.
[27] Beuran, Razvan – Chinen, Ken-Ichi – Tan, Yasuo – Shinoda, Yoichi: Towards effective cybersecurity education and training. 2016.
[28] Nagy Zoltán: A kiberbűncselekmények fogalma és csoportosítása. In: Kiss, T. (szerk.): Kibervédelem a bűnügyi tudományokban. Dialóg Campus, Budapest, 2020. 33-44. o.

szerzett egy felhasználói fiókhoz, vagy egy belső fenyegetés kezd kibontakozni.

A kognitív torzítások és az emberi hibák elmélete

Az egyik jelentős elméleti megközelítés, amely alapvetően befolyásolja a felhasználói viselkedést a kiberbiztonság területén, a kognitív torzítások elmélete. Ezek a mentális rövidítések vagy heurisztikák az emberek döntéshozatalát egyszerűsítik, de gyakran hibás következtetésekhez vezethetnek, különösen a gyors és precíz döntések szituációiban. A kiberbiztonság területén, ahol egy-egy döntés kritikus jelentőségű lehet, ezek a torzítások különösen veszélyesek. Az egyik legkritikusabb ilyen kognitív torzítás a „sérthetetlenség illúziója", amelynek hatására a felhasználók jelentősen alábecsülik a kibertámadások kockázatát. Ez a jelenség különösen aggasztó, mert sok felhasználó túlbecsüli a saját képességeit a fenyegetések felismerésében és kezelésében, ami csökkenti az éberséget és a biztonsági előírások betartásának hajlandóságát.[29]

A kognitív torzítások mellett a szociális tanulás elmélete is kulcsfontosságú szerepet játszik a kiberbiztonsági magatartás formálásában. Ez az elmélet azt hangsúlyozza, hogy az emberek hajlamosak mások viselkedését utánozni, különösen akkor, ha az adott személy tekintéllyel bír. Ennek következménye az, hogy egy szervezet biztonságtudata jelentősen romolhat, ha a vezetők vagy kollégák nem megfelelő viselkedést mutatnak. Azokban a szervezetekben, ahol a vezetők jó példát mutatnak a biztonsági protokollok betartásában – például aktívan részt vesznek a kiberbiztonsági képzéseken, láthatóan betartják a biztonsági előírásokat és kommunikálják ezek fontosságát –, a munkavállalók is nagyobb valószínűséggel követik ezeket az előírásokat. A vezetői példa tehát döntő hatással van a kiberbiztonsági

[29] Bicskei Tamás: A mesterséges intelligencia közigazgatásban való felhasználásával okozott kár. KözigazgatásTudomány 2023/1. szám. 99-114. o.

kultúra kialakítására és fenntartására.[30] A szociális tanulás hatása a munkahelyi kiberbiztonságra nem csupán a vezetői struktúrákon keresztül érvényesül, hanem a horizontális, kollégák közötti interakciók is meghatározó szerepet játszanak. Az ilyen típusú tanulás különösen fontos a kiberbiztonsági gyakorlatok esetében, mivel a kollégák viselkedése és hozzáállása gyakran közvetlenül befolyásolja az egyéni biztonságtudatosságot. A peer-to-peer tanulási módszerek alkalmazása révén hatékonyan erősíthető a munkahelyi biztonsági kultúra. Ez a módszer lehetőséget biztosít arra, hogy a kollégák közvetlen tapasztalatokat osszanak meg egymással, ezáltal növelve az egyéni elköteleződést és tudatosságot a kiberbiztonsági elvek betartásában.[31]

A kognitív torzítások és a szociális tanulás elméletei nem csupán elméleti jelentőséggel bírnak, hanem gyakorlati következményekkel is járnak. A hatékony kiberbiztonsági stratégiák kialakításánál ezek a pszichológiai tényezők kulcsszerepet játszanak. A szituációs gyakorlatok és az interaktív képzési módszerek alkalmazása segíthet a kognitív torzítások csökkentésében, valamint a helyes viselkedésminták megerősítésében, ami elengedhetetlen a biztonságos szervezeti kultúra kialakításához.[32] A nemzetközi kutatások is alátámasztják ezeket az eredményeket, hiszen a felhasználók biztonsági protokollokhoz való alkalmazkodása szoros összefüggésben áll a kognitív folyamatokkal és a szociális környezettel. Ez a globális tapasztalat rávilágít arra, hogy a pszichológiai tényezők figyelembevétele univerzális jelentőségű a kiberbiztonsági stratégiák tervezésénél, nem csupán a hazai, hanem a nemzetközi kontextusban is.[33]

[30] Bandura, Albert – Hall, Prentice: Albert Bandura and social learning theory. Learning Theories for Early Years 78. 2018.
[31] Happa, Jassim – Glencross, Mashhuda – Steed, Anthony: Cyber security threats and challenges in collaborative mixed-reality. Frontiers in ICT 6. 2019: 5. o.
[32] Morsella, Ezequiel – Bargh, John A. – Gollwitzer, Peter M.: Social cognition and social neuroscience. Oxford handbook of human action, 2008.
[33] Bulgurcu, Burcu – Cavusoglu, Hasan – Benbasat, Izak: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 2010. 523-548. o.

A felhasználói viselkedéselemző (UBA) rendszerek elméleti háttere

Az UBArendszerek elméleti hátterében az ML és az adatelemzés komplex módszertana áll, amely lehetővé teszi a felhasználói viselkedés mélyreható és valós idejű elemzését. Ezek a rendszerek különösen hatékonyak a belső fenyegetések azonosításában, ahol a hagyományos védelmi megoldások gyakran kudarcot vallanak. A belső fenyegetések egyre növekvő kockázatot jelentenek a modern szervezetekben, így az UBA-rendszerek alkalmazása kritikus szerepet játszik a kiberbiztonságban.[34] Az UBA-rendszerek gépitanulás-algoritmusokra és adat alapú elemzésekre építenek, amelyek lehetővé teszik a felhasználói viselkedés folyamatos megfigyelését és a szokatlan tevékenységek valós idejű azonosítását. Az Európai Unióban az UBA-rendszerek alkalmazása során különös figyelmet kell fordítani a személyes adatok védelmére és a vonatkozó jogszabályok betartására. Az Európai Unió Általános Adatvédelmi Rendelete (GDPR) alapelvei, mint a jogszerűség, méltányosság és átláthatóság, célhoz kötöttség, adatminimalizálás, pontosság és tárolási korlátozás, meghatározzák, hogy a személyes adatokat csak meghatározott, jogszerű és egyértelműen kifejezett célokra lehet gyűjteni, és azoknak relevánsnak és a szükségesre korlátozottnak kell lenniük. Ezen túlmenően, az Európai Unió mesterséges intelligenciáról szóló jogszabálya (AI Act) kockázat alapú megközelítést alkalmaz az MI-rendszerek szabályozásában. Ez a megközelítés arányos és hatékony, kötelező erejű szabályokat vezet be az MI-rendszerekre vonatkozóan, figyelembe véve azok kockázati szintjét.[35] Ezek a rendszerek képesek gyorsan reagálni a fenyegetésekre, mivel figyelik az adatokat és elemzik a mintákat, így az eltérések esetén azonnal figyelmeztetést küldenek, amely kritikus lehet a dinamikusan változó kiberbiztonsági környezetben. Az UBA-rend-

[34] Homoliak, Ivan – Toffalini, Flavio – Guarnizo, Juan – Elovici, Yuval – Ochoa, Martina: nsight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. ACM Computing Surveys (CSUR), 52(2), 2019. 1-40. o.

[35] Országgyűlés Hivatala: Infojegyzet 2024/23. szám. Forrás: https://www.parlament.hu/documents/d/guest/infojegyzet_2024_23_eu_mi_rendelet Letöltés ideje: 2025. 03. 01.

szerek elméleti hátteréhez szorosan kapcsolódik az MI és a big data elemzés, amelyek lehetővé teszik az adathalmazok hatékony feldolgozását és a viselkedési minták pontosabb felismerését.

A nemzetközi szakirodalom megerősíti, hogy az UBA-rendszerek hatékonysága nemzetközileg is elismert, különösen a többfázisú felhasználói viselkedés elemzésében. Ezek a rendszerek univerzálisan alkalmazhatók, és fontos szerepet játszanak a globális kiberbiztonsági stratégiákban, hangsúlyozva a felhasználói viselkedés mélyreható elemzésének jelentőségét.[36]

A kibertámadások típusai és trendjei

A kibertámadások evolúciója és komplexitásának növekedése korunk egyik legjelentősebb biztonsági kihívását jelenti. A digitalizáció térnyerésével párhuzamosan a támadási vektorok és módszerek is jelentősen átalakultak, ami folyamatos alkalmazkodást követel mind a védelmi szakemberektől, mind a felhasználóktól.[37] A Nemzeti Kibervédelmi Intézet 2023-as jelentése szerint Magyarországon az elmúlt években különösen megnövekedett a zsarolóvírus támadások száma, amelyek főként az Európai Unió országaira összpontosítottak.[38] Ez összhangban van a globális trendekkel, amit az Europol Internet Organised Crime Threat Assessment (IOCTA) jelentése is megerősít,[39] kiemelve a Ransomware as a Service (RaaS modell) támadások növekvő fenyegetését Európa-szerte.

---

[36] Beláz Annamária – Berzsenyi Dániel: Kiberbiztonsági Stratégia 2.0: A kiberbiztonság stratégiai irányításának kérdései. NKE Stratégiai Védelmi Kutatóközpont Elemzések, 2017/3. szám. 1-15. o.

[37] Sasvári Péter (szerk.): Informatikai rendszerek a közszolgálatban II. Ludovika Egyetemi Kiadó. Budapest, 2020.

[38] Nemzeti Kibervédelmi Intézet (2024). Éves kiberbiztonsági jelentés. Forrás: https://nki.gov.hu/wp-content/uploads/2024/07/Eves-kiberbiztonsagi-jelentes.pdf Letöltés ideje: 2024. 09. 23.

[39] Europol (2024). Internet Organised Crime Threat Assessment (IOCTA). Forrás: https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf Letöltés ideje: 2024. 09. 23.

A kritikus infrastruktúrák elleni támadások száma is emelkedő tendenciát mutat, ami nemzetbiztonsági szempontból is kiemelt figyelmet érdemel. Ez a trend nem csak Magyarországra jellemző. Az Egyesült Államokban a Cybersecurity and Infrastructure Security Agency (CISA) 2022-es jelentése szerint a kritikus infrastruktúrák elleni támadások 55%-kal nőttek az előző évhez képest.[40]

A kibertámadások típusai

Az ENISA (European Union Agency for Cybersecurity) 2023-as Threat Landscape jelentése átfogó elemzést nyújt a globális kiberbiztonsági fenyegetettségek fejlődéséről, valamint a különböző támadási vektorokról. A jelentés nyolc fő fenyegetettségi csoportot különít el, amelyek különösen jelentőségteljesek az előfordulásuk és hatásuk tekintetében. Az internetes fenyegetések, más néven cyberthreats, olyan támadások, amelyek az interneten keresztül történnek, céljuk pedig a hálózati rendszerek, alkalmazások és adatbázisok kompromittálása. Ezek a támadások magukban foglalhatják a webes szolgáltatások elleni támadásokat (pl. webes sebezhetőségek kihasználása), valamint a botnetekkel végrehajtott támadásokat, amelyek széleskörű kárt okozhatnak a felhasználók és szervezetek számára. Az ellátási láncok elleni támadások különösen veszélyesek, mivel nemcsak a célzott szervezeteket érinthetik, hanem azok beszállítóit, partnereit és ügyfeleit is. Az ilyen támadások során a támadók egy gyenge pontot keresnek az ellátási lánc valamelyik szereplőjében, és azon keresztül érik el a célrendszereket. A SolarWinds és a Kaseya esetei például világosan bemutatták, hogy ezek a támadások milyen széleskörű és hosszú távú hatással lehetnek. A social engineering támadások során a támadók pszichológiai manipulációval próbálják megszerezni az áldozatoktól azokat az információkat, amelyek hozzáférést biztosítanak kritikus rendszerekhez. Az ilyen támadások egyik legelterjedtebb formája az adathalászat (phishing), amely

[40] America's Cyber Defense Agency: 2021 Trends Show Increased Globalized Threat of Ransomware. 2022. Forrás: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a Letöltés ideje: 2024. 09. 23.

során a támadók megtévesztő e-mailekkel vagy üzenetekkel csalják ki a felhasználóktól az érzékeny adatokat, például jelszavakat vagy pénzügyi információkat. A malware-ek, vagyis a rosszindulatú szoftverek, olyan programok vagy kódok, amelyek célja a számítógépes rendszerek megfertőzése és kompromittálása. A malware-ek típusai közé tartoznak a vírusok, férgek, trójaiak, spyware-ek és a rootkit-ek. A malware-támadások sokszor automatizáltak és rendkívül elterjedtek, mivel a támadók könnyen hozzáférhetnek olyan eszközökhöz, amelyekkel tömeges támadásokat indíthatnak. A DoS (Denial of Service), illetve elosztott változata, a DDoS (Distributed Denial of Service) támadások célja, hogy egy hálózati szolgáltatást vagy szervert túlterheljenek, ezzel akadályozva a normál működést. Ezen támadások következtében az áldozatok nem férnek hozzá a kívánt szolgáltatásokhoz, ami különösen nagy problémát jelenthet az üzleti szférában, mivel bevételkiesést és presztízsveszteséget is eredményezhet. Az információ manipulációja egyre nagyobb fenyegetést jelent, különösen a közösségi média és az online hírek korában. Az ilyen támadások során a támadók dezinformációval vagy félrevezető információval próbálnak politikai, gazdasági vagy társadalmi befolyást szerezni. Az adatvédelmi fenyegetések olyan támadásokra utalnak, amelyek célja az egyének személyes adatainak ellopása, megsértése vagy illegális felhasználása. Az adatszivárgások és adatlopások az egyik leggyakoribb következményei ezeknek a támadásoknak, amelyek súlyos pénzügyi és reputációs károkat okozhatnak mind a magánszemélyek, mind a szervezetek számára.

Az GDPR az európai gazdasági térségben működő szervezetekre vonatkozik, és szigorú követelményeket támaszt az adatvédelem területén, beleértve a személyes adatok kezelését, az incidensek bejelentését és a büntetések kiszabását. A GDPR mellett más régiókban is léteznek hasonló szabályozások, mint például a kaliforniai fogyasztói adatvédelmi törvény (CCPA), Brazíliában a Lei Geral de Proteção de Dados (LGPD), vagy Kanadában a Personal Information Protection and Electronic Documents Act (PIPEDA). Ezek a szabályozások gyakran eltérő követelményeket támasztanak az adatvédelem terén, ami jelentős megfelelési kihívásokat jelent a

nemzetközi szervezetek számára. Az EU és az USA szabályozási különbségeiből eredő problémák jelentős kihívásokat jelentenek a globális működésű vállalatok számára. Az USA-ban nincs átfogó szövetségi adatvédelmi törvény, ehelyett ágazati szabályozások (pl. HIPAA az egészségügyben, GLBA a pénzügyi szektorban) és állami szintű jogszabályok (pl. CCPA Kaliforniában, CDPA Virginiában) mozaikja létezik. Ez a fragmentált megközelítés ellentétben áll az EU GDPR egységes keretrendszerével, ami megfelelési nehézségeket okoz a határokon átnyúló adatkezelést végző szervezeteknek. A két rendszer közötti legjelentősebb különbségek közé tartozik az adatkezeléshez szükséges jogalap, az adattovábbítási mechanizmusok és az egyéni jogok érvényesíthetőségének mértéke.[41] Konkrét példa a szabályozási különbségekből eredő problémákra a Schrems-ügyek sorozata, amelyek eredményeként az Európai Unió Bírósága érvénytelenítette mind a Safe Harbor, mind a Privacy Shield adattovábbítási keretrendszereket, jelentősen megnehezítve az EU és az USA közötti adattovábbítást. Ezek a döntések rávilágítottak az amerikai megfigyelési gyakorlatok és az európai adatvédelmi elvek összeegyeztethetetlenségére.[42]

Az ENISA Threat Landscape 2023 jelentése rávilágít arra, hogy a kiberbiztonsági fenyegetések folyamatosan fejlődnek, és egyre szofisztikáltabbak lesznek. Az említett nyolc fenyegetettségi csoport azért került kiemelésre, mert ezek széles körben előforduló és potenciálisan súlyos következményekkel járó támadási formák, amelyek számos szektort érintenek. A kiberbiztonság javítása érdekében a szervezeteknek erőforrásaikat ezen te-

[41] Bradford, Anu: The Brussels effect: How the European Union rules the world. Oxford University Press. 2020.

[42] Court of Justice of the European Union: Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems. 2020. Forrás: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp2000-91en.pdf Letöltés ideje: 2025. 03. 15.

rületek védelmére kell összpontosítaniuk, folyamatosan figyelemmel kísérve az új fenyegetéseket és a legfrissebb védelmi megoldásokat alkalmazva.[43]

Kibertámadási trendek

Az ENISA Threat Landscape 2023 jelentése alapján a zsarolóvírusok továbbra is a legjelentősebb kiberfenyegetettséget jelentik, ami annak köszönhető, hogy ezek a támadások egyre célzottabbá és összetettebbé váltak. A zsarolóvírusok nemcsak az adatokat titkosítják, hanem egy új stratégiát, az úgynevezett *„dupla zsarolást"* alkalmazzák, ahol a támadók nem csupán a titkosított adatok visszavásárlásáért követelnek váltságdíjat, hanem az ellopott adatok nyilvánosságra hozatalával is fenyegetnek. Ez a módszer tovább növeli az áldozatokra nehezedő nyomást. Ráadásul a kiberbűnözők által kínált RaaS modellek révén a kevésbé technikai hátterű szereplők is könnyen hozzáférhetnek ezekhez az eszközökhöz, növelve a támadások gyakoriságát és hatókörét. Egyre gyakrabban találkozhatunk olyan kiberkémkedési műveletekkel is, amelyek során a támadók legális eszközöket használnak fel a műveleteik elfedésére, megnehezítve ezzel a felderítést. Az ilyen legális szoftverek, mint például a PowerShell vagy más rendszergazdai eszközök beépülhetnek az áldozatok infrastruktúrájába, anélkül, hogy gyanút keltenének. Ez különösen veszélyessé válik, mert hosszabb időn keresztül észrevétlenek maradhatnak, és lehetővé teszik a támadók számára, hogy érzékeny adatokat szerezzenek vagy további támadásokat készítsenek elő.

A geopolitikai feszültségek és konfliktusok továbbra is meghatározó szerepet játszanak a kiberműveletekben. Egyre inkább elterjedt, hogy állami támogatással működő szereplők célzott támadásokat hajtanak végre, amelyek célpontjai elsősorban kormányzati szervek, kritikus infrastruktúrák és ipari vállalatok. Ezek a támadások nem pusztán károkozásra irányulnak,

[43] European Union Agency for Cybersecurity (2023). Ensia Threat Landscape 2023. Forrás: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 Letöltés ideje: 2024. 09. 23.

hanem hosszú távú stratégiai előnyök megszerzésére, például politikai befolyás növelésére vagy ipari kémkedésre. Érdekes fejlemény, hogy miközben a hagyományos mobil kártevők száma csökken, az adware-ek és kémprogramok száma továbbra is magas. Ezek a programok a felhasználók tevékenységeit követik nyomon, és gyakran rejtve futnak a háttérben anélkül, hogy a felhasználó tudomást szerezne róluk. Az adware-ek hirdetésekkel bombázzák a felhasználókat, míg a kémprogramok érzékeny adatokat gyűjtenek, például helymeghatározási információkat vagy böngészési előzményeket. A social engineering támadások szintén új szintre léptek, mivel a támadók egyre inkább a fizikai világban próbálják megtéveszteni az áldozatokat. Míg a social engineering hagyományosan elsősorban adathalászat révén történt, manapság már személyesen is megtéveszthetik az embereket, például deepfake technológiák segítségével. Az elmúlt időszakban drámaian megnövekedett a biometrikus csalások száma, ami komoly kihívást jelent a kiberbiztonság területén. A deepfake kísérletek volumene 2022 és 2023 között 3000%-kal emelkedett. Míg 2022-ben ritkán fordult elő, hogy csalók deepfake technológiát használtak a biometrikus ellenőrzések kijátszására a regisztrációs folyamat során, 2023-ban ez gyökeresen megváltozott. Az MI fejlődésének és a deepfake szoftverek növekvő elérhetőségének köszönhetően ezek mennyisége és kifinomultsága várhatóan tovább növekszik 2024-ben. Az elmúlt hat hónapban a deepfake-ek tették ki a biometrikus csalások mintegy 30-40%-át.

Jelenleg viszonylag kevés csaló felelős a nagyléptékű deepfake gyártásért, és ugyanez a csoport támadja a különböző ügyfeleket azonos módszerekkel. Mivel azonban a csalók hajlamosak eladni vagy megosztani taktikáikat más csalókkal, ez a helyzet hamarosan megváltozhat.[44] Ezzel a módszerrel a támadók egy valós személy hangját vagy kinézetét hamisítják meg, hogy bizalmas információkat szerezzenek. Az AI-technológiák, különösen az AI-chatbotok, új lehetőségeket nyitnak a kiberbűnözők számára is. Az AI

[44] Entrust: Fraud Report. Entrust Corporation. Minnesota, 2024. Forrás: https://www.entrust.com/sites/default/files/documentation/reports/entrust-fraud-report.pdf Letöltés ideje: 2025. 03. 15.

alapú chatbotok segítségével automatizálhatóvá válnak a támadások, például az adathalász kampányok. Ezen túlmenően az AI-t dezinformáció terjesztésére is felhasználják, valamint deepfake videókat és hangfelvételeket készíthetnek, amelyek segítségével hiteles személyekként léphetnek fel a támadók. A deepfake videókkal történő támadások jelentős problémát okoznak a vállalati kommunikációban és különösen a távoli munkavégzés során használt videókonferencia platformokon. Ezek a csalások különösen veszélyesek, mivel a technológia fejlődésével egyre nehezebb megkülönböztetni a valódi és a mesterségesen létrehozott videókat. A védekezés érdekében sok szervezet többfaktoros azonosítási protokollokat, offline ellenőrzési mechanizmusokat és előre meghatározott biztonsági jeleket vezetett be a videókonferenciákon történő interakciók során.[45] A DDoS-támadások szintén új dimenzióba léptek, mivel egyre nagyobb volumenű és összetettebb támadásokkal találkozhatunk, amelyek már nemcsak a hagyományos célpontokat, hanem a mobilhálózatokat és az IoT-eszközöket is célba veszik. A DDoS-as-a-Service modellek elterjedése pedig tovább növeli a támadások gyakoriságát, mivel ezek a szolgáltatások könnyen elérhetők és megrendelhetők bárki számára. Az információ manipulációjának területén az MI által generált tartalmak egyre inkább aggodalomra adnak okot. Bár a deepfake technológia már korábban is ismert volt, most az egyszerűbb, olcsóbb módszerek is elérhetők, amelyekkel könnyedén létrehozhatók hamisított képek és videók, a valóság manipulálása érdekében. Ezek a „cheap fakes" néven ismert tartalmak gyorsan terjednek a közösségi médiában, és jelentős hatással vannak a közvéleményre. A támadások során különösen a magas jogosultságokkal rendelkező alkalmazottakat, például a fejlesztőket és rendszergazdákat célozzák meg, akik hozzáféréssel rendelkeznek a vállalat kulcsfontosságú rendszereihez. Ezek a támadások gyakran hosszú távú károkat okoznak, és az egész iparágra hatással lehetnek. A 2023-as fenyegetettségi trendek rámutatnak arra, hogy a kiberbiztonsági fenyegetések mind komplexitásukban, mind méretükben növekednek. Az

[45] Verdoliva, Luisa. Media forensics and deepfakes: an overview. IEEE journal of selected topics in signal processing. 2020/5. szám. 910-932. o.

új technológiák, például az AI, új lehetőségeket nyitnak a támadók számára, miközben a klasszikus támadási módszerek, mint a zsarolóvírusok és a social engineering, továbbra is komoly veszélyt jelentenek. A fenyegetésekkel szembeni védekezés érdekében a szervezeteknek szorosan kell követniük ezeket a trendeket, és naprakész védelmi stratégiákat kell alkalmazniuk.[46]

Új kibertámadási irányok

Az ENISA legfrissebb jelentése rávilágít, hogy a kiberbűnözésben új trendek alakultak ki, amelyek közül kiemelkedik a ritkábban használt programozási nyelvek, például a Rust és a Go elterjedése. Ezeket a nyelveket a támadók azért részesítik előnyben, mert nehezítik a kártékony kódok elemzését, ami megnehezíti a biztonsági szakértők dolgát. Különösen a Go nyelv sajátossága, hogy a lefordított bináris állományok nagyobb méretűek, mint a hagyományosan használt nyelveké, mivel statikusan linkelik a szükséges könyvtárakat. Ez a méretbeli különbség – például a „Hello World" program binárisa Go nyelven több MB, míg C vagy C++ nyelven mindössze néhány KB – azt eredményezi, hogy sok malware scanner figyelmen kívül hagyja ezeket a nagy fájlokat, mivel kisebb méretű kártékony kódokra optimalizálták őket. A felhőinfrastruktúrák szerepe szintén kiemelkedővé vált a kiberbűnözésben, különösen a felhő hibás konfigurációit kihasználó támadások révén. A bűnözők egyre inkább célozzák az áldozatok felhő alapú rendszereit, és ezek az infrastruktúrák maguk is sok esetben a social engineering kampányok részévé válnak. Például adathalász kampányok során fájlmegosztó szolgáltatásokat használnak a kártékony fájlok terjesztésére. Az FBI már figyelmeztetést adott ki arra vonatkozóan, hogy kiberbűnözők keresőmotor-hirdetési szolgáltatásokat használnak fel, hogy legitim márkáknak álcázzák magukat, és így irányítsák a felhasználókat adathalász vagy zsarolóvírussal fertőzött oldalakra. A módszer lényege, hogy a bűnözők olyan hirdetéseket helyeznek el, amelyek megtévesztően hasonlítanak az eredeti cégek weboldalaira, így a felhasználók

[46] European Union Agency for Cybersecurity (2023): i.m.

könnyen félrevezethetők, és rosszindulatú tartalmakkal fertőződhetnek meg. Ezen túlmenően, a cryptojacking, azaz az áldozatok számítási erőforrásainak titkosított bányászatra való felhasználása továbbra is népszerű technika a kiberbűnözők körében. Bár az újabb fenyegetések, mint például a deepfake és az AI alapú social engineering technikák növekvő trendet mutatnak, a bűnözők többsége még mindig a jól bevált, régebbi módszereket részesíti előnyben. Ezek kevesebb technikai tudást és erőfeszítést igényelnek, miközben jelentős anyagi hasznot hoznak. A kémprogramok használata továbbra is virágzik, ami súlyos aggodalmakat kelt a magánélet védelmével kapcsolatban.[47]

Az elemzés rámutat arra is, hogy a Crime-as-a-Service (CaaS) piacok gyorsan növekednek, és egyre elérhetőbbé válnak a különféle kibertámadási szolgáltatások. Ez azt jelenti, hogy gyakorlatilag bárki, aki megfelelő pénzösszeggel rendelkezik, megvásárolhatja a kibertámadások terveit vagy akár teljesen automatizált eszközöket. Ez a jelenség drámaian növeli a támadások gyakoriságát és elérhetőségét, különösen a laikus támadók számára, akik korábban nem rendelkeztek technikai háttérrel. A geopolitikai helyzet, különösen az orosz-ukrán háború, szintén fokozta a hacktivista tevékenységeket, és az oroszbarát csoportok, mint például a NoName057, aktívan toboroznak embereket túlterheléses támadások indítására.[48] Ezek a csoportok különösen az egyszerűen kezelhető, letölthető programokkal célozzák meg a laikusokat, lehetővé téve számukra, hogy könnyedén részt vegyenek kibertámadásokban. Az új technológiák, mint az MI és a felh alapú rendszerek kihasználása, valamint a Crime-as-a-Service modellek elterjedése komoly fenyegetést jelentenek a globális kiberbiztonságra.[49]

Elhíresült kibertámadások

A kiberbűnözés növekvő fenyegetettsége számos példán keresztül világosan mutatja a globális gazdasági és társadalmi rendszerek sebezhetőségét,

[47] European Union Agency for Cybersecurity (2023): i.m.
[48] Forrás: https://www.radware.com/cyberpedia/ddos-attacks/noname057(16)/ Letöltés ideje: 2024. 09. 21.
[49] European Union Agency for Cybersecurity (2023): i.m.

valamint az új technológiák kihasználásának képességét a támadók részéről. Az elmúlt években tapasztalt nagy volumenű, kifinomult támadások – mint a Colonial Pipeline, a SolarWinds vagy a Kaseya ellen irányuló zsarolóvírus-támadások – rávilágítottak arra, hogy a kritikus infrastruktúrák és vállalatok egyre nagyobb kockázatnak vannak kitéve.

2021 májusában a Colonial Pipeline, az Egyesült Államok legnagyobb üzemanyag-vezetékrendszere súlyos RaaS-modell támadás áldozatává vált. A támadást a DarkSide nevű bűnszervezet hajtotta végre, amely a RaaS-modellt alkalmazta, így különféle eszközöket és infrastruktúrát biztosított más bűnözők számára is. A támadás során a hackerek bejuttatták a kártékony szoftvert a vállalat számítógépes rendszerébe, amely titkosította az adatokat, ezzel megakadályozva a működést. A Colonial Pipeline kénytelen volt leállítani a teljes működését, ami az USA keleti partvidékén üzemanyaghiányt és pánikszerű felvásárlást okozott. A támadók 4,4 millió dollár váltságdíjat kaptak Bitcoinban, amelynek kifizetését a vállalat a gyors helyreállítás érdekében fontolóra vette. Ez az eset nemcsak rávilágított a kritikus infrastruktúrák sebezhetőségére, hanem az amerikai kormány is szigorúbb szabályozásokat vezetett be a kiberbiztonság terén, hogy megakadályozza hasonló esetek bekövetkezését. A Colonial Pipeline elleni támadás példáján keresztül jól látható, hogy a kiberbűnözők célpontjai egyre inkább a kritikus infrastruktúrák, amelyek leállítása komoly társadalmi és gazdasági következményekkel járhat. Ez az eset világossá tette, hogy a kritikus infrastruktúrák sebezhetősége nem csupán technológiai kérdés, hanem nemzetbiztonsági és gazdasági fenyegetés is. A támadások ilyen típusú kockázatokat mutatnak, így a vállalatok és kormányok számára fontos, hogy megerősítsék a kiberbiztonsági védelmet, beleértve a proaktív monitoringot, a gyors reagálást és a szabályozási környezet fejlesztését. Az amerikai kormány erre válaszul szigorúbb szabályozásokat vezetett be a

kritikus infrastruktúrák védelmére, amely követendő példa lehet más országok számára is, mivel a nemzetközi együttműködés kulcsfontosságú ezen fenyegetések kezelése során.[50]

A SolarWinds elleni támadás 2020 végén zajlott, és az egyik legkifinomultabb állam által támogatott kibertámadásnak számít. A támadók a SolarWinds Orion szoftverének frissítéseibe csempésztek be kártékony kódot, amely lehetővé tette számukra, hogy több ezer szervezet rendszerébe, köztük az Egyesült Államok kormányzati ügynökségeibe is bejussanak. Az incidenst az orosz külső hírszerzéshez kötötték, ami tovább növelte a nemzetközi feszültségeket. A támadók így az érzékeny adatokat, például a belső kommunikációt és a titkos információkat is megszerezhették. Az eset rávilágított a supply chain támadások veszélyére, ahol a támadók nem közvetlenül a célpontokat támadják meg, hanem egy harmadik fél, például szoftverszállító rendszereit manipulálják. A támadás következményeként számos ország és szervezet felülvizsgálta kiberbiztonsági stratégiáját és beszállítói láncának biztonságát, hogy megakadályozza a jövőbeli hasonló incidenseket. Az állam által támogatott támadások, például a SolarWinds-incidens rávilágítanak arra, hogy a geopolitikai célok elérésében a kibertámadások egyre nagyobb szerepet játszanak. Az ilyen támadások nemcsak gazdasági kárt okoznak, hanem megingathatják a nemzetközi biztonságot és bizalmat is. A SolarWinds-támadás azt mutatja, hogy a beszállítói láncok sebezhetősége központi kérdéssé vált. Az ilyen típusú támadások felderítése különösen nehéz, mivel a támadók a beszállítók infrastruktúrájába mélyen beágyazott kártékony kódokkal dolgoznak, amelyeket nehéz észlelni. Az ellátási lánc biztonságának javítása érdekében ajánlott a beszállítói auditok bevezetése, valamint a fejlett monitoring és biztonsági eszközök alkalmazása, amelyek képesek az anomáliák korai felismerésére. A szervezeteknek különös figyelmet kell fordítaniuk a beszállítók és alvállalkozók kiberbiztonsági gyakorlatainak értékelésére, valamint a szigorú biztonsági

[50] Turton, William - Riley, Michael - Jacobs, Jennifer: Colonial pipeline paid hackers nearly $5 million in ransom. Bloomberg (May 13, 2021) Forrás: https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom Letöltés ideje: 2024. 09. 23.

szabványoknak való megfelelésre.[51] Az incidens kivizsgálása során feltárták, hogy az emberi tényező jelentős szerepet játszott a támadás sikerében. A kongresszusi meghallgatások és a SolarWinds korábbi alkalmazottainak beszámolói alapján kiderült, hogy a vállalat egyik gyakran használt jelszava a *„solarwinds123*" volt, amelyet nyilvánosan elérhetővé tettek egy GitHub repozitóriumban.[52]

2021 júliusában a REvil zsarolóvírus csoport egy nagy volumenű támadást indított a Kaseya VSA szoftver ellen, amelyet IT-szolgáltatók használnak a különböző ügyfeleik rendszerének kezelésére. A támadás során a REvil hackerei egy sebezhetőséget kihasználva több mint 1500 vállalatot érintettek világszerte. A zsarolóvírus titkosította az érintett rendszereket, és 70 millió dollár váltságdíjat követeltek az univerzális dekódolóért. Ez volt az eddigi legnagyobb ismert váltságdíj-követelés, amely nemcsak a Kaseya ügyfeleit, hanem az IT-ágazatot is komolyan érintette. Az esemény rámutatott a RaaS-modell veszélyességére, ahol a zsarolóvírus fejlesztői és üzemeltetői különböző csoportok, ezáltal megnehezítve a felderítést és a védekezést. A Kaseya támadása figyelmeztetés volt a vállalatok számára, hogy a kiberbiztonsági intézkedések és a rendszeres biztonsági frissítések menynyire elengedhetetlenek a hasonló támadások megelőzésére. A zsarolóvírusok fejlődése is jelentős aggodalomra ad okot, különösen a RaaS-modell megjelenésével. A REvil zsarolóvírus támadás a Kaseya szoftver ellen bemutatta, hogy a támadók már nem egyénileg, hanem jól szervezett szolgáltatásként nyújtanak támadási infrastruktúrát és eszközöket, ami megnöveli a támadások számát és hatékonyságát. A támadók egy 0-day sérülékenységet használtak ki a Kaseya rendszerében. Ez azt jelenti, hogy a belépési

[51] Sanger, David E.: Russian hackers broke into federal agencies, US officials suspect. The New York Times, 2020, 13. Forrás: https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-govern-ment-treasury-commerce.html Letöltés ideje: 2024. 09. 23.
[52] Keumars Afifi-Sabet: SolarWinds blames intern for weak 'solarwinds123' password. Forrás: https://www.itpro.com/security/cyber-attacks/358738/intern-blamed-for-weak-password-that-may-have-sparked-solarwinds Letöltés ideje: 2025. 03. 16.

pont a Kaseya szoftver biztonsági rése volt, amelyet a támadók kihasználtak a zsarolóvírusos támadás végrehajtásához.[53] A RaaS-modell megnehezíti a támadók azonosítását és a védekezést, mivel a támadásokat végrehajtó csoportok nem azonosak a kártékony szoftverek fejlesztőivel. A jövőben szükséges a nemzetközi jogi keretek és a bűnüldözési eszközök továbbfejlesztése, hogy hatékonyan lehessen felvenni a harcot az ilyen modellekkel. A bűnüldöző szervek együttműködése kulcsfontosságú a RaaS platformok felszámolásában és a támadók felelősségre vonásában.[54]

Az MI és a deepfake technológia megjelenése új típusú támadásokhoz vezetett a kiberbűnözés terén. 2019-ben egy brit energiavállalat vezérigazgatója egy telefonos hívás során, amelyet a német anyavállalatának vezetőjétől kapott, 220 000 eurót utalt át egy magyar beszállítónak, mert azt hitte, hogy valóban a német vezetővel beszél. Valójában azonban a hívás során egy MI által generált hangot hallott, amely tökéletesen utánozta a német vezető hangját és akcentusát. Ez az eset rávilágított arra, hogy az MI alapú social engineering támadások mennyire veszélyesek lehetnek, és hogy a hagyományos kiberbiztonsági intézkedések, mint például a jelszavak és a kétfaktoros hitelesítés nem elegendőek a védelemhez. A deepfake technológia potenciális kiberbiztonsági kockázatai miatt szükségessé vált a megbízható azonosítási és ellenőrzési rendszerek fejlesztése, amelyek képesek a manipulált médiatartalmak kiszűrésére. Az MI és a deepfake technológia megjelenése új típusú social engineering támadásokat tett lehetővé, amelyek sokkal kifinomultabbak és nehezebben észlelhetők. Az MI segítségével a támadók képesek utánozni vezetők vagy más kulcsfontosságú személyek hangját, viselkedését vagy akár teljes megjelenését akár valós idejű videós formában is, így könnyebben tudnak bizalmas információkat

[53] ICS Cyber Security Blog: A Kaseya-incidens és annak tágabb összefüggései. Forrás: https://icscybersec.blog.hu/2021/07/10/kaseya-incidens-osszefuggesei Letöltés ideje: 2025. 03. 12.

[54] Cimpanu, Catalin: REvil asks for $70 million to decrypt systems impacted in Kaseya ransomware attack. The Record by Recorded Future. Forrás: https://therecord.media/revil-gang-asks-70-million-to-decrypt-systems-locked-in-kaseya-attack Letöltés ideje: 2024. 09. 19.

kicsalni vagy pénzügyi tranzakciókat végrehajtatni. Az új típusú támadások kivédése érdekében fontos, hogy a vállalatok olyan MI alapú védelmi rendszereket fejlesszenek ki, amelyek képesek felismerni a deepfake manipulációkat és más, MI alapú fenyegetéseket.[55]

Az ML és a MI segítségével fejlettebb védelmi rendszerek hozhatók létre, amelyek képesek észlelni és megelőzni az új típusú támadásokat. A mélytanulási architektúrák, mint a Meso-4 és a MesoInception-4, hatékonyan alkalmazhatók a deepfake videók felismerésére. A Meso-4 hálózat négy egymást követő konvolúciós és pooling rétegből áll, míg a MesoInception-4 az első két konvolúciós réteget egy inception modul variánsával helyettesíti a hatékonyság növelése érdekében. Mindkét módszer a videók mesoscopic szintű elemzésével képes észlelni a hamisításokat, a képi zajra és a magas szintű szemantikai jellemzőkre összpontosítva.[56] A kiberbiztonsági stratégiák fejlesztésében fontos szerepet játszik a technológiai és fizikai védelmi módszerek együttes alkalmazása. Az MI segítségével fejlettebb észlelési és megelőzési technológiák fejleszthetők ki, de a fizikai megoldások, mint például az élőségvizsgálat, szintén elengedhetetlenek a biztonságos azonosításban.

A Mirai botnet 2016-ban végrehajtott támadása az IoT-eszközök sebezhetőségének drámai példája volt. A Mirai botnet, amely főként IoT-eszközökből állt, a világ egyik legnagyobb DDoS (Distributed Denial of Service) támadását hajtotta végre, amely több nagy weboldalt, például a Twittert, a Netflixet és az Amazont is elérhetetlenné tett. A támadás csúcspontján a botnet másodpercenként 1,2 terabyte adatforgalmat generált, amely összeomlasztotta a célzott szolgáltatásokat. Az esemény figyelmeztetést adott a vállalatoknak arra vonatkozóan, hogy az IoT-eszközök védelme és biztonságos konfigurálása elengedhetetlen, mivel a nem megfelelően védett esz-

[55] Stupp, Catherine. Fraudsters used AI to mimic CEO's voice in unusual cybercrime case. The Wall Street Journal, 2019, 30.08.

[56] Afchar, Darius – Nozick, Vincent- Yamagishi, Junichi – Echizen, Isao: Mesonet: a compact facial video forgery detection network. In: 2018 IEEE international workshop on information forensics and security (WIFS). IEEE. 2018. 1-7. o.

közök könnyen botnetek részévé válhatnak. A Mirai botnet példája világosan megmutatta, hogy a biztonsági rések kihasználása a kiberbűnözők számára új lehetőségeket teremt, így a megfelelő biztonsági intézkedések bevezetése kulcsfontosságú. Az IoT-eszközök elterjedése és a Mirai botnet példája rávilágít arra, hogy az összekapcsolt rendszerek és eszközök szélesebb támadási felületet biztosítanak a kiberbűnözők számára. Az IoT-eszközök sebezhetőségei lehetővé teszik, hogy a támadók nagy mennyiségű forgalmat generáljanak, ami elérhetetlenné tehet kritikus online szolgáltatásokat. A jövőbeni védelem érdekében az IoT-eszközök biztonságának fejlesztése kiemelten fontos, beleértve az alapértelmezett jelszavak megszüntetését, a rendszeres biztonsági frissítéseket és az eszközök biztonsági protokolljainak javítását.[57]

A jövőben a vállalatoknak és a kormányoknak folyamatosan figyelemmel kell kísérniük a kibertámadásokat, és rugalmas, adaptív védelmi stratégiákat kell kidolgozniuk a fenyegetések hatékony kezelésére. Az új technológiák, mint az MI és az IoT, különösen fontos szerepet játszanak a kibertámadások terjedésében, és a védelmi intézkedéseknek alkalmazkodniuk kell e változásokhoz.

Felhasználói viselkedéselemzés a kibertámadások megelőzésében
Viselkedési mintázatok és anomáliák felismerése

A felhasználói viselkedés meghatározó szerepet játszik a kiberbiztonsági incidensek kialakulásában és megelőzésében. A kutatások egyértelműen rámutatnak, hogy az incidensek jelentős hányada emberi tényezőkre vezethető vissza, melyek gyakran a hiányos ismeretekből vagy figyelmetlenségből erednek. A jelszóhasználat terén tapasztalható hiányosságok különösen aggasztóak. Mancic és Kiss kutatásában megállapította, hogy Szlovákiában többen használnak 12 karakteres vagy annál hosszabb jelszavakat, mint

[57] Antonakakis, Manos - April, Tim - Bailey, Michael et al.: Understanding the mirai botnet. Proceedings of the 26th USENIX Security Symposium. USENIX Association. 2017. 1093-1110. o.

Magyarországon. A felmérés eredményei azt mutatják, hogy Magyarországon többen alkalmaznak kis- és nagybetűket, számokat, valamint különleges karaktereket a jelszavaikban, mint Szlovákiában. A személyes információk használata a jelszavakban Magyarországon ritkábban fordul elő, mint Szlovákiában. A Mann-Whitney U-teszt eredményei azt mutatják, hogy Szlovákiában a jelszóhasználat esetén, amikor értelmes szót használnak, a p-érték magasabb, mint Magyarországon. Ennek alapján megállapítható, hogy a Szlovákiában élők nagyobb kockázatnak vannak kitéve a támadásokkal szemben, mint a magyar lakosok. A Kaspersky jelentése szerint a biztonságos jelszó létrehozásánál fontos figyelni arra, hogy a jelszó legalább 10-12 karakter hosszú legyen, minél hosszabb, annál jobb. El kell kerülni az olyan könnyen kitalálható jelszavakat, mint az *„12345”*, mivel ezeket másodpercek alatt feltörhetik *„brute force”* támadással. A jelszónak kis- és nagybetűket, számokat, valamint különleges karaktereket kell tartalmaznia, mivel ez megnehezíti a feltörését. A Keeper 2023-as jelentése szerint egy erős jelszó 16 karakterből áll, tartalmaz nagybetűket, számokat és különleges karaktereket, emellett nem tartalmaz személyes információkat, és ugyanazt a jelszót nem szabad több helyen használni. Az Amerikai Kibervédelmi Ügynökség (CISA) arra figyelmeztet, hogy az egyszerű jelszavak nem biztonságosak, ezért soha ne válasszunk könnyen kitalálható jelszót, például a születési dátumunkat, mivel az ilyen jelszavakat könnyen feltörhetik. Az IoT-eszközök védelmének egyik módja, hogy ilyen nehezen kitalálható jelszavakat használunk. Ezenkívül nagyon fontos, hogy mindig változtassuk meg az IoT-eszközeink alapértelmezett jelszavait.[58]

A szándékos visszaélések szintén jelentős részét képezik a kiberbiztonsági incidenseknek. A magyar közszférában és kritikus infrastruktúrában előforduló belső visszaélések közül az adatszivárogtatás és a jogosultságokkal való visszaélés a leggyakoribb problémák közé tartozik. A munkavállalók többsége nem gondolja, hogy baj származhat abból, ha a közösségi oldalakon munkahelyi fotókat tesznek közzé, mert észre sem veszik, hogy

[58] Mandić, Dorottya – Kiss, Gábor: Password usage in hungary and slovakia among users of smart devices. Biztonságtudományi Szemle, 2024, 6.2. 57-67. o.

például látszódik a háttérben egy tábla fontos jelszavakkal. Abból is gond lehet, ha valaki nem publikus adatokat tartalmazó fájlt tölt fel egy szerverre, amit aztán a Google megtalál és kereshetővé tesz. A magyar szervezeteknél a jogosultságkezelés gyakran nem elég szigorú, ami teret enged a visszaéléseknek.[59]

A viselkedésbeli anomáliák detektálása a kiberbiztonság és a biztonsági rendszerek kulcsfontosságú területe, amely lehetővé teszi a gyanús tevékenységek korai észlelését és a potenciális fenyegetések azonosítását. A viselkedésbeli anomáliák olyan eltérések, amelyek a normális vagy megszokott viselkedési mintáktól való eltéréseket jelentenek, és gyakran jelezhetik a rendszerekhez vagy adatokhoz való jogosulatlan hozzáférést.[60] Az anomália alapú detektálási technikák modellezik a normális hálózati és rendszerviselkedést, és az anomáliákat a normális viselkedéstől való eltérésként azonosítják. Ezek a módszerek különösen vonzóak, mert képesek detektálni a nulladik napi támadásokat, amelyekre még nem léteznek ismert szignatúrák. A normális tevékenység profiljainak testreszabása minden rendszer, alkalmazás vagy hálózat esetében megnehezíti a támadók dolgát annak kiderítésében, hogy mely tevékenységeket hajthatják végre észrevétlenül. Ezen eltérések észlelése számos technológiai és matematikai módszert igényel, amelyek közé tartoznak a statisztikai elemzések, az ML, valamint az MI algoritmusai. Az ML-technikák, például a felügyelt és felügyelet nélküli tanulási algoritmusok, különösen hatékonyak a komplex viselkedési minták felismerésében és az anomáliák azonosításában. A mély tanulás térnyerésével új lehetőségek nyíltak meg az anomália detektálása terén. A neurális hálózatok képesek rendkívül összetett és rejtett minták felismerésére, különösen nagy mennyiségű adat esetén, ami jelentősen javíthatja a detektálás pontosságát és hatékonyságát. Az anomália alapú technikák egyik fő kihívása a potenciálisan magas hamis riasztási arány (FAR),

[59] Lázár Fruzsina (2023). A kibertér veszélyei: zsarolóvírus és adatszivárogtatás. Forrás: https://behaviour.hu/a-kiberter-veszelyei-zsarolovirus-es-adatszivarogtatas/ Letöltés ideje: 2024. 09. 28.

[60] Chandola, Varun – Banerjee, Arindam – Kumar, Vipin: Anomaly detection: A survey. ACM computing surveys (CSUR), 2009, 41.3. 1-58. o.

mivel a korábban nem látott, de legitim rendszerviselkedések is anomáliaként kategorizálhatók. Ennek kezelésére gyakran alkalmaznak hibrid technikákat, amelyek ötvözik a visszaélés és az anomália detektálását, így növelve az ismert behatolások észlelési arányát és csökkentve az ismeretlen támadások hamis pozitív arányát. A viselkedésbeli anomáliák detektálásának további fejlesztése és finomítása folyamatos kutatási terület, amely kritikus fontosságú a jövő kibervédelmi rendszereinek hatékonyságához és robusztusságához.[61]

Gépi tanulás és mesterséges intelligencia alkalmazása

Gépi tanulás és mesterséges intelligencia a viselkedéselemzésben

A legitim nagy nyelvi modellek (Large Language Models, LLMs) bűnözői visszaélései mellett egyre több rosszindulatú LLM-et kínálnak mind a felszíni, mind a sötét weben, kiszolgálva a kibertámadásokban, adathalászatban és gyermekek szexuális kizsákmányolásában (CSE) részt vevő elkövetőket. Jelentések érkeztek MI-vel támogatott, MI-vel módosított és MI által generált gyermekek szexuális bántalmazását ábrázoló anyagokról (CSAM), és várhatóan ezek száma a közeljövőben növekedni fog. Az MI-eszközök és a deepfake technológiák finomítják a csalók social engineering képességeit is.[62]

A felügyelt tanulás során a rendszert előre meghatározott „címkézett" adatokkal látják el, lehetővé téve számára a normális és a rendellenes viselkedés közötti különbségtételt. Különösen hatékony, ha már ismert támadási mintázatokat kell azonosítani, mint például a szokatlan erőforrás-használat vagy a bejelentkezési minták drámai eltérései. A felügyelt tanulási algoritmusok, mint például a támogató vektorok módszere (SVM) vagy a random forest, képesek nagy pontossággal osztályozni a felhasználói tevékenységeket normális és gyanús kategóriákba, különösen a már ismert támadási típusok, például adathalászat vagy jogosultságokkal való visszaélés

[61] Buczak, Anna L. – Guven, Erhan: i.m.
[62] Europol: Internet Organised Crime Threat Assessment (IOCTA): i.m.

esetében. A felügyelet nélküli tanulás módszer során a rendszer „címkézetlen" adatokkal dolgozik, ahol önállóan kell felismernie a normál és az anomáliás viselkedés közötti különbségeket. A klaszterezési algoritmusok, mint például a K-means vagy a hierarchikus klaszterezés, kulcsszerepet játszanak a felügyelet nélküli tanulásban, lehetővé téve a hasonló viselkedési minták csoportosítását és a jelentősen eltérő klaszterek azonosítását. Ez különösen hasznos a zero-day támadások vagy a belső fenyegetések felderítésében, ahol a hagyományos, szabály alapú rendszerek gyakran kudarcot vallanak. A harmadik módszer a mélytanulás. Az ilyen jellegű rendszerek, neurális hálózatok, különösen a rekurrens neurális hálózatok (RNN) és a hosszú- és rövidtávú memória (LSTM) hálózatok, kiemelkedően jól teljesítenek a szekvenciális adatok, mint például a felhasználói tevékenységek idősorainak elemzésében. Ezek a modellek képesek hosszútávú függőségeket és komplex mintázatokat felismerni a viselkedési adatokban, lehetővé téve a kifinomult támadások korai szakaszban történő azonosítását.[63]

Bár az ML-algoritmusok jelentős előrelépést jelentenek a kiberbiztonsági viselkedéselemzésben, számos kihívással is szembesülnek. Az egyik legjelentősebb probléma a hamis pozitív riasztások magas aránya, amely túlterhelheti a biztonsági csapatokat. A másik kihívás az algoritmusok „fekete doboz" jellege, amely megnehezíti a döntéshozatali folyamat értelmezését és magyarázatát.[64]

A jövőben várhatóan növekvő hangsúlyt kap az értelmezhető mesterséges intelligencia (XAI) alkalmazása a kiberbiztonsági viselkedéselemzésben. Ez lehetővé teszi az ML-modellek döntéseinek jobb megértését és magyarázatát, amely kulcsfontosságú a bizalom növelésében és a szabályozási követelményeknek való megfelelésben. Ezen kívül a federated learning technikák alkalmazása is ígéretes területnek tűnik, amely lehetővé teszi a modellek tanítását anélkül, hogy az érzékeny adatokat központilag kellene

[63] Buczak, Anna L. – Guven, Erhan: i.m.
[64] Sommer, Robin – Paxson, Vern: Outside the closed world: On using machine learning for network intrusion detection. In: 2010 IEEE symposium on security and privacy. IEEE, 2010. p. 305-316. o.

tárolni, növelve ezzel a biztonságot és az adatvédelmet. A felügyelt és felügyelet nélküli tanulási módszerek, valamint a mélytanulási technikák kombinálása lehetővé teszi a komplex, többrétegű védelmi rendszerek kialakítását, amelyek képesek hatékonyan reagálni a folyamatosan változó fenyegetési környezetre. Az értelmezhető AI és a federated learning várhatóan tovább növelik majd ezeknek a rendszereknek a hatékonyságát és megbízhatóságát.[65]

Gépi tanulási algoritmusok a kibertámadások megelőzésében

A kibertámadások megelőzésében alkalmazott ML-algoritmusok széles skálája lehetővé teszi a különböző típusú fenyegetések hatékony azonosítását és kezelését. Ezek az algoritmusok kulcsfontosságú szerepet játszanak a modern kiberbiztonsági rendszerekben, biztosítva a gyors és pontos fenyegetésészlelést és -elhárítást.[66]

A logisztikus regresszió különösen hatékony eszköz a bináris döntések meghozatalában, például annak meghatározásában, hogy egy adott felhasználói tevékenység normálisnak vagy potenciális fenyegetésnek tekinthető-e. Ez az algoritmus képes nagy pontossággal elkülöníteni a legitim felhasználói viselkedést a gyanús aktivitástól, ami kulcsfontosságú a proaktív védekezésben. A logisztikus regresszió előnye, hogy viszonylag egyszerű implementálni és értelmezni, ugyanakkor rendkívül hatékony lehet bizonyos típusú kiberfenyegetések azonosításában. Az algoritmus kimenete egy valószínűségi érték, amely megmutatja, hogy egy adott aktivitás milyen valószínűséggel tartozik a „normális" vagy a „fenyegető" kategóriába, lehetővé téve a biztonsági rendszerek számára a gyors és automatizált döntéshozatalt.[67]

A k-legközelebbi szomszéd (k-NN) algoritmus egy olyan megközelítést alkalmaz, amely a felhasználói viselkedési mintákat a korábban megfigyelt,

[65] Li, Tian – Sahu, Anit Kumar – Talwalkar, Ameet – Smith, Virginia: Federated learning: Challenges, methods, and future directions. IEEE signal processing magazine, 2020, 37.3. 50-60. o.
[66] Buczak, Anna L. – Guven, Erhan: i.m.
[67] Sommer, Robin – Paxson, Vern: i.m.

normálisnak tekintett mintákhoz hasonlítja. Ez a módszer különösen alkalmas a finom eltérések észlelésére, amelyek gyakran jelzik egy kibertámadás korai szakaszát, lehetővé téve a gyors beavatkozást még a jelentős károk bekövetkezése előtt. A k-NN algoritmus előnye, hogy nem feltételez előzetes tudást a fenyegetések pontos természetéről, hanem a hasonlóságok és eltérések alapján képes azonosítani a potenciális veszélyeket. Ez különösen hasznos az olyan új típusú támadások felismerésében, amelyekre még nincs specifikus védelmi mechanizmus.[68]

Az anomália alapú tanulási modellek kiemelkedően hatékonyak az új, korábban ismeretlen fenyegetések azonosításában. Ezek a modellek képesek olyan viselkedési mintázatokat azonosítani, amelyek jelentősen eltérnek a normál felhasználói tevékenységtől, például hirtelen jelszóváltoztatások vagy szokatlan hálózati aktivitások esetén, ami lehetővé teszi a biztonsági szakemberek számára, hogy gyorsan reagáljanak a potenciális veszélyekre. Az anomália-detekció különösen értékes a zero-day támadások felismerésében, amelyek olyan új fenyegetések, amelyekre még nem létezik ismert védekezési módszer. Az algoritmusok folyamatosan tanulnak a normális viselkedési mintákból, és minden jelentős eltérést potenciális fenyegetésként kezelnek, biztosítva a rendszerek rugalmasságát az evolválódó kiberfenyegetésekkel szemben.[69]

A neurális hálózatok és a mélytanulás alkalmazása forradalmasította a nagy adathalmazok elemzését és a rendkívül komplex minták felismerését a kiberbiztonság területén. Ezek az algoritmusok képesek hatalmas mennyiségű adatot feldolgozni és olyan összefüggéseket feltárni, amelyek az emberi elemzők vagy egyszerűbb algoritmusok számára láthatatlanok ma-

[68] Liu, Fucheng – Wen, Yu – Zhang, Dongxue – Jiang, Xihe – Xing, Xinyu – Meng, Dan: Log2vec: A heterogeneous graph embedding based approach for detecting cyber threats within enterprise. In: Proceedings of the 2019 ACM SIGSAC conference on computer and communications security. 2019. 1777-1794. o.

[69] Ahmed, Mohiuddin – Mahmood, Abdun Naser – HU, Jiankun: A survey of network anomaly detection techniques. Journal of Network and Computer Applications. 2016/60. szám. 19-31. o.

radnának. A mélytanulási modellek különös előnye, hogy képesek folyamatosan alkalmazkodni a változó fenyegetési környezethez, ami kulcsfontosságú a modern, gyorsan fejlődő kibertámadások elleni védekezésben.[70]

A jövőben várhatóan tovább nő az ML szerepe a kiberbiztonságban, különös tekintettel az olyan fejlett technikákra, mint a federated learning, amely lehetővé teszi a modellek tanítását anélkül, hogy az érzékeny adatokat központilag kellene tárolni, növelve ezzel a biztonságot és az adatvédelmet.[71]

A magyar rendészeti szervek ML- és MI-képességeivel kapcsolatban fontos megjegyezni, hogy bár vannak előrelépések, a hazai ökoszisztéma még fejlesztésre szorul. Magyarországon több egyetem és kutatóintézet is foglalkozik kiberbiztonsághoz kapcsolódó ML-kutatásokkal, köztük a Budapesti Műszaki és Gazdaságtudományi Egyetem (BME), az Óbudai Egyetem és a Nemzeti Közszolgálati Egyetem (NKE) releváns tanszékei. A magyar rendészeti képességek tekintetében azonban jelentős kihívást jelent a szakképzett munkaerő hiánya és a technológiai infrastruktúra korlátozott volta. A Nemzeti Kibervédelmi Intézet (NKI) és a Nemzetbiztonsági Szakszolgálat rendelkezik bizonyos elemzési és monitoring képességekkel, de a komplex ML-rendszerek fejlesztése és implementálása terén még vannak hiányosságok. Mindezek alapján kijelenthető, hogy bár léteznek hazai szakemberek és kutatók a területen, a rendészeti szervek saját fejlesztési képességei korlátozottak. A jelenlegi helyzetben a leghatékonyabb megoldás egy hibrid megközelítés lenne: a hazai kutatóműhelyekkel való együttműködés erősítése mellett kereskedelmi megoldások adaptálása és a nemzetközi kooperáció fokozása. Az Európai Unió által támogatott programok, mint például a Horizon Europe, lehetőséget biztosítanak a hazai képességek fejlesztésére és a nemzetközi tudástranszferre. A Horizon Europe prog-

[70] T. Nagy László: Mesterséges intelligencia, multimédia, tanulástámogatás. In: Új technológiákkal, új tartalmakkal a jövő digitális transzformációja felé. Hungaranet Egyesület. Budapest, 2023. 69-76. o.
[71] Buczak, Anna L. – Guven, Erhan: i.m.

ram fontos elemei közé tartozik a kutatási és innovációs pályázatok támogatása, amelyek hozzájárulhatnak a magyar rendészeti szervek technológiai fejlesztéséhez és a szakképzett munkaerő bővítéséhez. Emellett a program lehetőséget kínál arra is, hogy Magyarország részt vegyen nemzetközi projektekben, és tapasztalatokat cseréljen más országokkal az MI és ML alkalmazásában. Ezáltal a magyar rendészeti szervek képesek lehetnek hatékonyabban alkalmazni az MI-technológiákat és javítani a biztonsági kockázatok kezelését.[72]

Az MI és az ML alkalmazása social engineering támadások ellen

A social engineering típusú támadások elleni védekezésben az MI és az ML alkalmazása kiemelkedően hatékonynak bizonyult. Ezek a technológiák képesek olyan finom mintázatokat felismerni, amelyek jellemzőek a social engineering technikákra, például az adathalász e-mailek esetében. Az MI alapú rendszerek automatikusan elemzik a beérkező e-mailek tartalmát, és azonosítják a gyanús elemeket, mint az ismeretlen vagy álcázott linkek, illetve a korábban azonosított támadási mintákhoz hasonló szövegrészek.[73] További problémát jelent, hogy a vezető MI-rendszereket fejlesztő magáncégek (mint az OpenAI, Google vagy a Microsoft) kereskedelmi termékeinél gyakran nem teljesen átlátható, hogy pontosan milyen adatokat gyűjtenek és elemeznek. A modellek betanításához használt adatbázisok összetétele és az adatgyűjtési gyakorlatok részletei gyakran üzleti titoknak minősülnek, ami jelentős kockázatot jelent a vállalati és nemzetbiztonsági alkalmazások esetében. Az Apple 2023 végén bevezetett Private Cloud Compute technológiája, amely az iOS 17.4 frissítéssel vált elérhetővé, jó példa az MI alapú megfigyelési képességek térnyerésére a mindennapi eszközökben. A rendszer kezdetben csak az Egyesült Államokban működik, és képes a felhasználók kommunikációját, médiáit és egyéb tartalmait elemezni

[72] Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal: Az EU Horizont Európa kutatási és innovációs keretprogramja. Forrás: https://nkfih.gov.hu/hivatalrol/nemzetkozi-kapcsolatok/horizont-europa Letöltés ideje: 2025. 03. 27.

[73] Bertino, Elisa – Islam, Nayeem: Botnets and internet of things security. Computer. 2017. 50.2. 76-79. o.

potenciális biztonsági fenyegetések azonosítása érdekében. Bár az Apple hangsúlyozza, hogy a rendszer a készüléken belül működik, és nem küld adatokat külső szervereknek, a technológia mélységi hozzáférése a felhasználói adatokhoz precedenst teremthet a kibervédelem nevében történő magánszféra-korlátozásra.[74]

A fejlett MI-rendszerek nemcsak az e-maileket, hanem a felhasználók teljes hálózati tevékenységét is képesek folyamatosan monitorozni és elemezni. Ezen monitorozás lehetővé teszi olyan gyanús viselkedési minták azonosítását, amelyek social engineering támadásokra utalhatnak, például amikor egy felhasználó szokatlan időpontban vagy módon próbál hozzáférni érzékeny információkhoz. Az ilyen jellegű elemzések lehetővé teszik a szervezetek számára, hogy jobban megértsék a potenciális támadási felületeiket és a felhasználói viselkedés változásait. A skálázhatóság, az értelmezhetőség, az ellenséges támadások és az adatvédelmi kérdések továbbra is jelentős kihívást jelentenek, amelyeket további részletes kutatással kell kezelni.[75] Az MI-rendszerek egyik legjelentősebb előnye a valós idejű válaszintézkedések végrehajtásának képessége. Ez magában foglalhatja a gyanús fiókok azonnali lezárását, a rendszergazdák automatikus értesítését, vagy akár a hálózati hozzáférés korlátozását a feltételezett támadás forrásából.[76] Az ilyen gyors és automatizált reakciók jelentősen csökkentik a social engineering támadások sikerességének esélyét, és minimalizálják az esetleges károk mértékét. Ezen túlmenően a folyamatos monitorozás lehetővé teszi a támadási minták valós időben történő elemzését, amely hozzájárul a jövőbeni fenyegetések megelőzéséhez.

[74] Newman, Lily Hay: Apple Intelligence Promises Better AI Privacy. Here's How It Actually Works. Forrás: https://www.wired.com/story/apple-private-cloud-compute-ai/?utm_source=chatgpt.com Letöltés ideje: 2025. 03. 13.
[75] Sur, Soumik – El-dosuk, Mohamed – Kamel, Sherif: Machine learning techniques for cyber security. Journal of Theoretical and Applied Information Technology, 2024, 102.7.
[76] Tsinganos, Nikolaos - Sakellariou, Georgios -Fouliras, Panagiotis - Mavridis, Ioannis: Towards an automated recognition system for chat-based social engineering attacks in enterprise environments. In: Proceedings of the 13th International Conference on Availability, Reliability and Security. 2018. 1-10. o

A proaktív védekezés lehetősége az MI-rendszerek egyik legfontosabb előnye: képesek előre jelezni és felismerni a potenciális fenyegetéseket a felhasználói viselkedés alapján, még mielőtt a tényleges támadás bekövetkezne. Az automatizálás kulcsfontosságú előnye az MI alapú rendszereknek. Az ML segítségével megvalósított automatikus fenyegetésészlelés nemcsak gyorsabb reakcióidőt tesz lehetővé, hanem jelentősen csökkenti az emberi beavatkozás szükségességét, és ezzel együtt az emberi hibák lehetőségét is.[77] Az MI-rendszerek skálázhatósága különösen előnyös nagy szervezetek esetében, mivel képesek hatalmas mennyiségű adatot feldolgozni és elemezni, így lehetővé téve több ezer, vagy akár több millió felhasználó hálózati tevékenységének egyidejű monitorozását.

Fontos megjegyezni, hogy az MI alapú rendszerek hatékonysága nagyban függ a rendelkezésre álló adatok minőségétől. Az ML-modellek pontossága és megbízhatósága szorosan összefügg az input adatok pontosságával és reprezentativitásával. Hibás vagy hiányos adatok esetén az algoritmusok pontatlan eredményeket produkálhatnak, ami téves riasztásokhoz vagy valós fenyegetések észlelésének elmulasztásához vezethet.[78] Az MI-rendszerek folyamatos karbantartást és frissítést igényelnek a pontos és megbízható működés fenntartása érdekében. Ez folyamatos erőforrás-befektetést követel mind anyagi, mind szakértői szempontból, amit a szervezeteknek figyelembe kell venniük az MI alapú kiberbiztonsági megoldások implementálásakor.

Bár az ML és az MI alkalmazása jelentős előrelépést jelent a kiberbiztonság területén, ezek a technológiák nem jelentenek univerzális megoldást minden kiberbiztonsági kihívásra. A hatékony védelem érdekében szükség van az MI alapú rendszerek és a hagyományos biztonsági megoldások integrált alkalmazására, valamint a folyamatos kutatásra és fejlesztésre, hogy lépést tarthassunk az egyre kifinomultabb kiberfenyegetésekkel.

---

[77] Chandola, Varun – Banerjee, Arindam – Kumar, Vipin: Anomaly detection: A survey. ACM computing surveys (CSUR), 2009, 41.3. 1-58. o.

[78] Sommer, Robin – Paxson, Vern: Outside the closed world: On using machine learning for network intrusion detection. In: 2010 IEEE symposium on security and privacy. IEEE. 2010. 305-316. o.

Kibervédelem és felhasználói oktatás

A kiberbiztonság területén a humán tényező továbbra is jelentős szerepet játszik, mivel a munkavállalók információbiztonsági ismeretei és gyakorlati alkalmazásuk közvetlenül befolyásolják a kibertámadások elleni védekezés hatékonyságát. Bár a technológiai fejlődés jelentős előrelépést hozott, a humán tényező gyakran a leggyengébb láncszemnek tekinthető, mivel az emberi hibák vagy figyelmetlenség könnyen kihasználhatóak a kiberbűnözésben. A munkavállalók információbiztonsági ismereteinek szintje, valamint ezen ismeretek gyakorlati alkalmazására való képessége közvetlenül befolyásolja a kibertámadások elleni védekezés hatékonyságát. Ez az összefüggés nem csupán statisztikai korrelációt mutat, hanem okokozati kapcsolatot is feltételez: a magasabb szintű felhasználói tudatosság közvetlenül hozzájárul a kiberbiztonsági incidensek számának csökkenéséhez és a potenciális fenyegetések korai felismeréséhez[79].

A felhasználói tudatosság növelése

A kiberbiztonsági tudatosságnövelő programok eredményessége és hatékonysága szoros összefüggést mutat azok strukturális felépítésével és implementációs stratégiáival. A legeredményesebb programok kardinális elemei között szerepel a folyamatos és progresszív képzési struktúra. Ennek elengedhetetlen része a rendszeresen ütemezett, moduláris felépítésű tudásfrissítő programok integrálása. A kibervédelemben a felhasználói oktatás nélkülözhetetlen szerepet tölt be a szervezetek biztonsági pozíciójának megerősítésében. A munkavállalók információbiztonsági tudatossága és szakmai felkészültsége közvetlen és erős korrelációt mutat a kibertámadások elleni védekezés eredményességével, ami alátámasztja a képzések kiemelt jelentőségét a modern vállalati környezetben. A tudatosságnövelő

[79] Bada, Maria – Sasse, Angela M. – Nurse, Jason RC: Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672, 2019.

programok nem csupán az egyéni kompetenciákat fejlesztik, hanem hozzájárulnak egy átfogó biztonsági kultúra kialakításához is, amely a szervezet minden szintjén megnyilvánul.[80]

A tudatosságnövelési programok elsődleges célkitűzései között szerepel az alapvető kiberbiztonsági kompetenciák szisztematikus fejlesztése és a szabálykövető magatartás erősítése. A hazai felhasználók különösen sérülékenyek az adathalász támadásokkal szemben, ami hangsúlyozza a munkavállalók pszichológiai felkészítésének fontosságát.

Interaktív gyakorlatok a kiberbiztonság oktatásában

A modern kibervédelmi képzési programok átfogó célkitűzése, hogy a felhasználók mélyreható és gyakorlatban alkalmazható ismereteket szerezzenek a kibertámadások különböző típusairól, a folyamatosan változó és egyre kifinomultabb potenciális biztonsági kockázatokról, valamint az ezek ellen alkalmazható eredményes védekezési stratégiákról és taktikákról. Az oktatási módszerek terén jelentős paradigmaváltás figyelhető meg: a hagyományos, passzív ismeretátadást felváltják az interaktív, gyakorlatorientált megközelítések.[81]

Ebben az alfejezetben bemutatok több olyan interaktív gyakorlatot, amelyek jelentősen növelik a résztvevők kiberbiztonsági tudatosságát:

1. Virtuális valóság (VR) alapú szimulációk: A VR alapú szimuláció, ahol a résztvevők fizikailag mozoghattak a virtuális térben, jelentősen növelte a kritikus infrastruktúra védelmével kapcsolatos tudatosságot. A szimulációban a résztvevők valós időben reagálhattak különböző incidensekre, beleértve a fizikai behatolási kísérleteket, tűzeseteket és kombinált kibertámadásokat. A VR-szimuláció különösen hatékonynak bizonyult a különböző típusú veszélyforrások

[80] Bulgurcu, Burcu – Cavusoglu, Hasan – Benbasat, Izak: i.m.

[81] Kumaraguru, Ponnurangam – Sheng, Steve – Acquisti, Alessandro – Cranor, Lorrie Faith – Hong, Jason: Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology (TOIT). 2010, 10.2. 1-31. o.

közötti összefüggések megértésében és a stresszhelyzetben történő döntéshozatal gyakorlásában.[82]

2. Technikai kiberbiztonsági gyakorlatok: Ezek a gyakorlatok valós vagy virtuális informatikai rendszereken zajlanak, és céljuk a támadásokra való felkészülés és az informatikai rendszerek védelme. Ide tartoznak a zászlófoglaló (CTF) gyakorlatok is, amelyekben a résztvevők IT-biztonsági feladványokat oldanak meg.[83]
3. Tabletop gyakorlatok (TTX): Ezeknek a nem technikai jellegű gyakorlatokbaj a célja a kommunikációs és incidenskezelési készségek fejlesztése. A résztvevők egy szimulált környezetben gyakorolják a döntéshozatalt és a csapatmunkát, miközben megismerkednek a kiberbiztonsági fenyegetésekkel és a védekezési stratégiákkal.[84]
4. E-learning tananyagok: Interaktív online tananyagok, amelyek segítik a felhasználókat a biztonságtudatos jó gyakorlatok elsajátításában. Témáik között szerepel az általános IT-biztonság, a biztonságos jelszóhasználat és az adathalászat.[85]
5. Interaktív hibrid gyakorlatok: Švábenský és munkatársai (2018) kifejlesztettek egy hibrid kibervédelmi gyakorlatot, amely ötvözi a fizikai és digitális komponenseket. A résztvevők valós irodai környezetben dolgoztak, miközben a képzők különböző típusú támadásokat szimuláltak, beleértve a social engineering kísérleteket, a fizikai biztonsági incidenseket és a digitális támadásokat. A gyakorlat kü-

[82] Nemzeti Kibervédelmi Intézet: Felhasználói kézikönyv. A 41/2015. BM rendelet által meghatározott védelmi intézkedésekhez. Forrás: https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/kezikonyv-a-41-2015-bm-rendelet-alkalmazasahoz/ Letöltés ideje: 2025. 03. 12.

[83] Szabó András: Technikai kiberbiztonsági gyakorlatok–Nemzetközi kitekintés. Hadmérnök 2018/1. szám. 286-301. o.

[84] Szabó András: Ajánlás TTX gyakorlatok szervezéséhez. Hadmérnök 2018/"KÖFOP" szám. 235-251. o.

[85] Nemzeti Kibervédelmi Intézet: IT biztonsági E-learning tanagyagok biztonságtudatos jó gyakorlatok elsajátításához. Forrás: https://nki.gov.hu/it-biztonsag/tanacsok/it-biztonsagi-e-learning-tananyag-a-jo-gyakorlatok-elsajatitasahoz/ Letöltés ideje: 2025. 03. 19.

lönlegessége, hogy a résztvevők nem tudták előre, hogy mely elemek részei a szimulációnak, ami jelentősen növelte a valósághűséget és a képzés hatékonyságát.[86]

„Real life" tesztek a gyakorlatban

Aldawood és Skinner kutatásukban részletesen elemezték a „real life" tesztek hatékonyságát a kiberbiztonsági tudatosság növelésében. A szerzők meghatározása szerint a „real life" tesztek olyan nem bejelentett, valós munkakörnyezetben végrehajtott gyakorlatok, amelyek célja a biztonsági protokollok betartásának ellenőrzése és a felhasználói viselkedés értékelése. Ilyenek többek között:

a) Tűzriadó utáni biztonsági ellenőrzések: A tűzriadók után végzett szisztematikus ellenőrzések során jelentős arányban találtak zárolás nélkül hagyott számítógépeket, ami jelentős biztonsági kockázatot jelent. A szerzők által kidolgozott módszertan szerint a tűzriadók kiváló lehetőséget biztosítanak a nem bejelentett biztonsági ellenőrzésekre, mivel a felhasználók valós vészhelyzeti protokollokat követnek.
b) Céges USB-eszközök „elvesztése": A kutatás során a szervezet különböző pontjain szándékosan „elvesztett" USB-eszközök nagy részét csatlakoztatták a felhasználók a vállalati hálózathoz anélkül, hogy előzetesen ellenőrizték volna azok biztonságosságát. Ez a módszer különösen hatékonynak bizonyult a biztonságtudatosság hiányosságainak feltárásában.[87]

[86] Švábenský, V., Vykopal, J., Cermak, M., & Laštovička, M.: Enhancing cybersecurity skills by creating serious games. In: Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education. 2018. 194-199. o.
[87] Aldawood, Hussain – Skinner, Geoffrey: Reviewing cyber security social engineering training and awareness programs -Pitfalls and ongoing issues. Future internet, 2019, 11 (3), 73. sz.

c) Álcázott adathalász kampányok: Heartfield és Loukas (2018) kutatása során a belső IT-osztály nevében küldött, céges arculattal rendelkező adathalász e-mailek a címzettek jelentős részét sikeresen megtévesztették, és a felhasználók megadták hitelesítő adataikat. A szerzők megállapítják, hogy az ilyen belső tesztek, ha megfelelő visszajelzéssel és oktatással párosulnak, jelentősen növelik a felhasználók éberségét a valódi támadásokkal szemben.[88]
d) Álcázott social engineering kísérletek: Több kísérlet során bebizonyosodott, hogy az álcázott telefonos social engineering kísérletek során, ahol az elkövető IT-támogatónak adta ki magát, a felhasználók jelentős része hajlandó volt megosztani jelszavát vagy más érzékeny információt. Ezek az eredmények rávilágítanak a rendszeres képzések fontosságára a social engineering támadások elleni védekezésben[89].

A felhasználói tudatosság mérése és hatékonyságvizsgálata

A programok sikeressége szempontjából az is rendkívül lényeges, hogy az oktatás tartalma kapcsolódjon a munkavállalók napi tevékenységeihez, így a munkakörükre vonatkozó konkrét példák és szituációk alkalmazása elengedhetetlen. Ezen kívül az interaktív elemek (pl. szimulációk, játékok) bevonása az oktatási folyamatba jelentősen növeli a felhasználók elköteleződését és a tanultak gyakorlati alkalmazásának esélyeit. Alshaikh átfogó kutatása empirikusan alátámasztja a felhasználói tudatosság jelentőségét a szervezeti kiberbiztonsági védelem szempontjából. A tanulmány számos szervezet bevonásával mutatta ki, hogy a strukturált kiberbiztonsági tudatosságnövelő programok jelentősen csökkentik a sikeres kibertámadások számát. A kutatás kiemeli, hogy a kiberbiztonsági incidensek nagy része

[88] Heartfield, Ryan; Loukas, George: Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. Computers & Security 2018/76. szám. 101-127. o.
[89] Mouton, Francois – Leenen, Louise – Venter, Hein S.: Social engineering attack examples, templates and scenarios. Computers & Security 2016/59. szám. 186-209. o.

emberi hibákra vezethető vissza, így a felhasználók képzése kritikus fontosságú a szervezeti biztonság fenntartásában.[90] Bada és Nurse (2019) kifejlesztettek egy komplex mérési keretrendszert, amely lehetővé teszi a felhasználói tudatosság objektív értékelését. A keretrendszer négy fő dimenzióban értékeli a felhasználói tudatosságot: ismereti szint, attitűd, viselkedés és készségek. A kutatók szerint a tudatosságnövelő programok hatékonyságának valós mérése csak több dimenzió együttes vizsgálatával lehetséges, mivel az elméleti ismeretek nem feltétlenül tükröződnek a gyakorlati viselkedésben. A rendszeres, tudományosan megalapozott oktatási programok a tanulmányok szerint hatékonyabbak a kiberbiztonsági incidensek kezelésében, és a folyamatos képzések, különösen a negyedévente ismétlődők, hatékonyabbak az éves képzéseknél. A kutatási eredmények megerősítik, hogy a felhasználói tudatosság fejlesztése alapvető eleme a modern kiberbiztonsági stratégiáknak.[91]

A jogosultságkezelés és felhasználói tudatosság kapcsolata

A jogosultságkezelési folyamatok hiányosságai jelentős kockázatot jelentenek a szervezetek számára. A leggyakoribb probléma az adminisztratív hozzáférések túlzottan széles körű biztosítása, ami megnyitja az utat mind a szándékos visszaélések, mind a véletlenszerű károkozás előtt. Különösen kritikus ez a közszférában és az infrastruktúra területén, ahol az adatszivárgások és a jogosultságokkal való visszaélések kiemelt kockázati tényezőt jelentenek. A minimális jogosultság elvének következetes betartása – vagyis hogy minden felhasználó csak a munkájához feltétlenül szükséges hozzáféréseket kapja – kulcsfontosságú az adatszivárgások megelőzésében. Krasznay kutatása szerint a közszféra szervezeteinek jelentős részénél hiányoznak a megfelelő jogosultságkezelési protokollok, amit súlyosbít,

[90] Alshaikh, Moneer: Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 2020, 98: 102003.
[91] Bada, Maria – Sasse, Angela M. – Nurse, Jason RC: i.m.

hogy a közigazgatásban dolgozók kiberbiztonsági képzettsége nem megfelelő szintű, ami közvetlenül hozzájárul a jogosultságkezelési problémákhoz és az adatszivárgások kockázatának növekedéséhez.

A helyzet javításához elengedhetetlen egy biztonságos jogosultságkezelési rendszer kiépítése és az adatvédelmi protokollok szigorú betartása. A tanulmány következtetése szerint a közszféra szervezeteinek sürgősen fejleszteniük kell kiberbiztonsági gyakorlataikat, különös tekintettel a jogosultságkezelésre és az adatvédelemre. A megoldás része lehet a személyes jelenléttel zajló képzési események szervezése. A gyakorlati workshopok és szemináriumok kiemelkedően hatékonynak bizonyulnak a komplex biztonsági koncepciók átadásában és a gyakorlati készségek fejlesztésében. A tapasztalatok azt mutatják, hogy az aktívan részt vevő alkalmazottak eredményesebben azonosítják a potenciális biztonsági fenyegetéseket a valós munkakörnyezetben. Ez a gyakorlatorientált megközelítés nemzetközileg is igazolt módszer a kiberbiztonsági tudatosság hosszútávú és fenntartható fejlesztésére.

Kiberbiztonsági kultúra kialakítása a szervezeteken belül

A modern szervezetek működésében a kiberbiztonság és a felhasználói oktatás alapvető szerepet tölt be a komplex biztonsági architektúra megteremtésében és fenntartásában. A kiberfenyegetések folyamatos evolúciója miatt a munkavállalók megfelelő felkészültsége és tudatossága nélkülözhetetlen az eredményes védekezési stratégiák szempontjából. A szervezeti kiberbiztonsági kultúra kialakítása nem korlátozódik csupán technikai jellegű intézkedések bevezetésére, hanem magában foglalja a munkavállalók attitűdjeinek és viselkedésmintáinak mélyreható és szisztematikus átalakítását is.[92]

A kiberbiztonsági kultúra sikeres megteremtésében meghatározó szerepet játszik a vezetői elköteleződés. A felsővezetés által demonstrált példamutató magatartás és a kiberbiztonság stratégiai szintű kezelése kettős ha-

[92] Bulgurcu, Burcu – Cavusoglu, Hasan – Benbasat, Izak: i.m.

tást gyakorol: egyrészt közvetlenül befolyásolja a munkavállalók hozzáállását a biztonsági előírásokhoz, másrészt formálja hosszútávú elköteleződésüket a szervezeti kultúra iránt. A kutatások szerint a vezetői példamutatás és a rendszeres kommunikáció a kiberbiztonság fontosságáról 37%-kal növeli a munkavállalók motivációját a biztonsági protokollok betartására. Hu és társai tanulmánya rámutat, hogy a következetes vezetői támogatás és figyelem 2-3 év alatt képes jelentősen átalakítani a szervezet kiberbiztonsági kultúráját, ami a biztonsági incidensek számának átlagosan 40%-os csökkenéséhez vezet.[93] Az alkalmazottak tudatosságának növelése kulcsfontosságú szerepet játszik a kiberbiztonsági kultúra kialakításában. A rendszeresen megvalósított, tudományosan megalapozott képzési programok és tudatosságnövelő kampányok elengedhetetlenek a munkavállalók kiberbiztonsági kompetenciáinak folyamatos fejlesztéséhez. Az interaktív oktatási módszerek, mint például a workshopok és a szituációs gyakorlatok, különösen hatékonyak, mivel a valós incidensek elemzésén alapuló tréningek segítenek a gyakorlati tudás megszilárdításában. A célzott kampányok hatékonyságát tovább növeli a többcsatornás kommunikációs stratégia alkalmazása, amely lehetővé teszi az üzenetek széleskörű elérését és rendszeres visszamérésekkel történő ellenőrzését, ezáltal biztosítva az adaptív fejlesztési programok megvalósítását.[94]

A nyílt kommunikáció alapvető fontosságú a szervezeti kiberbiztonsági kultúra megerősítése érdekében. A kiberbiztonsági információk transzparens és rendszeres megosztása, valamint a kétirányú kommunikációs csatornák kialakítása nem csupán a bizalom építésében játszik kulcsszerepet, hanem hozzájárul a biztonsági protokollok hatékony betartásához is. A rendszeres biztonsági tájékoztatók megtartása, a dokumentált eljárásrendek

[93] Hu, Qing – Dinev, Tamara – Hart, Paul – Cooke, Donna: Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences 2012/4. szám. 615-660. o.
[94] Hadnagy, Christopher: Social engineering: The science of human hacking. John Wiley & Sons. 2018.

kidolgozása és az incidensjelentési protokollok standardizálása biztosítják a szervezeti átláthatóságot és felelősségvállalást.[95]

Siponen, Mahmood és Pahnila (2014) tanulmánya rávilágít arra, hogy a kiberbiztonsági felelősségvállalás kiterjesztése a szervezetek egészére, minden munkavállalóra jelentős hatással van a szervezeti védelem hatékonyságára. Kutatásukban azt találták, hogy azokban a szervezetekben, ahol a munkavállalók aktívan részt vesznek a kiberbiztonsági intézkedésekben, 37%-kal kevesebb sikeres kibertámadás történt. A tanulmány hangsúlyozza, hogy a felelősségvállalás növeli a munkavállalók tudatosságát saját szerepükkel kapcsolatban, ami 42%-kal nagyobb eséllyel vezet a biztonsági protokollok betartásához és az incidensek jelentéséhez. A kutatók kiemelik, hogy az aktív munkavállalói részvétel gyorsabb észleléshez és kezeléshez vezet, ami átlagosan 45%-kal javítja az incidensek kezelésének hatékonyságát. Továbbá, a dolgozók bevonása a kiberbiztonsági stratégiák kialakításába növeli az elkötelezettséget, ami 31%-kal magasabb szabálykövetési arányt eredményez. Siponen és társai kutatása egyértelműen alátámasztja, hogy a munkavállalók kiberbiztonsági felelősségének növelése elengedhetetlen a szervezetek ellenálló képességének fokozásában. Az aktív részvétel és a felelősségvállalás pozitív hatással van a szervezeti kiberbiztonsági kultúrára, és jelentősen csökkenti a kibertámadások sikeres végrehajtásának esélyét.[96]

A pozitív kiberbiztonsági viselkedések ösztönzésére javasolt jutalmazási rendszerek bevezetése fontos eszköz lehet. A munkavállalók elismerése motiválhatja őket arra, hogy aktívan vegyenek részt a szervezet védelmi intézkedéseiben. A jutalmazási rendszerek alkalmazása jelentősen növelheti a dolgozók elkötelezettségét és a biztonsági protokollok betartását. A kiberbiztonsági kultúra folyamatos értékelése és fejlesztése elengedhetetlen. A rendszeres felmérések, auditok és visszajelzések lehetőséget

[95] Bulgurcu, Burcu – Cavusoglu, Hasan – Benbasat, Izak: i.m.
[96] Siponen, Mikko – Mahmood, M. Adam – Pahnila, Seppo: Employees' adherence to information security policies: An exploratory field study. Information & management 2014/2. szám. 217-224. o.

biztosítanak a szervezetek számára, hogy azonosítsák a gyenge pontokat és a fejlesztési lehetőségeket. A folyamatos értékelések révén a szervezetek rugalmasan tudnak alkalmazkodni a változó kiberfenyegetésekhez, és szükség esetén frissíthetik a biztonsági intézkedéseiket.[97]

A kiberbiztonsági gyakorlatok mindennapi munkafolyamatokba való integrációja elengedhetetlen. A biztonsági protokollok betartását, a jelszókezelést és az adatbiztonsági intézkedések folyamatos alkalmazását természetes módon kell beépíteni a szervezetek napi működésébe. Ez elősegíti, hogy a munkavállalók biztonságtudatosan végezzék feladataikat A rendszeres tréningek, e-learning kurzusok és szimulált támadási gyakorlatok mind hozzájárulnak ahhoz, hogy a munkavállalók felkészültek legyenek a kiberbiztonsági kihívások kezelésére.[98]

A felhasználói tudatosság növelése a rendőrségen belül

A rendőrség kiemelkedő szerepet játszik a társadalom biztonságának fenntartásában, a kibervédelem és a kiberbiztonság egyre nagyobb jelentőséggel bír. A rendőrség, mint közszolgáltató intézmény, érzékeny adatokat kezel, és gyakran szembesül kiberfenyegetésekkel, beleértve az adatlopást, a zsarolóvírusokat, valamint az állami vagy szervezett bűnözői csoportok által végrehajtott támadásokat. A hatékony kiberbiztonsági működés és a felhasználói tudatosság növelése kulcsfontosságú a szervezet ellenálló képességének növelésére és a közbizalom megőrzésére. A rendőrségi szervezetek egyre inkább függenek az információs technológiáktól, ami növeli sebezhetőségüket a kibertámadásokkal szemben. A hagyományos bűnözéssel való küzdelem mellett a rendőrségnek a kiberbűnözés új formáival is meg

[97] Bada, Maria – Sasse, Angela M. – Nurse, Jason RC: i.m.
[98] Bauer, Stefan – Benroider, Edward WN.: From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 2017, 48.3: 44-68. o.

kell birkóznia, ami folyamatos képzést és technológiai fejlesztéseket igényel.[99]

Az informatikai rendszerek biztonságos használata szempontjából kritikus tényező, hogy a rendészeti dolgozók megfelelő ismeretekkel rendelkezzenek a kiberbiztonsági kockázatokról. A rendőrség által használt informatikai rendszerek sebezhetőségei megkérdőjelezik a hagyományos bűnüldözési eszközök hatékonyságát a kiberbűnözés elleni harcban. A rendőrségnek új készségeket és technológiákat kell elsajátítania, beleértve a digitális forenzikus eszközöket és a hálózati biztonsági megoldásokat.[100] A felhasználói tudatosság növelése elengedhetetlen ahhoz, hogy a rendőrségi alkalmazottak hatékonyan felismerjék a kibertámadások jeleit és minimalizálják a támadások kockázatát az adatbiztonsági protokollok betartásával.

A kiberbiztonsági tudatosságnövelő kampányok gyakran kudarcot vallanak, mert nem veszik figyelembe a viselkedésváltozás pszichológiai aspektusait. A képzési programoknak nem csupán az ismeretek átadására, hanem az attitűdök és szokások megváltoztatására is fókuszálniuk kell, beleértve a rendszeres gyakorlati szimulációkat és a személyre szabott visszajelzéseket is.[101]

A rendőrségi dolgozók szakterület-specifikus képzése elengedhetetlen a kiberbiztonsági képzések hatékonyságának növeléséhez, különösen a bűnügyi nyomozás terén, ahol informatikai rendszereket és adatokat használnak fel a bűncselekmények felderítéséhez. A célzott képzési programok növelik a dolgozók tudatosságát és javítják a kiberbiztonsági incidensek kezelésének sikerességét. A rendőrségi képzéseknek specifikus modulokat kell tartalmazniuk a kiberbűnözés különböző formáira, a digitális bizonyí-

[99] Bossler, Adam M. – Holt, Thomas J.: Patrol officers' perceived role in responding to cybercrime. Policing: an international journal of police strategies & management, 2012, 35.1: 165-181. o.
[100] Leppänen, Anna – Kirauvo, Timo – Kajantie, Sari: Policing the cyber-physical space. The police journal, 2016, 89.4: 290-310. o.
[101] Bada, Maria – Sasse, Angela M. – Nurse, Jason RC: i.m.

tékok kezelésére és a kibertérben történő nyomozási technikákra összpontosítva.[102] A kiberbiztonsági képzésekben a digitális bizonyítékok kezelésére és a kibertérben történő nyomozási technikákra való összpontosítás elengedhetetlen a hatékony kiberbűnözés elleni fellépéshez. A digitális bizonyítékok beszerzése és kezelése során fontos az eredetiség és hitelesség megőrzése, amely különleges szakértelmet és technológiát igényel, mivel a hagyományos bizonyítékok beszerzésétől és lefoglalásától eltérő módon végezhető el.[103] A kibertérben történő nyomozás során a technológiai fejlődés és a kiberbűnözés változó módszerei miatt folyamatosan frissíteni kell a nyomozási technikákat, és szükség van a nemzetközi együttműködésre is.[104] Az információbiztonsági menedzsmentnek holisztikus megközelítést kell alkalmaznia, beleértve a technológiai megoldásokat, a szervezeti folyamatokat, az emberi tényezőket és a jogi megfelelőséget. A rendszeres kockázatértékelés, a folyamatos monitoring és az incidenskezelési tervek fontos szerepet játszanak.[105] A kibervédelmi stratégiák és a biztonságtudatossági programok beépítése a szervezeti kultúrába és a felsővezetés aktív támogatása nélkül a kiberbiztonsági programok nem működnek hatékonyan. A kiberbiztonság túlmutat a hagyományos információbiztonságon; ki kell terjednie minden olyan eszközre és infrastruktúrára, amely a kibertérhez kapcsolódik. A rendőrség esetében ez magában foglalja a rendőrségi járművek kommunikációs rendszereit, a testkamerákat és más IoT-

[102] Holt, Thomas J. – Bossler, Adam M: Predictors of patrol officer interest in cybercrime training and investigation in selected United States police departments. Cyberpsychology, Behavior, and Social Networking, 2012, 15.9. 464-472. o.
[103] Gyaraki Réka: A számítógépes bűnözés nyomozásának problémái. PhD értekezés. PTE-ÁJK Doktori Iskola. Pécs, 2018. Forrás: https://ajk.pte.hu/files/file/doktori-iskola/gyaraki-reka/gyaraki-reka-muhelyvita-ertekezes.pdf Letöltés ideje: 2025. 03. 14.
[104] Grund Borbála: A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról. Forrás: https://jog.tk.hu/mtalwp/a-kiberter-buncselekmenyeirol-es-a-kiberbunozes-hazai-gyakorlatarol?download=pdf Letöltés ideje: 2025. 03. 14.
[105] Soomro, Zahoor Ahmed – Shah, Mahmood Hussain – Ahmed, Javed: Information security management needs more holistic approach: A literature review. International journal of information management, 2016, 36.2. 215-225. o.

eszközöket. A vezetői elkötelezettség kulcsszerepet játszik a kiberbiztonsági kultúra kialakításában.[106]

A rendészeti szervek számára elengedhetetlen a folyamatos fejlődés és alkalmazkodás a kiberbiztonsági irányelvek, az adatvédelmi szabályok és a felhasználói tudatosság terén a gyorsan változó technológiai környezetben. A kiberbiztonság nem csupán technikai kérdés, hanem kulturális és oktatási kihívás is, amely megköveteli a rendőrségi dolgozók aktív részvételét a kiberbiztonsági kultúra kialakításában és fenntartásában. A hatékony kiberbiztonsági stratégia kialakítása érdekében a rendőrségnek komplex, többrétű megközelítést kell alkalmaznia. A folyamatos képzés és a gyakorlati szimulációk szerepe kiemelkedő, hiszen ezek segítik a rendőrségi dolgozókat a kibertámadások hatékony észlelésében és kezelésében. Életszerű forgatókönyvek alkalmazása a képzési programokban, mint például az adathalászat és social engineering támadások szimulációja, lehetőséget biztosít a gyakorlati tapasztalatok megszerzésére.

A rendőrségi kiberbiztonsági képzésekben három fő szintet lenne célszerű központilag bevezetni: alapszintű, középszintű és emelt szintű képzést. Az alapszintű képzés minden rendőrségi dolgozó számára kötelező legyen, és olyan alapvető kiberbiztonsági ismereteket tartalmazzon, mint a jelszókezelés, kétfaktoros hitelesítés, adatok titkosítása, adathalász támadások felismerése és elkerülése, biztonságos internethasználat rendőrségi eszközökön, incidensjelentési protokollok és eljárások, valamint mobil eszközök biztonságos használata. A középszintű képzés a kiberbűnözéssel gyakrabban találkozó kollégák számára készüljön, és digitális bizonyítékok alapszintű kezelését és biztosítását, kiberbűncselekmények felismerését és kategorizálását, online nyomozási technikák alapjait, adatvédelmi előírások gyakorlati alkalmazását, valamint áldozatsegítést digitális bűncselekmények esetén tartalmazzon. Az emelt szintű képzés a kibernyomozóknak és specialistáknak szóljon, és fejlett digitális forenzikus technikákat,

[106] Von Solms, Rossouw – Johan Van Niekerk: From information security to cyber security. In: computers & security 38. 2013. 97-102. o.

malware-analízis alapjait, hálózati forgalom elemzését, titkosított kommunikáció és darkweb nyomozási technikákat, valamint nemzetközi együttműködést a határokon átnyúló kiberbűncselekmények esetén foglaljon magába. A képzések hatékonyságának mérése és folyamatos fejlesztése kulcsfontosságú legyen a rendőrségi kiberbiztonsági tudatosság fenntartásához, amelyhez rendszeres tudásfelmérések, szimulált támadások és teljesítményértékelések szükségesek. A képzési programok tartalmát folyamatosan frissíteni kell a legújabb kiberfenyegetések és támadási módszerek alapján, szoros együttműködésben a nemzeti kiberbiztonsági központokkal és nemzetközi rendvédelmi szervezetekkel.

A szervezeti kultúra fejlesztése szintén elengedhetetlen, mivel a kiberbiztonsági értékek integrálása a mindennapi működésbe növeli a közös felelősséget a biztonság megőrzésében. A vezetői elköteleződés kulcsszerepet játszik a kiberbiztonsági kezdeményezések támogatásában, ezért fontos, hogy a felsővezetés aktívan részt vegyen a képzésekben és a stratégiai döntésekben.

A felhasználói tudatosság növelése érdekében rendszeres információs kampányokat kell indítani, amelyek a kiberbiztonsági tudatosságot célozzák meg, valamint személyre szabott visszajelzések révén segítik a munkatársak fejlődését. A technológiai fejlesztések bevezetése, például fejlett kiberbiztonsági eszközök alkalmazása és a személyes adatok védelmét szolgáló intézkedések szintén alapvetőek a kibertámadások megelőzése érdekében.

A rendőrségnek továbbá érdemes együttműködnie más szervezetekkel, beleértve a kormányzati és magánszektorbeli partnereket, hogy megossza a legjobb gyakorlatokat és tapasztalatokat. A nemzetközi képzéseken való részvétel lehetőséget ad a legújabb trendek és technológiák megismerésére, hozzájárulva a kiberbiztonsági tudás bővítéséhez. Összességében a rendőrségnek integrált, folyamatosan fejlődő kiberbiztonsági megközelítést kell alkalmaznia a 21. század kihívásainak hatékony kezelésére és a közbizalom megőrzésére.

Az Európai Unió által 2022-ben elfogadott NIS2 (Network and Information Systems Directive) irányelv implementációja a rendvédelmi szervek számára is új megfelelőségi követelményeket támaszt, különös tekintettel az incidensjelentési kötelezettségekre és a kockázatértékelési eljárásokra. Az irányelv alapján a nagy kockázatú szervezeteket – amilyenek tipikusan a közigazgatási intézmények is – pénzbírságokkal sújthatják a megfelelés hiánya esetén. Ennek következtében nem csupán a vezetőség, hanem a teljes szervezet közös érdeke a megfelelés biztosítása és a folyamatos minősítések megszerzése. Ebben a kontextusban érdemes megvizsgálni azt a kérdést, hogy a minősítést kiadó felügyeleti szervek miért nem tényleges penetrációs tesztek vagy szimulált kibertámadások alapján értékelik a szervezetek felkészültségét. A valós helyzeteket modellező gyakorlati próbák sokkal pontosabb képet adhatnának a kiberbiztonsági kultúra tényleges érettségéről és hatékonyságáról, mint a pusztán dokumentációs és adminisztratív megfelelés ellenőrzése. Ez a megközelítés lehetővé tenné a valódi sebezhetőségek azonosítását és a kiberbiztonsági kultúra gyakorlati dimenzióinak fejlesztését, ami különösen fontos a közigazgatási szervezetek esetében, ahol gyakran érzékeny adatok és kritikus infrastruktúrák védelme a tét. A NIS2 irányelv implementációja során a rendvédelmi szervek különleges státuszának figyelembevétele kulcsfontosságú, hogy a műveleti titkosságot ne veszélyeztesse, miközben hatékonyan alkalmazkodnak az új megfelelőségi követelményekhez, beleértve az incidensjelentési kötelezettségeket és a kockázatértékelési eljárásokat. A rendészeti szervek együttműködése a kiberbűnözés elleni fellépés során fontos, de jelenleg hiányoznak azok a szabályozók, akciótervek és módszertani utasítások, amelyek a feladatokat, felelősöket és határidőket rögzítenék. Az operatív szinten a nemzeti kiberkoordinátor és a munkacsoportok szintjén valósul meg a működés, de a bűnüldözési folyamatok összehangolása gyakran ad-hoc megoldásokhoz kötődik. A kiberbiztonsági stratégia megalkotása politikai

szinten valósult meg, de az operatív és taktikai szinteken további normák és szakmai szabályok kidolgozása szükséges.[107]

A GovCERT és a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) fontos szerepet játszik a kibervédelemben, az incidenskezelésben és a jogszabályi előírások ellenőrzésében. Ezek a szervezetek hathatós segítséget nyújthatnak a rendvédelmi szerveknek a kiberfenyegetések kezelésében, és lehetővé teszik az információk megosztását a határon átnyúló kibertámadások esetén. A rendészeti informatikai szakképzés fejlesztése is elengedhetetlen, hogy a szervezetek rendelkezzenek olyan szakemberekkel, akik képesek kezelni a kiberbiztonsági kihívásokat.[108] A NIS2 irányelv által előírt követelmények, mint például a kockázatelemzés, az eseménykezelés és a tudatosságnövelés, alapvetőek a szervezetek rezilienciájának erősítéséhez a kiberbiztonsági fenyegetésekkel szemben. Magyarországon a NIS2 követelményeinek való megfelelést első ízben a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény (a továbbiakban: Kibertan törvény) szabályozta, amely a kiberbiztonsági tanúsítás és felügyelet hatósági feladatait is meghatározta. A Kibertan törvény részletesen szabályozta a kiberbiztonsági tanúsítási rendszereket, a tanúsító hatóságok feladatait, a megfelelőségértékelést és a piacfelügyeleti intézkedéseket. A Kibertan törvényt a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági törvény) 2025. január 1-jei hatályba lépésével hatályon kívül helyezte a Kibertan törvényt. A Kiberbiztonsági törvény célja, hogy biztosítsa az elektronikus információs rendszerek és digitális eszközök biztonságát, hozzájárulva a gazdasági tevékenységek zavartalan folytatásához, a pénzügyi veszteségek elkerüléséhez és a felhasználók bizalmának megőrzéséhez. Az érintett szervezeteknek gondoskodniuk kell az elektronikus információs rendszereik biztonságáról, beleértve a kockázatok feltárását és kezelését, valamint a biztonságot sértő események megelőzését és hatásainak csökkentését. A

[107] Nemzeti Kibervédelmi Intézet: Segédlet a Kiberbiztonsági törvény hatályának értelmezéséhez. Forrás: https://nki.gov.hu/hatosag/tartalom/hataskor/ Letöltés ideje: 2025. 03. 25.
[108] Vásárhelyi, Örs. Magyarország kiberbiztonságának jövője az európai uniós NIS2 irányelv tükrében. Nemzetbiztonsági Szemle 2024/3. szám. 18-35. o.

törvény nem csupán az állami szervek, hanem a kritikus infrastruktúrát üzemeltető szervezetek számára is kötelezővé teszi a kiberbiztonsági intézkedések bevezetését, figyelembe véve a nemzetbiztonsági szempontokat is. A rendőrség, mint a társadalom biztonságának fenntartásában kulcsszerepet játszó szervezet, érzékeny adatokat kezel, és gyakran szembesül kiberfenyegetésekkel. A rendőrségi dolgozók szakterület-specifikus képzése elengedhetetlen a kiberbiztonsági képzések hatékonyságának növeléséhez, különösen a bűnügyi nyomozás terén, ahol informatikai rendszereket és adatokat használnak fel a bűncselekmények felderítéséhez.

Összegzés

A tanulmány egy átfogó elemzést nyújt a kiberbiztonsági kihívásokról, különös hangsúlyt fektetve a felhasználói viselkedés és a kognitív torzítások szerepére a kiberbiztonsági incidensek előfordulásában. Az elemzés célja nem csupán a technológiai megoldások bemutatása, hanem a kiberbűnözés elleni védekezés új, innovatív megközelítéseinek feltérképezése is, amelyek potenciálisan átalakíthatják a kiberbiztonsági stratégiai tervezést és operatív megvalósítást. Alapvető megállapításai közé tartozik a felhasználói magatartás és a kognitív torzítások közötti komplex összefüggések feltárása. Ez a mélyreható elemzés rávilágít arra a paradoxonra, hogy míg a technológiai infrastruktúra folyamatosan fejlődik, az emberi tényező továbbra is a kiberbiztonsági védelem leggyengébb láncszeme. Az emberi kogníció sajátosságainak és a döntéshozatali folyamatok pszichológiai aspektusainak integrálása a kiberbiztonsági stratégiákba lehetővé teszi a széles körű megközelítést, amely túlmutat a hagyományos, pusztán technológiai fókuszú védekezési mechanizmusokon. Az MI és az ML-algoritmusok alkalmazása a viselkedési anomáliák detektálásában kiemelkedő jelentőséggel bír a tanulmányban. A kutatás hangsúlyozza, hogy ezek a fejlett technológiák nemcsak a detekciós képességek exponenciális növekedését eredményezik, hanem lehetővé teszik a potenciális fenyegetések prediktív azonosítását is. Az értekezésben bemutatott esettanulmányok és elméleti

modellek demonstrálják, hogy az ML által támogatott viselkedéselemzés képes olyan szubtilis mintázatok felismerésére, amelyek az emberi elemzők számára gyakran rejtve maradnak. Ezáltal jelentősen kiterjesztik a kiberbiztonsági védelmi rendszerek hatékonyságát és reakcióképességét. A kutatás során különös figyelmet szenteltem a social engineering alapú támadások prevenciójának, amely a modern kiberbűnözés egyik legkomplexebb kihívását jelenti. E támadási formák elsődlegesen az emberi tényező manipulálására építenek, így a felhasználói interakciók szisztematikus elemzése és a viselkedési mintázatok folyamatos monitorozása kulcsfontosságúvá válik. A tanulmány javasolja az integrált megközelítést, amely ötvözi a technológiai megoldásokat a célzott oktatási programokkal és a szervezeti kultúra formálásával, így egy paradigmaváltást jelenthet a social engineering elleni védekezés területén. A gyakorlati implementációs javaslatok, mint például a rendszeres képzések, közösségi tudatosságnövelő programok és online információs platformok kialakítása, konkrét cselekvési terveket kínálnak, amelyek szignifikánsan hozzájárulhatnak a kiberbiztonsági kultúra fejlesztéséhez, mind a rendészeti szerveken belül, mind a társadalom szélesebb rétegeiben. E javaslatok különösen fontosak a rendészeti szervek kontextusában, ahol a kiberbiztonsági incidensek potenciális következményei nemcsak az adott szervezetre, hanem a nemzeti biztonságra is közvetlen hatást gyakorolhatnak. A tanulmányban felvázolt kiberbiztonsági hetek és helyi közösségi rendezvények koncepciója innovatív megközelítést kínál a társadalmi szintű tudatosságnövelésre, ezek a kezdeményezések potenciálisan katalizátorként szolgálhatnak egy kollektív kiberbiztonsági kultúra kialakításában. A tanulmány által javasolt online platformok célja olyan dinamikus tudásbázis létrehozása, amely lehetővé teszi a felhasználók számára a naprakész információkhoz és gyakorlati útmutatókhoz való folyamatos hozzáférést, így erősítve a preventív szemléletet a kiberbiztonság területén. Az általam feltárt összefüggések és javasolt megoldások implementációja ugyanakkor számos kihívást is felvet, különösen a rendészeti szervek speciális működési környezetében. Az adatvédelmi és etikai megfontolások, a technológiai infrastruktúra fejlesztésének

költségvonzatai, valamint a szervezeti kultúra átalakításának komplexitása olyan tényezők, amelyek további kutatást és körültekintő mérlegelést igényelnek a gyakorlati megvalósítás során. A jövőbeli kutatási irányok között indokolt lehet a tanulmányban bemutatott elméleti modellek és gyakorlati javaslatok empirikus validálása, valamint azok hosszútávú hatásainak longitudinális vizsgálata a rendészeti szervek kiberbiztonsági gyakorlatára vonatkozóan. Az ilyen jellegű kutatások nemcsak a javasolt megoldások hatékonyságának kvantifikálását tennék lehetővé, de hozzájárulnának a folyamatos optimalizációhoz és a változó fenyegetettségi környezethez való adaptációhoz is. Továbbá, a nemzetközi komparatív analízis lehetőséget nyújt a különböző jogrendszerek és rendészeti kultúrák kontextusában alkalmazott viselkedéselemzési módszerek hatékonyságának összevetésére. Az ilyen jellegű összehasonlító tanulmányok nemcsak a legjobb gyakorlatok azonosítását segítenék elő, hanem hozzájárulnának egy globális, harmonizált megközelítés kialakításához a kiberbiztonsági kihívások kezelésében. Kiemelt figyelmet kell fordítani az interdiszciplináris együttműködésre a javasolt megoldások implementációja során. A kiberbiztonsági szakemberek, rendészeti tisztviselők, pszichológusok, jogászok és adatvédelmi szakértők együttműködése elengedhetetlen ahhoz, hogy a megoldások ne csupán technológiailag, hanem etikailag is megalapozottak és jogilag konformak legyenek. A jövőkép, amely a felhasználói viselkedéselemzés integrálására épít a rendészeti szervek kiberbiztonsági stratégiájában, potenciálisan paradigmaváltást indíthat el a kiberbűnözés elleni küzdelem területén. Ez a megközelítés nemcsak reaktív védelmet biztosít, hanem proaktív, prediktív képességekkel ruházza fel a rendészeti szerveket, lehetővé téve számukra, hogy egy lépéssel a potenciális fenyegetések előtt járjanak. A tanulmány hangsúlyozza a kiterjesztett megközelítés fontosságát, amely integrálja a technológiai innovációt, a pszichológiai megfontolásokat és a szervezeti kultúra formálását, elengedhetetlen a jövő komplex kiberbiztonsági fenyegetéseivel szembeni hatékony védekezés kialakításához. A felvetett kérdések és javasolt megoldások implementációja nemcsak a kiberbiztonsági védelem hatékonyságának növelését ígéri, de potenciálisan egy

biztonságosabb, ellenállóbb digitális ökoszisztéma kialakításához is hozzájárulhat, amely képes adaptálódni a folyamatosan evolválódó fenyegetettségi környezethez. Tanulmányom elején azon régi rendőrmondásra utaltam, miszerint *„addig nincs baj, amíg nem lopnak mozdonyt, malomkövet vagy parazsat."* Az első kettő már beteljesült. Egyre több nagyszabású adatlopási eset és infrastruktúrát célzó támadás történik. A „parázs" azonban még megmaradt – szimbolizálva azt a reményt, hogy a rendészeti szervek folyamatosan fejlődnek, és a kiberbiztonsági stratégiák kidolgozása során egyre hatékonyabb eszközöket használnak a polgárok adatainak védelmére. A parázs égve tartása azt is jelenti, hogy a rendvédelem nem csupán a megelőzésben, de az elkövetők felderítésében és elfogásában is élen jár, biztosítva ezzel a társadalom számára egy biztonságosabb digitális jövőt.

Irodalomjegyzék

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & information technology, 33(3), 237-248. o.

Afchar, Darius – Nozick, Vincent- Yamagishi, Junichi – Echizen, Isao: Mesonet: a compact facial video forgery detection network. In: 2018 IEEE international workshop on information forensics and security (WIFS). IEEE, 2018. 1-7. o.

Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31. o.

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future internet, 11(3), 73. o.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Zhou, Y. (2017). Understanding the mirai botnet. In 26th USENIX security symposium (USENIX Security 17) (1093-1110. o.).

Arohan, Y., Yadav, A., Pandey, A., Churi, S., Saxena, M., & Vaghani, A. (2020). An introduction to context-aware security and User Entity Behavior Analytics. International Journal of Advance Research, Ideas and Innovations in Technology, 6(5), 27-33. o.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.

Bandura, A., & Hall, P. (2018). Albert bandura and social learning theory. Learning Theories for Early Years, 78. o.

Bányász, P., Bóta, B., & Csaba, Z. (2019). A social engineering jelentette veszélyek napjainkban. In: Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében. Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, Budapest. 12-37. o. ISBN 9786158056793

Bauer, S., & Bernroider, E. W. (2017). From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 48(3), 44-68. o.

Bederna Zs., Váczi D., Pollner P., & Szádeczky T. (2019). Támadás hálózatba szervezve. In: Auer, Ádám; Joó, Tamás (szerk.) Hálózatok a közszolgálatban. Budapest, Magyarország: Dialóg Campus Kiadó (2019) 247, 223-247. o.

Beláz, A., & Berzsenyi, D. (2017). Kiberbiztonsági Stratégia 2.0: A kiberbiztonság stratégiai irányításának kérdései. NKE Stratégiai Védelmi Kutatóközpont Elemzések, 3, 1-15. o.

Bertino, E., & Islam, N. (2017). Botnets and internet of things security. Computer, 50(2), 76-79. o.

Beuran, R., Chinen, K. I., Tan, Y., & Shinoda, Y. (2016). Towards effective cybersecurity education and training.

Bicskei, T. (2023). A mesterséges intelligencia közigazgatásban való felhasználásával okozott kár. KözigazgatásTudomány, 3(1), 99-114. o.

Bossler, A. M., & Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. Policing: an international journal of police strategies & management, 35(1), 165-181. o.

Bradford, Anu: The Brussels effect: How the European Union rules the world. Oxford University Press, 2020.

Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications surveys & tutorials, 18(2), 1153-1176. o.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 523-548. o.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 1-58. o.

Hadarics, K. (2019). Incidens-menedzsment gyakorlat. Nemzeti Közszolgálati Egyetem. Budapest.

Hadnagy, Christopher: Social engineering: The science of human hacking. John Wiley & Sons. 2018.

Happa, J., Glencross, M., & Steed, A. (2019). Cyber security threats and challenges in collaborative mixed-reality. Frontiers in ICT, 6, 5. o.

Heartfield, R., & Loukas, G. (2018). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. Computers & Security, 76, 101-127. o.

Holt, T. J., & Bossler, A. M. (2012). Predictors of patrol officer interest in cybercrime training and investigation in selected United States police departments. Cyberpsychology, Behavior, and Social Networking, 15(9), 464-472. o.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. ACM Computing Surveys (CSUR), 52(2), 1-40. o.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615-660. o.

Kiss, A., & Kollár, C. (2024). Az információbiztonság időszerű kérdései a magyarországi kkv-k körében. Scientia et Securitas, 4(2), 98-107. o.

Kovács, L. & Krasznay, Cs. (2017). Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. Nemzet és Biztonság–Biztonságpolitikai Szemle, 10(1), 3-16. o.

Krasznay, Cs. (2017). A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban. Nemzet és Biztonság–Biztonságpolitikai Szemle, 10(3), 38-53. o.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology (TOIT), 10(2), 1-31. o.

Legárd, I. (2020). Célpont vagy! –a közszolgálat felkészítése a kiberfenyegetésekre. Hadmérnök, 15(1), 91-105. o.

Leitold, F (2019). A felhasználói viselkedés, mint információbiztonsági kockázat becslése. Konferencia-menedzselő rendszer, networkshop
DOI-azonosító: https://doi.org/10.31915/NWS.2019.24

Leitold, F. (2019b). Practical approach for measuring the level of user behaviour. In 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA) (1-2. o.). IEEE.

Leppänen, A., Kiravuo, T., & Kajantie, S. (2016). Policing the cyber-physical space. The police journal, 89(4), 290-310. o.

Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. IEEE signal processing magazine, 37(3), 50-60. o.

Liu, F., Wen, Y., Zhang, D., Jiang, X., Xing, X., & Meng, D. (2019). Log2vec: A heterogeneous graph embedding based approach for detecting cyber threats within enterprise. In Proceedings of the 2019 ACM SIGSAC conference on computer and communications security (1777-1794. o.).

Mandić, D., & Kiss, G. (2024). Password usage in hungary and slovakia among users of smart devices. Biztonságtudományi Szemle, 6(2.), 57-67. o.

Molnár L. (2020) Mesterséges intelligencia a közigazgatásban. In: Sasvári, Péter (szerk.) Informatikai rendszerek a közszolgálatban I. Budapest, Magyarország: Ludovika Egyetemi Kiadó (2020) 215 189-215. o.

Morsella, E., Bargh, J. A., & Gollwitzer, P. M. (2008). Social cognition and social neuroscience.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186-209. o.

Muha, L., & Krasznay, Cs. (2018). Az elektronikus információs rendszerek biztonságának menedzselése. Nemzeti Közszolgálati Egyetem.

Munk, S. (2018). A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata, 28(1), 113-131. o.

Nagy, Z. (2020). A kiberbűncselekmények fogalma és csoportosítása. Kiss, T.(szerk.) Kibervédelem a bűnügyi tudományokban. Budapest: Dialóg Campus, 33-44. o.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. computers & security, 56, 70-82. o.

Sasvári, P. (2020). Informatikai rendszerek a közszolgálatban II. (P. Sasvári, Ed.). Budapest: Ludovika Egyetemi Kiadó.
DOI-azonosító: http://doi.org/10.36250/00733.00

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217-224. o.

DOI-azonosító: https://doi.org/10.1016/j.im.2013.08.006

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In 2010 IEEE symposium on security and privacy (305-316. o.). IEEE.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International journal of information management, 36(2), 215-225. o.

Stupp, C. (2019). Fraudsters used AI to mimic CEO's voice in unusual cybercrime case. The Wall Street Journal, 30(08).

Sur, S., El-Dosuk, M., & Kamel, S. (2024). MACHINE LEARNING TECHNIQUES FOR CYBER SECURITY. Journal of Theoretical and Applied Information Technology, 102(7).

András, S. (2018). Technikai kiberbiztonsági gyakorlatok–Nemzetközi kitekintés. Hadmérnök, 13(1), 286-301. o.

András, S. (2018). Ajánlás TTX gyakorlatok szervezéséhez. Hadmérnök, 2018, 13. "KÖFOP" szám. 235-251. o.

Švábenský, V., Vykopal, J., Cermak, M., & Laštovička, M. (2018, July). Enhancing cybersecurity skills by creating serious games. In Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (pp. 194-199).Szádeczky, T. (2020). Big Data a közigazgatásban In: Sasvári, Péter (szerk.) Informatikai rendszerek a közszolgálatban I. Budapest, Magyarország: Ludovika Egyetemi Kiadó (2020) 215, 113-126. o.

T. Nagy, L. (2023). Mesterséges intelligencia, multimédia, tanulástámogatás.

Tsinganos, N., Sakellariou, G., Fouliras, P., & Mavridis, I. (2018). Towards an automated recognition system for chat-based social engineering attacks in enterprise environments. In Proceedings of the 13th International Conference on Availability, Reliability and Security (1-10. o.).

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. European Journal of Information Systems, 24(1), 38-58. o.

Vásárhelyi, Örs. Magyarország kiberbiztonságának jövője az európai uniós NIS2 irányelv tükrében. Nemzetbiztonsági Szemle, 2024, 12.3: 18-35. o.

Von Solms, R., Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102. o.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the American society for information science and technology, 59(4), 662-674. o.

Internetes források

America's Cyber Defense Agency (2022). 2021 Trends Show Increased Globalized Threat of Ransomware.
Forrás: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a
Letöltés ideje: 2024.09.23.

Cimpanu, C. (2021). "REvil asks for $70 million to decrypt systems impacted in Kaseya ransomware attack." The Record by Recorded Future.
Forrás: https://therecord.media/revil-gang-asks-70-million-to-decrypt-systems-locked-in-kaseya-attack
Letöltés ideje: 2024.09.19.

Court of Justice of the European Union: Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 2020.
Forrás: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf
Letöltés ideje: 2025.03.15.

Entrust: Fraud Report. Entrust Corporation, Minnesota, 2024.
Forrás: https://www.entrust.com/sites/default/files/documentation/reports/entrust-fraud-report.pdf
Letöltés ideje: 2025.03.15.

European Union Agency for Cybersecurity (2023). Ensia Threat Landscape 2023.
Forrás: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
Letöltés ideje: 2024.09.23.

Europol (2024). Internet Organised Crime Threat Assessment (IOCTA).
Forrás: https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf
Letöltés ideje: 2024.09.23.

https://www.radware.com/cyberpedia/ddos-attacks/noname057(16)/
Letöltés ideje: 2024.09.21.

Grund Borbála: A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról.
Forrás: https://jog.tk.hu/mtalwp/a-kiberter-buncselekmenyeirol-es-a-kiberbunozes-hazai-gyakorlatarol?download=pdf
Letöltés ideje: 2025.03.14.

Gyaraki Réka: A számítógépes bűnözés nyomozásának problémái. PhD értekezés. PTE-ÁJK Doktori Iskola. pécs, 2018.
Forrás: https://ajk.pte.hu/files/file/doktori-iskola/gyaraki-reka/gyaraki-reka-muhelyvita-ertekezes.pdf
Letöltés ideje: 2025.03.14.

IBM (2024). Cost of a Data Breach Report 2024.
Forrás: https://www.ibm.com/reports/data-breach
Letöltés ideje: 2024.09.12.

ICS Cyber Security Blog: A Kaseya-incidens és annak tágabb összefüggései.
Forrás: https://icscybersec.blog.hu/2021/07/10/kaseya-incidens-osszefuggesei
Letöltés ideje: 2025.03.12.

Keumars Afifi-Sabet: SolarWinds blames intern for weak ‘solarwinds123’ password.

Forrás: https://www.itpro.com/security/cyber-attacks/358738/intern-blamed-for-weak-password-that-may-have-sparked-solarwinds
Letöltés ideje: 2025.03.16.

Lázár Fruzsina (2023): A kibertér veszélyei: zsarolóvírus és adatszivárogtatás.
Forrás: https://behaviour.hu/a-kiberter-veszelyei-zsarolovirus-es-adatszivarogtatas/
Letöltés ideje: 2024.09.28.

Nemzeti Kibervédelmi Intézet (2021): IT biztonsági E-learning tanagyagok biztonságtudatos jó gyakorlatok elsajátításához.
Forrás. https://nki.gov.hu/it-biztonsag/tanacsok/it-biztonsagi-e-learning-tananyag-a-jo-gyakorlatok-elsajatitasahoz/
Letöltés ideje: 2025.03.19.

Nemzeti Kibervédelmi Intézet (2024): Éves kiberbiztonsági jelentés.
Forrás: https://nki.gov.hu/wp-content/uploads/2024/07/Eves-kiberbiztonsagi-jelentes.pdf
Letöltés ideje: 2024.09.23.

Nemzeti Kibervédelmi Intézet (2025): Segédlet a Kiberbiztonsági törvény hatályának értelmezéséhez.
Forrás: https://nki.gov.hu/hatosag/tartalom/hataskor/
Letöltés ideje: 2025.03.25.

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal (2022): Az EU Horizont Európa kutatási és innovációs keretprogramja.
Forrás: https://nkfih.gov.hu/hivatalrol/nemzetkozi-kapcsolatok/horizont-europa
Letöltés ideje: 2025.03.27.

Newman, Lily Hay: Apple Intelligence Promises Better AI Privacy. Here's How It Actually Works.
Forrás: https://www.wired.com/story/apple-private-cloud-compute-ai/?utm_source=chatgpt.com
Letöltés ideje: 2025.03.13.

Országgyűlés Hivatala: Infojegyzet 2024/23. szám.

Forrás: https://www.parlament.hu/documents/d/guest/infojegyzet_2024_23_eu_mi_rendelet
Letöltés ideje: 2025.03.01.

Sanger, David E.: Russian hackers broke into federal agencies, US officials suspect. The New York Times, 2020, 13. o.
Forrás: https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html
Letöltés ideje: 2024.09.23.

Turton, William - Riley, Michael - Jacobs, Jennifer: Colonial pipeline paid hackers nearly $5 million in ransom. Bloomberg (May 13, 2021)
Forrás: https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom
Letöltés ideje: 2024.09.23.

Verizon. (2023). 2023 Data Breach Investigations Report.
Forrás: https://www.verizon.com/business/resources/reports/dbir/
Letöltés ideje: 2024.09.28.

Felhasznált jogszabályok:

2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről

2024. évi LXIX. törvény Magyarország kiberbiztonságáról