125 Gábor Dénes Emlékév

Erasmus+

FSFT2026

THE FUTURE OF SECURITY
THE FUTURE OF TRUST

ABSZTRAKTKÖTET

FSFT2026

THE FUTURE OF SECURITY
THE FUTURE OF TRUST

TARTALOMJEGYZÉK

DENNIS GABOR UNIVERSITY

DIGITAL HORIZONS

09:15-10:00 REGISZTRÁCIÓ

10:00-10:10 REKTORI KÖSZÖNTŐ (DR. ZIMÁNYI KRISZTINA, PLENÁRIS TEREM/GÁBOR DÉNES TEREM)

10:10-12:10 PLENÁRIS ELŐADÁSOK (PLENÁRIS TEREM/GÁBOR DÉNES ELŐADÓ)

10:10-10:30 • **Bor Olivér**, kiberbiztonsági menedzser, Ernst & Young Tanácsadó Kft.

10:30-10:50 • **Rónaszéki Péter**, ügyvezető, partner, FORTIX Consulting Kft. - From Compliance to Trust: Why Security Only Works When People Change

10:50-11:10 • **Szekeres Béla**, CISA, Expert Security Ltd. - Early Detection of IT Security Incidents

11:10-11:30 • **Dellei László György**, Információbiztonsági vezető, Pécsi Tudományegyetem - Ghost in the Machine: AI Agents in SOC

11:30-11:50 • **Dr. Monika Nowikowska online**, Assistant Professor, War Studies University - A Redefinition of the Concept of Information in Cyberspace

11:50-12:10 • **Dr. Zsuffa András**, CISO, Rufusz Computer Zrt. - The Cyber-Gap Is Opening

12:10-13:00 EBÉDSZÜNET (I. EMELET)

13:00-13:20 • **Dr. Tóth Tamás**, osztályvezető, Nemzetbiztonsági Szakszolgálat - Az infokommunikáció fejlődésének egyes biztonsági aspektusú kihívásai

13:20-14:10 • **Bagi Tamás, Hatvani István, Keszthelyi Dániel, Panyi Zsolt**, Panel beszélgetés

14:10-14:30 • **Suti Péter**, AEGIS: MI-alapú NIS2 megfelelőség-menedzsment - a megbízható, zárt kibervédelmi irányítás felé

14:30-15:00 KÁVÉSZÜNET (I. EMELET)

15:00-17:00 SZEKCIÓK

15:00-17:00 - 1. DIGITAL TRUST FRONTIERS (SZEKCIÓ1/GÁBOR DÉNES ELŐADÓ)

SZEKCIÓVEZETŐ: DR. ZSUFFA ANDRÁS

- **Fehér Sándor**, Vezérigazgató · White Hat IT Security - From Privileged Users to AI Agents: Emerging Attack Surfaces and Detection Challenges in Cybersecurity
- **Dr. Bács Zoltán Görgy** - Dynamic Risk Analysis and Assessment System with Predictive Capabilities for Crime Prevention
- **Fülöpné Bártfai Fanni** - Critical Infrastructures - Resillusion?
- **Vukovics Árpád online** - Cybersecurity of Space Infrastructure
- **Gulyás István** - The Significant Cybersecurity and Digital Trust Challenges of Virtual Reality (VR)
- **Dr. Zsuffa András**, Szekcióvezet - Zárás

15:00-16:40 - 2. ADAPTÍV KIBERVÉDELEM (SZEKCIÓ2/NEMES TIHAMÉR TEREM)

SZEKCIÓVEZETŐ: DR. BERKE JÓZSEF

Å Szabó Lajos - Kvantum számítógépek kiberbiztonsági kockázatai, a mesterséges intelligencia kiberbiztonsági aspektusai

Å Sági Gábor János - A mesterséges intelligencia kettős szerepe a kiberbiztonságban: támadás és védelem

Å Miklós Márton - AI-Quantum ütközés korszaka

Å Dr. Horváth Ferenc - Új képzési módszerek alkalmazásának tapasztalatai egy technológia központú információgyűjtő szervezetnél

Å Dr. Máté István Zsolt - Kiberbiztonság az igazságügyi informatikában - az igazságügyi informatika kiberbiztonsága: módszertani szinergiák a NIS2 korszakában

15:00-16:40 - 2. ADAPTÍV KIBERVÉDELEM (SZEKCIÓ3/TRÉNINGTEREM)

SZEKCIÓVEZETŐ: DR. KOZMA-BOGNÁR VERONIKA

- **Belinszki Zoltán** - Védeni a védhetetlent?
- **Gulyás Zsuzsa** - A kiberbiztonság vakfoltja - az értelmezési sérülékenység, mint strukturális kockázat a technikai megfelelés határain túl
- **Irányi Csaba** - Az AI pipeline árnyoldala: kiberbiztonsági fenyegetések a modellezési folyamatban
- **Dr. Berek László** - Az online tudományos kommunikáció, mint kritikus digitális bizalmi infrastruktúra
- **Laska Pál Károly** - Az információbiztonsági tudatosság mérésének modernizációja és nagymintás empirikus validálása

PLENÁRIS ELŐADÁSOK

SZABÁLYOZÁSTÓL A REZILIENCIÁIG: A NIS2 IMPLEMENTÁCIÓJÁNAK GYAKORLATI TAPASZTALATAI

Bor Olivér
Manager, EY, Doktorandusz, NKE HDI, oliver.bor@hu.ey.com

Absztrakt: A kiberfenyegetések gyors ütemű fejlődése alapvetően átírta a szervezeti kiberbiztonsági kockázatok természetét és kezelésének logikáját. Az ENISA 2025-es fenyegetettségi jelentése szerint az európai DDoS-támadások száma az előző évhez képest 85%-os növekedést mutat, miközben a támadók egyre kifinomultabb, többfokozatú módszereket alkalmaznak, amelyek célja az incidenskezelő csapatok figyelmének elterelése párhuzamosan zajló, komolyabb behatolásokról (ENISA, 2025). Eközben a PurpleSec adatai arra utalnak, hogy a kibertámadások közel 98%-a valamilyen pszichológiai manipulációs technikára épít, ami az emberi tényező megkerülhetetlen szerepét hangsúlyozza a kiberbiztonsági védekezésben (PurpleSec, 2024). A kiberbűnözés globális gazdasági kára 2026-ban várhatóan megközelíti a 9,5 billió dollárt, ami a kritikus infrastruktúrák és az összekapcsolt digitális ökoszisztémák védelmét stratégiai prioritássá emeli (Bor, 2025b).

Ebben a kontextusban az Európai Unió 2022/2555 számú irányelve – a NIS2 – nem csupán szabályozási mérföldkövet jelent, hanem a kiberreziliencia felé mutató stratégiai szemléletváltás katalizátora is. Az irányelv magyarországi implementációját a 2024. évi LXIX. törvény valósítja meg, amely a korábbi, szűk állami fókuszú Ibtv.-vel szemben paradigmaváltást képvisel: egy proaktív, kockázatalapú, auditálható és incidenskezelés-orientált kiberbiztonsági ökoszisztémát teremt, amely az állami és magánszféra szereplőit egyaránt érinti (Bor, 2025a). A köz-magán együttműködések – mint a kollektív kiberreziliencia meghatározó eszközei – e keretrendszerben különös jelentőséget kapnak, ugyanakkor hatékony működésük kizárólag világos jogi, intézményi és szervezeti feltételek fennállása esetén biztosítható (Bor, 2025b).

Az előadás három tematikus tengelyen épül fel. Először áttekinti a jelenlegi kiberbiztonsági fenyegetettségi trendeket, különös tekintettel az ellátási lánc sérülékenységeire, az emberi tényező kitüntetett szerepére és a hibrid fenyegetések megjelenésére. Ezt követően bemutatja a NIS2 irányelv lényegi elemeit, szabályozási logikáját és a magyar implementáció sajátosságait. Az előadás harmadik, gyakorlati részében NIS2-felkészítési és auditálási tapasztalatok kerülnek bemutatásra: milyen tipikus szervezeti, eljárási és tudatossági hiányosságokkal szembesülnek az érintett szervezetek a megfelelőség elérése és fenntartása során. Az előadás konklúziója szerint a szabályozói megfelelőség szükséges, de

önmagában nem elégséges feltétele a valódi szervezeti rezilienciának: a hosszú távú ellenálló képesség kialakítása folyamatos kockázatértékelést, intézményes tudatosságfejlesztést és stratégiai szemléletet igényel, amelynek alapjait az empirikus kutatások is megerősítik (Palicz et al., 2022; Bor, 2025a).

Kulcsszavak: NIS2, kiberbiztonság, kiberreziliencia, kockázatkezelés, audit

IRODALOMJEGYZÉK

1. Bor, O. (2025a). Szabályozási szemléletváltás: A NIS2 hatása a magyar kiberbiztonsági szabályozásra. Hadmérnök.
2. Bor, O. (2025b). Kiberfenyegetések és kollektív védelem: nemzeti és nemzetközi kötelezettségek, együttműködések. Szakmai Szemle.
3. ENISA. (2025). ENISA Threat Landscape 2025. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
4. Palicz, T., Bonnyai, T., Bencsik, B., Pintér, L., Hornyik, Zs., Joó, T., Bor, O., & Dombrádi, V. (2022). Biztonságtudatosság a kibertérben – a 2020-as országos lakossági felmérés eredményei. Belügyi Szemle.
5. PurpleSec. (2024). 2024 cyber security statistics: The ultimate list of stats, data & trends. https://purplesec.us/resources/cyber-security-statistics
6. Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) a hálózati és információs rendszerek biztonságáról (NIS2 irányelv). Az Európai Unió Hivatalos Lapja, L 333, 80–152.
7. 2024. évi LXIX. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről (Kibertv.). Magyar Közlöny, 2024/101.
8. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.). Magyar Közlöny, 2013/79.

SZELLEM A GÉPBEN: AI ÜGYNÖKÖK A SOC-BAN

DELLEI László György
CISO, University of PÉCS, dellei.laszlo@pte.hu

Absztrakt: A Security Operations Centerek (SOC-ok) működése jelentős átalakuláson megy keresztül a mesterséges intelligencia térnyerésének hatására. A hagyományosan biztonsági elemzők által végzett feladatok – mint a riasztások triázsolása, események korrelációja és incidensek vizsgálata – egyre inkább AI-alapú képességekkel egészülnek ki, különösen a viselkedéselemző rendszerek (User and Entity Behavior Analytics – UEBA) esetében. Az előadás célja annak bemutatása, hogy az AI-alapú megoldások miként alakítják át a SOC működését gyakorlati nézőpontból. Röviden áttekinti azokat a területeket, ahol az automatizáció már jelenleg is kézzelfogható előnyöket biztosít, például a riasztási zaj csökkentése, az anomáliák gyorsabb felismerése és a döntéstámogatás terén. Ezzel párhuzamosan elemzi azokat a határokat is, ahol az emberi szakértelem továbbra is elengedhetetlen marad. Az előadás három központi kérdésre fókuszál: mely SOC feladatok automatizálhatók reálisan, hogyan változik a biztonsági elemző szerepe, valamint milyen kockázatokat hordoz az AI túlzott alkalmazása. Gyakorlati példákon keresztül bemutatásra kerül, hogy az AI-alapú modulok hogyan képesek bizonyos esetekben kiváltani vagy támogatni az elemzői tevékenységeket, miközben olyan kihívások is megjelennek, mint az átláthatóság, az elszámoltathatóság és a bizalom kérdése, különösen szabályozott környezetekben (pl. NIS2).

Az előadás bemutatja a „kiterjesztett SOC" (augmented SOC) koncepcióját, ahol az emberi és mesterséges intelligencia együttműködése biztosítja a hatékony és kontrollált működést, hozzájárulva a szervezeti reziliencia növeléséhez.

Kulcsszavak: SOC, mesterséges intelligencia, UEBA, kiberbiztonság, automatizáció, NIS2, incidenskezelés

BIBLIOGRAPHY

1. ENISA. (2023). Artificial Intelligence and Cybersecurity: Challenges and Opportunities.
2. European Union. (2022). Directive (EU) 2022/2555 (NIS2 Directive).
3. RSA Security. (2023). NetWitness Platform Overview and UEBA Capabilities.
4. Sarker, I. H. (2021). AI in Cybersecurity: A Comprehensive Review. Journal of Network and Computer Applications.

AZ INFORMÁCIÓ FOGALMÁNAK ÚJRAÉRTELMEZÉSE A KIBERTÉRBEN

Nowikowska Monika
Informatikai Jog Tanszékvezető, War Studies University in Warsaw,
m.nowikowska@akademia.mil.pl

Absztrakt: Az „Információ fogalmának újraértelmezése a kibertérben” című tanulmány a kommunikációs paradigma evolúciós átalakulását elemzi: a megbízhatóságon alapuló hagyományos modelltől a gyorsaság és az algoritmikus tartalomkiválasztás által meghatározott kortárs modell felé történő elmozdulást.

A szöveg fő tézise az információ szerepének átalakulása: az objektív tudást közvetítő értékhordozóból az információ egyre inkább „zajjá” válik. A digitális korban a hagyományos tekintélyek és a tényellenőrzési folyamatok jelentősége csökken, miközben az azonnaliság kerül előtérbe. Az információ a befogadó figyelmének megszerzésére szolgáló eszközzé válik.

E transzformáció egyik kulcseleme a közösségi média algoritmikus működése. Ezek elsődleges célja nem az értékes tartalmak közvetítése, hanem olyan tartalmak előnyben részesítése, amelyek erős érzelmi reakciókat váltanak ki és felhasználói aktivitást generálnak. Ennek következtében a megbízhatóság háttérbe szorul a kattintásvadász tartalmakkal szemben. E mechanizmusok az úgynevezett figyelemgazdaság jelenségéhez vezetnek, amelyben nem az üzenet minősége, hanem a felhasználó platformon eltöltött ideje jelenti a legnagyobb piaci értéket.

A szerző rámutat arra, hogy az információval túlterhelt kibertérben az egyén képtelenné válik a rendelkezésre álló adatok érdemi feldolgozására, ami felszínes befogadáshoz vezet. A tudást rövid üzenetek váltják fel. A kibertérben az információ tömegesen előállított, múlékony és kontextusától megfosztott jelenséggé válik, ami polarizációhoz és a dezinformáció terjedéséhez vezet. Ez az újraértelmezés új készségek kialakítását követeli meg a közönségtől, mivel a digitális ökoszisztémában a figyelemért folytatott küzdelem felülírja az igazság keresését.

Kulcsszavak: algoritmusok, figyelemgazdaság, kattintásvadászat, kommunikáció, dezinformáció, információ

IRODALOMJEGYZÉK

1. Malinowski, M. (2022), Algorytm rekomendacji bazujący na sesjach rekomendacji działający na podstawie zachowań użytkowników oraz atrybutów obiektów w systemie e-Commerce, Wydawnictwo Wojskowa Akademia Techniczna.
2. Nowikowska, M., Kozłowski, M. (2025), Analiza wybranych zagrożeń dla tożsamości cyfrowej wynikających z postępu technologicznego, Journal of Modern Science, no. 3, vol. 63, pp. 781-798
3. 3Noga, E. (2023), Personalizacja treści i profilowanie użytkowników: wybrane zjawiska psychometrii w serwisach społecznościowych na przykładzie Facebooka w świetle analizy piśmiennictwa, Acta Universitatis Lodziensis Folia Librorum, no 2(37), pp. 13-38.

MEGFELELÉSBŐL BIZALOM: A KIBERBIZTONSÁG CSAK AKKOR MŰKÖDIK, HA AZ EMBEREK VÁLTOZNAK

Rónaszéki Péter, CISM, CDPSE, ISO27001 LA, LI, ISO22301 LA
ügyvezető, partner, FORTIX Consulting Kft., peter.ronaszeki@fortix.hu

Absztrakt: Az elmúlt években a szervezetek jelentős erőforrásokat fordítottak kiberbiztonsági kontrollok, megfelelési keretrendszerek és tudatosságnövelő programok bevezetésére. Ennek ellenére a sikeres kibertámadások – különösen a social engineering alapú incidensek – száma folyamatosan növekszik. Ez az ellentmondás rámutat a formális megfelelés és a tényleges szervezeti ellenállóképesség közötti kritikus szakadékra.

Az előadás a megfelelés-alapú biztonsági megközelítések korlátait vizsgálja, és amellett érvel, hogy a kiberbiztonság hatékonysága végső soron az emberi viselkedésen és döntéshozatalon múlik. Valós példákon – többek között deepfake alapú csalásokon és social engineering támadásokon – keresztül mutatja be, hogy a támadók egyre inkább kognitív torzításokat, bizalmi viszonyokat és időnyomást használnak ki technikai sérülékenységek helyett.

Gyakorlati tapasztalatokra és több szervezetnél megfigyelt mintázatokra építve az előadás egy emberközpontú kiberbiztonsági szemléletet mutat be, amelyben a „bizalom” mérhető és kezelhető kockázati tényezőként jelenik meg. Rávilágít arra is, hogy a hagyományos tudatosságnövelő programok gyakran nem eredményeznek tartós viselkedésváltozást, és miért van szükség folyamatos, kontextus-alapú megközelítésre a kritikus döntési helyzetek befolyásolásához.

Az eredmények azt mutatják, hogy a szervezeteknek túl kell lépniük a megfelelésen, és viselkedésalapú megközelítést kell alkalmazniuk, amely az alkalmazottak döntéseire és reakcióira fókuszál. Ez jelentős hatással van a biztonsági programok kialakítására, a kockázatkezelésre és a vezetői felelősségvállalásra a folyamatosan változó fenyegetési környezetben.

Kulcsszavak: kiberbiztonság, digitális bizalom, emberi tényező, social engineering, deepfake, viselkedésalapú biztonság, döntéshozatal, kockázatkezelés

IRODALOMJEGYZÉK

1. Infoguard AG. (2026). Social engineering and AI: The human psyche as a target. InfoGuard Blog.
2. AwareGO. (2026). Social engineering techniques: A deep dive into the psychology of the human hack.
3. Reality Defender. (2025). The psychology of deepfakes in social engineering.

AEGIS: MI-ALAPÚ NIS2 MEGFELELŐSÉG-MENEDZSMENT – A MEGBÍZHATÓ, ZÁRT KIBERVÉDELMI IRÁNYÍTÁS FELÉ

Suti Péter
Üzletfejlesztési igazgató, Spartan Code Kft., suti.peter@spartancode.hu

Absztrakt: A folyamatosan szigorodó szabályozási környezet — a NIS2 irányelv, a GDPR, a DORA és az EU AI Act együttes hatásaként — egyre növekvő megfelelési terhet ró a különböző méretű szervezetekre. Mindeközben a kiberfenyegetések szaporodása nem csupán jogszabályi megfelelést, hanem valódi, mérhető biztonsági rezilienciát követel meg. A tanulmány a Spartan Code által fejlesztett AEGIS megfelelőség-menedzsment platformot, és annak MI-alapú NIS2 modulját mutatja be, bizonyítva, hogy a mesterséges intelligencia képes a compliance életciklust — a munkaigényes, dokumentumközpontú folyamatot — intelligens, automatizált irányítási munkafolyamattá alakítani. A NIS2 megfelelés egyik kulcskihívása a szervezeti tudás — szabályzatok, eljárások, hanganyagok és informális gyakorlatok — biztonságos, strukturált összegyűjtése, és megfelelési bizonyítékokká történő átalakítása. Az AEGIS platform ezt egy MI-ügynök alapú feldolgozási folyamaton keresztül valósítja meg, amely képes multimodális bemenetek (dokumentumok, hanganyagok, strukturált adatok) kezelésére.

A kinyert tudást egy biztonságos, strukturált intelligens adattár tárolja, majd kompetenciatérképre épülő interjú-ügynökök segítségével célirányos, strukturált értékeléseket készít az érintett stakeholderekkel. A feltárt tudás közvetlenül egy teljes körű NIS2 munkafolyamatba épül be: követelményelemzés, GAP-analízis, intézkedési terv kezelés, automatizált szabályzatgenerálás és átfogó audit-támogatás — mindezt zárt, szuverén környezetben. A hagyományos megközelítésektől eltérően, amelyek érzékeny megfelelési adatok külső auditorokkal vagy harmadik feles eszközökkel való megosztását igénylik, az AEGIS teljes körű adatszuverenitást biztosít: az auditorok kontrollált hozzáféréssel dolgoznak a platformon belül, és egyetlen érzékeny adat sem hagyja el a rendszert. Ez az architektúra egy kritikus, de kevéssé tárgyalt feszültséget old fel a kibervédelmi megfelelés területén: az átláthatóság (adatok megosztása auditorokkal és hatóságokkal) és a biztonság (érzékeny üzemeltetési adatok zártan tartása) közötti ellentmondást. Az előadás amellett érvel, hogy az MI-alapú zárt körű megfelelési rendszerek a megbízható kibervédelmi irányítás következő határát képviselik, összhangban a konferencia „A biztonság jövője — A bizalom jövője” mottójával.

Kulcsszavak: compliance menedzsment NIS2, MI-ügynök, intelligens adattár, adatszuverenitás, zárt audit környezet, automatizált szabályzatgenerálás

IRODALOMJEGYZÉK

1. European Parliament and the Council. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555
2. Lewis, J. A. (2023). Cyber Governance in an Uncertain World. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/cyber-governance-uncertain-world
3. Gao, Y., Xiong, Y., Gao, X., Jin, H., Liu, H., Xiong, Z., Li, Z., Shen, Z., Wu, F., & Wang, H. (2024). Retrieval-augmented generation for large language models: A survey. arXiv preprint arXiv:2312.10997. https://arxiv.org/abs/2312.10997
4. ENISA. (2023). NIS2 implementation: Key challenges and emerging best practices. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/nis2-implementation
5. Schmitt, P., & Flechais, I. (2023). Automated compliance: Risks and opportunities of AI-driven regulatory adherence. Computers & Security, 128, 103170. https://doi.org/10.1016/j.cose.2023.103170

IT BIZTONSÁGI ESEMÉNYEK KORAI DETEKCIÓJA

Szekeres Béla
CISA, Expert Security, bela.szekeres@xsec.eu

Absztrakt: Amelyik hálózatot fel akarják törni, azt fel is törik. A kérdés az, időben észrevesszük-e ahhoz, hogy a kárt mérsékelhessük, esetleg megelőzhessük. Sajnos a nemzetközi tapasztalatok elég rosszak, az elmúlt években a detektálás átlagos ideje nem csökkent. A szoftverfejlesztési ciklusok felgyorsultak, az informatikai rendszerek egyre komplexebbé válnak, ezek mind növelik az informatikai biztonsági sérülékenységek esélyeit. Utóbbiak kihasználására a támadóknak számos új eszköz áll rendelkezésére. Az előadásban azt járjuk körül, milyen eszközeink vannak a korai detekcióra, mik a kihívások, amikkel szembenézünk és mit tehetünk ezek leküzdésére. Kitérünk azokra a tervezési alapelvekre, amiket érdemes már az informatikai környezet kialakításakor követni. Foglalkozunk a védelmi rendszerekhez szükséges emberi erőforrásokkal, illetve azok szűkös voltának következményeivel. Kitérünk arra, hogy milyen gyakori tévképzetek élnek a döntéshozókban, és ezek a tévképzetek milyen következményekkel járnak. Az előadás végén áttekintjük, milyen változásokat hozhatnak a közelmúlt szabványai, mind pozitív, mind negatív oldalról.

Az előadás állítása az, hogy az IT biztonsági környezet kialakítása nem egy egyszeri tevékenység, hanem egy folyamatos utazás, ahol elég rosszak az esélyeink, de ha a meglevő eszközeinket ésszerűen használjuk, az esélyeink jelentősen javíthatók.

Kulcsszavak: korai detekció, SIEM, tervezett biztonság

IRODALOMJEGYZÉK

1. Yaman Roumani (2021), Detection time of data breaches https://www.sciencedirect.com/science/article/abs/pii/S0167404821003321
2. Australian Signals Directorate (2024), Identifying and Mitigating Living Off the Land Techniques https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/identifying-and-mitigating-living-off-the-land-techniques
3. Sławomir Żurawski1, Aneta Chrząszcz, et al. (2025), Effectiveness of Information Security Incident Management Systems: Identifying Practices, Challenges and Development Perspectives https://ersj.eu/journal/3922/download/Effectiveness+of+Information+Security+Incident+Management+Systems+Identifying+Practices+Challenges+and+Development+Perspectives.pdf

AZ INFOKOMMUNIKÁCIÓ FEJLŐDÉSÉNEK EGYES BIZTONSÁGI ASPEKTUSÚ KIHÍVÁSAI

Tóth Tamás
osztályvezető, Nemzetbiztonsági Szakszolgálat, toth.tamas@nbsz.gov.hu

Absztrakt: Az információs és kommunikációs technológiai környezet (IKT) fejlődésével kapcsolatos trendek közé sorolható a konnektivitás, a konvergencia, a multimodalitás, az adatvédelem erősödése, a biztonság aspektusából pedig, hogy az új diszruptív technológiák adta infokommunikációs lehetőségeket a bűnüldöző, nemzetbiztonsági szervezetek tevékenységével érintettek is alkalmazzák. Az IKT környezet biztonsági aspektusú elemzése igen összetett, komplex szemléletet követel meg, amely okán szükséges a társadalmi, technológiai, jogi és a biztonsági környezet elemzése.

A társadalmi, felhasználói trendek, tendenciák kapcsán megállapítható, hogy a Föld kb. 8,3 Mrd. lakosára 8,8 Mrd. mobil telefon jut, több mint 6 Mrd. rendelkeznek internethozzáféréssel, amely számok növekedést mutatnak, akár csak az internet használatának egységnyi ideje. A legnépszerűbb internet-fogyasztási eszközök az okos telefonok, a szolgáltatások pedig a kommunikációs alkalmazások.

A technológia környezet kapcsán látható, hogy az újgenerációs mobilkommunikációs hálózatok exponenciálisan növekvő kiszorító hatással vannak a korábbiakra, az adatátviteli sebesség, a sávszélesség és a szolgálatás lefedettségi igény növekedésével, a késleltetési idő csökkenésével, a hálózatokon megjelenő egyre heterogénebb és fejlettebb biztonsági markerekkel ellátott adatcsomagok megjelenésével. A fentiek okán 2030-ra várható a földfelszíni hírközlő hálózatok architektúrális felépítésének elmozdulása a légtér, a világűr irányába, amelyet egyrészről az okosváros ökoszisztémák elterjedése iránti igény indukálja. Az új infokommunikációs technológiák szabályozása kapcsán megjelenik a hatékonyság és az aktualitás kérdése, az adatvédelem és a biztonság értékduáljának egyensúlya, az emberi jogi fundamentalizmus térnyerése és a globális szolgáltatások okán a hatékony nemzetközi jogi szabályozás, a multi- és bilaterális együttműködés szükségessége.

A biztonsági környezet kapcsán látható, hogy az internettechnológia alapú végpont-végpont közötti titkosítást biztosító kommunikációs alkalmazások a terrorizmus, a bűnszervezetek, a szélsőséges csoportok, valamint a gyermekek szexuális kizsákmányolása kapcsán is alkalmazásra kerülnek, így az azokon végbement kommunikáció törvényes ellenőrzése össztársadalmi érdek.

A szolgáltatások globális jellege, a hálózati infrastruktúra és kriptográfia fejlődése, a hatékony szabályozás iránti igény, valamint a titkosított kommunikációs alkalmazások bűnös tevékenység során történő alkalmazása kihívásként értékelhető a törvényes kommunikációellenőrzés szempontjából, amely a biztonsági érdekekre hat negatívan. Így szükséges az eredményes nemzetközi együttműködés a szolgáltatókkal, a hatékony jogszabályi környezet kidolgozása, valamint olyan alternatív kriptográfiai megoldás kialakítása, amely egymást kiegészítve biztosítja az elvárt adatvédelmet és a biztonsági érdekek érvényesülését.

Kulcsszavak: infokommunikáció, Információs és Kommunikációs Technológiák, bűnüldözés, nemzetbiztonság, terrorizmus, szervezett bűnözés

IRODALOMJEGYZÉK

1. Tóth, T. (2024). Az IKT környezet változásainak hatásai az információgyűjtés 21. századi fejlődésére. Doktori (PhD) értekezés. NKE HDI. https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/101088
2. Kovács, Z. (2015). Az infokommunikációs rendszerek nemzetbiztonsági kihívásai. Doktori (PhD) értekezés. NKE KMDI. https://adoc.tips/az-infokommunikacios-rendszerek-nemzetbiztonsagi-kihivasai.html
3. Lapsánszky, A. (Eds.) (2013). Hírközlési-szabályozás, hírközlési-igazgatás hazánkban és az Európai Unióban. Wolters Kluwe CompLex Kiadó.

NYÍLIK A CYBER-OLLÓ

Zsuffa András
CISO, Rufusz Computer Zrt., zsuffa.andras@rufusz.hu

Absztrakt: A kiberbiztonsági fenyegetések becslésekor abból indulunk ki, hogy a védekező és a támadó képességek azonosak. Ha megvizsgáljuk a rendelkezésre álló empirikus adatokat, a valós kép ennél bonyolultabb és kellemetlenebb. Több, egymástól független forrás – iparági incidensadatok, fenyegetési riportok és mesterséges intelligencia képességmérések – azt mutatja, hogy a támadói oldal fejlődése nem lineáris, hanem gyorsuló és több dimenzióban egyszerre jelentkező. A sérülékenységek kihasználásához szükséges idő drámai módon, folyamatosan rövidül, egyes esetekben hetekről napokra vagy órákra csökken. A támadási módszerek egyre nagyobb arányban épülnek skálázható, automatizált és újrahasznosítható elemekre, miközben a támadói ökoszisztéma egyre inkább üzleti jelleggel szerveződik. Ezzel párhuzamosan a mesterséges intelligencia gyors ütemben növeli az offenzív képességeket, rövid ciklusokban bővítve az automatizálható és delegálható támadási feladatok körét. Ezek a trendek nem csupán a támadások számának növekedését jelentik, hanem a támadói képességek minőségi átalakulását: a gyorsaság, a skálázhatóság és az adaptivitás együttes erősödését. Ennek következtében a védekező oldal hagyományos, reaktív és megfelelőség-központú megközelítése strukturális hátrányba kerül. Az előadás központi állítása, hogy a „cyber-olló" nem pusztán nyílik, hanem a jelenlegi védekezési modellek mellett ennek sebessége is növekszik. A kérdés így már nem az, hogy a különbség megszüntethető-e, hanem az, hogy milyen új megközelítésekkel lehet annak növekedését lassítani, illetve a hatásait kezelhető keretek között tartani.

Kulcsszavak: Cyber-olló, támadás-automatizáció, AI, aszimmetria

IRODALOMJEGYZÉK

1. Erukude, S. T., Marella, V. C., & Veluru, S. R. (2026).AI-driven cybersecurity threats: A survey of emerging risks and defensive strategies. arXiv. https://arxiv.org/abs/2601.03304
2. Iturbe, E., Llorente-Vazquez, O., Rego, A., Rios, E., & Toledo, N. (2024). Unleashing offensive artificial intelligence: Automated attack technique code generation. Computers & Security, 147, 104077. https://doi.org/10.1016/j.cose.2024.104077
3. Zhuo, T. Y., Ding, Y., Guo, W., & Meng, R. (2026). To defend against cyber attacks, we must teach AI agents to hack. arXiv. https://arxiv.org/abs/2602.02595
4. Charan, P. V. S., Chunduri, H., Anand, P. M., & Shukla, S. K. (2023). From text to MITRE techniques: Exploring the malicious use of large language models for generating cyber attack payloads. arXiv. https://arxiv.org/abs/2305.15336

1. DIGITAL TRUST FRONTIERS

DINAMIKUS KOCKÁZATELEMZŐ ÉS -ÉRTÉKELŐ RENDSZER ELŐREJELZŐ KÉPESSÉGEKKEL A BŰNMEGELŐZÉSBEN

BÁCS Zoltán György
Adjunktus, Nemzeti Közszolgálati Egyetem, bacs.zoltan.gyorgy@uni-nke.hu

Absztrakt: A Ludovika Közszolgálati Egyetem emeritus professzora, Finszter Géza közismert kifejezése szerint a társadalom által leginkább tolerálható bűncselekmény az, amelyet egyáltalán nem követtek el. Ezt a logikát követve állítható, hogy a bűnmegelőzés a bűnüldöző szervek egyik kulcsfontosságú területe.

Mely bűncselekmények megelőzésének kellene abszolút prioritást élveznie? A válasz olyan egyszerű, mint amilyen összetett. Különböző jogi szempontok és nyomozati technikák szükségesek a zsebtolvajlás vagy a rendkívül kifinomult kiberbűnözés megelőzéséhez. A bűnüldöző szervek logikáját követve az erőfeszítéseket a nagyobb anyagi és pénzügyi károkat okozó, széles körben elterjedt bűncselekmények megelőzésére kell összpontosítani, amelyek hatással lehetnek a társadalomnak a hivatalos szervekbe, a bűnüldöző szervekbe, az igazságszolgáltatási rendszerbe, sőt még a kormányba vetett bizalmára is.

Ezeket a bűncselekményeket többnyire a kibertérben követik el, ezért nevezzük őket kiberbűnözésnek. Az elkövetők hamis személyazonosságot használnak, bankok, jótékonysági szervezetek, pénzügyi intézmények, bűnüldöző szervek, szolgáltatók stb. képviselőinek adják ki magukat. Céljuk az átlagemberek bizalmának elnyerése, akik csak akkor jönnek rá, hogy bűncselekmény áldozatai lettek, amikor szembesülnek azzal, hogy bankszámlájukat feltörték.

Az ilyen típusú bűncselekmények megelőzése sokkal bonyolultabb, mint a többi bűncselekményé. A szükséges információkat előzetesen össze kell gyűjteni a kibertér általános átvizsgálásával, különös figyelmet fordítva az adatbázisok illegális kereskedelmére a dark weben. Az első feladat a dark web megfigyelésére szolgáló operatív képesség elérése, hogy tisztázzák a kiberbűnözésben részt vevő főbb szereplőket, és feltárják tevékenységük mintázatait. Ezt követően lehetővé válik az azonos mintázatokat mutató tevékenységek észlelése. A következő fázis a bűncselekményekben részt vevő elektronikus eszközök nyomon követése és fizikai helyük meghatározása. Mindezen funkciók megvalósíthatók egy új információs megközelítés és egy új dinamikus elemző és értékelő rendszer létrehozásával, amely az új információelméleten alapul (Gondolatok az információ szerepéről...). Az új információelmélet képes a kockázati tényezők dinamikus változásainak detektálására azok lehetséges fenyegető következményeitől függően (Network-researched Based Dynamic Method in Crime Prevention and Investigation).

A dinamikus kockázatelemző és -értékelő rendszer egy másik páratlan előnye a prediktív képessége. Ennek eredménye az informatikai eszközökön alapuló és a dark webhez kapcsolódó bűncselekmények lehetséges csökkenése. A rendszer képes dinamikus előrejelzést adni a bűnözés előre látható tendenciáiról is.

Kulcsszavak: információelmélet, dinamizmus, bűnözés csökkentése

IRODALOMJEGYZÉK

1. Bács Zoltán György: Gondolatok az információ szerepéről – más, egyéni szemszögből NEMZETBIZTONSÁGI SZEMLE (ONLINE) 11 : 3 pp. 83-92. , 10 p. (2023)
2. Zoltán György BÁCS: Network-researched Based Dynamic Method in Crime Prevention and Investigation In: Dobák, Imre; Farkas, Johanna (szerk.) 2nd Law Enforcement Security and sychology (LEPSY) CEEPUS Network Conference Budapest, Magyarország : Law Enforcement and Psychology CEEPUS Network (2025) 58 p. ISBN: 9789634986812
3. Új, innovatív módszer megalapozása az elemző-értékelő munkában MAGYAR RENDÉSZET 22 : 3 pp. 83-99. , 17 p. (2022)

A MAGAS JOGOSULTSÁGÚ FELHASZNÁLÓKTÓL AZ AI AGENTEKIG: ÚJ TÁMADÁSI FELÜLETEK ÉS DETEKCIÓS KIHÍVÁSOK A KIBERBIZTONSÁGBAN

Fehér Sándor
ügyvezető igazgató, White Hat IT Security, sandor.feher@whitehat.eu

Absztrakt: Az előadás célja, hogy két korábbi, valós incidensen alapuló esettanulmányon keresztül bemutassa, miként tudtak támadók magas jogosultságú felhasználói fiókok kompromittálásával sikeresen behatolni vállalati hálózatokba, majd oldalirányú mozgással, jogosultságkiterjesztéssel és kritikus rendszerek elérésével jelentős üzleti és biztonsági kárt okozni. Az esettanulmányok rávilágítanak arra, hogy a privilegizált hozzáférések megszerzése régóta kiemelt célpontja a támadóknak, mivel ezek révén a védelem megkerülése és a szervezeti infrastruktúra feletti kontroll megszerzése lényegesen könnyebbé válik.

Az előadás ezt a támadói logikát helyezi át a jelenlegi technológiai környezetbe, ahol egyre több szervezet alkalmaz mesterséges intelligencián alapuló agenteket üzleti, fejlesztési, üzemeltetési vagy biztonsági folyamatok támogatására. Az AI agentek gyakran rendszerekhez, adatokhoz, API-khoz és automatizált döntési folyamatokhoz férnek hozzá, ezért jogosultságaik kompromittálása a klasszikus privilegizált felhasználói fiókokhoz hasonló, sőt bizonyos esetekben annál összetettebb kockázatot jelenthet. Különös kihívást okoz, hogy az AI agentek viselkedésének monitorozása, naplózása és anomáliadetektálása jelenleg sok szervezetnél kevésbé érett, mint a hagyományos felhasználói vagy rendszerszintű hozzáférések felügyelete.

Az előadás záró része rendszerezetten bemutatja a tíz legtipikusabb AI kiberbiztonsági kockázatot, különös tekintettel a jogosultságkezelésre, adatvédelemre, prompt-manipulációra, modell- és API-visszaélésekre, valamint a detekciós és governance-képességek hiányosságaira.

Kulcsszavak: AI ügynökök, kiber biztonsági incidens, AI kockázatok

IRODALOMJEGYZÉK

1. 1 MITRE. (n.d.). MITRE ATLAS™. Retrieved May 7, 2026, from https://atlas.mitre.org/
2. OWASP Foundation. (2025). OWASP Top 10 for Large Language Model Applications 2025. OWASP. https://genai.owasp.org/resource/owasp-top-10-for-llmapplications-2025/
3. Uber Team. (2022, September 16). Security update. Uber Newsroom. https://www.uber.com/-newsroom/security-update/
4. CyberArk Blog Team. (2022, September 20). Unpacking the Uber breach. CyberArk. https://www.cyberark.com/resources/blog/unpacking-the-uber-breach

KRITIKUS INFRASTRUKTÚRÁK - REZILLÚZIÓ?

Fülöpné Bártfai Fanni
doktorandusz, NKE-KMDI, fannibartfai@gmail.com

Absztrakt: A kibertámadások mögött számos motiváció meghúzódhat a gazdasági haszonzerzéstől a politikai-ideológiai célok elérésén át egészen a klasszikus katonai műveletek végrehajtásáig. [1] Az a közös azonban bennük, hogy minden ilyen jellegű támadásnak attraktív célpontot jelenthetnek a kritikus infrastruktúrák, ugyanis a modern társadalmak működése nagymértékben függ az infokommunikációs rendszerektől. [2]

Az elmúlt öt év számos jelentős példát szolgáltatott a kritikus infrastruktúrák elleni kibertámadásokra. A 2021-es Colonial Pipeline incidens során zsarolóvírus-támadás következtében az Egyesült Államok keleti partjának üzemanyag-ellátása jelentősen sérült, ami rávilágított a kiberfizikai rendszerek közvetett sérülékenységére és a gazdasági következmények súlyosságára. Hasonló fenyegetések jelentek meg Európában is, ahol repülőtereket és energetikai rendszereket érintő összehangolt, hibrid jellegű támadások tesztelték a védelmi képességeket.

A biztonsági környezet megváltozása fokozott intézkedéseket igényelt szövetségesi, európai és nemzeti szinten egyaránt [3], amely életre hívta a kritikus szervezetek rezilienciájáról szóló 2022/2557 irányelvet (CER).

Az irányelv célja az egyenszilárd és egységes szintű ellenállóképesség kialakítása az Unióban, amely a kritikus infrastruktúráktól megköveteli olyan intézkedések és eljárások kialakítását és fenntartását, amelyek biztosítják a működés folytonosságát és a zavarokkal szembeni ellenállóképességet. Ezen követelményhalmaz két sarokpontja a megfelelő és teljes működési környezetre kiterjedő kockázatelemzés és ellenállóképességi terv. Az érintett szervezeteknek meg kell érteniük, hogy ezen dokumentumok elkészítése és naprakészen tartása túlmutat az adminisztratív terheken, amelyek pusztán a jogszabályi megfelelésen, helyette versenyképesség növelő hatással szolgálhatnak. Ugyanis a reziliens működés, a megfelelő, a szervezet működésén és folyamatain alapuló, a gyakorlatban is tesztelt készenléti tervezési vagy incidenskezelési tervek egy esetlegesen bekövetkező incidens elhárítási idejét csökkenthetik, amely által az okozott károk mértéke is szignifikánsan csökkenthető.

Azon szervezetek esetében pedig, akik már rendelkeznek nemzetközi szabványokon alapuló, valós működést tükröző integrált irányítási rendszerrel (pl ISO 27001, ISO 22301), egy ellenállóképességi terv elkészítése nem idegen, hiszen valós üzletmenetfolytonossági és katasztrófaelhárítási tesztelt tervvel, szolgáltatáskatalógussal és teljes környezetre vonatkozó kockázatelemzéssel rendelkeznek.

Az előadás során bemutatásra kerülnek azok a módszertanok, amelyek implementálása során egy megfelelő ellenállóképességi terv hogyan szolgálhat gyakorlati útmutatóként.

Kulcsszavak: kritikus infrastruktúra, kiberbűnözés, kiberműveletek, reziliencia

IRODALOMJEGYZÉK

1. Krasznay Csaba (szerk) (2023): Taktikák és stratégiák a kiberhadviselésben
2. Kovács László (2023): Hadviselés a 21. században: kiberműveletek
3. Mógor Judit – Angyal István (2025): A kritikus infrastruktúrák ellenálló képesség fejlesztését célzó szabályozás mérföldkövei 2022-2025

A VIRTUÁLIS VALÓSÁG (VR) JELENTŐS KIBERBIZTONSÁGI ÉS DIGITÁLIS BIZALMI KIHÍVÁSAI

Gulyás István
kutató, Dunaújvárosi Egyetem, igulyas@mac.com

Absztrakt: A virtuális valóság (VR) és kiterjesztett valóság (XR) technológiák gyors térnyerése új dimenziókat nyit a digitális interakciókban, ugyanakkor jelentős kiberbiztonsági és digitális bizalmi kihívásokat is generál. Jelen tanulmány célja a VR-alapú rendszerek biztonsági kockázatainak és a bizalom fenntarthatóságának elemzése, különös tekintettel a kibertámadások evolúciójára, a szoftver- és ellátásilánc-biztonságra, valamint a kritikus infrastruktúrák védelmére.

Az eredmények rámutatnak, hogy a VR rendszerek kibővített támadási felületet kínálnak a szenzorok, biometrikus adatok és valós idejű adatfeldolgozás miatt, amely túlmutat a hagyományos informatikai rendszerek kockázatain. A kibertámadások fejlődése – beleértve a zsarolóvírusokat, adathalászatot, deepfake-alapú szociális manipulációt és szolgáltatásmegtagadási támadásokat – egyre kifinomultabb módon célozza a virtuális környezeteket, kihasználva az identitáskezelés és hitelesítés hiányosságait. A VR-platformok IoT-jellegű architektúrája miatt a hagyományos sebezhetőségek (pl. rossz konfigurációk, szoftverhibák) továbbra is relevánsak, de új, immerszív-specifikus fenyegetésekkel egészülnek ki.

Kiemelt kockázati tényezőt jelentenek a szoftverellátási láncok, ahol harmadik fél komponensek és fejlesztői eszközök kompromittálása rendszerszintű sérülékenységeket idézhet elő. A modern kibertámadások jelentős része indirekt módon, beszállítói láncokon keresztül valósul meg, ami a VR-ökoszisztémák esetében különösen kritikus a magas fokú integráció miatt. A VR-szoftverekben azonosított hibák – különösen az interfész- és erőforráskezelési sebezhetőségek – tovább növelik a kockázatokat, különösen a fejlesztési életciklus korai szakaszában.

A kritikus infrastruktúrák (pl. egészségügy, ipari rendszerek, oktatás) VR-alapú integrációja további biztonsági követelményeket támaszt. A VR-eszközök működésének megszakítása vagy manipulációja közvetlen hatással lehet az operatív folyamatokra, így ezek védelme a hagyományos IT-biztonságon túlmutató, több rétegű védekezési stratégiát igényel.

Összességében a digitális bizalom fenntartása VR-környezetekben komplex, interdiszciplináris megközelítést igényel, amely magában foglalja a „zero trust” architektúrák alkalmazását, a folyamatos monitorozást, a szabványosított biztonsági keretrendszereket, valamint a felhasználói tudatosság növelését. Jelen tanulmány hangsúlyozza, hogy a jövő VR-ökoszisztémáinak biztonsága kulcsfontosságú a technológia széles körű elfogadottságának és a digitális gazdaság stabilitásának biztosításában.

Kulcsszavak: virtuális valóság, kiberbiztonság, digitális bizalom, kritikus infrastruktúrák

IRODALOMJEGYZÉK

1. Cayir, A., Odeleye, B. P., & O'Hagan, A. (2024): Security and privacy in virtual reality: a literature survey., DOI: 10.1007/s10055-024-01079-9
2. P. Wang, H. Liang, S. Wu, & L. Sun (2024): Sensor Security in Virtual Reality: Exploration and Mitigation, DOI: 10.1145/3643832.3661389
3. H. Zhang, X. Li, & J. Wei (2025): An Empirical Study on Virtual Reality Software Security, DOI: 10.48550/arXiv.2507.17324

AZ ŰRINFRASTRUKTÚRA KIBERBIZTONSÁGA

Vukovics Árpád
Alumni, Capella University, 107 Meryton Dr. Dallas, GA 30157, arpad.vukovics@mac.com

Absztrakt: Az előadás célja, hogy bemutassa az űrinfrastruktúra kiberbiztonságának növekvő jelentőségét, különösen annak fényében, hogy a műholdak és a hozzájuk kapcsolódó rendszerek egyre fontosabb szerepet töltenek be a modern társadalomban, a gazdaságban, a közbiztonságban, a védelemben és a globális kommunikációban. Az előadás áttekinti az űrrendszerek főbb elemeit, beleértve a földi, űrbeli, kommunikációs és felhasználói szegmenseket, valamint bemutatja, hogy az analóg, elkülönített és hardveralapú rendszerekről a hálózatba kapcsolt, digitális és szoftveralapú megoldások felé történő elmozdulás hogyan növeli a kibertámadások lehetőségét. Kiemeli, hogy a műholdas rendszerek biztonsága közvetlenül kapcsolódik a mindennapi élethez, például a GPS-hez, az internet-hozzáféréshez, a logisztikához, a közművekhez, az időjárás-előrejelzéshez és a katasztrófaelhárításhoz. Az előadás ismerteti a legfontosabb kiberbiztonsági alapelveket, így a bizalmasságot, sértetlenséget, rendelkezésre állást, megbízhatóságot, hitelességet, elszámoltathatóságot és letagadhatatlanságot. Külön figyelmet kapnak a fő fenyegetési vektorok, például az ellátási lánc sebezhetőségei, a felhőalapú infrastruktúra kockázatai, a jelzavarás, a rosszindulatú szoftverek, a belső fenyegetések és a hasznos teher eltérítése. A 2022-es Viasat KA-SAT támadás konkrét példaként szemlélteti a lehetséges következményeket. Végül az előadás kitér a jövőbeli kockázatokra és a lehetséges védekezési megoldásokra.

Kulcsszavak: Műholdas kiberbiztonság; kiberfenyegetések; műholdas kommunikáció; földi szegmens biztonsága; jelinterferencia; Viasat KA-SAT támadás; kvantumrezisztens titkosítás.atellite cybersecurity; cyber threats; satellite communications; ground segment security; signal interference; Viasat KA-SAT attack; quantum-resistant encryption

BIBLIOGRAPHY

1. Pratt, T., & Allnutt, J. (2020). Satellite Communications (3rd ed.) Wiley. ISBN 9781119482178
2. SANS Cyberdefense (2024). The Risk to Space: Satellite Communications Systems and Ground Networks as Attack Targets. Retrieved from: https://www.youtube.com/watch?v=Myk8QzXbmq8
3. Peled, R., Aizikovich, E., Habler, E., Elovici, Y., & Shabtai, A. (2023). Evaluating the Security of Satellite Systems.Cornell University. arXiv preprint arXiv:2312.01330.
4. NIST (n.d.). Cybersecurity framework, 2025. Retrieved from: https://www.nist.gov/cyberframework
5. Barett, T. (2024). Looking to the skies: The importance of satellite cybersecurity. Retrieved from: https://www.ussc.edu.au/the-importance-of-satellite-cybersecurity

2. ADAPTÍV KIBERVÉDELEM

ÚJ KÉPZÉSI MÓDSZEREK ALKALMAZÁSÁNAK TAPASZTALATAI EGY TECHNOLÓGIA KÖZPONTÚ INFORMÁCIÓGYŰJTŐ SZERVEZETNÉL

Horváth Ferenc
NBSZ, fhorvath25@gmail.com

Absztrakt: A kiberbiztonság alapköve az ember. Annak érdekében, hogy a felhasználó ne váljon a leggyengébb láncszemmé, nem elég csupán oktatni, szemléletet is kell formálni, biztonságtudatosságot is ki kell alakítani. Ahhoz, hogy a tanultak a gyakorlati életben is hasznosuljanak, az oktatásnak minden idegrendszeri szintet be kell vonnia a tanulási folyamatba, amik a fejleszteni kívánt kompetencia megvalósulása során is érintettek lehetnek. Nem elég a hagyományos, poroszos oktatási elveket a digitális térbe áthelyezni. Az igazi áttörést az jelenti, amikor magukat a tanulókat, az ő igényeiket és sajátosságaikat sikerül fókuszba helyezni. Amikor a tanulásra szorítás helyett a tanulás lehetőségének felhasználóbarát megteremtése válik elsődlegessé. Az ismeretátadás helyett a kompetenciafejlesztés, a közlés helyett az interakció, a beszéd helyett a multimodális megtapasztalás, a kötelezés helyett a gamifikáció, az emlékezet tesztelés helyett a gyakorlati alkalmazás, az oktatói hatalom helyett a partneri bevonás. Az előadás áttekinti, milyen kihívásokat leküzdve, milyen eredményekkel lehet ezen elvek mentén kialakítani egy szervezet oktatási rendszerét.

Kulcsszavak: Kiberbiztonsági tudatosság, Szemléletformálás, Multimodális tanulás, Kompetenciafejlesztés, Gamifikáció

IRODALOMJEGYZÉK

1. Horváth, F., (2024). Új képzési módszerek alkalmazásának tapasztalatai a Nemzetbiztonsági Szakszolgálatnál. NEMZETBIZTONSÁGI SZEMLE (ONLINE) (2064-3756): 12 2 pp 81-97. https://orcid.org/0000-0001-8639-2700
2. Horváth, F., (2022). “From Top to Toe”: Choosing the Appropriate Training Method NEMZETBIZTONSÁGI SZEMLE (ONLINE) (2064-3756): 10 3 pp 44-56. doi: 10.32561/nsz.2022.3.4

KIBERBIZTONSÁG AZ IGAZSÁGÜGYI INFORMATIKÁBAN - AZ IGAZSÁGÜGYI INFORMATIKA KIBERBIZTONSÁGA: MÓDSZERTANI SZINERGIÁK A NIS2 KORSZAKÁBAN

MÁTÉ István Zsolt
igazságügyi informatikai szakértő, Nemzeti Szakértői és Kutató Központ,
mateizs@nszkk.gov.hu

Absztrakt: Az igazságügyi informatika és a kiberbiztonság hagyományosan elkülönülő területek az alkalmazott tudományokon belül. A köztük fennálló metodológiai szakadék alapvető oka a megközelítésmódok divergenciája: míg az igazságügyi informatika alapvetően ex post (post-mortem) vizsgálatokra építve, feltáró-elemző nézőpontból vizsgálja a digitális nyomokat a bizonyítás érdekében, addig a kiberbiztonság fókusza az ex ante típusú prevencióra és a valós idejű, aktív incidenskezelésre irányul.

Napjainkban azonban a két szakterület konvergenciája felgyorsult. A kiberfenyegetések komplexitása és a bizonyítékok volatilitása új módszertani szinergiákat követel meg, melynek eredményeként a védelmi és a feltáró funkciók határvonalai elmosódnak. Erre reflektál a forenzikus készenlét (forensic readiness) koncepciója is: a rendszerek olyan tudatos tervezése, amely biztosítja a jogilag releváns bizonyíték-szolgáltatást a védelmi mechanizmusok sérelme nélkül.

Az előadás esettanulmányokon keresztül világít rá e komplex kihívásokra – az ISO/IEC 27043:2015 szabvány módszertani bázisán és a NIS2 irányelv keretrendszerében –, végül pedig olyan adaptív szakértői válaszokat fogalmaz meg, amelyek a technológiai fejlődés és a szigorodó jogi környezet közepette is fenntarthatóvá teszik a digitális bizalmat.

Kulcsszavak: kiberbiztonság, igazságügyi informatika, forenzikus készenlét, módszertani konvergencia

IRODALOMJEGYZÉK

1. Máté, I. Zs. (2018). Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe [Expert investigation of attacks against information systems – the role of recording digital traces]. Belügyi Szemle / Academic Journal of Internal Affairs, 66(7–8), 36–54.
2. Máté, I. Zs. (2020). Az igazságügyi informatikai szakértő feladatai [The tasks of the digital forensic expert]. In P. Ruzsonyi (Ed.), Közbiztonság: Fenntartható biztonság és társadalmi környezet tanulmányok III. [Public Security: Sustainable Security and Social Environment Studies III] (pp. 1871–1894). Ludovika Egyetemi Kiadó.
3. Máté, I. Zs., Darabos, Z., Morber, Sz. K., & Sándor, G. (2021). Módszertani levél az elektronikus adatok vizsgálatának általános alapelveiről [Methodological Guideline on the general principles of the examination of electronic data]. Hungarian Chamber of Judicial Experts (MISZK).
4. Máté, I. Zs. (2025). Mesterséges intelligencia az igazságügyi szakértői munkában [Artificial intelligence in forensic expert work]. In J. Répás (Ed.), Alverad-Bánki Nemzetközi Kiberbiztonsági és Kutatás-Fejlesztési Konferencia: Konferenciakötet – Book of Abstracts [Alverad-Bánki International Cybersecurity and Research & Development Conference: Conference Proceedings – Book of Abstracts] (p. 67). Óbudai Egyetem; Alverad Technology Focus Kft.
5. Máté, I. Zs. (2026). Forensic expert case registry (2007–2026) [Unpublished raw data].

AI-QUANTUM ÜTKÖZÉS KORSZAKA

Miklós Márton
CEO, ACPM IT Zrt. Elnök, Magyar Kiberbiztonsági Klaszter, marton.miklos@acpmit.com

Absztrakt: 2026-ra a kiberbiztonság világában beköszöntött a „Collision Era” (az ütközés korszaka), mivel a frontier AI modellek és a quantum computing konvergenciája alapjaiban változtatta meg a globális biztonsági paradigmákat.

Jelen kutatás célja az „Automated Offense” megjelenésének elemzése, valamint az emberi szakértelem és a gépi sebesség közötti hagyományos határok ebből fakadó összeomlásának vizsgálata. A tanulmány rámutat arra a sürgető kényszerre, amely a szervezeteket a reaktív, manuális biztonsági modellektől az AI-native, quantum-resilient keretrendszerek felé tereli.

Az AI területén végbement legutóbbi fejlemények sorsfordító pillanatot hoztak a kiberbiztonság mint iparág számára. A Mythos sikeresen automatizálta a high-severity zero-day sebezhetőségek feltárását – mint például egy évtizedes Apache ActiveMQ hiba esetében –, hetek helyett percek alatt. Ez a felgyorsulás egy „remediation crisis”-t (elhárítási válságot) idézett elő, amelyet az a szűk keresztmetszet jellemez, ahol az AI által generált bug reportok mennyisége meghaladja az emberi hibajavítási kapacitást.

Ezzel párhuzamosan a „Harvest Now, Decrypt Later” (HNDL) támadások terjedése és a közeledő „Q-Day” az RSA és az Elliptic Curve titkosítás funkcionális élettartamát fenyegetik.

A kutatás megállapítja, hogy a cryptographic agility többé nem választható opció; a szervezeteknek át kell állniuk a NIST által jóváhagyott Post-Quantum Cryptography (PQC) szabványokra, mint például az ML-KEM, hogy túléljék a kvantumátállást.

Emellett az előadás azonosít egy stratégiai elmozdulást a continuous compliance irányába, amely automatizálja az olyan összetett, 2026-os mandátumoknak való megfelelést, mint az EU AI Act. Végezetül, a sikeres védekezés 2026-ban megköveteli a quantum-enhanced AI alkalmazását a remediation folyamatok automatizálására, ezáltal felvéve a versenyt az automated offensive eszközök sebességével.

Kulcsszavak: posztkvantum kriptográfia, AI-natív védelem, Claude Mythos, Q-nap, kriptográfiailag releváns kvantumszámítógép, automatizált támadás, folyamatos megfelelés, elhárítási válság, „gyűjtsd be most, fejtsd vissza később” típusú támadások

IRODALOMJEGYZÉK

1. Anthropic Red Team Report (April 7, 2026): "Assessing Claude Mythos Preview's Cybersecurity Capabilities." Key Fact: Documented the model's ability to find 27-year-old bugs in OpenBSD and 16-year-old flaws in FFmpeg.
2. Radware Blog (April 28, 2026): "Anthropic Claude Mythos and the 2026 Cybersecurity Landscape." Key Fact: Details on Project Glasswing, the defensive coalition of 40 organizations (Google, Microsoft, etc.) testing Mythos before public release.
3. Help Net Security (April 9, 2026): "Claude helps researcher dig up decade-old Apache ActiveMQ RCE vulnerability (CVE-2026-34197)." Key Fact: Horizon3.ai researcher used Claude to identify a 13-year-old "unauthenticated RCE" path in the ActiveMQ Classic codebase.
4. Cybernews (April 8, 2026): "AI is breaking bug bounty programs by finding too much." Key Fact: Coverage of HackerOne pausing new submissions for the Internet Bug Bounty due to the overwhelming volume of AI-assisted reports outstripping human patch capacity.
5. Cloud Security Alliance Whitepaper (April 13, 2026): "Claude Mythos: AI Vulnerability Discovery and Containment Failures." Key Fact: Analysis of the "Remediation Gap"—where discovery speed increased by 10,000% while patching speed remained linear.
6. CISA Technical Advisory (January 24, 2026): "Product Categories for Technologies Using Post-Quantum Cryptography Standards." Key Fact: Mandated that federal agencies stop procuring legacy (RSA/ECC) products for "Widely Available" categories like Cloud and Web Browsers.
7. NIST Special Publication (March 2026): "NIST IR 8547: A Roadmap for Transitioning to Post-Quantum Cryptography." Key Fact: Official finalization and implementation guide for ML-KEM and ML-DSA algorithms.
8. Google Cloud Security (November 2025): "Cybersecurity Forecast 2026: The Rise of Harvest Now, Decrypt Later (HNDL) Infrastructure."
9. Deutsche Telekom Event (March 18, 2026): "TRANSFORM 2026: Scaling AI & Data for a Trusted Digital Future." Key Fact: Keynote by Klaus Werner on using AI Security Agents to embed governance directly into the network fabric.
10. Openlayer Blog (April 24, 2026): "EU AI Act Post-Market Monitoring Guide: April 2026 Enforcement." Key Fact: Explains the Article 72 requirement for continuous monitoring and how major telcos like Telefonica use Openlayer to automate real-time compliance evidence.
11. European Commission (February 2, 2026): "Standardized Template for AI Post-Market Monitoring Plans." Key Fact: The regulatory trigger that forced telcos to move from static audits to automated AI monitoring.
12. Google Cloud Security Forecast 2026: Comprehensive report on "Shadow Agents" and the virtualization of the threat landscape.
13. CVE-2025-59536: Documentation of the first major "AI Supply Chain" RCE discovered in popular AI coding assistants.

A MESTERSÉGES INTELLIGENCIA KETTŐS SZEREPE A KIBERBIZTONSÁGBAN: TÁMADÁS ÉS VÉDELEM

Sági Gábor János
kiberbiztonsági szakértő, gaborjanos.sagi@hungarocontrol.hu

Absztrakt: A mesterséges intelligencia (MI) rohamos fejlődése alapvetően átformálta a kibertér támadási és védelmi taktikáit, kettős felhasználású technológiává téve azt. A kibertámadók MI-alapú eszközökkel automatizálják és skálázhatóvá teszik műveleteiket. Generatív modellek segítségével személyre szabott, kontextus-tudatos adathalász kampányokat és deepfake tartalmakat hoznak létre (Mohamed, 2023). Gépi tanulással adaptív, önmutáló kártevőket fejlesztenek, amelyek elkerülik a hagyományos védelmi rendszereket (Telrandhe et al., 2025), valamint megtévesztő mintákat alkalmaznak az ML-alapú detektorok megkerülésére vagy mérgezésére (Vitorino et al., 2023). Ezzel párhuzamosan a kibervédők is egyre szélesebb körben alkalmazzák az MI-technológiákat. Mély tanulási módszerek javítják a behatolásdetektálást és az anomália-felismerést komplex hálózati forgalmi minták elemzésén keresztül (Nakıp & Gelenbe, 2024). Önfelügyelt tanulási megközelítések valós idejű fenyegetésdetektálást tesznek lehetővé változó támadási vektorokkal szemben (Neha & Bhatia, 2025). Az MI-alapú fenyegetés-intelligencia rendszerek prediktív kockázatértékelést végeznek és gyorsítják a biztonsági műveleti központok (SOC) munkafolyamatait (Sharma, 2024). Az automatizált incidenskezelő platformok csökkentik a reagálási időt (Nnaka et al., 2025). Az MI kettős felhasználása azonban komoly kihívásokat vet fel, a védelmi rendszerek maguk is sebezhetők ellenséges támadásokkal szemben, ezért hibrid megközelítésekre, támadásokra történő felkészítésre és folyamatos újratanításra van szükség (Mohamed, 2025). A kutatás rávilágít, hogy az MI-vezérelt kiberbiztonság hatékonysága kizárólag a technológiai megoldások és a humán felügyelet integrált, szinergetikus alkalmazásával biztosítható.

Kulcsszavak: MI kibervédelemben, MI kibertámadásban, kiberbiztonság

IRODALOMJEGYZÉK

1. Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. Cogent Engineering, 10(2), Article 2272358. https://doi.org/10.1080/23311916.2023.2272358
2. Mohamed, N. (2025). Cutting-edge advances in AI and ML for cybersecurity: A comprehensive review of emerging trends and future directions. Cogent Business & Management, 12(1), Article 2518496. https://doi.org/10.1080/23311975.2025.2518496
3. Nakıp, M., & Gelenbe, E. (2024). Online self-supervised deep learning for intrusion detection systems. IEEE Transactions on Information Forensics and Security, 19, 5668–5683. https://doi.org/10.1109/TIFS.2024.3402148
4. Neha, & Bhatia, T. (2025). Adaptive intrusion detection system leveraging dynamic neural models with adversarial learning for 5G/6G networks. In Proceedings of the 2025 4th International Conference on Computer Technologies (ICCTech) (pp. 103–107). IEEE. https://doi.org/10.1109/ICCTech66294.2025.00028
5. Nnaka, K. I., Mbamalu, P. O., Nwaigbo, J. C., Ozo-ogueji, P. C., Njoku, V. I., & Ekechi, C. C. (2025). AI-powered threat detection: Opportunities and limitations in modern cyber defense. World Journal of Advanced Research and Reviews, 27(2), 210–223. https://doi.org/10.30574/wjarr.2025.27.2.2854
6. Sharma, S. K. (2024). AI-enhanced cyber threat detection and response systems. Shodh Sagar Journal of Artificial Intelligence and Machine Learning, 1(2), 43–48. https://doi.org/10.36676/ssjaiml.v1.i2.14
7. Telrandhe, A. V., Nishane, D., Puri, C., & Gayaki, U. (2025). AI-powered threat detection and response system for next-gen cyber defense. In Proceedings of the 2025 2nd International Conference on Electronic Circuits and Signaling Technologies (ICECST) (pp. 1132–1137). IEEE. https://doi.org/10.1109/icecst66106.2025.11307219
8. Vitorino, J., Praça, I., & Maia, E. (2023). SoK: Realistic adversarial attacks and defenses for intelligent network intrusion detection. Computers & Security, 134, Article 103433. https://doi.org/10.1016/j.cose.2023.103433

KVANTUM SZÁMÍTÓGÉPEK KIBERBIZTONSÁGI KOCKÁZATAI, A MESTERSÉGES INTELLIGENCIA KIBERBIZTONSÁGI ASPEKTUSAI

Szabó Lajos
Igazgató, Nemzeti Kiberbiztonsági Intézet, lajos.szabo@nki.gov.hu

Absztrakt: Az előadás célja a kvantumszámítógépek és a mesterséges intelligencia (AI) kiberbiztonsági vonatkozásainak áttekintése, különös tekintettel a technológiai fejlődésből eredő jövőbeni kockázatokra és alkalmazkodási lehetőségekre. A kvantumszámítástechnika fejlődése várhatóan jelentős hatással lesz a jelenleg alkalmazott kriptográfiai megoldásokra, különösen a széles körben használt aszimmetrikus titkosítási módszerekre. Az előadás bemutatja a kvantumfenyegetés idődimenzióját, valamint a „harvest now, decrypt later" megközelítésből fakadó kockázatokat, amelyek elsősorban a hosszú távon érzékeny adatok esetében jelentenek problémát. Az előadás kitér a poszt kvantum kriptográfia és a kripto-agilis rendszerek szerepére, valamint a szervezetek felkészülési lehetőségeire is. A második témakör a mesterséges intelligencia kiberbiztonsági aspektusait vizsgálja támadói és védekezési oldalról egyaránt. Az előadás ismerteti az AI által támogatott adathalász kampányok, deepfake technológiák, automatizált sebezhetőség-kutatás és AI-alapú malware-fejlesztés legfontosabb trendjeit és kockázatait. Emellett bemutatja az AI védelmi célú felhasználási lehetőségeit is, például az anomáliadetektálás, spam- és csalásszűrés, valamint a hálózati forgalomelemzés területén. Az előadás következtetése szerint a kvantumszámítástechnika és a mesterséges intelligencia nemcsak technológiai, hanem stratégiai és szemléletbeli kihívást is jelent a kiberbiztonság számára.

Kulcsszavak: kvantumszámítógép, poszt kvantum kriptográfia, mesterséges intelligencia, kiberbiztonság, deepfake, AI-alapú támadások, kripto-agilitás

IRODALOMJEGYZÉK

1. Nemzeti Kiberbiztonsági Intézet. (2025). Kvantumszámítógépen fut a DOOM? 1. rész [Podcast epizód] https://kibertamadas.simplecast.com/episodes/kvantum-szamitogepen-fut-a-doom-1-vendegunk-dr-asboth-janos-orokzold
2. Nemzeti Kiberbiztonsági Intézet. (2025). Kvantumszámítógépen fut a DOOM? 1. rész [Podcast epizód] https://kibertamadas.simplecast.com/episodes/kvantumszamitogepen-fut-a-doom-2-vendegunk-dr-asboth-janos-orokzold
3. Nemzeti Kiberbiztonsági Intézet. (2024). Mesterséges intelligencia a kiberbűnözés szolgálatában – az AI-vezérelt adathalászat új korszakában. https://nki.gov.hu/it-biztonsag/hirek/mesterseges-intelligencia-a-kiberbunozes-szolgalataban-az-ai-vezerelt-adathalaszat-uj-korszaka/?utm_source=chatgpt.com
4. Google Cloud Threat Intelligence Blog (2025). Threat actor usage of AI tools for cyber operations. https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools?utm_source=chatgpt.com

3. DIGITÁLIS INTEGRITÁS VS. MANIPULÁLT VALÓSÁG

VÉDENI A VÉDHETETLENT?

Belinszki Zoltán
doktorandusz, PTE, zbelinszki72@gmail.com

Absztrakt: Az internetre felkerülő tartalmak védelme a technika és az eszközök folyamatos fejlődése, a szabályozás szigorodása, az információbiztonság globálissá tételét célzó lépések ellenére sem oldható meg száz százalékosan. Számos területen működhet az önkorlátozás, vagyis a világhálón megosztott tartalom szűrése, csökkentése.

A művészet területén ez a választás elfogadhatatlan. Az alkotók nem csupán az önkifejezés lehetőségét vesztenék el, hanem közönségük nagy részét is. Egy zenekar nem teheti meg, hogy nem teszi föl egy új dal videóját az internetre, nehogy mások lemásolják, és új dalokat generáljanak belőle, reklámbevételt szerezve az „új albummal". Egy divattervező nem teheti meg, hogy nem adja közre friss kreációját, nehogy a fast fashion ürügyén illetéktelenek keressenek pénzt belőle. Egy irodalmár nem teheti meg, hogy nem publikálja a versét, nehogy Coelho-mémként lássa viszont.

A művészek egy része jogos önvédelemként speciális szoftvereket használ szerzői jogai megőrzése érdekében. A platformjog paradigmát váltott: előzetes intézkedésekre készteti a nagy közösségi platformokat.

Milyen módon növelhető az információbiztonság a művészet területén? A globális szabályozás illúzió vagy az egyetlen megoldás? Tekinthető-e önálló alkotásnak mások műveinek újraértelmezése? A jogosultak biztonságérzetét érintő témákról, mint az ezt felmérő kutatás kiindulópontjairól szól az előadás.

Kulcsszavak: művészet, információbiztonság, szerzői jog, ex ante

IRODALOMJEGYZÉK

1. Konrád, B. (2026): Újabb zenekar lett AI-csalás áldozata Spotify-on. www.dalszerzo.hu
2. Hohmann, B. (2025): Válogatott fejezetek az európai platformjog köréből. PTE ÁJK, Pécs
3. Pogácsás, A. – Újhelyi, D. (2025): Szellemi alkotások joga (2.átdolg.kiad.), Budapest, Pázmány Press, 2025

AZ ONLINE TUDOMÁNYOS KOMMUNIKÁCIÓ, MINT KRITIKUS DIGITÁLIS BIZALMI INFRASTRUKTÚRA

Berek László
könyvtárigazgató, Óbudai Egyetem, berek.laszlo@uni-obuda.hu

Absztrakt: A tudományos kommunikációs ökoszisztéma napjainkra a digitális társadalom egyik meghatározó bizalmi infrastruktúrájává vált. A kutatási eredmények nemcsak a tudományos közösség működését határozzák meg, hanem közvetlen hatással vannak az egészségügyre, az energetikára, az iparra, az oktatásra, valamint a stratégiai és szabályozási döntéshozatalra is. Ennek következtében a tudományos kommunikáció integritása és hitelessége már nem kizárólag akadémiai kérdés, hanem információbiztonsági és társadalmi bizalmi probléma is.

Az előadás azt vizsgálja, hogy a gyorsan fejlődő digitális környezet és a generatív mesterséges intelligencia megjelenése milyen új sérülékenységeket hozott létre a tudományos publikációs és kommunikációs rendszerekben. Bemutatásra kerülnek azok a fenyegetések, amelyek a tudományos információk hitelességét veszélyeztetik, beleértve az AI-generált tudományos tartalmakat, a manipulált peer review folyamatokat, a citation manipulation jelenségét, a predátor folyóiratok működését, valamint a paper mill hálózatok térnyerését.

Az előadás külön figyelmet fordít arra, hogy a tudományos publikációs ökoszisztéma miként értelmezhető egy komplex digitális ellátási láncként, ahol a kompromittált vagy manipulált tartalom a kritikus infrastruktúrákhoz hasonló kockázatokat eredményezhet. A tudományos dezinformáció, a manipulált kutatási eredmények és az AI-alapú tartalomelőállítás következményei nemcsak az akadémiai reputációt, hanem a társadalmi bizalmat és a szakpolitikai döntéshozatalt is közvetlenül érintik.

Az előadás bemutat továbbá olyan lehetséges intézményi és információbiztonsági megközelítéseket, amelyek hozzájárulhatnak a tudományos kommunikáció integritásának védelméhez. Külön hangsúlyt kapnak az előzetes kéziratellenőrzési modellek, az AI-alapú detekciós megoldások, a predátor folyóiratok szűrésére alkalmas módszerek, valamint az egyetemi könyvtárak és kutatástámogató szervezetek szerepe a tudományos bizalom fenntartásában.

Kulcsszavak: Tudományos kommunikáció, Digitális bizalom, Információbiztonság, Generatív mesterséges intelligencia, Kutatásintegritás, Predátor folyóiratok

IRODALOMJEGYZÉK

1. Berek, L. (2023). Researcher's Choice or Just a Necessity? The Consequences of Publishing in a Predatory Journal. Interdisciplinary Description of Complex Systems, 21(4), 324-332. https://doi.org/10.7906/indecs.21.4.1
2. Berek, L. (2025). Az egyetemi könyvtárak szerepe a tudományos kibocsátás biztonságában és az intézményi reputáció erősítésében. Safety and Security Sciences Review, 4(7), 1. https://doi.org/10.12700/btsz.2025.7.4.1
3. Berek, L. (2024). Artificial Intelligence-Generated Text in Higher Education—Usage and Detection in the Literature. Interdisciplinary Description of Complex Systems, 22(3), 238-245. https://doi.org/10.7906/indecs.22.3.1
4. Pierce, M. (2025). Academic Librarians, Information Literacy, and ChatGPT Sounding the Alarm on a New Type of Misinformation. College and Research Libraries News, 86(2), 68-70. https://doi.org/10.5860/crln.86.2.68
5. De, S., & Mondal, P. (2025). Assessing the Impact of Misinformation by Predatory Journals on Academic Integrity. Serials Librarian, 86(1-2), 17-28. https://doi.org/10.1080/0361526X.2025.2471922

A KIBERBIZTONSÁG VAKFOLTJA - AZ ÉRTELMEZÉSI SÉRÜLÉKENYSÉG, MINT STRUKTURÁLIS KOCKÁZAT A TECHNIKAI MEGFELELÉS HATÁRAIN TÚL

Gulyás Zsuzsa
Gábor Dénes Egyetem oktató, PTE ÁJK doktorandusz, MÉDÉSZ-kutató és oktatásfejlesztő,
gulyas.zsuzsa@medesz.hu

Absztrakt: A kiberbiztonság területén a sérülékenység fogalma hagyományosan technikai keretek között értelmeződik. A biztonsági kockázat azonosítása elsősorban rendszerszintű hibákhoz, konfigurációs hiányosságokhoz és támadási felületekhez kapcsolódik. Ez a megközelítés azonban egy olyan réteget hagy figyelmen kívül, amely nem a rendszer működéséből, hanem az értelmezés eltéréseiből fakad. A tanulmány abból a feltevésből indul ki, hogy a biztonsági incidensek egy jelentős része nem technikai meghibásodás következménye, hanem annak a diszkrepanciának az eredménye, amely a szabályozási előírások, az operátori értelmezés és az automatizált rendszerek végrehajtási logikája között keletkezik. Ebben az értelemben a sérülékenység nem kizárólag a kódban, hanem a jelentés szintjén jelenik meg. Az elemzés az értelmezési sérülékenységet olyan strukturális kockázati kategóriaként vezeti be, amely a kommunikációs határok mentén jön létre. Ezek a határok nemcsak ember és rendszer között húzódnak, hanem szervezeti egységek, szakmai keretek és normatív elvárások között is. A biztonsági működés ebben a térben nem egyszerűen technikai megfelelés kérdése, hanem az értelmezési koherencia fenntartásának problémája is. A tanulmány amellett érvel, hogy a jelenlegi kiberbiztonsági gyakorlat a kockázat egy részét láthatóvá teszi, miközben egy másik részét rendszerszinten elfedi. Az értelmezési eltérések azonosítása nélkül a biztonsági beavatkozások gyakran tüneti szinten maradnak, és nem érintik a működési zavarok tényleges forrását.

Kulcsszavak: Értelmezési sérülékenység, kiberbiztonság, szemantikai kockázat, szervezeti kommunikáció, megfelelés, ember-gép interakció, értelmezési eltérés, strukturális kockázat, jelentésintelligencia, MÉDÉSZet

IRODALOMJEGYZÉK

1. Bada, M., Sasse, M. A., & Nurse, J. R. C. (2019). Cybersecurity awareness campaigns. ACM Computing Surveys, 52(4).
2. ENISA. (2023). Threat landscape report. European Union Agency for Cybersecurity.
3. Floridi, L. (2022). Ethics of information. Oxford University Press.
4. Kiss, A. (2022). Kiberbiztonság és humán tényezők. Hadmérnök, 17(2).
5. NIST. (2020). Cybersecurity framework. National Institute of Standards and Technology

AZ AI PIPELINE ÁRNYOLDALA: KIBERBIZTONSÁGI FENYEGETÉSEK A MODELLEZÉSI FOLYAMATBAN

Irányi Csaba
Gépi tanulási mérnök, e-Corvina Kft., csaba.iranyi@gmail.com

Absztrakt: Az előadás a gépi tanulási modellezés kibervédelmi aspektusait a teljes AI életcikluson keresztül vizsgálja, a helyi környezetben futó adatfeldolgozástól a felhős tanításon át egészen az éles kiszolgálásig. Középpontba kerül, hogy az adattudományi és modellezési pipeline nem pusztán technológiai innováció, hanem egyben kiterjedt támadási felület is, ahol az adatok, modellek, szoftver-összetevők és szolgáltatások egyaránt célponttá válhatnak. Szó lesz az érzékeny adatok – személyes, egészségügyi, minősített vagy üzleti titkot képező információk – elleni támadásokról, valamint arról, hogy a nagy mennyiségű, időben elnyújtott adatmozgatások és archiválások miként teremtenek nehezen észlelhető adatszivárgási és jogosulatlan hozzáférési kockázatokat. Az előadás bemutatja az adatmérgezés különböző formáit is: hogyan torzíthatók a nyílt forrásból gyűjtött, megvásárolt vagy saját előállítású adatkészletek, miként jelenhet meg félrecímkézés, elfogultság, manipulált asszociáció vagy rejtett szándék a tanító adatokban. Külön figyelmet kapnak a transfer learning és a fine-tuning sebezhetőségei, beleértve az alapmodellek módosítását, a rejtett triggerek elhelyezését, valamint a hamis vagy megtévesztő publikus modellgyűjtemények veszélyeit. Az előadás kitér a modell lopásra, a súlyok és paraméterek manipulálására, továbbá a keretrendszerek, API-k, notebookok, pluginek és nyílt forrású könyvtárak elleni ellátási lánc alapú támadásokra is. Végül a felhős szolgáltatások kompromittálása, a több-bérlős környezetek kockázatai és a DDoS támadások pénzügyi, reputációs és jogi következményei rajzolják ki azt a valós fenyegetési képet, amelyben a modern AI-rendszereknek működniük kell.

Kulcsszavak: gépi tanulás, kibervédelem, adatmérgezés, felhőbiztonság, modellintegritás

IRODALOMJEGYZÉK

1. Gu, T., Dolan-Gavitt, B., Garg, S. (2019). BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain. New York University. https://doi.org/10.48550/arXiv.1708.06733
2. Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, Ch., Prakash, A., Kohno, T., Song, D. (2018). Robust Physical-World Attacks on Deep Learning Models. University of Michigan. https://doi.org/10.48550/arXiv.1707.08945
3. Madry, A., Makelov A., Schmidt L., Tsipras D., Vladu A. (2019). Towards Deep Learning Models Resistant to Adversarial Attacks. MIT. https://doi.org/10.48550/arXiv.1706.06083

AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG MÉRÉSÉNEK MODERNIZÁCIÓJA ÉS NAGYMINTÁS EMPIRIKUS VALIDÁLÁSA

Laska Pál Károly
doktorandusz, Nemzeti Közszolgálati Egyetem, Laska.Pal.Karoly@uni-nke.hu

Absztrakt: A kiberbiztonsági incidensek mintegy háromnegyede emberi tényezőre vezethető vissza, ezért a humán biztonságtudatosság objektív mérése a kiberreziliencia egyik kulcskérdése. A nemzetközi szakirodalomban legszélesebb körben alkalmazott HAIS-Q (Human Aspects of Information Security Questionnaire) azonban már nem képes lekövetni a digitális környezet változásait — a mesterséges intelligencia, a felhőalapú szolgáltatások, az IoT-eszközök és a modern autentikációs megoldások által támasztott új kihívásokat. Kutatásunk ezért egy új mérőeszköz, a SAM (Security Awareness Model) kidolgozására és validálására vállalkozott.

A SAM a kontingenciaelmélet keretében a HAIS-Q alapjaira épül, ám azt jelentősen kibővíti és modernizálja. A modell hét fókuszterületen (autentikáció, internetes szolgáltatások, információkezelés, eszközhasználat, incidensmenedzsment, szabályozás, tudatosság) és tíz dimenzión keresztül, a Tudás–Attitűd–Viselkedés (KAB) szemléletben, 120 tételes kérdőívvel, hierarchikus formatív mérési modellként operacionalizálja az információbiztonsági tudatosságot.

A modell empirikus validálását két nagymintás, országosan reprezentatív adatfelvétellel végeztük el: lakossági (n = 3 144) és vállalati (n = 2 184) körben, IPF-súlyozással és SmartPLS-alapú strukturális egyenletmodellezéssel (PLS-SEM). A dimenziók megbízhatósága megfelelőnek bizonyult (Cronbach-α > 0,8). Eredményeink több sztereotípiát is megdöntenek: a magas tudás önmagában nem vezet biztonságtudatos viselkedéshez — a legerősebb hatás az attitűdhöz kötődik (β = 0,769), amely mediáló és moderáló szerepet egyaránt betölt; az idősebb korosztály objektíven tudatosabb, mint a digitális bennszülöttek; a KKV-szektorban dolgozók pedig alulbecsülik saját tudatossági szintjüket. A jövedelem hatása csak közvetett, elsősorban az iskolai végzettségen keresztül érvényesül.

A SAM-modell alkalmas longitudinális mérésekre, profilalkotásra, kockázati zónák azonosítására, valamint az ISO/IEC 27001, a NIS2 és a GDPR humán követelményeinek dokumentálható mérésére. A kutatás gyakorlati hozadéka: a hatékony prevenció kulcsa nem a tudásátadás, hanem az attitűdformáló, élményalapú és gamifikált beavatkozások.

Kulcsszavak: Security Awareness Model, információbiztonsági tudatosság, HAIS-Q, KAB-modell, PLS-SEM, kiberreziliencia

IRODALOMJEGYZÉK

1. Bak, G., Berek, L., Som, Z., Ujhegyi, P., & Répás, J. (2024). On the way to updating the measurement of information security awareness: A literature analysis. Interdisciplinary Description of Complex Systems, 22(3), 305–316.
2. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004
3. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165–176. https://doi.org/10.1016/j.cose.2013.12.003
4. Hermawan, D. S., Setiadi, F., & Oktaria, D. (2022). Measurement level of information security awareness for employees using KAB model with study case at XYZ agency. In 2022 1st International Conference on Software Engineering and Information Technology (ICoSEIT) (pp. 174–179). IEEE. https://doi.org/10.1109/ICoSEIT55604.2022.10029989

FSFT2026

THE FUTURE OF SECURITY
THE FUTURE OF TRUST


DENNIS GABOR
UNIVERSITY
DIGITAL HORIZONS