NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2025. 47. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58 A2D0 E9DD E078 ABD3 E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- RIASZTÁSOK
- TÁJÉKOZTATÁSOK
- BBA+ BESZÁMOLÓ

NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍREK

Az ASUS a DSL-routerek kritikus sérülékenységére hívja fel a figyelmet

(bleepingcomputer.com)

Az ASUS figyelmeztetést adott ki több DSL-sorozatú routert érintő kritikus sebezhetőségről. A CVE-2025-59367 azonosítón nyomon követett sérülékenység egy hitelesítés megkerülést (authentication bypass) lehetővé tevő sebezhetőség, amely távoli, nem hitelesített támadók számára adhat közvetlen hozzáférést olyan eszközökhöz, amelyek az internethez csatlakoznak és nem rendelkeznek a legfrissebb firmware-rel. **Bővebben...**

A Fortinet javította a FortiWebet érintő nulladik napi sérülékenységet

(bleepingcomputer.com)

A Fortinet megerősítette, hogy javította azt a kritikus, nulladik napi sérülékenységet, amelyet aktívan kihasználtak a FortiWeb webalkalmazás-tűzfal (web application firewall) bizonyos verziói ellen. **Bővebben...**

Kerberoasting 2025-ben: így védhetők meg a szolgáltatásfiókok

(bleepingcomputer.com)

A Kerberoasting típusú támadások továbbra is komoly kihívást jelentenek az Active Directory-t üzemeltető informatikai szakemberek számára. Ez a technika lehetővé teszi a kiberbűnözők számára, hogy egy kezdetben alacsony jogosultságú felhasználói fiókból rövid idő alatt magasabb szintű jogosultságot szerezzenek, akár egészen az Active Directory (AD) környezet legmagasabb szintjéig. **Bővebben...**

A RondoDox botnet az XWiki-platformot veszi célba

(bleepingcomputer.com)

A RondoDox botnet a CVE-2025-24893 azonosítón nyomon követett, kritikus RCE-sérülékenység (remote code execution) kihasználásával az XWiki platformot célozza.
Bővebben...

15 Tbps-os DDoS-támadás érte a Microsoft Azure-t az Aisuru botnetről

(bleepingcomputer.com)

A Microsoft bejelentette, hogy az Aisuru botnet több mint 500 000 IP-címről indított egy masszív, 15,72 Tbps (terabit/másodperc) csúcsértékű DDoS-támadást az Azure hálózata ellen.
A támadók rendkívül nagy sebességű UDP-floodokat alkalmaztak, amelyeket egy Ausztráliában található konkrét nyilvános IP-cím ellen irányítottak.
Bővebben...

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

2025. 11. 14. — 2025. 11. 20.

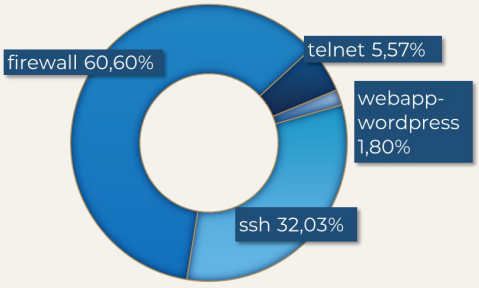
Fenyegetettségi szint:

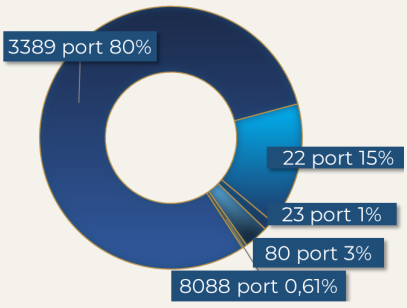
alacsony | közepes | magas | kritikus

Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok

Az adatsorok melletti nyilak az előző héthez viszonyított változásokat mutatják.

Az elosztott kormányzati IT biztonsági csapdarendszerből (GovProbe1) származó adatok





NEMZETI KIBERBIZTONSÁGI INTÉZET

RIASZTÁSOK TÁJÉKOZTATÁSOK

Riasztás
Microsoft termékeket érintő sérülékenységekről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI) riasztást ad ki a **Microsoft szoftvereket érintő kritikus kockázati besorolású sérülékenységek** kapcsán, azok súlyossága, kihasználhatósága és a szoftverek széleskörű elterjedtsége miatt.

A Microsoft 2025. november havi biztonsági csomagjában összesen **63 különböző biztonsági hibát** javított, köztük **1 db nulladik napi (zero-day) sebezhetőséget** is amelyet a Microsoft tájékoztatása szerint támadók kihasználhattak, mivel már a javítás előtt publikálásra került.

Elolvasom

Tájékoztatás Adobe szoftverek sérülékenységeiről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI) **tájékoztatót ad ki az Adobe szoftverfejlesztő cég termékeit érintő sérülékenységekkel kapcsolatban**, azok súlyossága, valamint az egyes biztonsági hibákat érintő aktív kihasználások miatt.

Elolvasom

BBA+ BESZÁMOLÓ

Global Cyber Conference 2025

2025. október 22-23.

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet** munkatársai **Széchenyi Terv Plusz pályázat** részeként szakmai ismeretbővítésen vesznek részt a súlyos és szervezett, határon átnyúló bűncselekmények elleni küzdelem, illetve ilyen jellegű bűncselekmények megelőzésének fejlesztése céljából.

A projekt célja a kiberfenyegetések elleni fellépéshez szükséges friss ismeretek gyűjtése és megosztása a hazai kiberbiztonsági szakemberekkel.

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

BBA+ BESZÁMOLÓ

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

A Nemzeti Kiberbiztonsági Intézet munkatársai **2025. október 22-23.** között részt vettek a Zürichben megrendezésre kerülő éves **Global Cyber Conference 2025 eseményen**.

A konferencia fő célja az **aktuális kiberbiztonsági trendek, a mesterséges intelligencia térnyerése, valamint a kibervédelem és kiberreziliencia nemzetközi tapasztalatainak bemutatása** volt. Kiemelt hangsúlyt kapott a **szakmai közösség összekapcsolása**, valamint a köz- és magánszféra közötti együttműködés erősítése. A rendezvény színvonalát jól tükrözte a részt vevő szervezetek köre: többek között a svájci Nemzeti Kiberbiztonsági Központ (NCSC), a Palo Alto Networks, a UBS, a DHL, a Siemens Energy és az EY vezető szakértői tartottak előadásokat.

A program fő témái az alábbi területekre fókuszáltak:

- AI-alapú fenyegetésészlelés és védekezés,
- Zero Trust architektúrák és identitásalapú biztonsági modellek,
- Ellátási láncok kiberrezilienciája és a harmadik felek kockázatkezelése,
- AI-etika és kormányzás nagyvállalati és szabályozói nézőpontból.

A plenáris előadások és panelbeszélgetések egyértelművé tették, hogy a mesterséges intelligencia a támadók és a védők oldalán is új korszakot nyit. Olyan jelenségek, mint a „shadow AI”, az AI-vezérelt adathalász és deepfake támadások vagy az automatizált SOC-működés új lehetőségeket, ugyanakkor komoly kockázatokat is teremtenek.

A résztvevők egyetértettek abban, hogy a humán tényező, az átlátható irányítás és a bizalom továbbra is a kiberreziliencia alapjai maradnak – még a legfejlettebb technológiai környezetben is.

A konferencia gyakorlatorientált megközelítése és magas szintű nemzetközi részvétele lehetőséget biztosított:

- tapasztalatcserére,
- kapcsolatépítésre,
- valamint a svájci kiberbiztonsági modell – különösen az állami-piaci együttműködés és a „Resilience by Design” szemlélet – megismerésére.

Kiknek ajánlott a beszámoló megismerése?

- Kiberbiztonsági szakemberek számára
- Vállalati IT-biztonsági csapatoknak
- Kiberfenyegetés-kutatóknak és elemzőknek
- Biztonsági mérnököknek és fejlesztőknek

A konferencia legfontosabb előadási az alábbiakban foglalhatók össze.

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

BBA+ BESZÁMOLÓ

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

Cyber Defence in Swiss Armed Forces

(Divisionär (Major General) Simon Müller, Chief of Cyber Command, Swiss Armed Forces)

Az előadás betekintést nyújtott a **Svájci Fegyveres Erők kibervédelmi stratégiájába**, amely a fizikai és digitális hadszínterek összekapcsolására épül. A kiberparancsnokság célja, hogy az ellenfélnél **gyorsabb döntési ciklusokat** (OODA-loop) biztosítson, ezáltal informatikai fölényt szerezzen.

A hadsereg **három adatközpontot üzemeltet**, köztük két olyan létesítményt, amelyek nukleáris támadásoknak is ellenállnak, továbbá saját optikai hálózattal és áramellátással rendelkezik. Vészhelyzet esetén decentralizált, „mini adatközpontokból" álló infrastruktúrára állnak át, hogy a létfontosságú adatok helyben is elérhetők maradjanak. A szolgáltatások redundáns módon, a **PACE-modell** (Primary–Alternate–Contingency–Emergency) alapján épülnek fel, ahol a legvégső szintet akár analóg rendszerek is jelenthetik. Az előadó hangsúlyozta: **a kiberbiztonság nem luxus, hanem stratégiai beruházás** – „minél felkészültebb egy nemzet, annál ritkábban válik támadás célpontjává".

Securing Switzerland's Digital Future through Collaboration

(Silvan Schellenberg, CISO Switzerland – UBS)

Schellenberg előadásának középpontjában a **nemzeti és ágazatközi együttműködés** állt, amelyet Svájc digitális jövőjének alapköveként határozott meg. Egy valós esettanulmányban két információbiztonsági vezető (CISO) közötti gyors információmegosztás akadályozott meg egy mesterséges intelligencia által generált adathalász kampányt. Ez szerinte tökéletes példája annak, hogy nem a technológia, hanem az emberek közötti bizalom képes életeket és adatokat megvédeni.

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

Az UBS aktívan részt vesz a Swiss Finance Sector Cyber Security Centre (FS-CSC) és a Nemzeti Kiberbiztonsági Központ (NCSC) közös tevékenységeiben, valamint több nemzetközi kezdeményezésben, mint például a Geneva Dialogue és a Digital Security Switzerland.

Schellenberg kiemelte a mesterséges intelligencia és a kvantumtechnológia kettős természetét: ezek a technológiák **egyszerre hordoznak jelentős kockázatokat és ígéretes fejlődési lehetőségeket.**

A jövő zálogát egy jól képzett, etikus és sokszínű szakembergárdában látja, hiszen – ahogy fogalmazott – „**reziliens rendszert csak reziliens emberek képesek felépíteni**”.

The 2025 Threat Landscape – What Keeps CISOs Awake at Night

(Tim Brown, CISO – SolarWinds)

Brown előadása az **egyre gyorsuló fenyegetési ciklusokra** hívta fel a figyelmet: míg korábban az átlagos észlelési idő 26 nap volt, 2024-re ez 7 napra csökkent, és a gyors támadások esetében 2026-ra mindössze 1–2 órát prognosztizálnak. A CISO szerint a hagyományos, emberi döntéshozatalra épülő védekezés már nem elegendő; a jövő az **autonóm biztonsági műveleti központok** (SOC-ok) és a **gépi tanulásra épülő védelmi megoldások** irányába mutat.

A támadók és a védők közötti „**fegyverkezési versenyben”** a mesterséges intelligencia mindkét oldal eszközévé vált. Brown úgy véli, a kiberbiztonsági iparágnak szemléletváltásra van szüksége: ahelyett, hogy újra és újra „levágjuk a pók fejét”, **rendszerszintű, együttműködésen alapuló stratégiákat kell kialakítani**. A hatékony védekezés kulcsa nem a tökéletesség elérése, hanem annak biztosítása, hogy az üzleti működés fennmaradjon még kompromittált környezetben is.

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

Cyber Resilience Reality Check

(Frank Fischer, Group CISO – DHL Group)

Frank Fischer előadása gyakorlati megközelítésben mutatta be, mit jelent a **valódi kiberreziliencia** egy globális, több kontinensen működő logisztikai vállalat esetében. Rámutatott, hogy a **védekezés nem csupán technológiai kérdés**, hanem a szervezeti kultúra és a folyamatérettség eredménye is.

A DHL-nél évente több ezer biztonsági eseményt elemeznek, és a tapasztalatokból kiindulva tudatosan építik be a **„fail fast, learn fast" szemléletet** a működésükbe. Fischer hangsúlyozta, hogy a krízishelyzetekre való felkészülés nem pusztán elméleti gyakorlat: a vállalat rendszeresen teszteli helyreállítási képességeit, beleértve a beszállítói láncot és az üzleti partnereket is.

Zárásként kiemelte: a reziliencia lényege nem abban rejlik, hogy soha ne hibázzunk, hanem abban, hogy amikor az elkerülhetetlen mégis bekövetkezik, **képesek legyünk gyorsan, átláthatóan és összehangoltan reagálni.**

Supply Chain Security in Turbulent Times

(Roman Haltinner, Cybersecurity Competency Leader – EY Switzerland)

Roman Haltinner előadásában a **beszállítói láncok sebezhetőségére** hívta fel a figyelmet, mint a modern gazdaság egyik Achilles-sarkára. Kiemelte, hogy a globális ellátási láncok ma már oly mértékben összekapcsoltak, hogy akár egyetlen IT-hiba vagy frissítési anomália is hetekre megbéníthatja a logisztikai folyamatokat – ahogy arra egy svájci példa is rávilágított, amikor egy szoftverhiba következtében a sajtkészletek eltűntek a boltok polcairól.

A szakértő szerint a kiberreziliens beszállítói láncok kialakításának kulcselemei:

- a teljes körű átláthatóság,
- az autonóm és redundáns működés,
- valamint a kiberbiztonsági követelmények szerződéses rögzítése a partnerek felé.

Bár az új uniós és svájci szabályozások – például a NIS2 és a Cyber Resilience Act – fontos lépést jelentenek, önmagukban nem elegendőek. Csak akkor lehetnek igazán hatékonyak, ha a vállalatok valódi, kockázatmegosztáson alapuló bizalmi kultúrát alakítanak ki.

Resilience by Design – CISO Perspectives

(Christine Fahlberg (Swisscard AECS GmbH), Marcos Marrero (H.I.G. Capital), Marcel Zumbühl (Swiss Post, Samir Aliyev (Swiss Cyber Institute)

A panelbeszélgetés középpontjában a **reziliencia tudatos és tervezett építése** állt. A résztvevők egyetértettek abban, hogy a biztonsági kultúrát **nem utólag** kell ráépíteni a szervezetre, hanem annak „DNS-ébe” kell kódolni **már a kezdetektől**.

A Swiss Post esettanulmánya jól példázta az emberi tényező jelentőségét: 60 000 munkatárs közül két alkalmazott ébersége akadályozta meg a Black Basta zsarolóvírus támadását, bizonyítva, hogy az **aktív dolgozói részvétel a leghatékonyabb védelmi vonal**.

A panel tagjai hangsúlyozták a hibák nyílt és konstruktív kezelésének fontosságát is – **a vezetők feladata példát mutatni, nem hibást keresni**. Technológiai szempontból a mikroszegmentáció, az identitásalapú hozzáférés-kezelés, valamint a Zero Trust architektúra kerültek előtérbe, mint a reziliencia kulcselemei.

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

A beszélgetés zárógondolata szerint a reziliencia nem egy egyszeri projekt, hanem folyamatos tanulás, önreflexió és bátorság kérdése.

Third-Party & Supply Chain Risk Governance – Lessons from Recent Mega-Breaches

(Tim Brown (SolarWinds), Frank Fischer (DHL Group), Filip Nowak (Ferrero), Brett Conlon (American Century Investments)

A panelbeszélgetés a **beszállítói láncban keletkező kockázatok vállalati szintű kezelésére** fókuszált. Tim Brown szerint a SolarWinds-incidens rávilágított arra, hogy a kockázat kollektív jellegű: még a legszigorúbb kontrollintézkedések mellett is megfertőződhet az egész ökoszisztéma.

Frank Fischer (DHL) hangsúlyozta, hogy a vállalatoknak elsősorban a **váratlan eseményekre kell felkészülniük**, és az üzletmenet-folytonosságot nem évente, hanem **folyamatosan kell tesztelniük**, beleértve az ellátási lánc kritikus pontjait is.

A résztvevők kiemelték: a CrowdStrike-hoz köthető frissítési hiba példája jól mutatja, hogy akár egyetlen technikai anomália is globális hatással járhat. A legfontosabb tanulságok között szerepelt a rugalmas rendszerarchitektúra, az adaptív válságkezelés, valamint a proaktív és átlátható kommunikáció.

A beszélgetés zárógondolata szerint a jövőben nem az lesz a döntő, ki tudta elkerülni a támadásokat, hanem az, ki képes **gyorsan, transzparensen és együttműködve reagálni a válsághelyzetekre.**

AI-Driven Malware & Adaptive Threats

(Axel Fehrmann, Group CISO – Emil Frey Group)

Axel Fehrmann előadásában arra világított rá, **hogyan alakítja át a mesterséges intelligencia a kiberfenyegetések természetét**. A hagyományos vírusok és trójai programok helyét egyre inkább tanuló és adaptív támadások veszik át, amelyek célzottan az emberekre és a bizalmi rendszerekre irányulnak.

A bemutatott példák között szerepelt egy deepfake-alapú pénzügyi csalás is: egy vállalat pénzügyi vezetője 25 millió dollárt utalt át egy hamisított videóhívás hatására. Az AI-vezérelt támadók ma már képesek személyre szabott manipulációra, hangutánzásra, sőt érzelmi ráhatásra is.

Fehrmann hangsúlyozta, hogy a jövő biztonságának kulcsa nem kizárólag technológiai eszközökben – mint például tűzfalakban – keresendő, hanem az **emberi ítélőképesség fejlesztésében** és megerősítésében.

Záró gondolata különösen erős hatást gyakorolt a hallgatóságra:

„Ha a következő támadás nem a hálózatodban, hanem a hitedben történik – felkészültél rá?”

AI Threat Intelligence – Hype or Reality (Panel)

(Axel Fehrmann (Emil Frey Group), Katerina Mitrokotsa (University of St. Gallen), Yassine Ilmi (Thomson Reuters), Robert Kang (Loyola Law School / USC Center for AI and Digital Policy)

A panelbeszélgetés központi kérdése az volt, mennyiben megalapozott az **MI-alapú fenyegetésfelderítés** körüli várakozás.

BBA+ BESZÁMOLÓ

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

Katerina Mitrokotsa rámutatott, hogy a mesterséges intelligencia több mint két évtizede jelen van az anomáliadetektálás területén – például IDS/IPS rendszerekben –, így a jelenlegi felhajtás inkább egy **evolúciós lépcső**, semmint forradalmi áttörés.

Axel Fehrmann az MI-t „gondolati sparring partnerként" jellemezte: a generatív modellek különösen hasznosak lehetnek egy-egy fenyegetés kontextusának gyorsabb megértésében és strukturálásában.

Yassine Ilmi a tanítóadatok minőségének és az AI-modellek megbízhatóságának kérdését emelte ki. Szerinte a zárt rendszerek ugyan nagyobb biztonságot nyújtanak, viszont kevésbé rugalmasak új fenyegetések azonosításakor.

A panel egyetértett abban, hogy a leghatékonyabb megközelítés **több modell kombinációján**, valamint az emberi felülvizsgálaton alapul.

A beszélgetés zárógondolata szerint:

- az MI nem helyettesíti az elemzőt, hanem megtöbbszörözi a hatékonyságát – ha megfelelően irányított és kontrollált környezetben alkalmazzák.

What will happen next: Future AI Security Playbook

(Andy Schneider, Chief Security Officer EMEA Central – Palo Alto Networks)

Az előadás a **mesterséges intelligencia-alapú korszak** (AI-native era) **kibervédelmi hatásait** vizsgálta, ahol az automatizáció és a gépi döntéshozatal fokozatosan átveszi az ember szerepét az incidenskezelésben.

Andy Schneider előadó adatai szerint az AI-t alkalmazó rendszerek közötti adatforgalom havi szinten 32%-kal növekszik, ami éves szinten akár harmincszoros emelkedést is eredményezhet. A támadások észlelési ideje drasztikusan rövidül: míg 2021-ben a medián „tartózkodási idő” (dwell time) 26 nap volt, 2026-ra ez 7 napra, a leggyorsabb támadások esetében akár 5 órára csökkenhet.

A prezentáció kitért a **„Shadow AI” jelenségre** is – arra a növekvő problémára, hogy a vállalatok sokszor több tucat **nem engedélyezett mesterségesintelligencia-eszközt használnak**, amelyek komoly biztonsági kockázatot jelentenek. Schneider szerint a kiberbiztonság fordulóponthoz érkezett: a védelem paradigmája az ember-vezérelt modellről a gép-vezérelt (machine-led security) megközelítésre vált át.

A jövő sikeres védekezési stratégiáját az **„Amplify – Govern – See” hármas modellben** foglalta össze. Ez az MI képességeinek erősítésére (amplify), szabályozására (govern), valamint az átláthatóság biztosítására (see) épül. A cél, hogy a biztonsági rendszerek képesek legyenek önállóan tanulni, döntéseket hozni és reagálni – miközben az ember szerepe a stratégiai irányításra korlátozódik.

Schneider záró gondolata szerint 2026-ra az önfejlesztő mesterséges intelligencia válhat a kiberbiztonság valódi motorjává.

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

A Role Model for Other Industries to Increase Cyber Resilience – The Swiss FS-CSC

(August Benz, President – Swiss FS-CSC; Deputy CEO & Head of International and Transformation – Swiss Banking)

A bemutató a Swiss Financial Sector Cyber Security Centre (FS-CSC) működését és példamutató szerepét ismerteti, amely más iparágak számára is követendő lehet. A szervezet célja a **svájci pénzügyi szektor kiberrugalmasságának erősítése és felkészítése egy rendszerszintű kiberválságra.**

A kibertámadások bejelentési kötelezettsége a kritikus infrastruktúrák számára 2025. április 1-jén lépett hatályba, amit a Svájci Szövetségi Tanács március 7-én elfogadott szabályozása alapozott meg. Az első fél évben 164 bejelentés történt. Fontos azonban, hogy a pénzügyi szektor már 2020 óta köteles incidenseit jelenteni a FINMA felé – ennek hazai megfelelője a Magyar Nemzeti Bank.

Az FS-CSC **három fő tevékenységet** végez: kiber-gyakorlatokat szervez, információs platformot működtet, és válságkezelést koordinál. A **válságkezelés három szakaszban zajlik**: normál, krízis és poszt-krízis időszakokban.

A modell sikerének alapja a **köz- és magánszféra együttműködése**, a gyors reagálás és a szektorszintű felkészültség. Ez a megközelítés más ágazatok számára is értékes mintát nyújthat.

NEMZETI KIBERBIZTONSÁGI INTÉZET

AI, Accountability, and the Human Role

(Dr. Gunay Kazimzade, AI Governance Advisor – Siemens Energy)

Az előadás központi gondolata az volt, hogy az **„AI-torzítás”** (AI bias) **nem a kódsorokban kezdődik, hanem az emberekben** – minden adat és algoritmus magán viseli az emberi döntések, értékek és előítéletek lenyomatát.

A felelősségvállalás kérdése három szinten értelmezhető: egyéni, szervezeti és piaci szinten. A hagyományos felelősségi modellek azonban nehezen alkalmazhatók a mesterséges intelligencia rendszerek gyakran átláthatatlan működésére. Ezért van szükség a **megosztott felelősség elvének** érvényesítésére, amely nemcsak technikai, hanem etikai alapú elszámoltathatóságot is megkövetel.

A biztonság kulcsa az átláthatóság, a folyamatos ellenőrzés és a váratlan eseményekre való szervezeti felkészültség. Az **AI-elszámoltathatóság** célja nem a hibáztatás, hanem a felelősségteljes előrelátás és az etikus gondnokság (stewardship) kialakítása.

Az előadás egyik legfontosabb üzenete szerint az AI-elszámoltathatóság csak akkor valósulhat meg, ha a technológiai és etikai dimenziók mellett az emberi szerep és a szervezeti kultúra is tudatosan integrálódik. A biztonság és az etika tehát nem pusztán technológiai kihívások, hanem elsősorban emberi feladatok is.

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

BBA+ BESZÁMOLÓ

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

AI in InfoSec: Real-World Lessons from the Front Lines

(Panelbeszélgetés – több szakértő részvételével)

Az előadás **az információbiztonság és a mesterséges intelligencia metszéspontját** vizsgálta, két fő nézőpontból: a **lehetőségek** (Opportunities) és a **kockázatok** (Risks) oldaláról. A panelisták valós példákon keresztül mutatták be, hogyan erősítheti az AI a kiberbiztonságot, ugyanakkor milyen új típusú fenyegetéseket idézhet elő.

A mesterséges intelligencia által kínált lehetőségek között kiemelkedő szerepet kapott:

- az adathalász- és kártevőminták automatizált felismerése,
- a természetes nyelvfeldolgozás (NLP) alkalmazása szabályzatok és előírások elemzésére,
- a naplóadatok és incidensek gyors feldolgozása,
- a Security Operations Center (SOC) műveletek támogatása – például riasztások korrelálása, elemzése és automatizált jelentéskészítés révén.

Továbbá szó esett AI-alapú asszisztensek szerepéről a biztonságos kódolás támogatásában, illetve chatbotok alkalmazásáról az incidenskezelés során.

A kockázati oldalról a résztvevők több tényezőt is kiemeltek:

- AI-generált adathalász támadások,
- automatikusan létrehozott exploitok,
- a „Shadow AI” (ellenőrizetlenül használt MI-eszközök) terjedése,
- modelltorzítás és adatmérgezéses támadások,
- hibás nagy nyelvi modell (LLM) kimenetekből fakadó téves döntések,

- valamint a biztonsági operációs központokban tapasztalható riasztásfáradtság (alert fatigue).

A panel egyértelmű konklúziója szerint a mesterséges intelligencia kettős természetű eszköz: megfelelő irányítás és etikus alkalmazás mellett kulcsszerepet játszhat a védekezés megerősítésében, ám kontroll nélkül a támadók kezében is rendkívül hatékony fegyverré válhat.

IT/OT Convergence & Critical Infrastructure Protection

(Filip Nowak (Ferrero), Markus Lüthi (City of Zurich Police), Patrick Gilliéron (Siemens Schweiz AG), Andreas Schneider (TX Group)

A panelbeszélgetés az **informatikai** (IT) és az **üzemeltetési technológiai** (OT) **rendszerek összekapcsolódásából fakadó kihívásokat** vizsgálta. A résztvevők egyetértettek abban, hogy az eltérő biztonsági kultúrák közötti **kommunikációs szakadék** jelenti az egyik legnagyobb kockázatot.

Míg az OT-szakemberek gyakran a „ha működik, ne nyúlj hozzá” elvét követik a folytonosság érdekében, addig az IT világában a kontroll, az auditálhatóság és a rendszeres frissítés az elsődleges szempont. Ez az eltérés nehezíti a közös nyelv és szemlélet kialakítását.

A beszélgetés kiemelte a közös hálózatok, a közös kockázatkezelési gyakorlatok, valamint a shared situational awareness – azaz a megosztott helyzetértékelés – fontosságát.

A panel tagjai szerint a jövő biztonságának kulcsa:

- a tudásmegosztás erősítése IT és OT szakemberek között,
- a pótlási képzés (succession training) megvalósítása, mivel számos kritikus infrastruktúránál a nyugdíjba vonuló, tapasztalt OT-szakértők tudásvesztése komoly kockázatot jelent,

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

BBA+ BESZÁMOLÓ

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

- valamint az IT és OT rendszerek elkülönített identitás- és jogosultságkezelése, hogy egyetlen kompromittált fiók se indíthasson el láncreakciós jellegű támadást.

Global Cybersecurity Governance 2.0

(Daniel Hünermann (Nestlé), Orhan Osmani (International Telecommunication Union – ITU), Lido Dekker (Geneva Centre for Security Sector Governance – DCAF)

A fórum a **globális kiberkormányzás új dimenzióit** vizsgálta, különös tekintettel a technológiai, intézményi és kulturális együttműködés szerepére.

Orhan Osmani az ITU képviseletében bemutatta a **Global Cybersecurity Index** (GCI) jelentőségét, amely nem csupán az egyes országok technikai érettségét, hanem azok kiberbiztonság iránti politikai és stratégiai elkötelezettségét is méri.

Lido Dekker kiemelte, hogy a kibervédelem terén a hagyományos, hierarchikus irányítási modellek egyre kevésbé működőképesek. Helyüket a **co-governance** – vagyis a megosztott döntéshozatalon, közös felelősségen és átláthatóságon alapuló kormányzási megközelítés – veszi át.

Daniel Hünermann gyakorlati példákon keresztül mutatta be, hogyan fejlődik a **vállalati kiberirányítás** a megfelelésközpontú (compliance-based) szemléletből egy **reziliencia-orientált biztonsági kultúra** felé, ahol a folyamatos alkalmazkodás és tanulás kerül előtérbe.

A résztvevők hangsúlyozták, hogy **a fejlett és fejlődő országok közötti kiberképességbeli szakadék** a globális biztonság egyik legsebezhetőbb pontja. A kiberbűnözők gyakran gyorsabban és hatékonyabban működnek együtt, mint az államok vagy nemzetközi szervezetek.

A fórum záró gondolata szerint a jövő kiberkormányzásának nem csupán jogi keretrendszerekre kell épülnie, hanem egy **bizalmi ökoszisztémára**, amelyben a normák, a szervezeti kultúra és a közös tanulás fontosabb szerepet kapnak, mint a puszta szabályozás.

Quantum-Ready Cryptography & Transition Strategies

(Andy Schneider, Chief Security Officer EMEA Central – Palo Alto Networks)

Andy Schneider előadása a közelgő kvantumkor kapcsán szükségessé váló **kriptográfiai átállás kihívásait és lépéseit** elemezte.

Kiemelte, hogy a szervezetek számára első lépésként **kriptográfiai eszköztár-felmérést** kell végezniük, vagyis pontosan fel kell térképezniük, hol és milyen titkosítási technológiákat alkalmaznak. Ezt követően egy **poszt-kvantum kriptográfiai** (PQC) **migrációs tervet** kell kidolgozni, amely figyelembe veszi a meglévő rendszerek teljesítmény- és erőforrás-igényeit is.

A **„harvest now, decrypt later" típusú támadások** – vagyis a most titkosított adatok későbbi, kvantumszámítógéppel történő visszafejtése – ellen Schneider **hibrid titkosítást** javasolt, amely klasszikus és poszt-kvantum algoritmusokat egyaránt alkalmaz. Emellett a hosszú távon érzékeny adatok esetében a Quantum Key Distribution (QKD) használata is indokolt lehet.

Az előadó hangsúlyozta, hogy a kvantumbiztos védelem nem csupán technológiai, hanem stratégiai szintű feladat, amely vállalati tudatosságot, szervezeti elkötelezettséget és folyamatos tesztelést igényel.

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

BBA+ BESZÁMOLÓ

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

The Future of Cloud Security: Privacy, Compliance, and Confidential AI

(Patrick McCarthy, Senior Cybersecurity Advisor – Huawei Cyber Security Transparency Center (Brussels)

Patrick McCarthy előadásában a **felhőbiztonság jövőjét** vizsgálta a mesterséges intelligencia fejlődése és az adatvédelmi szabályozások összefüggésében. Kiemelt figyelmet szentelt a **„Confidential AI" koncepciónak**, amely a következő évek egyik központi trendje lehet.

Ez olyan **felhőalapú MI-szolgáltatásokat** jelent, ahol az adatok feldolgozása titkosított, auditálható és szabályozott környezetben történik – biztosítva ezzel az adatvédelmi követelményeknek való megfelelést és a felhasználói bizalom fenntartását.

McCarthy hangsúlyozta, hogy a felhőszolgáltatásokhoz kapcsolódó kiberkockázatokat nemcsak a technológiai infrastruktúra, hanem a **szerződéses feltételek** is meghatározzák. Ilyen kritikus tényezők többek között az adatkezelési szabályozások, az exit-stratégia, valamint a szolgáltatási szintmegállapodások (SLA-k). Mindez azt jelzi, hogy a felhőbiztonság egyre inkább technikai, jogi és etikai kérdéssé is válik.

Az előadó szerint a jövő felhőbiztonsági ökoszisztémáját három alappillér határozza meg:

- a bizalomra épülő együttműködés,
- az MI-biztonság integrálása a szolgáltatásokba,
- valamint a transzparens, szabályozott adatkezelés.

Ask Me Anything: Metrics for Measuring Cyber Resilience

(Sascha Maier (SV Group), Tana Dubel (Logitech), Marc Minar (EY Switzerland), Samir Aliyev (Swiss Cyber Institute)

A záró panelbeszélgetés a **kiberreziliencia mérhetőségének dilemmáit** járta körül. A résztvevők egyetértettek abban, hogy a jelenleg használt mutatók – például a javítócsomagok (patch-ek) száma, a szolgáltatási szintmegállapodások (SLA-k), vagy a hibaelhárítási idő (MTTR) – nem tükrözik valósághűen a szervezeti felkészültséget és alkalmazkodóképességet.

A jövőben a hangsúly egyre inkább **viselkedési mutatókra**, **válságkezelési reakcióidőre**, valamint az emberi tényező szerepére helyeződik át. Ez utóbbi különösen fontos, hiszen a felhasználók és a munkatársak reakciói gyakran döntőek egy támadás kimenetele szempontjából.

A panel kiemelte: a kiberreziliencia nem egyetlen audit vagy szabályozási megfelelés eredménye, hanem egy folyamatos tanulási, tesztelési és adaptációs folyamat, amelyben a hibákból és válsághelyzetekből levont tanulságok sokszor értékesebbek, mint a formális megfelelőség.

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

BBA-PLUSZ-3.1.2-24-2024-00004. sz. pályázat részeként

Összefoglalás

A kétnapos rendezvény egyik legfontosabb tanulsága, hogy a **kiberreziliencia** kérdése messze **túlmutat a technológiai eszközökön és megoldásokon**. Bár a fejlett infrastruktúra, a mesterséges intelligencia és a kriptográfia kulcsszerepet játszanak a kiberbiztonság megerősítésében, a **valódi ellenálló képesség ökoszisztéma-szintű együttműködésből, szervezeti kultúrából és folyamatos tanulásból születik.**

A különböző szekciók és előadások egyértelművé tették, hogy a biztonság nem kizárólag technikai megfelelés, hanem **stratégiai gondolkodás**, **átláthatóság** és **emberi ítélőképesség** kérdése is. A panelbeszélgetések rendre hangsúlyozták: a legfejlettebb védelmi rendszerek is sérülékenyek maradnak, ha hiányzik a szervezetek közötti bizalom, a belső kultúrában pedig nincs helye a hibák nyílt és tanulási célú kezelésének.

A **svájci modell inspiráló** példát kínál arra, hogyan lehet egy digitálisan fejlett társadalomban decentralizált, emberközpontú és bizalomra épülő védekezést kialakítani. Az állami és magánszektor közötti együttműködés, a közös kockázatkezelés, valamint az etikus technológiahasználat mind hozzájárulnak egy olyan reziliens rendszer felépítéséhez, amely nemcsak reagál a fenyegetésekre, hanem alkalmazkodni is képes hozzájuk.

A konferencia zárógondolata így foglalható össze: a kiberreziliencia nem egy végállapot, hanem folyamatos gyakorlat, amely az emberek felkészültségén, a szervezetek együttműködésén és a technológia felelős alkalmazásán nyugszik.