NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2025. 26. hét

HÍREK

- A Cisco AnyConnect VPN sérülékenysége
- Admin jog szerezhető az ASUS Armoury Crate kihasználásával
- Súlyos sérülékenység a WordPress „Motors” témában: veszélyben az admin jogosultság
- Új típusú mobil kártevő támadja a kriptotárcákat: megjelent a SparkKitty malware
- Kritikus fenyegetés a Microsoft Exchange szerverek ellen

STATISZTIKAI ADATOK

- Incidensek eloszlása típus és kockázati besorolás szerint
- Események eloszlása csapdatípusok alapján
- Támadott port szerinti eloszlás

TÁJÉKOZTATÁSOK

- Tájékoztatás az MVM Next Energiakereskedelmi Zrt. nevével visszaélő visszaélő SMS üzenetekkel kapcsolatban
- Tájékoztatás Technikai támogatásnak álcázott online csalások

BESZÁMOLÓ

- Cyber Intelligence Europe 2025
  Madrid, Spanyolország

KONTAKT

edt@nki.gov.hu

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D

NEWS

IT biztonsági
HÍREK

A Cisco AnyConnect VPN sérülékenysége
(gbhackers.com)

A vállalati hálózatok biztonsága kiemelten fontos napjainkban, különösen mivel a dolgozók távoli munkavégzése egyre inkább a mindennapi üzleti működés részévé válik. Az egyik legelterjedtebb VPN megoldás, amelyet a vállalatoka biztonságos távoli hozzáférés biztosítására használnak, a Cisco AnyConnect VPN. **Bővebben...**

Admin jog szerezhető az ASUS Armoury Crate kihasználásával
(bleepingcomputer.com)

A CVE-2025-3464 azonosítón nyilvántartott, 8.8-as súlyosságú ASUS Armoury Crate sérülékenység kihasználásával rendszergazdai jogosultságok szerezhetők az érintett számítógépeken. A sebezhetőség az AsIO3.sys nevű rendszerkomponensben található. **Bővebben...**

Új típusú mobil kártevő támadja a kriptotárcákat: megjelent a SparkKitty malware
(bleepingcomputer.com)

2024 februárjától kezdődően egy új mobil kártevő, a SparkKitty aktív terjedését figyelték meg szakértők, amely Android és iOS platformokat egyaránt célba vesz. A Kaspersky jelentése szerint ez a kártevő egy korábbi malware, a SparkCat továbbfejlesztett változata lehet. **Bővebben...**

Kritikus fenyegetés a Microsoft Exchange szerverek ellen
(thehackernews.com)

A Microsoft Exchange szerverek hosszú évek óta a cégek és kormányzati szervezetek egyik legfontosabb kommunikációs eszközei közé tartoznak. Ugyanakkor, ezek az infrastruktúrák gyakran a támadók célkeresztjében állnak. **Bővebben...**

Súlyos sérülékenység a WordPress „Motors” témában: veszélyben az admin jogosultság
(bleepingcomputer.com)

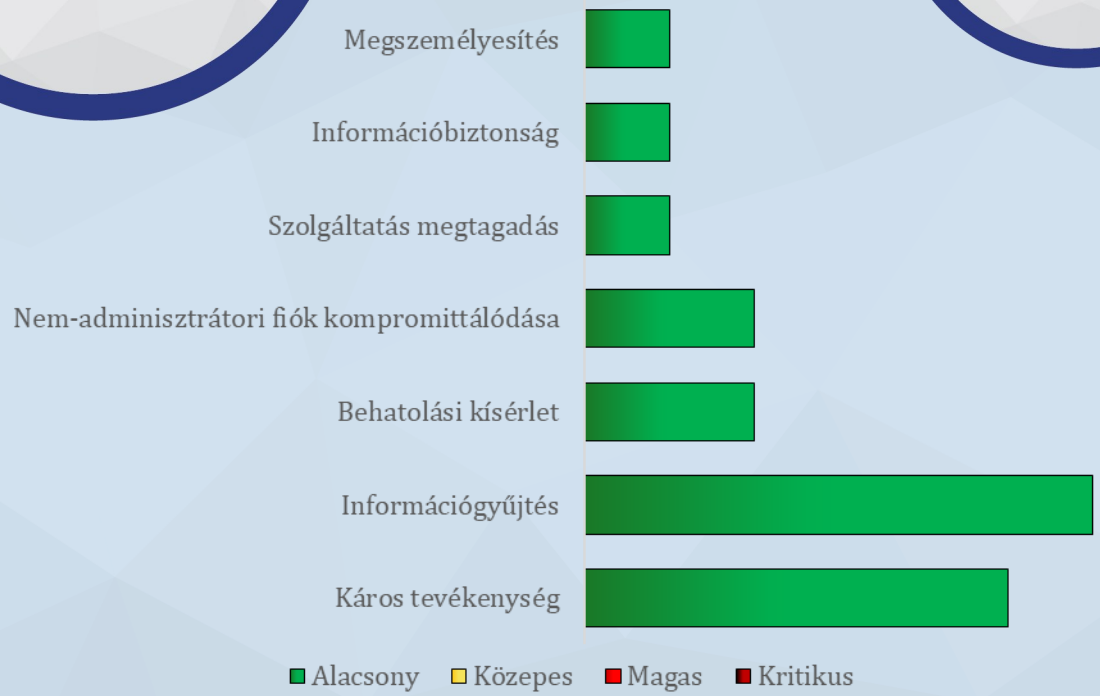
A WordPress világszerte a legnépszerűbb tartalomkezelő rendszer, azonban népszerűsége miatt a kiberbűnözők folyamatos célpontja is. A sablonok és bővítmények sebezhetőségei különösen nagy veszélyt jelentenek, hiszen ezek gyakran közvetlen hozzáférést biztosítanak a webhelyek kritikus funkcióihoz.
Bővebben...

Statisztikai Adatok

2025.06.20.-2025.06.26.

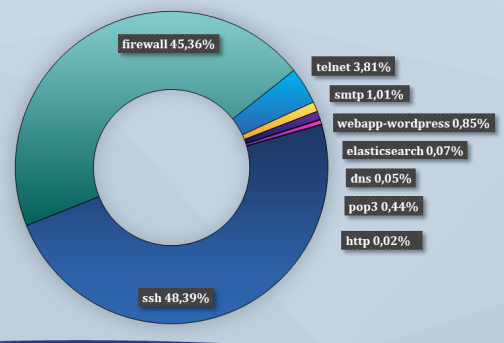
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

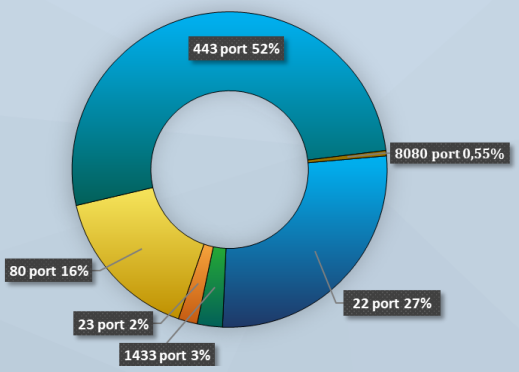
Fenyegetettségi szint: alacsony



Incidensek eloszlása típus és kockázati besorolás szerint

Az elosztott kormányzati IT-biztonsági csapdarendszerből (Gov1probe) származó adatok:





További érdekességekért, látogasson el **weboldalunkra**!

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK

Tájékoztatás az MVM Next Energiakereskedelmi Zrt. nevével visszaélő SMS üzenetekkel kapcsolatban

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet** az MVM Next Energiakereskedelmi Zrt. nevével és arculati elemeivel visszaélő, adathalász hivatkozást tartalmazó szöveges üzenetek (SMS) terjedésére hívja fel a figyelmet.

Az MVM Next Energiakereskedelmi Zrt. tájékoztatása szerint a legújabb **csalási kísérletek** most **SMS-ben érkeznek** az ügyfelekhez és **nem létező tartozásra vonatkoznak**.

Bővebben...

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el LinkedIn oldalunkra!

TÁJÉKOZTATÓK, SÉRÜLÉKENYSÉGEK, RIASZTÁSOK

Tájékoztatás
Technikai támogatásnak álcázott online csalások

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet** tájékoztatót ad ki a technikai támogatásnak álcázott csalások újabb formájának megjelenésével kapcsolatban.

A Malwarebytes kutatásokért felelős igazgatója által feltárt valós esetek alapján a csalók hamis keresési találatokkal élnek vissza, kihasználva a felhasználók bizalmát az ismert márkák – például az Apple, a Microsoft, a Facebook, a Netflix, a Bank of America vagy a PayPal – iránt.

Bővebben...

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el LinkedIn oldalunkra!

Aktuális tartalmak

NEMZETI KIBERVÉDELMI INTÉZET

1996 NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

Kapu az internethez: böngéssz biztonságosan!

[örökzöld]

Ebben az epizódban a **böngészők** világába merülünk el – azokba az eszközökbe, amelyeket nap mint nap használunk, mégis ritkán gondolunk rájuk **biztonsági szempontból**. Megnézzük, hogyan fordíthatják a hackerek ezeket az ártalmatlannak tűnő programokat a felhasználók ellen, és **mit tehetünk** annak érdekében, hogy ne mi legyünk a következő célpont.

Meghallgatom

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el LinkedIn oldalunkra!

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

Cyber Intelligence Europe 2025

2025. április 29-30.

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi 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.

Széchenyi Terv Plusz Építsük együtt Magyarországot!
Magyarország Kormánya
Az Európai Unió társfinanszírozásával

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

A **Nemzeti Kibervédelmi Intézet** munkatársai részt vettek a 2025. április 29-30. között Madridban megrendezésre kerülő éves **Cyber Intelligence Europe** konferencián.

A nemzetközi rendezvény célja az volt, hogy elősegítse a tapasztalatcserét azok között a szakemberek között, akik a **kormányzati kiberbiztonsági stratégiák** kidolgozásán és megvalósításán dolgoznak. A kétnapos konferencia során a kiberbiztonság aktuális kihívásait, gyakorlati megközelítéseit és fejlődési irányait vitatták meg. Az esemény esettanulmányokon és szakértői előadásokon keresztül nyújtott átfogó képet a kiberbűnözési trendekről, a fenyegetések monitorozásáról, a felkészültségről és a potenciális kibertámadásokra adott válaszlépésekről. Kiemelt figyelmet kapott az **EU-tagállamok közötti együttműködés** és az **adatmegosztás** szerepe a kritikus infrastruktúrákat érő, nagyszabású kibertámadások elleni fellépésben. A spanyol kormányzati szervek nemzeti kiberbiztonsági programokban betöltött szerepét is bemutatták, átfogó képet nyújtva az európai kiberbiztonsági helyzetről.

Kiknek ajánlott a beszámoló megismerése?

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

A szakmailag legfontosabb előadások és bemutatók rövid összefoglalója az alábbiakban olvasható.

Széchenyi Terv Plusz Építsük együtt Magyarországot!
Magyarország Kormánya
Az Európai Unió társfinanszírozásával

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

LITHUANIAN NATIONAL APPROACH TO CYBER DEFENSE

(Antanas Aleknavicius)

„A Litván Nemzeti Kiberbiztonsági Központ (**NCSC-LT**) munkatársa előadásában a litván kibervédelmi architektúrát és annak működési elveit mutatta be.

A rendszer stratégiai és operatív szintekre tagolódik: a **kormányzati stratégiai célkitűzések** alá rendelten működnek olyan szervezetek, mint a Honvédelmi Minisztérium, a Nemzeti Válságkezelő Központ, valamint a Kiberbiztonsági Tanács. Ezek felett áll az **NCSC**, amely az operatív végrehajtásért felelős, és koordinálja az együttműködést a rendőrséggel, adatvédelmi hatóságokkal, hírszerzési szolgálatokkal és a 2025-től működő új kiberparancsnoksággal is.

Az NCSC stratégiájának egyik alappillére a **háromvonalas védelmi modell**: az első vonalban a szervezetek saját **SOC**-jai (Security Operations Center) dolgoznak, a második vonalat az NCSC és a szektorális információmegosztási csoportok alkotják (pl. **SISAC** – Sectoral ISACs), a harmadik pedig a nemzeti **CTAC** (Cyber Threat Analysis Capability) csapat, amely elemzéseket, fenyegetésvadászatot és támogató hírszerzést nyújt. Ez a modell lehetővé teszi a strukturált és rétegzett védekezést az ország különböző szintjein.

Külön figyelmet kaptak az oktatási és gyakorlati programok. **Litvániában több mint 65 000 regisztrált felhasználó vesz részt a kibertérhigiéniai képzésekben**, míg a **CYBER SHIELDS** nevű éves gyakorlat a kritikus infrastruktúrák SOC-munkatársait célozza meg. Emellett kötelező a vezetők és információbiztonsági tisztek képzése is.

Az **oktatási rendszer** három fő területre koncentrál: tudatosság (awareness), reagálási képesség és proaktív fenyegetésfelderítés.

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

Az előadás egyik leginnovatívabb eleme az új **DNS-szűrési mechanizmus** volt, amely Litvánia teljes internetes forgalmát monitorozza és blokkolja a veszélyes domaineket. A **„Vasaris”** nevű rendszer már közel 10 000 domaint tiltott le, napi szinten több mint 36 000 blokkolási eseményt hajt végre. Ez a rendszer akár 15 percen belül érvényesíti a szankciókat az internetszolgáltatóknál, így jelentősen csökkenti a káros tartalmak elérésének kockázatát.

Az NCSC egyik kiemelt fejlesztése a Nemzeti Kiberincidenskezelő Platform (**NCIMP**), amely az összes bejelentést – e-mailen, telefonon, API-n vagy online űrlapon – egységes rendszerben fogadja, automatizált deduplikációval és CTI-alapú elemzéssel támogatva a kezelést. **A cél** a teljes nemzeti rálátás biztosítása, az ismétlődő jelentések kiszűrése, valamint a reagálás sebességének javítása.

ROMANIAN CYBERSECURITY STRATEGY

(Dan Cimpean)

A román Nemzeti Kiberbiztonsági Igazgatóság (**DNSC**) munkatársa átfogó képet nyújtott az ország kiberbiztonsági stratégiájáról, szervezeti struktúrájáról és a közelmúltban bekövetkezett incidensek kezeléséről. A DNSC egy közvetlenül a miniszterelnök alá rendelt, stratégiai jelentőségű szerv, amelynek célja, hogy Romániát nemzetközi szinten is vezető szereplőként pozícionálja a kiberbiztonság területén. A szervezet 2030-ig 1063 fős személyi állomány kialakítására törekszik, ezzel is jelezve, hogy **a kibertér védelme nemzetbiztonsági prioritás**.

A DNSC által koordinált **stratégia** öt pilléren nyugszik: beruházások ösztönzése, oktatás és képzés, kiberbiztonsági kultúra fejlesztése, kutatás-fejlesztés támogatása, valamint nemzeti és nemzetközi együttműködések erősítése. A szervezet tevékenysége magában foglalja az incidenskezelést, digitális forenzikát, fenyegetéselemzést és sebezhetőség-menedzsmentet.

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

Ezen túlmenően **a DNSC stratégiai szereplő** a különböző európai uniós mechanizmusokban (pl. ENISA, ECCC, ECSO), valamint NATO-partneri kapcsolatokban.

Az előadás **két konkrét esettanulmányon keresztül** mutatta be a hibrid és ellátási láncokat érintő kibertámadások jelentőségét. 2024 februárjában **egy ransomware támadás** 26 román kórház működését bénította meg, míg 2022 márciusában egy 850 szervert érintő, energiaszektor elleni támadást követett **fake news kampány**, amely a lakosság pszichológiai destabilizálását célozta. A DNSC ugyan nem aktiválta az EU-CyCLONe válságkezelési mechanizmust, azonban gyors belső koordinációval és a kommunikációs hálózatok stabilizálásával **sikerült elkerülni a rendszerszintű károkat**.

A DNSC külön figyelmet fordít a TOR-hálózaton keresztül történő támadások észlelésére. 2024-ben Románia IP-szinten is feltérképezte a kibertámadásokhoz használt végpontokat, és azok jelentős részét az orosz-ukrán háborúval összefüggésben azonosította. A DNSC egyik jelentős lépése volt a **kockázatos szoftverek és szolgáltatások** – például antivírus programok, VPN-ek, EDR-ek – **betiltása** az állami infrastruktúrákban.

A prezentáció kitért az Európai Unió növekvő szabályozási környezetére is. A DNSC aktívan alkalmazza és véleményezi a DORA, NIS2, Cybersecurity Act, Digital Services Act és a Cyber Diplomacy Toolbox elemeit. A DNSC szerepe nem csupán végrehajtó, hanem szabályozó és képviseleti funkciót is betölt: az állam részéről ő a kompetens **hatóság** az összes civil kibertérrel kapcsolatos kérdésben.

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

COMBATING CYBERCRIMES IN GERMANY

(Daniele Schmidt)

A német Szövetségi Bűnügyi Hivatal (Bundeskriminalamt – **BKA**) Kiberbűnözés Elleni Osztályának helyettes vezetője előadásában átfogó képet nyújtott a **zsarolóvírusok** (ransomware) **elleni nyomozások** gyakorlati megközelítéseiről, különös tekintettel a nemzetközi bűnszervezetek szétzúzására irányuló műveletekre. Az előadás egyik központi eleme az volt, **hogyan lehet a támadások „gyökerét”,** vagyis a szervezeti struktúrákat **célba venni**, nem csupán az eszközöket és technikákat.

A BKA egyik jelentős eredménye az **„Operation Endgame” hadművelet**, amelyet több nemzetközi partnerrel közösen hajtottak végre, és amely célzottan a Trickbot, SmokeLoader és más malware-infrastruktúrák mögött álló személyeket és szervezeteket vette célba. Az előadás bemutatta azon személyeket is – köztük több orosz nemzetiségű kiberbűnözőt –, akik a különböző alrendszerek (pl. Crypter, Coder, Researcher, Infrastructure) működtetéséért feleltek. Az akció nyilvános elfogatóparancsokkal és digitális „körözési oldalakkal” is járt, mint például a operation-endgame.com és a bustedcrime.network.

Az előadó hangsúlyozta, hogy az **MI-eszközök fejlődése** nemcsak **a védekezési képességeket**, hanem **a bűnözői technikák komplexitását is fokozza**. A mesterséges intelligenciát felhasználó támadások száma és minősége is nőtt az elmúlt években, különösen a célzott adathalászat és társadalmi manipuláció területén. A BKA-nál jelenleg is kiemelt kutatási terület az **AI-alapú malware azonosítása** és az automatizált elemzési kapacitások fejlesztése.

Az előadás külön kiemelte, hogy az információmegosztás és a technikai forródrótok (**hotline-rendszerek**) jelentősen hozzájárultak a sikeres letartóztatásokhoz és infrastruktúrák

Széchenyi Terv Plusz Építsük együtt Magyarországot!
Magyarország Kormánya
Az Európai Unió társfinanszírozásával

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

lebontásához. A BKA partneri együttműködésben dolgozik az Europollal, valamint számos EU- és NATO-tagállam bűnüldöző szerveivel.

A közös nyomozócsoportok (JIT – Joint Investigation Teams) és az összehangolt „takedown" akciók stratégiai fontosságúak a transznacionális **kiberfenyegetések kezelése** szempontjából.

Az előadás utolsó része arra is rámutatott, hogy a darknet piacterek, privát kriptovaluta-tárcák és decentralizált infrastruktúrák jelentős kihívást jelentenek a bűnüldözés számára. Azonban a következetes, profilalapú nyomozás és a nyílt forrású adatgyűjtés (OSINT) kombinálása lehetőséget ad arra, hogy még ezekben a környezetekben is **azonosíthatók és nyomon követhetők** legyenek **az elkövetők**.

EDA'S CYBER DEFENCE PROGRAMME AND REGIONAL COOPERATION

(David Antunes)

Az Európai Védelmi Ügynökség (**EDA**) kiberhaderő-fejlesztési programmenedzsere előadásában átfogó áttekintést adott az EDA kiberhadviselési képességeinek fejlesztéséről, valamint az európai tagállamok közötti védelmi együttműködés támogatásának intézményi kereteiről. Az EDA egyedülálló módon **az EU egyetlen olyan ügynöksége**, amelynek irányító testülete miniszteri szinten ülésezik, így közvetlen **politikai súllyal bír a tagállami döntéshozatalban** is.

A prezentáció hangsúlyozta, hogy az EDA három stratégiai szerepet tölt be:

(1) a tagállamok közötti **technológiai és képességfejlesztési együttműködés** fóruma,
(2) **interfész** az EU politikái és a katonai operatív igények között, valamint
(3) **koordinációs mechanizmus** a NATO és EU védelmi tervezési folyamatai között. Jelenleg közel 300 aktív projekt fut az ügynökség portfóliójában, amelyek közül egyre több kapcsolódik közvetlenül a **kiberbiztonság** és **kiberhadviselés** témaköréhez.

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

Az előadás kiemelte a 2023-as EU képességfejlesztési prioritások közül a **„Full Spectrum Cyber Defence Operations Capabilities”** és a **„Cyber Warfare Advantage and Readiness”** területeket. Az előbbi célja agilis és adaptív kiberképességek kiépítése, míg az utóbbi innovatív technológiák fejlesztését és a haderők tesztelési kapacitásainak bővítését célozza.

A programok középpontjában az interoperabilitás, a szabványosítás és a közös műveleti képességek állnak, különös tekintettel a **C4ISTAR** (Command, Control, Communications, Computers, Intelligence, Surveillance, Target Acquisition and Reconnaissance) **rendszerek**re.

Kiemelt projektként szerepelt a **MILCERT Operational Network** (MICNET), amely egy EU-szintű katonai incidenskezelő hálózatot (Computer Emergency Response Teams – CERT) hoz létre. Szintén említésre került az **EU Cyber Domain Coordination Centre** (CDCC), amely a stratégiai incidenskoordinációért felelős, valamint a **Cyber Ranges Federation**, amely nemzeti és közös kiberharctér-gyakorlatokat
integrál egy európai keretbe. Emellett a **„CyberCO”** parancsnoki konferenciák – amelyek sorban Belgiumban, Magyarországon (2024), Lengyelországban (2025 Q1) és Dániában (2025 Q2) kerültek és kerülnek megrendezésre – biztosítják a katonai kiberparancsnokok közötti közvetlen tapasztalatcserét.

Az EDA előadás végén az előadó kiemelte a **PESCO program** (Permanent Structured Cooperation) keretében zajló kiberbiztonsági együttműködéseket, mint például a **CTIRISP** (Cyber Threats and Incident Response Information Sharing Platform), a **CIDCC** (Cyber and Information Domain Coordination Centre) és a **CRF** (Cyber Ranges Federation). A cél, hogy ezek a kezdeményezések közvetlenül hozzájáruljanak az EU stratégiai autonómiájához a kibertérben, miközben biztosítják a NATO-val való kompatibilitást is.

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

GROUP-IB PRESENTATION

A **Group-IB** regionális igazgatója (Olaszország és Ibériai-félsziget) előadásában a kiberbűnözés legújabb formáiról, globális trendjeiről és a cég által kínált technológiai megoldásokról számolt be. A Group-IB 60 országban van jelen, több mint 1 550 magas technikai igényű nyomozásban vett részt, és világszerte 11 egyedi digitális bűnözés-ellenállási központot működtet. A szervezet fő tevékenysége a fenyegetések azonosítása, a dark web monitorozása, incidensreakció, valamint rendvédelmi szervekkel történő operatív együttműködés.

Az előadás középpontjában a 2025-ös évre vonatkozó **High-Tech Crime Trends Report** állt, amely több ezer támadás elemzésén keresztül mutatja be az európai és globális kiberfenyegetettségi képet. A jelentés alapján **Európában a zsarolóvírusok a legfőbb veszélyt jelentik**, élén a Lockbit (182 támadás), Ransomhub (126) és 8base (77) csoportokkal. A leginkább célba vett szektor a gyártás, az üzleti szolgáltatások és az ingatlanpiac volt. A DLS (dedicated leak site) mechanizmusok – az adatszivárgás fenyegetésével kombinált zsarolás – kiemelt szerepet játszanak a nyomásgyakorlásban.

A bemutató további hangsúlyt fektetett a hacktivizmus és az **APT** (advanced persistent threat) típusú támadások európai jelenlétére. Az oroszbarát **NoName057(16) csoport** például DDoS kampányokat indított NATO-tagállamok ellen, míg az ukrán **IT Army** célba vette az orosz pénzügyi és kormányzati rendszereket. A 2024-es adatok alapján az APT támadások 18,24%-kal emelkedtek, különösen az **APT28** és a **Sticky Werewolf csoportok** aktivitása révén, amelyek közintézményeket és kutatóközpontokat támadtak meg.

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

A prezentációban részletes előrejelzések is szerepeltek. A **kriptovaluták elterjedése** új pénzmosási módszereket nyitott meg a bűnözők előtt, míg a **DeFi-platformok** (decentralizált pénzügyi rendszerek) anonimitást biztosítanak számukra. Emellett a **mesterséges intelligencia alkalmazása** – például automatikus phishing, sérülékenység-felderítés vagy deepfake-es csalás – tovább bővítette a támadók eszköztárát. A fenyegetések új színterekre is átterjedtek, például szabályozott üzenetküldő platformokról a dark webre és titkosított kommunikációs csatornákra.

Az előadás zárásaként az előadó ismertette azokat a **proaktív** megközelítéseket, amelyek révén a Group-IB támogatja a bűnüldöző szerveket – például a **spanyol és latin-amerikai „Kaerb" művelet**, amely 480 000 áldozattal járó csalóhálózatot számolt fel, vagy a Grandoreiro trójai támadássorozat felszámolása Brazíliában. A cég technológiai platformjai lehetővé teszik az élő adatkorrelációt, célzott elkövetőprofil-képzést és az incidensek valós idejű nyomon követését.

INNOVATING THE NATIONAL RESPONSE: A REPUTATIONAL STRATEGY TO ADDRESS A LARGE-SCALE CYBERCRISIS

(Ivan Montforte Fugarolas)

A **Katalán Kibervédelmi Ügynökség** munkatársa előadásában egy rendkívül részletes és strukturált modellt mutatott be a kiberbiztonsági incidensek nemzeti szintű kezelésére. A prezentáció egyik kiindulópontja az volt, hogy a **modern biztonsági kihívások** – ideértve a fegyveres konfliktusokat, energiabiztonságot, tömeges migrációt és a kiberfenyegetéseket – ma már elválaszthatatlanul **összefonódnak.** A **PwC** Digitális Bizalom Felmérésének eredményeire hivatkozva elhangzott, hogy a kibertámadás ma már a globális CEO-k első számú félelme, megelőzve az inflációt és gazdasági recessziót.

A Katalán Kibervédelmi Ügynökség felépítésének és mandátumának ismertetése során kiderült, hogy az intézmény évente több mint 2 175 incidenssel foglalkozik, és több mint 4,4 milliárd támadást

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

detektáltak az elmúlt év során. A Generalitat de Catalunya (Katalónia kormánya) különböző szervezetein belül – mint az egészségügy, önkormányzatok, egyetemek, kritikus infrastruktúrák – negyedóránként történik biztonsági esemény. Az Ügynökség három alapfeladata:

(1) közszolgáltatásként működő **kiberbiztonsági védelem**,

(2) **a kiberbiztonság** mint stratégiai gazdasági szektor **fejlesztése**, és

(3) az **állami informatikai rendszerek védelme**.

Az előadás kiemelt esettanulmánya a 2023. március 5-én történt **Hospital Clínic de Barcelona elleni zsarolóvírus-támadás** volt. A támadást követően azonnal összehívták a válságkabinetet, és az incidens kezelését – a technikai, jogi, kommunikációs és operatív dimenziók bevonásával – példaszerű módon koordinálták. A válsághelyzet kezelésében különösen fontosnak bizonyult a médiával való kapcsolat, a társintézmények azonnali informálása, valamint a technikai csapatok működésének transzparens kommunikációja a döntéshozók felé.

Az incidens tapasztalataira építve Monforte ismertette az új, **integrált incidenskezelési protokollt**, amely túlmutat a hagyományos CERT-alapú izoláció–reakció modelljén. A **„to be" protokoll** többek között tartalmazza a támadás mértékének komplex értékelését (pl. lakossági hatás, közszolgáltatások elérhetősége), a biztonsági mentések alternatív rendszerekkel történő helyreállítását, az **IOCs** (Indicator of Compromise) valós idejű megosztását a nemzeti szervekkel, valamint a nyilvános és belső kommunikációs folyamatok előre definiált kezelését. A protokoll két döntéshozó bizottságot is bevezet: a technikai válságkabinetet és az intézményi–kommunikációs kabinetet.

Az előadás záró szakaszában bemutatásra került az incidensek súlyosságának azonosítására szolgáló checklist, a különböző szereplők felelősségi mátrixa (adatvédelmi felelős, rendőrség, távközlési hatóság), valamint az egyes szinteken alkalmazandó eljárások (eszközök leválasztása, adatvédelem értesítése, médiakommunikáció befagyasztása stb.). Mindez egy robusztus, skálázható és szabályozott struktúrát eredményezett, amely példaértékű a decentralizált közigazgatási környezetek számára.

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

COMBATING CYBERCRIMES ACROSS HUNGARY

(Csáki Levente)

A **Nemzeti Védelmi Szolgálat** (NVSZ) Kiberfelderítő Osztályának vezetője előadásában átfogó képet nyújtott azokról a csalástípusokról és kiberbűnözési trendekről, amelyek a magyarországi lakosságot és a közszférát érintik, valamint bemutatta az NVSZ szakmai szerepvállalását az ezek elleni fellépésben. A prezentáció fókuszában az e-mail alapú csalások, romantikus átverések, közösségi média alapú pénzkicsalások és banki névvel való visszaélések álltak.

Az előadás első részében a **leggyakoribb internetes csalástípusokat mutatta be**: örökség visszaszerzési csalások, romantikus kapcsolatépítésre épülő pénzkicsalások, befektetési átverések és magas hozamot ígérő, de tényleges kifizetést nem nyújtó ajánlatok. Kiemelte, hogy ezen sémák célja **az áldozatok aktív bevonása**: hamis bizalom kialakítása után érzékeny adatokat és közvetlen pénzügyi tranzakciókat kérnek. A bemutatott példák alapján a támadók gyakran nyelvtanilag hibás e-maileket küldenek, hamis webcímeket (pl. „otp.bank.freewebpage.hu”) használnak, és valótlan személyazonossággal lépnek kapcsolatba az áldozatokkal.

Az NVSZ által végzett tevékenységek négy fő kategóriába sorolhatók:

(1) bűnmegelőzés,
(2) helyszíni támogatás,
(3) forenzikus szakértői eljárások és
(4) elemzői támogatás.

A kiberfelderítő csoport feladatai közé tartozik a védett szervezetek tagjai elleni támadások detektálása, korrupciós célú kibertámadások vizsgálata, valamint az ügyészségekkel és nyomozó hatóságokkal való együttműködés. A helyszíni támogatás során technikai eszközökkel segítik a rejtett IT-komponensek azonosítását és az adatok helyszíni mentését.

Széchenyi Terv Plusz Építsük együtt Magyarországot!
Magyarország Kormánya
Az Európai Unió társfinanszírozásával

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

Külön figyelmet kaptak az **OSINT-alapú elemzési tevékenységek**, mint például a kapcsolati hálók feltérképezése, nyílt adatbázisokból származó információk validálása, valamint az adathalász támadásokhoz kapcsolódó webcímek és infrastruktúrák vizsgálata.

A **gyermekvédelem** kiemelt területként jelent meg: az NVSZ saját eszközpark fejlesztését tervezi a kiskorúak elleni online bűncselekmények feltárására, valamint szülők és pedagógusok számára szóló tudatosságnövelő kampányokat is szervez.

Az előadásban szereplő jövőbeni irányok közé tartozik a malware-elemzés megerősítése, dark web figyelési kapacitások bővítése, valamint új gyermekvédelmi eszközök beszerzése. Emellett a **Cybershield projekt** keretében kiállításokon, oktatási rendezvényeken való részvétel és ismeretterjesztő kiadványok publikálása révén erősítik a megelőzést.

SECURING SPANISH CRITICAL INFRASTRUCTURE AND BUILDING CAPABILITIES

(Maite Carli Garcia)

A **spanyol Ipari Kibervédelmi Központ** (CCI – Centro de Ciberseguridad Industrial) kommunikációs vezetője és EU-koordinátora előadásában a kritikus ipari infrastruktúrák (CIIP) kiberbiztonsági helyzetéről, a különböző szektorok érettségéről és a CCI által alkalmazott védelmi módszertanokról számolt be. Az előadás középpontjában az **energia-, víz- és közlekedési ágazat kiberfenyegetettsége** állt, kiegészítve az élelmiszeripar, vegyipar és egészségügy irányába tett kutatási és fejlesztési kiterjesztésekkel.

A különböző iparágakra jellemző technológiai sokféleség és eltérő fejlettségi szint komoly kihívásokat jelent a **CIIP-védelem** számára. A villamosenergia-ágazat – noha vezető szerepet tölt be a kibervédelmi kapacitásokban – komplexitása és beszállítói struktúrája miatt továbbra is sebezhető.

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

A víziközmű-ágazatban például a feldolgozott technológiák eltérő életciklusa, a szűk költségvetés és a korlátozott szakértelem miatt magas a kockázati szint.

A CCI által alkalmazott szektorális megközelítés lényege, hogy **minden ágazatban 12–15 valós fenyegetési forgatókönyvet azonosítanak**, és ezek alapján hatáselemzési táblákat készítenek. Az öt fázisból álló módszertan (fenyegetések azonosítása, hatáselemzés, érettségi felmérés, ajánlások kidolgozása, gyakorlatok) az iparági szereplők – üzemeltetők, integrátorok, gyártók – bevonásával történik. A prezentáció során bemutatásra került egy **vízipari ágazatra vonatkozó felmérés** is, amely jól példázta a kockázatértékelés gyakorlati alkalmazását.

A **MACIN** nevű **új platform** egy szektor- és folyamatalapú érettségi modellt kínál, amelyhez illesztett biztonsági követelménycsomagok tartoznak. A platform célja, hogy standardizáltan, mégis testre szabottan segítse az iparágakat saját kibervédelmi bázisuk meghatározásában és fokozatos erősítésében. A platform első verziója 2025 júniusában válik elérhetővé, és a tervek szerint az energiaágazat pilot projektjei mentén bővítik tovább.

Az előadás külön szekcióban foglalkozott a **beszállítói lánc** kiberbiztonságával. A fő kihívások közé tartozik a szakértői hiány, a beszállítók túlzott száma és a követelmények kontextus nélküli meghatározása. A CCI szerint a büntetésalapú auditálás helyett a **közös felelősség és együttműködés elvét kell érvényesíteni.** A szabályozások – például a NIS2 irányelv vagy az IEC 62443 szabvány – mellett egyre nagyobb jelentőséget kap a PDCA (Plan-Do-Check-Act) ciklus alapú, folyamatos kockázatmenedzsment.

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

OVERVIEW OF THE CURRENT DUTCH THREAT LANDSCAPE

(Dr. Noortje Henrichs)

A **Holland** Belügyminisztériumhoz tartozó **Nemzeti Kiberbiztonsági Központ** (NCSC-NL) szakértője a holland kibertér jelenlegi fenyegetettségi helyzetét, a fenyegetési típusok kategorizálását és a védekezési mechanizmusokat mutatta be előadásában. A bemutató külön figyelmet szentelt a kiberkémkedés, a ransomware-hullámok, az ellátási lánc sérülékenységei, valamint a hacktivista aktivitások aktuális megjelenési formáinak.

A **NCSC-NL** egy **többfunkciós nemzeti központ**, amely koordinálja a CERT/CSIRT tevékenységeket, válságkezelést biztosít, valamint nyílt és zárt információmegosztási csatornákon keresztül kapcsolatot tart fenn a közszféra és a magánszektor szereplőivel. A központ része a Nemzeti Detekciós Hálózatnak (**NDN**), amely valós idejű fenyegetésdetekcióra és megosztásra épül, és jelentős szerepet játszik a kritikus infrastruktúrák védelmében. A hálózat gyakran jelez kifinomult támadási mintákat, mint például a QBot, Pikabot vagy SocGholish malware-ek észleléseit.

A fenyegetések négy fő kategóriába sorolhatók:

(1) kiberkémkedés – **SeaTurtle** és **Coathanger kampányok** révén;
(2) kiberbűnözés – főként többfaktoros zsarolóvírus-támadásokkal és specializált támadásszolgáltatásokkal;
(3) hacktivizmus – például a **NoName057(16)** által indított DDoS támadások politikai célpontok ellen; valamint
(4) szabotázs – orosz eredetű kiberműveletek és kritikus holland infrastruktúrák (közlekedés, politikai pártok, közüzemek) elleni célzott műveletek.

A holland katonai hírszerzés szerint ezek közül több már konkrét fizikai szabotázsra való előkészületként értékelhető.

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

A szakértő kiemelte, hogy az **ellátási lánc biztonsága** komoly hiányosságokat mutat. Nemcsak a közvetlen beszállítók, hanem az alvállalkozók és a karbantartó szolgáltatók is potenciális belépési pontokat jelentenek. Ezt a problémát súlyosbítja, hogy a hálózati perifériás eszközök – például VPN-szerverek, tűzfalak, routerek – gyakran nyilvánosan elérhetők, elavult firmware-rel működnek, és kevéssé védettek. Az edge device-okra irányuló célzott támadások emelkedő tendenciát mutatnak.

Az előadás kitért a **mobil eszközök elleni támadások felerősödésére** is, ahol a támadók az érzékeny személyes és pénzügyi adatok megszerzését célozzák, valamint a felügyeleti (surveillance) rendszerek megkerülését. Az **MFA-t** (multi-factor authentication) **megkerülő módszerek** terjedésével a támadók egyre rugalmasabbak és technikailag felkészültebbek: a **„Man-in-the-Middle"** (AiTM) típusú támadások során a támadó közvetítő szerepet tölt be a felhasználó és az eredeti weboldal között, gyakran Microsoft 365 környezeteket kompromittálva.

INCREASING EUROPE'S CYBERSECURITY CAPABILITIES

(Polyvios Hadjiyiangou)

Az **Európai Kiberbiztonsági Kompetencia Központ** (ECCC) operatív igazgatója előadásában átfogó képet adott a szervezet küldetéséről, eszköztáráról, projektportfóliójáról és jövőbeni stratégiáiról. Az **ECCC** célja, hogy megerősítse az EU stratégiai autonómiáját a kiberbiztonság területén, támogassa a technológiai szuverenitást, és növelje az európai kiberipar globális versenyképességét. Az intézmény az Európai Unió Cybersecurity Strategy-jének technológiai és operatív végrehajtó „motorjaként" funkcionál.

Az ECCC három fő pilléren keresztül fejti ki hatását:

(1) a **Stratégiai Agenda**, amely egy fenntartható és koherens iparági, technológiai és kutatási stratégiát biztosít;

(2) **pénzügyi eszközök** – különösen a Horizon Europe (HE) és a Digital Europe Programme (DEP),

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

amelyek több száz millió eurós forrásból támogatják a kutatást és a gyakorlati bevezetést; (3) a **Kiberközösség**, amely nemzeti koordinációs központok (NCC-k), kutatóintézetek, ipari szereplők és állami szervek együttműködésén alapuló hálózat.

A bemutató során részletes ismertetést kaptunk a 2021–2024-es időszak fő projektjeiről: több mint 160 projekt zajlik 500 millió euró értékben, melyek célja a biztonsági műveleti központok (SOC-ok) kiépítése, a NIS2 és CRA (Cyber Resilience Act) előírásainak támogatása, valamint új technológiák (pl. post-quantum kriptográfia, AI-alapú védelem) gyakorlati tesztelése és bevezetése. Külön kiemelést kaptak az olyan területek, mint a cyber range infrastruktúrák fejlesztése, a hands-on képzések és a nemzeti szintű incidensreagálás összehangolása.

A 2025-ös évre vonatkozó tervek között szerepel a generatív mesterséges intelligencia kiberbiztonsági alkalmazása, új operatív eszközök bevezetése, a post-quantum algoritmusok protokollszintű integrációja és validációja, valamint a Privacy Enhancing Technologies (PETs) fejlesztése. A **Horizon Europe program** 2025-ben 90 millió eurós költségvetéssel támogatja ezeket az új irányokat, míg a **DEP** új hívásai (DEP8 és DEP9) többek között a nemzeti cyber-hubok fejlesztésére és a vészhelyzeti mechanizmusok kiépítésére fókuszálnak.

Az ECCC kulcsszerepet játszik a **Cyber Solidarity Act** végrehajtásában is. Ez magában foglalja az európai kiberfigyelmeztető rendszer (ECAS) kiépítését, a kritikus ágazatok (egészségügy, kommunikáció, pénzügy) védelmi képességeinek tesztelését, valamint a tagállamok közötti technikai segítségnyújtás mechanizmusainak bevezetését. Az előadás szerint az ECCC fontos missziója, hogy harmonizálja a NIS2, CRA, GDPR, DORA és az AI Act előírásait, különösen az SME-k, kormányzati szervek és dual-use (civil-katonai) projektek támogatásában.

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

A CEPOL szerepe a kiberbűnözés elleni uniós képzési rendszer megerősítésében

A **CEPOL** (European Union Agency for Law Enforcement Training) oktatási szakértője részletesen ismertette az ügynökség kibervédelemre vonatkozó stratégiai irányait, képzési struktúráját és az aktuális európai kiberfenyegetésekre adott válaszokat a képzés oldaláról. A CEPOL immár több mint húsz éve szolgálja az uniós tagállamok és társult országok rendvédelmi szerveit, célja pedig, hogy európai szinten egységes, magas színvonalú tudásmegosztást és gyakorlatorientált képzést biztosítson a rendészeti hatóságok számára.

Az előadás kiemelte a **CEPOL 2024–2030 közötti stratégiájának négy alapvető célkitűzését**:

(1) az ügynökség pozícionálása az EU rendvédelmi képzések központjaként,
(2) közös rendvédelmi kultúra kialakítása,
(3) a képzések akkreditációjának támogatása, valamint
(4) hatékony, modern ügynökségi működés megvalósítása.

Ennek részeként a CEPOL nemcsak **onsite** (személyes jelenlétet igénylő), hanem **online** kurzusokat, webinarokat, e-tananyagokat és mikro-tanulási (cyber bites) formátumokat is kínál, különös figyelmet fordítva a kiberbűnözés, online csalások, e-bizonyítékok, forenzikus eszközhasználat és OSINT témakörökre.

Az ügynökség kiemelten kezeli a képzések stratégiai tervezését: az **EU-STNA** (Strategic Training Needs Assessment) keretrendszerben a tagállamok és partnerek bevonásával azonosítják a legfontosabb képzési szükségleteket, melyeket az **OTNA** (Operational Training Needs Analysis) módszertan alapján operatív szintre bontanak le. A 2024-es év kiemelt területei közé tartozik az emberkereskedelem, gyermekek szexuális kizsákmányolása, mesterséges intelligencia a bűnüldözésben, pénzügyi bűncselekmények és az elektronikus bizonyítékok kezelése.

Széchenyi Terv Plusz Építsük együtt Magyarországot!
Magyarország Kormánya
Az Európai Unió társfinanszírozásával

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

A **Training Competency Framework on Cybercrime** (cTCF) **modell** külön figyelmet érdemel: ez a keretrendszer részletesen meghatározza a kiberbűnözés elleni fellépésben szükséges szerepköröket és kompetenciákat (pl. nyomozók, forenzikus elemzők, hírszerzési elemzők). A cél, hogy a különböző tagállamok és intézmények egységesen és célzottan képezhessék ki szakembereiket a jövő kiberfenyegetéseire való reagálás érdekében. A **CEPOL Cybercrime Academy** keretében 2025-ben több mint 20 új képzést indítanak, köztük ransomware nyomozások, dark web és kriptovaluta, mobilforenzika, mesterséges intelligencia, valamint OSINT „train the trainer" tanfolyamokat.

Az előadás külön hangsúlyozta a **CEPOL Exchange Programme** jelentőségét, amely lehetővé teszi, hogy az uniós tagállamok szakemberei egyhetes, gyakorlatorientált csereprogramok keretében közvetlenül tapasztalatot szerezzenek más országok rendvédelmi gyakorlatairól. A cél itt nem pusztán tudásátadás, hanem a nemzetközi operatív együttműködés személyes kapcsolatokon alapuló erősítése.

THREAT INTELLIGENCE – HELPING TO SECURE GOVERNMENT OF MALTA INFRASTRUCTURE

(Roderick Lia)

Málta kormányzati CSIRT-jének (**govmtCSIRT**) és a kiberfenyegetés-elemző egység (CTI) vezetője előadásában a máltai állam kiberbiztonsági stratégiájának központi elemeit és operatív működését mutatta be. A prezentáció fókuszában a **proaktív védekezési modell** állt, amely a fenyegetések előrejelzésén, viselkedésalapú elemzéseken, valamint valós idejű detekciós és reagálási képességeken alapul. A máltai kormányzati hálózatok védelméért felelős **MITA** (Malta Information Technology Agency) egy ISO-tanúsított, 330 fős szakértői csapattal működő, állami informatikai szolgáltató.

A bemutató szerint a proaktív védekezés célja nemcsak az incidensek kezelése, hanem azok megelőzése. Ennek eszköztárába tartozik a felhasználói viselkedés-analitika (UBA), folyamatos monitoring, patch-menedzsment, red teaming és threat hunting tevékenységek, valamint a „Zero Trust"

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

architektúra bevezetése. Lia hangsúlyozta, hogy a döntéshozatal csak megalapozott, valós kockázatelemzésre épülő formában lehet hatékony, és hogy a rosszul kalibrált automatizmusok nagyobb kárt is okozhatnak (pl. üzletmeneti leállás, hibás válaszreakciók).

A **threat intelligence szerepe** kulcsfontosságú a máltai rendszerben: az IOC-k (Indicators of Compromise), TTP-k (taktikák, technikák, eljárások) és viselkedésminták alapján működő SIEM, EDR és NDR rendszerek támogatják a valós idejű észlelést. Az **„Enhanced Detection Capabilities" koncepció** jegyében a red team–blue team együttműködés, valamint a „baseline" viselkedésminták azonosítása és a figyelmeztetési zaj folyamatos szűrése is központi szerepet játszik. Az észlelés pontossága, valamint az MTTR és MTTD (Mean Time to Respond / Detect) csökkentése kritikus operatív cél.

A prezentáció részletesen tárgyalta a fenyegető aktorok profilozásának módszertanát is, különös tekintettel a **MITRE ATT&CK keretrendszer** használatára. Ez lehetővé teszi a fenyegető csoportok taktikáinak és célpontjainak előrejelzését, az észlelési logikák testreszabását, valamint a vadászatirányítás finomhangolását („hunt for signs of Group X's TTPs"). Az elemzések alapján az elemzők célzottan tudják tájékoztatni a döntéshozókat a releváns kockázatokról és az azokra adandó válaszokról.

Az előadás zárásában az előadó hangsúlyozta a bizalomra épülő belső és nemzetközi együttműködés jelentőségét. A **threat intelligence** csak akkor működik hatékonyan, ha **strukturált** (STIX/TAXII) formátumú, kontextushoz kötött és időben megosztott információkon alapul. A máltai rendszer aktívan részt vesz közösségi védelmi platformokban, megosztja a detekciós szabályait (pl. Sigma, YARA) és rendszeresen részt vesz közös gyakorlatokon.

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

ITALIAN CYBER SECURITY OVERVIEW

(Stefania Ducci)

Az **olasz Nemzeti Kiberbiztonsági Ügynökség** (ACN – Agenzia per la Cybersicurezza Nazionale) képviseletében tartott előadás részletes betekintést adott az olasz kibervédelmi architektúrába, annak jogi és szervezeti kereteibe, valamint a stratégiai együttműködésekbe. Az előadás középpontjában az **ACN szerepe** állt, amelyet az olasz kormány a 2021-es 82. számú törvényerejű rendelettel hozott létre, ezzel új intézményi alapokra helyezve a kibertér védelmét. Az ACN célja, hogy biztosítsa az állam kiber-rezilienciáját, koordinálja a nemzeti és nemzetközi szereplők közötti együttműködést, és stratégiai szinten vezesse az ország kiberbiztonsági politikáját.

Az olasz modell három szinten működik: **stratégiai–politikai** (miniszterelnöki és miniszteri bizottsági szint), **operatív–végrehajtói** (ACN mint végrehajtó szerv), valamint **technikai–taktikai** (CSIRT Italia, technológiai háttérintézmények, kutatási központok). A rendszer az ágazati minisztériumokkal (pl. belügy, hadügy, egészségügy, energetika), a titkosszolgálatokkal (AISE, AISI, DIS), valamint az egyetemekkel és iparági szereplőkkel is strukturált együttműködési formát alkalmaz. Az ACN ugyanakkor nem csupán hatósági, hanem koordinatív, tanúsító, ellenőrző és stratégiai tervező szerepköröket is ellát.

Kiemelt szerep jut az ACN által irányított **„National Cybersecurity Cell”** nevű operatív egységnek, amely válságkezelési, incidenskezelési és gyakorlat-szervezési feladatokat lát el. Ez a szervezet működik közre a **CSIRT Italia** jelentései alapján beérkező események elemzésében, a jelentős incidensek interszektoriális koordinációjában, valamint a nemzetközi együttműködések technikai támogatásában is. Az egység 8 alapfeladatot lát el, köztük a kiberkrízisek súlyosságának meghatározását, a válaszintézkedések koordinációját, az információmegosztás biztosítását, és a nemzetközi gyakorlatokban való részvételt.

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

A prezentáció részletesen kitért az ACN nemzetközi beágyazottságára is. Az ügynökség aktívan részt vesz többoldalú (pl. G7 Cybersecurity Working Group) és kétoldalú együttműködésekben, valamint kulcsszerepet vállal a NIS2 irányelv nemzeti implementációjában, az EU szabályozási csomagjainak (pl. Cyber Resilience Act, Digital Services Act) gyakorlati alkalmazásában. Ezen túlmenően az ACN felügyeli a nemzeti tanúsítási rendszert, részt vesz a nemzeti cloud és kvantumkriptográfiai technológiák fejlesztésében, valamint kapcsolatot tart fenn az ipari szereplőkkel, akadémiai partnerekkel és civil szervezetekkel.

Az ACN tevékenysége kiterjed a kríziskezelés szcenárióinak előkészítésére és gyakorlatok végrehajtására is. Külön hangsúlyt kapott a nemzeti kiberbiztonsági stratégia végrehajtása, az oktatás és képzés támogatása, valamint az ellenőrzési és szankcionálási mechanizmusok működtetése. Az **„Európai digitális szuverenitás”** és a **„technológiai autonómia”** jelszavak jegyében az ACN célja, hogy Olaszország aktív formálója legyen a közös európai kibervédelmi irányvonalaknak.

VMRAY PRESENTATION

A **VMRay** prezentációja a vállalat legfrissebb fenyegetési jelentésén (**Threat Landscape Report 2024/2**) és a szervezet elemzői tapasztalatain alapult. A VMRay egy **vezető sandbox-elemzési megoldásokat kínáló cég**, amelynek ügyfélkörébe Fortune 100 vállalatok, vezető bankok, technológiai óriások és kormányzati szervek tartoznak. A prezentáció fókuszában a modern fenyegetések észlelése, a kártevők és adathalász-támadások fejlődése, valamint az automatizált és mély elemzés technológiai válaszai álltak.

A prezentáció hangsúlyozta, hogy az új fenyegetésekre nemcsak gyorsan, de mélyrehatóan is reagálni kell. A VMRay platformja képes fájlok, URL-ek és e-mailek elemzésére, és on-premise vagy felhőalapú környezetben is alkalmazható. A rendszer **definitív döntést hoz** az elemzett objektumokról, miközben viselkedésalapú analízist és átlátható, reprodukálható vizsgálatot biztosít.

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

A **VMRay sandbox technológiája kiemelkedik** a piacon az eváziós technikákkal szembeni ellenálló képessége révén, és számos – más eszközök által nem detektált – támadást képes azonosítani.

A 2025-re vonatkozó fenyegetési trendek között három fő csoport emelkedik ki:

(1) a **mesterséges intelligencia** visszaélésszerű alkalmazása (pl. phishing e-mailek automatizált generálása, kódgenerálás LLM-ekkel),

(2) **ellátási lánc támadások** (pl. Chrome-bővítmények megfertőzése, VPN-szolgáltatók kompromittálása), valamint

(3) kifinomult **adathalász-módszerek**, mint például QR-kód alapú támadások, megbízható forrásból származó e-mailek, illetve Google szolgáltatásokat kihasználó átirányítások (pl. meet.google.com spoofing). Az innováció sebessége miatt a detekciós és válaszadási eszközök folyamatos finomhangolása elengedhetetlen.

A prezentáció külön **kitért a leggyakrabban észlelt kártevőcsaládokra**: Lumma, QuasarRAT, Emotet, AgentTesla, XWorm, GuLoader, xRAT, Stealc, Amadey és CobaltStrike. Ezek közül több is képes többfaktoros hitelesítést (MFA) megkerülni, illetve olyan kódolt kommunikációt folytat, amely hagyományos eszközökkel nehezen detektálható. A támadók új módszerei közé tartozik az ún. "PasteJacking", a .URL fájlokkal történő MSHTML kihasználása, és az EOL (end-of-life) hardvereken futó rendszerek támadása.

A VMRay küldetése, hogy olyan eszközt biztosítson, amely képes a korábban nem detektált fenyegetések azonosítására. A technológia fő előnye a gyorsaság és az elemzési mélység kombinációja: **a rendszer valós időben képes reagálni a támadásokra**, miközben komplex támadási láncokat (multi-stage chains) is felismer. A prezentáció végén kiemelésre került: a támadók alkalmazkodóképessége és kreativitása miatt nem elegendő pusztán reaktív módon védekezni, hanem proaktív detekcióra és intelligens elemzésre van szükség.

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

UKRAINE CYBER SECURITY STRATEGIES AND POLICIES

(Ivan Kalabashkin)

Az **Ukrán Biztonsági Szolgálat** (SBU) Kiberosztályának képviseletében tartott előadásában átfogó képet adott a kibertérben zajló hadműveletekről, amelyek Ukrajna ellen irányultak a 2021–2025 közötti időszakban. A bemutató nemcsak a támadások típusaira és következményeire fókuszált, hanem az elhárítás során szerzett tapasztalatokat, szervezeti válaszokat és módszertani tanulságokat is részletesen feltárta. A prezentáció megrázó, ugyanakkor tanulságos betekintést adott a digitális frontvonal valóságába.

Az SBU Cyber Department tevékenysége több vektor mentén szerveződik: kibertámadások detektálása és visszaverése, kritikus infrastruktúrák rejtett sérülékenységének tesztelése, állami digitalizációs projektek biztonsági felügyelete, valamint dezinformációs és pszichológiai műveletek (PSYOP) elleni fellépés. Emellett aktív hírszerzési és bűnügyi nyomozási feladatokat is ellát, különös tekintettel a kiberkémkedés és kibertámadások során elkövetett nemzetközi jogsértésekre.

Az előadás középpontjában a 2023. december 12-én végrehajtott masszív **kibertámadás** állt, amely **Ukrajna legnagyobb mobilszolgáltatóját, a Kyivstart érte**. A támadás során 932 virtuális gépet és 165 fizikai szervert töröltek, a cég technológiai hálózatát (pl. domain kontrollerek, felhőalapú adattárak) tönkretették, valamint több mint 7 000 felhasználói gépen próbáltak vírusokat futtatni. A támadás célja a szolgáltatás teljes blokkolása, a felhasználói bizalom megingatása és a hálózati eszközök fizikai megsemmisítése volt.

Szintén részletesen bemutatásra került a 2024 végén az **Ukrán Igazságügyi Minisztériumot ért támadássorozat**, amely több nemzeti regisztert (ingatlan-nyilvántartás, családi állapot, járműnyilvántartás) bénított meg.

Széchenyi Terv Plusz Építsük együtt Magyarországot!
Magyarország Kormánya
Az Európai Unió társfinanszírozásával

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

A támadási lánc tipikus APT mintázatot követett: adathalász e-mailek, Living-off-the-Land eszközhasználat, DNS-alapú C2 kommunikáció, majd fokozatos kiterjeszkedés és adatgyűjtés, végül destruktív támadás (adatok törlése, hamisítás, regiszterek módosítása). Legalább 37 millió rekordot szivárogtattak ki, köztük személyes azonosítókat, elérhetőségeket, családi kapcsolatokat.

A támadások célja kettős volt:

(1) technikai destabilizáció – az állami szolgáltatások megbénítása, adatvesztés, pénzügyi károkozás;

(2) pszichológiai hatás – a lakosság bizalmának megingatása, a kormány inkompetensnek való feltüntetése.

A támadásokhoz kapcsolódó dezinformációs kampányokat Telegramon és álhírportálokon vezették le, többek között a XakNet Team nevű csoport közvetítésével. A károk pénzügyi, társadalmi és információs értelemben is súlyosak voltak.