NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2025. 28. hét

HÍREK

- Kritikus sebezhetőségek a Sudo parancssori eszközben – jogosultságkiterjesztés veszélye fenyegeti a Linux rendszereket
- Androidos kártevők új hulláma: riasztó növekedés a mobil fenyegetések terén
- Kritikus sebezhetőség a PHPMailer-ben
- Az Atomic macOS infostealer hátsó ajtót telepít a perzisztens támadásokhoz
- Az alapértelmezett jelszavak láthatatlan kockázatai – Egyetlen „1111” is elég

STATISZTIKAI ADATOK

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

TÁJÉKOZTATÁSOK

- Tájékoztatás a SECTOR 16 csoport magyar geotermikus rendszer elleni támadásával kapcsolatban

BESZÁMOLÓ

- Barcelona Cybersecurity Congress 2025

KONTAKT

edt@nki.gov.hu

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D

NEWS

IT biztonsági

HÍREK

Androidos kártevők új hulláma: riasztó növekedés a mobil fenyegetések terén

(gbhackers.com)

2025 második negyedévében jelentősen megnőtt az Android operációs rendszert célzó rosszindulatú programok aktivitása. A kártékony szoftverek fejlődése nem csupán a mennyiségükben, hanem a kifinomultságukban is megmutatkozik. **Bővebben...**

Kritikus sebezhetőség a PHPMailer-ben

(gbhackers.com)

Az Egyesült Államok Kiberbiztonsági és Infrastruktúra Biztonsági Ügynöksége (CISA) figyelmeztetést adott ki egy évek óta ismert, de mára ismét aktívan kihasznált sebezhetőséggel kapcsolatban, amely a széles körben alkalmazott PHPMailer könyvtárat érinti. **Bővebben...**

Az Atomic macOS infostealer hátsó ajtót telepít a perzisztens támadásokhoz

(bleepingcomputer.com)

Egy malware elemző fedezte fel az Atomic macOS info-stealer (más néven “AMOS“) egy új verzióját, amely hátsó ajtót (backdoor) telepít, hogy a támadók számára folyamatos hozzáférést biztosítson a rendszerekhez. **Bővebben...**

Az alapértelmezett jelszavak láthatatlan kockázatai – Egyetlen „1111” is elég

(thehackernews.com)

Egy víznyomás-állomás, amely világméretű problémára világít rá: 2025-ben iráni hackereknek sikerült kompromittálniuk egy víznyomás-állomást az Egyesült Államokban, amely mintegy 7000 embert látott el vízzel. **Bővebben...**

Kritikus sebezhetőségek a Sudo parancssori eszközben – jogosultságkiterjesztés veszélye fenyegeti a Linux rendszereket

(thehackernews.com)
(gbhackers.com)

A Linux és Unix-szerű operációs rendszerek egyik alapeszköze, a Sudo, nemrégiben két súlyos biztonsági rést tartalmazó frissítésen esett át. A problémákat a Stratascale kutatója, Rich Mirch fedezte fel, és a CVE-2025-32462, valamint a CVE-2025-32463 azonosítószámokat kapták. **Bővebben...**

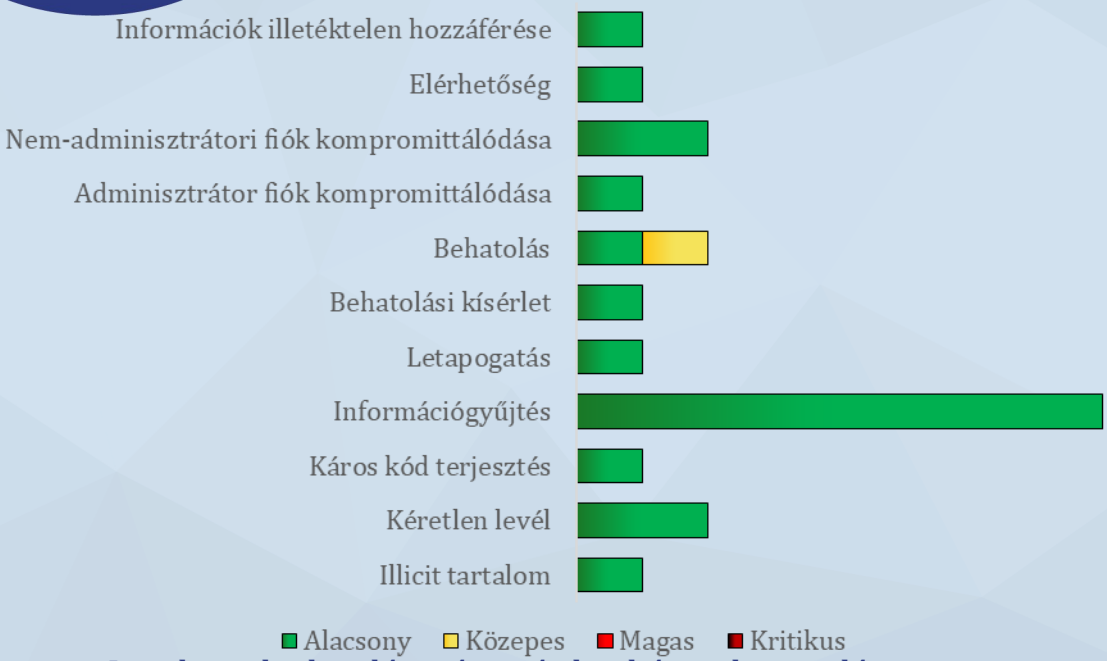
További hírekért, látogasson el **weboldalunkra**!

Statisztikai Adatok

2025.07.04.-2025.07.10.

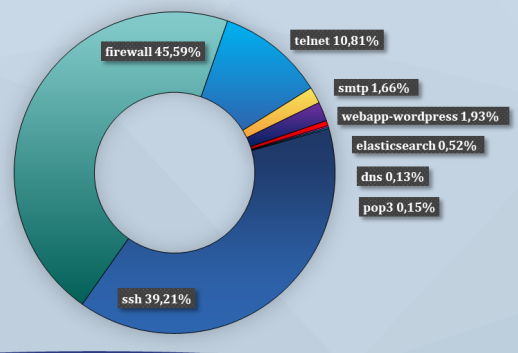
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

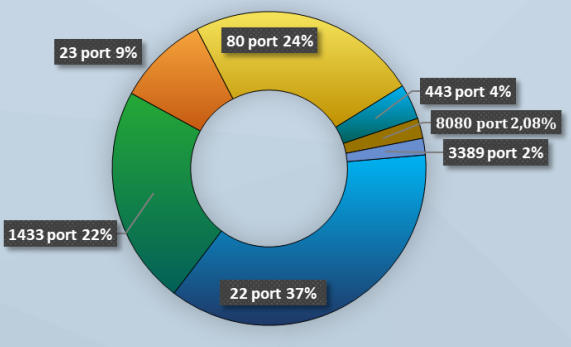
Fenyegetettségi szint: közepes



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 a SECTOR 16 csoport magyar geotermikus rendszer elleni támadásával kapcsolatban

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet** felhívja a figyelmet a **SECTOR 16** nevű **hackercsoport** által elkövetett kibertámadásra, amely 2025 júliusában egy magyarországi geotermikus termelőrendszert célzott meg.

A támadók sikeresen behatoltak a termelőüzem kritikus vezérlési interfészébe, amely révén részletes betekintést nyertek a rendszer működésébe és biztonsági beállításaiba.

Bővebben...

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

Aktuális tartalmak

NEMZETI KIBERVÉDELMI INTÉZET

1996 NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

JUBILEUMI ADÁS!
Kérdeztetek, válaszolunk!

[különkiadás]

A **Kibertámadás! 100. epizódjában** egy kis különlegességgel készültünk. Egészen eddig mi kérdeztünk: kollégáktól, szakértőktől, vendégektől, azonban most fordult a kocka, és ti kérdeztetek tőlünk. Következzenek tehát a ti kérdéseitek, és a mi válaszaink!

Köszönjük, hogy már 100 epizód óta hallgattok, követtek minket!

Meghallgatom

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

LinkedIn

További érdekességekért, látogasson el **weboldalunkra**!

Aktuális tartalmak

NEMZETI KIBERVÉDELMI INTÉZET

1996 NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

Végpontvédelem és annak megvalósítása II. Szervezeti stratégia, oktatás és jövőálló biztonság

kiberbiztonsági elemzés

Jelen dokumentum a **„Végpontvédelem és annak megvalósítása I.” című tanulmány folytatása**, amely a technológiai alapokat és a főbb fenyegetettségeket mutatta be. Ez a kiadvány a végpontvédelem szervezeti, stratégiai és oktatási megközelítésére összpontosít, gyakorlati javaslatokat adva a tudatos és hosszú távon is fenntartható védelem kialakításához.

Elolvasom

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

LinkedIn

Aktuális tartalmak

NEMZETI KIBERVÉDELMI INTÉZET

1996 NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

Szakpolitikai szempontok útmutató Az elektronikus információbiztonságra vonatkozó követelmények

A Nemzeti Kiberbiztonsági Hatóság a **megújult hazai kiberbiztonsági jogszabályi változások** kapcsán **szakpolitikai útmutatót** ad közre.

Elolvasom

Hogyan védjük meg az időseket a csalásoktól? SANS OUCH!

Megjelent a **SANS** és a Nemzetbiztonsági Szakszolgálat **Nemzeti Kibervédelmi Intézet** közös kiadványának **2025. júliusi száma**, melyben az **idősebb korosztály online biztonságával foglalkozunk**. Bemutatjuk azt, hogy **miért válnak** az idősek a különféle **csalások célpontjává**, illetve javaslatokat teszünk arra vonatkozóan, **hogyan előzhetők meg** ezek a támadások.

Elolvasom

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

Linked in

További érdekességekért, látogasson el **weboldalunkra**!

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

NEMZETI KIBERVÉDELMI INTÉZET

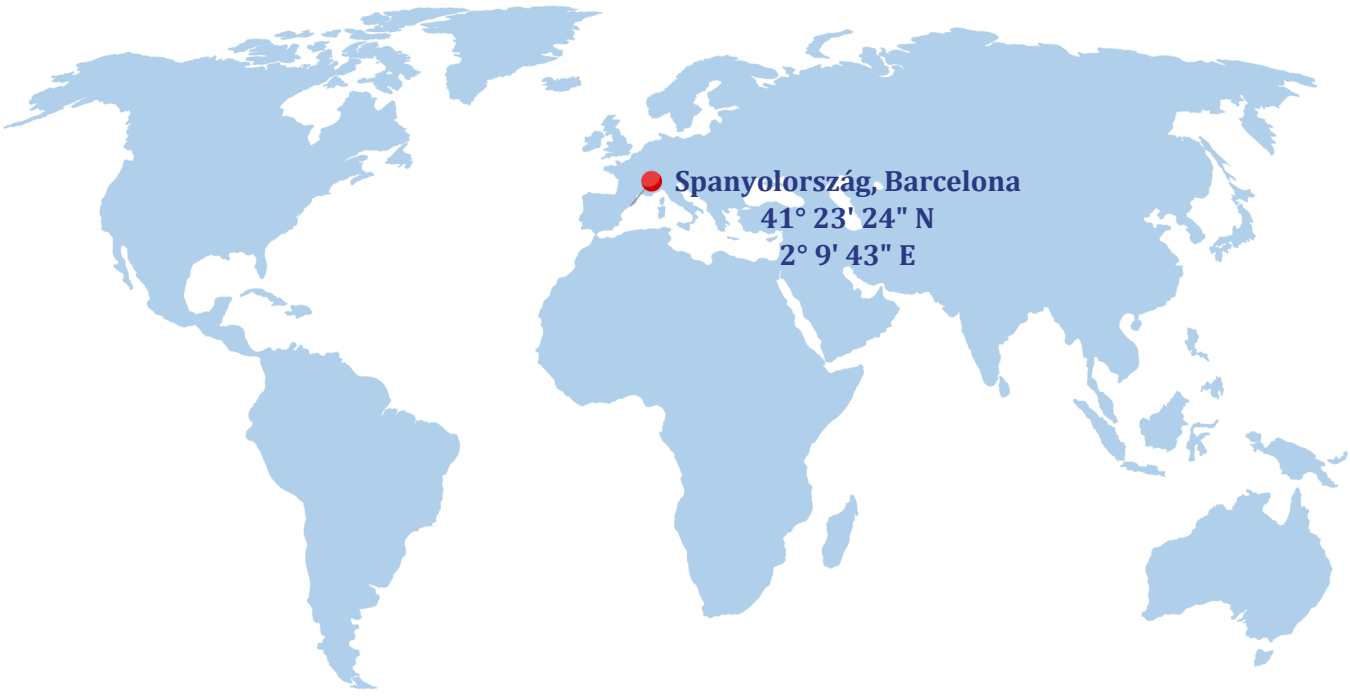
1996 NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

Barcelona Cybersecurity Congress 2025

2025. május 12 - 15.

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. május 12-15. között Barcelonában megrendezésre kerülő éves Barcelona **Cybersecurity Congress** konferencián.

A Barcelona Cybersecurity Congress (BCC) a vállalati és ipari kiberbiztonság kihívásaira fókuszáló szakmai rendezvény, ahol a hangsúly a gyakorlati megoldásokon, az élő demonstrációkon és a szabályozási trendek értelmezésén van. A cél, hogy a résztvevők testközelből ismerhessék meg, hogyan védekezhetnek hatékonyan a gyorsan változó fenyegetettségi környezetben. A rendezvény 2022 óta közösen kerül megrendezésre az **IoT Solutions World Congress**-szel (IOTSWC). Bár az együttműködés célja a két terület közötti szinergiák bemutatása, az idei évben egyértelműen az IOTSWC volt hangsúlyosabb – jelentősen több kiállító jelent meg ezen a területen, különösen az ázsiai gyártók részéről.

A BCC főként az EU NIS2 irányelv piaci szereplők gyakorlati alkalmazásával, zero-trust alapú rendszerek kialakításával, valamint a mesterséges intelligenciára épülő fenyegetésészleléssel foglalkozott. A szakmai tartalom bemutatását termékdemók, kutatási előadások és CISO-kerekasztalok segítették. Az IOTSWC oldalon idén inkább az 5G, a műhold és az eSIM-alapú megoldások továbbá a LoRaWAN technológiák kerültek előtérbe, gyakorlati példákon keresztül érzékeltetve ezek ipari alkalmazását – többek között az okosváros-fejlesztések, autóipari rendszerek és energiamenedzsment területén.

A rendezvényen részt vevő kiállítók körülbelül 70%-a IoT, 30%-a pedig kiberbiztonsági fókuszú volt. Közös jellemzőjük, hogy túlnyomórészt üzleti célú jelenléttel, konkrét termékek és szolgáltatások értékesítési szándékával vettek részt – a kiállítóközönséget elsősorban ipari és technológiai szereplők, integrátorok, valamint feltörekvő startupok alkották.

Kiknek ajánlott a beszámoló megismerése?

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

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

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

Mesterséges hackerek – az autonóm támadórendszerek árnyékában

(Roberto Clavero)

Az előadás meglehetősen provokatív címe mögött egy valós, **gyorsan közeledő technológiai fordulópont** állt: az autonóm mesterséges intelligencia alapú rendszerek megjelenése a kibertámadások eszköztárában. Az előadó több nézőponton keresztül világította meg, hogyan alakítják át az úgynevezett **Agentic AI**-k – azaz **önálló döntéshozásra és alkalmazkodásra képes MI rendszerek** – a támadók módszertanát és a védekezés lehetőségeit.

A prezentáció elején a résztvevők betekintést nyerhettek abba, **miként képesek** ezek **az ügynökszerű MI-k** klasszikus LLM-ekre (nagy nyelvi modellekre) épülve, emberszerű rugalmassággal és etikai korlátok nélkül **végrehajtani komplex támadási szcenáriókat**. Attól különlegesek az ilyen rendszerek, hogy nemcsak végrehajtják a parancsokat, de képesek tanulni saját hibáikból, újrafogalmazni céljaikat, vagy akár **„on-the-fly"** (valós időben) módosítani a támadókódokat – ez jelentősen megnehezíti az észlelést és a visszakövetést is.

Az előadó részletesen bemutatta az Agentic AI-k által kínált lehetőségeket: privilégium-eszkaláció, reverse engineering automatizálása, polimorf malware-ek generálása, és általánosságban a támadások gyorsítása. Ugyanakkor az előadás kitért a jelenlegi korlátokra is: az **MI modellek továbbra is hajlamosak „hallucinációkra",** vagyis nem valós állítások gyártására, és **a támadók** gyakran jelentős pénzügyi és technikai akadályokba ütköznek saját modell fejlesztésekor – így jelenleg főként **előre gyártott, támadásra optimalizált MI eszközöket használnak.**

Kiemelt figyelmet kapott a **„Dark AI as a Service"** piac is, ahol különféle, illegális célokra szánt mesterséges intelligenciák – mint például WormGPT, FraudGPT vagy DarkBert – bukkantak fel.

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

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

Ezek kifejezetten támadó funkciókat szolgálnak ki: phishing kampányok, kulcsnaplózók, zsarolóvírusok és más kártékony kódok generálására használhatók. Összességében **az előadás gondolatébresztő** módon mutatta be, hogy **az MI immár nemcsak védelmi, hanem offenzív célokra is éretté vált.**

A fenti előadás megtalálható a BCC YouTube-csatornáján az alábbi linken.

OWASP Top 10 sebezhetőség a nagy nyelvi modellekben

(Joan Regidor Sanfeliu, Andres Cancho Fernández)

Az előadás fókuszát az OWASP (**Open Worldwide Application Security Project**) közösség által összeállított, LLM-ekre szabott **„Top 10" sebezhetőségi lista** adta. A példák között helyet kaptak a legismertebb és legveszélyesebb támadási módszerek: prompt injection és jailbreaking technikák, információszivárgást okozó hibák, a modellek viselkedésének manipulálása, adatmérgezéses (data poisoning) támadások, valamint a nem várt, „hallucinált" válaszok, amelyek megtévesztő vagy káros kimenetekhez vezethetnek.

A prezentáció hangsúlyozta, hogy **az LLM-ek** – legyen szó chatbotokról, ügyfélszolgálati automatizációról vagy belső tudásbázisokról – jelentős előnyöket kínálnak, de ezek a rendszerek **újfajta, összetett fenyegetéseket is hordoznak.** Külön kiemelték az AI Agents, azaz önálló műveletekre képes intelligens modulok veszélyeit, amelyek ha rossz kezekbe kerülnek, szinte észrevétlenül hajthatnak végre érzékeny adatok ellopására vagy manipulálására irányuló támadásokat.

Az előadó nemcsak a problémákra hívta fel a figyelmet, hanem konkrét megoldási javaslatokkal is élt: szó volt a megelőzés és kontroll szerepéről, a szervezeti felelősség jelentőségéről, valamint arról is, hogy a biztonság nemcsak technikai, hanem stratégiai kérdés is. A hangsúly többször is arra került, hogy **az LLM-ek** bevezetése során nem elég csupán a technológiát érteni – a **működtetéshez tudatosság, folyamatos monitoring és belső szabályozás is szükséges.**

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

Hogyan reagáljunk egy EU-szintű áramszünetet okozó kibertámadásra

(Carlos Valderrama)

Az előadás egy rendkívül **aktuális és összetett válsághelyzetet szimulált**: egy Európa-szerte elterjedő kibertámadást, amely SCADA-rendszerek (**energetikai vezérlőrendszerek**) **megbénításával** tömeges **áramszünetet okoz**. A gyakorlat hátteréül egy fiktív, államilag támogatott hackercsoport, a „DarkGrid" által végrehajtott, zero-day sebezhetőséget kihasználó zsarolóvírus-támadás szolgált.

A gyakorlat célja nemcsak a technikai válaszadás szimulálása volt, hanem a szervezeti együttműködés, a válságkommunikáció és a döntéshozatali folyamatok integrált tesztelése is – mindezt az NIST SP 800-61 és ISO 27035 szabványok keretrendszerében.

A **szimulált forgatókönyv** szerint a támadás utáni 30. perctől kezdve a résztvevőknek 90 perc állt rendelkezésükre, hogy Spanyolország áramellátásának 99%-át helyreállítsák – miközben párhuzamosan kellett kezelniük jogi, kommunikációs és technikai feladatokat. A gyakorlat során hangsúlyt kapott a különböző szakterületek közötti koordináció, a felelősségek egyértelmű kijelölése, valamint a másodlagos gazdasági és társadalmi következmények mérséklése is. A téma egyik legfontosabb üzenete a **proaktív kiberreziliencia fontossága** volt: nem elég vészhelyzetben reagálni, hanem már a nyugalmi időszakokban is ki kell alakítani a fenntartható visszaállítási stratégiákat.

A fenti előadás megtalálható a BCC YouTube-csatornáján az alábbi linken.

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

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

Valós tapasztalatok a mesterséges intelligencia kiberbiztonsági alkalmazásáról

(Kirti Kumar)

A prezentáció gerincét a **SHIELD** nevű **hatlépcsős keretrendszer** adta, amely az AI-alkalmazás teljes életciklusát lefedi. Az első szakasz, a **STRATEGISE**, arra hívta fel a figyelmet, hogy **az AI-t nem szabad általános varázseszközként kezelni** – először mindig világosan meg kell határozni, mely biztonsági problémákra keresünk megoldást, és mely mesterséges intelligencia-megközelítés (pl. felügyelt tanulás, mélytanulás vagy generatív modellek) a legalkalmasabb ezekre.

A **HARMONISE** fázis az AI és a vállalati **kiberbiztonsági funkciók** – mint például detektálás, reagálás vagy helyreállítás – **összehangolását** célozta, valós példákon keresztül bemutatva az automatizált fenyegetésészlelés vagy incidenskezelés előnyeit. Az **IMPACT** lépés külön figyelmet szentelt annak, **hogyan mérhető ténylegesen az AI által nyújtott érték**: nem csupán költségmegtakarításban, hanem a reagálási idők javulásában, a fenyegetések azonosításának pontosságában és az általános kockázatcsökkentésben.

Az **ENABLE** szakasz a **szervezeti érettségre** koncentrált: rávilágított, hogy egy sikeres AI-alapú védelem nem működik megfelelő csapatstruktúra, keresztfunkcionális együttműködés, és olyan új működési modellek nélkül, mint például az MLOps vagy az AI guardrails. A **LEARN** lépés kifejezetten tanulságos volt: itt olyan **gyakori hibák** kerültek szóba, mint az adatok elégtelensége, a túlzott várakozások, a modellek értelmezhetetlensége, vagy éppen az elfogult adatbázisokból eredő torzítások.

Végül a **DEPLOY** rész egy jól strukturált **bevezetési stratégiát vázolt fel**, amely a kis léptékű pilot projektektől indulva egészen az AI széleskörű, skálázható és fenntartható alkalmazásáig vezet. Az előadó hangsúlyozta: a mesterséges intelligencia bevezetése nem egyszeri projekt, hanem egy folyamatos fejlődést igénylő folyamat, amely során a biztonsági csapatnak és a teljes szervezetnek tanulnia, alkalmazkodnia és újrahangolnia kell magát.

A fenti előadás megtalálható a BCC YouTube-csatornáján az alábbi linken.

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

Pengeélen táncolva – a kibervédelem új dimenziói

(Jose de la Cruz)

Az előadás középpontjában a modern kiberbiztonsági fenyegetések komplexitása és az azokra adott válaszok álltak. Az előadó a jelenlegi helyzetet nem csupán technológiai kihívásként, hanem üzleti és szabályozási oldalról is megközelítette. **A kiberbűnözők módszerei egyre kifinomultabbak:** célzott támadásokat hajtanak végre, amelyek nemcsak anyagi, hanem komoly reputációs károkat is okozhatnak a vállalatoknak. Ezzel párhuzamosan a szabályozási környezet is folyamatosan szigorodik – különösen a **DORA és a NIS2 irányelv követelményei** jelentenek új szintű kihívást.

Az előadás során bemutatott **Trend Vision One platform** egy átfogó és rugalmas megoldást kínál erre az új kihívásrendszerre. Külön figyelemre méltó, hogy a platform **képes lefedni minden támadási felületet** – legyen szó végponti védelemről, e-mailekről, cloud szolgáltatásokról vagy hálózati forgalomról. **Egyetlen, egységes felületen** kínál **átlátható és testreszabható biztonsági kezelést**, így ideálisan illeszkedik akár kis-, akár nagyvállalatok működésébe.

A **Trend Micro** az eseményen gyakorlati bemutatóval is készült, amelyet a Hacking Village keretében szerveztek. Itt **élő környezetben demonstrálták**, hogyan képes a platform automatizált fenyegetésfelderítésre, valamint incidensválaszra – például egy ismert exploit-alapú támadás valós idejű blokkolását és az érintett erőforrások gyors izolálását is láthattuk.

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

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

Kvantumkriptográfia – a jövő biztonsági kihívásai és lehetősége

(Aitor Brazaola-Vicario)

Az előadás középpontjában a **kvantumszámítógépek** által jelentett, egyre valóságosabb fenyegetés állt, amely a jelenlegi, **klasszikus titkosítási eljárások megbízhatóságát kérdőjelezi meg**. A résztvevők betekintést nyerhettek abba, hogyan alakul át a kiberbiztonság, ha a kvantumtechnológia eléri azt a szintet, ahol képes lesz gyorsan feltörni a ma használt titkosításokat, például az RSA vagy ECC algoritmusokat.

Az előadás nemcsak a veszélyeket, hanem a megoldásokat is vizionálta, különösen a **kvantumkulcs-megosztás** (QKD) lehetőségét, amely az egyik legígéretesebb technológia a kvantumkorszak biztonsági kihívásaira. A QKD segítségével olyan titkosítási kulcsokat lehet generálni és megosztani, amelyek fizikai törvényszerűségek alapján garantáltan **nem hallgathatók le észrevétlenül**.

A prezentáció gyakorlati példát hozott a QKD bevezetésére az energetikai szektorban, ahol különösen kritikus a kommunikáció védelme. Az egyik bemutatott projektben kísérleti jelleggel integrálták a kvantumkommunikációt egy már működő energiahálózatba, amely során kihívást jelentett a meglévő infrastruktúrával való kompatibilitás, valamint a nagy távolságokra történő adatátvitel stabil fenntartása.

A technikai aspektusokon túl az előadó részletesen kitért arra is, hogy a **kvantumkommunikáció** elterjedéséhez nemcsak technológiai, hanem szabályozási és iparági együttműködésekre is szükség lesz. A résztvevők megtudhatták, hogy jelenleg milyen kutatási irányok uralják a területet – különösen a kvantumhálózatok, kvantumismétlők és hibrid (klasszikus + kvantum) architektúrák fejlesztése kapcsán.

A fenti előadás megtalálható a BCC YouTube-csatornáján az alábbi linken.

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

Kvantumkommunikáció és posztkvantum kriptográfia

(Deepa Shinde)

Az előadás arra a kérdésre keresett választ, hogyan készülhetnek fel a szervezetek a kvantumszámítógépek elterjedésével bekövetkező kriptográfiai fordulópontra.

A **kvantumkommunikáció** és a **posztkvantum kriptográfia** (PQC) ugyanis nemcsak egy új technológiai trendet jelentenek, hanem alapjaiban írják át a biztonságról alkotott fogalmainkat.

A prezentáció során a kvantumkommunikáció működési elveit – mint például a kvantumkulcs-megosztást – röviden ismertették, majd a hangsúly a posztkvantum algoritmusokra került, amelyek **képesek ellenállni a kvantumszámítógépek támadásainak**. Az előadó bemutatta, hogy az RSA, ECC és más klasszikus eljárások hosszú távon védtelenekké válnak, ezért már most szükséges olyan algoritmusokat tesztelni és integrálni, amelyek nemcsak elméletileg biztonságosak, hanem a jelenlegi rendszerekhez is illeszthetők.

Külön figyelmet kapott a **Microsoft „Quantum Safe”** kezdeményezése, amely gyakorlati eszközökkel és útmutatókkal segíti a vállalatokat az átállásban. E program célja, hogy segítsen azonosítani a szervezet által használt, potenciálisan veszélyeztetett kriptográfiai elemeket, valamint biztosítsa a zökkenőmentes migrációt kvantumbiztos megoldásokra. A beszámoló **gyakorlati tanácsokkal is szolgált**: hogyan térképezzük fel a jelenlegi IT-ökoszisztémát, mely rendszerek frissítése kritikus, és milyen időtávlatban érdemes végrehajtani az átállást. Konkrét példaként elhangzott, hogy az olyan alkalmazások, amelyek **TLS/SSL** kapcsolatot használnak (pl. webes adminfelületek, API-k, VPN-megoldások), **különösen sérülékenyek** lehetnek a jövő kvantumtámadásaival szemben. Szóba került a belső PKI infrastruktúra felülvizsgálata is: érdemes már most azonosítani, hol használnak hosszú lejáratú tanúsítványokat, RSA-alapú kulcsokat vagy aláíró modulokat.

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

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

Az előadó javasolta, hogy **a migrációt érdemes tesztkörnyezetekkel kezdeni** kisebb, majd fokozatosan áttérni a nagyobb volumenű rendszerekre, például az ügyfélkapcsolati platformokra vagy az adatbázis-titkosítási megoldásokra. A **tervezési időtávlatként 3–5 év került meghatározásra**, különösen a nagyvállalati és szabályozott ágazatok esetében.

A fenti előadás megtalálható a BCC YouTube-csatornáján az alábbi linken.

Cyberwatch – sérülékenységek feltárása, priorizálása és kezelése hatékonyan

(Julien Piera)

A közönség betekintést nyerhetett abba, hogy a puszta sebezhetőségi listák önmagukban nem elegendők – **a kontextus és a priorizálás döntő jelentőségű a hatékony reagáláshoz**. Az előadó hangsúlyozta, hogy a különféle értékelő keretrendszerek – például a CVSS, EPSS vagy akár gépi tanulással támogatott pontozók – együttes használata jóval árnyaltabb képet ad a fenyegetések valódi súlyáról, mint bármelyik önmagában.

A prezentáció második felében a **Cyberwatch** vállalat képviselője mutatta be **saját fejlesztésű platformjukat**, amely pontosan ezt a többdimenziós megközelítést támogatja. A rendszer kiemelkedő erőssége, hogy képes egyszerre feldolgozni többféle sebezhetőségvizsgáló rendszer kimenetét, és azok eredményeit egységesített felületen értelmezhető formában jeleníti meg. A platform fejlesztésénél kiemelt szempont volt a **könnyű integrálhatóság**: kompatibilis a legtöbb elterjedt ticketing rendszerrel (pl. Jira), patch management eszközzel, CI/CD pipeline-okkal, valamint MDM megoldásokkal is. Ez nemcsak az információk áramlását teszi folyamatosabbá, hanem **jelentősen csökkenti a manuális beavatkozás igényét** – különösen nagy, összetett IT-rendszerekben.

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

A Cyberwatch egyik legérdekesebb újítása az ún. **„Prioritization 3D" módszertan** volt. Ez a **háromdimenziós rangsorolási mechanizmus** nemcsak a sérülékenység technikai súlyosságát veszi figyelembe, hanem azt is, hogy az adott hiba mennyire kihasználható, illetve mekkora üzleti hatással járna a sikeres kihasználása. **A rendszer** így **segíti a SOC csapatokat** abban, hogy a legsürgősebb és legnagyobb kockázattal járó fenyegetésekre koncentráljanak, ezáltal optimalizálva az erőforrások elosztását és minimalizálva a potenciális károkat.

IoT műholdakon keresztül – jövőbeli trendek és fejlesztések

(Frank Zeppenfeldt)

Az előadás a műholdas technológiák és az IoT (**Internet of Things**, Dolgok Internete) összefonódásának jövőjébe adott betekintést, különös hangsúlyt fektetve a technológiai szabványosításra és az európai űrkutatási törekvésekre. A prezentáció egyik kiindulópontja az volt, hogy az **Európai Űrügynökség műholdas kommunikáció** részlege kulcsszerepet játszott abban, hogy a nem földi hálózatok (**Non-Terrestrial Networks** – NTN) hivatalosan is bekerüljenek a **3GPP szabványokba** (3rd Generation Partnership Project; nemzetközi együttműködés, amely a mobil távközlési szabványok fejlesztéséért felel). Ez mérföldkőnek számít, hiszen így a műholdas kommunikáció egyenrangú része lett a globális mobilkommunikációs ökoszisztémának.

Az előadás másik jelentős eleme a **kis teljesítményű műholdas IoT-szabványok** fejlődése volt. Az ilyen rendszerek kifejezetten az **alacsony adatforgalmú, de globális lefedettséget igénylő eszközök** – például mezőgazdasági szenzorok, tengeri konténerek, vagy távoli környezetvédelmi megfigyelők – számára kínálnak megoldást. A prezentáció kitért arra is, hogy ezek a technológiák hogyan egészítik ki a földi IoT-hálózatokat, különösen ott, ahol nincs vagy nem gazdaságos a hagyományos lefedettség kiépítése.

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

A technológiai fejlesztések mellett az előadó hangsúlyozta a **szinergiák** fontosságát más űralapú szolgáltatásokkal, mint például a **földmegfigyelés** vagy a **navigáció**. Például, a műholdas IoT-eszközök által gyűjtött adatok közvetlenül integrálhatók lehetnek a földmegfigyelő műholdak által szolgáltatott képi információkkal, így **komplexebb döntéstámogató rendszerek épülhetnek ki** – akár környezetvédelmi, akár logisztikai célokra.

Okosabb IoT: gépi látás és energiahatékonyság eszközszinten

(Nicolas Gaude, Francesco Mattioli)

Az előadó egy olyan gyakorlati megközelítést mutatott be, amely az **edge-alapú** (edge computing avagy eszközszintű feldolgozás) **IoT megoldások** és a **mesterséges intelligencia ötvözésével** kínál jövőbemutató válaszokat a valós idejű érzékelés kihívásaira. A fókuszban a népszerű **YOLO** (You Only Look Once) gépi látásmodell és annak integrációja állt, melyet az előadók kis teljesítményű, energiahatékony STM32N6 mikrovezérlőkbe (MCU-kba) ágyaztak. Ez a megoldás lehetővé teszi, hogy edge-eszközök is képesek legyenek **valós időben objektumokat érzékelni**, azok mozgását követni, sőt testtartás- vagy pózfelismerést is végezni – mindezt felhőkapcsolat nélkül, lokálisan, rendkívül alacsony energiafelhasználás mellett.

A prezentáció során részletesen bemutatták azokat a **technológiai és mérnöki kihívásokat**, amelyekkel az AI-modellek ilyen korlátozott számítási kapacitással rendelkező eszközökbe való áthelyezése járt. Szó esett az optimalizációs folyamatokról, a memóriahasználat csökkentéséről és a valós idejű működéshez szükséges sebesség eléréséről is.

A végeredmény egy olyan **intelligens rendszer**, amely különösen hasznos lehet az ipari automatizálásban (például gépsorok hibafelismerésében), az autonóm robotikában, valamint az okosvárosok kamerarendszereiben, ahol fontos a gyors reakció, alacsony késleltetés és az önálló működés – mindezt a lehető legalacsonyabb energiafelhasználással.

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

Nincs több idő a reagálásra – a CISO szerepe az I(o)T biztonságában

(: DrBA MSc Jeroen Van Der Vlies)

Az **ipari (OT) és hálózatba kapcsolt (IoT) eszközök biztonsága** már régóta nem csak az informatikai munkatársakat érinti. A **szervezetek digitális átalakulása** új kockázati terepet teremtett, amelyben a CISO-knak (**Chief Information Security Officer**) kulcsszerepük van. Kiderült, hogy az I(o)T biztonság egyre inkább stratégiai jelentőségű kérdéssé válik, amely közvetlenül kapcsolódik a vállalati működés folytonosságához és a versenyképességhez.

A prezentáció gyakorlati példákon keresztül mutatta be, hogy **a vállalatokat érintő fenyegetések** – például zsarolóvírusok vagy akár nemzetállami támadások – hogyan béníthatják meg a gyártósorokat vagy logisztikai rendszereket. Külön kiemelésre került, hogy ezek a támadások nemcsak **adatvesztéssel**, hanem közvetlen **pénzügyi kárral** és hosszú távú **reputációromlással** is járhatnak.

A szakértő rámutatott, hogy a **megfelelő védekezéshez** nemcsak technikai megoldásokra, hanem **szervezeti átalakításokra is szükség van**. A vezetőknek be kell emelniük a kiberbiztonságot az üzleti döntéshozatal szintjére és annak kultúráját a szervezet minden rétegébe át kell ültetni. A beszámoló **gyakorlati javaslatokat is adott**: ilyen például a **Zero Trust** architektúra bevezetése, kockázatértékelési rendszerek alkalmazása, valamint a CISO közvetlen bevonása a felsővezetői tanácsokba.

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

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

Az IoT hálózati kapcsolatok jövője

(Nicole Russo)

A növekvő számú okoseszköz és a gyorsan változó alkalmazási környezet miatt ma már nem elegendő egyetlen kommunikációs szabványra támaszkodni: az **ökoszisztéma jövőjét** a rugalmas, interoperábilis és energiatakarékos hálózatok jelentik. A **jelenlegi IoT-megoldások** gyakran fragmentáltak, különböző protokollokat használnak, mégis közös bennük, hogy a biztonság és a fenntartható adatátvitel kulcsfontosságú kérdések.

Az előadó általa bemutatott **Myriota UltraLite szolgáltatás** olyan eszközöket céloz, amelyek akár távoli, infrastruktúra-mentes területeken is képesek adatokat gyűjteni és továbbítani, miközben az akkumulátor élettartamuk években mérhető. Az újonnan ismertetett **HyperPulse hálózat** az 5G és L-sávú műholdas (GEO) technológiákra épül, és lehetőséget kínál mezőgazdasági, logisztikai, ipari vagy környezetvédelmi szenzorok globális összekapcsolására. Szó eset arról is, hogy a **jövő IoT-infrastruktúrájának** nemcsak a teljesítményre és lefedettségre **kell fókuszálnia**, hanem **a kiberbiztonságra is**. A jogosulatlan hozzáférés és az adatszivárgás veszélye minden platform esetében valós, ezért a beépített védelem és a skálázhatóság **kulcselemei a következő generációs fejlesztéseknek**.

LoRaWAN – tíz év innováció, a jövő kibontakozása

(Alper Yegin)

Az előadás a **LoRaWAN technológia** tízéves fejlődéstörténetét járta körül, amely alatt az alacsony energiaigényű, nyílt szabványú vezeték nélküli kommunikációs protokoll egy kezdetben ígéretes technológiából ipari és globális szinten elismert megoldássá nőtte ki magát. A résztvevők betekintést nyerhettek abba, hogy a **LoRa Alliance ökoszisztémája** hogyan segítette elő ezt a növekedést, különös hangsúlyt helyezve az energiatakarékosságra, skálázhatóságra és az interoperábilis működésre.

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

Az előadó kiemelte, hogy ma már számos országban a **LoRaWAN az IoT infrastruktúra gerincét képezi** – különösen az olyan iparágakban, mint az energiaszektor, az okos városok, a mezőgazdaság vagy a víz- és hulladékgazdálkodás. Konkrét példákkal illusztrálta, hogyan használják a technológiát közüzemi mérőórák távleolvasására, parkolásmenedzsmentre, levegőminőség-monitorozásra vagy épp távoli állapotfigyelésre ipari berendezések esetén. A LoRaWAN nem csupán technológiai, hanem **gazdasági és környezeti szempontból** is előnyös: alacsony költségű kiépítés, hosszú akkumulátor-élettartam és fenntartható működés jellemzi. A prezentáció végén szó esett a **jövőbeli irányokról** is – például a roaming, a szatellit LoRa, valamint a globális lefedettséget célzó stratégiák előretöréséről, melyek új távlatokat nyitnak meg a technológia előtt.

IoT az űrből – műholdas megoldások és jövőbeli kilátások

(Alper Yegin)

Az előadás a **LoRaWAN technológia** és a **műholdas hálózatok** összefonódását vizsgálta, különös tekintettel arra, hogyan válhat a nem földi (**non-terrestrial**) hálózatok használata a jövő IoT-rendszereinek szerves részévé. A prezentáció betekintést adott a **legújabb technológiai fejlesztésekbe**, amelyek lehetővé teszik, hogy a **LoRaWAN protokollt műholdas kapcsolatban is alkalmazzák** – különösen olyan régiókban, ahol földi infrastruktúra nem vagy csak korlátozottan áll rendelkezésre.

A hallgatóság megismerhette, hogyan **integrálják a műholdas IoT-kommunikációt** professzionális alkalmazásokba, például mezőgazdasági vagy logisztikai területeken, és milyen konkrét esettanulmányokon keresztül vezették be a technológiát a végfelhasználók számára. Az előadó példákkal világította meg, hogy egyes iparágak már most is profitálnak a globális lefedettségből és az alacsony sávszélesség-igényű, de megbízható adatátvitelből.

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

Fontos szerep jutott a **LoRa Alliance** szabványosítási munkájának is: a szervezet az interoperabilitás és az ökoszisztéma fenntarthatóságának biztosításával támogatja a technológia elterjedését.

A jövőbe tekintve az előadás egy világos irányvonalat vázolt fel, ahol a LoRaWAN és a műholdas kapcsolatok konvergenciája **új korszakot hozhat a globális, vezeték nélküli IoT-megoldásokban** – a sarkvidéktől a tengeri konténerszállításig.

Beltéri pozícionálás újragondolva – AI-alapú, infrastruktúra-mentes zónakövetés

(Henry Huang)

Az előadó a **valós idejű beltéri helymeghatározás** korszerű lehetőségeit járta körül, különös tekintettel az iparági igényekre a személyzet és eszközök nyomon követésében.

A hagyományos megoldások – melyek általában összetett infrastruktúrát és jelentős telepítési költségeket igényelnek – helyett az előadó egy **innovatív megközelítést** vázolt fel, amely a LoRaWAN technológia és a mesterséges intelligencia együttes alkalmazásán alapul. Ez a kombináció lehetővé teszi az ultraalacsony energiafogyasztást, a nagy kiterjedésű lefedettséget, valamint a költséghatékony beltéri és kültéri követést, akár infrastruktúra kiépítése nélkül is.

A prezentáció külön hangsúlyt fektetett arra, **hogyan használhatók AI-modellek a pozícióadatok értelmezésére és zónakövetésre** anélkül, hogy pontos GPS-koordinátákra vagy bonyolult szenzorrendszerekre lenne szükség. Az elhangzott példák között szerepelt egy olyan gyártóüzem, ahol a megoldás segítségével valós időben követik a dolgozók tartózkodási helyét és mozgását a biztonsági előírások betartásának támogatására, illetve egy logisztikai központ, ahol az eszközök és járművek nyomon követése optimalizálta a rakodási folyamatokat.

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

Az emberek és a környezet védelme LoRaWAN-nal

(Ivan Arkipof, Robin Wulfes, Christoph Wergen,Olivier Beaujard, Yoav Ludmer)

A **LoRaWAN technológia** nem csupán egy hatékony adatátviteli megoldás az IoT világában, hanem egyben **kulcsfontosságú eszköz** lehet a fenntarthatósági célok elérésében is. A prezentáció olyan valós példákon keresztül mutatta be a technológia alkalmazását, ahol a környezetvédelem, a munkabiztonság és az energiahatékonyság kézzelfogható eredményeket hozott.

Elhangzott egy, a mezőgazdaságban alkalmazott megoldás, ahol a szenzorhálózatokkal kombinált **LoRaWAN-alapú rendszer** lehetővé tette a vízfogyasztás optimalizálását, a talajnedvesség valós idejű követését, és ezáltal jelentős megtakarításokat hozott mind a költségek, mind az ökológiai lábnyom tekintetében. Egy másik példa egy ipari telephely volt, ahol a **LoRaWAN érzékelők** segítségével monitorozták a levegő minőségét, a zajszintet és az energiafogyasztást, így proaktívan tudtak beavatkozni a környezetre ártalmas folyamatok esetén. Az előadó hangsúlyozta, hogy a **LoRaWAN** egyik **legnagyobb előnye** az alacsony energiafogyasztás és a hatalmas lefedettségi képesség, amely lehetővé teszi, hogy a legeldugottabb vagy legköltségérzékenyebb környezetben is megvalósítható legyen az IoT-alapú adatgyűjtés és beavatkozás.

Kódtól a pajzsig – a DevSecOps jövője az MI és a LAZARUS révén

(Panagiotis Markovits, Adriana Freitas)

Az előadó a **LAZARUS** nevű, hároméves, EU által finanszírozott projektet mutatta be, amely a szoftverbiztonság modernizálását tűzte ki célul a DevSecOps szemlélet mentén. A projekt egy olyan **mesterséges intelligenciára épülő platformot fejlesztett**, amely a teljes szoftverfejlesztési életciklusban (**Software Development Lifecycle** – SDLC) képes automatizált sebezhetőség-érzékelésre, titkos kulcsok kiszűrésére, és a biztonságos fejlesztési gyakorlatok előmozdítására.

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

A workshop során a résztvevők **gyakorlati bemutatót** láthattak a **LAZARUS rendszer működéséről**, és megismerhették, hogyan képes a platform különböző fejlesztői környezetekben (pl. GitHub workflow-k vagy CI/CD pipeline-ok) már a kódsorok írása közben jelezni a hibás biztonsági megoldásokat vagy a rosszul kezelt titkos adatokat (pl. jelszavak, API-kulcsok). Szó esett többek között a Secret **Management Detection** és az automatikus hibajavító javaslatok funkcióiról is.

Rugalmasság és méretezhetőség az IoT világában – eSIM technológiával

(Panagiotis Markovits, Adriana Freitas)

Az előadás középpontjában az **IoT eSIM** (különösen az **SGP.32 szabvány**) állt, amely forradalmasítja a gépek közötti kommunikációban (M2M) használt hagyományos megoldásokat. A közönség betekintést nyerhetett abba, hogy miként válik lehetővé a fizikai SIM-kártyák nélküli, **távoli szolgáltatóváltás** az IoT eszközök esetében – anélkül, hogy bárkit a helyszínre kellene küldeni. Ez a rugalmasság nemcsak a gyorsabb eszköztelepítést segíti elő, hanem hosszú távon jelentős költségmegtakarítással is jár.

Külön kiemelésre került, hogy a technológia nagyban **megkönnyíti a globális működést** is: az eszközöket bármilyen országban üzembe lehet helyezni úgy, hogy a helyi távközlési szabályozásoknak megfelelő szolgáltatót lehet választani – akár a működés során dinamikusan is. Az előadásból az is kiderült, hogy az IoT eSIM nemcsak technológiai, hanem **stratégiai előnyt is nyújt**: függetlenedni lehet az egyes szolgáltatóktól, egyszerűsödik az eszközök életciklusának kezelése, és a piaci igényekre is gyorsabban lehet reagálni. A megoldás tehát nemcsak választási szabadságot, hanem skálázhatóságot is kínál – ami különösen fontos az egyre nagyobb számú IoT eszközt üzemeltető vállalatok számára.