NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2025. 19. hét

HÍREK

- Obfuszkáció – A láthatatlan háború
- AgeoStealer: Célkeresztben a játékosok
- Folytatódik a sor: kibertámadás áldozata lett a Harrods és a Co-op is
- 13 millió kattintást értek el a Dracula adathalász szolgáltatással
- Súlyos sebezhetőségeket találtak az Apple AirPlay protokollban

STATISZTIKAI ADATOK

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

BESZÁMOLÓ

- CVE/First VulnCon 2025 & Annual CNA Summit konferencia

KONTAKT

edt@nki.gov.hu

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D

NEWS

IT biztonsági
HÍREK

Obfuszkáció – A láthatatlan háború
(cert.pl)

A támadók az elemzést megnehezítő technikák, például az **obfuszkáció** alkalmazásával próbálják akadályozni a **visszafejtést**, amely a védelmi oldalon dolgozó kutatók egyik fő eszköze a rosszindulatú kód működésének megértésére. Az obfuszkáció célja, hogy a programkód szándékosan **értelmezhetetlenné, zavarossá váljon**, miközben a működése változatlan marad. **Bővebben...**

AgeoStealer: Célkeresztben a játékosok
(flashpoint.io)

A Flashpoint kutatása szerint az ***AgeoStealer*** egy új, **célzottan játékosokat támadó malware**, amely social engineering technikákra épít. A kampányok során a támadók **játékfejlesztői csoportnak** álcázzák magukat, és béta tesztelésre hívják meg a kiszemelt áldozatokat, főként Discordon keresztül. **Bővebben...**

Folytatódik a sor: kibertámadás áldozata lett a Harrods és a Co-op is
(bleepingcomputer.com)

A Marks and Spencer a múlt héten kibertámadás áldozata lett, amely az online rendelési rendszereinek, az érintésmentes fizetési rendszerének és a Click & Collect szolgáltatásának megszakadásához vezetett. **Bővebben...**

13 millió kattintást értek el a Dracula adathalász szolgáltatással
(bleepingcomputer.com)

884 000 hitelkártyaadatot loptak el a Dracula Phishing-as-a-Service (Phaas) adathalász szolgáltatást nyújtó platform segítségével. Az SMS-ben érkező káros hivatkozásokra 2023 és 2024 közötti időszakban mintegy 13 milliószor kattintottak világszerte. **Bővebben...**

Súlyos sebezhetőségeket találtak az Apple AirPlay protokollban
(bleepingcomputer.com)

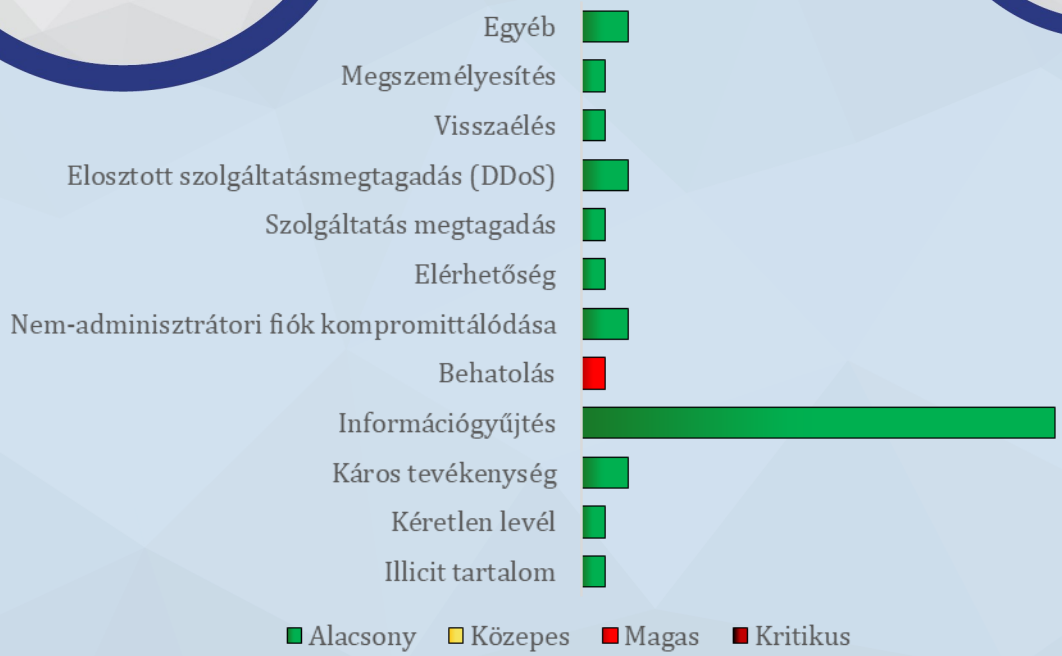
A kiberbiztonsági szakemberek újabb **kritikus** sérülékenységekre hívták fel a figyelmet az **Apple AirPlay** protokolljában és az **AirPlay SDK**-ban. Az Oligo Security kutatói által felfedezett, ***AirBorne*** gyűjtőnéven ismertté vált hibák **23 különböző sebezhetőséget** tartalmaznak. Ezek a sérülékenységek lehetővé teszik többek között a **távoli kódfuttatást** (RCE), a **felhasználói interakció** megkerülését, a **man-in-the-middle** (MITM) és **szolgáltatásmegtagadásos** (DoS) támadásokat, valamint **hozzáférés-vezérlési listák** (ACL) megkerülését. **Bővebben...**

Statisztikai Adatok

2025.04.30.-2025.05.08.

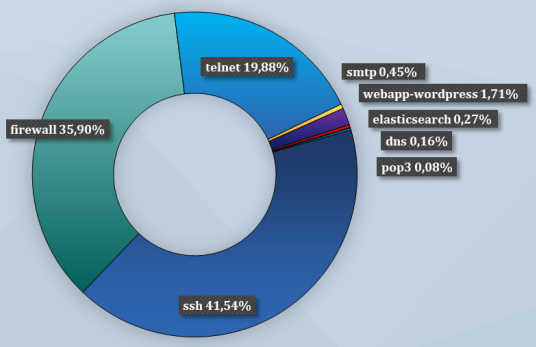
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

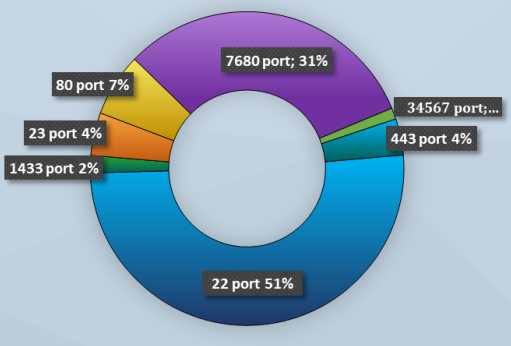
Fenyegetettségi szint: közepes



Incidensek eloszlása típus és kockázati besorolás szerint

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





További érdekességekért, látogasson el **weboldalunkra**!

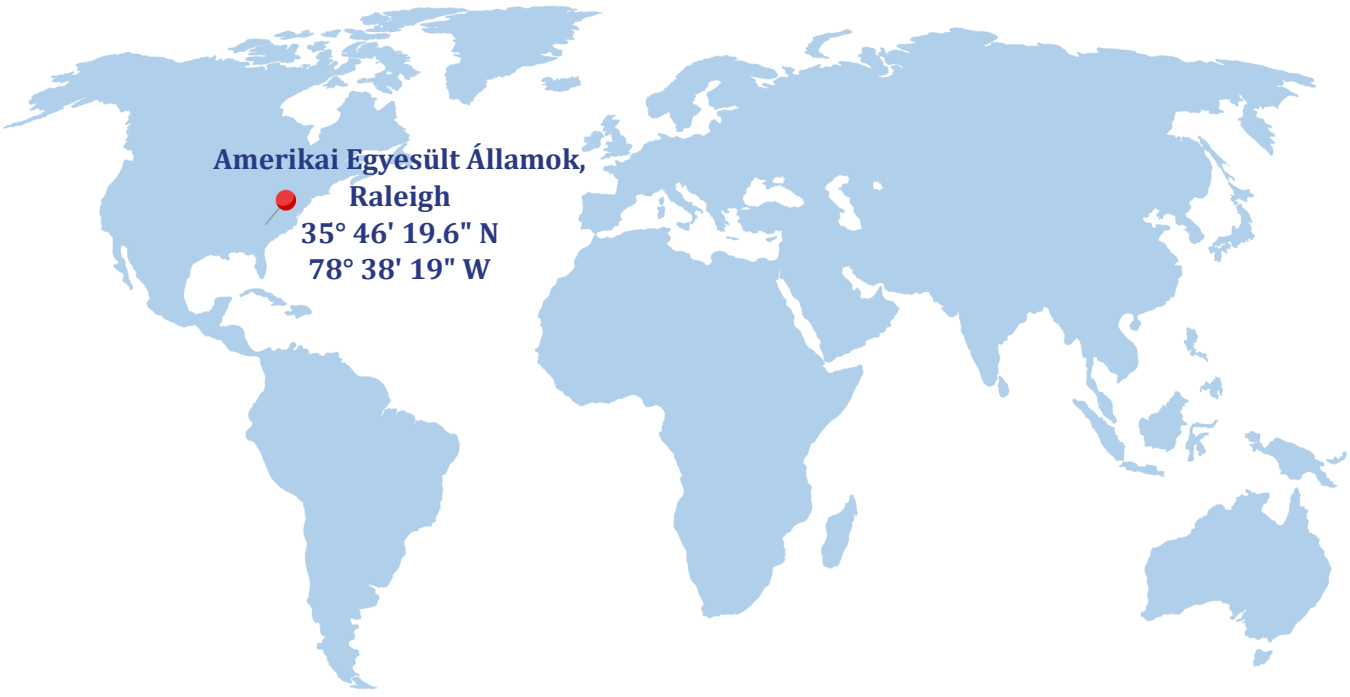
BBA-PLUSZ-3.1.2-24-2024-00003. sz. pályázat részeként

CVE/First VulnCon 2025 & Annual CNA Summit konferencia

2025. április 7-10.

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet** munkatársai **Széchenyi Terv Plus 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-3.1.2-24-2024-00003. sz. pályázat részeként

A Nemzeti Kibervédelmi Intézet munkatársai részt vettek a 2025. április 07-10. között Raleigh-ben megrendezésre kerülő éves CVE/FIRST VulnCon 2025 & Annual CNA Summit konferencián. A FIRST és a CVE Program által közösen szervezett rendezvényen számos IT biztonsággal, kibervédelemmel, továbbá sebezhetőségkezeléssel foglalkozó nemzetközi szakember tartott előadást a legkülönfélébb témákban. Az egyes előadás-blokkok 30-120 perc terjedelműek voltak. Az Észak-Karolina Állami Egyetem McKimmon Center konferenciaközpontja színvonalas helyszín volt, rengeteg előadóteremben, párhuzamosan zajló előadások, panelbeszélgetések, valamint workshopok mellett egy hatalmas bemutatóteremben számos technológiai szereplő állt elő az IT biztonság területén kínált legújabb megoldásaival.

A konferencia vezértémája a **sebezhetőségkezelési ökoszisztéma fejlesztése** volt, illetve a **mesterséges intelligenciák sérülékenységeinek detektálása**. Számos olyan megoldásról halhattak a résztvevők, melyek az AI technológiák sebezhetőségeinek bekategorizálására, kockázatkezelésére és az ezekhez kapcsolódó biztonsági szabványok fejlődésére összpontosítottak. Betekintést nyertek számos kutatásba, esettanulmányba és gyakorlati megoldásba, amelyek segíthetnek a modern biztonsági fenyegetések hatékony kezelésében.

A szakmailag legfontosabb előadások rövid összefoglalója az alábbiakban olvasható.

Kiknek ajánlott a beszámoló megismerése?

- Minden kiberbiztonsági szakember számára.
- Sérülékenységvizsgálattal foglalkozó specialisták számára.

BBA-PLUSZ-3.1.2-24-2024-00003. sz. pályázat részeként

Belgian Federal Government invites Ethical Hackers for First-Ever 'Hack the Government' Event

(Susan Bushe — Centre for Cybersecurity Belgium)

A Belgiumi Szövetségi Kormány a tavalyi évben első alkalommal rendezte meg a „Hack the Government" eseményt, amely során **etikus hackerek azonosították és jelentették a kormányzati rendszerekben fellelhető biztonsági sebezhetőségeket**. A 2024-es esemény célja a nemzeti kiberbiztonság erősítése, valamint a kormány és a polgárok közötti bizalom növelése volt. A rendezvény során akormány különböző bug bounty platformokkal, például a HackerOne, illetve a Bugcrowd szolgáltatásokkal működött együtt, hogy biztonságos környezetet biztosítson a hackerek számára. Az etikus hackerek a kormányzati rendszerek sebezhetőségeit közvetlenül azonosították és segítettek azok kijavításában. Az esemény tapasztalatai, valamint tanulságai fontos lépést jelentettek Belgium kiberbiztonsági stratégiájának fejlesztésében, és hozzájárultak a közszolgáltatások digitális biztonságának javításához. Az esemény sikeres lebonyolítása után a kormány elkötelezett maradt a jövőbeni együttműködések és a transzparens, biztonságos digitális környezet fenntartása mellett. Ennek következtében már tervezési fázisban van az esemény 2025-ös folytatása.

Securing the Future: Navigating AI Vulnerabilities and Evolving Security Practices

(Lisa Bradley & Sarah Evans—Dell)

Ebben az előadásban Lisa Bradley és Sarah Evans azt mutatták be, hogy az AI (mesterséges intelligencia) egyre növekvő használata milyen új biztonsági kihívásokat szül a szoftverek világában. Rámutattak, miszerint az **AI-modellek nem csupán „black boxok", hanem olyan komplex rendszerek**, amelyek sebezhetőségei nagyon eltérnek a hagyományos szoftverhibáktól. Ezek közé tartozik például az **adatmanipuláció**, vagy az AI-tanítás során bekövetkező **torzulások**. Az előadás célja az volt, hogy megmutassa, hogyan lehet a hagyományos PSIRT folyamatokat adaptálni az **AI-központú biztonsági környezetekhez**.

BBA-PLUSZ-3.1.2-24-2024-00003. sz. pályázat részeként

Models and Systems: How to Think About Vulnerabilities and Artificial Intelligence

(Erick Galinkin - NVIDIA)

Az előadás rávilágított arra, miszerint a mesterséges intelligencia, de különösen a generatív nagy nyelvi modellek használata hogyan változtatja meg a **sebezhetőségekről és a CVE-azonosítók hozzárendeléséről való gondolkodásmódot**. A prezentáció bemutatta a különbségeket a mesterséges intelligencia modellek és rendszerek között, továbbá azt, hogy a CNA (Center for Naval Analyses) kutatóközpont jelenlegi működési szabályai szerint miképpen kellene kezelni a mesterséges intelligenciát a sérülékenységkezelés területén.

Comprehensive Vulnerability Management Framework for Nuclear Facilities: Integrating Security, Safety and Risk Assessment

(Ieck-Chae Euom & Joon-Seok Kim & Seong-Su Yoon—System Security Research Center, Chonnam National University)

A Rendszerbiztonsági Kutatóközpont négyéves kutatómunka során fejlesztette ki az **NVAS-t (Nuclear Vulnerability Analysis System)**, ami egy újfajta sebezhetőségkezelési és kereszt-hatásvizsgálati keretrendszer nukleáris létesítmények számára. Az NVAS **átfogó sebezhetőségi elemzéseket végez** a kritikus eszközökön, figyelembe véve a működési jellemzőket és a potenciális digitális, illetve fizikai kockázatokat, hogy biztosítsa a nukleáris létesítmények rendszereinek védelmét a kibertámadásoktól, a fizikai betörésektől és a műszaki meghibásodásoktól egyaránt. Az előadás az atomerőművekre jellemző sajátosságokat figyelembe vevő **sebezhetőség-értékelési módszertanokra**, valamint a biztonsági intézkedések és a **biztonsági tervezési szabványok** közötti kölcsönhatások elemzésére összpontosított. Az előadás résztvevői megismerkedhettek azon legújabb iparági normákkal és szabványokkal, amelyek elősegítik a nukleáris létesítmények kibervédelmi stratégiájának folyamatos fejlesztését.

BBA-PLUSZ-3.1.2-24-2024-00003. sz. pályázat részeként

„I Can Do This All Day." – CVD From a Governmental Perspective

(Tassilo Thieme—German Federal Office for Information Security [BSI])

Az előadásban bemutatásra került, hogy az elmúlt évek során a BSI (Németországi Szövetségi Információbiztonsági Hivatal) miképpen alakította ki a **koordinált sebezhetőségi közzétételi (CVD) eljárását**, illetve milyen kihívásokkal néztek szembe a hivatal munkatársai ennek során. A belga kormánnyal ellentétben itt nem került bevezetésre „Bug Bounty" program, hanem helyette egy **„Vulnerability Report Program"** volt amit meghirdettek és bevezettek. Ennek következtében a sérülékenységek bejelentésére vonatkozó eljárásrend, valamint az ehhez használatos formanyomtatvány többször is át lett tervezve.

Exploited CVEs of 2024: Lessons for Vendors and Defenders

(Patrick Garrity—VulnCheck)

Patrick Garrity előadásában a 2024-ben először kihasznált sebezhetőségeket elemezte. Részletesen bemutatásra kerültek a **kihasznált CVE-k trendjei és mintái**, valamint az, **hogyan lehet előre jelezni a potenciális támadásokat**. Az előadás során a résztvevők betekintést nyerhettek abba, hogyan azonosíthatják a kockázatokat még a kihasználás előtt, továbbá miképpen erősíthetik meg a védelmi intézkedéseket.

Securing Citizen Developers: A New Opportunity to Build Safe Applications

(Kayla Underkoffler—Zenity)

Kayla Underkoffler előadásában a **„citizen developer"** (nem szakmai fejlesztő) platformok biztonsági kihívásait tárgyalta. A szakértő bemutatta, hogyan lehet biztonságos alapokat létrehozni ezekben a platformokban, és hogyan lehet megelőzni a sebezhetőségek bevezetését a fejlesztési folyamatokba. Az előadás során a résztvevők gyakorlati tanácsokat kaptak a biztonságos alkalmazásfejlesztés

Challenges in Open Source Software Identification

(Martin Prpic—Red Hat)

Martin Prpic a **nyílt forráskódú szoftverek (OSS) komponenseinek azonosítási problémáiról** beszélt, amelyek egyre kritikusabbá válnak a szoftverellátási lánc biztonsága szempontjából. Rámutatott, hogy nincs egységes, univerzálisan használt azonosítási módszer vagy rendszer, és a különböző platformok (pl.: GitHub, Maven, PyPI) máshogy kezelik a verziókat, hash-eket vagy metaadatokat. Ez megnehezíti a sebezhetőségek visszakeresését, követését és kezelését. Az előadás kulcspontja az volt, hogy milyen **szabványosítási lépések lennének szükségesek** ahhoz, hogy ezek a komponensek jobban nyomon követhetők és beazonosíthatók legyenek biztonsági szempontból a sérülékenységkezelési ökoszisztémán belüli együttműködés javításának érdekében.

Identifying Malicious OSS Across Ecosystems

(Dan Fiedler—Microsoft)

Dan Fiedler a Microsoft oldaláról hozott gyakorlati példákat arra, **hogyan lehet felismerni és kiszűrni rosszindulatú nyílt forráskódú csomagokat különböző ökoszisztémákban**, például a NPM, PyPI vagy RubyGems platformokon. Bemutatott egy eszközkészletet és több elemzési módszert (pl.: viselkedéselemzés, automatikus kódvizsgálat, metadata-anomáliák keresése), amelyek segítenek detektálni azokat a csomagokat, amelyek például adathalász célokat szolgálnak, vagy backdoorokat tartalmaznak. Az egyik kiemelt eset a „typosquatting” jelenség volt, amikor rosszindulatú fejlesztők a népszerű csomagokhoz nagyon hasonló nevű csomagokat tesznek közzé.

BBA-PLUSZ-3.1.2-24-2024-00003. sz. pályázat részeként

Building a PSIRT for a Standards Organization

(Jim Duncan)

Jim Duncan előadása abba nyújtott betekintést, hogyan lehet „**sebezhetőségkezelő csapatot" (PSIRT** – Product Security Incident Response Team) létrehozni és működtetni egy szabványosító szervezet keretein belül. Az ilyen típusú szervezetek különleges környezetet jelentenek, hiszen gyakran versenytárs cégek is együtt dolgoznak közös iparági szabványokon. Duncan bemutatta, milyen nehézségekkel jár a **biztonsági problémák nyilvánosságra hozatala**, valamint a konfliktusok kezelése, miközben az átláthatóságot és a bizalomépítést is szem előtt kell tartani. Az előadás során esettanulmányokon keresztül mutatta be, hogyan lehet hatékony és agilis PSIRT-et építeni egy ilyen összetett közegben.

Towards a Minimum Viable Enumeration of Vulnerabilities

(Jay Jacobs— Analygence Labs & Art Manion—Empirical Security)

Az előadás középpontjában az **MVVE** (Minimum Viable Vulnerability Enumeration) koncepciója állt, amely azon alapul, hogy a **sérülékenység-kezelés első**, illetve **legfontosabb fázisa a felfedezés**, ami megtörténte nélkül a teljes kezelési folyamat meghiúsul. Az MVVE szerint egy sérülékenységi rekordnak tartalmaznia kell egy egyedi, publikus azonosítót, továbbá elegendő információt ahhoz, hogy a termék fogyasztója elindíthassa a kezelés folyamatát, valamint, hogy az adott sérülékenység egyértelműen elkülöníthető legyen másoktól. A bemutató során elemezték a sérülékenység-kezelés négy szakaszát (felfedezés, priorizálás, mitigáció és visszacsatolás) és megvizsgálták, hogy mely adatmezők támogatják ezeket a fázisokat. Kiemelték, hogy az MVVE-hez elegendő csupán két kulcselem: a sérülékenység azonosítója és a termék azonosítója. Az olyan kiegészítő információk, mint például a CVSS, CWE vagy EPSS értékek, csak az úgynevezett „Adequate Vulnerability Enumeration" (AVE) szinthez szükségesek. Az előadás célja az volt, hogy tisztább képet adjon arról, mely adatelemekre van valóban szükség a sérülékenységek hatékony nyilvántartásához és kezeléséhez – különösen az első, kritikus lépésben: a felfedezésben.

Madness of Vulnerability Management in Modern Cloud, Container, How to Win the Battle Practitioners View

(Francesco Cipollone—Phoenix Security & Nate Sanders—Bazaarvoice)

2015 óta a konténerizált környezetek és a modern szoftverfejlesztési gyakorlatok alapjaiban változtatták meg az alkalmazások építésének és védelmének módját. Ezek az újítások teljesen átalakították a kiberbiztonsági környezetet, így eddig nem látott kihívásokat hoztak a sebezhetőségkezelés terén, különösen a méretezhetőség, a komplexitás, valamint az adatok konzisztenciája kapcsán. A panelbeszélgetésen bemutatták, miként segíthet egy **kockázatalapú megközelítés** e kihívások kezelésében, gyakorlati módszerekkel és alkalmazható tanulságokkal, mivel a széttöredezett, elszigetelt biztonsági adatok gyakran akadályozzák a sebezhetőségek hatékony priorizálását. Az előadás olyan stratégiákat taglalt, amelyekkel különböző eszközökből, illetve környezetekből származó adatokat lehet egységesíteni, hogy átfogó, jól áttekinthető képet adjanak a biztonsági helyzetről. A szakértők betekintést nyújtottak az **automatizált priorizálásba és javítási folyamatokba**, különös tekintettel a konténeres, valamint a szerver nélküli architektúrák kihívásaira. Bemutatták, hogyan segíthet a sebezhetőségek kontextusba helyezése (pl.: a szoftverellátási lánc vagy futásidejű környezetek alapján) abban, hogy a szervezetek a legkritikusabb kockázatokra összpontosíthassák erőforrásaikat.

Vulnerability Poker: Real or AI Fake Vulnerabilities?

(Madison Oliver—GitHub & Tobias Heldt—XOR.Tech)

Ez az interaktív előadás egyfajta workshopként működött, ahol a résztvevőknek az volt a feladata, hogy eldöntsék: egy adott sebezhetőségleírás valódi-e, vagy mesterséges intelligencia által generált. Az előadók célja az volt, hogy rávilágítsanak arra, **milyen nehézségeket jelent a sebezhetőségi adatok hitelességének ellenőrzése** a jelenlegi deepfake és AI-központú korszakban. Az előadás egyúttal rámutatott arra, mennyire fontos a forrásellenőrzés, illetve, hogy a PSIRT csapatoknak egyre kifinomultabb módszereket kell alkalmazniuk a dezinformációk kiszűrésére.

BBA-PLUSZ-3.1.2-24-2024-00003. sz. pályázat részeként

Don’t Forget the Little Guy: Vulnerability Management in Operational Technology

(Alex Assante—Network and Security Technologies & Kylie McClanahan—Bastazo)

Az előadás keretében bemutatásra kerültek az **IT és az OT területek közötti különbségek**, valamint az ezekből fakadó kihívások. Amíg az IT környezetben egy kiforrott folyamatról van szó, addig az OT területéről ez nem mondható el, így folyamatosan egyedi kihívások elé állítja az OT-ban dolgozó szakembereket. A két terület különbségének megértése kulcsfontosságú az OT környezetek biztonságossá tételéhez, amelyek egyre szorosabb kapcsolatban állnak, továbbá egyre inkább függenek egymástól az informatikai rendszerekkel. Az előadás során egy **valós amerikai elektromos közmű szolgáltatónál feltárt sérülékenység kezelését prezentálták**, mely kitért az aktuális, a területre jellemző szabályozási követelményekre, a szükséges adatigényekre, valamint az OT környezetek jövőbeni egyedi kihívásaira.

Towards a Vulnerability Reporting Specification

(Marta Rybczynska—Eclipse Foundation)

Az Európai Unió kiberbiztonsági stratégiájaként 2024-ben elfogadott és bevezetett **CRA (Cyber Resilience Act) új szabványt írt elő a sebezhetőségi jelentési folyamatok tekintetében**. Az Európai Unió egyik legnagyobb, nyílt forrású termékekkel kapcsolatos „best practice” szabályokat kidolgozó vállalataként, továbbá a francia Open Regulatory Compliance csoport tagjaként, az előadó a törvény követelményeinek hatására egy olyan új minimális sebezhetőségi jelentési szabályzatot dolgozott ki és mutatott be részletesen, amely állítása szerint minden nyílt forráskódú projektre vonatkozhatna, illetve bárki számára ingyenesen, valamint nyílt forráskódú licenc alatt már jelenleg is szabadon elérhető.

BBA-PLUSZ-3.1.2-24-2024-00003. sz. pályázat részeként

Vulnerability Data Analysis with Google Sheets and Apps Script for Fun and Profit

(Andrew Pollock—Google, Open Source Security Team)

Andrew Pollock bemutatta, hogyan lehet hatékonyan elemezni sérülékenységi adatokat – például CVE-azonosítókat a Google Táblázatok és az Apps Script segítségével. Szemléltetésre került miként lehet gyorsan, vizuálisan, illetve rugalmasan kezelni a sebezhetőségi információkat anélkül, hogy bonyolult vagy drága eszközökre lenne szükség. Az előadás központi eleme az **ImportJSON nevű előre elkészített Apps Script könyvtár** volt, amely lehetővé teszi JSON alapú REST API-k lekérdezését közvetlenül a táblázatból, mintha beépített függvény lenne. Az előadó bemutatta, hogyan lehet sablont készíteni egy Google Sheet-ben, így az Apps Script integrálása csak egy egyszeri lépés, és a későbbi használat már gördülékenyen megy. Az előadás során gyakorlati példákon át került demonstrálásra, hogyan kérdezhetők le adatok a különböző forrásokból – mint a CVE List (MITRE), az NVD (National Vulnerability Database), az OSV.dev (Google), vagy a GitHub Advisory Database –, valamint ezek miképpen jeleníthetők meg a táblázatban például a CVE kiadójával, leírásával, súlyosságával vagy érintett termékeivel együtt. Az előadó hasznos technikákat is bemutatott, például a TEXTJOIN, FILTER, UNIQUE, vagy TRANSPOSE függvények használatát, valamint tippeket adott a Named Range-ek alkalmazására és a fölösleges újraszámítások elkerülésére.

Product Security Incident Response at a Fortune 500 SaaS

(Garrett McNamara—ServiceNow)

Az előadás során ismertetésre került, hogy az Amerikai Egyesült Államok 500 legnagyobb vállalata tekintetében a **termékbiztonsági incidensek és sebezehetőségek kezelését** miképpen végzi a ServiceNow vállalat, továbbá ez SaaS-technológiai környezetben milyen kihívásokkal, valamint lehetőségekkel jár. A kockázatalapú gyors döntéshozatalt az expozíció nagyarányú mérésének és a kiaknázási tevékenység nyomon követésének képessége teszi ezt lehetővé az előadó tájékoztatása alapján. Az incidensekhez köthető kihívások közé tartozik a könnyen felfedezhető és gyakran a publikus internethez kapcsolódó támadási felületek nagy száma.

BBA-PLUSZ-3.1.2-24-2024-00003. sz. pályázat részeként

Scaling Vulnerability Management: A Scale-Up's Journey to Enterprise-Grade Security

(Niels Hofmans— Intigriti)

Az előadó arról osztotta meg a tapasztalatait, hogyan lehet hatékonyan skálázni a sebezhetőségkezelést egy gyorsan növekvő vállalat biztonsági igényeihez igazítva. A cégeknél gyakran szűkösek az erőforrások, miközben egyre szigorúbb biztonsági követelményeknek kell megfelelniük, így különösen fontos az átgondolt, automatizált megközelítés. Niels bemutatta, hogyan építettek ki egy **saját fejlesztésű sebezhetőségkezelési folyamatot** Go nyelven, amely közvetlenül integrálódik a SIEM rendszerükbe és képes különféle sérülékenységi adatforrásokat összevonni. A folyamat kulcsa a sebezhetőségi metaadatok kibővítése, amely lehetővé teszi a valóban releváns problémák priorizálását. Az előadás során gyakorlati példákat mutattak be arra, hogyan támaszkodnak a strukturált adatokra a döntéshozatal során, hogyan használnak self-service portálokat és SIEM dashboardokat az érintettek tájékoztatására, és hogyan követik nyomon a sérülékenységek trendjeit. Az előadás hasznos iránymutatásokat nyújtott azoknak a szervezeteknek, amelyek hatékonyabbá szeretnék tenni a sebezhetőségkezelési folyamataikat és a meglévő erőforrásaikból a legtöbbet szeretnék kihozni.

Adversarial Intelligence: Redefining Application Security Through the Eyes of an Attacker

(Mahesh Babu & Roy Talyosef— Kodem)

Ez az előadás az alkalmazásbiztonság új megközelítését mutatta be, amely az alkalmazásokat a támadók szemszögéből vizsgálja. A prezentáció során a szakértők bemutatták, hogyan lehet az **alacsony és közepes kockázatú sebezhetőségeket kombinálva sikeres támadásokat végrehajtani**. A résztvevők megismerkedhettek azokkal az eszközökkel és technikákkal, amelyek segítenek az ilyen típusú fenyegetések felismerésében és mérséklésében, különösen a felhőalapú és elosztott rendszerekben.

BBA-PLUSZ-3.1.2-24-2024-00003. sz. pályázat részeként

Breaking the Bot: GenAI Web App Attack Surface & Exploitation

(Ken Smith—Praetorian)

A workshop célja az volt, hogy gyakorlati tudást adjon biztonsági szakemberek, penetrációs tesztelők és webfejlesztők számára a generatív mesterséges intelligenciára (GenAI) épülő alkalmazások sebezhetőségeinek felismerésében, kihasználásában és javításában. Ahogy a vállalatok egyre gyorsabban integrálják a nagyméretű nyelvi modelleket (LLM-eket), illetve más GenAI technológiákat rendszereikbe, **új támadási felületek és sebezhetőségi típusok jelennek meg**, amelyeket a hagyományos biztonsági tesztelési módszerek nem feltétlenül fednek le megfelelően. A résztvevők először megismerkedtek a GenAI alkalmazások alapvető architektúrájával, különös figyelmet fordítva az olyan elemekre, mint a rendszerpromptok és a modell API-k, amelyek alapvetően megkülönböztetik ezeket a hagyományos webes megoldásoktól. Ezt követően egy tipikus GenAI-alapú webalkalmazás fenyegetésmodelljének kidolgozásán keresztül lett szemléltetve a **Threat Modeling folyamata**. A gyakorlati szekció az OWASP Top 10 – LLM-alkalmazásokra vonatkozó – listájára épült, kiemelve a prompt injectiont és jailbreaking technikákat, hibás kimenetkezelést, valamint rendszerprompt szivárgást. A résztvevők egy szándékosan sebezhető GenAI-alkalmazáson végezhettek el különféle támadásokat: prompt injection technikák kivitelezése, érzékeny adatok kiszivárogtatása modellmanipulációval, XSS sérülékenységek kihasználása hibás kimenetkezelésen keresztül. Ezen felül említésre került több olyan sérülékeny nyelvi modell is, amelyekben eltérő szinteken át lehetett gyakorolni ezen technikákat (pl.: a Lakera AI cég által létrehozott Gandalf AI Rendszer).

BBA-PLUSZ-3.1.2-24-2024-00003. sz. pályázat részeként

OpenEoX - Unified Machine-Readable Approach to Software and Hardware Product Lifecycle Data Representation

(Przemysław Roguski— Red Hat Poland)

Az előadás bemutatta a Secure Software Development Lifecycle (SDLC) kihívásait, és azok megoldásainak lehetőségeit. A különböző biztonsági tevékenységek, például a sebezhetőségkezelés, a licenceknek való megfelelés vagy a support ellenőrzése érdekében a szoftver- és hardvergyártóknak különböző metaadatokra (pl.: CSAF, VEX vagy SBOM) van szükségük. Szinte minden gyártó közzéteszi a termékei életciklusára vonatkozó adatmeghatározásokat, de nincs szabványosítás a formátum és a szállítási módszer körül. A prezentáció rámutatott a pontos termékazonosítás, a termékverzió, a támogatási modell, illetve a céldátumok technikai és nem technikai szempontjainak fontosságára, amelyek jelentős segítséget nyújthatnak az ügyfeleknek a különböző életciklus- vagy támogatási, szabályozási követelmények, valamint biztonsági vonatkozások tekintetében.

A konferencia előadásainak felvételei hamarosan elérhetők lesznek a FIRST hivatalos YouTube csatornáján.

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