NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2025. 27. hét

HÍREK

- Sérülékeny Bluetooth fejhallgatók:
  Hallgatózás és eszközátvétel egy karnyújtásnyira
- Globális NFC-támadáshullám: Az ESET figyelmeztet az érintésmentes fizetés új veszélyeire
- Súlyos biztonsági rések több száz Brother nyomtatóban
- Kritikus sebezhetőség a Forminator WordPress bővítményben
- Szintet lépett az adathalászat: PDF-ekkel támadnak a márkát utánzó kampányok

STATISZTIKAI ADATOK

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

BESZÁMOLÓ

- RSA Conference
  Amerikai Egyesült Államok, San Francisco

KONTAKT

edt@nki.gov.hu

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D

NEWS

IT biztonsági
HÍREK

Sérülékeny Bluetooth fejhallgatók: Hallgatózás és eszközátvétel egy karnyújtásnyira
(gbhackers.com)

A vezeték nélküli hangtechnológia térnyerése új kényelmi szintet hozott a felhasználók számára, ugyanakkor komoly biztonsági kockázatokkal is járhat, derült ki egy nemrégiben napvilágra került biztonsági elemzésből, amelyet a német ERNW kiberbiztonsági cég mutatott be a TROOPERS konferencián. **Bővebben...**

Globális NFC-támadáshullám: Az ESET figyelmeztet az érintésmentes fizetés új veszélyeire
(gbhackers.com)

Az ESET kiberbiztonsági kutatói új, aggasztó támadási módszert azonosítottak, amely a Near Field Communication (NFC) technológiát használja ki, eredetileg cseh banki ügyfeleket célozva, ám mára globális méreteket öltött. **Bővebben...**

Súlyos biztonsági rések több száz Brother nyomtatóban
(theverge.com)

A legkritikusabb felfedezett hiba a CVE-2024-51978 azonosítót, és **9.8-as CVSS pontszámával** a legmagasabb szintű, „kritikus” minősítést kapta. **Bővebben...**

Szintet lépett az adathalászat: PDF-ekkel támadnak a márkát utánzó kampányok
(gbhackers.com)

A Cisco Talos biztonsági kutatócsapat **riasztó fejleményre** hívta fel a figyelmet: egyre több, **kifinomult adathalász kampány** használ **PDF mellékleteket**, hogy ismert márkákat – például a **Microsoftot, a DocuSign-t vagy a Dropboxot** – utánozva csapdába csalják az áldozatokat. **Bővebben...**

Kritikus sebezhetőség a Forminator WordPress bővítményben
(gbhackers.com)

A sebezhetőség – amely a **CVE-2025-6463** azonosítót kapta – több mint **600 000 aktív weboldalt** érint világszerte, és lehetővé teszi, hogy **hitelesítés n élküli támadók tetszőleges fájlokat töröljenek** a szerveren. A hibát **8.8-as (magas) CVSS pontszámmal** minősítették, és a potenciális következmények között szerepel a teljes weboldal átvétele és távoli kódfuttatás lehetősége is.
Bővebben...

További hírekért, látogasson el **weboldalunkra**!

Statisztikai Adatok

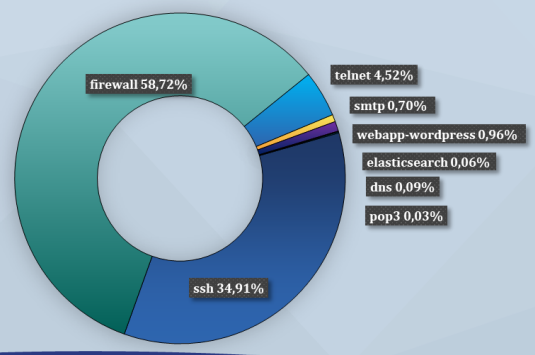
2025.06.27.-2025.07.03.

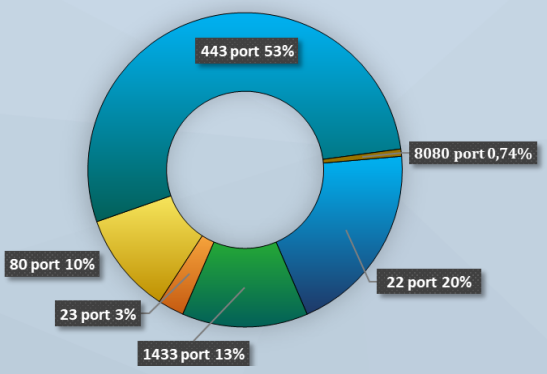
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: alacsony

Incidensek eloszlása típus és kockázati besorolás szerint

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





További érdekességekért, látogasson el **weboldalunkra**!

RSA Conference

2025. április 28. – május 1.

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.

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

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 28.— május 1. között San Franciscoban megrendezésre kerülő RSA konferencián. A világ egyik legjelentősebb kiberbiztonsági eseménye idén több mint **44.000** résztvevőt vonzott a San Francisco-i Moscone Centerbe, ezzel ismét megerősítve globális vezető szerepét a szakmai konferenciák között. Az esemény során **több mint 730 előadó** tartott prezentációt, **450-nél is több szekcióban**, valamint **650 kiállító** mutatta be legújabb technológiai fejlesztéseit és termékeit az expó területén.

Főbb témák és tanulságok:

- **Mesterséges intelligencia és gépi tanulás a kiberbiztonságban** – kiemelt szerepet kaptak a támadások prediktív felismerését és megelőzését célzó fejlesztések.
- **Zero Trust architektúra** – továbbra is középpontban maradt, gyakorlati megközelítéssel és konkrét vállalati példákkal kiegészítve.
- **Supply chain security** – a beszállítói láncok védelme kiemelt figyelmet kapott, különösen a harmadik felek által jelentett kockázatok csökkentésének lehetőségeire fókuszálva.
- **Szabályozási környezet és megfelelés** – több szekció is foglalkozott a legújabb szabályozásokkal, például a NIS2 irányelvvel és az amerikai szövetségi előírásokkal, különös hangsúlyt fektetve azok gyakorlati alkalmazására.

Kiknek ajánlott a beszámoló megismerése?

- Minden kiberbiztonsági szakember számára
- Sérülékenységvizsgálattal foglalkozó specialisták számára
- Kiberfenyegetés-kutatóknak és elemzőknek
- Biztonsági mérnököknek és fejlesztőknek

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

Pig Butchering and the Threat of Transnational Organized Crime

(Erin West)

Az előadáson bemutatott online csalási módszert magyarul disznóvágásra fordíthatnánk, azonban véleményem szerint inkább a **„kivéreztetés”** felelne meg jobban névként, hiszen a csalás végeredményeként **az áldozat minden pénzét elveszti vagy akár adósságot is felhalmoz**. A hazánkban is ismert Nigériai herceg, „unokázós” csalás, illetve a kisebb összegű SMS csalások, mint például a csomag utáni vám, vagy postaköltség megfizetésével ellentétben itt **nem egy egyszeri fix összeg**, hanem **az áldozat teljes vagyonának megszerzése** a cél.

A módszer az alábbi lépésekből áll:

1. A csalók rendszerint álprofilokat használnak, és kapcsolatfelvétel céljából **közösségi médián**, **üzenetküldő appokon** (pl. **WhatsApp**, Telegram) vagy **társkereső oldalakon** keresik meg az áldozatokat. Itt jellemzően egy dekoratív, jómódú nő vagy férfi (áldozat preferenciájának megfelelő) látszatát keltik.
2. Hosszú időn keresztül **bizalmat építenek ki**, gyakran romantikus vagy baráti kapcsolat látszatát keltve.
3. Az áldozatot **rábeszélik** arra, hogy **fektessen be kriptovalutába**, rendszerint egy **hamis vagy manipulált befektetési platformon** keresztül, amit az elkövetők üzemeltettnek. Az áldozat által befizetett összeget látszólag jóváírják az oldalon az egyenlegéhez, azonban ez a kriptovaluta egyenesen a csalók tárcájába kerül. (Jellemzően USDT-Tether nevű kriptovalultát váltatnak, amelynek árfolyam megközelítőleg az amerikai dollárhoz kötött)
4. A kezdeti befektetések **gyakran valódi hozamot mutatnak**, ami **fokozza az áldozat bizalmát**. A saját álbefektetési oldalukon látszólag megnövelik az áldozat befektetésének értékét, így színlelve a rendkívül magas hozamú befektetés működőképességét.
5. A csalók ekkor arra ösztönzik az áldozatot, hogy **még több pénzt fektessen be**.

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

6. Miután jelentős összeget invesztált be az áldozat, és a látszólag magas álhozamokkal még meg is emelték az álbefektetési oldalon látszó összeget, azt javasolják, hogy **ideje kivenni a befektetést**, mert „úgy értesültek ismerősüktől”, hogy jelentősen esni fog a befektés értéke.
7. Ezt követően felhívják az áldozat figyelmét a kifizetésnél, hogy a magas hozamra **adót kellene fizetni** és csak annak megfizetése után hajthatják végre kifizetés tranzakcióját.
8. Miután az áldozat a jellemzően rendkívül magas hozamra egy **jelentősebb adóösszeget is befizet** a csalók számlájára, **végleg megszakítják vele a kapcsolatot**.

A csalás neve arra utal, hogy az áldozatot úgy hizlalják, mint egy sertést, mielőtt levágják, vagyis kifosztják. Az áldozatok az elképzelésekkel ellentétben **nem csak idős hölgyek**, hanem **megegyező arányban nők és férfiak, ugyan úgy 50 év alatti és feletti korral**. A módszert gyakran jól szervezett bűnbandák alkalmazzák, különösen Délkelet-Ázsiából. A prezentációt tartó hölgy egy nonprofit céget hozott létre az áldozatok megsegítésére. Elmondta, hogy nem régiben járt **egy telepen** Kambodzsában, ahonnan ilyen csalásokat hajtottak végre szervezetten. Tapasztalatai szerint, akik közvetlenül elkövetik a csalások kommunikációs részét maguk is áldozatok. Jellemzően **mélyszegénységben élő embereknek ígérnek helyi viszonylatban jólfizető IT munkát**, azonban a felvételüket követőn **elveszik az irataikat és fegyveresen őrzött telepekre szállítják őket**, ahol embertelen körülmények között kell előre megírt forgatókönyv szerint végrehajtaniuk a csalásokat, akár napi 16 órában. Ezek mögött a csalások és emberrablások mögött **jól szervezett ázsiai, kínai bűnbandák állnak**, akik nem ritkán a helyi rendvédelmi szervekkel is kapcsolatban állnak, hogy szabadon gyakorolhassák ezen cselekedeteiket.

Összességében elmondható, hogy az ilyen fajta csalások elleni védekezés legegyszerűbb és leghatékonyabb módja az **állampolgárok körében végzett tudatosítás**.

Az előadás ide kattintva megtekinthető.

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

Show Me Your ID(E)!: How APTs Abuse IDEs

(Tom Fakterman, Daniel Frank)

Az APT csoportok (APT – Advanced Persistent Threat) az elmúlt években egyre gyakrabban célozták meg a **szoftverfejlesztői környezeteket**, mint alternatív bejutási pontokat a vállalati rendszerekbe. A „Show Me Your ID(E)!" című előadás a fejlesztői eszköztár egyik kevéssé védett, mégis kritikus komponensére, az **integrált fejlesztői környezetekre** (IDE – Integrated Development Environment) koncentrált, és bemutatta, hogyan használják ki ezeket a támadók észrevétlen hozzáférés és adatlopás céljából.

Az előadás első részében ismertetésre került, hogy **miért vonzók az IDE-k** az APT-k számára. A fejlesztők rendszerint széleskörű jogosultságokkal rendelkeznek, gyakran férnek hozzá érzékeny forráskódokhoz és infrastruktúrához. Az olyan népszerű környezetek, mint a Visual Studio vagy a VS Code, különféle bővítményeken, **kódcsomagokon és távoli eléréseken keresztül manipulálhatók**, akár anélkül is, hogy a fejlesztő észlelné a visszaélést.

Konkrét esettanulmányok bemutatásával – például a **Koi Stealer** és **RustDoor** kampányok – világítottak rá arra, hogyan képesek a támadók megtévesztő álláshirdetések vagy hamis GitHub-projektek segítségével rosszindulatú kódot futtatni a fejlesztők számítógépén. Ezek a támadások gyakran olyan projekteken keresztül zajlanak, amelyek **csomagolt formában tartalmazzák a kártékony kódot**, például **Python setup.py** fájlokban, melyek észrevétlenül letöltik és végrehajtják a kártékony állományt.

A prezentáció továbbá kitért a **low-code fejlesztői platformok** (pl. Microsoft Power Automate) sebezhetőségeire is, ahol kártékony automatizálási folyamatok épülhetnek be legitim üzleti folyamatba. Ezek a platformok különösen veszélyesek, mivel **nem igényelnek kártevő telepítést**, hanem a jogos felhasználói műveleteket kihasználva végzik az adatszerzést vagy a jogosultságnövelést..

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

További példák ismert **VS Code-bővítmények**, **Python-csomagok**, illetve nyílt forráskódú tárolók (pl. GitHub) manipulálásán keresztül kerültek bemutatásra. Az előadás végén egy élő demonstráció is tartottak, amelyben bemutatták, **hogyan lehet visszaélni a VS Code CLI** (Command Line Interface) **és távoli „Dev Tunnel" funkcióival** az észrevétlen hálózati hozzáférés érdekében.

Az előadás **nemcsak a technikai támadási módszereket** mutatta be, hanem **gyakorlati védelmi javaslatokat is megfogalmazott** a kódellenőrzés, a megbízhatósági lánc felülvizsgálatára, a naplózás és riasztás bekapcsolására, valamint az alkalmazottak biztonságtudatosságának növelésére.

Konklúzióként elmondható, hogy a fejlesztői környezetek védelme **kritikus tényezővé vált** az APT-kel szembeni küzdelemben, és a szervezeteknek proaktívan kell védekezniük ezen új típusú fenyegetésekkel szemben.

Az előadás ide kattintva megtekinthető.

Adventures in the Underland: Uncommon Hacker's Persistence Methods

(Paula Januszkiewicz)

A bemutató technikai mélységben ismertette azokat a módszereket, amelyekkel **támadók hosszú távon képesek fenntartani jelenlétüket** kompromittált rendszerekben.

A „perzisztencia" a támadási lánc azon szakasza, amely lehetővé teszi, hogy a támadó rendszeres újraindítás, frissítés vagy akár részleges fertőzés-eltávolítás után is **megőrizze hozzáférését a rendszerhez**. A hagyományos megoldások ellen védelmi technikák már széles körben alkalmazottak, azonban a prezentáció olyan **kevésbé ismert, ritkán dokumentált eljárásokat mutatott be**, amelyek nem tartoznak a szokásos észlelési körbe.

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

A bemutatott technikák között szerepeltek „**fileless persistence**” módszerek, amelyek során a támadó nem tárol fájlokat a lemezen, hanem például **PowerShell**, **WMI** vagy más natív eszköz segítségével hajt végre műveleteket kizárólag memóriában. Ez jelentősen megnehezíti a hagyományos antivírus megoldások számára a támadás felismerését. A hatékony detektáláshoz elengedhetetlen a viselkedéselemzésen alapuló figyelőrendszerek, valamint részletes naplózási (logging) konfigurációk alkalmazása.

Az előadás rámutatott, hogy az eseménynaplók – megfelelően beállítva – **képesek felfedni a gyanús tevékenységeket**, azonban a nyers adatok értelmezése jelentős elemzői kompetenciát igényel. A prezentációban szimulált támadási forgatókönyvek kerültek bemutatásra, amelyek során élő példák szemléltették, miként történik egy rejtett hozzáférés kiépítése és megtartása. Az elemzések **részletesen bemutatták a támadási pontokat**, a **kompromittált komponenseket** és a **védekezéshez javasolt eljárásokat**.

A bemutatott tartalom alapján megállapítható, hogy a korszerű támadások jelentős része **már nem kizárólag a hozzáférésszerzésre összpontosít**, hanem annak **hosszú távú fenntartására**. Ennek megfelelően a védekezés is túllép a peremvédelmi megoldásokon, és egyre inkább fókuszál a **belső viselkedési anomáliák detektálására**, a **rendszerkonfigurációk folyamatos auditjára** és a **támadási minták korai felismerésére**. Az ismertetett módszerek ismerete elősegíti az aktív fenyegetések korai azonosítását és a károk minimalizálását.

Az előadás ide kattintva megtekinthető.

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

Every Move You Make, Every App You Play I'll Be Watching You

(Mattia Epifani)

Az előadás célja annak bemutatása volt, hogy a **modern okostelefonok hogyan gyűjtenek széleskörű adatokat** a felhasználók napi szokásairól, viselkedéséről, és hogyan alkalmazhatóak ezek az adatok a felhasználói tevékenységek rekonstruálására.

A mai okostelefonok számos olyan adatot gyűjtenek, amelyek nemcsak az alkalmazások működésére vonatkoznak, hanem a felhasználók napi aktivitásaira is. Az okostelefonok például **hely-adatokat**, **alkalmazás-használati időket**, **hívásokat**, **üzeneteket és egyéb interakciókat** rögzítenek, melyek az egyén viselkedésének és szokásainak feltérképezésére alkalmasak. Az előadásban kiemelésre került, hogy a felhasználók **gyakran nem is tudnak arról, hogy az okostelefonjaik ilyen mértékben rögzítenek adatokat.** Az okostelefonokban tárolt információk – például helyadatok és alkalmazás-használati időpontok – segíthetnek rekonstruálni az egyén napi rutinját és tevékenységeit.

Az előadó ismertette, hogyan alkalmazható a „**digital forensics**” eszköztára a mobiltelefonokon található adatok, például **GPS-naplók és alkalmazás-használati adatok elemzésére**. A helyadatok például részletes információkat adhatnak arról, hogy a felhasználó milyen helyeken járt, mikor és mennyi ideig tartózkodott ott, míg az alkalmazás-használati adatok az egyes programok használatának gyakoriságát és időpontjait rögzítik.

Ezen adatok segítségével a szakemberek **képesek rekonstruálni egy személy napi tevékenységeit**, például az adott személy által látogatott helyszíneket, az alkalmazott eszközöket és az ezekhez kapcsolódó szokásokat. Ez a fajta adatgyűjtés különösen **hasznos lehet bűnügyi nyomozásokban**, ahol az egyes események időpontja és helyszíne fontos lehet.

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

Bár ezek az adatok **hasznos eszközként szolgálhatnak a nyomozásokban**, az előadás hangsúlyozza, hogy az adatvédelmi és etikai kérdések is alapvető fontosságúak. A mobiltelefonok által gyűjtött adatok érzékenyek, és a helytelen kezelésük jogi és etikai problémákhoz vezethet. Az előadásban szó volt az **adatvédelmi törvények**, valamint az **egyéni jogok védelmének fontosságáról** a digitális adatok elemzése során. A szakemberek számára alapvető, hogy tisztában legyenek a törvényi előírásokkal, és az adatok felhasználásakor mindig tartsák szem előtt a felhasználók jogait is.

Az előadás ide kattintva megtekinthető.

Conversations with a GenAI-Powered Virtual Kidnapper

(Perry Carpenter)

A generatív mesterséges intelligencia (GenAI) alkalmazása új dimenziót nyit a csalások, megtévesztések és szociális manipulációs támadások terén. A 2025-ös RSA konferencia egyik kiemelt előadása, „**Conversations with a GenAI-Powered Virtual Kidnapper**”, demonstratív módon mutatta be, hogy a jelenlegi technológiai környezetben a deepfake és LLM-alapú (nagy nyelvi modell) rendszerek hogyan képesek **valós időben szimulált emberrablást** vagy **más sürgető, érzelmi reakciót kiváltó helyzeteket előidézni.**

A prezentáció alapján világossá vált, hogy a mesterséges intelligenciával támogatott valós idejű csalások **képesek megtéveszteni** még a legóvatosabb felhasználókat is. A **nyelvi modellek** és **hangszintetizátorok** kombinációja révén a támadók képesek valós személyek hangját meggyőzően utánozni, és valós időben kapcsolatba lépni az áldozattal például telefonon keresztül. E technológia érzelmi manipulációval párosítva **olyan krízishelyzeteket szimulál, amelyek komoly pszichológiai nyomást gyakorolnak az áldozatokra**.

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

Különösen aggasztó az úgynevezett „**adversarial prompting**” jelensége, amely során a támadók képesek a nyelvi modellek működését oly módon befolyásolni, hogy azok **etikátlan**, **veszélyes** vagy **félrevezető válaszokat generáljanak**. Ez a technika **nemcsak a támadások hatékonyságát növeli**, hanem **megnehezíti az észlelésüket is**, különösen automatizált rendszerek esetén. Mindezekhez hozzájárul, hogy a szükséges technológiai elemek – nyelvi modellek, szintetikus hanggenerátorok, felhőalapú kommunikációs API-k – széles körben és olcsón elérhetők. Ez lehetővé teszi, hogy **alacsony erőforrásigényű**, de rendkívül **hatékony támadásokkal akár tömeges célzást** hajtsanak végre.

Rövid távon ezek a támadások **bizalmi válsághoz vezethetnek** a lakosság és az állami intézmények között. Az érintett szervek számára sürgető szükség van reagálóképes protokollok kialakítására és az alkalmazottak célzott képzésére. A lakosságban **pánikreakciók alakulhatnak ki**, ha nem tudják megkülönböztetni a valós fenyegetést a szintetikusan generáltaktól.

Hosszú távon a mesterséges intelligencia alapú csalások **strukturális biztonsági kockázatot is jelentenek**. A technológia felhasználható lehet politikai destabilizációra, társadalmi nyugtalanság gerjesztésére, vagy akár kritikus infrastruktúrák megtévesztésére is. A kiberhadviselés új formája alakulhat ki, amelyet nehéz detektálni, és amely ellen jelenleg **nem áll rendelkezésre megfelelő védelmi mechanizmus**. Mindez újfajta jogszabályi és szabályozási környezet kialakítását teszi szükségessé.

A nemzetbiztonsági szolgálatoknak ki kell alakítaniuk a **mesterséges intelligencia-alapú fenyegetések korai észlelését biztosító monitoringrendszereket**, és figyelemmel kell kísérniük az MI-felhasználást pszichológiai műveletek és dezinformációs kampányok során. A kiberbiztonsági szerveknek elengedhetetlen a **szintetikus médiatartalmak felismerésére alkalmas technológiák fejlesztése**, illetve a **nyilvánosság és a szakemberek képzése**.

A bűnüldöző hatóságoknak **ki kell bővíteniük az eszköztárukat**, beleértve a mesterséges hang- és videómanipulációk kriminalisztikai vizsgálatát, valamint a digitális bizonyítékok új típusainak kezelését. Emellett ajánlott **etikai keretrendszerek kidolgozása** is az állami szimulációs tréningekre, különös tekintettel az érzékeny társadalmi témákra.

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

Az előadásban bemutatott „**FAIK**" modell – amely a „**Freeze & Feel**", „**Analyze**", „**Investigate**" és „**Know**" lépéseket tartalmazza – jól alkalmazható a lakosság és a köztisztviselők tudatosságának növelésére. Az MI-vel támogatott támadásokra adott válasz egyik kulcsa a **kritikus gondolkodás** és a **források hitelességének folyamatos ellenőrzése** lesz.

Összefoglalva: a mesterséges intelligencia térnyerése nem csupán lehetőséget, hanem **komoly biztonsági kihívást is jelent**. A jelenlegi intézményi és szabályozási rendszerek nem tudják megfelelően kezelni az e technológiából fakadó kockázatokat. Haladéktalan, integrált, több szervet átfogó stratégiai fellépésre van szükség a mesterséges intelligencia által generált fenyegetések kezelése érdekében.

Az előadás ide kattintva megtekinthető.

From Leak to Breach: How Hackers Use AI to Exploit Stolen Source Code

(Sherri Davidoff, Matt Durrin)

Mesterséges Intelligencia Alkalmazása Forráskód Alapú Kibertámadásokban

Az RSA 2025 konferencia egyik kiemelt előadása, „**From Leak to Breach: How Hackers Use AI to Exploit Stolen Source Code**" rámutatott arra, **hogyan változtatja meg alapjaiban a kiberbiztonsági fenyegetéseket a mesterséges intelligencia (MI) alkalmazása**. A prezentációban bemutatott példák révén világossá vált, hogy a forráskód szivárgása nem csupán vállalati probléma, hanem rendszerszintű nemzetbiztonsági kockázattá válhat, különösen akkor, ha az MI-t a támadók kezébe adjuk.

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

A hagyományos védelemi rendszerek és sebezhetőségi vizsgálatok eddig manuális vagy félig automatizált módszereken alapultak. Azonban az előadás során demonstrált eszközök – például a WormGPT – **képesek automatizált módon elemezni** nagy mennyiségű forráskódot, és perceken belül azonosítani kritikus sebezhetőségeket, beleértve a hardcoded jelszavakat, API tokeneket, vagy klasszikus sérülékenységeket, mint a SQL injection vagy remote code execution. Különösen aggasztó, hogy a támadók hozzáférnek olyan szoftvercsomagokhoz és komponensekhez, amelyeket a **kormányzati és kritikus infrastruktúrák is használnak** (pl. Springboot, Magento). Az MI nemcsak felismeri a sérülékenységeket, de képes az exploitok vázlatos kidolgozására is. Bár ezek a próbálkozások nem mindig működnek elsőre, a technológia fejlődésével ezek az eszközök **egyre pontosabbá és veszélyesebbé válnak**.

Az előadás rávilágított arra is, hogy a szoftverellátási lánc biztonsága nem csupán a fejlesztői csapatokon múlik, hanem az **egész ökoszisztémát érinti**. A prezentációban szereplő támadási szcenáriók alapján egyértelmű, hogy a támadók **képesek gyenge pontokat találni** akár nyílt forráskódú szoftverekben, akár szállítók által fenntartott rendszerekben. Az MI-eszközök segíthetnek a teljes folyamat automatizálásában: a sérülékenység felfedezésétől a kiaknázásig.

Rövid távon ez azt jelenti, hogy a támadások sebessége és hatékonysága **drámaian nőni fog**. A védelmi oldalon dolgozó szakembereknek új eszközökre és módszertanokra van szükségük: automatizált sérülékenység-keresésre, gépi tanulással támogatott forráskód-ellenőrzésre, valamint valós idejű forráskódszivárgás-érzékelésre. Hosszú távon a legnagyobb fenyegetést az jelenti, hogy az MI képes lehet **nulladik napi sérülékenységek gyors detektálására és kiaknázására**, megelőzve a hivatalos frissítések és figyelmeztetések megjelenését.

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

Az állami szervek számára ez stratégiai kihívást jelent. A nemzetbiztonsági szolgálatoknak fel kell mérniük, hogy mely kritikus informatikai rendszerek forráskódjai kerülhettek illetéktelen kezekbe, és hogy ez milyen következményekkel járhat. A kiberbiztonsági hatóságoknak olyan előrejelző rendszereket kell telepíteniük, amelyek **képesek az MI-vezérelt támadások korai jeleit detektálni**. A bűnüldöző szerveknek pedig **újfajta digitális bizonyítékként kell kezelniük** az MI által generált exploitokat, és megfelelő képzést kell biztosítani a személyzet részére ezen fenyegetések kezeléséhez.

Az előadás által sugallt legfontosabb üzenet, hogy az **MI nemcsak a védekezést erősítheti, hanem a támadókat is soha nem látott előnyhöz juttathatja**. A jövőbeni stratégiáknak ki kell terjedniük a szállítói lánc auditjára, a fejlesztői gyakorlatok megerősítésére, valamint arra, hogy minden új szoftverkomponenst MI-rezisztens módon fejlesszenek. Emellett kritikus fontosságú a védelmi oldalon dolgozók képzése az **MI-alapú fenyegetések felismerésére és kezelésére**.

Összegzésül: az MI-forradalom **új korszakot nyitott** a kiberfenyegetések világában. Az állami szerveknek most van lehetőségük arra, hogy **felkészülten reagáljanak**, mielőtt ezek a fenyegetések rendszerszintű károkat okoznának. Ez **integrált**, **proaktív** és **koordinált** védelmi stratégiát követel meg minden kormányzati szerv részéről.

Az előadás ide kattintva megtekinthető.

Creating Calm in the Storm

(Sydney Delp)

Sydney Delp a Target Corporation védelmi igazgatóság vezetője által a „**Creating Calm in the Storm**” címen tartott előadás célja, hogy bemutassa, hogyan lehet **hatékonyan reagálni a kibertámadásokra és a vészhelyzetekre**, amelyek a digitális világban egyre gyakoribbá válnak. Hangsúlyozza a proaktív tervezés és a rugalmasság fontosságát, mivel a kibertámadások kiszámíthatatlanok és változatosak. Gyakorlatilag egy mai korban hatékony incidensreagáló csoport kialakítására vonatkozóan **adott tanácsokat**.

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

Főbb pontok:

- **Csapatok és folyamatok értékelése**: Az első lépés a meglévő csapatok és folyamatok felmérése, hogy megfelelő tervet lehessen kidolgozni az EIM (Enterprise Information Management) funkció kiépítésére. Az előadó javasolja, hogy az értékelést követően azonnal kezdjék el a szükséges partnerek azonosítását, akik keresztfunkcionális támogatást nyújthatnak.
- **Eszkalációs definíciók kidolgozása**: A következő lépés a definíciók és az eszkalációs folyamatok megtervezése az események súlyossága szerint. Ezek a keretek segítenek azonosítani, hogy mely események igényelnek azonnali figyelmet, és hogyan kell azokat kezelni.
- **Javasolt időkeretek**:
  - **Első három hónap**: Az EIM funkció alapjainak megteremtése, kulcsfontosságú partnerek azonosítása.
  - **Hat hónap**: A tervek bemutatása a felső vezetésnek, kulcsfontosságú játékkönyvek és folyamatirányelvek beépítése, és egy gyakorlat megszervezése az elkészült tervek tesztelésére.
- **Rugalmasság a tervezésben**: az előadó hangsúlyozza, hogy nem lehet minden lehetséges kibertámadást előre megtervezni. Ezért fontos, hogy a keretrendszer rugalmas legyen, és képes legyen alkalmazkodni a váratlan helyzetekhez.
- **Támogató folyamatok**: A keretrendszernek tartalmaznia kell támogató folyamatokat, amelyek segítik a gyors és hatékony reagálást a kibertámadásokra. Fontos, hogy minden funkcióra több egységet kell kiképezni, amely nem csak a helyettesítést, hanem a kereszttámogatást is biztosítja. Ebben a folyamatban ma már elkerülhetetlen az AI használata.

Az előadás ide kattintva megtekinthető.

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

Symmetric Key Cryptography

(Seres András)

Az ELTE kutatójának "**Symmetric Key Cryptography**" című előadásának célja, hogy bemutassa a **szimmetrikus kulcsú titkosítás alapelveit**, **alkalmazási területeit** és a modern informatikai **biztonságban betöltött szerepét**, amely a quantum computing idejében felértékelődik.

A szimmetrikus titkosítás alapjai: A szimmetrikus kulcsú titkosítás lényege, hogy a **titkosító és visszafejtő folyamatokhoz ugyanazt a kulcsot használják**. Ez a megközelítés gyors és hatékony, különösen nagy mennyiségű adat esetén. A leggyakoribb algoritmusok közé tartozik az **AES** (Advanced Encryption Standard), **DES** (Data Encryption Standard) és **3DES** (Triple DES). A szimmetrikus titkosítást széles körben használják az iparban, például adatátvitel során, fájlok titkosítására és a biztonságos kommunikáció biztosítására. Az online banki szolgáltatások és e-kereskedelmi platformok is alkalmazzák ezt a technológiát, hogy megvédjék az érzékeny adatokat, mint például a hitelkártya-információkat. Az előnyök közé tartozik a gyors működés és a kevés számítási erőforrás igény. Ezen kívül a szimmetrikus titkosítás **egyszerűbb**, mint az aszimmetrikus megközelítés, mivel csak egy kulcsot kell kezelni. A hátrányok közé tartozik a kulcskezelés problémája; ha a kulcsot illetéktelenek megszerzik, az adatok biztonsága veszélybe kerül. Továbbá, a kulcsot mindkét félnek **biztonságosan kell megosztania**, ami kihívást jelenthet. A kulcskezelés a szimmetrikus titkosítás egyik legfontosabb aspektusa. Fontos, hogy a kulcsok biztonságban legyenek, és rendszeresen frissüljenek, hogy csökkentsék a sérülékenységeket. A kulcsok generálása, tárolása és megosztása során be kell tartani a legjobb gyakorlatokat, például a **kulcsok titkosítását és a biztonságos tárolást**.

A szimmetrikus titkosítás jövője a **kvantumszámítástechnika fejlődésével is összefonódik**. A kvantumszámítógépek képesek lehetnek a klasszikus titkosítási algoritmusok feltörésére, ezért új, kvantumrezisztens algoritmusok kifejlesztésére van szükség. A kutatók és a szakemberek folyamatosan dolgoznak a szimmetrikus titkosítási technológiák fejlesztésén, hogy azok megfeleljenek a jövő kihívásainak.

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

Az előadás során az osztályok szerepe a kriptográfiában került középpontba, különösen a kvadratikus osztályok és azok alkalmazásai kapcsán. Az osztálycsoportok alapját a **bináris kvadratikus formák képezik**, amelyek egy adott diszkriminánssal rendelkező formák halmazát alkotják, és Gauss óta ismert csoportstruktúrát mutatnak. Az osztálycsoportok tagjai általában (**a,b**) formában vannak megadva, és a Gauss által felfedezett csoportművelet révén összetartozó elemekből állnak. Ezek az osztálycsoportok nagyban hozzájárulnak a kriptográfiában alkalmazott **biztonságos hash függvények kialakításához**, mivel az általuk képzett csoportok rendje ismeretlen a nyilvánosság számára, ami növeli a biztonságot. Az előadás kitért arra is, hogy az osztálycsoportokat az algebrai tulajdonságok és a formák eloszlása jellemzi, és fontos szerepet töltenek be olyan kriptográfiai protokollokban, mint a **zero-knowledge proof** vagy a **verifiable delay functions**. Emellett bemutatták, hogy a modern alkalmazásokban a megbízható és biztonságos hash függvények kialakítása érdekében elengedhetetlen az algebrai alapokra épülő, illetve a **Wesolowski-féle kiterjesztett hash függvények** használata. Az osztálycsoportok így nemcsak a matematikai elmélet szempontjából fontosak, hanem központi szerepet játszanak a biztonságos kriptográfiai rendszerek fejlesztésében is.

A kutatás további részletei ide kattintva megtekinthetők.

Guardians of the Cyber Galaxy: Allies Against AI-Powered Cybercrime

(Sean Farrell)

Sean Farrell az INTERPOL kiberbűnözés elleni egység vezetője, Andrew Sczygielski az FBI kiberbűncselekmények felderítésére alakult igazgatóság vezetője Guardians **of the Cyber Galaxy: Allies Against AI-Powered Cybercrime** című panelbeszélgetésen az AI-alapú kiberbűnözés **növekvő fenyegetéseire és azok elleni küzdelem lehetőségeire** fókuszált. Hangsúlyozták, hogy a kiberbűnözők egyre kifinomultabb módszerekkel használják az AI-t támadásaik során. Az adatok szerint például az AI-t alkalmazó **spamkampányok költségei 95%-kal csökkentek** a bűnözők számára, míg az AI által generált tartalmak, mint például a deepfake videók és hangfelvételek, egyre gyakoribbak és veszélyesebbek.

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

Az előadás kitért arra, hogy az AI-támadások, mint például a **phishing**, a **botnetek**, az **automatikus sérülékenység kihasználás** és a **hamisított identitások**, mind növelik a bűncselekmények hatékonyságát és elrejtését. Ezért kiemelt hangsúlyt kapott a **köz- és magánszféra közötti együttműködés erősítése**, amely lehetővé teszi a fenyegetések gyorsabb felismerését és hatékonyabb kezelését. Fontos lépések közé tartozik a helyi FBI-irodákkal való kapcsolattartás, a meglévő biztonsági intézkedések felülvizsgálata, AI-alapú eszközök bevezetése, valamint a személyzet képzése.

Az előadás végén **konkrét lépéseket javasoltak** a szervezetek számára, például a kockázatelemzések elvégzése, stratégiai partnerségek kialakítása és a rendszeres képzések szervezése. Összességében az esemény rámutatott arra, hogy a hatékony védekezés érdekében elengedhetetlen a **folyamatos innováció** és az **együttműködés** a különböző szereplők között az AI-alapú kiberfenyegetések elleni harcban.

Protecting the Digital Community: A Scam Awareness Playbook

(Ayelet Biger-Levin)

Ayelet Biger-Levin, az előadásában a **digitális közösségek védelmének kritikus jelentőségére** hívta fel a figyelmet a "**Protecting the Digital Community: A Scam Awareness Playbook**" című prezentációjában. Az előadás központi témája a globálisan növekvő online csalások problémája volt, amelynek gazdasági hatásai 2023-ban elérték az 1,03 billió dollárt. Az előadó részletesen bemutatta, hogy a szervezett bűnözői csoportok **egyre fejlettebb technológiai eszközöket**, például mesterséges intelligencia által generált üzeneteket, deepfake videókat és szintetikus hangokat alkalmaznak, hogy megtévesszék az áldozatokat és manipulálják érzelmi állapotukat. A támadások során kiváltott érzelmek – jellemzően **félelem, sürgetettség vagy öröm** – jelentősen **gyengítik az áldozatok racionális döntéshozatali képességét**, ami meggondolatlan cselekvésekhez és jelentős anyagi károkhoz vezet.

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

Az elemzés rávilágított arra, hogy a csalások áldozatai legnagyobb arányban a **18–44 év közötti korcsoportból kerülnek ki**, ugyanakkor a legsúlyosabb pénzügyi veszteségeket az **idősebb, 55 év feletti korosztály szenvedi el**. Ez a jelenség hangsúlyozza a támadók kifinomult célzási stratégiáit, amelyek az idősebbek **pénzügyi eszközeire** fókuszálnak, míg a fiatalabbak esetében az **érzelmi manipuláció és a gyors reakciók előidézése** dominál. A támadási vektorok között kiemelt helyen szerepel az e-mail, az SMS, a közösségi média platformok és az azonnali üzenetküldő alkalmazások, ahol a támadók gyakran hivatalosnak tűnő üzenetekkel, hamis banki értesítésekkel vagy nyereményjátékokkal próbálnak bizalmat ébreszteni.

A statisztikai adatok szerint az áldozatok mindössze **4%-a képes visszaszerezni** a csalások során elvesztett pénzösszegeket, amely jól szemlélteti a jelenlegi védekezési mechanizmusok – különösen a pénzforgalmi rendszerek szintjén történő kontrollok – elégtelenségét. Emellett a csalások jelentős pszichológiai következményekkel is járnak: az **áldozatok 36%-a számolt be tartós lelki sérülésekről**, beleértve a szégyenérzetet, a depressziót, a szorongást és a másokba vetett bizalom elvesztését.

Az előadás hangsúlyozta, hogy a csalások elleni hatékony fellépés **legfontosabb eszköze az oktatás**, amely minden korosztály számára elengedhetetlen. Ayelet három kulcskoncepciót azonosított a tudatosságnövelő programok középpontjában: az **adatvédelem és a kiberbiztonság alapelveinek megértését és alkalmazását** (például erős jelszavak létrehozását, többfaktoros hitelesítés alkalmazását), az **online kapcsolatokkal szembeni kritikus attitűd kialakítását** (az online ismeretségek idegenek maradnak, még akkor is, ha hosszú ideje tart a kommunikáció), valamint az **irreálisan kedvező ajánlatokkal szembeni szkepticizmust**. A többfaktoros hitelesítés (**MFA**) bevezetése különösen kiemelt jelentőségű, mivel ez a technológia jelentősen csökkentheti a fiókfeltörések sikerességét, még jelszószivárgás esetén is.

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

Összegzésként Ayelet arra buzdította a hallgatóságot, hogy a prezentációban **elsajátított ismereteket aktívan alkalmazzák** saját közösségeikben: kezdjék el a csalásokkal kapcsolatos **tudatosság növelését** közvetlen környezetükben, a következő hetekben mutassanak empátiát és nyitottságot a téma iránt, a következő hónapokban pedig **rendszeresen frissítsék tudásukat** a csalási trendek alakulásáról. A digitális közösségek védelme **közös felelősség**, amely folyamatos odafigyelést, technológiai felkészültséget és társadalmi szolidaritást igényel.

Az előadás ide kattintva megtekinthető.

525,600 Assessments Later—Top Mobile App Risks since 2022

(Andrew Hoog)

A mobilalkalmazások napjainkra szinte minden személyes, üzleti és társadalmi tevékenységünk részévé váltak. 2023-ra világszerte **több mint 7,21 milliárd okostelefon volt** használatban, és az alkalmazás letöltések száma elérte a 255 milliárdot. Egy átlagos felhasználó 60–90 alkalmazást tart az eszközén.

Az előadás célja az volt, hogy átfogó képet adjon arról, milyen kockázatokat rejtenek magukban a mobilalkalmazások, és miért különösen nehéz ezeket a hibákat felfedezni.

Miért nehéz a mobilalkalmazások hibáinak felismerése?

Az előadás kiemelte, hogy a mobilplatformok számos korlátozást vezetnek be:

- **Platform korlátozások**: root-hozzáférés hiánya, sandboxing, korlátozott API- és biztonsági telemetria-hozzáférés.
- **Támadási felület**: alkalmazásokba épített böngészők, 18+ érzékelő (pl. GPS), valamint nagymértékű harmadik fél SDK-használat.
- **Fejlesztési környezet**: évente változó Android- és iOS-keretrendszerek, új nyelvek (Swift, Kotlin) korlátozott biztonsági eszköztámogatással.

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

Főbb kockázati területek

A 2022–2025 közötti több mint félmillió alkalmazásértékelés alapján az alábbi kockázati kategóriák rajzolódtak ki:

- **Adatvédelmi kockázatok**: érzékeny adatok helytelen kezelése.
- **Pénzügyi kockázatok**: hibák pénzügyi veszteségekhez vezethetnek.
- **Fraud**: csalási lehetőségek megjelenése.
- **Ellátási lánc problémák**: harmadik fél által biztosított SDK-k sérülékenységei.
- **Szabályozási megfelelés hiánya**: GDPR, CCPA és más előírások megsértése.
- **Márka- és hírnévkockázatok**.
- **Új technológiák által okozott veszélyek**.

Példák a valódi világból

Több gyakorlati példát is bemutattak, köztük:

- **My Security Account App**: hitelesítési hibát tártak fel (CISA-25-051-05).
- **SparkCat**: iOS-alkalmazásban maradt debug szimbólumokból visszafejthető volt a fejlesztők adata.
- **DeepSeek iOS**: titkosítás nélküli adatátvitel és gyenge kulcskezelés.
- **Pushwoosh SDK**: orosz hátterű, de amerikai cégnek álcázott szolgáltató, több mint 2,3 milliárd eszköz adatait gyűjtötte.
- **SourMint SDK**: távoli kódfuttatásra alkalmas backdoor egy SDK-ban.
- **Qardio Health iOS**: érzékeny adatok szivárgása CVE-2025-20615 azonosítóval.

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

Tipikus problémák a mobilalkalmazásoknál

A bemutatott statisztikák szerint az alkalmazások:

- **72%**-ban nem sztrippelt debug szimbólumokat tartalmaznak.
- **61%**-ban gyenge vagy elavult kriptográfiát alkalmaznak.
- **15%**-ban ismert sebezhetőségekkel rendelkező komponenseket használnak.
- **19%**-ban keménykódolt kriptográfiai kulcsokat tartalmaznak.
- **75%**-ban hiányoznak adatvédelmi célmegjelölések az App Store-ban.

Mit tehetnek a szervezetek?

A javasolt lépések a következők voltak:

- **Alkalmazáskészlet felmérése:** az összes használt vagy fejlesztett alkalmazás leltározása, majd kockázati profil szerinti kategorizálása.
- **Alkalmazások tesztelése:** az OWASP MASVS szabvány alapján kockázati szint szerinti biztonsági tesztek meghatározása, mobil-specifikus dinamikus tesztelési eszközökkel (pl. mobSF).
- **Folyamatos biztonsági tesztelés:** minden új alkalmazásverzió ellenőrzése, eredmények integrálása mobil EDR/MTD rendszerekbe, kockázatkezelési jelentésekbe.

Az előadó ismertette az export-intune-apps nevű egyszerű parancssori eszközt, amely lehetővé teszi a Microsoft Intune rendszerből származó alkalmazáskészlet gyors exportálását, valamint az adatok kiegészítését és elemzését különböző formátumokban.

Összefoglalva: a mobilalkalmazások biztonsági hibáinak feltárása összetett feladat, mivel a hagyományos, webalkalmazásokra szabott tesztelési módszerek nem fedik le megfelelően a mobil specifikus kockázatokat. Sem az Apple, sem a Google alkalmazásboltjai nem garantálnak alapos biztonsági ellenőrzést. Az előadás fő üzenete az volt, hogy a szervezeteknek saját hatáskörben, proaktív módon kell elvégezniük a mobilalkalmazások rendszeres biztonsági vizsgálatát és védelmét.

Az előadás ide kattintva megtekinthető.

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

10 Common Flaws in Incident Response Plans

(Alex Waintraub)

Alex Waintraub, a VMG Health kiberbiztonsági igazgatója előadásában az **incidenskezelési tervek fontosságát** és **leggyakrabb hibáit** ismertette. Az előadás kiindulópontja az volt, hogy a kiberbiztonsági incidensek elkerülhetetlenek, ezért a szervezeteknek muszáj előre felkészülniük rájuk. Az F-secure felmérése szerint 2023-ban mindössze a vállalatok 45%-ának volt IRP-je, ami lassú javulást mutat a 2019-es 33%-hoz képest, ami pedig az IBM felméréséből származó érték.

A CISA definíciója szerint az IRP:

- Meghatározza a szerepeket és a felelősségi köröket
- Iránymutatást ad a kulcsfontosságú tevékenységekhez
- Meghatározza a kulcsszereplőket
- Megfogalmazásra kerül benne a Kommunikációs stratégia
- Proaktív és stratégiai keretrendszerként funkcionál

Az előadó ezután **személyes véleményét mondta el** felsorolás formájában. Az első és leggyakrabb hiba az, hogy a **vállalatoknak egyáltalán nincs terve**. Fontos lenne azonosítaniuk és rangsorolniuk a legnagyobb kockázatokat, és aköré építeniük az incidenskezelési stratégiájukat.

A második leggyakrabb hiba az egyértelmű **szerepkörök és felelősségi körök meghatározásának hiánya**. Ez zavarodást okoz a kommunikációban, ezzel elvonja a csapat energiáját a valós probléma megoldásától.

A harmadik hiba az, hogy **a csapatok „silószerűen" csak a saját dolgukkal foglalkoznak**. Az előadó egy személyes történetet osztott meg ezzel kapcsolatban. A történetben kibertámadás érte a céget, ahol dolgozott. Az IT osztály csak a saját dolgával törődve a saját szabályzatuk alapján minél hamarabb törölte a fertőzött eszközök tárhelyeit, és minél hamarabb újra lábra állította a cég rendszereit. A kiberbiztonsági csapat viszont még várni szeretett volna, ugyanis meg akarták mutatni a biztosítónak

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

A negyedik hiba a **nem megfelelő kommunikációs stratégia**. Ez szorosan összekapcsolódik a második hibával. Fontos, hogy előre meghatározott módon történjen a kommunikáció, ugyanis a legrosszabb esetben a támadó élhet a támadás által kialakult káosz adta lehetőségekkel, és social engineering támadásként felveheti a kapcsolatot az érintett céggel.

Az ötödik hiba a **jogi megfelelés figyelmen kívül hagyása**. A jogban meghatározott szabályok elég jó alapot adnak az incidensek kezeléséhez, és a figyelmen kívül hagyásukból semmi pozitív nem származik: egy kibertámadás okozta károkon kívül esetenként még büntetést is kell fizetnie az érintett cégnek.

A hatodik hiba, hogy **nem kérnek segítséget, ha nem bírnak el a feladattal**.

A hetedik, hogy **túl statikus az IRP**. A kibertámadások és a támadók stratégiája rendkívül gyorsan változik, ezért a hatékonyság növelésének érdekében érdemes időnként újragondolni az incidenskezelési tervet is, hogy jobban illeszkedjen az új fenyegetésekhez.

A nyolcadik, hogy **nem készülnek fel a legrosszabb eshetőségre**.

A kilencedik, hogy **nem tesztelik az IRP-t**. Az előadó egy filmhez hasonlítja az incidenskezelést: amikor a színészek és a rendező felvétel előtt leülnek és még egyszer utoljára átbeszélik mi fog történni a felvétel közben. Az incidenskezelés résztvevői időnként egy kerekasztal beszélgetés formájában szóban szimulálhatnak egy incidenst, és egymástól kérdezve, egymásnak válaszolva tesztelhetik egymás tudását, így biztosak lehetnek benne, hogy éles helyzetben „reflex-szerű” lesz a reakció.

Az utolsó leggyakrabb hiba, hogy a **tervet nem megfelelően hajtják végre**.

Az előadás ide kattintva megtekinthető.

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

Protecting What Matters—Your Family & Home

(Dr. Chris Pierson)

Dr. Chris Pierson előadásában a **személyes kiberbiztonság és adatvédelem legfontosabb kérdéseiről beszélt**, különös tekintettel arra, hogyan védhetjük meg családunkat és otthonunkat a modern kibertámadásoktól. Az előadás egyik fő üzenete az volt, hogy a támadók ma már **nemcsak vállalatokat, hanem közvetlenül az egyes embereket és családokat is célba veszik**. Az internetes bűncselekmények okozta veszteségek mértéke évről évre nő, 2023-ban elérte a **12,5 milliárd dollárt**, és a leggyakrabb bűncselekmények között a befektetési csalások, az üzleti e-mail kompromittálás, a technikai támogatásnak álcázott csalások, adatszivárgások és a romantikus csalások szerepelnek.

A kiberbűnözők az **egyének és családok publikus adataira**: például névre, címre, telefonszámra, e-mail címekre, közösségi média profilokra és IP-címekre építve hajtanak végre célzott, kifinomult támadásokat. Az előadó hangsúlyozta, hogy az egyik elsődleges védekezési lépés a **támadási felület csökkentése**, amely az adatbróker oldalakról történő személyes adatok eltávolítását, valamint a deep web és dark web szivárgások figyelemmel kísérését jelenti. A kiszivárgott jelszavakat, felhasználói fiókokat érdemes frissíteni.

Az előadó kiemelte, hogy a **kulcsfontosságú online fiókok** – e-mail, pénzügyi szolgáltatók, egészségügyi rendszerek és közösségi média oldalak – **védelme elsődleges fontosságú**. Véleménye szerint nem a teljes internetes jelenlét tökéletes védelmére kell törekedni, hanem arra, hogy a legkritikusabb szolgáltatásoknál **alkalmazzunk legalább kétlépcsős azonosítást**, még ha SMS-alapon is, amelyik a leggyengébbnek mondható. A biztonságos eszközhasználat szintén elengedhetetlen: minden családi eszközre (telefonok, tabletek, számítógépek) **telepíteni kell legalább egy vírusirtót**, **rendszeresen frissíteni kell a rendszereket, és gondoskodni kell a megfelelő beállításokról**. Bizonyos kutatások szerint a családok átlagosan **7-ből 1** esetben használnak kiszivárgott jelszavakat, **5-ből 1** okosotthon könnyedén elérhető kívülről, és **4-ből 1** személyes eszköz fertőzött valamilyen kártevővel.

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

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

Az előadás külön blokkot szentelt az **otthoni hálózat és az IoT eszközök védelmének**. Az alapvető lépések közé tartozik a Wi-Fi hálózat elkülönítése vendéghálózatra és az okoseszközök **gyakori firmware-frissítése**. Az előadó ezután amerikai állampolgárokra vonatkozó specifikus tanácsokat adott, amit a magyar gyakorlatba nem lehet beépíteni.

Különös hangsúlyt kapott az **emberi tényező védelme is**. Pierson szerint a legtöbb kiberbiztonsági fenyegetés nem a technológiát célozza meg, hanem az emberek érzelmeire próbál hatni. A technikai támogatásnak álcázott csalások, a szociális média fiókokból indított támadások, a ransomware fertőzések és a különféle zsarolási kísérletek mind a **logikus gondolkodás háttérbe szorítására építenek**. Az előadó arra buzdította a hallgatóságot, hogy legyenek tudatosak és óvatosak a bejövő hívásokkal, az ismeretlen linkekkel és a közösségi médiában megjelenő szokatlan üzenetekkel szemben.

Végezetül az előadó egy **havi ütemezést javasolt** a családoknak a biztonsági intézkedések bevezetésére. A véleménye szerint a **szétosztott tudatosítás sokkal hatásosabb**, mintha egyszerre próbáljuk rázúdítani tudásunkat a családunkra. Májusban javasolt a családtagokkal való beszélgetés a csalásokról, júniusban a vendég Wi-Fi beállítása, júliusban és augusztusban a kétlépcsős azonosítás alkalmazása 10-10 fiókon, szeptemberben vírusírtók telepítése minden eszközre, októberben az adatbróker oldalakról való adattörlés, novemberben deep/dark web ellenőrzések végzése.

Az előadás ide kattintva megtekinthető.