NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 23. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- IT BIZTONSÁGI TIPP
- BBA+ BESZÁMOLÓK

KIBERTÁMADÁS! PODCAST

NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍREK

FIFA nevével visszaélő adathalász kampányokra figyelmeztet az FBI

(bleepingcomputer.com)

Az FBI figyelmeztetést adott ki a 2026-os labdarúgó-világbajnokság közeledtével megjelenő, a FIFA hivatalos weboldalát megszemélyesítő adathalász kampányokkal kapcsolatban. A támadók célja a személyes és a pénzügyi adatok megszerzése, valamint hamis jegyek és VIP csomagok értékesítésén keresztül további pénzügyi csalások elkövetése. **Bővebben...**

Egy aktívan kihasznált Android zero-day sérülékenységet javított a Google

(bleepingcomputer.com)

A Google kiadta a 2026. júniusi Android biztonsági javítócsomagot, amelyben 124 sebezhetőség, köztük egy aktívan kihasznált nulladik napi sérülékenység is javításra került. Az Android Framework CVE-2025-48595 számú sebezhetőség kihasználása kódfuttatást és jogosultságeszkalációt tesz lehetővé a támadók számára az Android 14-es vagy újabb verziójú eszközökön. **Bővebben...**

HTTP/2-fejléckezelési hiba miatt támadható több népszerű webszerver

(blog.calif.io)

Kutatók nyilvánosságra hoztak egy több népszerű webszervert érintő HTTP/2-alapú támadási módszer részleteit, miután a sérülékenység javításai több szoftver esetében is elérhetővé váltak. A sérülékenység abból adódik, hogy számos szerver ugyan korlátozza a HTTP-fejlécek összesített méretét, de nem szab felső határt a fejlécmezők számára. **Bővebben...**

Újabb Signal phishing kampány terjed

(malwarebytes.com)

A Signal hosszú ideje a biztonságos kommunikáció egyik etalonjának számít. Az alkalmazás végpontok közötti titkosítást használ, ezért sok újságíró, aktivista, vállalati vezető és biztonságtudatos felhasználó választja mindennapi kommunikációra. **Bővebben...**

Instagram fiókok feltörésére használták a Meta AI chatbotját

(techcrunch.com)

Az elmúlt napokban több felhasználó is arról számolt be a Redditen és az X-en, hogy feltörték az Instagram fiókjukat. A támadó feltehetően VPN kapcsolatot használt a célpontok feltételezett helyzetének elrejtéséhez, így el tudta kerülni az Instagram automatikus fiókvédelmi mechanizmus aktiválását. **Bővebben...**

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

2026. 05. 29. - 2026. 06. 04.

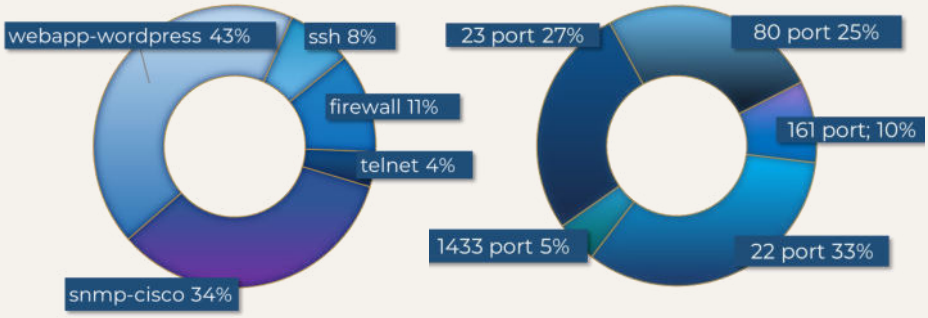
Fenyegetettségi szint:

alacsony | közepes | magas | kritikus

Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok

Az adatsorok melletti nyilak az előző héthez viszonyított változásokat mutatják.

Az elosztott kormányzati IT biztonsági csapdarendszerből (GovProbe1) származó adatok



NEMZETI KIBERBIZTONSÁGI INTÉZET

IT BIZTONSÁGI TIPP

Mobiltelefonok biztonságos használata

A mobiltelefonok mára már nem csupán kommunikációs eszközök, hanem a **digitális identitásunk központi elemei**, ezért a rajtuk tárolt adatok és hozzáférések rendkívül **értékesek a kiberbűnözők számára**. A mobiltelefonok elleni támadások jelentős része viszont nem kizárólag technikai sérülékenységekre épül, hanem **legtöbbször a felhasználók figyelmetlenségét és megszokásait használják ki**.

Az NBSZ NKI alábbi kiadványában igyekszünk bemutatni az okostelefonokra leselkedő veszélyeket, a leggyakoribb felhasználói hibákat, illetve olyan biztonsági ajánlásokat, amelyekkel jelentős mértékben csökkenthetők az eszközhasználatból, utazásból és a közösségi médiahasználatból eredő kockázatok.

Elolvasom

További érdekességekért, olvassa el korábbi tippünket is!

Hogyan védekezhetünk a böngésző a böngészőben támadás ellen?

BBA+ BESZÁMOLÓ

FIRST Peak Incident Response Technical Colloquium 2026

2026. május 5-6.

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

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

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

BBA+ BESZÁMOLÓ

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

A Nemzeti Kiberbiztonsági Intézet munkatársai **2026. május 5-6.** között részt vettek a **Genfben** megrendezésre kerülő éves **FIRST Peak Incident Response Technical Colloquium konferencián**.

A FIRST (Forum of Incident Response and Security Teams) 1990 óta működő, nemzetközi nonprofit szervezet, amely több mint 800 CSIRT/CERT-et, és független kutatót tömörít a köz-, magán- és akadémiai szektorokból, több mint 100 országból. **A szervezet célja a hatékony információáramlás biztosítása a megbízható incidenskezelők között. Magyarországot az NBSZ NKI képviseli a FIRST szervezetben.**

A FIRST Peak Incident Response Technical Colloquium 2026 olyan szakmai rendezvény, amely a **globális internet-infrastruktúra stabilitásának és ellenálló képességének kérdéseit állítja középpontba**. A fókusz a közösen használt, kritikus technológiai alapelemeken van, különösen a Domain Name System (DNS) és a Border Gateway Protocol (BGP) szerepén, de a rendezvény ennél tágabban is az internet működését biztosító alapinfrastruktúrák sérülékenységeit, működési kockázatait és védelmi lehetőségeit vizsgálja.

A kollokvium célja, hogy technikai, működtetési, kutatási és szakpolitikai nézőpontból egyaránt foglalkozzon ezekkel a rendszerekkel. Nemcsak azt elemzi, hogy milyen műszaki gyengeségek, támadási lehetőségek és üzemeltetési kihívások érintik a kritikus internetes komponenseket, hanem azt is, hogy ezek miként kapcsolódnak az incidensek felismeréséhez, mérsékléséhez és az összehangolt reagáláshoz. A rendezvény abból az alapvetésből indul ki, hogy a globális

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

internet alaprétegeinek biztonsága nem kizárólag technológiai kérdés, hanem működési, szervezeti és szabályozási dimenziója is van.

A konferencia egyik fontos sajátossága, hogy kifejezetten **közös párbeszédet kíván teremteni a technikai közösség és a döntéshozói, szabályozói oldal között**. Ennek érdekében nemcsak incidenskezelő szakembereket és kutatókat szólít meg, hanem a szakpolitikai és irányítási közeg szereplőit is, külön szakpolitikai fókuszú sávot is biztosítva számukra. A rendezvény így olyan fórumként értelmezhető, amely az internetes ökoszisztéma különböző szereplőit — üzemeltetőket, válaszadó csapatokat, kutatókat, szabályozói és kormányzati szereplőket — egy közös gondolkodási térbe kívánja bevonni.

A konferencián számos szakmai előadás hangzott el, azonban egyes előadások TLP Amber vagy Red minősítéssel voltak ellátva, így az alábbiakban csak a TLP Clear szintű eladások összefoglalóit közöljük.

Kiknek ajánlott a beszámoló megismerése?

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

A konferencia legfontosabb előadási az alábbiakban foglalhatók össze.

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

Open Source Software as Underfinanced Critical Infrastructure

(Christian Folini @ Netnea, CH)

A **nyílt forráskódú szoftvereket** az előadás nem egyszerűen fejlesztői közösségi termékekként, hanem **a mai digitális világ egyik alapvető infrastruktúrájaként** értelmezte. Christian Folini abból indult ki, hogy az internetes szolgáltatások, a felhőplatformok, a mobiltelefonok és a különféle üzleti rendszerek tömegesen támaszkodnak olyan nyílt forráskódú összetevőkre, amelyek nélkül a digitális működés jelentős része egyszerűen leállna. Ehhez képest ezeknek a projekteknek a nagy része **rendkívül gyenge anyagi háttérrel működik**: sok esetben nincs valódi bevételük, a fejlesztők önkizsákmányoló módon, szabadidejükben dolgoznak rajtuk és a támogatási felhívások gyakran visszhang nélkül maradnak. Az előadás egyik legerősebb állítása éppen az volt, hogy ezen kritikus digitális infrastruktúra jelentős része valójában **alulfinanszírozott, sérülékeny emberi munkára épül.**

Ennek érzékeltetésére több példát is hozott, köztük a **curl projektet**, amelyet a világ egyik legelterjedtebb szoftverösszetevőjeként említett és amely hosszú időn át lényegében egyetlen fejlesztő szabadidős munkájára épült. Ebből azt a következtetést vonta le, hogy még a legkritikusabb, legnagyobb hatású nyílt forráskódú elemek sem feltétlenül kapnak arányos pénzügyi vagy szervezeti támogatást. A nagy technológiai szereplők, illetve a különféle alapítványok időnként enyhítik ugyan a nyomást, de ez többnyire csak akkor történik meg, amikor már **komoly biztonsági esemény vagy nyilvános kudarc** irányítja rá a figyelmet a problémára.

A probléma gyakorlati oldalát a **OWASP CRS** példáján keresztül mutatta be, amely a webalkalmazás-tűzfalak világában meghatározó szabálykészletnek számít. Az előadás szerint ez a projekt tipikusan nyílt forráskódú kezdeményezés abból a szempontból, hogy nyitott licenc alatt érhető el, ugyanakkor nem tipikus abban az értelemben, hogy már viszonylag jelentős piaci

hatással rendelkezik. Elmondása szerint a kereskedelmi piac jelentős része ezt a szabálykészletet használja közvetlenül vagy közvetve, több nagy felhő- és tartalomszolgáltató is erre épít, mégis csak korlátozott számú aktív fejlesztő dolgozik rajta és a szponzoráció továbbra sem arányos azzal az üzleti értékkel, amelyet a projekt a piacnak nyújt. Folini különösen kritikus volt azzal a gyakorlattal szemben, amikor **a nagy szereplők a nyílt forráskódú projektek támogatását nem ellátásbiztonsági, hanem marketingkérdésként kezelik**. Az egyik fő állítása az volt, hogy ez hibás szemlélet: ha egy cég a bevételtermelő szolgáltatását ilyen komponensekre építi, akkor annak fenntartható támogatását a saját ellátási lánca részeként kellene kezelnie.

Az előadás második nagy témája a mesterséges intelligencia hatása volt. Folini szerint **a nyílt forráskódú projektekre nehezedő nyomást az MI nem csökkenti, hanem inkább fokozza**. Egyrészt a nyílt forráskód nyilvános természete eleve megkönnyíti a sérülékenységek keresését, másrészt az újabb nyelvi modellek és automatizált eszközök drasztikusan megnövelik a hibakeresés, a támadási minták feltárása és a kódbeküldések mennyiségét. Míg korábban sok MI által készített hibajelzés és kódbeküldés gyenge minőségű volt, addig 2025-re egyre több már első ránézésre is jónak számít, ezért azokat sokkal nehezebb kiszűrni. Ez azt eredményezi, hogy a fejlesztőknek ma már nem pusztán több bejelentést kell kezelniük, hanem jóval nagyobb szellemi terhelés mellett kell eldönteniük, hogy egy-egy javaslat valóban hasznos, hibás vagy kifejezetten rosszindulatú-e. **Az MI tehát nemcsak a támadók hatékonyságát növeli, hanem a védekező oldalon a szűkös emberi kapacitást is felemészti.**

Az előadó szerint ez a folyamat **hosszabb távon közvetlenül veszélyezteti a digitális infrastruktúra biztonságát.** Ha a nyílt forráskódú projekteket túlterheli a hibajelentések, a kódbeküldések és a folyamatos biztonsági vizsgálatok tömege, akkor nő a fejlesztői kiégés, romlik az ellenőrzés minősége, és emelkedik annak a kockázata is, hogy rosszindulatú szereplők fokozatosan bizalmi pozícióhoz jutnak egy-egy projektben. Az előadás szerint ez különösen veszélyes úgy, hogy a legtöbb szervezet még mindig nem lát rá teljes mélységben a saját

szoftver-ellátási láncára, és gyakran a közvetlen komponenseken túli függőségeket sem kezeli érdemben. Így egy alulfinanszírozott, túlterhelt nyílt forráskódú projekt gyengesége könnyen sokkal szélesebb körben okozhat problémát, mint amennyire elsőre kitűnik.

A lezárásban az előadó szükségesnek nevezte, hogy a **kritikus nyílt forráskódú projektek finanszírozása rendezettebbé váljon**, ehhez pedig olyan modellekre van szükség, amelyek nem alkalmi adományokra, hanem fenntartható támogatási mechanizmusokra épülnek. Szóba került az **állami szerepvállalás**, a nyílt forráskódú **alapítványok** megerősítése, valamint az a megközelítés is, hogy **a vállalatoknak ténylegesen finanszírozniuk kellene** a saját digitális ellátási láncuk kritikus elemeit. Folini szerint a kibervédelmi és ellátásbiztonsági szabályozások — köztük az európai Kiberreziliencia Rendelet — csak akkor lesznek valóban hatékonyak, ha a szervezetek nemcsak elvben, hanem pénzügyileg is **felelősséget vállalnak** azokért a nyílt forráskódú komponensekért, amelyekre a működésük épül.

OpenSource and Open Data, How Those Will Improve Resilience and Strategic Autonomy?

(Mika Lauhde @ Luxembourg House of Cybersecurity, LU)

Az előadás azt a kérdést járta körül, hogy Európa miként tudna nagyobb digitális ellenálló képességet és stratégiai önállóságot elérni a nyílt forráskódú megoldások és a nyílt adatok tudatosabb használatával. A kiindulópont az volt, hogy a digitalizáció, az automatizáció, a mesterséges intelligencia, az adatáramlások és a kvantumtechnológiák fejlődése **egyszerre növeli a függőségeket és a sérülékenységeket,** miközben a **kiberbiztonsági működéshez szükséges adatokhoz való hozzáférés továbbra is erősen korlátozott**.

Lauhde ezt nem pusztán technológiai, hanem **európai versenyképességi és stratégiai problémaként** értelmezte.

A gondolatmenet egyik erős eleme az volt, hogy **az európai digitális környezetet ma nagyrészt nem európai szereplők uralják.** Ennek érzékeltetésére az előadó több példát is hozott: a böngészők, a mobil operációs rendszerek és más alapvető digitális platformok piacán Európa legfeljebb korlátozott szereplő, miközben a kontinens gazdaságának döntő részét kis- és középvállalkozások adják, amelyek különösen kiszolgáltatottak ezeknek a függőségeknek. A történeti visszatekintésben azt is hangsúlyozta, hogy Európa korábban rendelkezett olyan technológiai elemekkel, amelyekre önállóbb digitális ökoszisztéma épülhetett volna, de ezek jelentős része elveszett vagy más régiók hasznosították tovább. Az előadás ebből azt a következtetést vonta le, hogy az európai **„stratégiai digitális autonómia”** nem elméleti jelszó, hanem tudatos iparági, állami és közösségi együttműködést igénylő gyakorlati cél.

Erre válaszként mutatta be a **Luxembourg Cybersecurity Factory kezdeményezést**, amelyet a Luxembourg House of Cybersecurity keretében építenek. A modell négy pillérre támaszkodik: egy adatmegosztási térre, egy mesterséges intelligenciával foglalkozó központra, egy kvantumtechnológiai laborra és egy úgynevezett Cyber Commons Office-ra. A cél nem az, hogy Luxemburg önmagában oldja meg a problémát, hanem hogy gyorsító és katalizátor szerepet vállaljon, vagyis olyan eszközöket, adatokat, együttműködési formákat és közösségi struktúrákat hozzon létre, amelyek más európai szereplők számára is hasznosíthatók. Az előadás szerint ebben a megközelítésben **a nyílt forráskódot nem olcsó alternatívaként, hanem stratégiai digitális infrastruktúraként kell kezelni.**

Külön hangsúlyt kapott a **kiberbiztonsági adatok** kérdése. Lauhde vitatta azt a nézetet, hogy Európában önmagában kevés adat áll rendelkezésre; szerinte inkább az a gond, hogy az adatok széttagoltan, elszigetelt környezetekben vannak jelen, és ezért nem alakul ki belőlük valódi kritikus tömeg. A bemutatott adatmegosztási megközelítés lényege az volt, hogy **a résztvevők a saját, tisztított és strukturált adataikat egy közös térbe helyezik**, ahol ezeket mesterséges intelligenciával lehet gazdagítani és elemezni. Az elképzelés szerint így nem csupán mindenki a

BBA-PLUSZ-31.2-24-2024-00004. sz. pályázat részeként

BBA+ BESZÁMOLÓ

saját korlátozott adatvagyonát használhatja tovább, hanem a közösből származó, nagyobb értékű eredményhez is hozzáférhet. Ez egyszerre szolgálhat üzleti célokat, valamint a nemzeti és európai kibervédelmi ellenálló képesség erősítését.

Az előadás végén az is világossá vált, hogy a technológia önmagában nem elegendő. A valódi akadályok között az előadó a finanszírozást, a közbeszerzési logikát, az adózási és könyvelési szemléletet, a politikai döntéshozatalt, valamint a nyílt forráskódot övező tévhiteket emelte ki. Külön hangsúlyozta, hogy **a nyílt forráskód nem „ingyenes”** a szó egyszerű értelmében, hanem más költségszerkezettel működik, és ezt a szervezeteknek meg kell tanulniuk helyesen értelmezni. Az összkép alapján az előadás erősen stratégiai és részben jövőkép-jellegű volt: azt próbálta megmutatni, hogy a nyílt forráskódra, nyílt adatokra és európai együttműködésre épülő modell nemcsak technikailag lehetséges, hanem **hosszabb távon szükséges** is lehet ahhoz, hogy Európa a digitális térben kevésbé kiszolgáltatott szereplő legyen.

Geopolitical Cybersecurity Threats and National Security

(Rick Logan-Stanford @ TTCSIRT, TT)

A kibertér ebben az előadásban nem egyszerűen technológiai környezetként, hanem egy alacsony intenzitású, **folyamatosan aktív hadszíntérként** jelent meg, ahol az államok stratégiai célokat követnek anélkül, hogy átlépnék a hagyományos fegyveres konfliktus nyílt küszöbét. A hangsúly azon volt, hogy az államilag támogatott műveletek, a fejlett, tartós fenyegetések és az állami, illetve bűnözői szereplők összefonódása egyre inkább elmosódottá teszi a kémkedés, a szabotázs és a hadviselés közötti határokat. Az előadás szerint ma már **nem feltétlenül bombákkal és nyílt katonai csapásokkal zajlik a nyomásgyakorlás, hanem hálózatokba történő behatolással, kritikus rendszerek felderítésével és a társadalmi, gazdasági működés gyenge pontjainak tesztelésével.**

A gondolatmenetet több ismert incidenssel támasztotta alá. A **Stuxnet** példáján keresztül azt

emelte ki, hogy egy **kiberművelet fizikai és társadalmi következményekkel is járhat**, még akkor is, ha nem jár közvetlen emberáldozatokkal. Az **ukrán áramszolgáltatást érintő támadást és a NotPetya-esetet** úgy mutatta be, mint olyan műveleteket, amelyek túlmutattak a közvetlen technikai káron: súlyos gazdasági hatást, ellátási problémákat és tartós bizalmi sérülést okoztak. A **SolarWinds-ügy** pedig azt szemléltette, hogy a beszállítói láncon keresztüli kompromittálás milyen mélységben érintheti kormányzati és vállalati rendszerek széles körét. Az előadás egyik fontos állítása az volt, hogy ezek az esetek nem elszigetelt incidensek, hanem egy tartós geopolitikai küzdelem megnyilvánulásai.

Külön hangsúlyt kapott az a megközelítés, hogy az államok sokszor nem közvetlenül saját nevükben hajtanak végre kiberműveleteket, hanem közvetítőként bűnözői vagy félkatonai jellegű szereplőket használnak. Ez azért veszélyes, mert a támadás formálisan egy zsarolóvírus-csoporthoz vagy más bűnözői szereplőhöz köthető, miközben a geopolitikai haszon máshol csapódik le. Az előadó szerint ez a modell **megnehezíti a felelősség egyértelmű megállapítását**, és csökkenti a hagyományos elrettentés erejét is. Ezzel összefüggésben a beszállítói lánc elleni támadásokat a jelenlegi környezet egyik legfontosabb kockázataként írta le, mert ezek révén a támadók úgy juthatnak be nagyobb szervezetekhez vagy állami rendszerekhez, hogy közben a közvetlen célpont valójában csak egy megbízhatónak hitt szolgáltató vagy partner.

Az előadás lezárása már inkább javaslatokra épült. A legfontosabbak között szerepelt a köz- és magánszféra közötti szorosabb együttműködés, a kritikus infrastruktúrák ellenálló képességének tudatos fejlesztése, a hálózati szegmentálás, a tartós működési zavarokra is felkészített incidenskezelési tervek, valamint a beszállítói kockázatok következetesebb kezelése. Emellett hangsúlyozta a **nemzetközi normák, a nyilvános attribúció és a szankciós eszközök** szerepét is, vagyis azt, hogy a **kibertérben zajló konfliktusokat nem lehet pusztán technikai védekezéssel kezelni**. Összességében az előadás azt a képet rajzolta fel, hogy a kiberkockázat

BBA+ BESZÁMOLÓ

ma már nem kizárólag informatikai vagy bűnüldözési kérdés, hanem a nemzetbiztonság, a gazdasági stabilitás és a geopolitikai mozgástér egyik meghatározó tényezője.

Visibility, Blocking, and Impact: Operationalizing DNS Cybersecurity at Scale in the Swiss Context

(John Todd @ Quad9, CH)

Az előadás középpontjában az állt, hogy a DNS milyen módon használható gyakorlati, nagy léptékű biztonsági eszközként, különösen olyan környezetekben, ahol nem lehet minden végpontra külön védelmi megoldást telepíteni. John Todd a svájci székhelyű, nonprofit Quad9 működésén keresztül mutatta be ezt a modellt. A **Quad9 nyilvános DNS-feloldó szolgáltatásként működik,** amely a rosszindulatú domainekhez tartozó lekérdezéseket blokkolja, miközben adatvédelmi szempontból is szigorú működést követ: nem tárol IP-címeket, és a felhasználói adatokkal kapcsolatban kifejezetten visszafogott adatkezelési modellt alkalmaz. Az előadás szerint a DNS erre azért alkalmas, mert szinte minden internetes kapcsolat valamilyen DNS-lekérdezéssel indul, ezért ez a réteg nagyon széles láthatóságot ad a fenyegetési mintázatokra.

A bemutatott működési modell lényege az volt, hogy a Quad9 több tucat fenyegetési információforrásból kap rosszindulatú domainekre vonatkozó adatokat, ezeket rövid időközönként frissíti, majd a saját infrastruktúráján keresztül blokkolja az ilyen címek elérését. A szolgáltatás emellett visszajelzést is ad a fenyegetési információt biztosító partnereknek arról, hogy egy-egy blokkolt domainelem milyen gyakorisággal és nagyjából mely térségekben jelent meg. Ez a visszacsatolás **segíti a fenyegetési adatok pontosítását és a kampányok jobb megértését is**. Todd ezzel együtt hangsúlyozta, hogy a Quad9 önmagában nem „gyárt” fenyegetési adatokat, hanem inkább **közvetítő és végrehajtó szerepet tölt be**: a különböző forrásokból származó információkat olyan szolgáltatássá alakítja, amelyet

a végfelhasználók és szervezetek közvetlenül hasznosíthatnak.

A svájci adatok kapcsán az előadás több érdekes megfigyelést is kiemelt. Az egyik szerint a Svájcból érkező DNS-forgalom döntő része Svájcon belül is marad, ami adatvédelmi és működési szempontból kedvező. Emellett a svájci felhasználói körben a vállalati használat tűnt a legerősebbnek, ezt követte a lakossági forgalom, majd a tárhelyszolgáltatói szegmens. A blokkolási statisztikák alapján Svájcban is jelentős számú rosszindulatú lekérdezés jelenik meg naponta, de az előadás értelmezése szerint a svájci környezet nem tartozik a legfertőzöttebb vagy legkockázatosabb országok közé. Egy konkrét példán keresztül azt is bemutatta, hogyan válik láthatóvá egy támadási kampány DNS-szinten: egy orosz domainhez tartozó rosszindulatú forgalom néhány napon át több országban is megjelent, Svájcban pedig rövid, de jól kirajzolódó aktivitást mutatott. Ez jól szemléltette, hogy a DNS-adatokból nemcsak az derülhet ki, hogy valami rosszindulatú, hanem az is, **hogyan terjed földrajzilag és időben egy adott infrastruktúra vagy kampány.**

Todd szerint a DNS-alapú védelem különösen hasznos azoknál a szervezeteknél, amelyek korlátozott erőforrásokkal működnek, de valós fenyegetettséggel néznek szembe – például civil szervezeteknél, kisebb intézményeknél vagy olyan hálózatüzemeltetőknél, amelyek szeretnének egy alapvető, alacsony súrlódású védelmi réteget biztosítani a felhasználóiknak. Az üzenet tehát nem az volt, hogy a DNS-blokkolás minden problémát megold, hanem az, hogy megfelelően beépítve nagyon hatékony, széles körben alkalmazható és viszonylag könnyen bevezethető védelmi elem lehet.

Külön értéke, hogy egyszerre ad láthatóságot, csökkenti a tényleges felhasználói károkat, és olyan helyeken is működtethető, ahol összetettebb végpontvédelmi vagy hálózatfelügyeleti eszközök bevezetése nem reális.

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

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

Cybersecurity in a Geopolitical Context

(Florian Schütz @ NCSC.ch, CH)

A kiberbiztonság ebben az előadásban nem elsősorban technikai támadás–védekezés kérdésként jelent meg, hanem olyan területként, amelyet egyre erősebben alakítanak a geopolitikai viszonyok, a technológiai verseny és a szabályozási törekvések. Florian Schütz szerint hibás az a leegyszerűsített megközelítés, amely a kiberbiztonságot pusztán védekezési költségként kezeli, mert így könnyen háttérbe szorul a vezetői és politikai döntéshozatalban. Ehelyett azt hangsúlyozta, hogy **a biztonsági beruházások értéket is képesek teremteni**, például jobb piaci információ, megbízhatóbb működés vagy nagyobb stratégiai mozgástér formájában. Ennek illusztrálására egy korábbi e-kereskedelmi példát hozott, ahol egy támadás nyomán bevezetett technikai intézkedés végül új piaci felismerésekhez is vezetett.

Az előadás egyik fő gondolatmenete arra épült, hogy az 1990-es és 2000-es évek optimista, digitalizációtól demokratizálódást váró szemlélete mára háttérbe szorult, és helyette egyre inkább a biztonságpolitikai kockázatkeretezés vált meghatározóvá. Ezt Schütz összekapcsolta a **Snowden-ügy utáni kijózanodással,** valamint azzal a **technológiai versennyel**, amelyet ma elsősorban az Egyesült Államok és Kína közötti küzdelemként érzékelünk. Értelmezése szerint a világban jelenleg két nagy technológiai ökoszisztéma rajzolódik ki, és a többi szereplőnek — köztük Európának és Svájcnak is — úgy kell pozíciót találnia, hogy közben ne veszítse el a cselekvőképességét és az együttműködési lehetőségeit. A szabályozást ezért **kettős természetű eszközként** írta le: egyszerre szolgálhat legitim biztonsági célokat, ugyanakkor piacformáló, sőt piaclezáró hatása is lehet.

Különösen fontosnak nevezte **a fenyegetési információk megosztását**, mert szerinte a túlzott geopolitikai széttagolódás éppen a védekező oldalt gyengítheti. Ha a különböző államok és szervezetek a politikai bizalmatlanság miatt egyre kevésbé osztják meg egymással a releváns

technikai információkat, az végső soron a támadókat segíti. Svájc példáján keresztül azt emelte ki, hogy egy ország nem feltétlenül a legjobb a nyers információgyűjtésben, de erős lehet az elemzésben és az értelmezésben, ezért a nemzetközi együttműködésből való kiszorulás közvetlenül gyengítené a védekezőképességet. Ebből a szempontból a **kiberbiztonság** nemcsak technológiai, hanem **diplomáciai és bizalomépítési kérdés is**.

A mesterséges intelligencia kapcsán az előadás óvatosan optimista hangot ütött meg. Schütz nem vitatta a kockázatokat, de inkább azt hangsúlyozta, hogy **a mesterséges intelligencia valódi áttörést elsősorban a védekező oldalon hozhat**, ha azt a minőségbiztosítás, az észlelés, az elemzés és a biztonságosabb rendszerek tervezése felé fordítják. Véleménye szerint a digitális rendszerek egyik alapvető gondja ma az, hogy nem megfelelő mérnöki fegyelemmel készülnek, és ezen a ponton **az MI a védelem és a minőség javításának eszköze lehet.** Ugyanakkor azt is hangsúlyozta, hogy az ilyen rendszerek mögött rendkívül összetett, energia-, hűtési, félvezetőgyártási és nyersanyag-ellátási lánc áll, amely maga is mélyen geopolitikai kérdés. Az előadás végső üzenete ezért az volt, hogy a kiberbiztonság jövőjéről nem lehet elszigetelten gondolkodni: a technológiai fejlesztések, a geopolitikai erőviszonyok, a szabályozás, a bizalom és a nemzetközi együttműködés együtt határozzák meg, milyen biztonság érhető el a gyakorlatban.

Securing a Global Infrastructure

(Stefan Lüders @ CERN, CH)

A **CERN** esetében a kiberbiztonság nem csupán egy nagy kutatóintézet belső védelmét jelentette, hanem egy **világméretűen összekapcsolt tudományos és műszaki infrastruktúra biztonságát** is. A hangsúly azon volt, hogy a CERN egyszerre működtet helyi adatközpontokat, ipari vezérlőrendszereket és részecskegyorsítókat, miközben kutatók, egyetemek és partnerintézmények globális hálózatával dolgozik együtt. Ebből következően egy távoli

BBA+ BESZÁMOLÓ

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

intézménynél bekövetkező incidens is könnyen elérheti a CERN környezetét, ezért a **nemzetközi incidenskezelési koordináció** itt nem kényelmi kérdés, hanem közvetlen önvédelmi érdek.

A működési környezet összetettségét az adta, hogy a CERN nemcsak saját helyi infrastruktúrára támaszkodik, hanem a nagy hadronütköztető által termelt adatok feldolgozásához világszintű számítási hálózatot használ. Ebben különböző országok adatközpontjai, egyetemi géptermei és kutatóintézeti rendszerei vesznek részt, eltérő technikai és biztonsági érettségi szinten. Az előadás világossá tette, hogy ez a modell **tudományos szempontból rendkívül hatékony, biztonsági szempontból viszont nehezen kezelhető**: egy kisebb, gyengébben védett partnerintézményen keresztül is el lehet jutni a nagyobb központok felé. Külön nehézséget jelent, hogy a CERN-ben a klasszikus kutatási, egyetemi jellegű környezet és az ipari vezérlőrendszerek világa egyszerre van jelen, vagyis a nyitottság és a szigorú kontroll igénye folyamatosan ütközik egymással.

A bemutatott incidensek azt szemléltették, hogy a **támadások gyakran kompromittált felhasználói fiókokból, feltört szerverekből vagy rosszul kezelt helyi incidensekből indulnak**, majd az **összekapcsolt tudományos hálózatokon keresztül továbbterjednek**. Az is elhangzott, hogy a károk nemcsak technikaiak: ha egy partneri adatközpont hosszabb időre kiesik, az közvetlenül csökkenti a kutatáshoz rendelkezésre álló számítási kapacitást, növeli a költségeket, és reputációs veszteséget is okozhat. Lüders ebből azt a következtetést vonta le, hogy a sikeres védelemhez nem elég a központi technikai kontroll; szükség van működő nemzetközi kapcsolatrendszerre, gyors kommunikációra és arra, hogy a résztvevők ismerjék egymást, illetve bízzanak egymásban. Az előadás szerint az **incidenskezelés jelentős része valójában közösségépítés és folyamatos koordináció.**

Ennek megfelelően a CERN és partnerei több szinten szerveztek közös biztonsági együttműködést. Ide tartozott a kapcsolattartók hálózata, a rendszeres válaszkészségi tesztelés, a közös gyakorlatok, a gyakorlati incidenskezelési képzések és az egyszerűsített segédanyagok

is. Lüders külön hangsúlyozta, hogy sok esetben nem a technikai tudás hiánya a legnagyobb gond, hanem a rossz első reakció: amikor valaki pánikszerűen belenyúl egy kompromittált rendszerbe, és ezzel megsemmisíti a bizonyítékokat vagy ront a helyzeten. A CERN ezért nemcsak a saját infrastruktúráját védi, hanem képzésekkel és koordinációval a partneri környezet ellenálló képességét is igyekszik javítani. Az összkép alapján az előadás fő tanulsága az volt, hogy egy ilyen globális, széttagolt infrastruktúrában a biztonság nem tartható fenn kizárólag technikai eszközökkel; **a működő védelemhez nemzetközi együttműködésre, közös eljárásokra és hosszú idő alatt felépített bizalomra is szükség van.**

About Time: A Blueprint for Operating Resilient, Sovereign, and Authenticated NTP at Global Scale

(Raphael Seebacher @ Open Systems, CH)

Az időszinkronizáció nem háttérszolgáltatásként, hanem a modern informatikai és biztonsági működés egyik csendes, de kritikus alaprétegeként vezette fel az előadó. Raphael Seebacher abból indult ki, hogy az **egységes idő nélkül megbízhatatlanná válhat a tanúsítványok ellenőrzése, a többtényezős hitelesítés, a naplók összevetése, sőt akár az Active Directory működése is.** A kiinduló incidens egy 2019-es eset volt, amikor egy helyi GPS-alapú referenciaóra elvesztette a pontos időforrást, a rendszer pedig egy korábbi konfigurációs döntés miatt nem a várt módon kezelte ezt a helyzetet. A hiba nem látványos összeomlásként jelentkezett, hanem „csendes hibaként”: az időforrás minősége romlott, de ezt csak egy ügyfél észlelte, amikor a saját alárendelt órái már nem tudtak megfelelően szinkronizálni. Az előadás egyik fő tanulsága az volt, hogy az **időszinkronizáció tipikusan addig láthatatlan, amíg el nem romlik – akkor viszont sok más rendszerrel együtt válik kritikussá.**

A technikai magyarázat jól érzékeltette, hogy az NTP működése első látásra egyszerű, valójában azonban sok olyan tényezőtől függ, amely globális környezetben jelentős kockázatot hordoz.

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

BBA+ BESZÁMOLÓ

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

Az időt a kliensek több forrásból próbálják megállapítani, majd ezekből számítják ki a saját eltérésüket, ezért a rendszer alapvetően a redundanciára és az összevetésre épít. Seebacher külön hangsúlyozta, hogy a rossz idő nem egyszerűen kényelmetlenség: ha az órák „ugranak”, akkor **ugyanaz az időbélyeg több különböző eseményhez is tartozhat, ami különösen incidenskezelésnél és naplóelemzésnél problémás**. Ezért a nyers átállítás helyett az órákat inkább fokozatosan kell „visszahúzni” vagy „gyorsítani”, hogy a rendszeridő ne sérüljön meg. Innen vezette le, hogy egy globális infrastruktúránál az időterjesztést **is önálló, tudatosan megtervezett szolgáltatásként kell kezelni,** nem pedig „egyszer beállítottuk, aztán majd működik” alapon.

Az **Open Systems** megközelítése erre egy **többrétegű modellt** épített. A legfelső szinten megbízható referenciaidő-forrásokat választottak, például nemzeti mérésügyi intézeteket, egyetemeket vagy más, kellően stabil szolgáltatókat, miközben arra is figyeltek, hogy ezek földrajzilag, hálózatilag és politikailag is kellően diverzek legyenek. A következő szinten saját, globálisan elosztott időterjesztő réteget működtettek, amely a referenciaforrásokból veszi át az időt, majd azt a világ különböző pontjain futó, több mint tízezer menedzselt csomópont felé osztja szét. Ezzel egyszerre tudtak méretezhető rendszert kialakítani és elkerülni azt is, hogy minden kliens közvetlenül a felső szintű forrásokat terhelje. Az előadás szerint a jó architektúra itt nemcsak a pontosságról szólt, hanem a szuverenitásról is: arról, hogy a szervezet minél inkább saját maga kontrollálja, honnan veszi az időt, és milyen minőségben terjeszti tovább.

A bemutatott gyakorlati problémák azt is megmutatták, hogy **az időszinkronizáció globális méretben tele van valós üzemeltetési nehézségekkel.** Előkerültek a szolgáltatói szintű szűrések, a régi operációs technológiai rendszerek sajátosságai, az eltérő ügyfélviselkedések, sőt még az is, hogy egyes berendezések túl gyakran kérdezik le az időt, vagy egyszerre több protokollváltozatot használnak. Ezek a helyzetek nem elméleti hibák, hanem napi üzemeltetési kihívásokként jelentek meg. Ugyanilyen fontos volt a megfigyelhetőség kérdése: Seebacher

külön kiemelte, hogy az Open Systems a korábbi, ügyféljelzésen alapuló hibafelismerést fokozatosan valós idejű telemetriára és proaktív minőségfigyelésre cserélte le. A gyakorlatban ez azt jelentette, hogy a rendszerből részletes mutatókat, naplókat és állapotinformációkat gyűjtöttek, ezekből áttekintő felületeket építettek, majd fokozatosan olyan riasztásokat vezettek be, amelyek már nem egy-egy hiba bekövetkezése után, hanem annak jeleinél figyelmeztetnek.

Az előadás záró része a **hitelesített idő** felé vezető útra, vagyis a **Network Time Security** bevezetésére fókuszált. Az alapgondolat az volt, hogy ma a legtöbb időforrás-hitelesítés nélküli NTP-t használ, vagyis a kliens gyakran nem tudja bizonyítani, hogy valóban attól a szervertől kapta az időt, akitől gondolja. A NTS ezt a problémát modern, titkosított kulcscsere és egyszer használatos hitelesítési elemek révén oldja meg, úgy, hogy közben nagy léptékben is kezelhető marad. Seebacher ugyanakkor nem úgy mutatta be ezt, mint már teljesen kiforrott, mindenhol kész megoldást, hanem mint olyan irányt, amelybe már most érdemes elindulni. Az összkép alapján az előadás fő üzenete az volt, hogy az időszinkronizációt ma már nem szabad láthatatlan háttérszolgáltatásként kezelni: ellenálló, megfigyelhető, szuverén és hitelesített működése a biztonságos digitális infrastruktúra alapfeltétele.

Securing the DNS Infrastructure at Global Scale
(Bill Woodcock @ Packet Clearing House, US)

A DNS-infrastruktúra ebben az előadásban nem pusztán technikai szolgáltatásként, hanem olyan globális kritikus kommunikációs infrastruktúraként jelent meg, amelyet sem egyetlen állam, sem egyetlen piaci szereplő nem képes önmagában, elszigetelten biztonságosan működtetni. Bill Woodcock a Packet Clearing House működésén keresztül mutatta be, hogy a legfontosabb országkódos felső szintű domainek, gyökérnévszerverek és más alapvető DNS-szolgáltatások megbízhatósága valójában egy **nemzetközi, sűrűn összekapcsolt hálózaton múlik**. A hangsúly azon volt, hogy a szuverenitás a DNS esetében nem jelenthet teljes izolációt,

BBA+ BESZÁMOLÓ

mert a valódi rendelkezésre állás, rugalmasság és ellenálló képesség éppen a globális összekapcsoltságból és az együttműködő üzemeltetésből fakad.

A PCH modellje szerint a DNS-szolgáltatás alapja a **földrajzilag és hálózatilag szétszórt, anycast elven működő infrastruktúra**. Az előadás részletesen bemutatta, hogyan jut el a zónaadat a rejtett elsődleges névszerverektől a bejövő rendszereken, aláíró infrastruktúrán és elosztó rétegen keresztül a világ több száz helyszínére. A műszaki logika lényege az volt, hogy a felhasználók mindig **a topológiailag legközelebbi példányhoz fordulnak**, és hiba vagy túlterhelés esetén a forgalom automatikusan a következő alkalmas helyszínre terelődik. Ez nemcsak sebességi és rendelkezésre állási előnyt jelentett, hanem támadások esetén is kulcsszerepet kapott: a túlterheléses forgalom **rendszerint csak a hálózat bizonyos pontjaira koncentrálódik**, miközben a világ többi része továbbra is kiszolgálható marad. Ennek feltétele azonban az, hogy a hálózat eleve úgy legyen méretezve, hogy az egyes csomópontok képesek legyenek elviselni a rájuk eső terhelést.

Különösen érdekes volt az a megközelítés, ahogyan a PCH a biztonságot és a piaci semlegességet összekapcsolta. Woodcock szerint nem mindegy, hogy egy DNS-szolgáltató **néhány nagy tranzitszolgáltatóra támaszkodik, vagy közvetlenül kapcsolódik** sok hálózathoz internetes csomópontokon keresztül. A PCH az utóbbit választotta, mert így nemcsak a teljesítmény javul, hanem biztosítható az is, hogy a szolgáltatás elérése ne függjön attól, ki melyik nagy szolgáltató ügyfele. Ez a döntés tehát egyszerre volt mérnöki és szabályozási jelentőségű: a DNS-hez való hozzáférést közérdekű, diszkriminációmentes szolgáltatásként kezelte, nem pedig kereskedelmi optimalizálási kérdésként. Az előadás ebből a szempontból azt is megmutatta, hogy a DNS-infrastruktúra kialakítása mögött számos olyan döntés áll, amely látszólag technikai, valójában azonban **közvetlen hatással van a digitális egyenlőségre és az országok tényleges önálló működőképességére.**

A záró rész már inkább az üzemeltetés és a bizalmi architektúra kérdéseire fókuszált. Szó esett

a DNSSEC kulcskezelésről, a fizikailag védett aláíró környezetről és arról, hogyan lehet ezt a fajta infrastruktúrát hosszú távon fenntarthatóan működtetni. Az előadás összképe alapján a fő tanulság az volt, hogy a **DNS biztonsága nem oldható meg pusztán helyi vagy nemzeti eszközökkel**. A valóban ellenálló és biztonságos működéshez olyan nemzetközi, műszakilag diverz és politikailag is tudatosan kialakított architektúrára van szükség, amely egyszerre kezeli a rendelkezésre állás, a támadástűrés, a semlegesség és a bizalom kérdéseit.

The Invisible Infrastructure: DNS Security from Authentication to Availability

(Branko Mijuskovic @ Proton AG, CH)

Az első állítás az volt, hogy az e-mailes **bizalom jelentős része valójában DNS-re épül**. Az SPF azt mondja meg, mely kiszolgálók küldhetnek levelet egy adott domain nevében, a DKIM azt teszi ellenőrizhetővé, hogy az üzenet tartalma és bizonyos fejlécei nem módosultak útközben, a DMARC pedig ezekre a mechanizmusokra építve segít a fogadó oldalnak eldönteni, hogyan kezelje az adott levelet. Vagyis a DNS nem pusztán névfeloldási szolgáltatásként jelent meg, hanem az e-mailes bizalom egyik vezérlési síkjaként is.

A technikai fókusz a DKIM-visszajátszásos támadásra került. Ennek lényege, hogy a támadó megszerez egy valóban hitelesen aláírt e-mailt, majd annak **a DKIM által védett részeit változatlanul hagyva újraküldi nagy mennyiségben saját infrastruktúráról**. Mivel a DKIM-aláírás formálisan továbbra is érvényes marad, a fogadó oldal könnyen hitelesnek tekintheti az üzenetet. Az előadás szerint ez különösen nehezen kezelhető, mert a klasszikus ellenőrzések nem feltétlenül jeleznek egyértelmű hibát: az SPF ugyan elbukhat, de ha a DKIM rendben van, a DMARC még mindig átengedheti a forgalmat. A Proton saját tapasztalata alapján ez nem elméleti probléma volt, hanem valós, nagy volumenű visszaélés, amely jelentős kézbesítési és reputációs hatással járt.

BBA+ BESZÁMOLÓ

A védekezés egyik fontos eleme az volt, hogy a DKIM-konfiguráció ne csak minimálisan legyen helyes, hanem **ellenálló** is. Ennek részeként szóba került a fejlécmezők szélesebb körű aláírása, hogy a támadók ne tudjanak új fejlécsorokat hozzáadni úgy, hogy közben az aláírás technikailag továbbra is érvényes maradjon. Emellett fontos szerepet kapott a **DNS-bejegyzések TTL-értékeinek megválasztása** is: a kulcsokhoz tartozó rekordokat úgy kell kezelni, hogy szükség esetén gyorsan lehessen kulcsot váltani, de közben a háttérrendszerek se kapjanak felesleges terhelést. A bemutatott gyakorlat szerint ehhez a gyorsítótárazás, az előtöltés és a háttérkiszolgálók tehermentesítése is szorosan hozzátartozik.

Az előadás másik fontos vonulata az volt, hogyan lehet **DNS-szinten felismerni és tompítani a visszaélésszerű forgalmat**. Ehhez nyílt forráskódú anomáliaészlelési megoldásokat, forgalomszabályozási technikákat és kernelközeli csomagszintű szűrést is bemutatott. A cél nem egyszerűen az volt, hogy a rendszerek „bírják a terhelést”, hanem hogy a legitim forgalom kiszolgálása mellett a visszaélésszerű lekérdezések hatását is csökkentsék. Külön kitért arra is, hogy a DKIM-rekordok CNAME-láncolása a gyakorlatban komoly teljesítmény- és késleltetési problémákat okozhat, ha a fogadó oldali szolgáltatók szigorú időkorlátokkal dolgoznak, és lépésről lépésre járják végig a feloldási láncot. Ilyen helyzetben a DNS teljesítménye közvetlenül befolyásolja az e-mailes hitelesítés megbízhatóságát.

A fő tanulság az volt, hogy az e-mailes hitelesség védelme **nem áll meg a levelezőszervereknél**. A DNS-réteg gyorsasága, gyorsítótárazási logikája, rekordstruktúrája és forgalomkezelése közvetlenül meghatározza, mennyire lesz ellenálló az egész hitelesítési lánc. A DNS ebben a megközelítésben valóban láthatatlan infrastruktúra, de éppen ezért különösen fontos, hogy ne pusztán működjön, hanem biztonsági szempontból is tudatosan legyen kialakítva.

Understanding What Makes DNS Abuse Easy: Operational Lessons for Defenders

(Maciej Korczynski @ Grenoble Alpes University / KOR Labs, FR)

A DNS-sel való visszaélések **nem egyenletesen oszlanak el** a domainregisztrációs ökoszisztémában: egyes regisztrátorok és szolgáltatási modellek lényegesen vonzóbbak a támadók számára, mint mások. Az előadás ezt a jelenséget a phishinghez használt, rosszindulatúan regisztrált domainek oldaláról vizsgálta, és arra kereste a választ, hogy mely működési és üzleti jellemzők csökkentik, illetve növelik a visszaélési kockázatot. A bemutatott kutatás szerint a támadók számára különösen kedvezőek az alacsony költségű regisztrációs modellek, az ingyenesen csomagolt kiegészítő szolgáltatások, valamint az automatizálást támogató folyamatok, például az alkalmazásprogramozási felületen keresztüli regisztráció vagy a könnyen tömegesíthető fióklétrehozás.

Ezzel szemben a szigorúbb **regisztrációs követelmények és az erősebb ellenőrzési lépések** egyértelműen kisebb visszaélési aránnyal társultak.

Az előadás egyik legfontosabb gyakorlati állítása az volt, hogy a védekező oldalnak **nemcsak a már aktív phishing domainekre kell reagálnia**, hanem magára a **regisztrációs környezetre is** érdemes figyelnie. Ha ismert, hogy mely regisztrátoroknál és milyen feltételek mellett jelenik meg aránytalanul sok rosszindulatú domain, akkor ez már önmagában hasznos kockázati jelzés lehet. Ez segítheti a megfigyelési prioritások kijelölését, a dúsítási és triázsolási folyamatok pontosítását, valamint azt, hogy a védekezés ne csak egyedi domainekre, hanem ökoszisztéma-szintű mintázatokra is épüljön. A beszéd szerint különösen fontos ezt azért megérteni, mert a phishing-kampányok jelentős része gyorsan cserélődő, eldobható domainekre támaszkodik, vagyis a visszaélés gazdaságossága és gyorsasága kulcsfontosságú szempont a támadók oldalán.

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

BBA+ BESZÁMOLÓ

Érdekes megállapítás volt, hogy bizonyos, intuitívan **fontosnak gondolt védekezési tényezők kisebb visszatartó hatással bírhatnak, mint várnánk**. Az egyik ilyen a **gyors utólagos intézkedés**, vagyis a domain felfüggesztésének sebessége. Az előadás szerint ez önmagában nem feltétlenül elég erős visszatartó tényező az egyszer használatos phishing-műveletekkel szemben, mert ezeknél a támadók eleve rövid élettartamú infrastruktúrával számolnak. Vagyis ha a rosszindulatú szereplő üzleti modellje arra épül, hogy gyorsan regisztrál, rövid ideig használ, majd továbblép, akkor az utólagos lekapcsolás csak korlátozottan növeli a számára jelentkező költséget. Ebből a szempontból az előadás inkább a megelőző súrlódások növelését tartotta fontosnak: azt, hogy már a regisztráció, a hitelesítés és a szolgáltatási hozzáférés fázisában váljon nehezebbé a tömeges visszaélés.

Az operatív következtetések ezért nem pusztán statisztikai jellegűek voltak. A bemutatott megközelítés szerint a védekező szervezetek használhatják ezeket az ismereteket arra, hogy **célzottabban figyeljék a magasabb kockázatú regisztrátorokat**, **korábban azonosítsák** a gyanús regisztrációs mintázatokat, és **eredményesebben működjenek együtt** a regisztrátorokkal, regisztrákkal és más érintett szereplőkkel. Az összkép alapján a phishing elleni fellépés nemcsak technikai szűrési vagy tiltási kérdésként jelent meg, hanem olyan területként is, ahol a szabályozási és üzemeltetési gyakorlat egymást erősítve növelheti a visszaélések költségét, miközben a legitim felhasználók terhelése még elfogadható szinten tartható.

Lessons Learned from Malicious Domain Measurement and Disruption

(Graeme Bunton @ NetBeacon, USA)

A rosszindulatú domainek elleni fellépés ebben az anyagban nem elméleti kérdésként, hanem nagy tömegű valós tapasztalatra épülő operatív problémaként jelent meg. A NetBeacon Institute az elmúlt években nagyszámú adathalászathoz és más visszaélésekhez használt domain jelentését támogatta, miközben folyamatosan mérte azt is, hogy ezeknél ténylegesen

mikor és milyen módon szűnik meg a károkozás. A beszéd egyik fő állítása az volt, hogy a **domainek elleni fellépés továbbra is értelmes és hatásos védelmi lépés**, de csak akkor, ha a jelentések jó minőségűek, a mérési módszertan kellően pontos, és a védekező oldal nemcsak egyedi domainekben, hanem kampányszintű mintázatokban gondolkodik.

Az egyik központi téma az volt, hogy a **mitigáció mérése jóval nehezebb**, mint elsőre látszik. Ha egy domain már nem oldódik fel, szerver- vagy ügyféloldali „hold" állapotba kerül, esetleg elsüllyesztett névszerverre mutat, az viszonylag jól értelmezhető. Sokkal nehezebb azonban megállapítani, mi történt akkor, ha a weboldal egyszerűen 403-as vagy 404-es hibát ad, esetleg más tartalmat szolgál ki. Ilyenkor nem mindig világos, hogy a regisztrátor, a tárhelyszolgáltató vagy maga a támadó változtatott-e az állapoton. A mérés ezért nemcsak arról szól, hogy a kár megszűnt-e, hanem arról is, hogy **ezt lehet-e hitelesen valamelyik szereplő beavatkozásához kötni**.

Az előadás szerint ez kulcskérdés, ha azt akarjuk megmondani, mely szolgáltatók reagálnak ténylegesen jól a visszaélésekre.

A bemutatott adatok alapján a megszüntetési arány összességében magas volt, sok **esetben 90% körüli**, és a legtöbb intézkedés viszonylag gyorsan, nagyjából két napon belül megtörtént. Ez önmagában biztató kép, ugyanakkor az előadó arra is rámutatott, hogy a gyorsabb reagálás mögött többféle ok állhat: egyrészt **javultak a jelentési gyakorlatok**, másrészt a regisztrációs **iparág is komolyabb nyomás alá került**, különösen azután, hogy az ICANN 2024-ben szigorúbb szerződéses kötelezettségeket vezetett be a rosszindulatú domainek kezelésére. Emellett az is látszott, hogy a támadók egyre gyorsabban elhasználható domainekkel dolgoznak, ami önmagában lefelé húzza a mérhető „élettartamot". Vagyis a gyors mitigáció nem minden esetben csak a védekező oldal javulását jelzi, hanem a támadói működés változását is.

Különösen érdekes volt a **jelentők minőségének kérdése**. Az előadás szerint nem minden visszaélésjelentés egyformán hatékony: a jó eredményt jellemzően a rövid, pontos, egyértelmű

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

BBA+ BESZÁMOLÓ

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

leírások, a támadott márka világos azonosítása és mindenekelőtt a képernyőképes bizonyítékok hozták.

A bemutatott példák alapján a **screenshot volt az egyik legerősebb előrejelzője** annak, hogy a domain ellen ténylegesen intézkedés történik. Ez különösen olyan regisztrátoroknál fontos, amelyek földrajzi vagy jogi okokból maguk nem tudják könnyen megtekinteni a rosszindulatú oldalt. Az előadás ebből azt a gyakorlati tanulságot vonta le, hogy a védekező közösségnek érdemes komolyan venni a jelentések minőségét, mert a rosszul összeállított bejelentések nemcsak alacsonyabb hatásfokkal működnek, hanem **összességében az egész ökoszisztéma reakcióképességét is rontják**.

A jövőre nézve a beszéd egyik legfontosabb eleme az volt, hogy az iparág **már nem maradhat meg az egy domain–egy jelentés** logikájánál. A phishingkampányok jelentős része ma már sorozatban előállított, hasonló nevű vagy azonos infrastruktúrára épülő domaineket használ, ezért egyetlen jól megalapozott jelentésből el kell tudni jutni a kapcsolódó domainek azonosításáig és közös kezeléséig. Az ICANN-nél zajló változások is ebbe az irányba mutatnak: a regisztrátoroknak várhatóan **nemcsak az egyedi bejelentett domaint kell majd vizsgálniuk**, hanem a **hozzá kapcsolódó más domaineket is**. Az összkép alapján az előadás fő mondanivalója az volt, hogy a rosszindulatú domainek elleni fellépés továbbra is fontos védelmi eszköz, de az igazán nagy hatás már nem az egyedi lekapcsolásokban, hanem a kampányszintű felismerésben, a jobb minőségű jelentésekben és az ökoszisztéma szereplőinek fokozatos felkészítésében rejlik.

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

Detecting Malicious Domain Registration Batches: Patterns, Prevalence, and Implications for Incident Response

(Carlos Gañán @ ICANN, NL)

A rosszindulatú domainek regisztrációja nem elszigetelt, egyedi esetekként jelennek meg, hanem **sokszor tömegesen**, **rövid idő alatt végrehajtott tevékenységként**. A bemutatott kutatás abból indult ki, hogy a támadók gyakran egyszerre nagyobb domain csomagokat regisztrálnak adathalász kampányokhoz, kártevőterjesztéshez vagy vezérlőszerver-infrastruktúrához, miközben a GDPR utáni környezetben a korábban jól használható WHOIS-alapú szereplőazonosítás jelentősen beszűkült. A vizsgálat ezért arra keresett új megoldást, hogy hogyan lehet a nyilvánosan továbbra is elérhető, „vékony” regisztrációs adatokból — például a regisztrátor, a névszerverek és a létrehozási idő alapján — ilyen tömeges regisztrációs mintázatokat felismerni.

A bemutatott módszer lényege az volt, hogy nem egy ismert rosszindulatú domainből indultak ki, hanem magukból a **regisztrációs eseményekből próbálták meg azonosítani** azokat a klasztereket, amelyek ugyanazon regisztrátoron, ugyanazokkal a névszerverekkel egymáshoz közeli időpontban jöttek létre. Ezt követően külön szűrési lépésekkel próbálták elkülöníteni a valóban gyanús csoportokat a legitim, például viszonteladói vagy tömeges üzleti regisztrációktól. A kutatás egyik fontos eredménye az volt, hogy a vizsgált időszakban az újonnan regisztrált gTLD domainek **legalább 16%-ánál volt kimutatható** ilyen hullámszerű regisztrációs minta.

Az is jól látszott, hogy bizonyos fenyegetéstípusok — különösen a spam — jóval gyakrabban épültek ilyen tömeges regisztrációra, mint más visszaélési kategóriák.

Az előadás gyakorlati jelentőségét az adta, hogy ez a megközelítés nemcsak leíró statisztikát adott, hanem **közvetlenül használható incidenskezelési előnyt is**. Ha egyetlen domain már

BBA+ BESZÁMOLÓ

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

felkerült egy tiltólistára, akkor a bemutatott klaszterezési módszer segítségével azonosítani lehetett az ugyanabba a regisztrációs hullámba tartozó további domaineket is. A kutatás szerint ezzel **jelentősen meg lehetett növelni** az ismert rosszindulatú domainek körét: egyetlen már ismert domainből kiindulva sok esetben több további, nagy valószínűséggel visszaélésszerűen használt domain is azonosíthatóvá vált, még azelőtt, hogy azok bármely fenyegetési adatforrásban megjelentek volna. Ez különösen **fontos operatív előny**, mert a védekező oldal így hamarabb reagálhat, és nem csak követheti a kampányokat, hanem részben meg is előzheti őket.

A bemutatott eredmények arra is rámutattak, hogy a tömeges regisztrációs minták és a visszaélések előfordulása között **statisztikailag kimutatható kapcsolat áll fenn**, vagyis egy regisztrátornál tapasztalható magasabb batch-regisztrációs arány jó előre jelzője lehet az emelkedett visszaélési kockázatnak. Ez az incidenskezelés, a fenyegetésfelderítés és a szabályozási oldal számára is fontos következményekkel járhat. A fő tanulság az volt, hogy a rosszindulatú domainek vizsgálatában érdemes nemcsak az egyedi domainekre, hanem a regisztrációs ökoszisztéma működési mintázataira is figyelni, mert ezekből korábban és nagyobb összefüggésben lehet felismerni a támadói infrastruktúrát.

The Role of Formal Verification in Isolating Critical Services

(David Cock @ Neutrality, CH)

David Cock azt a gondolatot állította a középpontba, hogy a számítástudományban régóta léteznek olyan formális módszerek, amelyekkel matematikailag igazolható egy szoftver viselkedése, mégis ezek ipari alkalmazása sokáig korlátozott maradt. Az előadás szerint azonban az elmúlt években a szoftververifikáció már nem pusztán akadémiai különlegesség, hanem fokozatosan **valódi mérnöki gyakorlattá válik**, és különösen a nagy kockázatú, kritikus rendszereknél érdemes újra komolyan venni.

A fő állítás az volt, hogy ma már bizonyos szoftverek esetében elérhető a gyakorlatban is használható, formálisan bizonyított **helyesség és elkülönítés**. Az előadó ezt nem elméleti jövőképként írta le, hanem olyan irányként, amely már **több valós ipari megoldásban is megjelent**. Külön kitért arra, hogy sok modern, biztonságosabbnak tekintett technológia – például a Rust nyelv bizonyos tulajdonságai – valójában ugyanebből a formális háttérből táplálkozik, csak részben automatizált, szűkebb formában. A különbség szerinte az, hogy míg ezek a megoldások fontos előrelépést jelentenek, addig a teljes formális verifikáció jóval erősebb garanciákat adhat: nemcsak azt, hogy egy program „valószínűleg" helyesebben működik, hanem azt, hogy **meghatározott tulajdonságok szerint bizonyíthatóan nem tud másképp viselkedni**.

Az előadás második fele ezt egy konkrétabb biztonsági problémán keresztül tette kézzelfoghatóvá: hogyan lehet **több virtuális gépet vagy szolgáltatást ugyanazon a fizikai hardveren** úgy futtatni, hogy azok egymástól való elkülönítése ne **csak tervezési elv legyen, hanem bizonyított tulajdonság**. A bemutatott megközelítés szerint egy formálisan igazolt hipervizor vagy mikrokernel képes olyan izolációs garanciákat adni, amelyekkel kizárható például, hogy **az egyik vendégrendszer memóriát olvasson a másikból**, módosítsa annak végrehajtható állományait, vagy **bármilyen nem kívánt módon befolyásolja annak működését**. Ez különösen olyan környezetekben fontos, ahol az elkülönítés meghibásodása nem egyszerűen hibát, hanem komoly biztonsági vagy rendelkezésre állási problémát okozna. A hangsúly tehát nem azon volt, hogy egy újabb virtualizációs termékről van szó, hanem azon, hogy a kritikus szolgáltatások szeparációját erősebb bizonyossággal lehessen megvalósítani.

Az előadó ugyanakkor nem hallgatta el a nehézségeket sem. A formálisan verifikált szoftver nem azért költséges, mert maga a bizonyítás „luxus", hanem azért, mert **rendkívül fegyelmezett tervezést, pontos specifikációt és következetes mérnöki munkát igényel**. Vagyis a pluszköltség jelentős része valójában abból fakad, hogy a fejlesztés során nem lehet

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

BBA+ BESZÁMOLÓ

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

megspórolni azokat a lépéseket, amelyeket a hagyományos szoftverprojektek gyakran eleve elnagyolnak vagy elhagynak. Az előadás fő tanulsága ebből az volt, hogy a formális verifikáció nem minden rendszerhez indokolt, de azoknál a szolgáltatásoknál, ahol a meghibásodás vagy kompromittálódás következménye kiemelkedően súlyos, érdemes lehet **más költség–haszon logikával gondolkodni**. Ebben a megközelítésben a formálisan igazolt izoláció nem elméleti többlet, hanem olyan minőségi ugrás, amely alapvetően változtatja meg az üzemeltetői kockázatokat és döntési lehetőségeket.

What the Fuzz? Thorough Testing of Systems and Configurations

(Mathias Payer @ EPFL (HexHive), CH)

A szoftverhibák ebben az előadásban nem kivételes eseményekként, hanem a **modern, nagyméretű rendszerek természetes velejárójaként jelentek meg**. Mathias Payer abból indult ki, hogy az internet gerincét ma rendkívül összetett szoftverhalmok alkotják: böngészők, operációs rendszerek, kernelkomponensek, hálózati szolgáltatások, virtualizációs rétegek és felhőplatformok egymásra épülő világa. Ezekben a hibák nemcsak gyakoriak, hanem sok **esetben kihasználhatók is**. Az előadás egyik alapállítása az volt, hogy ezt a helyzetet nem lehet teljesen megszüntetni, ezért a cél nem a hibamentesség idealizált ígérete, hanem az, hogy a lehető legtöbb hibát minél korábban megtalálják, mielőtt támadók fordítják őket saját hasznukra.

A fuzz tesztelést ennek megfelelően úgy mutatta be, mint a **jelenlegi legpraktikusabb és legeredményesebb hibakeresési technikát**. A módszer lényege az, hogy a célprogram sokféle, részben véletlenszerűen, részben visszacsatolással irányítva előállított bemenetet kap, miközben a tesztelő figyeli, hogy a program **mely kódrészei futnak le**, illetve **hol omlik össze vagy viselkedik hibásan**. A fontos előrelépést nem önmagában a véletlenszerű tesztelés adta, hanem az, hogy a korszerű fuzzerek visszajelzést kapnak a program belső állapotáról, és ezt felhasználva

egyre célzottabban keresik az új viselkedési útvonalakat. Ez tette lehetővé, hogy a fuzz tesztelés ne csak kisebb komponenseken, hanem rendkívül összetett rendszereken — például böngészőkön, Linux kernelrészeken vagy Android összetevőkön — is hatékony legyen. Az előadásból az a kép rajzolódott ki, hogy ez a terület az elmúlt tíz évben kifejezetten gyors fejlődésen ment keresztül, és ma már valós fejlesztési és üzemeltetési döntéseket is befolyásol.

A gyakorlati nehézségek között külön hangsúlyt kapott, hogy a fuzz tesztelés nemcsak hibákat talál, hanem **rengeteg összeomlást és rendellenes állapotot is termel**, amelyeket utólag csoportosítani, értelmezni és rangsorolni kell. Az előadó szerint ez ma már önmagában skálázási probléma: a sikeres fuzz tesztelés után nem az a kérdés, hogy van-e hiba, hanem az, hogyan lehet a több tízezer vagy akár több százezer összeomlás közül gyorsan megtalálni a valóban fontos, kihasználható vagy rendszerszintű következményekkel járó hibákat. Ennek kezelésére olyan újabb módszereket mutatott be, amelyek **automatikusan klaszterezik** a hibákat, illetve **megpróbálják megbecsülni azok súlyosságát és kihasználhatóságát**. A cél ezzel nem a fejlesztők tehermentesítése önmagában, hanem az, hogy a javítási kapacitást a legfontosabb problémákra lehessen összpontosítani.

Az előadás utolsó része már a jövő irányait érintette. Payer szerint a mesterséges intelligencia a hibakeresésben várhatóan **egyre nagyobb szerepet kap**, különösen abban, hogy nagy kódbázisokban gyorsabban találjon gyanús mintázatokat, majd ezeket más technikákkal – például fuzz teszteléssel – validálni lehessen. Ugyanakkor azt is hangsúlyozta, hogy a hibák gyorsabb felismerése önmagában még nem oldja meg a problémát: szükség van **jobb elkülönítési megoldásokra**, **világosabb komponenshatárokra** és olyan **rendszerszintű tervezési módszerekre** is, amelyek csökkentik egy-egy hiba hatását. Az összkép alapján az előadás fő tanulsága az volt, hogy a fuzz tesztelést nem érdemes kizárólag hibavadászok vagy szoftverfejlesztők speciális eszközének tekinteni. A kritikus infrastruktúrát működtető rendszerek esetében ez egyre inkább olyan gyakorlati módszerré válik, amelyet az

BBA-PLUSZ-31.2-24-2024-00004. sz. pályázat részeként

BBA+ BESZÁMOLÓ

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

üzemeltetőknek és a védelmi oldalon dolgozóknak is érdemes beemelniük a robusztusabb működés kialakításába.

Behind the Scenes of Cybersecurity at Eurovision Song Contest 2025

(Carlos Verde, Olivier Spielmann @ Senthorus, CH)

Az Eurovíziós Dalfesztivál kiberbiztonsági védelme nem egyetlen informatikai rendszer biztosításaként merül fel, hanem egy rendkívül összetett, időkritikus és nagy nyilvánosságú rendezvény teljes működésének védelmeként. A 2024-es svájci győzelem után a szervezőknek nagyjából egy évük maradt arra, hogy a következő eseményt megtervezzék és lebonyolítsák, de a kiberbiztonsági keretek tényleges kialakítására ennél jóval kevesebb idő állt rendelkezésre. A kihívást tovább növelte, hogy **nem egyetlen szervezetről volt szó**: az eseményben egyszerre vett részt az EBU, az SRG és Basel városa, illetve kantonja, vagyis három eltérő működésű szereplőnek kellett közös biztonsági modellt kialakítania. A beszámoló alapján a legfontosabb korai felismerés az volt, hogy **a védelmet csak közös irányítással és napi szintű összehangolással lehetett kezelni**.

A kockázati kép ennek megfelelően több rétegből állt. Egyrészt számolni kellett klasszikus kiberveszélyekkel, például adathalászattal, szolgáltatásmegtagadási támadásokkal, hamis információs kampányokkal és jogosulatlan videóközvetítésekkel. Másrészt a geopolitikai és aktivista kitettség is valós volt, különösen az aktuális nemzetközi helyzet miatt. Harmadrészt a fizikai biztonság és a kiberbiztonság több ponton összekapcsolódott, hiszen egy ilyen rendezvénynél egy kibertámadás akár a műsorfolytonosságot vagy a helyszíni működést is veszélyeztethette. Az előadók szerint a védelem célját ezért három pontban foglalták össze: az emberek védelme, a rendezvény zavartalan lebonyolítása és Svájc reputációjának megőrzése.

A technikai kihívásokat elsősorban az okozta, hogy a fő helyszínen **több mint húsz különböző beszállító és szolgáltató saját rendszerekkel, saját hálózatokkal és eltérő protokollokkal**

dolgozott. Egy ilyen környezetben nem volt reális elvárás, hogy minden partner ugyanazokat a végpontvédelmi vagy naplózási megoldásokat vezesse be. Emiatt a csapat inkább hálózati szintű láthatóságot épített ki: érzékelőpontokat helyeztek el a főbb kapcsolódási pontokon, és a forgalomból próbálták meg megérteni, mi számít normális működésnek, illetve mi tér el ettől veszélyes módon. A beszámoló szerint a próbák és főpróbák különösen fontosak voltak, mert ezek alapján tudtak alapállapotot képezni a hálózati viselkedésről. A későbbi élő műsorok során a tényleges forgalmat ehhez a mintázathoz hasonlították, és így tudták gyorsan kiszűrni azokat az eltéréseket, amelyek további vizsgálatot igényeltek. Ez azért volt lényeges, mert az esemény idején óránként igen **nagy mennyiségű hálózati eseményt kellett kezelni**, és csak automatizáltabb logikával, előre elkészített játékkönyvekkel lehetett ezt operatívan kézben tartani.

A működés másik fontos pillére a **megelőző munka** volt. A csapat nemcsak valós idejű észlelésre támaszkodott, hanem jelentős hangsúlyt helyezett a fenyegetésfelderítésre, a beszállítói kockázatok felmérésére, a kulcsfontosságú eszközök azonosítására és a show-folytonossági tervezésre is. Külön együttműködtek a helyi rendőrséggel és más szereplőkkel, hogy a kibertérben megjelenő aktivitásokat a fizikai kockázatokkal össze tudják vetni. A valós incidensek között **volt bombafenyegetés, szolgáltatásmegtagadási támadás, hamis információs kampány és jogosulatlan streamelési tevékenység is**, de az előadás szerint ezek közül egyik sem vált valódi műsormegszakító eseménnyé. A fő tanulság az volt, hogy egy ilyen látható, időkritikus eseménynél a siker nem egyetlen technológiai eszközön múlik, hanem azon, hogy a biztonsági csapat mennyire tud előre gondolkodni, több szervezetet összehangolni, és a technikai, műveleti, kommunikációs és fizikai nézőpontokat egy közös védelmi keretbe rendezni.

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

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

Using passive DNS (and more) for Threat Research and creating your own CTI

(Tom Ueltschi @ Swiss Post CERT, CH)

A kutatás kiindulópontja az volt, hogy ha egy szervezet nagy mennyiségben képes kiszűrni és elkülöníteni a rosszindulatú e-mail mellékleteket, akkor ezek önmagukban is értékes nyersanyagot adnak egy saját fenyegetéskutatási rendszerhez. A bemutatott megközelítés szerint a mellékletekből **automatikusan futtatott kártevőelemzés segítségével** ki lehet nyerni a vezérlőszerverekre, malware-családokra és kampányokra vonatkozó adatokat, majd ezeket strukturált formában el lehet tárolni és tovább lehet dúsítani. A hangsúly azon volt, hogy ehhez ma már nem feltétlenül szükséges teljesen egyedi fejlesztés: sok részfeladat nyílt forráskódú eszközökkel is megoldható.

A munkafolyamat központi eleme egy saját, fájlokra és egyszerű szkriptekre épülő hírszerzési környezet volt, amelyben a rosszindulatú mellékletek elemzése, a mintákból kinyert vezérlési címek összegyűjtése, majd ezek MISP-ben való tárolása és összekapcsolása történt meg. A bemutatott gyakorlat szerint a MISP itt nemcsak tárolóként szolgált, hanem olyan központi csomópontként is, ahonnan a kutató vissza tudott térni a kapcsolódó IP-címekhez, domainekhez, fájlmintákhoz és kampányokhoz. A passzív DNS-adatok különösen fontos szerepet kaptak, mert ezek tették lehetővé, hogy a **már ismert vezérlőszerverekhez újabb domaineket és IP-címeket lehessen kapcsolni**, ezáltal tágabb infrastruktúraképet lehessen felépíteni. Az előadás egyértelműen azt az irányt képviselte, hogy a nyers indikátorok önmagukban keveset érnek; az igazi érték az összefüggések feltárásában van.

Különösen érdekes volt a NetBIOS-nevek felhasználása klaszterezési célra. A bemutatott kutatás szerint bizonyos, az internetre kinyitott RDP- vagy SMB-szolgáltatásokat futtató Windows-gépek NetBIOS-nevei megfigyelhetők különféle szkennelő platformokon, és ezek alapján olyan kapcsolatok tárhatók fel, amelyeket a klasszikus passzív DNS önmagában nem mutatna meg.

Ha ugyanaz a NetBIOS-név több, látszólag különálló vezérlési IP-címnél is felbukkan, az segíthet azonosítani, hogy valójában ugyanahhoz a fenyegetési klaszterhez tartoznak. Az előadásban több példát is bemutatott arra, hogyan lehet egy-egy ilyen klasztert hosszabb időn keresztül követni, összekapcsolni korábbi malware-mintákkal, valamint a célba vett szervezetek vagy címzettek körével. Ez a megközelítés kifejezetten operatív hasznot adott, mert a különböző fertőzési hullámok, malware-családok és infrastruktúraelemek így nem elszigetelt megfigyelésekként, hanem **tartósan újrahasznált támadói környezetként** jelentek meg.

Az elemzés végül a dinamikus DNS-szolgáltatásokon és regisztrációs e-mail-címeken keresztül még tovább ment: bizonyos esetekben a kutató nyilvános és korlátozott hozzáférésű szolgáltatások kombinálásával regisztrációs e-mail-címeket, sőt személyes adatokhoz közelítő nyomokat is talált, amelyek segíthettek a támadói oldalon használt perszónák vagy szereplők azonosításában. Ez már nemcsak technikai klaszterezést, hanem **potenciálisan bűnüldözési szempontból is érdekes összefüggéseket adott**. Az összkép alapján az előadás fő tanulsága az volt, hogy egy jól felépített, akár viszonylag egyszerű eszközökre támaszkodó saját CTI-folyamat is képes hosszabb távon értékes, mély összefüggéseket feltárni — különösen akkor, ha a malware-elemzés, a passzív DNS, a NetBIOS-alapú klaszterezés és az e-mailes támadásokból származó célpontadatok egy közös elemzési logikába kerülnek.

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

NEMZETI KIBERBIZTONSÁGI INTÉZET

BBA+ BESZÁMOLÓ

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

Identity & Access Management Conference 2026

2026. március 17.

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

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

A Nemzeti Kiberbiztonsági Intézet munkatársai **2026. március 17-én** részt vettek a **Stocholmban** megrendezésre kerülő **Identity & Access Management Conference 2026** eseményen.

Az IAM Conference Sweden egy éves szakmai rendezvény, amely az **azonosítás- és hozzáférés-kezelés (IAM)** legfontosabb aktuális kérdéseire fókuszál. Célja, hogy átfogó képet adjon a digitális azonosítás, a hozzáférés-kezelés, a privilégiumkezelt hozzáférések, a zéró bizalmi működési modellek és a felhőbiztonság legújabb fejlődési irányairól. A konferencia gyakorlati nézőpontból mutatja be, hogyan alakítják át az új technológiák és a szabályozási környezet változásai a területet, valamint milyen válaszokat adhatnak mind erre a szervezetek.

A konferencia 2026-os központi témája az azonosítás és hozzáférés-kezelés szerepe egy elsődlegesen **felhőalapú és mesterséges intelligencia által formált világban**. A rendezvény azt vizsgálta, hogyan változtatják meg a mesterséges intelligenciára épülő megoldások, a felhőnatív architektúrák és a digitális tárcák az IAM-gyakorlatot, és ezek milyen lehetőségeket, illetve kihívásokat jelentenek a szervezetek számára biztonsági, felhasználói élmény és megfelelőségi szempontból. Az IAM Conference Sweden egyúttal találkozási pontot is biztosított a terület szakemberei, iparági vezetői és megoldásszállítói számára. A program lehetőséget adott arra, hogy a résztvevők bevált gyakorlatokat ismerjenek meg, stratégiákat vitassanak meg, és tapasztalatot cseréljenek egymással.

Kiknek ajánlott a beszámoló megismerése?

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

A konferencia legfontosabb előadási az alábbiakban foglalhatók össze.

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

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

AI Security Unlocked:
Defending Identity in the Age of Intelligent Threats

(Michiel Stoop, azonosítási és hozzáférés-kezelési terület igazgató, Philips)

Michiel Stoop előadásában azt mutatta be, **hogyan alakítja át a mesterséges intelligencia a kiberbiztonságot** és ezen belül **különösen az azonosítási és hozzáférés-kezelési területet**. Kiemelte, hogy a mesterséges intelligencia ma már nem csupán hatékonyságnövelő eszköz, hanem egyre inkább a vállalati működés és a digitális szolgáltatások szerves része, ezért a használatát nem lehet pusztán technológiai kérdésként kezelni. A Philips példáján keresztül érzékeltette, hogy az egészségügyi technológiai környezetben a szoftverek, az adatok és az intelligens rendszerek egyre szorosabban kapcsolódnak egymáshoz, így a mesterséges intelligencia használata közvetlenül érinti a betegekhez, szakemberekhez és üzleti folyamatokhoz kapcsolódó adatkezelést is.

Az előadás egyik alapvető gondolata az volt, hogy a mesterséges intelligencia egyszerre jelent **komoly lehetőséget és komoly kockázatot**. Egyrészt gyorsítja a munkát, segíti a döntéselőkészítést és növeli a hatékonyságot, másrészt viszont sok esetben hiányoznak a beépített biztonsági korlátok, ezért ellenőrizetlen használata adatvédelmi, hozzáférés-kezelési és működésbiztonsági problémákat okozhat. Stoop ezt azzal a hasonlattal tette szemléletessé, hogy a mesterséges intelligenciát a szervezeteknek **fokozatosan digitális munkatársként kell kezelniük**. Ma még többnyire asszisztensként működik, később viszont már több intelligens szereplő is együtt dolgozhat egy feladaton, végső soron pedig részben önálló döntéseket is hozhat. Minél inkább ebbe az irányba haladunk, annál fontosabbá válik, hogy ezeknek a rendszereknek világos korlátokat, jogosultságokat és felügyeleti mechanizmusokat szabjunk.
Részletesen végigvette, hogy a mesterséges intelligenciára épülő rendszerek biztonsági kockázata nem pusztán magából a nyelvi modellből fakad, hanem abból, amikor **azt külső**

adatforrásokkal, tudásbázisokkal, alkalmazásokkal és más, önálló működésre képes összetevőkkel kapcsolják össze. Ilyenkor a rendszer már nemcsak válaszol, hanem keres, összekapcsol, értelmez, sőt akár műveleteket is végrehajt. Ebben a környezetben jelenik meg például a hibás következtetés vagy az úgynevezett „hallucináció" veszélye is, amikor a rendszer meggyőző formában ad pontatlan vagy kifejezetten hibás választ. Még nagyobb problémát jelentett az a helyzet, amikor több ilyen intelligens szereplő egymással is kapcsolatba lépett, mert ilyenkor már nehezen követhető, hogy pontosan milyen adatból, milyen engedéllyel és milyen döntési logika mentén jutottak el egy adott eredményig.

Az előadás identitás- és hozzáférés-kezelési szempontból arra mutatott rá, hogy a jövőben már nemcsak embereknek és hagyományos alkalmazásoknak kell jogosultságokat kezelni, hanem a **mesterséges intelligenciára épülő digitális szereplőknek is**. Ezeknek is kell tulajdonos, életciklus, engedélyezési logika, nyomon követhetőség és szükség esetén leállítási lehetőség. Stoop hangsúlyozta, hogy a hagyományos szerepköralapú jogosultságkezelés önmagában már nem lesz elegendő: finomabb, körülményekhez, adatokhoz és konkrét feladatokhoz igazodó engedélyezésre lesz szükség. Ugyanilyen fontosnak nevezte az **érzékeny adatok osztályozását**, **maszkolását, a jogosultságok láncolódásának megakadályozását** és a műveletek **teljes körű naplózhatóságát** is.

A Philipsnél ennek érdekében már kialakítottak egy saját, mesterséges intelligenciára vonatkozó biztonsági megközelítést és egy érettségi modellt, amely az azonosítási és hozzáférési biztonságot, az adatvédelmet, a működés közbeni védelmet és a megfigyelhetőséget egyaránt figyelembe vette. Stoop szerint jelenleg még inkább az alapozási szakaszban járnak: szabályokat, architektúra-elvárásokat, biztonsági ellenőrzéseket és értékelési szempontokat dolgoztak ki, valamint elkezdték ezek alapján vizsgálni az új mesterséges intelligencia alapú megoldásokat. A következő lépések között említette az **engedélyezett alkalmazások körének kijelölését**, a **nem jóváhagyott megoldások visszaszorítását**, a **biztonsági műveleti központ bevonását** és a **technikai követelmények szervezeti szintű szabványosítását**. Az előadás végső üzenete az

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

BBA+ BESZÁMOLÓ

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

volt, hogy a mesterséges intelligencia biztonsága nem halasztható kérdés: a technológia gyors terjedése miatt a szervezeteknek már most ki kell alakítaniuk azokat a korlátokat és ellenőrzési pontokat, amelyekkel ezeket a rendszereket valóban biztonságosan lehet működtetni.

Assembling Access:
Custom Authorizations Meets Open Policy Agent at IKEA

(Johan Finndahl, tervezési menedzser és hozzáférés-szabályozási vezető, IKEA Group)

A hozzáférés-kezelés az IKEA-nál nem egyszerűen informatikai háttérfeladatként jelent meg, hanem olyan működési alapkérdésként, amely **közvetlenül befolyásolja ki, hol, mikor és milyen célból férhet hozzá az egyes rendszerekhez**. Egy ekkora, országokon és szervezeti szinteken átívelő vállalatnál a jogosultságok kezelése már nem tartható kézben kizárólag hagyományos szerepkörökkel vagy egyszerű csoportlogikával. A szervezeti méret, a bolti működés, a fejlesztői környezetek és a gyorsan változó üzleti igények együtt olyan összetett helyzetet hoztak létre, amelyben újra kellett gondolni, hogyan lehet a hozzáféréseket egyszerre központilag irányítani és mégis rugalmasan kezelni.

Az előadás első felében az IKEA saját fejlesztésű jogosultságkezelő szolgáltatása, az **Åtkomst** került a középpontba. Ezt a megoldást kifejezetten a jogosultságkezelés egyszerűsítésére tervezték, és három fő eleme a **szerepköralapú hozzáférés-kezelés**, a hierarchiára **épülő jogosultsági logika és a központi adminisztráció**. A rendszer lényege az, hogy az alkalmazások saját jogosultságokat és szerepköröket definiálhatnak, ezeket pedig egy hierarchikus szerkezethez lehet kötni. Így a hozzáférések nemcsak általános értelemben kioszthatók, hanem konkrét országokhoz, boltokhoz vagy más szervezeti egységekhez is kapcsolhatók. Ez jól

illeszkedett ahhoz a célhoz, hogy a megfelelő ember a megfelelő időben a számára szükséges alkalmazáshoz jusson hozzá.

Ez a modell ugyanakkor idővel elérte a határait. Egy idő után **már nem volt elég** azt megmondani, hogy valakinek van-e jogosultsága egy boltban vagy rendszerben, hanem azt is vizsgálni kellett, hogy az adott helyzetben valóban végrehajthatja-e a konkrét műveletet. Az előadásban erre bolti példát is hoztak: a rendelés-összekészítési jogosultság önmagában nem volt elég, figyelembe kellett venni a tényleges beosztást és az egyéb korlátozó feltételeket is. Ugyanez a probléma jelent meg az alkalmazásprogramozási felületeknél és a fejlesztői platformoknál, ahol a hozzáférést már nemcsak általános jogosultságok, hanem konkrét hívásokhoz és környezetekhez kötött szabályok alapján kellett szabályozni.

Erre a problémára válaszul került előtérbe az **Open Policy Agent**, amelyet nem a meglévő szolgáltatás lecserélésére, hanem **annak kiegészítésére kezdtek használni**. Ennek a jelentősége abban állt, hogy a központi jogosultságkezelés meg tudott maradni alapnak, miközben az egyes alkalmazások és felületek saját, részletesebb szabályokat is érvényesíthettek. Vagyis az Åtkomst továbbra is megmondhatta, hogy **egy felhasználónak milyen alapjogosultságai vannak**, az Open Policy Agent pedig azt dönthette el, hogy az **adott kérés az adott pillanatban, az adott körülmények között ténylegesen engedhető-e**.

Az előadás egyik fontos tanulsága az volt, hogy a hozzáférés-kezelést ma már **nem lehet pusztán központi, merev és előre kiosztott jogosultságokra építeni**. Olyan megoldásokra van szükség, amelyek egyszerre biztosítanak központi irányítást, üzleti érthetőséget és helyi rugalmasságot. Ebben a megközelítésben a saját fejlesztésű jogosultságkezelő szolgáltatás továbbra is stabil alap maradhatott, az Open Policy Agent pedig olyan szabályalapú kiegészítést adott hozzá, amellyel a hozzáférési döntéseket közelebb lehetett vinni a tényleges használati helyzethez. Ettől vált a rendszer **nemcsak technikailag korszerűbbé**, hanem a mindennapi működés szempontjából is **jobban használhatóvá**.

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

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

Identity Management:
The European Love Story You Didn't Know You Needed

(Sadrick Widmann, ügyvezető igazgató, Widas ID)

Az előadó szerint a digitális önrendelkezés nem merül ki az adatok földrajzi helyében vagy a szabályozási megfelelésben, hanem elsősorban ott dől el, hogy **ki szabályozza a digitális belépési pontokat**, vagyis az azonosítás, a hozzáférés és a bizalom infrastruktúráját. Ennek megfelelően az identitásmenedzsmentet nem egyszerű támogató technológiaként, hanem a biztonság, a bizalom és a szervezeti ellenálló képesség alaprétegeként helyezte el.

Az előadás jelentős része **Európa digitális helyzetének értelmezésére épült**. Ennek középpontjában az az állítás állt, hogy az európai szervezetek ugyan egyre gyakrabban beszélnek digitális szuverenitásról, de a gyakorlatban továbbra is jelentős mértékben Európán kívüli infrastruktúrákra és szolgáltatókra támaszkodnak. A felhőpiaci függőség, a nem európai nagy szolgáltatók dominanciája, valamint az a jelenség, hogy sok európai szoftverszolgáltató is ezekre az alapokra épít, mind azt a képet erősítik, hogy a valódi választási szabadság jelenleg korlátozott.

Kritikus hangon szólt az európai szabályozási környezetről is, különösen arról, hogy a jó szándékú kezdeményezések **gyakran széttöredezett végrehajtásba torkollnak**. Az eIDAS példáján keresztül azt a benyomást erősítette, hogy a közös európai digitális keretek létrehozása önmagában nem elég, ha azok a gyakorlatban nehezen használhatók, túl bonyolultak vagy országonként eltérő módon valósulnak meg. Ebből az a következtetés rajzolódott ki, hogy a digitális szuverenitást nemcsak szabályozni kell, hanem **ténylegesen működő, piacképes és használható európai platformokkal is alá kell támasztani**.

Ennek megoldására került prezentálásra a CEDAS szolgáltatás. A vállalatot az előadás

következetesen európai, hosszú távon gondolkodó, családi tulajdonú identitáskezelési szolgáltatóként pozicionálta, amely európai infrastruktúrára épít, és tudatosan az európai digitális önrendelkezés narratívájához kapcsolja magát. A cég a hagyományos tanácsadási projektekből jutott el egy önálló termékig, mert meglátásuk szerint szükség volt olyan identitás- és hozzáférés-kezelési megoldásra, amely jobban illeszkedik az európai adatvédelmi és működési elvárásokhoz.

Az egyik legfontosabb állítás az volt, hogy az identitásmenedzsment Európában stratégiai **jelentőségű terület,** és aki ezen a rétegen kontrollt szerez, az a digitális bizalom felett is nagyobb befolyást nyer.

Beyond Privilege: Modern PAM for a Dynamic, Hybrid World

(Matt Sturman, megoldástervezési igazgató, BeyondTrust)

Ez az előadás abból indult ki, hogy a növekvő biztonsági költések és a szigorodó megfelelőségi elvárások ellenére a **kiberkockázat továbbra sem csökken érdemben**. Ennek egyik fő oka az volt, hogy a támadók továbbra is azonosítási és jogosultsági gyengeségeket használnak ki, különösen azokat a rejtett jogosultsági útvonalakat, amelyeken keresztül fokozatosan magasabb szintű hozzáféréshez juthatnak. Az előadás szerint a hagyományos privilégiumkezelési megoldások **gyakran túl szűken értelmezik a problémát**, mert elsősorban a klasszikus kiemelt jogosultságú fiókokra összpontosítanak, miközben a valós kockázat sokszor a hétköznapi felhasználóktól induló, **egymásra épülő jogosultsági kapcsolatokban rejlik**.

A hangsúly ezért egy korszerűbb, identitásközpontú privilégiumkezelési megközelítésre került,

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

BBA+ BESZÁMOLÓ

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

amely nemcsak a rendszergazdai vagy technikailag kiemelt fiókokat védi, hanem minden olyan felhasználót és hozzáférést figyelembe vesz, amelyből emelt jogosultság vagy érzékeny hozzáférés vezethető le. Ez különösen fontos a hibrid környezetekben, ahol helyi rendszerek, felhőszolgáltatások, különféle identitásforrások és eltérő jogosultsági modellek működnek együtt. Az előadás alapján a modern privilégiumkezelés célja nem pusztán a hozzáférések zárolása vagy a jelszavak kezelése, hanem **a jogosultsági viszonyok átláthatóbbá tétele**, a **kockázatos hozzáférési útvonalak feltárása és a hozzáférések egyszerűbb, de szigorúbb szabályozása**.

Az ismertetett megközelítés kitért arra is, hogy az újabb, önállóbb működésre képes mesterséges intelligencia alapú megoldások támogathatják a védekezést. Ezek szerepe elsősorban abban jelenhet meg, hogy gyorsabban azonosítják a rejtett jogosultsági összefüggéseket, segítik a folyamatos felügyeletet, és rugalmasabban tudnak reagálni a változó kockázatokra. Az előadás összességében azt hangsúlyozta, hogy a privilégiumkezelést ma már nem lehet pusztán technikai fiókok védelmére szűkíteni: a teljes identitási környezetet kell úgy kezelni, hogy a szervezet egyszerre maradjon védett és működőképes egy gyorsan változó fenyegetési környezetben.

Delegated, Dynamic, Scalable: What Modern B2B IAM Should Look Like

(Jochen Raymaekers, senior kiemelt megoldástervező, Ping Identity)

A külső partnerek, beszállítók és más harmadik felek hozzáférése ebben az előadásban már nem **mellékes technikai kérdésként jelent meg**, hanem **a vállalati működés egyik alapvető bizalmi és kockázatkezelési problémájaként**. A hangsúly azon volt, hogy a szervezetek jelentős része még mindig széttagolt eszközökkel és kézi folyamatokkal kezeli ezeket a hozzáféréseket,

miközben a támadások és incidensek egyre nagyobb része valamilyen partneri vagy beszállítói kapcsolaton keresztül jelenik meg. Ebből az következett, hogy a kockázat már nem áll meg a saját munkatársaknál, hanem **kiterjed a teljes külső kapcsolati hálóra** is.

A B2B azonosítási és hozzáférés-kezelést az előadás nem egyszerűen a munkatársi vagy ügyféloldali azonosítás egyik változataként kezelte, hanem önálló problémaként. Itt nemcsak az a kérdés, hogy valaki beléphet-e egy rendszerbe, hanem az is, hogy milyen partneri kapcsolat alapján, meddig, kinek a felügyelete mellett és pontosan milyen célból kap hozzáférést. Ennek kapcsán nagy hangsúlyt kapott a delegált adminisztráció, vagyis az, hogy a külső partner a saját felhasználóit maga kezelhesse, de ellenőrzött vállalati keretek között.

A „dinamikus" megközelítés alatt azt értette, hogy a hozzáférési döntéseket nem lehet kizárólag statikus szerepkörökre építeni. A döntéseknek figyelembe kell venniük az aktuális körülményeket, a kapcsolat típusát, a kérés érzékenységét és a kockázati szintet is. Az előadás ezt összekapcsolta a megszemélyesítés, a csalás és a mesterséges intelligenciával támogatott megtévesztés növekvő kockázatával, vagyis azzal, hogy a digitális bizalom fenntartásához ma már erősebb ellenőrzési és hitelesítési mechanizmusokra van szükség.

Securing Your Network with Zero-Trust

(Jaens Stafren, EMEA értékesítési vezető, Keeper Security)

Az előadás arra épült, hogy a hagyományos, többrétegű védelmi modell ma már önmagában **nem ad elegendő biztonságot a vállalati hálózatok számára**. A kiindulópont az volt, hogy a támadók egyre gyakrabban nem közvetlenül a technikai peremvédelmet próbálják áttörni, hanem jogosultságokkal, hitelesítési adatokkal és a különböző rendszerek közötti hézagokkal

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

élnek vissza. Ebben a környezetben a védelem nem alapulhat többé azon a feltételezésen, hogy ami a hálózaton belül van, az eleve megbízhatóbb, mint ami kívülről érkezik.

Az ismertetett megközelítés szerint a hálózat védelmét **zéró bizalmi elvre kell építeni**, vagyis minden hozzáférést, eszközt és műveletet folyamatosan ellenőrizni kell, függetlenül attól, hogy a kérés honnan érkezik. Ennek három hangsúlyos eleme jelent meg: a folyamatos hitelesítés, a legkisebb szükséges jogosultság elve, valamint az eszközszintű titkosítás. A folyamatos hitelesítés azt a célt szolgálta, hogy a belépés ne egyszeri ellenőrzés legyen, hanem a rendszer a **munkamenet során is újra és újra értékelje a felhasználó és az eszköz megbízhatóságát**. A legkisebb szükséges jogosultság elve pedig azt biztosította, hogy a felhasználók és rendszerek csak ahhoz férjenek hozzá, ami az adott feladat elvégzéséhez feltétlenül szükséges.

A fő üzenet az volt, hogy a zéró bizalmi modell nem egyetlen terméket vagy technológiát jelent, hanem egy **olyan biztonsági működési keretet, amelynek célja a jogosulatlan oldalirányú mozgás megakadályozása a hálózaton belül**. Ha egy támadó mégis bejut egy rendszerbe, a megfelelően kialakított hitelesítési, jogosultságkezelési és titkosítási rétegek jelentősen csökkenthetik annak esélyét, hogy onnan további rendszerekhez vagy érzékeny adatokhoz férjen hozzá.

Mastering PAM: Overcoming Challenges and Unlocking Value

(Sourabh Jaiswal, megoldástervező, Sandvik)

Ez az előadás a privilégiumkezelés gyakorlati bevezetésének tapasztalataira épült, és azt a kérdést járta körül, hogyan lehet a PAM-megoldásokat valóban **hasznos biztonsági eszközzé tenni**, nem pedig **pusztán megfelelőségi kötelezettséggé**. A kiindulópont az volt, hogy sok

szervezet ugyan bevezet valamilyen privilégiumkezelési rendszert, de azt végül csak egyfajta központosított jelszókezelőként használja, így a megoldás nem tudja betölteni azt a stratégiai szerepet, amelyre eredetileg hivatott lenne. Az előadás ezzel szemben azt hangsúlyozta, hogy a privilégiumkezelés akkor teremt valódi értéket, ha nem elszigetelt technikai projektként, hanem a **biztonsági működés és az üzemeltetési folyamatok szerves részeként kezelik**.

A hangsúly a valós bevezetési nehézségeken volt: a különböző iparágakban eltérő környezetek, eltérő örökölt rendszerek és eltérő működési szokások mellett a PAM bevezetése rendszerint **több szervezeti támogatást, egyeztetést és előkészítést igényel**, mint azt kezdetben gondolnák. Az előadás szerint a siker kulcsa nem csupán a technológia kiválasztása, hanem az is, hogy a szervezet pontosan meghatározza, mit akar védeni, kik a kiemelt jogosultságú felhasználók, milyen munkafolyamatokat kell támogatni, és hogyan lehet az új szabályokat úgy bevezetni, hogy azok ne bénítsák meg a napi működést.

A bemutatott fejlettebb funkciók közül különösen fontos szerepet kaptak a jelszavak automatikus cseréje, az állandó kiemelt jogosultságok visszaszorítása, az időben korlátozott jogosultságadás és az automatizált műveletek támogatása. Az előadás alapján a PAM valódi előnye ott mutatkozik meg, amikor ezek a képességek **együtt csökkentik a tartósan fennálló kockázatos hozzáféréseket**, **javítják az ellenőrizhetőséget**, és **közben az üzemeltetési folyamatokat is kiszámíthatóbbá teszik**. A fő tanulság az volt, hogy a privilégiumkezelés akkor válik valódi üzleti és biztonsági értékké, ha nem csak megfelelőségi eszközként tekintenek rá, hanem a jogosultságok felelős, időszakos és célhoz kötött kezelésének alapjaként.

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

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

Privileged Access, Smarter Choices: Driving Security and Cost-Effectiveness

(Sebastian Stauber, biztonsági tervező, Assemblin Caverion Group)

Az előadás a privilégiumkezelést nem elsősorban technológiai termékként, hanem **üzleti döntési és architekturális kérdésként közelítette meg**. A kiindulópont az volt, hogy a kiemelt jogosultságok kezelése ma már a vállalati biztonság egyik alapköve, de a sikeres bevezetéshez nem elég egy PAM-eszköz beszerzése és technikai telepítése. A valódi nehézség ott kezdődik, amikor meg kell indokolni a vezetés felé, hogy pontosan **milyen védelmi értéket teremt a privilégiumkezelés**, milyen kockázatokat csökkent, és miért éri meg erre költeni olyan környezetben, ahol a költségcsökkentés és a beruházások szigorú igazolása állandó elvárás.

Az előadó saját vállalati környezetéből indult ki, ahol a költséghatékonyság és a biztonság egyszerre jelent meg meghatározó szempontként. A szervezet több országban működő, összetett műszaki szolgáltatási környezetben dolgozott, ezért a **biztonsági döntéseket folyamatosan össze kellett vetni azzal, hogy mi valósítható meg ésszerű ráfordítással**. Ebben a helyzetben a privilégiumkezelés különösen érzékeny területnek bizonyult: mindenki tudja, hogy fontos, de nehezebb számszerűsíteni, hogy a különböző PAM-funkciók milyen konkrét üzleti eredményt hoznak. Az előadás egyik legfontosabb gondolata ezért az volt, hogy nem „tökéletes” privilégiumkezelési környezetet kell építeni, hanem olyan védelmi környezetet, amely a szervezet tényleges szükségleteihez és lehetőségeihez igazodik.

Ennek alátámasztására egy kockázatalapú biztonsági architektúra-megközelítést mutatott be. A logika szerint a tervezést nem alulról, a konkrét termékfunkciókból kell indítani, hanem felülről, az üzleti elvárások és a működési követelmények felől. Először azt kell tisztázni, hogy a szervezet **milyen alapvető értékeket és szolgáltatásokat akar védeni**, **milyen üzleti kiesést akar elkerülni, és milyen típusú jogosulatlan hozzáférések jelentik a legnagyobb**

fenyegetést. Ebből lehet levezetni, hogy milyen biztonsági szolgáltatásokra van szükség, majd ezekhez milyen konkrét kontrollok, végül pedig milyen technológiai megoldások illenek. Az előadás szerint ez a gondolkodásmód azért hasznos, mert így a vezetés számára is világosan megmutatható, hogy az egyes PAM-elemek nem önmagukért léteznek, hanem egy üzleti kockázat kezelését szolgálják.

Külön hangsúlyt kapott az a felismerés is, hogy a privilégiumkezelést nem szabad egyetlen eszközre vagy termékre leegyszerűsíteni. Az előadó inkább „privilégiumkezelési védelmi környezetről" beszélt, amely több egymáshoz kapcsolódó elemből állhat. Ide tartozhat a kiemelt fiókok védelme, a külön adminisztrátori azonosítók használata, a munkamenetek felügyelete és naplózása, az időkorlátos hozzáférések kiadása, a tartósan fennálló emelt jogosultságok csökkentése, valamint az, hogy a hozzáférések mennyire illeszkednek a zéró bizalmi elvekhez. Az előadásból az derült ki, hogy egyes környezetekben például a jelszótárolásnál vagy a munkamenet-kezelésnél is fontosabb lehet egy vállalati szintű „széf", vagyis a hitelesítő adatok és kiemelt hozzáférések rendezett, központi kezelése. Más esetben viszont éppen az időben korlátozott hozzáférés vagy a tartós jogosultságok megszüntetése adhatja a legnagyobb védelmi értéket. **Nem minden funkció egyformán fontos minden szervezetnél**, ezért a kiválasztást a kockázat és a várható haszon alapján kell elvégezni.

Az előadás másik fontos rétege az volt, hogy a **privilégiumkezelést a megfelelőségi keretektől sem lehet elszakítani**. Szóba kerültek azok a szabványok, ajánlások és szabályozási elvárások, amelyek közvetlenül vagy közvetve érintik ezt a területet. Az előadó több különböző kontrollrendszert és keretrendszert is említett, és azt hangsúlyozta, hogy ezekben rengeteg releváns követelmény található, de egy szervezet számára nem az a valódi kérdés, hogy „mindent" be kell-e vezetni, hanem az, hogy miből mire van ténylegesen szükség, milyen mélységben, és milyen érettségi szinten. Ez a megközelítés különösen fontos akkor, ha a biztonsági csapatnak **korlátozott erőforrásokból kell valódi eredményt elérnie**.

BBA-PLUSZ-31.2-24-2024-00004. sz. pályázat részeként

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

Összességében az előadás egyik fő tanulsága az volt, hogy a privilégiumkezelésről szóló jó döntés nem ott kezdődik, hogy melyik gyártó termékét választják, hanem **ott, hogy a szervezet képes-e világosan meghatározni a saját kockázatait, üzleti igényeit és célzott védelmi prioritásait**. A PAM valódi értéke akkor mutatható meg, ha a technológiai funkciók visszavezethetők az üzleti nyelvre: például a szolgáltatáskiesés csökkentésére, a kontrollálatlan kiemelt hozzáférések visszaszorítására, az auditálhatóság javítására vagy a megfelelőségi terhek kezelhetőbbé tételére. Az előadás így végül nem egyszerűen arról szólt, hogyan kell PAM-ot bevezetni, hanem arról, hogyan lehet a privilégiumkezelést tudatos, arányos és vezetői szinten is vállalható biztonsági beruházássá formálni.

Transforming IAM to Deliver Business Value

(Pär Kidman, azonosítás- és hozzáférés-kezelési vezető, Swedbank)

A Swedbanknál az volt a cél, hogy az azonosítási és hozzáférés-kezelést ne csupán technikai platformként vagy megfelelőségi kötelezettségként kezeljék, hanem olyan működési képességként, amely **kézzelfoghatóan hozzájárul a bank stratégiai céljaihoz**. A kiindulópont az volt, hogy a banknál ez a terület korábban erősen technológia- és megfelelőségközpontúan működött, ami önmagában nem szokatlan egy nagy, szabályozott pénzügyi intézménynél. Ugyanakkor a változó fenyegetési környezet, az üzleti oldal növekvő elvárásai és az új technológiai kezdeményezések miatt **világossá vált, hogy az IAM csak akkor tud valódi szervezeti értéket teremteni**, ha nem eszközkészletként, hanem stratégiai képességként kezelik.

A banki környezet bemutatása fontos keretet adott ennek a gondolatnak. A Swedbank nemcsak nagy ügyfélkörrel rendelkező pénzintézetként jelent meg, hanem olyan szereplőként is, amely

számos **társadalmilag kritikus funkciót támogat**, például fizetési infrastruktúrát, bérfizetési folyamatokat és más alapvető pénzügyi szolgáltatásokat. Ebből következően az azonosítási és hozzáférés-kezelési kontrollok nem egyszerűen belső informatikai védelmi elemek, hanem a működési stabilitás és a bizalom alapfeltételei. Az előadás egyik lényeges pontja az volt, hogy ebben a helyzetben a szervezet **nem engedheti meg magának a széttagolt felelősségi viszonyokat**, az átláthatatlan tulajdonosi modellt vagy a kizárólag technológiai szempontból szervezett IAM-működést.

Ennek megfelelően az egyik első lépés az volt, hogy a bank **egyetlen, végponttól végpontig felelős IAM-szervezetbe vonta össze a korábban széttagolt feladatokat**. A folyamatok, a költségkeret, a technológia, a kockázati és megfelelőségi szempontok egy vezetés alá kerültek. Ez nem csupán szervezeti egyszerűsítést jelentett, hanem azt is, hogy az IAM végre úgy tudott fellépni a bankon belül, mint önálló működési képesség, nem pedig mint több csapat között szétszórt technikai felelősség. Az előadás szerint ez teremtette meg annak alapját, hogy a területet a továbbiakban üzleti nyelven is értelmezhetővé tegyék.

A stratégiai átalakítás másik fontos eleme az volt, hogy az IAM-et tudatosan **a bank biztonsági irányvonalához és üzleti prioritásaihoz igazították**. Ennek keretében a hangsúly áttevődött a technológiáról arra, hogyan támogatja az IAM a biztonságos működést, a kockázatok csökkentését, az egyszerűbb munkavégzést és a jobb felhasználói élményt. Az előadásban többször visszatért az a gondolat, hogy az üzleti oldal nem architektúrákat és platformokat érzékel, hanem azt, **mennyire könnyű valakit beléptetni**, **mennyire gyors a jogosultságadás**, **mennyire stabilak a szolgáltatások, és mennyi felesleges súrlódást okoz a napi működésben a biztonság**. Emiatt az IAM-csapat először az alapok stabilizálására, a megbízhatóság növelésére és a kézi munkák csökkentésére összpontosított, majd erre építve kezdett el a teljes üzleti élmény javításáról beszélni.

BBA-PLUSZ-31.2-24-2024-00004. sz. pályázat részeként

BBA+ BESZÁMOLÓ

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

Az előadás egyik legkézzelfoghatóbb példája a korszerű, adathalászatnak ellenálló **többtényezős hitelesítés bevezetése volt**. A bank korábban intelligens kártyákra épített, amelyek ugyan biztonságosnak számítottak, de sok működési korlátot és kivételkezelést okoztak. Egyes munkakörökben például a felhasználóknak egyszerre több rendszeren kellett dolgozniuk, ami a kártya alapú hitelesítés mellett nehézkes volt, más esetekben pedig ellátási és logisztikai problémák jelentkeztek az eszközök beszerzésében és kiadásában. Az új megoldások – például a korszerűbb, adathalászatnak ellenálló hitelesítési módszerek – bevezetésével nemcsak a biztonság nőtt, hanem csökkent a kivételek száma, javult a rugalmasság, és egyszerűbbé vált több új üzleti felhasználási eset támogatása is. Az előadás ezt a példát arra használta, hogy megmutassa: az IAM valódi üzleti értéke ott válik láthatóvá, ahol a biztonsági fejlesztés egyszerre javítja a megfelelőséget, a működést és a felhasználói oldalt.

Az előadás összességében azt hangsúlyozta, hogy az azonosítási és hozzáférés-kezelés érettsége nem ott mérhető, hogy milyen sok technológiai komponenst vezettek be, hanem ott, **hogy ezek mennyire átláthatóan, skálázhatóan és üzleti szempontból is értelmezhetően támogatják a szervezet működését**. A Swedbank példája azt mutatta meg, hogy az IAM akkor tud valódi szervezeti támogatottságot szerezni, ha a technikai részletek helyett a kockázatcsökkentés, az egyszerűbb működés, a jobb felhasználói élmény és a stratégiai célok nyelvén is képes megszólalni.