NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 12. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- CTI JELENTÉS, RIPORT
- BBA+ BESZÁMOLÓ

NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍREK

Hogyan tegyük biztonságossá az AI-ügynököket?

(bleepingcomputer.com)

Az agentikus mesterséges intelligencia (Agentic AI) alapjaiban alakítja át a vállalatok működését. Az AI-ügynökök már nem csupán támogató eszközök vagy fejlett chatbotok, hanem autonóm rendszerek, amelyek képesek tervezni, döntéseket hozni és műveleteket végrehajtani. Kódot generálnak, adatokat mozgatnak, tranzakciókat hajtanak végre, és több rendszeren átívelően működnek, gyakran emberi felügyelet nélkül, folyamatosan és gépi sebességgel. **Bővebben...**

Az Instagram megszünteti a titkosított chatelést

(thehackernews.com)

A Meta 2026 májusától leállítja a végponttól végpontig terjedő titkosítás (E2EE) támogatását az Instagram csevegéseknél ugyanis – a cég elmondása szerint – nagyon kevés felhasználó használta a funkciót a platform direkt üzeneteinél (DM). Azok, akik továbbra is end-to-end titkosítással szeretnének chatelni, a tech óriás az azonnali üzenetküldő alkalmazását, a WhatsApp-ot ajánlja. **Bővebben...**

Facebook-hirdetésekben terjedő manipulált videók irányítják a felhasználókat befektetési csalások felé

(helpnetsecurity.com)

A Bitdefender kutatása egy kiterjedt, több országot és nyelvet érintő online csalási ökoszisztémát azonosított, amely a Meta közösségi platformjain futtatott rosszindulatú hirdetési kampányokon keresztül irányította az áldozatokat befektetési csalásokba. **Bővebben...**

A WebKitet érintő biztonsági frissítést adott ki az Apple

(apple.com)

Az Apple 2026. március 17-én kiadta az iOS 26.3.1 (a), iPadOS 26.3.1 (a), macOS 26.3.1 (a) és macOS 26.3.2 (a) Background Security Improvements frissítéseket, amelyek az iOS 26.3.1, iPadOS 26.3.1, macOS 26.3.1 és macOS 26.3.2 rendszereken érhetők el.
Bővebben...

Steam-en terjedő káros kódok után nyomoz az FBI

(techcrunch.com)

A Szövetségi Nyomozóiroda (FBI) Seattle-i részlege nyomozást folytat a Steam játékpiactérre feltöltött, káros kódokat tartalmazó játékokkal kapcsolatban. Az áldozatkereső felhívásban olyan felhasználók közreműködését kérik, akik telepítették az FBI által felsorolt játékok valamelyikét és/vagy olyan információkkal rendelkeznek, amelyek segíthetik a nyomozást.
Bővebben...

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

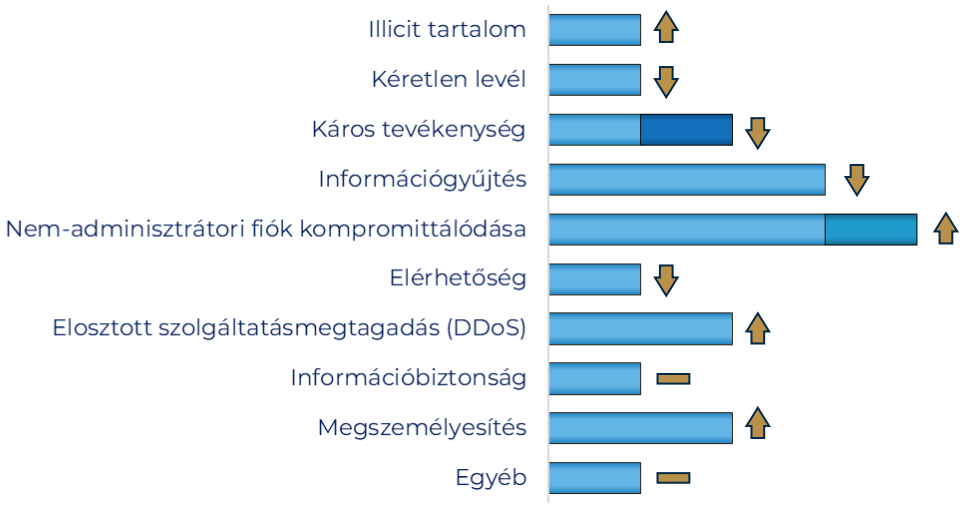
2026. 03. 13. — 2026. 03. 19.

Fenyegetettségi szint:

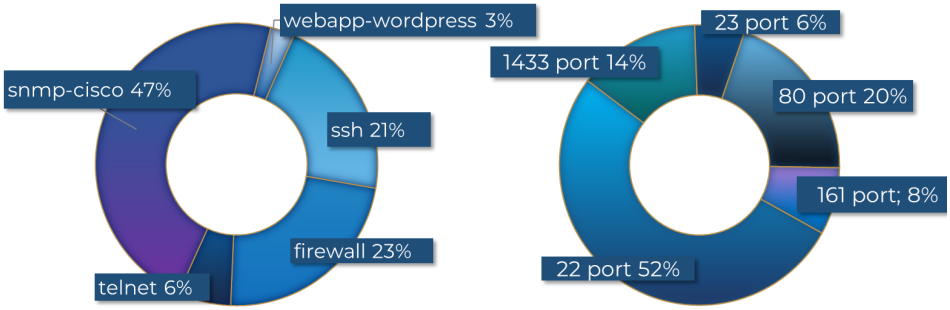
alacsony | közepes | **magas** | kritikus

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

HAVI CTI RIPORT

2026. február havi CTI riport

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet **havi rendszerességgel** ad ki **fenyegetéselemzést**, mely **összefoglalja** a **kibertér globális**, valamint **magyarországi helyzetét**. A riport megismerése megfelelő támpontot adhat az olvasó számára, hogy szervezete milyen IT biztonsági kihívásokkal nézhet szembe a közeli jövőben.

Elolvasom

Érdekli, hogyan formálhatják a jövőt a különböző kiberbiztonsági kihívások?

Fedezze fel velünk a legizgalmasabb témákat, a szakértői tippektől egészen a legújabb trendekig!
Kövesse podcastünket a legnépszerűbb felületeken!

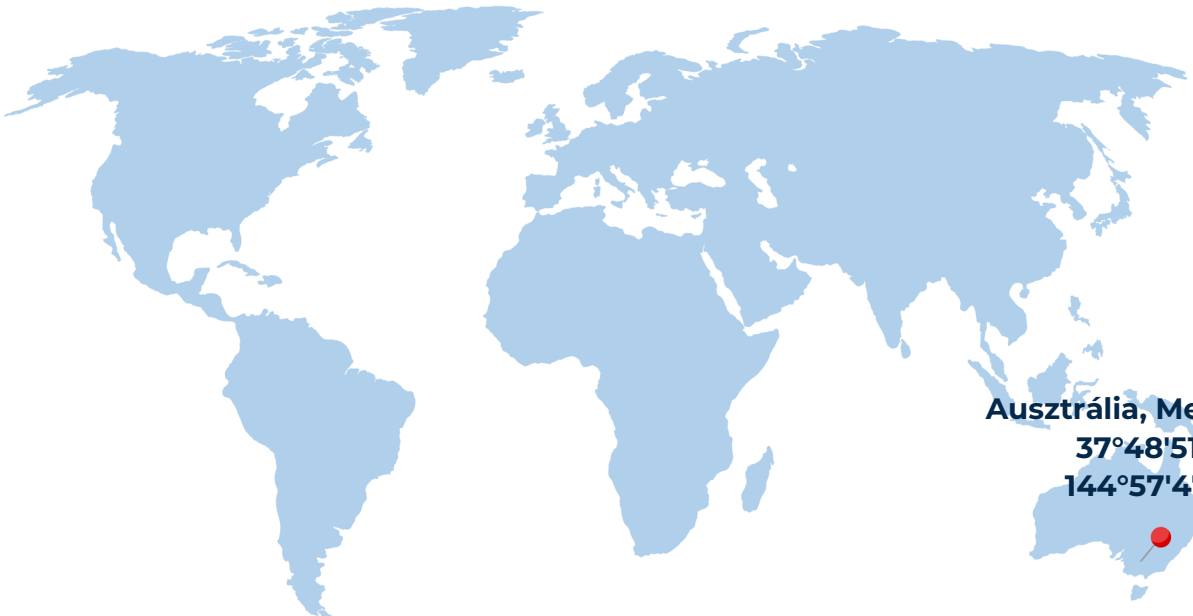
BBA+ BESZÁMOLÓ

COSAC APAC 2026 konferencia – Ausztrália, Melbourne

2025. február 24-26.

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-312-24-2024-00003. sz. pályázat részeként

BBA+ BESZÁMOLÓ

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

A Nemzeti Kiberbiztonsági Intézet munkatársai részt vettek a 2026. február 24-26. között a **Melbourne-ben** megrendezésre kerülő **COSAC APAC 2026** konferencián.

A rendezvény célja, hogy vezető szakértők, kutatók és iparági döntéshozók számára fórumot biztosítson a kiberbiztonság, információbiztonsági architektúrák és kockázatkezelési megközelítések legújabb trendjeinek és gyakorlati tapasztalatainak megvitatására. A konferencia egyik fő sajátossága az interaktív és kritikus szakmai párbeszéd: a szervezők tudatosan kerülik a hagyományos konferenciaformátumot, így nincsenek kereskedelmi kiállítók vagy értékesítési prezentációk, a hangsúly pedig a gondolatébresztő előadásokon és a résztvevők közötti szakmai vitákon van. A rendezvény ekképpen egy nemzetközi szakmai közösséget hoz össze, ahol a résztvevők nyitottan vitathatják meg az új megközelítéseket és innovatív biztonsági koncepciókat.

Kiknek ajánlott a beszámoló megismerése?

- Kiberbiztonsági szakértők, kutatók és iparági döntéshozók számára

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

BBA-PLUSZ-312-24-2024-00003 sz. pályázat részeként

Implementing the SABSA NIST CSF Community Profile

(Glen Bruce)

Az előadás az **NIST Cybersecurity Framework** (NIST CSF) **szerepét és korlátait vizsgálta**, rámutatva arra, hogy bár a keretrendszer meghatározza azokat az alapvető területeket, ahol kiberbiztonsági védelemre van szükség, a funkciók, kategóriák és alkategóriák jelenlegi struktúrája sok szervezet számára nem tekinthető teljeskörűnek. Bemutatásra került, hogy **az NIST** a hiányzó elemek pótlására a **Community Profile kiterjesztések létrehozását javasolja**, amelyek lehetővé teszik a keretrendszer iparágspecifikus, szabályozói vagy szervezeti igényekhez történő igazítását, ezáltal több szervezet számára alkalmazható, konkrét felhasználási esetekhez illesztett kiberkockázat-kezelési iránymutatás kialakítását. Az előadás középpontjában a **SABSA Institute** által támogatott **SABSA Enhance NIST Cybersecurity Framework** (SENC) **munkacsoport** projektje állt, amely olyan módszereket, eszközöket és útmutatókat fejleszt, amelyek segítségével a **NIST CSF 2.0 a SABSA biztonsági architektúra megközelítésével integrálható** a szervezetek működésébe. Ismertetésre került, hogy a projektcsapat elkészítette a NIST CSF kategóriáihoz és alkategóriáihoz illesztett SABSA üzleti attribútumok és attribútumprofilok példatárát, valamint jelenleg egy **SABSA-specifikus NIST CSF Community Profile kialakításán** dolgozik, amely új kategóriákat, illetve alkategóriákat tartalmaz a SABSA módszertannal összhangban. A bemutató egy első betekintést nyújtott ebbe a közösségi profilba, amely a célok szerint **megkönnyíti a CSF integrálását a biztonsági architektúrába**, és SABSA-specifikus implementációs példákon keresztül további gyakorlati iránymutatást biztosít a CSF alkategóriák alkalmazásához. Kiemelésre került az is, hogy az **NIST CSF alkalmazása** sok esetben elsősorban folyamatokra, technológiákra és kontrollokra koncentrál, miközben háttérbe szorul az üzleti érték és a kockázatok közötti kapcsolat; a **SABSA-alapú kiterjesztések és példák célja** ezért egy átfogóbb megközelítés biztosítása, amely hatékonyabban támogatja a vállalati szintű üzleti kockázatok kezelését és a biztonsági architektúra stratégiai szintű integrációját.

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

Enterprise Security Architecture – Using SABSA to Deliver ISO 27001 the Right Way

(Sarit Kannanoor)

Az előadás középpontjában az állt, hogy a vállalati biztonsági architektúra kialakításakor **milyen módon illeszthető össze a SABSA keretrendszer az ISO alapú irányítási rendszerekkel**. Bemutatásra került, hogy az információbiztonsági szakemberek jelentős része már ismeri az **ISO/IEC 27001** szabványt, illetve az IT szolgáltatásmenedzsmenthez kapcsolódó **ISO 20000** vagy **ITIL** megközelítést, miközben számos szervezet – különösen a kritikus infrastruktúrák, például közműszolgáltatók, víziközművek vagy közlekedési vállalatok – integrált irányítási rendszert működtet, amely egyetlen keretrendszerben egyesíti az olyan szabványokat, mint az **ISO 9001** (minőségirányítás), az **ISO 45001** (munkabiztonság) és az **ISO 14001** (környezetirányítás). Az előadás rámutatott arra, hogy egy vállalati biztonsági architektúrát tervező szakember számára **alapvető fontosságú ezen szabványok működésének megértése**, mivel a SABSA egyik legfontosabb előnye éppen az, hogy rugalmasan integrálható már meglévő irányítási és szabályozási keretrendszerekbe. A **SABSA teljes körű problémamegoldó architektúra-módszertanként** különböző eszközöket és technikákat biztosít a követhetőség, az indokolhatóság és a teljesség igazolására, ami a biztonsági döntések szakmai megalapozását is támogatja. Az előadás kitért arra a gyakori tapasztalatra is, hogy a SABSA képzéseken részt vevő szakemberek sokszor elméleti szinten megismerik a módszertant, ugyanakkor bizonytalanok abban, miként kezdhető meg annak gyakorlati alkalmazása egy szervezetben. Ennek megoldásaként került bemutatásra az a megközelítés, amely szerint a SABSA **eszköztára az ISO 27001 struktúráján belül is hatékonyan használható**. Példaként szerepelt az ISO 27001 szabvány 4.1-es pontja, amely a szervezeti kontextus megértését írja elő, és amely jól megfeleltethető a SABSA kontextuális architektúra rétegének, illetve a 6.1.3-as pontban előírt Statement of Applicability dokumentum, amely a biztonsági kontrollok indokoltságát és teljességét biztosító követhetőséget igényel – ennek strukturált

kidolgozását a SABSA módszertan eszközei hatékonyan támogatják. Az előadás **gyakorlati példákon keresztül szemléltette,** hogy a SABSA technikáival hogyan valósítható meg az ISO 27001 követelményeinek következetes és auditálható módon történő implementálása.

When SABSA met FAIR: A Framework Dynamic Duo

(Rodney Anderson)

Az előadás középpontjában a **SABSA** (Sherwood Applied Business Security Architecture) **keretrendszer és a FAIR** (Factor Analysis of Information Risk) **módszertan integrációja** állt, különös tekintettel arra, miként erősítheti a FAIR a kockázatalapú biztonsági döntéshozatalt és a biztonsági architektúra tervezésének megalapozottságát. Bemutatásra került, hogy a **FAIR** által biztosított **kvantitatív kockázatelemzés** képes jelentősen növelni a SABSA architektúra robusztusságát azáltal, hogy **számszerűsíthető módon értelmezi az információbiztonsági kockázatokat**. A két megközelítés összekapcsolása elsősorban a SABSA mátrix „Motivation" oszlopát támogatja, amely a biztonsági intézkedések mögött álló üzleti indokokat, vagyis a „miért" kérdését hivatott megválaszolni.

Az ismertetett módszertan szerint a FAIR által előállított, megbízható és strukturált kockázati becslések lehetővé teszik, hogy a biztonsági architektúra ne pusztán technikai megfontolásokon alapuljon, hanem szorosan illeszkedjen a szervezeti és üzleti célokhoz. Az előadás rámutatott arra is, hogy a **növekvő kibertámadási aktivitás** mellett egyre **nagyobb igény mutatkozik olyan biztonsági stratégiákra**, amelyek kockázatalapúak és mérhető formában is értelmezhetők. A **FAIR és a SABSA együttes alkalmazása** lehetőséget biztosít arra, hogy az összetett információbiztonsági kockázatok a vállalati architektúra kontextusában, mégis egyszerű, számszerűsíthető módon kerüljenek bemutatásra a döntéshozók és az érintett üzleti szereplők számára. Ez a megközelítés elősegíti a biztonsági prioritásokról és beruházásokról folytatott szakmai párbeszédet, valamint

BBA-PLUSZ-312-24-2024-00003 sz. pályázat részeként

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

erősíti a kockázatkezelési folyamatok átláthatóságát és a SABSA-alapú biztonsági architektúra megalapozottságát.

Optimising Information Asset Utilisation Through Co-Design and SABSA Integration

(Bethany Sinclair-Giardini)

Az előadás az **információs eszközök** (information asset) **életciklusát** vizsgálta, bemutatva, miként alakulnak át egy kezdetben egyetlen üzleti folyamathoz kapcsolódó információelemből a SABSA biztonsági architektúra-keretrendszer különböző rétegeiben stratégiai jelentőségű erőforrássá. A prezentáció részletesen tárgyalta, hogyan történik az **információs eszközök felhasználása**, illetve **manipulációja** különböző működési, megfelelőségi és biztonsági célok támogatása érdekében, valamint rámutatott arra is, hogy az ilyen **eszközök értékének maximalizálásához** kulcsfontosságú a **megfelelő tervezési módszertan** alkalmazása. Ennek kapcsán kiemelt szerepet kapott a **co-design** megközelítés, amely lehetővé teszi a belső és külső érintettek bevonását a tervezési folyamatba, így biztosítva, hogy az információs eszközökhöz kapcsolódó rendszerkonfigurációk összhangban legyenek az üzleti célokkal és a szabályozási követelményekkel. Az előadás kitért arra a gyakori problémára is, hogy a **rendszerfejlesztési projektek** során az információs eszközökkel kapcsolatos tervezési szempontok sok esetben csak késői fázisban jelennek meg, ami korlátozza a rendszer funkcionalitását és a megfelelőségi lehetőségeket. A bemutatott megközelítés ezzel szemben egy integrált modell alkalmazását javasolja, amelyben a **co-design alapú specifikációs workshopok** már a fejlesztési ciklus kezdetén bevonják az üzleti felhasználókat, ezáltal lehetővé téve, hogy az információs eszközök kezelése és tervezése a kezdetektől a rendszerarchitektúra szerves részét képezze, ami hosszú távon hatékonyabb működést, jobb megfelelőséget és stratégiai előnyöket eredményez a szervezetek számára.

How to Influence Your Way to Cyber Budgets

(Dimitri Vedeneev)

Az előadás a vezetői döntéshozók számára készített **kiberbiztonsági prezentációk** sajátosságait tárgyalta, kiemelve, hogy a **hatékony kommunikáció** alapfeltétele a technikai szakzsargonról a vállalati működés szempontjaira épülő narratívára történő tudatos átállás. Bemutatásra került, hogy **a kiberbiztonsági kockázatokat a felsővezetés számára érthető módon, üzleti hatásokra figyelemmel szükséges prezentálni**, különös tekintettel a potenciális pénzügyi veszteségekre, a szabályozói megfelelési kötelezettségek megsértésének következményeire, valamint a szervezeti reputációt érintő kockázatokra. Az előadás hangsúlyozta, hogy a **vezetői kommunikáció során** a megtérülés (ROI), a versenyelőny és a stratégiai támogatás fogalmait kell előtérbe helyezni, nem pedig kizárólag technikai sérülékenységekre koncentrálni. A **SABSA módszertan** alkalmazásával kapcsolatban ismertetésre került annak jelentősége, hogy a **biztonsági architektúra különböző rétegei** – a komponens- és fizikai szintektől egészen a kontextuális szintig – **közötti kapcsolat és visszakövethetőség egyértelműen bemutatható legyen**, ezáltal alátámasztva a biztonsági beruházások és döntések indokoltságát. Az előadó kitért a **vizuális történetmesélés** szerepére is, amelynek során kockázati mátrixok, költség-haszon elemzések és implementációs ütemtervek segítségével szemléltette a szükséges intézkedések sürgősségét és megvalósíthatóságát. Kiemelésre került, hogy a **kiberbiztonságot** nem költségközpontként, hanem **üzleti működést támogató képességként** célszerű pozícionálni, amely hozzájárul a bevételi források védelméhez és a digitális transzformációs kezdeményezések biztonságos megvalósításához. Az előadás szerint a sikeres prezentációk fontos eleme a költségvetéssel kapcsolatos kérdésekre való felkészülés, a mérhető teljesítménymutatók bemutatása, valamint a fázisokra bontott megvalósítási terv ismertetése, amely rövid távon gyors eredményeket, hosszabb távon pedig stratégiai fejlődést mutat. A meggyőző prezentációk végén konkrét erőforrásigények, reális időkeretek és egyértelmű felelősségi struktúrák kerülnek meghatározásra, miközben **a kiberbiztonsági beruházások**

BBA-PLUSZ-312-24-2024-00003 sz. pályázat részeként

BBA+ BESZÁMOLÓ

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

a szervezeti működés alapvető infrastruktúrájaként jelennek meg, nem pedig opcionális technológiai fejlesztésként.

Using the SABSA Matrix with Stakeholders to Define Project Perspectives and Actions

(Darren Skidmore)

Az előadás a SABSA keretrendszer egyik alapvető eszközének, a SABSA **Matrixnak a gyakorlati alkalmazását mutatta be** egy új biztonsági szolgáltatás (**Security Service**) tervezésének kontextusában. A bemutató során ismertetésre került, hogy a **mátrix miként rendezi logikai struktúrába az architektúra különböző rétegeit** és az azokhoz tartozó nézőpontokat, ezáltal támogatva a biztonsági követelmények rendszerezett feltárását. A projekt előkészítési szakaszában a módszertan alkalmazása elsősorban az érintett szereplőkkel (stakeholder) folytatott egyeztetések során bizonyult hasznosnak, mivel a mátrix segítségével strukturált módon kerültek feltárásra az egyes szereplők üzleti motivációi, elvárásai és a kívánt eredmények. A különböző nézőpontokat képviselő érintettek **rövid módszertani magyarázat után könnyen értelmezni tudták** a modell felépítését, ami elősegítette a közös gondolkodást és olyan szakmai párbeszédeket indított el, amelyek más megközelítésben nem feltétlenül merültek volna fel. Az előadás kitért arra is, hogy a **SABSA architektúra különböző rétegei** – például a szolgáltatásmenedzsment (Service Management) – lehetőséget biztosítottak a működési folyamatok, különösen a **BAU** (Business as Usual) működésben szükséges változtatások, valamint az érintett szervezeti egységek igényeinek pontosabb megfogalmazására. Bemutatásra került továbbá az a törekvés, hogy a módszertan alkalmazása ne csupán az adott projektre korlátozódjon, hanem hosszabb távon az egész vállalati működésben is megjelenjen a **SABSA-alapú szemlélet**, kiegészítve további információkkal, indoklásokkal, valamint a projekt előrehaladása során érintett rendszerek és csapatok részletes

dokumentálásával. **Az előadás összefoglalta** a bevezetés folyamatát, a gyakorlati alkalmazás során felmerült nehézségeket, valamint azokat a tapasztalatokat és eredményeket, amelyek rávilágítottak arra, hogy a **SABSA keretrendszer hatékony eszközként használható** a projektek biztonsági követelményeinek indoklásában, megtervezésében és kommunikálásában.

The Needs of the Many Outweigh the Needs of the Few, or the One - Spock

(Carol Sutton)

Az előadás a **SABSA** (Sherwood Applied Business Security Architecture) **módszertan** egyik alapvető megállapításából indult ki, amely szerint **egy apró, látszólag jelentéktelen hiba vagy félreértés a kockázatok kommunikációjában láncreakciószerű következményekhez vezethet** a szervezeti döntéshozatali lánc mentén. Ennek szemléltetésére a közismert mondás („**For want of a nail**...") került bemutatásra, amely jól illusztrálja, hogy a kockázatok, problémák és lehetőségek nem megfelelő kommunikációja milyen súlyos következményekkel járhat a felsőbb szinteken. A SABSA keretrendszer **a szervezeti fenyegetéseket üzleti kockázatokként értelmezi** , és hangsúlyozza, hogy a stratégiai célok és üzleti imperatívuszok kommunikációjához kapcsolódó kockázatok gyakran kommunikációs szakemberek bevonásával kezelhetők. Az előadás külön kitért arra, hogy **Ausztráliában** mind az állami és területi kormányzatok, mind a szövetségi kormány **egyre szélesebb körben alkalmazza a SABSA módszertant**, ugyanakkor felmerül a kérdés, hogy az eredetileg üzleti környezetre kidolgozott alapelvek milyen mértékben ültethetők át a kormányzati szférába.

A prezentáció ennek kapcsán azt vizsgálta, hogy a „**közjó előmozdítása**", amely bizonyos esetekben ütközhet a hagyományos vagy egyéni erkölcsi normákkal, miként befolyásolja a fenyegetések és kockázatok megfogalmazását és értelmezését a kormányzati döntéshozatalban. Felvetésre került az a kérdés is, hogy elegendő-e egyszerűen az üzleti szervezeteket kormányzati intézményekre

BBA-PLUSZ-312-24-2024-00003 sz. pályázat részeként

BBA+ BESZÁMOLÓ

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

„cserélni” a SABSA modellekben, vagy szükség van a módszertan mélyebb adaptációjára. Ezzel összefüggésben **Machiavelli** 1513-ban megfogalmazott **tanácsa** – miszerint **az állam védelme érdekében az uralkodónak meg kell tanulnia „nem jónak lenni”** – arra a dilemmára hívta fel a figyelmet, hogy az állami érdekek és a nemzetbiztonsági szempontok miként torzíthatják a kockázatelemzés kiindulópontját. Az előadás zárásaként annak lehetősége került megvizsgálásra, hogy **szükséges-e módosítani a SABSA folyamat bizonyos lépéseit** annak érdekében, hogy a kormányzati elemzések ne automatikusan a nemzetbiztonsági kontextussal induljanak, hanem a valós szervezeti célokból és kockázatokból épüljenek fel.

Implementing SABSA in Context: A Practical First Step

(Dan Schoemaker)

Az előadás középpontjában a **SABSA** (Sherwood Applied Business Security Architecture) keretrendszer **gyakorlati alkalmazásának** egyik lehetséges **kiindulópontja** állt, különös tekintettel arra a gyakori problémára, hogy a **SABSA Foundations képzés elvégzését követően** sok szervezet számára nem egyértelmű, **hol érdemes megkezdeni a módszertan tényleges bevezetését**. Az előadás során bemutatásra került, hogy a keretrendszer elméleti komplexitása könnyen elbizonytalaníthatja a szakembereket, ezért **célszerű egy jól körülhatárolt, alacsony kockázatú projekt kiválasztásával megkezdeni az implementációt**. Ennek példájaként a biztonsági csapat működését meghatározó **Team Charter** kialakítása került ismertetésre, amely strukturált módon rögzíti a szerepköröket, felelősségi köröket, valamint a kommunikációs csatornákat. Az előadás minden résztvevő számára érthető módon ismertette, hogy miként alkalmazhatók a SABSA architekturális koncepciói konkrét, gyakorlati lépések formájában. Részletesen bemutatásra kerültek azok a kihívások is, amelyek a projekt megvalósítása során felmerültek, továbbá az ezekből levont tanulságok, valamint az a pozitív hatás, amely a biztonsági csapat működési

hatékonyságában és együttműködésében volt megfigyelhető. Az ismertetett megközelítés rávilágított arra, hogy a **SABSA bevezetése nem feltétlenül igényel azonnali, átfogó átalakítást** a szervezet biztonsági programjában, hanem **fokozatos, kisebb lépésekben is megvalósítható**, ami stabil alapot teremthet a későbbi, komplexebb architekturális fejlesztésekhez.

„B" előadássorozat

From Value Chain to Prompt: AI Fast Track

(Dr Malcom Shore)

Az előadás középpontjában az **AI-megoldások üzleti értékteremtésének strukturált megközelítése** állt, különös tekintettel az **értéklánc-elemzés** szerepére az architektúra-tervezés során. Bemutatásra került az **AI Accelerator Playbook**, amely módszertani keretet biztosít az **AI value chain-ek** feltérképezéséhez és elemzéséhez, valamint ahhoz, hogy az üzleti folyamatok mentén azonosíthatók legyenek azok a pontok, ahol a **mesterséges intelligencia mérhető hozzáadott értéket** képes teremteni. Az előadás részletesen ismertette azokat a lépéseket, amelyek szükségesek az AI-alkalmazási lehetőségek szisztematikus feltárásához: az üzleti célok és stratégiai prioritások meghatározásától kezdve az értékteremtő folyamatok azonosításán és strukturálásán át egészen a technológiai és adatarchitektúra illesztéséig. Kiemelésre kerültek olyan **új architekturális eszközök és modellezési megközelítések**, amelyek támogatják az attribútumok és képességek értéklánchoz történő referenciatérképezését, ezáltal átláthatóbbá téve az AI-megoldások hatását az egyes üzleti funkciókra. Az előadás nemcsak a technológiai oldalra fókuszált, hanem részletes **stakeholder-analízist** is tartalmazott, bemutatva, hogy az érintettek – üzleti döntéshozók, IT-architektek, adatgazdák és végfelhasználók – milyen módon befolyásolják az AI-kezdeményezések sikerességét. Az ismertetett megközelítés alapján az AI-architektúra tervezése nem pusztán technológiai kérdésként, hanem integrált üzleti-transzformációs programként

BBA-PLUSZ-312-24-2024-00003 sz. pályázat részeként

BBA+ BESZÁMOLÓ

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

értelmezhető, amelyben az **értéklánc-alapú gondolkodás** biztosítja az átlátható priorizálást és a fenntartható üzleti eredményeket.

Beyond the Algorithm: Cultivating Trust in the AI Era

(Bharat Bajaj, Reshma Devi)

Az előadás központi témája a **mesterséges intelligencia (AI) mindennapi és üzleti környezetben betöltött**, egyre meghatározóbb **szerepe** volt, különös tekintettel a **bizalom** kérdésére, amely az innovációval párhuzamosan **alapvető követelménnyé** vált. Kiemelésre került, hogy az **AI-megoldások fejlesztése** során nem elegendő a technológiai előrelépésre koncentrálni, hanem **biztosítani kell a rendszerek felelős, biztonságos és megbízható működését** is. A bemutató a **„Trustworthy AI" koncepció** mentén azokat a tartópilléreket ismertette, amelyek a bizalom kiépítéséhez szükségesek: technikai védőkorlátok (technical guardrails) alkalmazása, etikai szempontok érvényesítése, erős adatvédelmi és adatkezelési keretrendszerek kialakítása, valamint a szigorú szabályozói megfelelés biztosítása. A szemléltetés szerint ezek az elemek egy stabil épület alapját és tartószerkezetét képezik, ahol a bizalom, az átláthatóság, az etika és a biztonság egységes, szabályozási környezet által lefedett rendszert alkotnak. Külön hangsúlyt kapott az **AI-ügynökök (AI agents)** térnyerése, amelyek **autonóm módon** képesek döntéseket hozni és műveleteket végrehajtani; esetükben a bizalom kérdése még hangsúlyosabb, mivel működésük közvetlen hatással lehet üzleti folyamatokra és felhasználókra. Elvárásként fogalmazódott meg, hogy ezek a rendszerek **etikus** működést tanúsítsanak, tevékenységük legyen **átlátható** és **auditálható**, biztosítsák az **adatok magas szintű védelmét**, aktívan kezeljék az algoritmikus torzításokat (bias), valamint maradéktalanul feleljenek meg a vonatkozó jogszabályi és iparági előírásoknak. Az előadás rávilágított arra, hogy a **bizalom kiépítése** nem csupán reputációs kérdés, hanem **üzleti alapkövetelmény**: a felelős tervezés és üzemeltetés teremti meg annak feltételeit, hogy az AI-megoldások széles körben, fenntartható módon és mérhető üzleti értéket teremtve

kerüljenek bevezetésre, miközben hozzájárulnak egy átláthatóbb és megbízhatóbb digitális ökoszisztéma kialakításához.

Human Crash-Test Dummies, and How AI has Taken the RED out of DREAD...

(Andy Prow)

Az előadás központi témája az volt, hogy a **modern mesterséges intelligencia alapjaiban alakította át a fenyegetettségi környezetet**, mivel a támadók korábban nem látott hatékonyságú és intelligenciájú eszközökhöz jutottak. Bemutatásra került, hogy a klasszikus **DREAD fenyegetettségi modell** – amely a Damage, Reproducibility, Exploitability, Affected Users és Discoverability szempontjai mentén értékeli a sérülékenységeket – napjainkra gyakorlatilag „**AD**”-re egyszerűsödik. Az érvelés szerint az **AI-alapú eszközök** drámai mértékben **növelik a sérülékenységek** reprodukálhatóságát, kihasználhatóságát és felfedezhetőségét, így ezek a tényezők a támadók számára már nem jelentenek érdemi akadályt. A **védekezési oldal** fókusza ezért egyre inkább a tényleges károkozás (**Damage**) mértékének csökkentésére és az érintett felhasználók számának minimalizálására (**Affected Users**) helyeződik át. Ennek kapcsán hangsúlyt kapott a **digitális biztonság** szerepe, amely nem csupán a behatolások megelőzésére, hanem a „**fail safely” elv** mentén tervezett rendszerek kialakítására összpontosít, vagyis arra, hogy egy kompromittálódás esetén a rendszer működése kontrollált módon, korlátozott következményekkel álljon le vagy degradálódjon. A koncepció szemléltetésére két autonóm járműarchitektúra összehasonlítása szolgált példaként: az egyik konstrukció magasabb szintű kiberbiztonsági védelmet biztosított, így kisebb valószínűséggel volt feltörhető, míg a másik tervezésében a biztonságtechnikai szempontok domináltak, így sikeres támadás esetén is alacsonyabb fizikai és működési kockázatot jelentett. Az előadás rávilágított arra, hogy a jövő rendszereinek tervezésekor a

BBA-PLUSZ-312-24-2024-00003. sz. pályázat részeként

BBA+ BESZÁMOLÓ

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

security és a safety integrált kezelése elengedhetetlen az AI által felgyorsított fenyegetési környezetben.

Space Engineering Inspired Cyber Resiliency

(Chathura Abeydeera, Andreas Dannert)

Az előadás a közelmúlt nagy visszhangot kiváltó IT szolgáltatás-kieséseiből indult ki, köztük a **CrowdStrike incidenséből**, valamint a **UniSuper teljes Google Cloud környezetének véletlen törléséből,** rámutatva arra, hogy a **kiberbiztonsági kockázatok** nem kizárólag rosszindulatú támadókhoz köthetők, hanem **emberi hibákból** és nem **megfelelően kialakított védelmi mechanizmusokból** is fakadhatnak. A prezentáció központi gondolata az volt, hogy a **kiberreziliencia** növeléséhez érdemes más mérnöki területek – különösen az űrmérnökség, a repülőgépipar és a redundáns rendszerek tervezése – bevált gyakorlataiból meríteni. Bemutatásra került, hogy az űrrendszereket extrém, hibát nem tűrő környezetre tervezik, ahol a megbízhatóságot többszintű redundancia biztosítja a hardverelemek, a szoftverkomponensek és a kommunikációs protokollok szintjén egyaránt. Ennek mintájára a kiberbiztonsági architektúrákban is alkalmazható a **rétegzett redundancia** (layered redundancy), amely **több védelmi vonal** kialakításával biztosítja az üzletmenet folytonosságát komponenshiba esetén; a hibatűrés (fault tolerance), amely lehetővé teszi a rendszer működésének fenntartását részleges meghibásodás mellett; a moduláris tervezés, amely cserélhető és frissíthető elemekre bontja a rendszert; valamint a szigorú tesztelési és szimulációs gyakorlat, amely még éles üzem előtt feltárja a potenciális sérülékenységeket. Az előadás **esettanulmányokon keresztül** szemléltette, miként ültethetők át ezek az elvek vállalati környezetbe, különös tekintettel a kritikus üzleti eszközök védelmére, és felhívta a figyelmet arra, hogy a **kiberreziliens rendszerek kialakítása** szemléletváltást igényel az egyszeri védelem helyett a **folyamatos működőképesség** biztosítása irányába. A bemutatott

megközelítések nem kész receptekként, hanem vitaindítóként kerültek pozicionálásra a biztonsági architektek számára, kiemelve az alulértékelt, nem szándékos eredetű kockázatokat, valamint az olyan meglévő keretrendszerek jelentőségét, mint a MITRE Cyber Resiliency Engineering Framework-je és a National Institute of Standards and Technology által kiadott Special **Publication 800-160**, amelyek iránymutatást adnak kiberreziliens rendszerek tervezéséhez és fejlesztéséhez.

Living in a World of Covert Channels

(Andy Clark)

Az előadás egy **2019 nagypéntekén elkövetett, walesi Anglesey térségében történt emberölési ügy technikai hátterét** mutatta be, amelyben 2020. február 24-én Terence Michael Whall ellen egyhangú esküdtszéki döntéssel született bűnös ítélet a 74 éves Gerald Corrigan meggyilkolása miatt.

A prezentáció részletesen ismertette, hogy az elkövető a **hagyományos kriminalisztikai bizonyítékok hiányában** – nem állt rendelkezésre közvetlen szemtanú és klasszikus forenzikus nyom – a „tökéletes bűncselekmény” illúziójában cselekedett, azonban a **digitális nyomok döntő szerepet játszottak** a bizonyításban. A bíróság előtt bemutatásra kerültek a Jaguar Land Rover által szolgáltatott telematikai adatok, amelyek **rögzítették a gyanúsított járművének helyzetét** a bűncselekményt megelőző napon végzett terepfelderítés során, továbbá dokumentálták a csomagtartó 23:11:04-kor történt nyitását és 39 másodperccel későbbi zárását, amikor a fegyver kivételére került sor. A Sky **műholdas szolgáltató adatai** igazolták, hogy az áldozat otthonában 00:08-kor még aktív volt a műholdas televíziós kapcsolat, majd 00:28-kor egy felvett műsor leállítását követően a jel megszűnt; a rendelkezésre álló bizonyítékok szerint az áldozat a hiba kivizsgálására kilépett a házból, ahol halálos lövés érte. A **jármű telematikai rendszere** a bűncselekményt követően ismét adatokat szolgáltatott a mozgásról, valamint a csomagtartó

BBA-PLUSZ-312-24-2024-00003 sz. pályázat részeként

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

nyitásáról és zárásáról, alátámasztva a menekülés körülményeit. Az eset rávilágított arra, hogy a modern járművek és otthoni rendszerek által generált, harmadik felekhez továbbított **technikai adatok milyen részletességgel rekonstruálhatják az eseményeket**, sok esetben a felhasználók teljes körű tudatossága nélkül. Az előadás záró részében hangsúlyozásra került, hogy ez az ügy csupán egy példa a hasonló adatátadási gyakorlatokra, és külön kitértek arra is, hogy a jármű–jármű (V2V) és jármű–infrastruktúra (V2I) kommunikáció szabványosodó ökoszisztémája új támadási felületeket teremthet, amelyeket rosszindulatú szereplők a megfigyelési és felderítési mechanizmusok kijátszására használhatnak fel.

Taming the Untrusted:
Zero Trust Approaches and Cross-Sector Case Studies

(Dr. Pierre Tagle)

Az előadás a **digitális korszak kibervédelmi kihívásainak átalakulását** helyezte középpontba, rámutatva arra, hogy napjainkban már nem az a kérdés, hogy egy szervezetet ér-e kibertámadás, hanem az, hogy **mikor következik be az incidens**. A hibrid munkavégzés, a felhőalapú szolgáltatások elterjedése és a fenyegetések növekvő komplexitása következtében a hagyományos, peremalapú védelmi modellek elvesztették hatékonyságukat, mivel az implicit bizalomra épülő architektúrák nem képesek megfelelően kezelni a modern támadási felületeket. A bemutató a kiberreziliencia (**cyber resilience**) koncepcióját, mint **stratégiai célt** definiálta, amelynek egyik meghatározó megközelítése a **Zero Trust modell**. Kiemelésre került, hogy a Zero Trust nem konkrét termék, hanem **szemlélet és keretrendszer**, amely az implicit bizalom teljes elutasítására és minden hozzáférési kérelem folyamatos, kontextusalapú ellenőrzésére épül. Az előadás részletesen ismertette a paradigma fejlődését, valamint tisztázta a Zero Trust körüli tévhiteket és a gyakorlati megvalósítás realitásait. Hangsúlyozásra került, hogy a **modell bevezetése egy többlépcsős**

BBA-PLUSZ-312-24-2024-00003 sz. pályázat részeként

folyamat, amely az úgynevezett **Crawl–Walk–Run megközelítés** mentén valósítható meg, és amely során az üzleti célokkal való szoros összehangolás, valamint az alapvető pillérek – identitáskezelés, eszköz- és hozzáférés-ellenőrzés, hálózati szegmentáció, folyamatos monitorozás – fokozatos kiépítése kulcsszerepet játszik. Három, eltérő szektorból származó esettanulmány – pénzügyi, ipari és non-profit területről – szemléltette, hogy a **Zero Trust megközelítés nem alkalmazható sablonszerűen,** hanem az adott szervezet működési sajátosságaihoz, szabályozási környezetéhez és kockázati profiljához igazítandó. Az ismertetett példák bemutatták a kiinduló kihívásokat, a választott architekturális és szervezeti lépéseket, valamint az elért eredményeket, különös tekintettel az érzékeny adatok védelmére, a megfelelőségi követelmények teljesítésére és a biztonságos működés fenntartására. Az előadás összegzése szerint a **kiberreziliencia elérése stratégiai cél,** amelyhez a Zero Trust szemlélet hatékony, de tudatosan és szervezetspecifikusan kialakított megvalósítást igénylő útvonalat kínál.

Mesh, Hype or Hope? Reassessing Cybersecurity Mesh Architecture (CSMA) in the Shadow of Zero Trust

(Abbas Kudrati)

Az információbiztonsági iparágban már jelenleg is számos architektúra-keretrendszer – például a Zero Trust, a SASE, a CARTA vagy a BeyondCorp – létezik, ezért a Gartner által bevezetett **Cybersecurity Mesh Architecture** (CSMA) kapcsán az előadás **központi kérdése** az volt, **indokolt-e egy újabb modell megjelenése**. A bemutató kritikai megközelítésben vizsgálta a CSMA célját, ígéretét és gyakorlati alkalmazhatóságát, különös tekintettel az identitásközpontú védelemre és a Zero Trust stratégiák bevezetésére. Részletesen ismertetésre kerültek a **CSMA alapelvei**, mint az elosztott érvényesítés (distributed enforcement), az identitásszövet (identity fabric) és a komponálhatóság (composability), majd ezek összevetése történt a már ismert biztonsági paradigmákkal. Konkrét vállalati felhasználási eseteken és architekturális mintákon keresztül került

BBA+ BESZÁMOLÓ

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

értékelésre, hogy a CSMA miként illeszthető be a modern enterprise környezetek technológiai rétegébe, illetve milyen korlátai azonosíthatók. Külön figyelmet kapott a nem emberi identitások kezelése, a hibrid infrastruktúrák védelme, valamint a biztonsági eszközök integrációjának régóta fennálló kihívása. Az előadás az architekturális túltervezés, a piaci fragmentáció és a stratégiai döntéshozatal dilemmáit helyezte fókuszba, rávilágítva arra, hogy a biztonsági vezetők számára a kérdés nem pusztán az adaptáció, hanem az is, hogy **egy újabb keretrendszer valódi evolúciós lépést jelent-e, vagy csupán egy újabb mozaikszó** a már így is telített szakmai diskurzusban.

Securing Australia's Federated Future: Rethinking Access, Trust, and Compliance Across Domains

(Ahmad Salehi Shahraki)

Az előadás **Ausztrália digitális infrastruktúrájának biztonsági kihívásait** elemezte, rámutatva arra, hogy a kormányzati szervek, egészségügyi hálózatok, kutatóintézetek és magánvállalatok működése ma már közös platformokra, szervezetek közötti adatáramlásra és multi-cloud architektúrákra épül, miközben az alkalmazott identitás- és hozzáférés-kezelési rendszerek többsége továbbra is centralizált, elszigetelt környezetekre tervezett modellekre támaszkodik. Bemutatásra került, hogy ezek a **hagyományos megoldások** nem képesek megfelelően kezelni a megosztott hatásköröket, az elosztott adatirányítást és az eltérő joghatósági megfelelőségi követelményeket. A szekció központi kérdése az volt, **miként biztosítható a hozzáférések védelme, a bizalom fenntartása és a szabályozói megfelelés** olyan rendszerekben, ahol az irányítás töredezett, ugyanakkor a szervezetek közötti együttműködés alapvető elvárás. Megoldásként egy korszerű, **Attribute-Based Access Control** (ABAC) elveire épülő hozzáférés-szabályozási keretrendszer került ismertetésre, amely finomszemcsés, attribútumalapú, szabályvezérelt döntéshozatalt tesz lehetővé, kiegészítve ún. „**privacy-preserving**” kriptográfiai technikákkal. Az egészségügyi és kormányzati szektorból származó esettanulmányok bemutatták,

hogy e modellek miként támogatják a biztonságos, doméneken átívelő együttműködést, csökkentik a kockázati kitettséget, és illeszkednek a nemzeti adatvédelmi reformokhoz, valamint a kiberbiztonsági stratégiákhoz. Az előadás kitért a **gyakorlati implementáció** lépéseire is, hangsúlyozva az adatszuverenitás, az átláthatóság és az interoperabilitás biztosítását úgy, hogy közben az innovációs képesség ne sérüljön.

High Assurance Computing in the Commercial Sector: Niche or Necessity?

(Andy Clark (Plenáris ülés))

Az előadás a **digitális transzformáció felgyorsulásának következményeit** vizsgálta a kereskedelmi vállalatok információbiztonsági kitettsége szempontjából, rámutatva arra, hogy a kifinomult kibertámadások, a növekvő szabályozói elvárások és a reputációs kockázatok egyre komplexebb védelmi megközelítést tesznek szükségessé. Bemutatásra került, hogy a **High Assurance Computing** (HAC), amely a helyesség, bizalmasság, sértetlenség és megbízhatóság szigorú követelményeire épül, korábban elsősorban a védelmi ipar, a repülőgépipar és a kritikus nemzeti infrastruktúra (CNI) területén volt jelen, ugyanakkor a kritikus infrastruktúrák kereskedelmi beszállítóktól való jelentős függősége miatt a magas megbízhatóságú számítástechnika elvei egyre inkább átszivárognak a vállalati szektorba is. Az előadás részletesen **ismertette** azokat a **stratégiai és technikai tényezőket**, amelyek a high assurance szemlélet vállalati adaptációját ösztönzik, külön kitérve a kriptográfiai rendszerek formális verifikációjára, a manipuláció-ellenálló (tamper-resistant) feldolgozási környezetekre, a biztonságos boot láncokra, a megbízható kulcsmenedzsmentre és az auditálható naplózási láncokra. Ezek az egykor speciális, szűk körben alkalmazott megoldások mára alapvető **kontrollokká váltak** olyan szektorokban, mint a pénzügyi szolgáltatások, az egészségügy vagy az ún. cloud-native SaaS platformok. Az előadás konklúziója szerint a folyamatosan változó fenyegetési környezetben és a digitális bizalom üzleti versenyelőnnyé válásának korszakában a **high**

BBA-PLUSZ-312-24-2024-00003 sz. pályázat részeként

BBA+ BESZÁMOLÓ

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

assurance computing vállalati alkalmazása nem csupán releváns, hanem elengedhetetlen követelmény.

The Pragmatist's Guide to Safely Automating the Management of Critical Infrastructure

(Luke Snell)

Az előadás középpontjában az a kérdés állt, hogy **miként automatizálható biztonságosan** az olyan kritikus infrastruktúrák üzemeltetése és menedzsmentje, amelyek a társadalom számára alapvető szolgáltatásokat nyújtanak, és amelyek meghibásodása súlyos, egymásra kiható következményekkel járhatnak, beleértve az emberéletek veszélyeztetését, jelentős környezeti károkat vagy szervezeti és kormányzati reputációvesztést. Az **ismertetett esettanulmány** egy ausztrál, magas kockázatú **ipari létesítmény ötéves átalakulási folyamatát mutatta be**, amelynek során **fokozatosan került bevezetésre az automatizált működés**. A folyamat alapját egy kockázat- és üzletközpontú megközelítés képezte, amelyet a **SABSA biztonsági architektúra-keretrendszer**, valamint a funkcionális biztonsági mérnöki szabványok (**IEC 61508 és IEC 61511**) támogattak. A bemutatott **módszertan eredményeként** nőtt a szervezeti folyamatérettség, fejlődtek a képességek, csökkent az operatív kockázat – a prezentáció szerint nagyságrendileg tízszeres mértékben –, valamint számos esetben sikerült a munkavállalókat eltávolítani a potenciálisan veszélyes műveletek közvetlen végrehajtásától. Az előadás kitért azokra a **gyakorlati felhasználási területekre** is, amelyek a felsővezetők és az üzemvezetők számára valódi üzleti értéket képviselnek, továbbá tárgyalásra került a kereskedelmi forgalomban elérhető megoldások (COTS) és a saját fejlesztések közötti döntési szempontok rendszere. Részletesen bemutatásra kerültek azok az **alapvető logikai szolgáltatások** is, amelyek lehetővé teszik az emberi és a gép által kezdeményezett munkafolyamatok egyértelmű megkülönböztetését, valamint szó esett a karbantartási adósság („**maintenance debt**”) szervezeti változáskezelésre gyakorolt hatásáról. Az

előadás további része az **eseményvezérelt automatizáció gyakorlati kihívásait**, illetve az **orkesztráció** fizikai rendszerekre történő **kiterjesztésének problémáit** tárgyalta. A bemutatott koncepciók egy gyártófüggetlen „**just-in-time network administration**” képesség felépítésén keresztül kerültek szemléltetésre, amelynek működését az előadás végén egy élő demonstráció mutatta be.

Bridging Business and Cybersecurity: An Enterprise Security Architecture Journey in the Australian Energy Sector

(Samuel Pinzon)

Az előadás egy **ausztrál energetikai vállalat** tapasztalatain keresztül mutatta be, miként alakítottak ki egy a **gyakorlatban is működő, skálázható vállalati biztonsági architektúrát a SABSA keretrendszer alkalmazásával**. A bemutató rámutatott arra, hogy a **SABSA** a kiberbiztonság szempontjából egyfajta „**összekötő elemként**” szolgált a szervezet különböző üzleti és technológiai területei között, támogatva az új üzleti kihívások kezelését, a digitális transzformációs törekvéseket, valamint a folyamatosan változó szabályozási környezethez való alkalmazkodást. Az előadás kiemelte, hogy a szervezetek működési modelljeinek átalakulásával és a fenyegetettségi környezet bizonytalanságának növekedésével a biztonsági architektek számára egyre nagyobb kihívást jelent olyan **interoperábilis, újrahasznosítható és az üzleti célokhoz igazodó kiberbiztonsági megoldások** kialakítása, amelyek hatékonyan illeszkednek a vállalati működésbe. Ennek szemléltetésére **konkrét példák és gyakorlati architekturális artefaktumok** kerültek bemutatásra, amelyek azt demonstrálták, hogy a SABSA-alapú megközelítés miként tette lehetővé a szervezet számára a gyors reagálást új üzleti prioritások megjelenésekor, például az elosztott energiatermelési erőforrások (Distributed Energy Resources – DER) integrációja során. Emellett ismertetésre került az is, hogyan támogatta ez a modell a **digitális transzformáció** keretében bevezetett, termékközpontú

BBA-PLUSZ-312-24-2024-00003 sz. pályázat részeként

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

és agilis fejlesztési működés kialakítását, valamint miként segítette a digitális termékek összehangolását a releváns iparági ajánlásokkal és szabályozási keretrendszerekkel, többek között az **ISA/IEC 62443** szabvánnyal és az ausztrál energetikai kiberbiztonsági keretrendszerrel (**Australian Energy Cybersecurity Framework – AESCSF v2.0**). Az előadás további fontos eleme volt annak bemutatása, hogyan lehet a biztonsági architektúra artefaktumait szinkronizálni a vállalati architektúra más területeivel, így az üzleti, információs, alkalmazás- és technológiai architektúrával, ezáltal biztosítva az egységes és koherens architekturális működést. Az ismertetett megközelítés alapján a **SABSA olyan átfogó, kockázatalapú architekturális keretként** került bemutatásra, amely komplex és gyorsan változó környezetben stratégiai támogató szerepet tölthet be a szervezeti kiberbiztonság fejlesztésében.

The Grammar of SABSA Attributes

(Kirk Nicholls)

Az előadás középpontjában az információbiztonsági és kockázatkezelési szakemberek munkájában kiemelt szerepet játszó **nyelvhasználat és fogalomalkotás** állt. Bemutatásra került, hogy a kockázatkezelési tevékenységek során különös körültekintéssel szükséges megválasztani az alkalmazott kifejezéseket, mivel az üzleti hajtóerők (**Business Drivers**), az attribútumok (**Attributes**), valamint ezek pontos és következetes definíciói alapvető elemei az Enterprise Security Architecture (**ESA**) eszköztárának. Az előadás rávilágított arra, hogy a **jól megfogalmazott fogalmi keretek** lehetővé teszik az összetett szervezeti és technológiai rendszerek leírását közérthető nyelven, miközben biztosítják a szükséges rugalmasságot és csökkentik a félreértelmezések kockázatát. Ismertetésre kerültek azok az **alapelvek és módszertani eszközök**, amelyek támogatják a robusztus attribútumok kialakítását, valamint bemutatásra került ezek gyakorlati hasznossága az ESA modellezési és elemzési folyamataiban. Az előadás külön hangsúlyt fektetett

arra, hogy a **pontos fogalmazás és a gondosan kialakított definíciók** nem csupán dokumentációs szerepet töltenek be, hanem közvetlen hatással vannak a szervezeti döntéshozatal és a kockázatértékelés minőségére is. A résztvevők betekintést kaptak abba, hogyan lehet a szakmai terminológiát következetesen alkalmazva olyan **attribútumrendszert kialakítani**, amely támogatja az enterprise szintű biztonsági architektúra modellezését, és amelynek kialakítása a lexikográfiai precizitáshoz hasonló alaposságot igényel.

Beyond Taxonomies A New Ontological Lens for SABSA Data Architecture

(Bethany Sinclair-Giardini, Carol Sutton)

Az előadás a **SABSA keretrendszer adatkezelési megközelítésének újraértelmezését** vizsgálta, különös tekintettel arra a jelenségre, hogy a szervezetek gyakran az adatmennyiséget tekintik értéknek, miközben **a valódi érték az adatok értelmezhető tudássá alakításából származik**. Bemutatásra került, hogy a SABSA modellben az adat kezdetben fizikai eszközként jelenik meg, és a hagyományosan alkalmazott eszközök – például az üzleti eszköz-taxonómia és az üzleti attribútum-taxonómia – sokáig hatékony keretet biztosítottak az adatok rendszerezésére, azonban hierarchikus merevségük egyre kevésbé illeszkedik a modern, dinamikus adat-ökoszisztémák működéséhez. Az előadás központi gondolata az volt, hogy a statikus taxonómiai megközelítést érdemes **ontológiai szemlélettel** felváltani, amely **rugalmasabb** módon képes leírni az adatok közötti kapcsolatokat, és ezáltal jobban támogatja a szervezeteket a bizonytalan vagy gyorsan változó környezetben történő döntéshozatalban. Kiemelt témaként szerepelt az **adattisztítás** (data cleansing) mint **adatgazdálkodási alapfeladat**, amelynek elhanyagolása jelentős strukturális és minőségi problémákhoz vezethet; **a metaadatok kettős szerepe**, amelyek egyszerre nyújthatnak mélyebb betekintést az adatokba, ugyanakkor a torzítások felerősítésének eszközei is lehetnek; valamint az OWL (**Web Ontology Language**) alkalmazhatósága, amely megfelelő használat mellett

BBA-PLUSZ-312-24-2024-00003 sz. pályázat részeként

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

az ontológiai modellek kialakításának fontos támogató eszköze lehet, ugyanakkor komplexitása miatt többletterhet is jelenthet a szervezetek számára. Az előadás egy **gyakorlati ontológiai modellt is bemutatott,** amely a SABSA konceptuális és kontextuális rétegeiben alkalmazva képes jobban leképezni a valós üzleti környezet komplex kapcsolatrendszereit, és támogatja azt a szemléletet, amely szerint az adat nem pusztán erőforrásként, hanem kapcsolatok hálózataként értelmezhető. Ennek eredményeként **a SABSA keretrendszer az intuitív, tapasztalati alapú döntéshozatalt strukturált információkkal képes kiegészíteni**, különösen olyan szervezetek esetében, ahol az adat a legfontosabb – vagy akár az egyetlen – stratégiai eszköz.

Architecting Stovepipes of Excellence: A Case Study on Connecting Threat Actors, TTPs, Controls, and Assurance Programs

(Dimitri Vedeneev)

Az előadás egy **valós esettanulmányon keresztül** mutatta be, miként alakítható ki átfogó biztonsági nyomonkövethetőség (**security traceability**) a szervezeti eszközök, az azokat érő fenyegetések és a kockázatcsökkentési beruházások között. Bemutatásra került az a megközelítés, amely szakít azzal a gyakorlattal, hogy a fenyegetettségi hírszerzés (threat intelligence), a védelmi kontrollok, az ellenőrzési tevékenységek és a biztonsági architektúra egymástól elszigetelten működjenek, és ehelyett egy olyan **integrált szemléletet alkalmaz**, amely **a modern szervezetek különböző területeit közös keretbe szervezi.** Az előadás ismertette, hogy a folyamat első lépéseként a **fenyegetési szereplők profilozása** történt meg, figyelembe véve céljaikat, képességeiket és a tipikusan célba vett szervezeteket. Ezt követően a támadók által leggyakrabban alkalmazott **taktikák és technikák feltérképezése** történt meg a **MITRE ATT&CK** keretrendszer segítségével. A módszertan kulcseleme az volt, hogy ezeket a támadási mintákat közvetlen kapcsolatba hozták a már **meglévő biztonsági kontrollokkal**, amely lehetővé tette a szervezet

számára, hogy egyértelműen azonosítsa a kritikus védelmi hiányosságokat, valamint azokat a területeket is, ahol indokolatlanul magas erőforrás-ráfordítás történt. Az elemzés során felszínre kerültek többek között a helyreállítási eljárások gyengeségei, a rendszerek közötti függőségek hiányos feltérképezése, valamint az operatív reziliencia célkitűzéseinek pontatlansága. Az így kialakított **összefüggésrendszer** lehetővé tette annak bemutatását a vezetés számára, hogy az egyes fenyegetések miként kapcsolódnak közvetlenül az üzleti kockázatokhoz, valamint hogy a biztonsági beruházások valóban a releváns kockázatok csökkentését szolgálják. A prezentációban kiemelt szerepet kapott a **SABSA architektúra-keretrendszer** is, amely a teljes folyamat során biztosította a biztonsági követelmények, a kontrollok és az üzleti célok közötti nyomonkövethetőség fenntartását.

Using Security Patterns to Protect Cloud

(Ken Fitzpatrik)

Az előadás a **biztonsági minták** (security pattern) **fogalmának és céljának bemutatásával** indult, külön kitérve arra, hogy ezek miként illeszkednek a SABSA architekturális keretrendszerhez. Ismertetésre került, hogy az iparágban többféle definíció és megközelítés létezik, különösen a nagy felhőszolgáltatók – például az AWS és az Azure – által publikált minták esetében, ugyanakkor hangsúlyt kapott annak bemutatása, hogy a gyakorlatban hogyan lehet azonosítani és kiválasztani a valóban hasznos és alkalmazható biztonsági mintákat. Az előadás ezt követően **a hatékony biztonsági minták megírásának és alkalmazásának módszereit** ismertette, bemutatva azokat a bevált gyakorlatokat, amelyek támogatják a következetes biztonsági tervezést, valamint azokat a tipikus hibákat, amelyek a minták kialakítása vagy használata során gyakran előfordulnak. Részletesen ismertetésre került az is, hogy a biztonsági minták miként integrálhatók a szervezeti gyakorlatba, és hogyan járulhatnak hozzá a biztonsági architektúra minőségének és következetességének javításához. Az előadás külön kitért arra is, hogy a biztonsági minták

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

alkalmazása sok esetben **gyakorlati szempontból hatékonyabb** megközelítést kínál, mint a kizárólag biztonsági szabványokra épülő tervezés, mivel a patternök konkrét architekturális problémákra adnak újrahasznosítható megoldásokat. Bemutatásra kerültek a SABSA keretrendszerhez illeszkedő **biztonsági minták létrehozásának alapvető lépései**, valamint egy gyakorlati példa is, amely egy **AWS környezetben alkalmazott biztonsági mintát** ismertetett, rávilágítva arra, hogy a szervezetek miként használják ezeket a megközelítéseket a rendszertervezés biztonsági megfelelőségének és megbízhatóságának biztosítására.

Privacy by Design: Building An adaptive Security Architecture

(Steven Bradley)

Az előadás a kiberbiztonsági szervezetek irányítási, kockázatkezelési, megfelelőségi és biztosítási keretrendszereinek (governance, risk, compliance, assurance) kialakítására ható aktuális tényezőket vizsgálta, különös tekintettel a döntéshozatali modellek átalakulására. **Bemutatásra került egy új szemlélet,** amely a hagyományosan központosított irányítási struktúrákkal szemben a **decentralizált működést helyezi előtérbe**, ahol a gyors döntéshozatal és az egyértelmű felelősségi körök fontosabb szerepet kapnak, mint a hierarchikus kontrollmechanizmusok. Az előadás rámutatott arra, hogy az ilyen **adaptív biztonsági modell alapfeltétele** a szervezet minden szintjén megvalósuló döntéshozatali képesség, amely csak hatékony kommunikáció és egy közös, mindenki számára elérhető és hiteles adatforrásra („single source of truth”) épülő információs környezet mellett működhet. A prezentáció során ismertetésre került egy olyan **biztonsági architektúra** kialakításának gyakorlati tapasztalata, amely ezen elveket követve kontrollmodellezésre, előre meghatározott küszöbértékekre, valamint valós idejű biztonsági adatok feldolgozására épül. Az előadók bemutatták, hogy egy **architekturális megközelítés** miként támogathatja a szervezeteket a gyorsan változó fenyegetési környezethez való alkalmazkodásban, különösen azokban az

esetekben, amikor a hagyományos, központi irányításra épülő biztonsági struktúrák már nem biztosítanak kellően rugalmas működést. Az ismertetett megközelítés gyakorlati **példákon keresztül mutatta be**, hogy a valós idejű biztonsági adatok, a kontrollalapú modellezés és a szervezeti szintű döntéshozatal integrációja miként járulhat hozzá egy hatékonyabb és adaptívabb kiberbiztonsági működési modell kialakításához, amely több szervezet számára is releváns lehet hasonló működési és irányítási kihívások esetén.

From Chessboard to Boardroom: A Shift in Ideology to Harness World Class Talent with SABSA

(Andrea Cimpean)

Az előadás középpontjában az a gondolat állt, hogy a vállalati biztonsági architektúrák tervezése során a **„tehetség" mint stratégiai érték** ritkán jelenik meg védendő erőforrásként, pedig hosszú távon ez is olyan **kritikus vagyonelem** lehet, amelynek fejlesztése, fenntartása és kockázatkezelése tudatos megközelítést igényel. A prezentáció a SABSA módszertan szemléletét alkalmazva mutatta be, **miként modellezhető és támogatható a kiemelkedő emberi teljesítmény kialakulása és fenntarthatósága**. Az előadás kiindulópontját a **Polgár nővérek oktatási kísérlete** jelentette, amely azt a feltevést vizsgálta, hogy a **zsenialitás** nem feltétlenül veleszületett tulajdonság, hanem **tudatosan kialakított környezeti és fejlesztési tényezők eredménye** lehet. Ennek analógiájára bemutatásra került, hogy a SABSA keretrendszer hogyan használható a tehetséghez kapcsolódó, nehezen mérhető immateriális értékek strukturált értelmezésére, valamint arra, hogy ezekhez célok, kontrollok és mérőszámok rendelhetők legyenek. A prezentáció kitért arra is, miként lehet a tehetséget mint „asset"-et azonosítani, mérni és a hozzá kapcsolódó kockázatokat kezelni, például a fejlődési környezet, a képzési folyamatok vagy a versenyfelkészülés strukturált tervezésén keresztül. A téma illusztrálására a versenysakk világából származó tapasztalatok kerültek bemutatásra,

BBA-PLUSZ-312-24-2024-00003 sz. pályázat részeként

BBA+ BESZÁMOLÓ

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

beleértve a junior világbajnokságokra való felkészülés során alkalmazott módszereket, a hosszú távú stratégiai tervezés jelentőségét, valamint azokat a sikereket és kudarcokat, amelyek rámutatnak arra, hogy a tehetség fejlődése számos, tudatosan alakítható tényező eredője. Az előadás így arra a kérdésre is választ keresett, hogy a tehetség inkább veleszületett adottság-e, vagy inkább gondosan felépített fejlesztési és környezeti rendszer eredménye, és bemutatta, hogy **az információbiztonsági architektúrák gondolkodásmódja hogyan alkalmazható az emberi potenciál strukturált fejlesztésének és fenntarthatóságának értelmezésére.**

Why Misinformed Teams Build Weak Security Programs

(Martin Choluj)

A szakmai tapasztalatok alapján a **leghatékonyabb információbiztonsági programok alapja** nem a költségvetés mértéke vagy az alkalmazott eszközök száma, hanem a **releváns adatokon alapuló kontextus,** amelynek hiányában a védelmi stratégiák elkerülhetetlenül elbuknak a valós fenyegetésekkel szemben. Az előadáson bemutatásra került, hogy a megfelelő adatkontextus nélkül működő biztonsági csapatok gyakran kénytelenek feltételezésekre alapozni döntéseiket, ami a tényleges kockázatokhoz nem illeszkedő kontrollok bevezetéséhez, valamint a prioritások hibás meghatározásához vezet. A prezentáció **esettanulmányokon keresztül szemléltette**, miként képes az **adatvezérelt megközelítés** hatékonyabbá tenni a fenyegetésmodellezést (threat modelling), az incidensreakciót és a kockázatértékelési folyamatokat. Ismertetésre kerültek továbbá olyan stratégiai módszerek, amelyek segítségével kontextusfüggő biztonsági funkciók hozhatók létre, olyan kommunikációs csatornák és folyamatok kiépítésével, amelyek az iparági felhajtás (hype) helyett a ténylegesen releváns, bizonyítékokon alapuló információkra összpontosítanak.

See No Evil?: Visualising Security Risk

(Steven Bradley)

Az információbiztonság egyik meghatározó alapművére, **Bruce Schneier Secrets & Lies** című könyvére alapozva az előadás során **elemzésre került az emberi kockázatérzékelés és a digitális fenyegetések közötti feszültség**, rámutatva, hogy a mindennapi életben jól működő ösztönök miért vallanak kudarcot az informatikai rendszerek elemzésekor. Bemutatásra kerültek a **kockázatészlelést torzító legfontosabb tényezők**, úgy mint a ritka események kiértékelésének nehézsége, az informatikai bizalmat érintő megerősítési torzítás (confirmation bias), valamint a kontrollérzet és a fenyegetések megszemélyesíthetőségének hatásai. A **kiberbiztonsági kockázatelemzést** különösen **összetetté teszik** a rendszerek közötti sok-sok kapcsolatú (many-to-many) összefüggések a kockázatok, vektorok, sérülékenységek, támadók és kontrollok mentén, ami jelentős kihívás elé állítja a GRC (Governance, Risk, and Compliance) és minőségbiztosítási keretrendszerek tervezőit az erőforrások optimalizálása során. Az előadáson ismertették az **Enterprise Architecture** (EA) eszközök azon legújabb fejlesztéseit, amelyek a kiberbiztonsági kockázatok vizualizációja révén kínálnak megoldást, lehetővé téve a virtuális környezettel való intuitív interakciót és a mélyebb helyzetfelismerést. A bemutatott **gyakorlati demonstráció** rávilágított arra, hogy a hagyományos, dokumentum alapú megközelítéssel szemben a **vizualizáció miként járulhat hozzá a biztonsági menedzsment hatékonyságához** a komplex összefüggések érthetőbbé tételével.

BBA-PLUSZ-312-24-2024-00003 sz. pályázat részeként

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

Architecting Cyber Security Self-Assurance

(Dimitrios Delivasilis)

A **kiberbiztonsági kockázat** napjainkban a szervezetek egyik legjelentősebb nem pénzügyi jellegű fenyegetése, amely a **digitális műveletek szinte minden területén jelen van**, és amelynek kezelését a támadások összetettsége, valamint a támadói képességek folyamatos fejlődése teszi rendkívül bonyolulttá. Az előadáson rávilágítottak arra, hogy a kiberkockázatok megfogalmazását gyakran magas fokú **szubjektivitás** jellemzi, mivel a biztonsági helyzetről szóló, időszerű adatokkal alátámasztott, teljes körű (360 fokos) kép kialakítása alapvető üzleti kérdések esetén is nehézségekbe ütközik. A prezentáció középpontjában az állt, miként támogathatja a gyorsabb és hatékonyabb döntéshozatalt a **biztonsági struktúra adatvezérelt, átfogó reprezentációja**, amely valós esettanulmányokon keresztül szemléltette az egyetlen hiteles adatforrás (single source of truth) szerepét a végrehajtható felismerések azonosításában és a javító intézkedések egyszerűsítésében. Bemutatásra került, hogy ez **az adatközpontú megközelítés** teremti meg az alapot a teljes infrastruktúrára kiterjedő önbiztosítási folyamatok (self-assurance) értelmezhető formává alakulásához, ami a kiberbiztonsági erőforrások optimalizálása mellett a folyamatok gördülékenyebbé tételével közvetlen üzleti és kereskedelmi előnyöket is biztosít a szervezet számára.

Authorised and Compromised – The Biometric Illusion

Előadó: Gaurav Vikash

A **biometrikus azonosítás** elterjedésével kapcsolatos rendszerszintű kockázatok elemzése során bemutatásra került, hogy bár e technológiát a **jelszavak kiváltására szánták**, a gyakorlatban **visszavonhatatlan és megváltoztathatatlan kulcsokká váltak**, amelyek komoly biztonsági

aggályokat vetnek fel. Az előadáson ismertették, hogy a **biometrikus adatok eredendően magas kockázatot hordoznak**, mivel ellentétben a jelszavakkal, **kompromittálódás esetén nem módosíthatók,** mégis a jelenlegi tárolási és továbbítási modellek többsége nem kezeli őket ennek megfelelő prioritással. **Valós példákon keresztül**, az indiai Aadhaar-rendszer adatszivárgásaitól a kereskedelmi forgalomban lévő okostelefonok arcfelismerő rendszereinek kijátszásáig **szemléltették**, hogy **a kényelmi szempontok gyakran felülírják a biztonságot**, miközben a biometrikus hamisítás (spoofing) és a téves pozitív eredmények kihasználása a kiforrott rendszerekben is jelenlévő fenyegetés. Rávilágítottak arra is, hogy a biometrikus rendszerekben alkalmazott hozzájárulási és átláthatósági folyamatok sokszor csupán formálisak, a legtöbb implementáció pedig kénytelen kompromisszumot kötni a pontosság, az auditálhatóság és a felhasználói jogok között. Zárásként elhangzott, hogy bár léteznek **módszerek a biometria biztonságos alkalmazására**, azok magas költségük és technológiai komplexitásuk miatt ritkán valósulnak meg a gyakorlatban a megfelelő szakmai sztenderdek szerint.

BBA-PLUSZ-312-24-2024-00003 sz. pályázat részeként

If Socrates was a CISO or Even Worse - Your Business Stakeholder

(Dimitrios Delivasilis)

A **kiberbiztonsági kockázatok összetettsége és kiterjedtsége** napjainkra az egyik legjelentősebb nem pénzügyi fenyegetéssé vált, amely a digitális műveletek szinte minden szegmensét érinti, folyamatos döntéshozatali kényszer elé állítva a szervezeteket az üzleti stratégia és a megfelelő szintű védelem egyensúlyának fenntartása érdekében. Az előadáson hangsúlyozásra került, hogy az **optimális haladási irány** meghatározásához az információk pontossága, teljessége és időbeni hozzáférhetősége kritikus fontosságú, ugyanakkor a megoldást szokatlan módon az ókori filozófia eszköztárában keresték. Bemutatásra került, **miként alkalmazható a szókratészi módszer az információbiztonsági kockázatkezelésben**, ahol az interaktív dialógus és a kérdezéstechnika

BBA+ BESZÁMOLÓ

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

lehetővé teszi a rögzült feltételezések tesztelését, a másfajta gondolkodásmódot és a meghozandó döntések következményeinek mélyebb megértését. A prezentáció során szemléltették, hogy a kiberbiztonsági szakemberek hogyan meríthetnek erőt a "**kontrariánus**", azaz az általánossal szembehelyezkedő gondolkodásból, és miként használhatják azt eszközként mind a tudatlanság feltárására, mind a valódi, **megalapozott tudás és biztonsági helyzetkép** kialakítására.

Architecting Human Resilience: Embedding Cyber-Aware Business Simulation into Enterprise Practice

(Derek Grocke)

A kiberfenyegetések folyamatos fejlődése mellett a **vállalati biztonsági tudatossági képzések stagnálása jelentős kockázatot hordoz**, amire megoldásként az előadáson a vállalati és biztonsági architektúra-alapú megközelítések, valamint a szimulációs és immerzív tréningek operatív gyakorlatba történő beágyazása került bemutatásra. Védelmi szektorból, kormányzati szervektől és szabályozott iparágakból származó, terepen tesztelt módszerek alapján ismertetésre került egy olyan **egységes modell**, amely az élményalapú tanulást, az architektúra-domaineket és a rendszerszemléletű gondolkodást ötvözve **teszi a megerősítő tanulást a mindennapi üzleti folyamatok részévé.** A prezentáció keretében újraértelmezték a hagyományos asztali gyakorlatokat (tabletop exercise), rávilágítva, hogy a folyamatorientált digitális iker-környezetek, a kiber lőterek (cyber range) és az üzletileg összehangolt szimulációs modellek nem csupán a technikai felkészültséget, hanem a **valós döntéshozatalt és az incidensreakció koordinációját** is fejlesztik.

Az előadáson hangsúlyozták, hogy a **valós világot modellező szimulációk** miként képesek követni a vállalati prioritásokat és szabályozási kötelezettségeket, miközben kiemelt figyelmet fordítottak az

architekturális irányításra, az életciklus-integrációra, valamint az olyan szabványokhoz való illeszkedésre, mint a **NIST SP 800-160, az ISO 42010** vagy az ausztrál kormányzati védelmi biztonsági politikai keretrendszer (**PSPF**).

Fear of the Dark

(Steven Kintakas)

Az **informatikai szektorban** gyakran használt „**legacy**" kifejezés **az elöregedő hardverekre, operációs rendszerekre és szoftverkörnyezetekre utal**, amelyeket a szervezetek gyakran az eszközök élettartamának végső kihasználása (sweating assets) érdekében tartanak üzemben, dacolva az életciklus-kezelés és a támogatás megszűnésének (end-of-life) kockázataival. Az előadáson bemutatásra került, hogy bár **ezek a rendszerek sokszor felügyelet nélkül is tovább működnek** és megtérülést termelnek, a gyártói támogatás hiánya, az alkatrészellátás akadozása, a szakértelem elvesztése és a növekvő sebezhetőségek miatt a környezet fejlődésével párhuzamosan **exponenciálisan nő a biztonsági kockázatuk**. A prezentáció rávilágított az érme másik oldalára is: a ma „következő generációsnak" vagy „élvonalbelinek" nevezett **technológiák jövőbeli fenntarthatóságára,** valamint a tervezett elavulás jelenségére, amely a „sötétségtől való félelem" metaforáján keresztül szemlélteti azt az állapotot, amikor a kritikus rendszerek váratlanul és helyreállíthatatlanul működésképtelenné válnak. Az elemzés során a **technológiai adósság** technológiai **felelősséggé** és elsüllyedt **költséggé** való átalakulását vizsgálták, amely a produktivitás csökkenése mellett akár a teljes üzemmenet leállásához és jelentős társadalmi-gazdasági károkhoz is vezethet. A szakmai diskurzus **célja** annak feltérképezése volt, hogy **a kiberbiztonsági szakemberek miként navigálhatnak e rejtőzködő kockázatok között, és hogyan kezelhetik a hosszú távú rugalmasság (resilience) és fenntarthatóság kihívásait** mind szervezeti, mind egyéni szinten.

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

Not Just Lean. But Lean & Mean.

(Joshua Qwek)

A **kiberbiztonsági képességek kiépítése** minden szervezetnél tudatos megközelítést igényel, amelynek során **meg kell találni az egyensúlyt** a szervezeten belül ható különféle érdekek és erővonalak között. Az előadáson elhangzott, hogy bár az első alkalommal is **sikeres implementáció** nem lehetetlen, ehhez többre van szükség egy egyszerű keretrendszer vagy módszertan puszta bevezetésénél. Bemutatásra került a **fejlődési út**, amelyen keresztül egy szervezet túlléphet a puszta hatékonyságra törekvő (lean) működésen, és egy olyan agilis, egyben határozott stratégiát alakíthat ki, amelyben minden egyes erőforrás és befektetés a lehető legnagyobb **hozzáadott értéket** képviseli. A prezentáció rávilágított arra, hogy a **védekezési pozíció miként alakítható át reaktívból proaktívvá**, biztosítva, hogy a kiberbiztonsági funkciók ne csupán követő, hanem alakító tényezőivé váljanak a vállalati folyamatoknak és a fenyegetések elleni fellépésnek.

2026. február 26. napi előadások összegzése

Building an AI Fast Track Agent

(Dr Malcolm Shore)

A konferencia harmadik napján a résztvevők **három egész napos workshop** közül választhattak. Mivel a kínálatban szereplő programok közül kettő specifikusan a csendes-óceáni térség sajátosságaira és az ottani párbeszédre fókuszált, delegációnk a **technológiai fókuszú „Building an AI Fast Track Agent” szekció** mellett döntött. Ez a választás lehetővé tette **a mesterséges intelligencia gyakorlati alkalmazásaiban** való mélyebb elmerülést és a különböző technikai implementációk folyamatainak elsajátítását.

Az első szekció során az **AI technológia alapjai és a gépi tanulástól az agentekig** (magyarul „ügynökök”) tartó fejlődési folyamat került ismertetésre a **Google Colab felületén** végrehajtott **gyakorlati bemutatókkal** együtt. A foglalkozás alatt olyan **feladatok lettek szemléltetve**, mint a képek tartalmának felismerése, a kártékony utasítások kiszűrése, valamint a **TCRTE** (Feladat, Kontextus, Szerep, Hangnem, Példa) prompt engineering keretrendszer alkalmazása. Az elméleti modul keretében a különböző agent-struktúrák és a RAG-rendszerek (Lekéréssel kiegészített generálás) mellett az **OWASP** szerinti legfontosabb kockázatok, mint például az **Agent Goal Hijack** (agent céljainak eltérítése), a **Tool Misuse** (eszközökkel való visszaélés) és a **Memory Poisoning** (memóriamérgezés) kerültek részletesen elemzésre. Ezen fenyegetések ellensúlyozására olyan „guardrail-megoldások” lettek bemutatva, mint a **Policy & Governance** (szabályozási és irányítási elvek), a **Human-in-the-loop** (folyamatba épített emberi ellenőrzés), valamint a bemeneti validáció és a kimeneti eredmények szűrése.

A második szekció keretében a folyamatos **tanulásra alkalmas, memória-központú agent megoldások** kerültek bemutatásra, ahol a memória-alrendszerek fejlődése lett szemléltetve az egyszerű tárolástól a rövid és hosszú távú memóriát használó architektúrákig. A gyakorlati részben a **Google Vertex platformja**, valamint a **Hindsight** mint többszintű memóriát kínáló, úgynevezett **memory-first** (memóriát preferáló) **rendszer** került ismertetésre.

Értékelés

A **konferencián elhangzott témák** több ponton is **támogatták a Belső Biztonsági Alap célkitűzését**, vagyis a kibertérben elkövetett, súlyos és szervezett – akár határon átnyúló – bűncselekmények felderítését és a kapcsolódó büntetőeljárások eredményességét. A **SABSA/NIST CSF/ISO 27001 fókuszú előadások** olyan módszertani eszközt adtak, amellyel a fenyegetések, kontrollok és döntések nyomon követhetően, auditálható módon kapcsolhatók össze, ezáltal javítva

BBA+ BESZÁMOLÓ

az incidensek kezelését és a bizonyítékok rendszerezését. A „**traceability**” megközelítés (szereplők–TTP-k–kontrollok összerendezése) segíti a hiányosságok priorizálását és a vezetői döntések megalapozását. A **Zero Trust, felhőbiztonsági minták és reziliencia témák** a hatáscsökkentést, a jobb naplózást és a rekonstruálhatóságot erősítették, ami közvetlenül támogatja a felderítést. Emellett a **digitális nyomokkal és AI-agent kockázatokkal** foglalkozó szekciók naprakész tudást adtak az új támadói módszerekről és azok mitigációjáról, elősegítve a kiberbűnözési ügyekben szükséges együttműködést és szakmai felkészültséget.

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