NEMZETI KIBERBIZTONSÁGI INTÉZET



HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 48. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- TÁJÉKOZTATÁS
- CTI JELENTÉS
- BBA+ BESZÁMOLÓ

KIBERTÁMADÁS! PODCAST

NEMZETI KIBERBIZTONSÁGI INTÉZET



HÍREK

Bankkártyaadatokat loptak el a Cleverbridge rendszereiből

(bleepingcomputer.com)

Adatvédelmi incidens érte az e-kereskedelmi platformot üzemeltető Cleverbridge-et, amelynek során a támadók az ügyfelek fizetési kártyaadatainak másolatához jutottak hozzá. A megszerzett információk között bankkártyaszámok, lejárati dátumok és CVV/CVC biztonsági kódok is szerepelnek. **Bővebben...**

Kínához köthető hackercsoport támadhatta meg az Európai Bizottság informatikai rendszereit

(euronews.com)

Az Európai Bizottság gyanúja szerint egy Kínához köthető hackercsoport állhat a szervezet informatikai rendszereit immár egy hónapja érintő, jelenleg is zajló kibertámadás mögött. A Bizottság informatikai részlege október 22-én észlelte a behatolást a belső hálózatában, azonban a támadást azóta sem sikerült teljesen megfékezni. **Bővebben...**

A LearnWorlds ingyenes próbaidőszakát használták fel adathalász kampányhoz

(quickscopeintel.com)

A The Register 2026. november 16-i beszámolója szerint egy támadó kihasználta a LearnWorlds ingyenes próbaidőszakra vonatkozó regisztrációs rendszerét, és 13 ezer adathalász e-mailt küldött ki, amelyekben hamis, YouTube-szerzői jogok megsértéséről szóló értesítéseket küldött. A támadás során a LearnWorlds alapvető rendszereit nem törték fel. **Bővebben...**

Újabb védelmi megoldás érkezik a Signalra

(bleepingcomputer.com)

A Signal üzenetküldő alkalmazás új védelmi funkciót vezet be, amelynek célja, hogy megakadályozza a beépített mesterséges intelligencia által vezérelt asszisztensek privát üzenetekhez történő hozzáférését iOS és Android rendszereken. **Bővebben...**

Csalási kampány során is kihasználhatták a WhatsApp egy hibáját

(securityweek.com)

Nemrég került javításra a WhatsApp egy alacsony besorolású hibája, amely kihasználása hitelesebbnek tűnő megtévesztő üzenetek megjelenítését tette lehetővé a csalók számára. A CVE-2026-23871 azonosítójú sebezhetőség a WhatsApp Android és a WhatsApp Business for Android alkalmazásokat érintette. **Bővebben...**

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

2026. 11. 20. - 2026. 11. 26.

Fenyegetettségi szint:

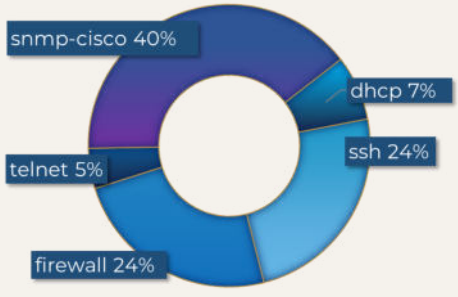
alacsony | közepes | **magas** | kritikus

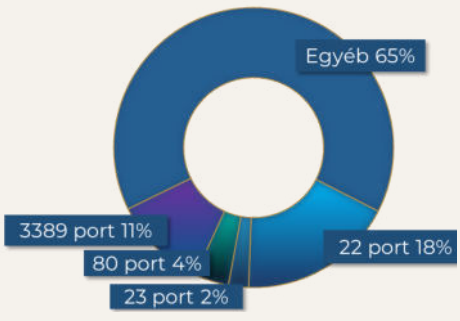
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok

Az adatsorok melletti nyilak az előző héthez viszonyított változásokat mutatják.



Az elosztott kormányzati IT biztonsági csapdarendszerből (GovProbe1) származó adatok





NEMZETI KIBERBIZTONSÁGI INTÉZET



TÁJÉKOZTATÁS

Tájékoztatás a Microsoft Entra Connect Health szolgáltatást érintő adatvédelmi incidensről

Felhívjuk figyelmét, hogy **adatvédelmi incidens** történt a **Microsoftnál**, miután a támadók kihasználták a **Microsoft Entra Connect Health** szolgáltatás API-ját érintő sérülékenységét.

A sérülékenység kihasználásával **jogosulatlan hozzáférést** szereztek rendszergazdai e-mail-címekhez, valamint tenantok konfigurációs adataihoz.

Elolvasom

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



NEMZETI KIBERBIZTONSÁGI INTÉZET

CTI JELENTÉS

A hackerek világa

Jelen dokumentum célja, a **hacker fogalom** kialakulásának és történeti fejlődésének rövid bemutatása, valamint az egyes **hackertípusok** és azok jellemzőinek részletes ismertetése.

A jelentés emellett kitér arra is, hogy a különböző szereplők **milyen célokkal és módszerekkel** alkalmazhatják technikai ismereteiket, illetve **milyen szerepet tölthetnek be** a kiberbiztonságban.

Elolvasom

Érdekesnek találta elemzésünket? Szívesen olvasna hasonló témakörben?

Figyelmébe ajánljuk *„Hozzáférési malware-ek”* című jelentésünket!



NEMZETI KIBERBIZTONSÁGI INTÉZET

BBA+ BESZÁMOLÓ

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

ENISA Cybersecurity Skills Framework Conference 2026

2026. november 4 - 5.

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.





NEMZETI KIBERBIZTONSÁGI INTÉZET

A Nemzeti Kiberbiztonsági Intézet munkatársai **2026. novenómber 4 - 5.** között részt vettek a **Larnacaban** megrendezésre kerülő éves **ENISA Cybersecurity Skills Framework** konferencián.

A **rendezvény célja** az európai kiberbiztonsági készségfejlesztés teljes ökoszisztémájának összekapcsolása volt. Az uniós intézmények, a tagállamok, az iparági szereplők, az akadémiai szféra és a képzési szolgáltatók képviselői tapasztalatokat cserélhettek, megvitathatták az új kihívásokat, és bemutathatták a kiberbiztonsági kompetenciák fejlesztésének jó gyakorlatait.

A **konferencia legfontosabb üzenete**, hogy Európa kiberbiztonsági ellenálló képessége jelentős mértékben függ a rendelkezésre álló szakértelemtől és a szolgáltatások megbízhatóságától. Az egységes európai kompetenciakeretek, a szakmai készségek elismerése és a szolgáltatók tanúsítása egyaránt hozzájárulhat ahhoz, hogy a szervezetek felkészültebben kezeljék a növekvő kiberfenyegetéseket.

- Kiberbiztonsági szakemberek számára
- Kiberfenyegetés-kutatóknak és elemzőknek
- Biztonsági mérnököknek és fejlesztőknek

A konferencia legfontosabb előadási az alábbiakban foglalhatók össze.

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



BBA+ BESZÁMOLÓ

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

A konferencia négy kiemelt stratégiai témakör köré épült:

1. A kiberbiztonsági kompetenciák európai elismerése:

Az egyéni kiberbiztonsági készségek tanúsítására, illetve elismertetésére vonatkozó uniós javaslat célja az átláthatóság, az összehasonlíthatóság és a kompetenciákba vetett bizalom erősítése, valamint a szakemberek EU-n belüli mobilitásának támogatása.

2. A mesterséges intelligencia hatása:

Az AI terjedése jelentősen átalakítja a kiberbiztonsági munkaköröket és az elvárt kompetenciákat. A téma az EU AI Action Plan összefüggésében is megjelent.

3. Az Európai Kiberbiztonsági Készségkeretrendszer (ECSF) felülvizsgálata:

A keretrendszer korszerűsítésének célja, hogy jobban igazodjon a biztonságos digitális termékek teljes életciklusához, az új technológiákhoz – különösen a mesterséges intelligenciához –, valamint az uniós szakpolitikai és jogszabályi változásokhoz. Az új változat kompetenciaszinteket is bevezet, amelyek segíthetik a képzési utak, a karrierfejlesztés és a munkaerő-felmérés egységesítését.

4. Az európai együttműködés erősítése:

A konferencia hangsúlyozta az uniós intézmények, a tagállamok, az iparág, a felsőoktatás és a képzési szolgáltatók közötti együttműködés fontosságát az európai kiberbiztonsági szakemberhiány kezelésében. A rendezvény két kiemelt előadása a kiberbiztonsági szakember-utánpótlás és kompetenciafejlesztés jövőjével, valamint a menedzselt biztonsági szolgáltatások (Managed Security Services – MSS) európai tanúsításának kialakításával foglalkozott. Ezek mellett további előadások vizsgálták a munkaerőpiaci igényeket, az oktatás és továbbképzés szerepét, valamint az állami és piaci szereplők együttműködésének lehetőségeit.



Az előadásokból kirajzolódott, hogy az európai kiberbiztonság megerősítéséhez nem elegendő a technológiai fejlesztés: megfelelően képzett szakemberekre, egységes kompetenciakeretekre, megbízható szolgáltatókra és az állami, illetve piaci szereplők szoros együttműködésére is szükség van.

Beyond Today's Skills: Building Europe's Cybersecurity Workforce for the Future

[Evangelos Ouzounis, ENISA]

Az **előadás központi üzenete** az volt, hogy a **kiberbiztonsági szakemberhiány** már nem egyszerű munkaerőpiaci probléma, hanem **Európa digitális ellenálló képességét alapvetően befolyásoló stratégiai kérdés**. Az Európai Bizottság State of the Digital Decade 2026 jelentése a kiberbiztonság kompetenciahiányt az EU kiberfenyegetettségét meghatározó öt strukturális tényező egyikeként azonosítja. Az előadáson bemutatott adatok szerint:

2024. júliusa és 2025. júniusa között közel 4900 jelentős kiberbiztonsági incidens történt az Európai Unióban. A kiberbiztonsági szakemberek 59%-a kritikusnak vagy jelentősnek ítéli saját kompetenciahiányát. Ez az arány 2024-ben még 44% volt. Az Európai Unió 2030-ra kitűzött, 20 millió információs és kommunikációs technológiában (a továbbiakban: IKT) jártasszakemberre vonatkozó céljának mindössze 52%-a teljesült. Az uniós IKT-szakemberek kevesebb mint 20%-a nő, és ezen a területen 2015 óta csak minimális előrelépés történt.

A probléma kezelésének egyik fontos eszköze a 2026. januárjában előterjesztett új **Cybersecurity Act 2** (CSA2) javaslat. A tervezet a kiberbiztonsági készségeket az európai kiberbiztonsági keretrendszer központi elemévé kívánja tenni. Ennek részeként jogi alapot teremtene az **Európai Kiberbiztonsági Készségkeretrendszer** (ECSF) számára, valamint európai tanúsítási rendszereket vezetne be az egyéni kiberbiztonsági kompetenciák elismerésére.

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



BBA+ BESZÁMOLÓ

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

Az ECSF-et már 19 tagállam alkalmazza különböző formákban, például nemzeti szabványként, képzési programok kialakításához, közszférában munkaerő-felvételnél és a munkaerő kompetenciáinak felmérésére.

Az ENISA munkája három fő területre épül:

1. A szerepkörök meghatározása: egységes európai fogalomrendszer kialakítása a kiberbiztonsági munkakörökre és kompetenciákra.

2. A készségek strukturálása: kompetenciaterületek és tudásszintek meghatározása, beleértve az egyes munkakörökhöz szükséges, mesterséges intelligenciához kapcsolódó készségeket is.

3. A kompetenciák elismerése: az igazolt készségek hitelességének és a szakmai minősítésekbe vetett bizalomnak az erősítése.

A kompetenciák elismerése különösen fontos az olyan területeken, ahol gyorsan és megbízhatóan bevethető szakemberekre van szükség. Ilyen például az **EU Cybersecurity Reserve,** amely a 2025. februárjában hatályba lépett **Cyber Solidarity Act** keretében megbízható és megfelelően képzett incidenskezelő szakemberek rendelkezésre állását célozza.

Managed Security Service Certification

[Georgia Bafoutsou, ENISA]

A téma jelentőségét a növekvő és egyre kifinomultabb kibertámadások, a komplex digitális és hibrid informatikai környezetek, valamint a külső biztonsági szolgáltatókra való fokozódó szervezeti támaszkodás adja. A szervezetek számára ezért **egyre fontosabb** annak igazolása, hogy az általuk igénybe vett **szolgáltatók megfelelő szakértelemmel, átlátható működéssel és megfelelő elszámoltathatósággal rendelkeznek**.



Az ENISA jelenleg egy európai tanúsítási rendszer előkészítésén dolgozik a menedzselt biztonsági szolgáltatásokra vonatkozóan, elsőként az incidenskezelési szolgáltatások területére összpontosítva. Fontos különbség, hogy a tervezett MSS-tanúsítás nem az egyes munkavállalók személyes tanúsítását jelenti, hanem a szolgáltató szervezet megfelelőségét vizsgálja. Ugyanakkor a rendszer meghatározott szakmai szerepkörökhöz kapcsolódó kompetenciakövetelményeket is tartalmaz. Ezek kialakításánál többek között az **ISO/IEC 27035-2:2022** szabványra és a **TS 18072** dokumentumra támaszkodnak.

Példaként az incidenskezelési koordinátor (Incident Response Coordinator) szerepkör hangzott el.

Cybersecurity Workforce Demand & Skills Evolution

[Adam TSAKALIDIS, CEDEFOP]

Az előadásban **bemutatott kutatás** azt vizsgálta, hogyan követhető közel valós időben az európai kiberbiztonsági munkaerő iránti kereslet, valamint a kapcsolódó kompetenciaelvárások változása.

Az elemzés az **Eurostat és a Cedefop Web Intelligence Hub** adataira épült, középpontjában pedig az **online álláshirdetések nagy volumenű vizsgálata** állt. A kutatás nemcsak azt tárta fel, hogyan oszlanak meg a szűkebb és tágabb értelemben vett biztonsági szerepkörök, hanem azt is, milyen tudást, kompetenciákat és tanúsítványokat várnak el a munkáltatók, illetve miként alakítja át a piacot a mesterséges intelligencia térnyerése és a szenioritással kapcsolatos elvárások változása.

Kiberbiztonsági szemmel ennek különös jelentősége van: a **szervezeti ellenálló képesség** ma már nem kizárólag technológiai kérdés. Legalább ilyen fontos, hogy megfelelően értsük a munkaerőpiaci szűk keresztmetszeteket, a szükséges kompetenciák változását és azt, hogy a security egyre több, hagyományosan nem biztonságinak tekintett munkakör részévé válik.

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



BBA+ BESZÁMOLÓ

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

Szakmai résztvevőként különösen érdekes volt látni, hogyan próbálja a kutatás meghaladni a hagyományos, lassabban frissülő kérdőíves felmérések korlátait. Az online álláshirdetések automatizált, nyelvi modellekkel támogatott feldolgozása több százmillió hirdetésből indult ki, a részletes elemzés pedig egy 2021 és 2025 közötti, négy nyelvet lefedő, 22,5 millió álláshirdetésből álló mintára épült.

A kutatók szintetikus álláshirdetési címekkel finomhangolt nyelvi modelleket alkalmaztak, amelyek segítségével mintegy 450 ezer kiberbiztonság-releváns hirdetést azonosítottak. Ezek közül körülbelül 155 ezer tartozott a szűken értelmezett, dedikált kiberbiztonsági szerepkörök közé (Core), míg 294 ezer olyan tágabb munkakört képviselt (Broad), amelyben a biztonság fontos feladatként vagy kompetenciaként jelenik meg.

A kiberbiztonság szempontjából releváns hirdetések aránya az összes vizsgált álláshirdetésen belül 2021-es 1,8 százalékról 2025-re 2,1 százalékra emelkedett. Eközben a biztonsági kompetenciák jelentős része nem dedikált cybersecurity pozíciókban, hanem például DevOps-, hálózati, felhő- és rendszergazdai munkakörökben jelenik meg.

Ez számunkra az előadás egyik legfontosabb üzenete: **a kiberbiztonság egyre kevésbé kezelhető kizárólag egy specializált szervezeti funkció feladataként**. A megfelelő védelmi képesség kialakításához azoknak a szakembereknek a biztonsági tudását is fejlesztenünk kell, akik napi munkájuk során rendszereket fejlesztenek, üzemeltetnek vagy felhőalapú infrastruktúrákat kezelnek.

A technológiai alapismeretek mellett a kommunikáció, az együttműködés, a kreativitás és a menedzsmentkészségek is hangsúlyosan jelennek meg. A vizsgált mintában mintegy 37 ezer hirdetés tett említést tanúsítványokról, amelyek között a vezetői, irányítási és auditálási fókuszú minősítések, például a CISSP, CISM és CISA meghatározó szerepet kaptak.

Mindez jól mutatja, hogy a technikai szakértelem önmagában egyre kevésbé elegendő. A szabályozott és ellenőrizhető működéshez **olyan szakemberekre is szükség van, akik értik a kockázatkezelést, a governance működését, valamint képesek a technikai kockázatokat üzleti és vezetői szempontból is értelmezhetővé tenni.**



Számunkra azonban az előadás legerősebb felismerése a munkaerőpiaci belépési küszöb emelkedése volt. Miközben az MI-hez kapcsolódó készségek említése valamennyi vizsgált nyelvben növekedett, különösen a tágabban értelmezett biztonsági szerepkörök, valamint az angol és spanyol nyelvű hirdetések esetében, a kifejezetten pályakezdőket célzó pozíciók aránya minden vizsgált nyelven csökkent. Ezzel párhuzamosan nőtt a szenior szakembereket kereső hirdetések súlya.

Az előadás alapján számunkra egyértelmű, hogy hosszú távon nem lehet kizárólag a munkaerőpiacról elérhető, kész szenior szakemberekre építeni.

A **szervezet kiberbiztonsági képességeinek fejlesztésében** ezért három területet érdemes egyszerre szem előtt tartani:

- a meglévő IT-, fejlesztői, üzemeltetési és infrastruktúra-szakemberek biztonsági kompetenciáinak tudatos fejlesztését;
- a technikai tudás mellett a governance-, kockázatkezelési, kommunikációs és vezetői készségek erősítését;
- valamint olyan fejlődési utak kialakítását, amelyek lehetővé teszik, hogy a kevésbé tapasztalt kollégákból később magas szintű kiberbiztonsági szakemberek váljanak.

A legfontosabb üzenet számunkra tehát nem egyszerűen az, hogy több cybersecurity szakemberre van szükség. Sokkal inkább az, hogy **a biztonsági kompetenciát szélesebb körben kell beépítenünk a szervezetek működésébe.**

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



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

Cybersecurity Higher Education Database (CyberHEAD)

[Christos PAPACHRISTOS, ENISA]

Az előadásban a **Cybersecurity Higher Education Database** (CyberHEAD) elmúlt hat évének tapasztalatait és eredményeit mutatták be.

Az előadás **átfogó képet adott az európai felsőoktatás kiberbiztonsági képzési kínálatáról**: hogyan változik az elérhető programok és a hallgatók száma, milyen mértékben jelenik meg a mesterséges intelligencia az oktatásban, hogyan kapcsolódnak a képzések az European Cybersecurity Skills Framework (ECSF) szerepprofiljaihoz, valamint milyen irányban fejlődhet tovább maga az adatbázis.

Vezetői és kiberbiztonsági szempontból mindez azért különösen releváns, mert képet ad arról, milyen szakmai utánpótlásra számíthatunk az európai felsőoktatásból, és mely területeken lehet szükség arra, hogy a munkáltatók saját képzési és kompetenciafejlesztési programokkal egészítsék ki az egyetemen megszerzett tudást.

A **CyberHEAD** fejlődése jól mutatja, hogy az európai felsőoktatás egyre nagyobb figyelmet fordít erre a területre. Az adatbázis ma már közel kétszáz validált felsőoktatási programot fog össze közel harminc európai országból, köztük magyarországi képzésekkel. Négy fő célcsoport számára biztosít átláthatóságot és összehasonlítható információkat: a leendő hallgatóknak, az egyetemeknek, a munkáltatóknak és a döntéshozóknak.

A növekedés üteme figyelemre méltó: míg 2013-ban még alig két tucat program indult, 2025-re már közel kétszáz képzés vált elérhetővé. A kínálatban a kétéves mesterképzések dominálnak, mellettük azonban egyéves mesterprogramok és hároméves alapképzések is megtalálhatók. A kurzusok többsége tandíjas, jellemzően jelenléti formában zajlik, és közel felük angol nyelven érhető el.

A növekvő képzési kínálat mögött ugyanakkor a végzett szakemberek száma már jóval árnyaltabb képet mutat. Az évente újonnan beiratkozók száma 2020 és 2025 között több mint kétszeresére, közel tízezer főre emelkedett, miközben évente körülbelül 4 500 hallgató fejezi be ténylegesen a képzést. Ez programonként átlagosan valamivel



több mint húsz végzett szakembert jelent. A nemek arányában szintén megfigyelhető változás: a női hallgatók és végzettek száma dinamikusan emelkedett, az európai átlag azonban továbbra is megközelítőleg 80 százalék férfi és 20 százalék nő.

Szakmai szempontból különösen fontos az ECSF-profilok fokozatos megjelenése a képzésekben. A mester- és posztgraduális programok jelentős része már olyan szerepkörökhöz igazodik, mint például az implementer, a CISO, az architect, a risk manager vagy a penetration tester. Ez azért lényeges, mert közelebb hozhatja egymáshoz az egyetemi képzésekben megszerezhető kompetenciákat és a munkaerőpiacon megjelenő szakmai elvárásokat.

Számunkra az előadás egyik legfontosabb felismerése a mesterséges intelligencia és a kiberbiztonság kapcsolatának oktatási megjelenése volt. Miközben a programok túlnyomó többsége ipari szakembereket is bevon oktatóként vagy vendégelőadóként, és jelentős részük tanúsítvány-felkészítést vagy szakmai gyakorlatot is biztosít, az MI-hez kapcsolódó biztonsági ismeretek még csak a képzések kisebb részében jelennek meg a tantervben.

Ez a technológia és az oktatás fejlődési üteme közötti különbség – többek között – humán erőforrás és vezetői nézőpontból különösen érdekes. A felsőoktatásból érkező szakmai tudásra fontos alapként tekinthetünk, de önmagában nem feltétlenül elegendő a gyorsan változó technológiai és kockázati környezetben. A frissen végzett kollégák kompetenciáinak fejlesztésében ezért továbbra is fontos szerepe lehet a szervezeten belüli szakmai képzéseknek és fejlődési lehetőségeknek.

Az előadás másik érdekes pontja a CyberHEAD jövője volt. Az ENISA jelezte, hogy az adatbázis fenntartását és továbbfejlesztését a jövőben szívesen átadná a szakmai közösségnek, illetve olyan projekteknek, amelyek a kiberbiztonsági készséghiány és a munkaerőpiaci trendek vizsgálatával foglalkoznak.

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



BBA+ BESZÁMOLÓ

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

A bemutatott adatok alapján a felsőoktatási képzések bővülése önmagában nem jelenti azt, hogy rövid távon megszűnik a kiberbiztonsági szakemberek iránti igény és a rendelkezésre álló utánpótlás közötti különbség. A hallgatói létszám növekedése pozitív tendencia, ugyanakkor a ténylegesen végzett szakemberek száma továbbra is korlátozott.

Szervezeti oldalról ezért három lehetőség rajzolódik ki:

- egyetemi együttműködések erősítése, amelyek révén már a képzés során kapcsolatot teremthetünk a jövő szakembereivel;
- gyakornoki programok és vendégelőadások tudatosabb alkalmazása, amelyek közelebb hozzák egymáshoz az akadémiai és az ipari elvárásokat;
- belső kompetenciafejlesztési programok kialakítása, különös tekintettel azokra az új területekre, például az MI-biztonságra, amelyek még kevésbé hangsúlyosan jelennek meg a felsőoktatási tantervekben.

A legfontosabb üzenet számunkra az, hogy az utánpótlás fejlesztését nem érdemes kizárólag a felsőoktatásra bíznunk. Érdemes már az egyetemi évek során kapcsolatot teremteni a jövő szakembereivel, majd ezt tudatos belső fejlődési lehetőségekkel továbbépíteni.



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

ECSF in the Age of AI

[Fabio DI FRANCO, ENISA és Argyro CHATZOPOULOU, Apiroplus Solutions]

Az előadásban azt mutatták be, **hogyan alakítja át a mesterséges intelligencia az európai kiberbiztonsági szerepprofilokat** és a hozzájuk kapcsolódó kompetenciaelvárásokat.

A téma középpontjában az **European Cybersecurity Skills Framework** (ECSF) továbbfejlődése állt. A 2020-ban indított, majd 2022-ben tizenkét szerepprofillal megjelent keretrendszernek ma már egy olyan környezethez kell alkalmazkodnia, amelyben az MI egyszerre új technológiai terület, potenciális támadási felület és a védekezést támogató eszköz.

A kérdést az európai szabályozási környezet változása is egyre aktuálisabbá teszi. Az előadás többek között az **AI Actre**, az általános célú MI-modellekhez kapcsolódó kötelezettségekre, a **Cybersecurity Act 2** javaslatra és az uniós MI-kiberbiztonsági cselekvési tervre is kitért.

Kiberbiztonsági szempontból számunkra az előadás legfontosabb gondolata az volt, hogy az MI megjelenése nem feltétlenül indokolja újabb és újabb biztonsági munkakörök létrehozását. Sokkal inkább azt kell megvizsgálnunk, hogyan változtatja meg a technológia a már létező szerepekhez szükséges tudást és kompetenciákat.

Az ENISA munkacsoportjának konzultációi azt az irányt erősítik, hogy az ECSF továbbra is egy feszes, tizenkét fókuszált profilból álló és technológiasemleges keretrendszer maradjon. Az új szerepkörök létrehozása helyett a tartósan releváns készségeket érdemes előtérbe helyezni, és csak akkor indokolt új szakmai profil bevezetése, ha ezt tényleges bizonyítékok támasztják alá.

Ehhez kapcsolódik a 2026 júniusában megjelent CWA 18398 keret megközelítése is. Eszerint egy új technológia különböző mértékben alakíthat át egy meglévő szakmai szerepet: bizonyos feladatok lényegében változatlanok maradhatnak, mások MI-



BBA+ BESZÁMOLÓ

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

asszisztált, MI-támogatott vagy MI-automatizált munkafolyamatokkal egészülhetnek ki, míg csak kivételes esetben indokolt egy teljesen új szakmai szerep kialakulásáról beszélni.

Az előadás egyik legérdekesebb része az volt, ahogyan ezt az elvet az ENISA a gyakorlatba ülteti. A munkacsoport három lehetséges megközelítést vizsgált: az MI-alapműveltség és a biztonságos MI-használat horizontális beépítését, a meglévő közös készségterületek frissítését, illetve az egyes szerepprofilok átfogó felülvizsgálatát.

Az ehhez kialakított ötlépcsős adaptációs módszertant két konkrét területen, a Cyber Incident Responder és a Penetration Tester profilokon tesztelték. A bemutatott megközelítés alapján az MI hatása már nem különálló technológiai kérdésként jelenik meg, hanem összekapcsolódik többek között a jogi megfeleléssel, a biztonsági kontrollokkal, az új kockázatokkal, az MI-alapú eszközök használatával és az ilyen technológiákat alkalmazó támadásokkal.

A Cyber Incident Responder profil esetében például olyan tudásterületek kerültek látókörbe, mint a gépi tanulási és MI-architektúrák alapjai, a promptolásra vagy ágensalapú munkafolyamatokra épülő elemzés, valamint a generatív MI-eszközök alkalmazása a riportkészítés során.

A Penetration Tester szerepkörnél ezzel szemben az MI-rendszerek tesztelése, az adversariális támadások elemzése, valamint a generatív mesterséges intelligencia social engineering tesztekben történő alkalmazása jelent meg új kompetenciaterületként.

A két példa jól szemlélteti, hogy az MI nem egyszerűen egy újabb eszköz a kiberbiztonsági szakemberek kezében: egyszerre módosíthatja a védendő környezetet, a támadási lehetőségeket és magukat a védekezéshez használt munkafolyamatokat.

Az előadás egyik legerősebb tanulsága, hogy a technológiai változásra nem feltétlenül új munkakörök létrehozása a megfelelő szervezeti válasz.



Az MI térnyerésével először azt érdemes megvizsgálni, hogyan változnak a meglévő biztonsági, fejlesztési és üzemeltetési szerepek, és ezekhez milyen új kompetenciákat kell hozzáadnunk.

Cybersecurity Skills in Portugal

[Andre SILVA, Portugál Nemzeti Kiberbiztonsági Központ]

Az előadás a **kiberbiztonsági szakember-utánpótlás és a szükséges kompetenciák folyamatos fejlesztésének jelentőségét** mutatta be a technológiai fejlődés, különösen a mesterséges intelligencia és az egyre inkább digitalizálódó, intelligens rendszerek térnyerésének tükrében. Kiemelte, hogy a technológiai változásokkal párhuzamosan a kiberbiztonsági készségeknek is folyamatosan fejlődniük kell, amelyhez a szükséges kompetenciák és képzési igények rendszeres felmérése, célzott fejlesztése, valamint az új technológiai környezethez történő alkalmazkodás elengedhetetlen. Az előadó ismertette Portugália e területen végzett munkáját, különös tekintettel az **Európai Kiberbiztonsági Készségkeretrendszer** (ECSF), a NIS2 irányelv hatálya alá tartozó ágazatok és a nemzeti sajátosságok összehangolására. Bemutatta továbbá a **C-Academy** képzési kezdeményezést, amely a rendelkezésre álló erőforrások hatékony felhasználására építve két fő képzési irányt alkalmaz: az online, széles körben hozzáférhető, alapozó és átfogó ismereteket biztosító képzéseket, valamint az egyetemi partnerekkel megvalósuló, gyakorlatorientált, specializált oktatási programokat.

Az előadás hangsúlyozta, hogy a korlátozott képzési erőforrások miatt nem lehetséges mindenkit minden területen képezni, ezért a kiemelt kompetenciaterületek azonosítására, a munkaerőpiaci hiányosságok felmérésére és a tényleges szakmai igényekhez igazodó képzések kialakítására kell helyezni a hangsúlyt. Az előadás záró gondolata szerint az egyre intelligensebbé váló digitális világban a biztonság fenntartásának egyik legfontosabb befektetése továbbra is az azt biztosító szakemberek tudásának és képességeinek fejlesztése.

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



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

ECSF 2.0: What's Under the Hood?

[Vasiliki SPILIOTI, ENISA]

Az előadás az **Európai Kiberbiztonsági Készségkeretrendszer** (European Cybersecurity Skills Framework – ECSF) 2.0 verziójának újdonságait, felépítését és gyakorlati alkalmazási lehetőségeit mutatta be. Az előadó ismertette, hogy az új keretrendszer megtartja a korábbi változatban meghatározott 12 kiberbiztonsági munkaköri profilt, ugyanakkor azok feladatait felülvizsgálja és pontosítja, a szükséges kompetenciákat pedig egységes, több munkaköri profilban is alkalmazható készségterületekbe rendezi. Kiemelt újdonságként jelent meg a készségek négy szintre történő besorolása (alapozó, gyakorlati, haladó, stratégiai/szakértői), amely az önállóság, a feladatok összetettsége és a szakmai befolyás mértéke alapján teszi lehetővé az egyes munkakörökhöz szükséges kompetenciaszintek meghatározását. Az előadás kitért a mesterséges intelligenciával kapcsolatos készségek valamennyi munkaköri profilba történő beépítésére, valamint a tudásterületek és az azokhoz kapcsolódó szakmai ismeretek, szabványok és keretrendszerek kialakítására is. Gyakorlati példákon keresztül szemléltette, hogy az **ECSF 2.0** miként támogathatja a munkavállalók kompetenciahiányainak azonosítását, a célzott képzési igények meghatározását, valamint a különböző kiberbiztonsági munkakörök közötti szakmai előmenetel és karrierutak megtervezését. Az előadás végén ismertették a keretrendszer véglegesítésének tervezett ütemezését, amelynek részeként 2027 első negyedévében nyilvános konzultációt terveznek, ezt követően pedig az ECSF 2.0 végleges közzététele várható.



Strengthening Cyber Skills: From National Initiatives to EU Cooperation

[Ioannis PANOLIAS, görög Nemzeti Kiberbiztonsági Hatóság]

Az előadás a kiberbiztonsági készségek erősítéséről szólt, a nemzeti kezdeményezésektől az európai szintű együttműködésig vezető útról. A **görög Nemzeti Kiberbiztonsági Stratégia 2026–2030** keretében négy stratégiai prioritást emelt ki, amelyek közül kiemelt szerepet kapott a készséghiány csökkentése (Specific Objective 1.B). Ennek részeként szó esett közszférás cyber range kialakításáról, nemzeti cselekvési tervről az oktatás és tudatosság terén, átfogó képzési programokról a közigazgatás számára, valamint a CISO-k átképzéséről és felkészítéséről. Az előadó bemutatta az **AKADIMOS** és a **CADMUS** európai projekteket, amelyeket a görög hatóság koordinál. Az AKADIMOS (2025–2027, 4 millió eurós költségvetéssel, Görögország, Ciprus, Olaszország, Spanyolország és Szlovénia részvételével) a European Cybersecurity Skills Academy támogatását célozza a koordináció, a közös európai referencia (ECSF), a készségmérés és a hosszú távú fenntarthatóság erősítésével. A CADMUS (2024–2027) a gyakorlati képzésekre fókuszál: célcsoportjai a közigazgatás, a kkv-k, az oktatók és a pályakezdők, eszközei pedig online kurzusok, bootcampek, cyber range-ek, játékok, hackathonok és szakmai gyakorlatok. A harmadik pillér a **CSC-EDIC** (Cybersecurity Skills Coalition – European Digital Infrastructure Consortium) volt, amely 2026. június 30-án jött létre hivatalosan, székhelye Athén.

Alapító tagjai Görögország, Ausztria, Horvátország, Ciprus és Szlovénia, megfigyelői pedig Csehország és Lengyelország. A szervezet négy tevékenységpilléren nyugszik: tudásgenerálás és képzés, érdekelt felek bevonása, finanszírozás és projektek, valamint a fejlődés mérése. Az előadás összességében azt mutatta be, hogyan kapcsolódnak össze a nemzeti prioritások (görög stratégia), a gyakorlati projektek (AKADIMOS, CADMUS) és a hosszú távú európai együttműködési keret (CSC-EDIC), hogy fenntarthatóbb és erősebb kiberbiztonsági szakembergárda jöjjön létre Európában.

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