NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 2. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- BBA+ BESZÁMOLÓK

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el LinkedIn oldalunkra vagy hallgassa meg podcast adásainkat!

KIBERTÁMADÁS! PODCAST

NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍREK

ClickFix támadások megtévesztő Windows BSOD képernyőkkel terjesztenek kártevőt

(bleepingcomputer.com)

Egy új, ClickFix mechanizmusra épülő social engineering kampány az európai vendéglátóipari szektort célozza. A támadók a Windows operációs rendszer összeomlását imitáló Blue Screen of Death (BSOD) képernyők megjelenítésével érik el, hogy az érintett felhasználók saját maguk futtassák a rosszindulatú kódot a rendszereiken. **Bővebben...**

Adobe ColdFusion szerverek koordinált támadások célkeresztjében

(securityweek.com)

A GreyNoise kiberbiztonsági vállalat figyelmeztetése szerint egy kiberbűnöző vagy kiberbűnözői csoport egy kezdeti hozzáférés megszerzésére irányuló művelet során nagyjából egy tucat, a ColdFusionhoz köthető sérülékenységet kísérelt meg kihasználni. **Bővebben...**

Lakossági proxyhálózatokon keresztül növekszik a Kimwolf Android botnet

(securityweek.com)

A Kimwolf nevű botnet több mint 2 millió Android-eszközt fertőzött meg, elsősorban lakossági proxyhálózatokon keresztül, állítja a kiberbiztonsági kutatásokkal foglalkozó Synthient. A Kimwolf legalább 2025 augusztusa óta aktív, és a közelmúltban az XLab is részletesen elemezte, külön kiemelve, hogy a hálózat képes lehet rendkívül nagy volumenű DDoS támadások indítására. **Bővebben...**

Aktívan kihasználják a D-Link sebezhetőségét régi DSL routerekben

(bleepingcomputer.com)

A kiberbűnözők aktívan kihasználnak egy nemrég azonosított parancsinjektálási sebezhetőséget, amely több, életciklusa végére ért (EoL) D-Link DSL gateway routert érint. A CVE-2026-0625 azonosítón nyomon követett sebezhetőség a dnscfg.cgi végpontot érinti, egy CGI-könyvtárban nem megfelelően szűrt bemenetek miatt.

Bővebben...

Kritikus sérülékenység az n8n platformon

(thehackernews.com)

A kiberbiztonsági kutatók egy kritikus súlyosságú sebezhetőséget azonosítottak az n8n munkafolyamat-automatizációs platformon. A CVE-2026-21858 azonosítón nyomon követett sérülékenység (CVSS pontszám: 10,0) az érintett n8n-példányok teljes kompromittálódásához vezethet.

Bővebben...

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

2025. 12. 19. — 2026. 01. 08.

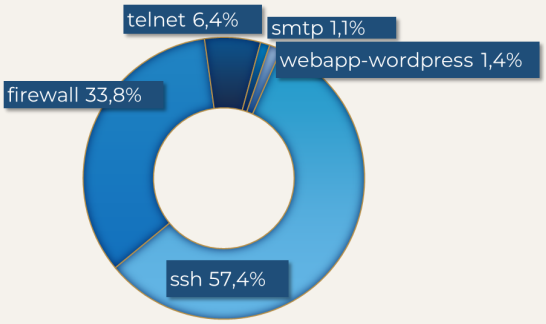
Fenyegetettségi szint:

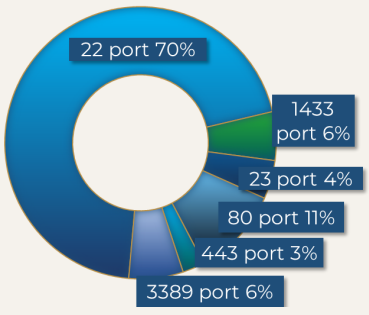
alacsony | közepes | magas | kritikus

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

BBA+ BESZÁMOLÓ

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

FIRST Cold Incident Response Konferencia 2025

2025. október 7 - 9.

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

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

A Nemzeti Kiberbiztonsági Intézet munkatársai **2025. október 7-9.** között részt vettek az Oslo-ban megrendezésre kerülő éves **FIRST Cold Incident Response** konferencián.

A **FIRST** (Forum of Incident Response and Security Teams) hálózatban Magyarországot az NBSZ NKI képviseli. Az Oslóban megrendezésre kerülő esemény első napján egy **workshopra** került sor, amely a **rosszindulatú programok terjesztésének vizsgálatára** fókuszált. A workshop gyakorlati fókuszú volt, ahol az előadó több szoftver alkalmazásán keresztül mutatta be a malwarek terjesztésének módjait. A **plenáris ülések** (október 8-9) során az előadások fókuszában az incidens reagálás, a támadói trendek és a különféle támadási csoportok taktikáinak elemzései álltak. A konferencián lehetőség nyílt **networkingre** is, amely során a finn **Arctic Security** cég kollégái bemutatták csapatunknak a CTI elemzési platformjukat.

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

Kiknek ajánlott a beszámoló megismerése?

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

A konferencia legfontosabb előadásai az alábbiakban olvashatók.

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

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

Workshop -
Rosszindulatú programok terjesztésének gyakorlati vizsgálata

A workshop a **rosszindulatú programok** e-mailen és weben keresztüli kézbesítésének elemzésére fókuszált, különös tekintettel a **fertőzési láncok** első szakaszaira. Az előadó **gyakorlati példákon keresztül** szemléltette a kártevőterjesztés felismerésének és vizsgálatának módszereit, mely után különböző fájltípusokat, többek között PowerShell és VBScript-szkripteket, makrós Office-dokumentumokat, HTML/HTA-letöltőket, LNK- és MSI-fájlokat, valamint EML e-maileket lehetett vizsgálni virtuális REMnux környezetben. **A cél** a minták dekódolása, az obfuszkált szkriptek és makrók visszafejtése, valamint az indikátorok (URL, domain, hash, parancsok) biztonságos kinyerése volt. A feladatok során a manuális elemzéshez **nyílt forráskódú eszközök**, mint az olevba, oledump.py, CyberChef, oletools, Wireshark, peepdf, pdf-parser, lnkinfo és msitools **használata** volt javasolt. A képzést Hans Kristian Strømme, a Norvég Egészségügyi és Önkormányzati CERT vezető elemzője tartotta.

Jørgen Bøhnsdalen
Előadás egy célzott norvégiai számlacsalásról

Az előadást Jørgen Bøhnsdalen a norvég **Health CERT** elemzője tartotta, aki egy Norvégiát évek óta érintő **számlacsalási kampányt mutatott be**. A csalások során a támadók rendkívül szofisztikált **hamis díjbekérő számlákat** küldtek ki az **egészségügyi szektorban** tevékenykedő cégeknek. A számlákon szereplő összeg bár nem volt túl nagy, de olyan sok céget tudtak becsapni (több alkalommal), hogy így is lényeges kárt okoztak nekik. A szakértő bemutatta, hogy elemzéseik során végül egy **támadói csoportra tudták visszavezetni a csalás sorozatot**, viszont nem tudták pontosan beazonosítani az elkövetőket. A számlacsalási kampány felhívta a figyelmet a szektor szereplő közti információáramlás fontosságára.

NEMZETI KIBERBIZTONSÁGI INTÉZET

Ågot Storne
Fenyegetettség vadászat kezdőknek

Ågot Stornes a **Norvég Munkaügyi és Jóléti Hivatal** informatikusának előadása a **fenyegetésvadászat** alapjairól szólt. Az előadó ismertette, hogyan lehet az **állami szféra korlátozottabb pénzügyi erőforrásainak kihasználásával** is megfelelő fenyegetettség vadászatot és elemzést felépíteni. Kiemelte, hogy a fenyegetettség vadászat egyik **kezdő lépése** a kliens megfelelő felmérése (például milyen típusú támadásokra vadászunk? Milyen típusú támadók jöhetnek szóba? Milyen technikákat fognak alkalmazni? Hol találhatunk nyomokat?). Ha az adott cég nem is rendelkezik korlátlan pénzügyi erőforrásokkal, egyszerű logelemzésekre **alapozva** is felépíthető egy alapszintű **threat hunt kapacitás**.

Raymond Hagen, Digdir
APT-k elleni védekezés

Raymond Hagen prezentációjában a **túlzott automatizáció kockázataira hívta fel a figyelmet** egy **SOC központ** bemutatásán keresztül. Amennyiben az elemzők hajlamosak teljes mértékben az automata rendszerekre hagyatkozni a detektálás során, akkor könnyen kialakulhat ún. **„silent failure”**, mely során egy **szofisztikált ATP átjut a rendszeren** (például egy jó **evasion technikának** köszönhetően, ami az automata rendszeren átment). Felhívta a figyelmet a **biztonsági csapatok tipikus hibáira** (reagálási hibák, túldetektálás technológiai függőség, tudás erózió) Az előadó kiemelte, hogy a **hatékony védekezés kulcsa** az APT-k elleni harcban egy SOC csapaton belül az automatizálás megfelelő mértékű használata, és a prioritásokra való fókuszálás.

BBA-PLUSZ-31.2-24-2024-0004. sz. pályázat részeként

BBA+ BESZÁMOLÓ

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

Marthe R. Rogndokken, Sopra Steria

Támadó aktorok profilozása

Az előadók betekintést nyújtottak a **fenyegető szereplők profilozásába**. A profilozás során a szakértők viselkedésminták, kommunikációs stílusok és műszaki jellemzők alapján próbálják minél pontosabban meghatározni, ki állhat egy támadás mögött. Bemutatásra került a **PACT attribúciós modell** is, ami a **kiberfenyegetés-attribúció** egyik elemzői megközelítése. A modell tulajdonképpen a **Diamond Modell** stratégiai kiegészítése, hiszen a támadó kilétéről és motivációjáról is leírást ad. (PACT, P: Political, A: Administartive, C: Cultural, T: Technical) A **PACT modell** nem csak **technikai értékelést ad**, hanem a **támadás szervezeti hátterét és kulturális kontextusát is figyelembe veszi**, ezáltal pontosabb képet kaphatunk egy adott aktorról.

NEMZETI KIBERBIZTONSÁGI INTÉZET

Webs Week 2025, Web 3.0 and AI konferencia

2025. november 26 - 27.

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

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

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

BBA+ BESZÁMOLÓ

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

A Nemzeti Kiberbiztonsági Intézet munkatársai részt vettek a **2025. november 26-27.** között Dubaiban megrendezésre kerülő **Webs Week Web 3.0.** konferencián. A konferencia célja, hogy hozzáférhetővé tegye a **legfrissebb tudást és innovációs megoldásokat** az IT technológia és kiberbiztonság, pénzügyi trendek, fintech, adatvédelem és a mesterséges intelligencia területén a résztvevők számára. Az első alkalommal 2024-ben megrendezett konferencia közösségi szemléletet képvisel, és arra törekszik, hogy **összekapcsolja a kiberbiztonsági közösségeket**, a szakembereket, fejlesztőket, kutatókat, vállalatokat és szponzorokat elősegítve a tudásmegosztást és az együttműködést.

Kiknek ajánlott a beszámoló megismerése?

- Incidenskezelők számára
- Digitális elemzéssel foglalkozó szakemberek számára
- Minden kiberbiztonsági szakember számára

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

A konferencia előadói a **mesterséges intelligencia**, a **Web 3.0** és a **digitális innováció** területének meghatározó szakértői. Az eseményen olyan vezetők és cégalapítók szólaltak fel, akik a blockchain, fintech és a decentralizált technológiák jövőjét formálják. Rajat Sakhuja, a Mastercard blokklánc és digitális eszközök igazgatója Dubajból érkezett, míg Kristijan Glibo, a Primary FZCO és a Beyondi alapítója a **startup világ innovációit** mutatta be. Ali Safri, az Avanza Innovations műszaki igazgatója a **Web3 megoldások gyakorlati alkalmazásáról** beszélt, Gustavo Antonio Montero pedig a Carter Capital elnökeként a **befektetési trendeket** ismertette a konferencia fő témájával kapcsolatba hozva.

David Palmer, a Vodafone Pairpoint Web3 platform társalapítója az **európai telekommunikációs szektor** perspektíváit mutatta be, míg Dr. Mahmoud Abdawi, a First Abu Dhabi Bank fintech partnerségi vezetője a **pénzügyi innovációk és a mesterséges intelligencia** kapcsolatát feszegette. Giovanni Everduin, a Commercial Bank International stratégiai és innovációs igazgatója a **banki digitalizáció kihívásait** elemezte. Emellett olyan előadók is szerepeltek, mint Lianna Adams, aki a **művészet és az AI technológia** összefonódásáról beszélt, vagy Una Wang, a LingoAI alapítója, aki a szakterületén legpraktikusabb és leggyakrabban használt **AI nyelvi megoldásokat** mutatta be.

A programban helyet kaptak **jogi és szabályozási kérdések** is Sadri Sali, blokklánctechnológiával foglalkozó európai jogász előadásában, valamint a **kiberbiztonság és adatvédelem** témái Aliasgar Dohadwala, a Dubai Chamber of Commerce képviseletében. A Binance intézményi kapcsolatokért felelős Paola Morán a **kriptoeszközök globális trendjeit** ismertette, míg Anna Tutova, a Coinstelegram vezérigazgatója a **médiakommunikáció** szerepét emelte ki a Web3 világában.

Összességében **az előadók a mesterséges intelligencia, a digitális pénzügyek és a kiberbiztonság legújabb fejleményeit mutatták be**, különös hangsúlyt fektetve arra, hogyan alakítják ezek a technológiák a gazdaságot és a társadalmat, valamint ez hogyan jelenik meg az európai színtéren és az egyesült arab emirátusi állampolgárok életében.

BBA-PLUSZ-31.2-24-2024-00003. sz. pályázat részeként

BBA+ BESZÁMOLÓ

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

Jogi panel

A panel során 5 kulcstéma került előtérbe:

Governance és felelősségvállalás a DAO-kban: Nathan Vandy (DappRadar) részletesen beszélt arról, hogy a **decentralizált autonóm szervezetekben** milyen „összecsengések” vannak döntéshozatal és a vezetői felelősség között? A jelenlegi nemzeti jogrendszerekben a felelősség személyhez vagy jogi entitáshoz kötődik, míg a DAO-kban ez elmosódik. Ez felveti a kérdést: **ki felelős egy hibás döntésért vagy egy jogsértő tranzakcióért?**

Szabályozási keretek és compliance: Karola Xenia Kassai (KassaiLaw) kiemelte, hogy a **Web3 és fintech területén a jogi megfelelés** nem csupán technikai kérdés, hanem **stratégiai kockázatkezelési elem** is. Az EU-ban például a **MiCA** (Markets in Crypto-Assets) rendelet próbálja lefedni a kriptoeszközök piacát, de a **DAO-k és DeFi projektek szabályozása** továbbra is „szürke zóna”.

Kiberbiztonság és adatvédelem jogi aspektusai: Aliasgar Dohadwala (Dubai Chamber of Commerce) hangsúlyozta, hogy a Web3 világában a **kiberbiztonsági incidensek jogi következményei** sokkal összetettebbek, mert a **decentralizált** rendszerekben nehéz azonosítani a felelős szereplőt.

Nemzetközi harmonizáció szükségessége: A decentralizált rendszerek globálisak, így a nemzeti jogszabályok önmagukban nem elegendőek. Az **EU MiCA rendelete** jó kezdet, de a világ többi részével való **összehangolás** elengedhetetlen. A konferencia előadói az **egységes nemzetközi jogalkotás lehetőségei** vonatkozásában is fogalmaztak meg a újító és kreatív gondolatokat.

Compliance és kockázatkezelés: A **jogi megfelelés** nem csupán szabályozási kérdés, hanem **reputációs és pénzügyi kockázat** is. Ezért a jogász szerepe stratégiai szinten felértékelődik.

Főbb üzenetek és álláspontok

1. Német perspektíva – Matthias Steger

Matthias Steger hangsúlyozta, hogy a **jogszabályoknak érthetőnek és életszerűnek kell lenniük**. Németországban a **szabályozás alapelve** az, hogy az IT technológiai fejlesztések önmagukban üdvözlendők, de a felhasználás módja a döntő. Példaként említette: Ma a nemzetközi kiberbiztonsági domain-ben mozogva IT technikailag lehetséges lenne robotokat fegyverrel felszerelni, de a jogi és etikai szabályozás kimondja, hogy ezt nem tesszük meg. Megítélése szerint **az AI használatát is korlátozni kell ott, ahol az emberi döntés és felelősség nem helyettesíthető**. Steger szerint a **nemzeti szabályozásnak** nemcsak jogszabályi tiltásokat, szankciós mechanizmusokat kell tartalmaznia, hanem pozitív kereteket, amelyek lehetővé teszik az innovációt, de megakadályozzák a visszaéléseket. **Ezért fontos, hogy az AI etikai és jogi kérdéseit már a középszintű oktatásban is tanítsuk, hogy a jövő generációi tudatosan használják ezeket a technológiákat.**

2. Dán perspektíva – Morten Rongaard

Morten Rongaard a **gyakorlati megvalósíthatóságot** és az **„akcióképességet”** emelte ki a szabályozási elemek kapcsán. Szerinte a kiberbiztonsági és jogi keretrendszernek nem elméleti szinten kell maradnia, hanem **olyan eszközöket és módszereket** kell biztosítania, **amelyek** valóban **alkalmazhatóvá válnak a gyakorlatban**. Álláspontja szerint **az AI-t** nem démonizálni kell, hanem **szabályozási keretek közé szorítani**. A **blockchain** ebben kulcsszerepet játszhat, mert

BBA+ BESZÁMOLÓ

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

„bizalmi horgonyként" működik: **minden tranzakció és döntés nyomon követhető**, auditálható. Rongaard szerint az AI nem autonóm „úr", hanem „intelligens szolga", amelyet az embernek kellen irányítani. Ehhez azonban **technikai és jogi kontrollmechanizmusokra** van szükség.

3. Egyesült Arab Emírségek perspektíva – Muhammad Salman Anjum és Amir Negm

Mindkét előadó kiemelte, hogy az **AI és Web3 integrációja a Közel-Keleten stratégiai prioritás**, de a szabályozásnak lépést kell tartania vele. Muhammad Salman Anjum szerint az AI által vezérelt rendszereknek **átláthatónak és auditálhatónak** kell lenniük, különösen a pénzügyi szektorban. Amir Negm hozzátette, hogy a decentralizált rendszerekben a **felelősség és a biztonság** kérdése kritikus, hangsúlyozta, hogy **az emberi kontroll nem veszítheti el a szerepét**, még akkor sem, ha az AI képes önálló döntésekre.

KassaiLaw

Karola Xenia Kassai (**KassaiLaw**) előadásában az **EU AI Act gyakorlati implementációjáról** beszélt, és egy világos megfelelőségi **roadmapet** vázolt fel, amely nemcsak jogi, hanem üzleti szempontból is stratégiai előnyt jelenthet. Az előadó beszámolt arról, hogy az EU AI Act az első olyan **átfogó szabályozás**, amely az AI rendszerek kockázati kategóriák szerinti besorolását, átláthatósági

és auditálhatósági követelményeit írja elő. A szankciós oldalt vizsgálva, a kiszabható bírságok rendkívül súlyosak. Akár 35 millió euró vagy a globális árbevétel 7%-a. Az előadó kiemelte, hogy a **jogi megfelelés nem opcionális**, hanem üzleti túlélési kérdésként kezelhető.

KassaiLaw által javasolt roadmap az AI Act implementációjára

1. Piaci hitelesség és előny

Miért fontos? Az AI Act-nek való megfelelés nemcsak jogi kötelezettség, hanem versenyelőny. Azok a cégek, amelyek elsőként demonstrálják a megfelelést, piaci bizalmat és új ügyfeleket szereznek.

„Akciópont”: Kommunikálni kell a megfelelőségi státuszt (pl. „AI Act Ready” tanúsítvány), ami új piacokra való belépést és partneri bizalmat épít.

2. Partnerség EU-s szereplőkkel

Miért fontos? Az AI Act harmonizált európai keretet hoz létre, így a nem EU-s cégeknek is együtt kell működniük EU-s partnerekkel.

„Akciópont”: Létre kell hozni compliance partnerségeket jogi tanácsadókkal, auditáló cégekkel és IT technológiai szolgáltatókkal.

3. Termék- és szolgáltatás-differenciálás

Miért fontos? Az AI Act előírja az átláthatóságot, kockázatértékelést és felhasználói tájékoztatást.

„Akciópont”: A termékekbe be kell építeni compliance-by-design megoldásokat (például AI döntések magyarázhatósága, audit trail).

BBA+ BESZÁMOLÓ

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

4. Kockázatcsökkentés és bírságok elkerülése

Miért fontos? A bírságok extrém magasak, ezért a megfelelés hiánya nemcsak pénzügyi, hanem reputációs katasztrófa.

„Akciópont”:

- Kockázati kategória meghatározása (AI Act szerint: tiltott, magas kockázatú, korlátozott kockázatú).
- Megfelelőségi dokumentáció: technikai fájl, kockázatelemzés, felhasználói tájékoztatás.
- Folyamatos monitoring és auditálás.

Keynote Forum

A **nyitó előadás** két fontos témát érintett. Gustavo Antonio Montero, a Carter Capital alapító elnöke arról beszélt, **hogyan alakult át a hagyományos pénzügyi rendszer a Web3 világába integrálódva**, és **milyen kihívásokkal szembesültek a gazdasági szereplők** e téren. Ezt követően José N., a VAF Compliance műveleti és termékvezetője az Egyesült Arab Emírségekből a **VARA szabályozás** és a **Web3 kapcsolatát elemezte**, kiemelve a **jogi keretek és a decentralizált technológiák közötti egyensúly** fontosságát.

NEMZETI KIBERBIZTONSÁGI INTÉZET

Session 1
Building the Web of Tomorrow

A panelbeszélgetést Saima Sabir, globális stratégiai tanácsadó és AI nagykövet moderálta. A résztvevők között volt Sheikh Muhammad Noman, a Pegasus Capital Investments alapító-vezérigazgatója, aki a **befektetési trendekről és a pénzügyi modellek jövőjéről** beszélt. Dixon Melitt James, a TeamX alapítója **az innováció és a startup ökoszisztéma** szerepét hangsúlyozta a Web3 fejlődésében. Guido Santos, a Genesis Digital Solutions társalapítója és vezérigazgatója a **digitális megoldások skálázhatóságáról** osztott meg gondolatokat, míg Ahmed Gamal, a VAST Data regionális értékesítési igazgatója az **adatkezelés és adattárolás** új kihívásait mutatta be.

BBA-PLUSZ-311-24-2024-00003. sz. pályázat részeként