



HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2025. 17. hét



HÍREK

- Kiberbiztonsági cég vásárol hackerfórumokon fiókokat, hogy bűnözők után kémkedjen
- Amikor a rendszert a saját eszközei árulják el
- Kritikus sebezhetőséget használnak ki a SonicWall SMA 100 eszközökön
- Mobilról ATM-hez, így másolják le a kártyát
- Pénzt lopnak a hamis telefonok



STATISZTIKAI ADATOK

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



BESZÁMOLÓ

- European Chatbot 2025 Edinburgh konferencia



KONTAKT

edt@nki.gov.hu

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D



További hírekért, látogasson el **weboldalunkra!**

NEWS

IT biztonsági HÍREK

Kiberbiztonsági cég vásárol hackerfórumokon fiókokat, hogy bűnözők után kémkedjen (bleepingcomputer.com)

A svájci Prodaft kiberbiztonsági cég új kezdeményezést indított „Sell Your Source” néven, amelynek keretében hitelesített és régebbi hacker fiókokat vásárol fórumokon azzal a céllal, hogy információkat gyűjtsön a kiberbűnözőkről. **Bővebben...**

Amikor a rendszert a saját eszközei árulják el (gbhackers.com)

A kiberbiztonság egyik legnehezebben detektálható fenyegetéstípusa ma már egyértelműen a **Living-off-the-Land (LOTL)** támadás. Ezek a módszerek **nem új kártékony szoftvereket** vagy fájlokat hoznak a rendszerbe, hanem a meglévő, olyan **legitim**, rendszerbe épített eszközöket fordítanak a rendszer ellen, mint például a *PowerShell*, *WMIC* vagy a *cmd.exe*. **Bővebben...**

Kritikus sebezhetőséget használnak ki a SonicWall SMA 100 eszközökön (bleepingcomputer.com)

A CISA figyelmeztetést adott ki az a **SonicWall Secure Mobile Access (SMA) 100 sorozatú eszközök** ellen irányuló támadásokkal kapcsolatban. **Bővebben...**

Mobilról ATM-hez, így másolják le a kártyát (thehackernews.com)

A SuperCard X névre hallgató, újonnan azonosított [malware-as-a-service \(MaaS\)](#) platform olyan módszert vezet be, amely az **NFC-technológiát** kihasználva teszi lehetővé bankkártyás csalások végrehajtását. **Bővebben...**



Pénzt lopnak a hamis telefonok (thehackernews.com)

A kínai gyártású, **olcsó Android készülékek előtelepített, trójai kódot** tartalmazó alkalmazásokkal kerültek forgalomba. Az applikációk, melyek többek között a WhatsApp és a Telegram hamisított verziói, kriptovaluta **clipper funkcióval** vannak felszerelve. A támadók **közvetlenül a gyártási és szoftver előtelepítési folyamatba** avatkoznak be. A kompromittált készülékeken a rosszindulatú kódokat magában a gyári szoftverbe integrálták. **Bővebben...**



További hírekért, látogasson el **weboldalunkra!**

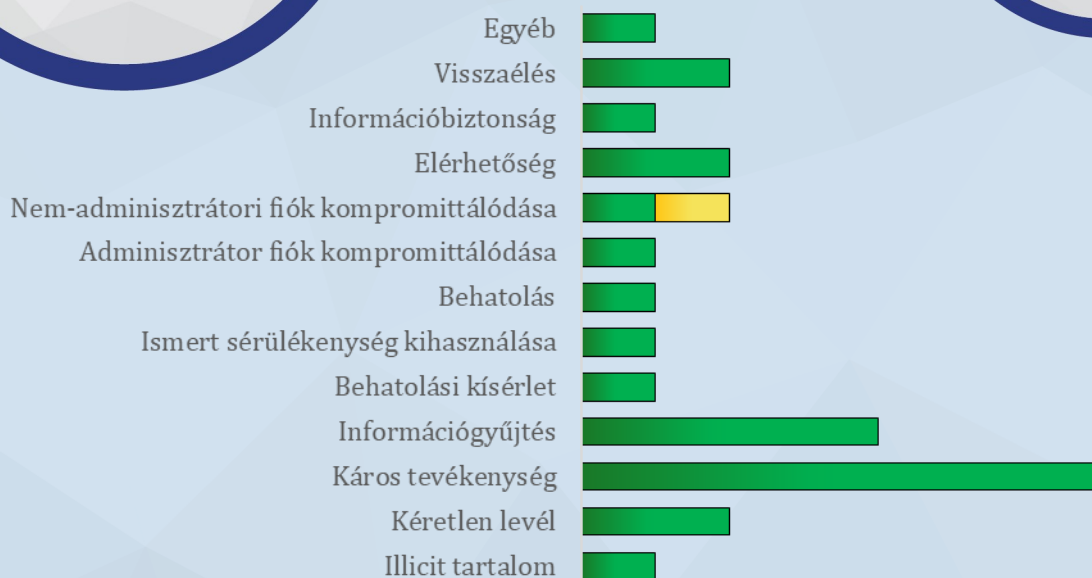
Statisztikai Adatok

2025.04.17.-2025.04.24.

Az NBSZ NKI által
kezelt incidensekre
vonatkozó statisztikai
adatok:



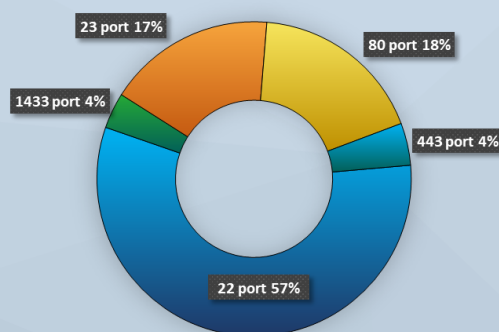
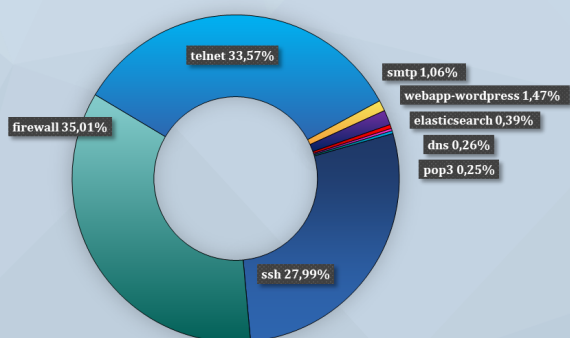
Fenyegetettségi
szint: közepes



■ Alacsony ■ Közepes ■ Magas ■ Kritikus

Incidensek eloszlása típus és kockázati besorolás szerint

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



További érdekességekért, látogasson el [weboldalunkra!](#)



Aktuális tartalmak



Kvantumszámítógépen fut a DOOM? #2 - Vendégünk Dr. Asbóth János

[örököld]

A kvantumszámítógépekről szóló dupla adásunk második részében kiderül, hogyan használhatók a **kvantumszámítóképek az adatok biztonságának növelésére**, mi az a **kvantum titkosítás** és mennyire valószínű, hogy a közeljövőben a kiberbűnözők könnyűszerrel tudnak majd kvantumszámítógéphez jutni.

A téma feldolgozásában segítségünkre volt
Dr. Asbóth János.

Meghallgatom

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



További hírekért, látogasson el **weboldalunkra!**



European Chatbot 2025 Edinburgh konferencia



2025. március 19-20.

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet munkatársai **Széchenyi Terv Plus 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.



**Széchenyi Terv
Plusz** Építsük együtt
Magyarországot!



MAGYARORSZÁG
KORMÁNYA



Az Európai Unió
társfinanszírozásával



A Nemzeti Kibervédelmi Intézet munkatársai részt vettek a 2025. március 19-20. között Edinburghban megrendezésre kerülő éves [European Chatbot & Conversational AI Summit](#) konferencián. Maga az esemény egy évente megrendezésre kerülő nemzetközi konferencia, amely a **beszélgetési mesterséges intelligencia** ([Conversational AI](#)) és a **nagyméretű nyelvi modellek** (LLM-ek) **gyakorlati alkalmazásaira fókuszál**. A *European Chatbot & Conversational AI Summit* 2025-ös kiadása különösen aktuális volt a technológia rohamos fejlődése és társadalmi hatásai miatt. A rendezvényen Európa-szerte és azon túlról is érkeztek előadók, köztük akadémiai szakértők, iparági innovátorok, termékfejlesztők és döntéshozók, akik saját esettanulmányokon, kutatásokon és piaci tapasztalatokon keresztül osztották meg meglátásaikat. A személyes és online jelenlét lehetősége miatt a részvétel különösen sokszínű és nemzetközi jellegű volt.

A kétnapos esemény során **több mint 40 előadás és panelbeszélgetés** hangzott el, amelyek között helyet kaptak technológiai bemutatók, etikai és szabályozási kérdéseket tárgyaló viták, valamint gyakorlati példák a vállalati, pénzügyi, oktatási és közigazgatási szektor AI-megoldásairól. A konferencia átfogó képet adott a beszélgetési AI aktuális trendjeiről, kihívásairól és jövőbeli lehetőségeiről.

A szakmailag legfontosabb előadások rövid összefoglalója az alábbiakban olvasható.

Kiknek ajánlott a beszámoló megismerése?

- Minden kiberbiztonsági szakember számára
- CTI specialisták számára



AI for Scotland (Tom Wilkinson)

Tom Wilkinson előadásában bemutatta, **hogyan alkalmazza a skót kormány a mesterséges intelligenciát a közszolgáltatások fejlesztésére és a skót gazdaság digitális átalakításának támogatására**. Adattudományi háttérrel rendelkező szakemberként részletes képet adott arról, miként épült be az AI a közpolitikákba és az államigazgatási döntésekbe.

Az előadás központi témái közé tartoztak:

- **AI a közszektorban** – hogyan segítette a mesterséges intelligencia az adatvezérelt döntéshozatalt, a közszolgáltatások hatékonyabb működtetését és az állampolgárok igényeire való gyorsabb reagálást.
- **Etikus és átlátható adatkezelés** – a skót kormány AI-stratégiájának egyik pillére a társadalmi bizalom erősítése és az átláthatóság megőrzése volt.
- **Gazdaságfejlesztés** – az AI szerepe az innováció ösztönzésében, a startup ökoszisztéma támogatásában és a munkaerőpiac átalakulásának elősegítésében.
- **Gyakorlati példák** – konkrét AI-alapú kezdeményezések, amelyek valódi hatást gyakoroltak a közigazgatási folyamatokra.

Tom Wilkinson, aki korábban több brit kormányzati szervnél is vezető adatstratégaként dolgozott, olyan hosszú távú szemléletet képviselt, amely az AI-t nemcsak technológiai, hanem társadalmi eszközként is kezelte. Előadása azt mutatta be, hogy a közszféra hogyan válhatott mintaadó szereplővé a mesterséges intelligencia felelős és hatékony alkalmazásában.





The Visionary's Edge: Mastering AI for impact (Christoph Esslinger, Ali Fenwick, Ph.D.)

Christoph Esslinger és Ali Fenwick arra világítottak rá, hogy a mesterséges intelligencia valódi értéke nem csupán a technológiai újdonságban rejlett, hanem abban, ahogyan képes volt hatást gyakorolni a szervezeti működésre, az emberi kapcsolatokra és a márkaélményre.

Esslinger a **"virtuális asszisztensek korának" eljövételéről beszélt**, és bemutatta, hogyan váltak ezek a rendszerek stratégiai eszközzé a vállalatok számára. Kifejtette, hogy egy jól megtervezett AI-asszisztens nem csupán kiszolgál, hanem márkát is épít – a felhasználók számára ugyanis a beszélgetés lett a legtermészetesebb kapcsolatfelvételi mód.

Ali Fenwick az AI és a humán viselkedés metszéspontját vizsgálta, különös tekintettel a szervezeti pszichológiára és a munkahelyi jólétre. Az előadásában hangsúlyozta, hogy a technológia bevezetését nem lehetett elválasztani az emberi tényezőktől: a pszichológiai biztonság, a motiváció és az identitás mind-mind meghatározták, hogyan reagálnak az emberek az AI-alapú rendszerekre.

Kiemelték, hogy az AI-nak nem csupán hatékornak kell lennie, hanem **„emberszerűnek”** is – és ennek eléréséhez **interdiszciplináris megközelítésre van szükség**. Esslinger a márka és ügyfél közötti új típusú kapcsolatról, Fenwick pedig az AI emberi beágyazottságáról beszélt – mindketten olyan gondolatokat hoztak, amelyek túlmutatnak a technológián, és a hatás valódi természetét helyezték fókuszba.



Beyond Voice Bots: The Future of Voice Conversational AI

(Ilan Avner)

Ilan Avner előadásában arra mutatott rá, hogy a beszédalapú mesterséges intelligencia ma már jóval túlmutat a klasszikus hangbotokon és IVR-rendszereken. A technológia fejlődése lehetővé tette, hogy a hangalapú AI ne csupán egy automatizált ügyfélszolgálati eszköz legyen, hanem **valós időben támogassa az ügyfélszolgálati munkatársakat** és érdemi információval lássa el őket a hívások során.

Az AI által generált valós idejű összefoglalók, témafelismerés és érzelemelemzés nemcsak gyorsabb és pontosabb kiszolgálást tettek lehetővé, hanem a háttérfolyamatokat is hatékonyabbá tették.

Az előadásban külön figyelmet kapott a technológia innovatív felhasználása, például a **valós idejű hangfordítás**, valamint az **akcentus-lágyítás**, amelyek különösen fontos szerepet játszanak a nemzetközi környezetben működő vállalatoknál. Ilan Avner hangsúlyozta, hogy az ilyen jellegű fejlesztések mögött komplex és skálázható technológiai infrastruktúra állt, amely biztosította a zökkenőmentes integrációt az üzleti kommunikációs rendszerekbe.

A példákon keresztül világossá vált, hogy a hangalapú mesterséges intelligencia már nem csupán egy segédeszköz, hanem **stratégiai elem** a vállalati digitális transzformációban. Az AudioCodes tapasztalatai alapján Avner rávilágított arra, hogy az AI-alapú hangtechnológiák új lehetőségeket nyitottak az ügyfélélmény fejlesztésében, és hozzájárultak a hatékonyabb, emberközpontú kommunikáció megvalósításához.





Engineering the future: Harnessing the power of AI to drive business growth (Eve Psalti)

Eve Psalti előadásában bemutatta, hogy a generatív mesterséges intelligencia (GAI) és a gépi tanulás (ML) miként váltak a technológiai fejlődés egyik legdinamikusabban növekvő területévé, amely minden iparágban éreztette hatását. Rávilágított arra, hogy a jelenlegi adatgazdaság robbanásszerű növekedésével az **AI egyre nagyobb szerepet játszik az üzleti folyamatok átalakításában és a mindennapi életünk formálásában.**

Az előadás során számos példán keresztül szemléltette, hogyan használták az AI-t különböző területeken. Megemlítette a **nagy nyelvi modelleket**, amelyek képesek voltak több milliárd adatpontot feldolgozni és összefoglalókat készíteni, valamint az **egyedi neurális hangmodelleket**, amelyek testreszabható beszélgetési AI-megoldásokat tettek lehetővé. Kitért arra is, hogy az AI hogyan könnyítette meg az ismétlődő, monoton feladatokat – például a számlafeldolgozást –, illetve miként járult hozzá az ügyfélértékelések érzelelemzéséhez.

Psalti hangsúlyozta, hogy az AI nem csupán az üzleti folyamatokat forradalmasította, hanem **új álláslehetőségeket is teremtett**, valamint új készségek elsajátítását követelte meg. Felhívta a figyelmet az AI-hoz kapcsolódó **kormányzási és etikai kérdésekre**, mint az elfogultság kezelése és a modellek átláthatósága. Az előadás végén arra ösztönözte a hallgatóságot, hogy tudatosan figyeljék az AI folyamatos fejlődését, és gondolkodjanak el azon, hogyan építhetik be ezt a technológiát mindennapi életükbe és üzleti stratégiáikba.



The intersection of linguistics and AI: academic solutions for language data (Graham Digby)

Graham Digby előadásában azt mutatta be, hogy a mesterséges intelligencia fejlődésének egyik legfontosabb, mégis gyakran alulértékelt hajtóereje a nyelvi adat. A nyelvészet és az AI találkozási pontjain keresztül világított rá arra, hogyan segítik az Oxford Languages magas minőségű, strukturált nyelvi adatbázisai a beszélgetési AI-rendszerek természetesebb, árnyaltabb és kulturálisan érzékeny működését.

Az előadás során Digby több szempontból közelítette meg a témát. Egyrészt bemutatta, hogy a fejlett AI-rendszerek hatékony működéséhez elengedhetetlen a **gazdag és precíz nyelvi háttér**. Részletesen kitért arra, hogyan alkalmazták az Oxford Languages adatállományait különböző iparágakban, az oktatástechnikától kezdve a technológiai óriásokig.

Kiemelte, hogy a valóban természetes ember-gép párbeszédhez nem elég a technológiai infrastruktúra – legalább olyan fontos az a **nyelvi és kulturális érzékenység**, amely lehetővé teszi a kontextushoz igazodó, befogadó kommunikációt. Az előadásban bemutatott stratégiák segítettek abban, hogy az AI-rendszerek ne csupán értelmezzenek, hanem valóban „megértsenek”, így támogatva a felhasználóbarát élményeket.

Digby külön hangsúlyt fektetett a **nyelvészet jövőbeli szerepére az AI fejlődésében**, és arra buzdította a hallgatóságot, hogy tekintsenek a nyelvi adatforrásokra nemcsak technikai erőforrásként, hanem mint a mesterséges intelligencia emberközelibbé tételének kulcsára.





Next level customer interaction: exploiting the power of Gen AI for Telefónica's customer service bot Aura

(Tina Rahman)

Tina Rahman előadásában bemutatta, hogyan alkalmazta a Telefónica Németországban a **generatív mesterséges intelligenciát ügyfélszolgálati chatbotja**, Aura fejlesztésében, és ezzel hogyan emelte magasabb szintre az ügyfélkapcsolatokat.

Az előadó részletesen ismertette, hogy a generatív AI milyen hatással volt a technológiai adaptációs ciklusokra, és **milyen lehetőségeket, valamint kockázatokat rejtett magában a virtuális asszisztensek bevezetése**. Kitért arra, hogyan zajlott a Conversational AI rendszerek bevezetése a Telefónicánál, különösen a német piacon, és milyen stratégiai szemlélet vezérelte a projektet.

Különös hangsúlyt kapott Aura teljesítményének elemzése: Tina Rahman konkrét mérőszámokon keresztül mutatta be, **hogyan teljesített a rendszer telefonos ügyfélszolgálaton és webes felületeken**.

Az előadás kitért azokra a tanulságokra is, amelyeket a generatív **AI-ra épülő proof-of-concept (PoC) projektek** során szereztek. Ezek a tapasztalatok segítették elő annak megértését, hogyan lehet a jövőben még személyre szabottabb, hatékonyabb és emberközelibb ügyfélélményt kialakítani a mesterséges intelligencia segítségével.



Practical application of LLMs to augment mature virtual assistants (Rui Teimao)

Rui Teimao előadásában gyakorlati példákon keresztül mutatta be, **hogyan egészítették ki az LLM-ek a már kiforrott virtuális asszisztenseket** a Lloyds Banking Groupnál. Hangsúlyozta, hogy a generatív AI nem feltétlenül váltotta le a meglévő rendszereket, sokkal inkább kiegészítette és új lehetőségeket nyitott meg azok továbbfejlesztésében.

Az előadó három fő területet emelt ki, ahol az LLM-ek értéket teremtettek:

1. **Pontosabb osztályozás** – másodlagos osztályozási rétegek bevezetésével javították a felhasználói kérések értelmezését.
2. **Hatékonyabb kiszolgálás** – a beszélgetések automatikus összegzésével csökkentették az ügyintézési időt (AHT).
3. **Szélesebb lefedettség** – a Retrieval-Augmented Generation (RAG) alkalmazásával kiterjesztették az asszisztensek tudását és válaszképességét.

Teimao hangsúlyozta a felelős AI-alkalmazás jelentőségét is, különösen a pénzügyi szektorban, ahol a biztonság, az átláthatóság és az elfogultság elleni védelem kiemelt szerepet kapott.

Az előadás során megosztotta a Lloyds tapasztalatait a generatív AI technológiák kutatásában és bevezetésében, emellett betekintést adott abba is, hogy milyen kihívásokkal jár ezeknek az új lehetőségeknek az integrálása egy már működő rendszerbe.





Agentic AI in 2025: hype, reality, and the road ahead

(Andreas Horn)

Andreas Horn előadásában kritikusan és gyakorlati tapasztalatokra építve járta körül az **„ügynök” (agent) fogalmának inflációját az AI világában**. Rámutatott, hogy 2025-re ez a kifejezés rendkívül sokféle jelentéstartalommal bír – az egyszerű, jól megírt promptoktól egészen a mesterséges általános intelligencia (AGI) víziójáig.

Az IBM AIOps vezetőjeként Horn betekintést adott azokba a kísérletekbe, amelyeket a cég AI-ügynökökkel folytatott az elmúlt időszakban. Elmondta, hogy bár technológiai szempontból történt előrelépés, például az **agent-alapú fejlesztési modellek** terén, a valós üzleti produktivitásnövekedés még sok esetben elmaradt a várakozásoktól. A látványos demók gyakran nem hozták meg a napi működésben is érezhető eredményeket, emiatt sok felhasználó hamar elvesztette érdeklődését.

Horn világossá tette, hogy a több lépésben gondolkodó, belső állapottal rendelkező és hosszú távú problémamegoldásra képes AI-ügynökök még mindig nem álltak készen a széles körű alkalmazásra. Ennek ellenére az agentic megközelítés terén elért eredmények reményt keltőek. Az előadás során végigvette, milyen technikai és szervezeti akadályokat kellett leküzdeni ahhoz, hogy az AI-ügynökök valóban transzformatív hatással bírjanak, és milyen lépések vezettek el ennek megvalósításához. Előadásával Horn igyekezett tisztázni a túlzott elvárásokat és rávilágítani azokra a realitásokra, amelyek mentén az AI-agentek valóban hasznos eszközei lehetnek a jövő digitális munkahelyének.

Introducing Mplus

(Koda Skurzewski)

Koda Skurzewski, az Mplus igazgatósági tagja és kereskedelmi vezérigazgatója bemutatta az Mplus platformot, amely egy **„minden az egyben” beszélgetési és agentic AI-megoldásként pozícionált ügyfélkapcsolati technológia**.

Az előadás során Skurzewski azt hangsúlyozta, hogy az Mplus nem csupán egy újabb AI-eszköz, hanem egy **teljesen integrált platform**, amely bármilyen rendszerrel képes együttműködni – vagy akár teljes egészében kiválthatja a meglévő technológiát. Megtudhattuk, hogy hogyan épül fel az Mplus a skálázhatóság, a megbízhatóság és a hosszú távú használhatóság jegyében.

Skurzewski kiemelte azokat a fejlesztéseket, amelyek az ügyfélélményt intelligensebbé, gyorsabbá és személyre szabottabbá tették: ilyenek voltak például a **mesterséges intelligencián alapuló hangszisztemek**, az **élő nyelvi fordítás**, az **érzelelemzés** és a **valós idejű operátori támogatás**. Az előadás nem csupán a technológiáról szólt, hanem arról is, hogyan lehet azt valóban emberszerű, hatékony és értékközpontú módon alkalmazni.

Koda lendületes, inspiráló stílusban mutatta be, miként alakította át az Mplus a vállalati ügyfélkapcsolati rendszereket a humán és a gépi erőforrások ötvöztetésével. Több, mint 100 leányvállalattal és egy sokrétű innovációs portfólióval az Mplus demonstrációja meggyőző példája volt annak, hogyan lehet a legújabb AI-fejlesztésekből valós, skálázható üzleti értéket teremteni.



Beyond the buzz: practical applications of LLM agents – Panelbeszélgetés (Muhammad Saad, Ruth Engemann, Aart Miedema, Laura Martín-Pérez González)

A panelbeszélgetés során a résztvevők arra keresték a választ, hogyan tudtak a nagy nyelvi modellek túllépni a hype-on, és **milyen konkrét üzleti és iparági előnyöket hoztak a gyakorlatban**. A beszélgetés középpontjában az LLM-agentek álltak, amelyek képesek voltak komplex feladatok elvégzésére, információk lekérésére, kontextus kezelésére és autonóm döntések meghozatalára.

Muhammad Saad a gyártás és ipari automatizálás területéről hozott példákat, ahol az LLM-agentek szerepet játszottak a **prediktív karbantartásban és a mérnöki támogatásban**. *Ruth Engemann* az energiaszektorból mutatott be olyan alkalmazásokat, ahol a hangalapú asszisztensek és LLM-agentek **javították az ügyfélszolgálatot és a belső hatékonyságot**. *Aart Miedema* a pénzügyi szektor nézőpontját képviselte, és azt vizsgálta, hogyan illeszkedtek ezek a rendszerek a **szigorúan szabályozott környezetbe**, míg *Laura Martín-Pérez González* a nyelvi oldalról világította meg a kihívásokat és a fejlődési lehetőségeket – különös tekintettel a **nyelvi modellek finomhangolására, kulturális érzékenységére és a többnyelvű támogatásra**.

A beszélgetés során nemcsak az eredmények, hanem a nehézségek is terítékre kerültek: ilyenek voltak például az agentek megbízhatóságával, skálázhatóságával és etikus alkalmazásával kapcsolatos kérdések. A panel minden résztvevője hangsúlyozta, hogy bár az LLM-agentek még fejlődés alatt álltak, már most is kézzelfogható értéket hoztak különböző iparágakban – ha megfelelő körülmények között, kellő szakértelemmel vezették be őket.

Conversational design IRL: what writing for robots has taught me about talking to humans (Cassie MacKenzie)

Cassie MacKenzie előadása személyes és szakmai tapasztalatokat ötvözve mutatta be, hogyan hatott a mesterséges intelligencia számára végzett beszélgetéstervezés (conversational design) az emberi kommunikációjára. A Scotiabank vezető tartalomtervezője **meta-megközelítésben** vizsgálta meg, **hogyan formálta át a „robotoknak írt szöveg” az emberekkel folytatott párbeszédeit** – és mit tanulhatott ebből mindenki, aki emberekkel dolgozik.

Az előadás középpontjában az **empátiaalapú tervezés** állt: Cassie azt hangsúlyozta, hogy a mesterséges intelligenciához tervezett párbeszédek során megtanult struktúrák, tónusok és stratégiák miként voltak hasznosak a munkahelyi interakciókban is – legyen szó ügyfelekről vagy kollégákról. Ugyanakkor rávilágított arra is, hogy a mesterségesen leegyszerűsített vagy túloptimalizált kommunikáció időnként akadályozta a valódi emberi kapcsolódást. Kiemelte, hogy **fontos egyensúlyt találni** a szakmai láthatóság, autonómia és együttműködés között, és a beszélgetéstervezési keretrendszereket nemcsak eszközként, hanem szemléletként is lehetett alkalmazni a humán munkakapcsolatokban. Cassie MacKenzie előadása inspirálóan hathatott azok számára, akik tartalommal, kommunikációval vagy UX-szel foglalkoznak, és azt keresik, hogyan lehet az AI-világban szerzett tudást visszaforgatni a humánabb szakmai működésbe.





AI chatbots: the good, the bad, and the ugly

(Koda Skurzewski)

Koda Skurzewski előadásában gyakorlati példákon keresztül mutatta be, **miért nem egyforma minőségű minden mesterséges intelligencián alapuló chatbot**. A résztvevők betekintést nyerhettek abba, hogyan különböztethetők meg az igazán hasznos AI-megoldások azoktól, amelyek csak bonyolítják az ügyfélélményt – vagy egyenesen ártanak neki.

Az előadás három részre bontva vizsgálta a chatbotok világát:

- **A jó** – működő, ügyfélbarát megoldások, amelyek gyorsítják és javítják a kiszolgálást, valódi értéket teremtenek.
- **A rossz** – félrevezető vagy gyenge AI-rendszerek, amelyek frusztrációt okoznak az ügyfeleknek.
- **A csúf** – példák olyan kudarcokra, amelyek hosszú távon rombolták a márkát vagy bizalmatlanságot keltettek.

Skurzewski élő bemutatóval is készült, ahol megmutatta, hogyan működött a **valós idejű nyelvi fordítás** mesterséges intelligencia segítségével. Külön hangsúlyozta, hogy az AI célja nem az emberi munkaerő leváltása, hanem annak megerősítése és támogatása. Rávilágított arra is, hogyan lehet felelősen és hatékonyan bevezetni AI-chatbotokat, és milyen szempontokat érdemes figyelembe venni egy technológiai beszállító kiválasztásakor.

The high stakes of AI: no brand can afford to fail

(Christoph Börner)

Christoph Börner előadásában arra hívta fel a figyelmet, hogy a mesterséges intelligencia gyors térnyerésével **az üzleti világban a bizalom nem luxussá, hanem alapvető követelménnyé vált**. Az AI-integráció sikere már nemcsak a technológiai fejlettségen múlik, hanem azon is, hogy a márkák mennyire tudják biztonságosan, felelősen és átláthatóan használni ezt az eszközt.

Az előadó hangsúlyozta, hogy még a legnagyobb, legmegalapozottabb vállalatok is komoly kockázatnak vannak kitéve, ha nem rendelkeznek megfelelő **AI-governance keretrendszerrel**. Részletesen bemutatta, hogy milyen következményekkel járhat az adatok félreértelmezése, az AI hibás döntései, vagy akár a felhasználók félretájékoztatása – ezek ugyanis hosszú távon a márkahűség és a piaci pozíció elvesztéséhez is vezethetnek.

Börner az erős **AI-bizalmi keretrendszer** kialakításának fontosságát hangsúlyozta, amely egyszerre szolgálja a felhasználók védelmét, a vállalat hírnevének megőrzését és a fenntartható technológiai növekedést. Az előadásban gyakorlati példákon keresztül mutatta be, hogyan lehetett megfelelő szabályozással, teszteléssel és átláthatósággal kezelni a kockázatokat, és miként vált az AI-tesztelés stratégiai eszközzé a márkaépítésben. Christoph Börner – aki a chatbotok és AI-megoldások tesztelésében úttörőnek számító Botium társalapítója is volt – előadásával azt üzent: az **AI nemcsak lehetőség, hanem felelősség is**, és aki ezt nem ismeri fel időben, komoly árat fizethet érte.



Start-up competition pitches

(Abdullah Al Wasif, Francesco (Francis) Signorato, Ursula Krobath, Daniel Shorr, Phil D Hall)

A konferencia ezen szekciójában öt ígéretes vállalkozás kapott lehetőséget arra, hogy bemutassa úttörő megoldásait a beszélgetési mesterséges intelligencia és hangtechnológia területéről. A verseny célja az volt, hogy reflektorfénybe helyezze a **leginnovatívabb korai fázisú vállalkozásokat**, amelyek **formálhatják a jövő digitális ügyfélmélményét**.

- **Abdullah Al Wasif** a UnityFlow AI képviselőként mutatta be, hogyan hozott létre egy olyan **többsz nyelvű hangfelismerő platformot**, amely különösen a **kisebbségi nyelvekre fókuszált**. A céljuk az volt, hogy lebontsák a nyelvi akadályokat és inkluzív technológiát biztosítsanak alulreprezentált közösségek számára is.
- **Francesco Signorato** a Nebuly élén azt demonstrálta, hogyan lehetett **skalázható és nyílt forráskódú megközelítéssel élményközpontú GenAI-termékeket fejleszteni**, amelyek valós igényekre reagáltak a felhasználói interfészek új generációjában.
- **Ursula Krobath**, a NERDPOLE alapítója, kiemelte, hogyan **ötvözte a nyelvészetet, a beszélgetési AI-t és a felhasználói élmény központú gondolkodást egyéni, B2B fókuszú tanácsadási szolgáltatásaiban**. Neurodivergens szemléletmódjának köszönhetően új perspektívákat nyitott a tervezési folyamatokban és a befogadó technológiai megoldások kialakításában.
- **Daniel Shorr** bemutatta a GoLLM ügynök-alapú elemző rendszerét, a D.A.V.E.-et, amely képes volt **nyers kérdőíradatokat átalakítani vizuálisan is értelmezhető, cselekvésre ösztönző betekintésekké**. A projekt mögött több közszektorbeli együttműködés és egy országos AI-felkészültségi felmérés is állt.
- **Phil D Hall** az Elzu-ltd. színeiben a www.mimi.coach nevű **motivációs interjú-alapú platformot** mutatta be, amely etikus, átlátható és adatvédelmi szempontból is felelősen kialakított AI-rendszert kínált. Az avatártechnológia és emberközpontú interakciók ötvöztetésével az AI-t egyfajta segítő, támogató szereplőként pozicionálta.

A pitch szekció változatos szemléletet és megközelítéseket vonultatott fel – a társadalmi hasznosságtól a technológiai innovációig –, és jól tükrözte, hogy a beszélgetési mesterséges intelligencia fejlődése mennyire sokrétű és interdiszciplináris lett.





The full-stop problem: how to overcome RAG's achilles heel (Kane Simms)

Kane Simms előadásában egy gyakorlati kihívást állított a középpontba, amellyel sokan találkoztak a **Retrieval Augmented Generation (RAG)** rendszerek alkalmazása során: az úgynevezett **„pont” vagy „full stop” problémát**. Ez a jelenség akkor jelentkezett, amikor a generatív AI válasza a visszakeresett információ alapján túlságosan rövid, töredékes vagy lehatárolt lett – ezzel csökkentve a felhasználói élményt és a rendszer hasznosságát.

Simms részletesen ismertette, hogyan akadályozta ez a jelenség a RAG rendszerek skálázását, különösen olyan környezetekben, ahol a természetes, folyamatos párbeszéd és a kontextus megértése kulcsfontosságú volt. Ahelyett, hogy pusztán a problémára koncentrált volna, gyakorlati megoldási javaslatokat is kínált: például a **generatív komponens intelligensebb vezérlését**, több forrásból történő **dinamikus információ-aggregálást**, valamint a **prompt-stratégiák optimalizálását**.

Az előadás célja az volt, hogy a RAG technológiát nem önmagában, hanem egy holisztikus, ügyfélművelő központú rendszer részeként mutassa be. Simms arra ösztönözte a közönséget, hogy a technológia határainak felismerése mellett annak továbbfejlesztésére is törekedjenek – különösen olyan megoldásokkal, amelyek a valós felhasználói igényekből indulnak ki. Kane Simms, aki a VUX World alapítójaként régóta foglalkozik hangalapú és beszélgetési AI-technológiákkal, előadásában világossá tette: a RAG jövője nem a sémák másolásában, hanem azok tudatos továbbgondolásában rejlik.

From Wikipedia to wonder: building real-time GenAI with Astra DB, streaming, and Langflow (Michel de Ru, Ted Haile)

Michel de Ru és Ted Haile mesterkurzusa látványos és interaktív bemutatót nyújtott arról, hogyan lehetett **valós idejű generatív AI-megoldásokat építeni Wikipedia-adatokból kiindulva**, a **DataStax technológiáira** építve. Az esemény során az érdeklődők nemcsak megfigyelői, hanem aktív résztvevői is lehettek egy modern AI-alkalmazás felépítésének – egészen az élő adatfolyamtól a működő AI-ügynökhöz.

Az előadás első részében az előadók élőben demonstrálták, hogyan lehetett a Wikipedia adatfolyamait betölteni az **Astra Streaming** segítségével, majd ezeket **Astra DB-be** integrálni, amely a gyors és hatékony AI-lekérdezésekhez szükséges vektoralapú adattárolást biztosította. Ezt követően bemutatták, hogyan lehetett a **Langflow** platformot használni agentic AI-workflowk létrehozására, amelyek képesek voltak valós idejű kérdések megválaszolására, összegzésekre és összetettebb feladatmegoldásra is.

Az esemény nemcsak fejlesztőknek, hanem üzleti döntéshozóknak is tartogatott értékes gondolatokat, különösen azok számára, akik élesben is szeretnék alkalmazni a generatív AI-t valós idejű ügyfélművelő vagy üzleti folyamatok támogatására.



The evolution of AI service: when machines talk and humans connect

(Mudabir Khan, Cassie MacKenzie, Jesse Lucas, Oksana Hagen)

A beszélgetés résztvevői arra keresték a választ, **hogyan változott meg a gépekkel folytatott kommunikáció természete**, és **milyen hatással volt mindez az emberi kapcsolatokra és márkáélményekre**. A panel során különösen nagy hangsúlyt kapott az a folyamat, amelyben az előre megírt, merev válaszokat fokozatosan felváltották a kontextusérzékeny, alkalmazkodó beszélgetési stílusok.

- *Mudabir Khan* nyelvészeti háttérre támaszkodva kiemelte, hogy a hang- és szövegalapú UX tervezés során **egyre fontosabbá vált a természetes nyelvi árnyalatok kezelése**, míg *Cassie MacKenzie* arról beszélt, hogyan lehetett **megtartani a márka hangját és hitelességét** akkor is, amikor AI végezte az ügyfélkommunikáció nagy részét.
- *Jesse Lucas* bemutatta, milyen tapasztalatokat szereztek a Lebaránál különböző piacokon futtatott chatbot-fejlesztések során, és hogyan lehetett megtalálni a megfelelő egyensúlyt a professzionális és a közvetlen kommunikációs stílus között. Külön kitért a **„konverzációs kereskedelem”** (conversational commerce) szerepére az ügyfélművelés javításában.
- *Oksana Hagen* a tudományos oldalról közelítette meg a kérdést: megosztotta legújabb kutatási eredményeit az **ember-gép interakció és a társas dinamika változásairól**, és arról, milyen újfajta kihívásokat jelentett az AI-rendszerek társas környezetbe való integrálása.

A beszélgetés során a résztvevők közösen azt is megvizsgálták, milyen gyakorlati keretrendszerek segítették elő, hogy az AI-kommunikáció ne távolítsa el a márkát az emberektől, hanem hiteles és emberközeli élményt nyújtson. A panel kiegyensúlyozottan ötvözte az ipari gyakorlatot és a tudományos nézőpontot, így átfogó képet adott a beszélgetési AI jövőjéről – és annak emberi oldaláról.





Transforming education with Vertex AI: smart virtual agents for universities (Stefano Carlini)

Stefano Carlini előadásában azt mutatta be, **hogyan alakította át a felsőoktatási intézmények működését a Vertex AI platformra épülő intelligens virtuális ügynökök alkalmazása.** A technológia lehetővé tette a chatbotok gyors fejlesztését és bevezetését, miközben jelentős hatást gyakorolt az egyetemek hallgatói támogatási rendszereire és belső folyamataira.

Az előadó három fő területre helyezte a hangsúlyt:

1. **Gyors fejlesztés és üzembe helyezés** – bemutatta, hogyan egyszerűsítette a Vertex AI az összetett, kontextusérzékeny chatbotok létrehozását, akár programozási tapasztalat nélkül is.
2. **Hallgatói élmény javítása** – konkrét példákon keresztül szemléltette, hogyan tudtak ezek az AI-megoldások éjjel-nappali tájékoztatást nyújtani, támogatni a beiratkozási folyamatokat, vagy segíteni a tanulmányi adminisztrációban.
3. **Működési hatékonyság növelése** – Carlini kiemelte, hogy az ismétlődő, időigényes feladatok automatizálásával az oktatási intézmények humán erőforrásai értékesebb, stratégiai feladatokra összpontosíthattak.

Az előadás során világossá vált, hogy a felhőalapú AI-megoldások nemcsak technológiai fejlesztést jelentettek, hanem valódi, mérhető előnyöket hoztak az oktatás világába – legyen szó költséghatékonyságról, skálázhatóságról vagy jobb hallgatói élményről.



Miért volt értékes az NBSZ NKI számára a European Chatbot & Conversational AI Summit 2025?

A *European Chatbot & Conversational AI Summit 2025* kivételes lehetőséget kínált az NBSZ NKI számára, hogy átfogó képet kapjon a mesterséges intelligenciára épülő beszélgetési rendszerek legfrissebb fejlesztéseiről, és azokat kibervédelmi szempontból is megvizsgálja. Bár az esemény fő fókuszában az ügyfélélmény és a vállalati hatékonyság növelése állt, a **bemutatott technológiák mögött meghúzódó biztonsági kockázatok és a védekezési lehetőségek** szinte minden előadásban közvetve vagy közvetlenül megjelentek.

A prezentációk alapján egyértelművé vált, hogy a generatív AI-megoldások – legyen szó ügyfélszolgálati chatbotokról, virtuális asszisztensekről vagy valós idejű hangalapú tolmácsolásról – **új támadási felületeket nyitnak meg**. A prompt injection, a nyelvi modellek manipulációja és az érzékeny adatok nem szándékos kiszivárgása komoly kihívás elé állítja a biztonsági szakembereket. A konferencia rámutatott, hogy a **védekezés nemcsak technológiai kérdés**, hanem a transzparens működést, visszakövethetőséget és szabályozottságot biztosító AI-irányítási keretrendszerek bevezetése is elengedhetetlen.

A prezentációk olyan példákat is felvonultattak, amelyek rávilágítottak az **LLM-alapú rendszerek működésének technikai és biztonsági korlátaira**. Az úgynevezett „full stop problémára” vagy az agentek megbízhatósági nehézségeire való utalások jól érzékeltették, hogy ezek a megoldások a kibervédelmi gyakorlatban csak **kellő elővigyázatossággal, alapos tesztelést követően alkalmazhatók**. Ugyanakkor az is világossá vált, hogy az ilyen rendszerek hatékony döntéstámogatást nyújthatnak olyan adatintenzív környezetekben, mint amilyen a kiberfenyegetések elemzése. A hallottak megerősítették, hogy az AI-ra épülő automatizációs eszközök – például automatikus összegzők, klaszterezők vagy érzelemelemzők – értékes támogatást jelenthetnek a túlterhelt elemzői kapacitások enyhítésére.

A chatbotok ügyfélinterakciós képességeiben rejlő lehetőségek különösen érdekes párhuzamokat mutattak **az incidenskezelő rendszerek működésével**. A konferencián elhangzott példák szerint a virtuális asszisztensek képesek voltak napi több ezer bejövő kérdést önállóan priorizálni, strukturálni és feldolgozni. Ez alapján valós alternatívát jelenthetnek az NBSZ NKI számára is olyan feladatok automatizálására, mint a bejelentések elsődleges kategorizálása vagy a támadásminták felismerése – természetesen **szigorúan szabályozott környezetben**, megfelelő kontrollmechanizmusokkal ellátva.



A rendezvényen bemutatott technológiai ökoszisztémák – köztük a Langflow, az Astra DB és Streaming, a Vertex AI vagy az Mplus platform – azt is világossá tették, hogy a mesterséges intelligencia biztonsági vizsgálatát nem lehet kizárólag hálózati vagy rendszerüzemeltetési szinten elvégezni.

A védelem kiterjed az adathasználatra, a modelltréning folyamatára, az interakciók során keletkező metainformációkra, valamint az AI-rendszerek működésének magyarázhatóságára és reprodukálhatóságára is.

Összességében a konferencia megerősítette azt a felismerést, hogy a beszélgetési mesterséges intelligencia nemcsak a civil vagy üzleti szektorban jelent áttörést, hanem **egyre fontosabbá válik kibervédelmi szempontból is**. A rendezvény tanulsága egyértelmű: az **AI nemcsak lehetőséget, hanem új típusú fenyegetést is hoz**, amelyre a kiberbiztonsági közösségnek proaktívan, szervezeten és tudatosan kell reagálnia.

A konferencián elhangzott előadások későbbiekben az esemény honlapján elérhetőek lesznek.