

AI CYBERSECURITY SUMMIT

Adatból előny vagy kockázat? Kiberbiztonság, AI és vállalati hatékonyság az új digitális korszakban

2026. 09. 08. 16:50

Innovation Hall

HUN · 30 perc

**Kerek István**

vezérigazgató · Everengine

**Takács Krisztián**

Nemzetközi stratégiai tanácsadó, a ViVeSec termékcsalád piacra viteléért felelős vezető · ViVeTech Nyrt.

**Márton Miklós**

vezérigazgató · ViVeTech Nyrt.

**Nagy Gábor**

Emberközpontú innovátor · Gaphopper | Virtuális karrier központ - alapító

Kerek István, Márton Miklós, Takács Krisztián és Nagy Gábor a kiberbiztonság, az adatvédelem és a mesterséges intelligencia kis- és középvállalkozások általi gyakorlati megvalósításának kritikus metszéspontjéről tárgyalnak.

MIRŐL VOLT SZÓ

Takács Krisztián kiemeli, hogy a vállalatok gyakran küzdenek az adatok védelmével még a belső hálózatokon belül is, és ezt a kihívást tovább súlyosbítja a COVID-19 idején szükséges távoli hozzáférés. Megjegyzi, hogy a munkavállalók gyakran feltöltenek érzékeny vállalati adatokat mesterséges intelligencia szolgáltatókra, anélkül, hogy tudatában lennének annak, hogy ezek a platformok felhasználhatják az információkat más modellek képzésére. Például a kis- és középvállalkozások gyakran nem rendelkeznek a nagyvállalatoknál szokásos hivatalos engedélyezési kezeléssel és belső ellenőrzésekkel.

Márton Miklós hangsúlyozza, hogy a kisvállalkozások számára a legfontosabb kockázat a specializált IT-biztonsági személyzet és a kialakított protokollok hiánya, ami sebezhetővé teszi őket a zsarolóvírusokkal szemben. Kerek István szerint az AI értékét az adja, hogy képes az emberi erőforrások megkettőzésére és a specifikus feladatok automatizálására, nem pedig általános célú eszközként való működésre. Például egy

vállalatnak a kritikus adatkörökre kellene összpontosítania, nem pedig arra, hogy egy AI-ügynök mindent tudjon. Ezek az elemek azt sugallják, hogy az AI-kiberkockázatok kezelésének funkcionális korlátozáson és célzott adatvédelmen keresztül kell megtörténnie.

KIEMELT MEGÁLLAPÍTÁSOK

- Európában körülbelül 27 millió kis- és középvállalkozás küzd napi szinten kiberbiztonsági kihívásokkal.
- AI modelleket gyakran úgy terveznek, hogy mindenáron választ adjanak, ami hallucinációkhoz vagy jogosulatlan adatok nyilvánosságra hozatalához vezethet.
- A leghatékonyabb módszer az AI üzleti célú biztonságos használatára, ha funkcióit szigorúan korlátozzuk bizonyos, szükséges feladatokra.

ÜZLETI HATÁS

A vita jelentős piaci lehetőséget azonosít a kis- és középvállalati szektor számára testreszabott, biztonságos AI-ügynökök biztosításában. Azáltal, hogy a vállalatok elmozdulnak az általános célú chatbotoktól a „korlátokkal” rendelkező specializált eszközök felé, növelhetik a hatékonyságot anélkül, hogy érzékeny információkat tennének ki. Kerek István megjegyzi, hogy a verseny egyre inkább azon fog múlni, hogy melyik AI-ügynök rendelkezik a legrelevánsabb, védett tudással. Ez a megközelítés lehetővé teszi a vállalkozások számára, hogy automatizálják az adminisztratív feladatokat, például a jogi titkársági munkát, miközben megőrzik az adatok integritását és megszüntetik a biztonsági réseket.

KÖVETKEZTETÉS

A felszólalók azt javasolják, hogy az egyének és a vállalkozások ellenőrizzék, milyen adatokat töltöttek fel az elmúlt hónapokban a nyilvános mesterséges intelligencia platformokra. Nagy Gábor azt javasolja, hogy az emberek kérdezzék meg a nagy nyelvi modelleket, hogy milyen konkrét adatokat tudnak róluk, hogy megértsék a kockázatokat. A panel arra a következtetésre jut, hogy a kiberbiztonság olyan terület, amelyet gyakran csak akkor vesznek észre, amikor probléma merül fel, ezért a proaktív oktatás és a biztonságos, korlátozott funkcionalitású mesterséges intelligencia ügynökök bevezetése elengedhetetlen a modern vállalkozások túléléséhez.

AI CYBERSECURITY SUMMIT

Data: Competitive Advantage or Risk? Cybersecurity, AI, and Corporate Efficiency in the New Digital Era

2026. 09. 08. 16:50

Innovation Hall

HUN · 30 perc

**István Kerek**
CEO · Everengine**Miklós Márton**
CEO · ViVeTech**Krisztián Takács**
International Strategic Advisor, responsible for the go-to-market strategy of the ViVeSec product family · ViVeTech**Gábor Nagy**
Human-Centered Innovator · Founder of Gaphopper | Virtual Career Center

István Kerek, Miklós Márton, Krisztián Takács, and Gábor Nagy discuss the critical intersection of cybersecurity, data protection, and the practical implementation of artificial intelligence for small and medium-sized enterprises.

WHAT WAS DISCUSSED

Miklós Márton highlights that the COVID-19 pandemic forced companies to open internal networks to the internet, creating significant risks when employees upload corporate data to AI service providers. Krisztián Takács emphasizes that small and medium-sized enterprises (SMEs) often lack the formal authorization systems and IT security standards that are common in large corporations, making them vulnerable to internal data leaks and external threats. For example, a large manufacturer was found to have 47 unauthorized Wi-Fi networks despite official policies forbidding them.

Gábor Nagy argues that the primary challenge for individuals and SMEs is often a lack of human resources to interpret data rather than a lack of technology itself. István Kerek explains that the value of AI lies in creating specific "guardrails" and security policies to prevent prompt injections or unauthorized data deletions. For

example, a hacker used a prompt injection to force an AI agent to send all contact information from an email to an external source. These elements collectively suggest that security must be balanced with functionality by limiting AI capabilities to specific, high-value business tasks.

KEY TAKEAWAYS

- Miklós Márton notes that there are 27 million SMEs in Europe facing daily cybersecurity challenges without dedicated IT security experts.
- István Kerek suggests that SMEs should focus on specific, critical data areas rather than trying to make AI agents know everything.
- Gábor Nagy points out that AI can create value by identifying "red flags" like bullying or depression in chat patterns by modeling human cognition.

BUSINESS IMPACT

The discussion identifies a clear market need for affordable, practical cybersecurity solutions tailored for the SME sector, which forms the backbone of the European economy. By implementing restricted AI agents that perform specific tasks—such as legal secretarial work—companies can increase efficiency and automate processes without exposing sensitive data to the public internet. This approach allows businesses to mitigate the risk of ransomware, which often only reveals the true value of data once it has been encrypted and stolen.

CONCLUSION

The speakers conclude by urging the audience to take immediate practical steps, such as auditing what data family members or colleagues have uploaded to public AI models over the last three months. They recommend asking AI models what data they know about the user to understand the scope of potential exposure. Finally, they call for a collaborative approach where security experts are involved in building AI agents to ensure that functionality does not come at the expense of safety.