

AI TRENDS

Agentic AI a piloton túl: hogyan kerüljük el a korai bevezetés hibáit?

2026. 09. 08. 11:40

MBH Bank Visionary Stage

HUN · 20 perc

**Dalos-Kovács Gabriella**

AI governance és AI stratégiai tanácsadó

Dalos-Kovács Gabriella, egy MI-irányítási és MI-stratégiai tanácsadó, keretrendszert hoz létre az AI-ügynökök kockázatainak és működési követelményeinek kezelésére vállalati környezetekben.

MIRŐL VOLT SZÓ

A prezentáció az AI-ügynököket megkülönbözteti a hagyományos chatbotoktól, gépi tanulási modellektől és a Generatív AI-től, mivel képesek önálló célokat követni, nem csupán részfeladatokat végrehajtani. Míg egy chatbot információt szolgáltat, egy ügynök önállóan cselekszik egy konkrét cél elérése érdekében, API-k meghívásával, adatbázisok elérésével és a terv szükség szerinti adaptálásával, például egy ügynök önállóan navigálhat különböző rendszerek között egy utazási foglalás teljesítéséhez.

Dalos-Kovács Gabriella hangsúlyozza, hogy az ügynökök gyors bevezetése „árnyékügynök” kockázatokat teremt, amikor eszközöket integrálnak a munkafolyamatokba megfelelő felügyelet vagy megfelelőségi ellenőrzések nélkül. Ezeknek a kockázatoknak a csökkentése érdekében a szervezeteknek olyan irányítási ciklust kell bevezetniük, amely magában foglalja a hozzáférési határok meghatározását, az engedélyezési kapuk létrehozását és egy ügynöklista fenntartását teljes ellenőrzési nyomvonalakkal. Ezek az elemek együtt biztosítják, hogy az autonóm tevékenységek biztonságos és mérhető határokon belül maradjanak.

KIEMELT MEGÁLLAPÍTÁSOK

- A vállalatok által kezelt ügynökök aránya várhatóan megduplázódik, 2025-ben mért 17%-ról 2026-ra 37%-ra.
- A kutatások szerint az MI-ügynök projektek 88%-a kudarcot vall, gyakran az infrastruktúra, a kormányzás vagy a megtérülés mérésének hiánya miatt.
- A 68%-os telepítési hiány azért áll fenn, mert az elfogadott ügynököknek csak 11%-a éri el sikeresen a termelési környezetet.

ÜZLETI HATÁS

A sikeres ügynök-implementáció jelentős eredményeket hozhat, például 171%-os sikerrátát alacsony kockázatú esetekben, vagy 20%-os bruttó eladásnövekedést értékesítési támogató ügynökök révén. Gyakorlati alkalmazások közé tartozik az IT-ügyfélszolgálati jegyek automatizálása, a szabályozási változások figyelése és a projektidőszakok kezelése. Azonban a magas kockázatú területeken, mint a pénzügyi tranzakciók vagy egészségügyi döntések, „emberi ellenőrzés” szükséges a biztonság és elszámoltathatóság fenntartásához.

KÖVETKEZTETÉS

Dalos-Kovács Gabriella azt javasolja, hogy kis kockázatú, nagy hatékonyságú ügynökökkel kezdjék, hogy tapasztalatot szerezzenek, mielőtt bővítenék az autonómiát. Azt tanácsolja a vállalatoknak, hogy hozzanak létre egy hivatalos irányítási programot, amely magában foglalja az értékelést, a besorolást és a mutatók folyamatos mérését, például a sikerarányokat és a tokenhasználatot, hogy igazolják a folyamatos befektetést.

AI TRENDS

Agentic AI Beyond the Pilot: How to Avoid the Pitfalls of Early Adoption

2026. 09. 08. 11:40

MBH Bank Visionary Stage

HUN · 20 perc

**Gabriella Dalos-Kovács**

AI governance and AI strategy consultant

Gabriella Dalos-Kovács, an AI governance and AI strategy consultant, establishes a framework for managing the risks and governance of AI agents as they transition from hype to standard business processes.

WHAT WAS DISCUSSED

Gabriella Dalos-Kovács distinguishes AI agents from traditional chatbots, machine learning models, and generative AI by their ability to pursue a specific goal autonomously rather than just performing sub-tasks. While a chatbot provides information and a standard process runs a set sequence, an agent identifies the necessary tools, calls APIs, and adapts its plan to reach a defined objective, for example, an agent that independently navigates various systems to complete a travel booking.

The presentation highlights the dangers of "shadow agents" that enter IT systems through functional integrations or developer tools without proper oversight. Gabriella Dalos-Kovács argues that organizations must implement a governance loop that includes defining access scopes, establishing approval gates, and maintaining an agent inventory with full audit trails. These elements are necessary to prevent agents from causing unintended damage while still leveraging their efficiency, for example, by restricting an agent's permissions to the minimum required for its specific task.

KEY TAKEAWAYS

- The percentage of companies managing agents is expected to double from 17% in 2025 to 37% in 2026.
- Approximately 88% of AI agent projects fail due to infrastructure gaps, governance hurdles, and a lack of ROI measurement.
- High-risk use cases involving financial transactions or legal documents require a "human in the loop" for final decision-making.

BUSINESS IMPACT

Effective agent deployment can yield significant returns, such as a 171% success rate for low-risk use cases or a 20% increase in gross sales through sales support agents. However, without proper governance, companies face a 68% deployment gap where projects fail to reach production environments. Organizations must prioritize scalable infrastructure and clear metrics, such as successful system calls and token usage, to justify the investment to leadership.

CONCLUSION

Gabriella Dalos-Kovács recommends starting with low-risk agents, such as those for IT helpdesk permissions, legal regulation monitoring, or project management assistance. She encourages the audience to move from full trust or total isolation toward a controlled, measurable framework that allows for the gradual expansion of agent autonomy.