

AI agent unikol z testu a otvoril nový trh pre kybernetickú bezpečnosť

22.7.2026 - Dominik Hapl | Across Private Investments

OpenAI priznalo jeden z prvých verejne známych prípadov, keď pokročilý AI agent vykonal kybernetický útok mimo priamej kontroly človeka. Model mal v testovacom prostredí preverovať svoje schopnosti, no dokázal uniknúť zo zabezpečeného systému, získať prístup na internet a preniknúť do infraštruktúry platformy Hugging Face. Pri útoku objavil nové zraniteľnosti a ukradol prihlasovacie údaje.

Pre finančné trhy je dôležité, že AI tým prestáva byť iba rastovým príbehom. Stáva sa aj zdrojom nových nákladov a rizík. Firmy budú musieť viac investovať do ochrany dát, kontroly AI agentov a testovania systémov pred ich nasadením. To môže zvýšiť výdavky technologických spoločností, no zároveň vytvára nový dopyt po kybernetickej bezpečnosti.

Najviac môžu z tejto zmeny ťažiť firmy, ktoré chránia cloud, identitu používateľov, dátové centrá a firemné siete. Doteraz bol hlavným problémom človek, ktorý použil AI na útok. Teraz vzniká aj scenár, v ktorom dokáže škodu spôsobiť samotný agent, ak dostane priveľkú voľnosť alebo zle nastavený cieľ. To zvyšuje význam bezpečnostného softvéru, poistenia proti kybernetickým útokom aj prísnejšej regulácie.

Pre investorov je to dvojsečný príbeh. Vývojári AI môžu čeliť vyšším nákladom, právnym sporom a tlaku na pomalšie uvádzanie nových modelov. Na druhej strane môže rásť celý trh ochrany digitálnej infraštruktúry. Kybernetická bezpečnosť sa tak mení z podpornej služby na jednu z podmienok, bez ktorej sa ďalšia vlna AI investícií nezaobíde.

<https://across.sk/ai-agent-unikol-z-testu-a-otvoril-novy-trh-pre-kyberneticku-bezpecnost>