

Gemini pri bezpečnostnom teste prenikol do systémov troch firiem. Google priznal incident

20.9.2026 - Milan Menšík | Zajtra studio spol.

Google potvrdil, že jeho umelá inteligencia Gemini sa v máji počas bezpečnostného testovania dostala do systémov troch externých spoločností. Podľa vyšetrovania denníka *The Wall Street Journal* model využil prístup na internet a prenikol do chránených systémov. Test prebiehal v spolupráci s bezpečnostnou firmou Irregular.

Gemini sa sám zastavil, keď zistil, že prenikol do skutočných systémov

Podobné prípady sa v poslednom období objavujú čoraz častejšie. S vlastnými bezpečnostnými problémami sa stretli aj **OpenAI** či **Anthropic**, čo vyvolalo diskusiu o rizikách vývoja pokročilých modelov. **V jednom prípade sa Gemini pokúšal uhádnuť heslo, až kým nezískal prístup do systému.** V ďalších dvoch situáciách využil prihlasovacie údaje, ktoré objavil vo verejne dostupnom online úložisku.

Gemini Live | Zdroj: Lenka Ivančíková

Google uviedol, že **model svoje konanie zastavil hneď po tom, ako zistil, že prenikol do skutočných systémov** a nie do simulovaného prostredia. Spoločnosť preto udalosť nepovažuje za príklad nesúlady modelu s bezpečnostnými pravidlami. **Ochranné mechanizmy podľa nej zabránili ďalšiemu pokračovaniu.** Google však prípad verejne neoznámil predtým, než ho kontaktoval *The Wall Street Journal*.

Mohlo by vás tiež zaujímať:

- Sériá Xiaomi 18 Pro príde už budúci týždeň. Toto je jej 5 kľúčových vlastností
- Trh s Android tabletmi klesá, no Honor rastie. Čo je za úspechom?
- Samsung chystá pre Galaxy S27 Ultra vylepšenie, po ktorom fanúšikovia dlho volajú

Názvy dotknutých spoločností nezverejnil, potvrdil však, že všetky tri o udalosti informoval. O prienikoch zároveň **upovedomil federálne úrady**. Problém vznikol aj preto, že bezpečnostná firma **Irregular** počas testovania **neúmyselne ponechala Gemini prístup na internet**. Následne spolupracovala s Googlom na úprave testovacích postupov. **Presná verzia Gemini použitá pri teste zatiaľ nie je známa.** Keďže k incidentu došlo v máji, nešlo o najnovšie modely predstavené neskôr.

<https://www.mojandroid.sk/gemini-pri-bezpecnostnom-teste-prenikol-do-systemov-troch-firiem>