

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **145** ze dne **2.6.2026**

Umělá inteligence brzy vyvolá "patchové tsunami".

Britská agentura pro kybernetickou obranu varuje, že umělá inteligence brzy zásadně otřese oblastí kybernetické bezpečnosti. Tím, že odhalí dlouho skryté softwarové chyby rychleji, než je vývojáři stihnou opravit.

V příspěvku na blogu technický ředitel Národního centra pro kybernetickou bezpečnost Ollie Whitehouse uvedl, že firmy by se měly připravit na nápor bezpečnostních aktualizací – doslova na "patchovou vlnu" –, protože nástroje umělé inteligence odhalují slabiny, které se hromadily po celá léta.

"Všechny organizace mají ‚technický dluh‘; nahromaděné technické problémy. Došlo k němu v důsledku upřednostňování krátkodobých zisků před vytvářením odolných produktů," napsal Whitehouse.

Varoval, že umělá inteligence je nyní schopna tyto slabiny identifikovat a zneužít "ve velkém měřítku a rychlým tempem", což nutí organizace k tomu, co popsal jako "nucenou nápravu".

Načasování není náhoda. Nové nástroje umělé inteligence od společností jako Anthropic a OpenAI jsou navrhovány tak, aby automaticky detekovaly, a dokonce opravovaly zranitelnosti. To sice může pomoci obráncům, ale zároveň útočníkům usnadňuje hledání stejných chyb.

"Očekáváme příliv aktualizací, které budou řešit zranitelnosti všech úrovní závažnosti, a předpokládáme, že řada z nich bude kritická," uvedl Whitehouse.

Aby se organizace vyrovnaly s tím, co přijde, NCSC je naléhavě vyzývá, aby snížily svou zranitelnost – počínaje systémy připojenými k internetu. I tak však samotné záplatování nemusí stačit. Starší systémy, které už nejsou podporovány, bude možná nutné zcela nahradit.

AV centrum ČR