

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **116** ze dne **19.8.2025**

AI pomáhá k vylepšení a urychlení kybernetických útoků

Ne všechny zranitelnosti jsou stejné. Některé z nich se ukázaly jako kritické body úniku a jsou neúnavně využívány kyberzločinci, kteří se snaží získat přístup do podnikových sítí. "Osvědčené útoky stále fungují, protože příliš mnoho organizací nedodržuje správnou kybernetickou hygienu. Zpoždění ve správě záplat, chybná konfigurace a špatná segmentace sítě vytvářejí ideální podmínky pro úspěch automatizovaně řízených útoků," vysvětluje Ondřej Štáhlavský, regionální ředitel společnosti Fortinet pro střední a východní Evropu.

Nárůst zneužití zařízení internetu věcí (IoT)

Podle nejnovější analýzy laboratoří FortiGuard Labs 2025 Global Threat Landscape Report bylo v roce 2024 zachyceno více než 97 miliard pokusů o zneužití, což ukazuje, jak kyberzločinci nepřetržitě sondovali odhalené systémy. Na zásadní bezpečnostní mezery poukazuje také nárůst zneužití zařízení internetu věcí (IoT) – nejčastějším cílem útoků jsou totiž routery, kamery a síťový hardware.

Mnoho organizací navíc nepřistupuje k zabezpečení internetu věcí stejně důsledně jako k tradičním prostředkům IT. Útočníci využívají výchozí přihlašovací údaje, zastaralý firmware a odhalená rozhraní pro správu jako vstupní body pro útoky většího rozsahu. Tato zařízení také často slouží jako bezpečné útočiště pro botnety.

Současná role AI v kybernetické kriminalitě

Kyberzločinci využívají umělou inteligenci především ke zvýšení účinnosti a rozsahu stávajících technik, jako je sociální inženýrství a nasazení malwaru. Jsou přitom metodičtí a vytrvalí a operují bez hranic.

Závažnějším dlouhodobým problémem je rychlost, s jakou tito aktéři sdílejí úspěšné metody a nástroje. Techniky vyvinuté jedním aktérem jsou často převzaty ostatními během několika týdnů.

"Při plánování obranných strategií je nezbytné předvídat, jak bude AI v nadcházejících letech měnit taktiky kyberzločinců. Potenciál budoucího pokroku v oblasti umělé inteligence, který může výrazně urychlit objevování zranitelností nultého dne, je vážným problémem, na který musí být obránci připraveni. Útočníci by například mohli využívat zranitelnosti v samotných systémech AI. Jelikož předvídáme, jak mohou útočníci v budoucnu využívat umělou inteligenci, je jasné, že boj proti pokročilejším hrozbám řízeným AI vyžaduje také vývoj naší obrany. Úspěch bude záviset nejen na technologii, ale také na spolupráci, flexibilitě a neustálém přizpůsobování," dodává Ondřej Štáhlavský.

Zdroj: AVcentrum ČR