ESET představuje nové funkce pro zabezpečení komunikace s chatboty a AI agenty

13.5.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Praha, 13. května 2026 — Společnost ESET, přední globální poskytovatel řešení v oblasti kybernetické bezpečnosti, oznámila připravované funkce kyberbezpečnostní ochrany, jejichž cílem je zabezpečit způsob, jakým zaměstnanci pracují s nástroji umělé inteligence. Nové funkce, které byly představeny na konferenci RSAC 2026 a jejichž spuštění je plánováno v letošním roce, umožní bezpečnostním týmům sledovat a vyšetřovat rizika spojená s každodenním používáním AI nástrojů a nasazováním AI agentů ve firmách, a to prostřednictvím platformy ESET PROTECT.

„S tím, jak se firmy stále více spoléhají na AI kvůli zvyšování produktivity a automatizaci, čelí rostoucím rizikům spojeným s únikem citlivých dat, porušením legislativních rámců a zavádějícími výstupy," uvádí Juraj Jánošík, ředitel vývoje automatizovaných systémů a umělé inteligence ve společnosti ESET. „Agentická AI přesouvá kyberbezpečnostní bojiště zpět na koncová zařízení. ESET strávil více než 30 let budováním špičkové ochrany koncových zařízení využívající AI a strojové učení, což nás staví do jedinečné pozice, ve které můžeme pomáhat firmám zabezpečit tuto další vlnu vývoje umělé inteligence přímo tam, kde vzniká."

Nástroje umělé inteligence se stávají součástí každodenních pracovních postupů a mnoho zaměstnanců v souvislosti s tím používá otevřené cloudové chatboty bez dohledu IT oddělení. To vytváří rizika v podobě tzv. stínového AI (Shadow AI) a vystavuje rizikům citlivá data, jako jsou interní dokumenty, API klíče, tajné informace či přihlašovací údaje. ESET na tuto situaci reaguje prostřednictvím různých technologií, které se dostávají co nejblíže ke zdroji. Jednou z nich je zabezpečený webový prohlížeč, který zachytí interakci s AI a v reálném čase analyzuje jak prompty (zadání úkolu či dotazu), tak odpovědi. Tím pomáhá předcházet úniku dat a detekovat škodlivý nebo zavádějící obsah dříve, než se dostane k uživatelům.

Během ukázek na konferenci RSAC 2026 označila nová bezpečnostní funkce škodlivé URL adresy v promptech chatbotů, zaznamenala tuto aktivitu na koncovém zařízení a zpřístupnila ji v platformě ESET PROTECT za účelem dalšího vyšetřování. Stejný přístup pak používá i při pokusech o tzv. prompt injection (vkládání škodlivých instrukcí do promptů), na skripty a zadávání citlivých dat, což organizacím umožňuje blokovat nebo monitorovat aktivitu v souladu s jejich pravidly. Bezpečnostní týmy získají díky logování v platformě ESET PROTECT přehled o tom, jak jsou AI nástroje v organizaci využívány, což jim pomůže efektivněji vyšetřovat rizika a prosazovat bezpečnostní politiky.

S tím, jak organizace rozšiřují využívání nástrojů agentické AI, se plocha útoku rozšiřuje nad rámec interakcí s chatboty a zahrnuje i nově vznikající rizika v dodavatelském řetězci umělé inteligence. Patří mezi ně kompromitované aplikační rámce a nástroje (AI frameworky), například trojanizované komponenty v široce používaných knihovnách, jako je LiteLLM. Dále mohou být rizikem autonomní agenti jako OpenClaw, kteří jsou schopni provádět akce v systému jen s omezeným dohledem. ESET již své zákazníky chrání před útoky v dodavatelském řetězci prostřednictvím kompromitovaných knihoven distribuovaných přes standardní repozitáře. V současnosti však zaznamenává nárůst těchto typů útoků, což společnost ESET utvrzuje v odhodlání věnovat se dalšímu výzkumu a vývoji v oblasti AI nástrojů.

V rámci svých širších inovací v oblasti zabezpečení AI představuje společnost ESET také bezplatný nástroj ESET AI Skills Checker. Tento veřejně dostupný skener i pro uživatele mimo ekosystém ESET využívá stejnou technologii jako řešení zabezpečení koncových zařízení a ESET LiveGuard. Analyzuje skilly (dovednosti) umělé inteligence na přítomnost škodlivého kódu nebo na možnost skrytých instrukcí či rizikového chování, a to pomocí vícevrstvé kontroly a cloudového sandboxingu.

Již více než 30 let je ESET průkopníkem v poskytování vysoce výkonného a snadno ovladatelného zabezpečení koncových zařízení, které je poháněno strojovým učením a umělou inteligencí. Nové funkce rozšiřují tento základ a pomáhají organizacím bránit se v dnešním rychle se měnícím prostředí kybernetických hrozeb, kde kyberzločinci stále častěji využívají AI k rozšiřování útoků, cílení na zaměstnance a automatizaci sofistikovaného sociálního inženýrství.

Jako jediný specializovaný člen Agentic AI Foundation (AAIF) z oblasti kybernetické bezpečnosti pracuje ESET také na zabezpečení nově vznikajících komunikačních protokolů AI agentů prostřednictvím spolupráce s lídry v oboru, jako jsou OpenAI, Amazon, Microsoft a Anthropic. Společně tato skupina usiluje o vytvoření důvěryhodných standardů, bezpečných návrhů protokolů a osvědčených postupů pro součinnost AI agentů.

Společnost ESET®, která byla založena v Evropě, je předním dodavatelem řešení kybernetické bezpečnosti s pobočkami po celém světě. Poskytuje špičková řešení kybernetické bezpečnosti, která pomáhají předcházet útokům ještě před jejich vznikem. ESET kombinuje technologie umělé inteligence (AI) a lidskou odbornost, čímž pomáhá předejít nově vznikajícím globálním kybernetickým hrozbám, ať již známým či dosud neznámým. Poskytuje zabezpečení pro firmy, kritickou infrastrukturu a jednotlivce. Ať už jde o ochranu koncových zařízení, cloudu nebo mobilních zařízení, řešení a služby společnosti ESET, které využívají technologie umělé inteligence a kladou důraz na cloudové prostředí, zůstávají vysoce efektivní s minimálními nároky na uživatele.

Technologie ESET jsou vyvíjeny v EU a zahrnují robustní systém detekce a reakce, ultra-bezpečné šifrování a multifaktorovou autentizaci. S nepřetržitou obranou v reálném čase a silnou místní podporou udržuje ESET uživatele v bezpečí a firmy v chodu bez narušení jejich provozu. Neustále se vyvíjející digitální prostředí vyžaduje progresivní přístup k bezpečnosti. Jen v České republice nalezneme tři výzkumná a vývojová centra společnosti, a to v Praze, Jablonci nad Nisou a Brně. Výzkumné pobočky po celém světě podporují aktivity společnosti v rámci Threat Intelligence, stejně jako její silná globální síť partnerů.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost naleznete například v online magazínu Dvojklik.cz nebo v online magazínu o IT bezpečnosti pro firmy Digital Security Guide. Nejčastějším rizikům pro děti na internetu se věnuje iniciativa Safer Kids Online, která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET, v podcastu RESET a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

Lucie Mudráková
Specialistka PR a komunikace
ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.com

Vítězslav Pelc
Senior manažer PR a komunikace
ESET software spol. s r.o.
tel: +420 720 829 561
vitezslav.pelc@eset.com

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-predstavuje-nove-funkce-pro-zabezpeceni-komunikace-s-chatboty-a-ai-agenty