Předpověď kybernetických hrozeb pro rok 2026: Boj o drony, nebezpeční AI agenti i nové geopolitické aliance

18.12.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Experti společnosti ESET zveřejnili predikci kybernetických hrozeb pro rok 2026. Nadcházející rok bude definován snahou mocností o krádeže technologií pro výrobu dronů, masivním nasazením nezabezpečených AI agentů do firemních struktur a formováním nových zpravodajských aliancí na Východě. Přinášíme přehled klíčových předpovědí napříč pěti hlavními oblastmi: APT skupinami, hrozbami pro mobilní platformy, umělou inteligencí (AI), vnějšími vztahy a ransomwarem.

Rok 2026 přinese v oblasti pokročilých trvalých hrozeb (APT) významný posun v cílech útočníků. „V roce 2026 přitáhne rozmach bezpilotních letounů (UAV) ve vojenské i komerční sféře pozornost hlavních aktérů hrozeb takzvané ‚Velké čtyřky' – Číny, Ruska, Íránu a Severní Koreje. Tyto státy se budou snažit ukrást duševní vlastnictví a shromažďovat vojensko-zpravodajské informace s cílem urychlit modernizaci svých arzenálů," vysvětluje Robert Šuman, vedoucí pražské výzkumné pobočky ESET.

Geopolitická situace povede i k novým taktikám jednotlivých států. „Rusko se nově zaměří na Evropu, konkrétně na země jako Německo, Francie a Polsko, které zahajují programy přezbrojení. Zároveň očekáváme, že běloruské APT skupiny, které se stávají agresivnějšími, by mohly s Ruskem vytvořit integrovanou zpravodajskou alianci ‚2 Eyes'," varuje Šuman.

„Čína mezitím prohloubí své angažmá v Latinské Americe v reakci na přítomnost USA a doma zpřísní dohled nad zahraničními návštěvníky. Severní Korea a Írán budou muset reagovat na mezinárodní tlak – zatímco Pchjongjang se pravděpodobně zaměří na ransomware jako nový zdroj příjmů, Írán bude hledat nové cesty v regionech, kde byli jeho tradiční spojenci oslabeni," doplňuje Šuman.

Oblast AI (umělé inteligence) projde v nadcházejícím roce 2026 dramatickým vývojem, který přinese nová rizika pro firmy i jednotlivce.

„Očekáváme, že AI agenti budou hluboce integrováni do podnikové infrastruktury, avšak jejich zabezpečení bude alarmujícím způsobem slabé. Situaci lze popsat metaforou továrny plné nově najatých dělníků, kde chybí manažeři, kteří by kontrolovali nejen kvalitu jejich práce, ale i to, aby nejednali škodlivě. To dramaticky rozšíří útočnou plochu, jelikož i základní chyby v konfiguraci mohou způsobit vážné úniky dat," říká Juraj Jánošík, vedoucí AI oddělení ve společnosti ESET.

Rizika se skrývají i v samotných modelech a jejich možném zneužití. „Ekosystém veřejně dostupných AI modelů bude zažívat další boom, ale mnohé budou distribuovány s neznámou vnitřní logikou, což zvyšuje riziko útoků přes dodavatelský řetězec. V oblasti sociálního inženýrství pak uvidíme nárůst vysoce kvalitních deepfakes a AI generovaných podvodů, které umožní i méně zdatným útočníkům provádět masivní kampaně. Velkou výzvou budou také pokročilí online boti, schopní ovlivňovat veřejné mínění, volby či automatizované náborové procesy," vypočítává Jánošík.

Uživatelé mobilních zařízení se musí připravit na sofistikovanější útoky.

„Očekáváme rostoucí počet rodin malwaru zejména pro mobilní platformu Android, které budou

využívat nástroje generativní AI. Existují již indikátory, že velké jazykové modely pomáhají generovat škodlivý kód, což snižuje vstupní bariéru pro kyberzločince bez technických znalostí," upozorňuje Lukáš Štefanko, bezpečnostní expert ve společnosti ESET, který analyzuje malware pro platformu Android.

„Kromě toho očekáváme nárůst podvodů založených na technologii NFC, které mohou využívat malware jako NGate. Tyto útoky budou podpořeny personalizovaným sociálním inženýrstvím, což ztíží jejich detekci. Organizace i uživatelé by se měli připravit na širší škálu scénářů útoků v ekosystému Android," dodává Štefanko.

Pro vlády a veřejný sektor bude rok 2026 znamenat nutnost posílení mezinárodní spolupráce.

„Aktivita státních aktérů i kyberzločineckých skupin zůstane nadále vysoká. V Evropě bude dominovat ruská kybernetická aktivita, která pravděpodobně nepoleví ani v případě příměří na Ukrajině. Státy budou čelit také kybernetickým žoldákům a komerčním firmám nabízejícím své služby k provedení útoků," komentuje Andy Garth, ředitel pro vládní záležitosti v ESETu.

„V reakci na tyto hrozby, včetně útoků na dodavatelské řetězce a kritickou infrastrukturu, očekáváme prohloubení spolupráce mezi NATO a EU v oblasti kybernetické obrany. Důraz bude kladen na digitální odolnost, technologickou suverenitu a legislativní rámce, které umožní efektivnější boj proti kyberkriminálním skupinám," uzavírá Garth.

V oblasti ransomwaru a krádeží dat se očekává pokračující nárůst počtu útoků a vývoj nástrojů.

„Ačkoli statistiky útoků rostou, důležitější je sledovat nové hráče, jako je gang Warlock, který přináší nebezpečné techniky obcházení detekce. Zatímco mediální pozornost přitahují útoky typu Zero day, většina incidentů bude v roce 2026 stále spoléhat na tradiční zranitelnosti, jako jsou slabá hesla nebo neaktualizované systémy," vysvětluje Jakub Souček, vedoucí pražského výzkumného týmu ESET.

„Významným trendem, který s námi zůstane i v roce 2026, je rostoucí popularita takzvaných ‚EDR killers' – nástrojů určených k vypnutí bezpečnostních řešení pro detekci a reakci na koncových zařízení uživatelů. To potvrzuje, že kvalitní ochrana je pro útočníky překážkou, kterou se snaží aktivně eliminovat," dodává Souček.

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/predpoved-kybernetickych-hrozeb-pro-rok-2026-boj-o-drony-nebezpecni-ai-agenti-i-nove-geopoliticke-aliance