

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **125** ze dne **18.11.2025**

Vydírání a ransomware jsou příčinou více než poloviny kybernetických útoků

Podle nejnovější zprávy Microsoft Digital Defense Report, připravené ve spolupráci s ředitelem pro informační bezpečnost Igorem Tsyganskiym, byla více než polovina kybernetických útoků s jasně známým motivem vedena vydíráním nebo ransomwarem.

Hrozby ze strany státních aktérů zůstávají vážné a trvalé, ale většina okamžitých útoků, kterým dnes organizace čelí, pochází od oportunistických zločinců usilujících o zisk.

Každý den Microsoft zpracuje více než 100 bilionů signálů, zablokuje přibližně 4,5 milionu nových pokusů o nasazení malwaru, analyzuje 38 milionů detekcí rizik krádeže identity a prověří pět miliard e-mailů kvůli malwaru a phishingu. Pokroky v automatizaci a snadno dostupné nástroje umožnily kyberzločincům – i těm s omezenými technickými znalostmi – výrazně rozšířit své operace. Využití umělé inteligence tento trend dále posílilo: kyberzločinci urychlují vývoj malwaru a vytvářejí realističtější syntetický obsah, čímž zvyšují efektivitu phishingových a ransomwarových útoků. Výsledkem je, že oportunističtí útočníci dnes cílí na každého – velké i malé organizace – a kyberkriminalita se stává univerzální, neustálou hrozbou, která proniká do našich každodenních životů.

V takovém prostředí musí vedení organizací chápat kybernetickou bezpečnost jako klíčovou strategickou prioritu – nikoli jen jako problém IT – a budovat odolnost technologií i provozu od základu. V šesté výroční zprávě Microsoft Digital Defense Report, která pokrývá období od července 2024 do června 2025, se zdůrazňuje, že tradiční bezpečnostní opatření již nestačí. Firmy potřebují moderní obranu využívající AI a silnou spolupráci napříč odvětvími i vládami, aby drželi krok s hrozbami. Pro jednotlivce mohou jednoduché kroky, jako je používání silných bezpečnostních nástrojů – zejména vícefaktorové autentifikace (MFA) odolné phishingu – znamenat zásadní rozdíl, protože MFA dokáže zablokovat více než 99 % útoků na identitu. Níže najdete některé klíčové poznatky.

Kritické služby jsou hlavním cílem

Útočníci se nadále zaměřují na kritické veřejné služby – cíle, jejichž narušení může mít okamžitý a přímý dopad na životy lidí. Například nemocnice a místní samosprávy jsou terčem útoků, protože uchovávají citlivá data nebo mají omezené rozpočty na kybernetickou bezpečnost, což často vede k používání zastaralého softwaru. V uplynulém roce měly útoky na tyto sektory reálné následky: zpoždění akutní lékařské péče, narušení pohotovostních služeb, zrušení školní výuky či zastavení dopravních systémů.

Ransomware útočníci se na tyto sektory zaměřují obzvláště, protože oběti mají omezené možnosti. Například nemocnice musí rychle obnovit zašifrované systémy – jinak mohou zemřít pacienti – což často vede k jediné možnosti, a to je zaplatit. Navíc vlády, nemocnice a výzkumné instituce uchovávají citlivá data, která mohou být odcizena a prodána na nelegálních trzích, které jsou součástí dark webu, čímž se podporuje další trestná činnost. Spolupráce vlády a průmyslu je zásadní pro posílení kybernetické bezpečnosti těchto sektorů – zejména těch nejzranitelnějších – a pro ochranu komunit i zajištění kontinuity péče, vzdělávání a pohotovostních služeb.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **125** ze dne **18.11.2025**

Státní aktéři rozšiřují své operace

Ačkoli kyberzločinci představují největší hrozbu z hlediska objemu útoků, státní aktéři stále cílí na klíčová odvětví a regiony, rozšiřují svou špionážní činnost a v některých případech se zaměřují i na finanční zisk. Geopolitické cíle nadále pohánějí nárůst státem podporované kybernetické aktivity, přičemž výrazně roste zájem o komunikační sítě, výzkum a akademickou sféru.

Klíčové poznatky:

- Čína pokračuje ve svém rozsáhlém úsilí napříč odvětvími s cílem provádět špionáž a krást citlivá data. Státní subjekty stále častěji útočí na nevládní organizace (NGOs), aby rozšířily své znalosti, a využívají skryté sítě a zranitelná zařízení připojená k internetu, aby získaly přístup a vyhnuly se odhalení. Staly se také rychlejší v operativním využívání nově odhalených zranitelností.
- Írán se při rozšiřování špionážních operací zaměřuje na širší spektrum cílů než kdykoli předtím, od Blízkého východu po Severní Ameriku. Nedávno tři íránské subjekty napojené na stát zaútočily na přepravní a logistické firmy v Evropě a Perském zálivu, aby získaly trvalý přístup k citlivým obchodním údajům, což zvyšuje pravděpodobnost, že Írán se předem připravuje na to, aby mohl zasahovat do komerčních přepravních operací.
- Rusko se sice stále soustředí na válku na Ukrajině, ale rozšířilo své cíle. Microsoft například zaznamenal, že ruští státní aktéři se zaměřují na malé podniky v zemích podporujících Ukrajinu. Ve skutečnosti patří všech deset zemí nejvíce zasažených ruskými kybernetickými aktivitami mimo Ukrajinu k Severoatlantické alianci (NATO), což představuje 25% nárůst oproti loňskému roku. Ruští aktéři mohou tyto menší společnosti vnímat jako méně náročné na zdroje, které mohou následně využít k přístupu k větším organizacím. Tito aktéři také stále více využívají ekosystém kyberkriminality pro své útoky.
- Severní Korea se nadále soustředí na generování příjmů a špionáž. V trendu, který si získal značnou pozornost, se tisíce severokorejských IT pracovníků ucházely o práci v podnicích po celém světě a své platy posílaly zpět severokorejské vládě. Když byli odhaleni, někteří z těchto pracovníků se obrátili k vydírání jako k dalšímu způsobu, jak přinést režimu peníze.

Kybernetické hrozby představované národními státy se stávají rozsáhlejšími a méně předvídatelnými. Navíc posun alespoň některých aktérů z řad národních států k dalšímu využívání ekosystému kyberkriminality ještě více komplikuje určení toho, kdo je za útok zodpovědný. Organizace musí sledovat hrozby ve svém oboru a spolupracovat s ostatními firmami i vládami, aby se dokázaly bránit útokům ze strany států.

Rok 2025 přinesl eskalaci využívání AI útočníky i obránci

V uplynulém roce využívali generativní AI jak útočníci, tak obránci. Útočníci ji používají k automatizaci phishingu, škálování sociálního inženýrství, tvorbě syntetických médií, rychlejšímu hledání zranitelností a vývoji adaptivního malwaru. Státní aktéři ji začali více zapojovat i do kybernetických vlivových operací, které se za posledních šest měsíců staly sofistikovanější, rozšířenější a cílenější.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **125** ze dne **18.11.2025**

Pro obránce je AI rovněž cenným nástrojem. Microsoft ji využívá k odhalování hrozeb, uzavírání detekčních mezer, zachytávání phishingu a ochraně zranitelných uživatelů. Jak se rizika i příležitosti AI rychle vyvíjejí, organizace musí klást důraz na zabezpečení svých AI nástrojů a školení týmů. Všichni – od průmyslu po vlády – musí být proaktivní, aby drželi krok s rostoucí sofistikovaností útočníků a zajistili, že obránci zůstanou napřed.

Útočníci se nevloupávají, ale přihlašují se

Navzdory rostoucí sofistikovanosti hrozeb je jedna statistika zásadní: více než 97 % útoků na identitu jsou útoky na hesla. Jen v první polovině roku 2025 vzrostl počet útoků na identitu o 32 %. Většina škodlivých pokusů o přihlášení probíhá prostřednictvím hromadného hádání hesel, přičemž útočníci získávají přihlašovací údaje především z úniků dat.

Úniky přihlašovacích údajů však nejsou jediným místem, kde útočníci mohou tyto údaje získat. Letos byl zaznamenán nárůst využívání malwaru typu infostealer, který dokáže ve velkém sbírat přihlašovací údaje a informace o online účtech, například tokeny relací v prohlížeči. Tyto odcizené informace se pak prodávají na kyberzločineckých fórech, což umožňuje komukoli získat přístup k účtům a provádět útoky, včetně nasazení ransomwaru.

Řešení je přitom jednoduché: použití vícefaktorové autentifikace (MFA) dokáže zastavit více než 99 % těchto útoků, i když má útočník správnou kombinaci uživatelského jména a hesla. Digital Crimes Unit společnosti Microsoft letos v květnu ve spolupráci s americkým ministerstvem spravedlnosti a Europolem narušil činnost nejpopulárnějšího infostealeru – Lumma Stealer.

AV centrum ČR