

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **113** ze dne **15.7.2025**

36 tisíc skenů za sekundu – analýzy provozu dokládají, jak si kyberzločinci mapují prostor

Automatické skenování v kyberprostoru dosáhlo v roce 2024 bezprecedentní úrovně a celosvětově vzrostlo o 16,7 %, což poukazuje na sofistikovaný a masivní sběr informací o vystavené digitální infrastruktuře. Tento masivní nárůst automatizovaného průzkumu znamená, že útočníci mají téměř v reálném čase přehled o možných způsobech útoku na různorodé cíle. Jakmile je tak zveřejněna nová zranitelnost, útočníci mohou okamžitě reagovat a zasáhnout organizace, které nestihly včas aplikovat záplaty. Tradiční reaktivní přístup k bezpečnosti je tak stále méně účinný.

Z analýzy společnosti Fortinet 2025 Global Threat Landscape Report vyplývá, že každou hodinu proběhnou po celém světě miliony pokusů o skenování, což potvrzuje vytrvalou snahu kyberzločinců zmapovat odhalené systémy před zahájením útoku. Aby bylo možné efektivně chránit organizace, je třeba pochopit, co útočníci hledají a jak se jejich skenování promítá do reálných rizik.

Příkladem může být protokol SIP, který reprezentuje více než 49 % zjištěných skenů. Zranitelnosti tohoto protokolu, který se široce používá v telekomunikacích, mohou umožnit útoky na odposlech a podvody při volání. Například hackerská skupina APT28 použila legitimní pověření k získání počátečního přístupu, udržení a exfiltraci dat ze sítě oběti. Využili také výchozí hesla výrobců k získání přístupu do podnikových sítí prostřednictvím zařízení IoT, jako jsou telefony, tiskárny a dekodéry videa. Dalším příkladem je komunikační protokol Modbus TCP určený pro průmyslovou automatizaci, který v analýze představuje přibližně 1,6 % skenů. Úřady varují, že někteří aktéři pokročilých trvalých hrozeb umí získat plný systémový přístup k více zařízením ICS/SCADA.

"Neustálé změny v oblasti hrozeb jsou zde již několik desetiletí. Nejnovější vývoj však představuje zásadní posun, který je způsoben všudypřítomností umělé inteligence (AI). Útočníci v důsledku toho nejen zkoumají nové taktiky, ale také mění své obchodní modely. Díky těmto technologickým vymoženostem zrychlují své operace nebývalou rychlostí a zaměřují se na zranitelné oblasti, tráví více času plánováním a průzkumem, aby mohli provádět cílenější, účinnější a ničivější útoky," říká Ondřej Štáhlavský, regionální ředitel společnosti Fortinet pro střední a východní Evropu a dodává: "Automatizace mění chování kyberzločinců ve všech fázích řetězce útoku. Zatímco čas bývá stejný, objem prováděných skenů zranitelností prudce roste. Hackeři automatizují své skenování, aby mohli efektivně prověřit všechny přístupové body, od cloudových rozhraní API až po provozní technologie. A darknetová fóra slouží jako rychle rostoucí trh se vším – od přihlašovacích údajů až po celé balíčky útočných sad. To poskytuje začínajícím i zkušeným kyberzločincům snadný přístup ke všemu, co je potřeba k provedení úspěšného narušení."

Zdroj: AVcentrum ČR