

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **91** ze dne **26.11.2024**

Objem DDoS útoků na české firmy dlouhodobě stagnuje. Intenzitě útoků kraluje Rusko

Objem DDoS útoků mířících na tuzemské firmy i v září stagnoval a navázal tak na předchozí měsíce. Nejvíce útoků míří již více než rok bez přestávky z Ruska, které v září šestý měsíc v řadě kralovalo také z pohledu intenzity útoků.

"V září podobně jako v předešlých měsících docházelo spíše k banálním a z hlediska složitosti primitivním DDOS útokům. Sofistikovanější typy útoků se vyskytují stále méně často. Začaly se ale objevovat útoky, které sice jsou ve svém základu jednoduché, ale opakují se s pravidelnou periodicitou. Smyslem takových útoků bylo evidentně to, aby udržely danou službu nefunkční nebo hůře dostupnou v konkrétní čas během dne. I takový primitivní útok pak může být efektivní a plnit to, o co útočníkům jde," uvedl Michal Štusák, expert na kybernetickou bezpečnost a spoludávající společnosti ComSource.

Podle přehledu DDoS útoků zachycených službami FlowGuard společnosti ComSource přesáhl v září počet zemí, ze kterých na firmy a instituce v České republice útoky mířily, hodnotu 200. Nejvíce útoků bylo z Evropy, která kralovala i z pohledu intenzity. Z pohledu zemí je již dlouhodobě největší počet útoků z Ruska (bez přestávky od července loňského roku), které je již půl roku také na první příčce intenzity útoků. Celkový objem odfiltrovaného škodlivého provozu zůstal v září v porovnání s předchozím měsícem na podobné úrovni.

Stále oblíbenější útoky přímo na aplikační vrstvě umožňují útočníkům efektivně zvýšit dopad útoků a servery provozující služby jednodušeji zahltnout i menší intenzitou síťového provozu. V kombinaci se zranitelností méně obvyklých internetových protokolů a nárůstem intenzity jednotlivých útoků to ukazuje na nutnost zabezpečení nových míst firemní IT infrastruktury. Jednotlivé útoky navíc v některých případech dosahují intenzity i přes 100 Gbps, tedy i tisíckrát více, než je kapacita běžného firemního připojení. I několikaminutový útok na servery tak zajistí nedostupnost služeb či internetových stránek.

Zdroj: AVcentrum ČR