

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **88** ze dne **5.11.2024**

Byla to jen otázka času: Malware a ransomware jako služba

Modely předplatného, jako jsou Malware-as-a-Service (MaaS) a Ransomware-as-a-Service (RaaS), výrazně snížily vstupní bariéru pro méně zkušené útočníky, což usnadňuje provádění komplexních útoků. Tento vývoj je zásadní změnou v oblasti kybernetických hrozeb.

Koncept "jako služba" je běžný v IT, například Software-as-a-Service (SaaS) nebo Device-as-a-Service (DaaS), a nyní si našel místo i mezi kyberzločinci v podobě Cybercrime-as-a-Service. Zkušení útočníci nyní prodávají své služby méně zkušeným, což vede k nárůstu kyberútoků.

Darktrace ve své pololetní zprávě pro rok 2024 zdůrazňuje, že MaaS zůstane dominantním faktorem v prostředí hrozeb. Nejčastějšími hrozbami jsou malware kradoucí informace, trojské koně, trojské koně pro vzdálený přístup (Remote Access Trojans - RAT), botnety a loadery. Darktrace také varuje před nárůstem útoků s dvojitým vydíráním, kdy útočníci po úspěšném ransomwarovém útoku znovu požadují výkupné.

V přehledu hrozeb zmiňuje Darktrace také trvalou oblíbenost e-mailového phishingu, s varovným zjištěním, že 62 % phishingových e-mailů obchází ověřování DMARC (Domain-based Message Authentication Reporting and Conformance). Toto selhání v ochraně zdůrazňuje nutnost modernizace bezpečnostních opatření v e-mailové komunikaci.

Ochrana proti MaaS a RaaS s využitím moderních technologií

Vzhledem k nárůstu těchto hrozeb je nezbytné, aby firmy zaujaly proaktivní přístup ke kybernetické bezpečnosti. Dříve nákladné bezpečnostní nástroje, které byly dostupné jen velkým korporacím, jsou nyní implementovatelné i v menších firmách. Mezi tyto technologie patří:

- Next-Generation Firewall (NGFW): Poskytují pokročilou ochranu proti hrozbám díky funkcím jako inspekce DNS provozu, blokování přístupu ke škodlivým doménám a detekce pokročilých hrozeb, které mohou být součástí MaaS a RaaS útoků.
- Threat Intelligence: Integrace s platformami Threat Intelligence umožňuje NGFW identifikovat a blokovat nové hrozby v reálném čase, včetně rozpoznání phishingových útoků, které by mohly sloužit jako vstupní bod pro MaaS a RaaS útoky
- Security Operations Center (SOC): Připojení k SOC poskytuje nepřetržitý dohled nad síťovým provozem, což umožňuje rychlou detekci a reakci na hrozby. SOC dokáže identifikovat neobvyklé aktivity v síti, které by mohly indikovat pokusy o spuštění malwaru nebo ransomwaru jako služby, a rychle podniknout nezbytné kroky k minimalizaci škod.

Díky moderním bezpečnostním nástrojům, jako jsou Next-Generation Firewall a služby SOC, mohou firmy zajišťovat efektivní ochranu proti rostoucím hrozbám.

"Více než dříve je nutné, aby kybernetická bezpečnost měla ve firmách prioritu a z reaktivních aktivit se změnila na proaktivní," řekl Petr Zahálka z Thein Security. "Firmy mají dnes na výběr dostatek vhodných nástrojů, které mohou zásadně přispět k vyšší kybernetické bezpečnosti."

Zdroj: AVcentrum ČR