Meziroční nárůst bezpečnostních incidentů o 36 % i největší útok v historii – rok 2024 v kostce

20.2.2025 - | T-Mobile Czech Republic

Nárůst v počtu zachycených kybernetických hrozeb, kratší reakční doba a nové technologie – takový byl rok 2024 pro Security Operations Center (bezpečnostní dohledové centrum, tzv. SOC) společnosti T-Mobile. V roce 2024 zpracovalo více než 30 000 bezpečnostních událostí, což představuje průměrně 82 incidentů denně. Oproti roku 2023 jde o nárůst o 36 %, což potvrzuje, že kybernetické hrozby nabývají na intenzitě i sofistikovanosti. Centrum se soustředí také na přípravu na nové legislativní výzvy vyplývající z implementace směrnice NIS2. Speciální dohledové centrum se stará o kyberbezpečnost firemních zákazníků a zaměřuje se na tři klíčové oblasti – ochranu sítí a infrastruktury, ochranu koncových zařízení a uživatelů a komplexní bezpečnostní monitoring IT infrastruktury zákazníků.

Základním předpokladem úspěšného zachycení takového útoku je reakční čas, který v rámci dohledového centra operátora činil v loňském roce v průměru 14 minut. U kritických útoků typu Distributed Denial of Service (DDoS) činil dokonce jen 6,5 minuty. Firmy jsou nejčastěji cílem DDoS útoků, proti nimž dohledové centrum T-Mobilu využívá službu DDoS Protection, která filtruje škodlivý provoz a propouští pouze validní data. „Počet kybernetických hrozeb a útoků meziročně narůstá, ale díky kombinaci pokročilých nástrojů a zkušeností našeho třicetičlenného týmu jsme schopni reagovat velmi rychle a minimalizovat tak jejich dopady. Loňský rok byl ale rekordní, především co se týče objemu jednotlivých útoků," uvedl Zdeněk Grmela, ředitel pro oblast kyberbezpečnosti divize pro firemní zákazníky společnosti T-Mobile. Experti SOC zaznamenali vloni největší DDoS útok o celkovém objemu 360 Gbps, což je o 40 % více než největší obdobný útok zaznamenaný v roce 2023 (258 Gbps). Celkem bylo odfiltrováno 340 TB škodlivého datového provozu, což odpovídá téměř 38 000 filmům ve Full HD kvalitě.

„Pravidelně investujeme do technologií, proto jsme již na začátku loňského roku zvýšili naši detekční kapacitu šestinásobně a filtrační kapacitu neboli maximální objem škodlivého provozu, který jsme schopni odfiltrovat, trojnásobně," doplňuje Grmela . Nejčastějším terčem vedle přímých útoků na infrastrukturu operátora byly v loňském roce státní a finanční instituce. Rostoucí využívání umělé inteligence (AI) útočníky při phishingových kampaních nebo vytváření malwaru na míru staví firmy před nové výzvy.Prostřednictvím ochrany koncových zařízení a uživatelů (XDR) chrání dohledové centrum desítky tisíc zařízení a uživatelů. Téměř 50 % detekcí využívá pokročilé technologie strojového učení a umělé inteligence, nikoli jen tradiční vzorce útoků. Přibližně 40 % útoků je pak blokováno automaticky, zatímco složitější případy řeší analytici SOC v režimu 24/7. Rostoucí počet kybernetických incidentů mimo jiné ukazuje, jak zásadní je investice do moderních technologií a spolupráce mezi soukromým a státním sektorem. IT infrastrukturu zákazníků dohlíží SOC prostřednictvím nástroje bezpečnostního monitoringu (SIEM). Ten umožňuje automatickou detekci podezřelých událostí pomocí analýzy dat z IT infrastruktury zákazníků, a dokonce i z průmyslových systémů. Průměrná doba analýzy a nahlášení incidentu zákazníkovi byla pouhých 25 minut od detekce. SIEM také pomáhá firmám splnit legislativní požadavky, jako je zákon o kybernetické bezpečnosti nebo směrnice NIS EU.

Implementace směrnice NIS2 do české legislativy proběhne letos právě prostřednictvím nového zákona o kybernetické bezpečnosti. Ten rozšiřuje regulace na více než 6 000 subjektů a zavádí

přísnější pravidla pro zabezpečení dodavatelských řetězců, hlášení incidentů a odpovědnost vedení firem. SOC T-Mobilu již nyní splňuje klíčové požadavky nové legislativy, jako je rychlé hlášení incidentů nebo implementace pokročilých technologií pro detekci hrozeb. S lužby jako SIEM, XDR a DDoS Protection jsou navrženy tak, aby zákazníkům pomohly nejen splnit legislativní povinnosti, ale především zajistily jejich bezpečnost v reálném čase . T-Mobile je největší operátor v ČR, který poskytuje mobilní služby již 6,5 milionům zákazníků. Neustále inovuje a rozšiřuje mobilní infrastrukturu a jako digitální leader T-Mobile zásadně přispívá digitalizaci Česka budováním a rozvojem optické infrastruktury s cílem naplnit svou dlouhodobou vizi o Propojené zemi.

Na průmyslovém využití 5G sítí T-Mobile spolupracuje s předními českými a moravskými technickými univerzitami, na nichž buduje privátní kampusové sítě. Společné projekty v podobě inovačních hubů a testbedů pak cíleně podporují digitalizaci firem, startupy a rozvoj inovačního prostředí v ČR. T-Mobile je stabilním a silným partnerem malých i velkých firem, kterým nabízí nejmodernější datacentra a pokročilá řešení pro bezpečnou a spolehlivou správu dat. Služby v oblasti kybernetické bezpečnosti či cloudová a systémová řešení využívají nejen korporace a státní správa, ale také drobní živnostníci. Jednou ze strategických priorit společnosti je ohleduplné a udržitelné podnikání. V rámci ESG agendy se T-Mobile dlouhodobě zaměřuje na opatření vedoucí ke zmírnění klimatických změn a zvyšování digitální gramotnosti české populace. Operátor cíleně podporuje neziskové organizace a znevýhodněné skupiny a pomáhá při mimořádných událostech.

Více informací o společnosti najdete na www.t-mobile.cz .

Kontakt na tiskové oddělení : press@t-press.cz