T Business Security Report

Report shrnuje důležité události v kybernetické bezpečnosti a statistiky týkající se kybernetických útoků zachycených bezpečnostním týmem expertů T-Mobile (CSIRT) za 3. čtvrtletí 2023. Aktuální vydání je zaměřeno na ochranu koncových zařízení (Endpoint Detection and Response).

AKTUÁLNÍ TRENDY

Ochrana koncových zařízení (EDR)

Endpoint Detection and Response (EDR) je technologie sloužící k ochraně koncových zařízení (pracovní stanice, servery nebo i mobilní zařízení) před kybernetickými hrozbami, jako jsou ransomware či malware obecně. EDR komplexně prověřuje veškeré dění na koncovém zařízení, kde je nainstalován, a nad rámec běžných antivirových detekcí provádí mimo jiné také behaviorální analýzu. Detekuje tak nejen již známé a popsané hrozby, ale také pozná obecné modely kybernetických útoků a podezřelého chování, čímž dokáže ochránit i před dosud neznámými útoky. Na tyto události pak může reagovat automatickou ochranou, ale poskytuje i mnoho nástrojů pro vyšetřování a možný manuální zásah ze strany pracovníků kybernetické bezpečnosti. EDR také zvyšuje viditelnost útoků a celkový přehled o chráněném prostředí. V dnešním bezpečnostním prostředí je nepostradatelným prvkem ochrany.

Reprezentativní příklady hrozeb, se kterými jsme se v praxi setkali, uvádíme níže.

Lumma Information Stealer

Information Stealer je specifická skupina malwaru, která se zaměřuje na exfiltraci citlivých dat – typicky se jedná o hesla, osobní a platební údaje a v posledních letech i přístupové údaje ke kryptopeněženkám. Jedním z novějších zástupců této skupiny je i malware Lumma. Tento Information Stealer je běžně prodáván na různých darknet fórech (tzv. Malware-as-a-Service) a zaměřuje se především na informace uložené v internetovém prohlížeči. Díky své nízké ceně (250$) a snadnému použití je velice populární. Je proto dostupný i pro méně pokročilé aktéry, kteří nemají rozsáhlé finanční zdroje nebo dovednost vyvíjet vlastní malware. S tímto typem malwaru jsme se již setkali u řady zákazníků, obvykle se maskuje za legitimní software, aby byl uživatel zmanipulován k jeho stažení a spuštění.
Námi podporované EDR řešení CrowdStrike Falcon jej běžně identifikuje již při pokusu o spuštění. EDR zablokuje proces již při jeho spuštění, díky čemuž se zabrání úniku potenciálně citlivých dat. Tímto se snadno předejde vzniku většího bezpečnostního incidentu, vyvolanému únikem exfiltrovaných citlivých informací.

Quasar RAT

Quasar Remote Access Trojan (RAT) je open source malware běžně využívaný řadou Advanced Persistent Threat (APT) skupin při různých kybernetických útocích. Dle některých výzkumů se jedná o jeden z vůbec nejpoužívanějších typů malwaru. Může být použit k zajištění persistence (tj. techniky pro zachování přístupu útočníka) na kompromitovaném systému, pro zvýšení uživatelských a přístupových práv, ale i pro další úkony. Jedna z našich posledních zkušeností s tímto malwarem je z prostředí zákazníka, kde bylo naše EDR nasazeno po rozsáhlém ransomware incidentu. Předchozí standardní antivirové řešení tento aktivní malware nedetekovalo, teprve nasazení EDR technologie jej okamžitě po instalaci zachytilo a eliminovalo.

NUKIB

Národní úřad pro kybernetickou bezpečnost (NÚKIB) varuje před hrozbou ransomwarových útoků skupiny LockBit. Ransomwarový gang LockBit je aktuálně jedním z nejaktivnějších kyberkriminálních aktérů na světě. Svou aktivitu postavil na bázi modelu ransomware jako služba (tzv. Ransomware-as-a-service, RaaS), v rámci, kterého poskytuje ransomware svým společníkům (tzv. affiliates) za podíl na zisku z výkupného. Ransomware LockBit byl v různých variantách již několikrát potvrzen v rámci incidentů evidovaných NÚKIB. Je tedy velmi pravděpodobné, že se novým cílem této skupiny mohou stát i další české subjekty.

Také T-Mobile Incident Response Team má s tímto malwarem bohaté zkušenosti získané z účasti na řadě zásahů při řešení závažných incidentů. Ve všech případech byl po instalaci EDR platformy schopen malware rozpoznat, což je vždy prvním nutným krokem pro úspěšná řešení incidentu.

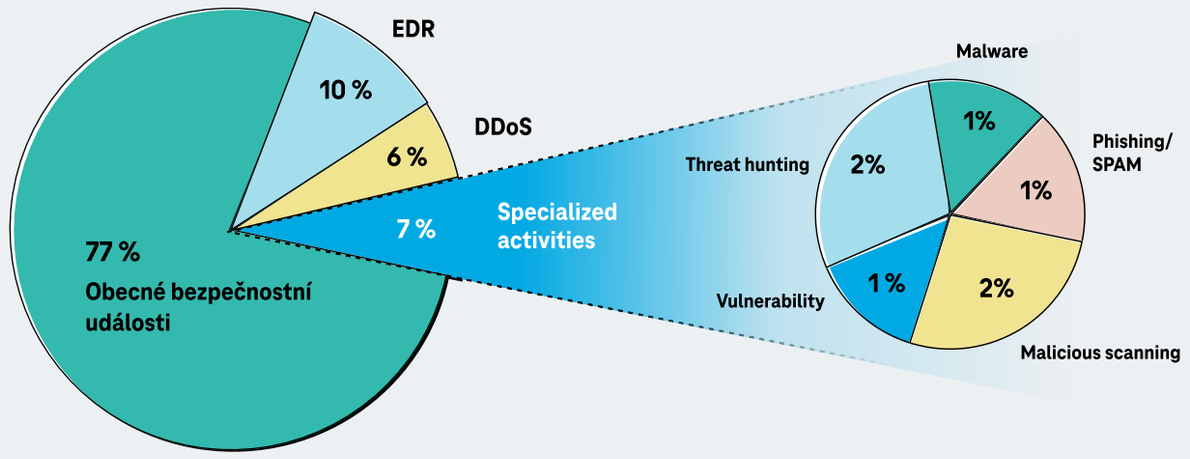
Pravidelný report

Tým bezpečnostních expertů T-Mobile (Computer Security Incident Response Team, CSIRT) se ve 3. čtvrtletí zabýval různými druhy bezpečnostních incidentů a aktivit.

Co řešil CSIRT T-Mobile v Q3/2023

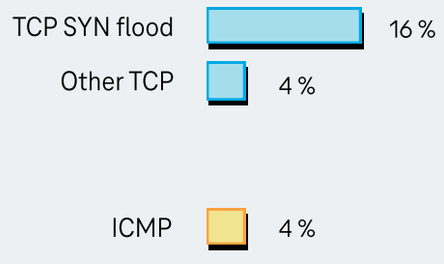
Na **CSIRT** bylo postoupeno přes 5200 bezpečnostních událostí

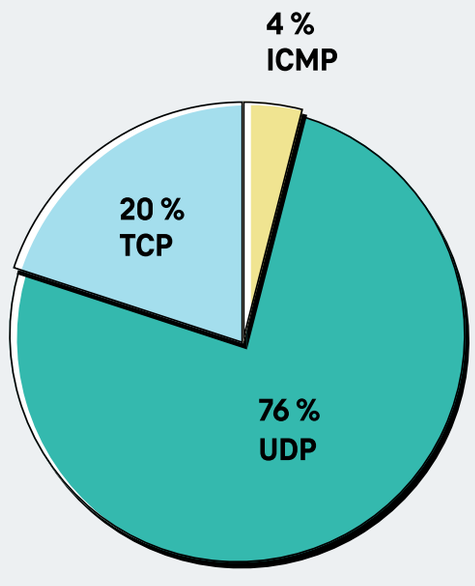
Náš 24x7 SOC zpracoval přes 42 900 bezpečnostních událostí



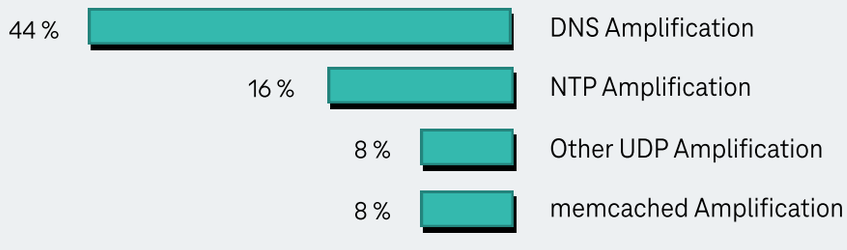
DDOS — TYPY DETEKOVANÝCH ÚTOKŮ

TCP SYN flood je typ DDoS útoku, který na koncové zařízení odešle množství požadavků na navázání spojení. Server se jimi zahltí, což způsobí jeho nedostupnost.

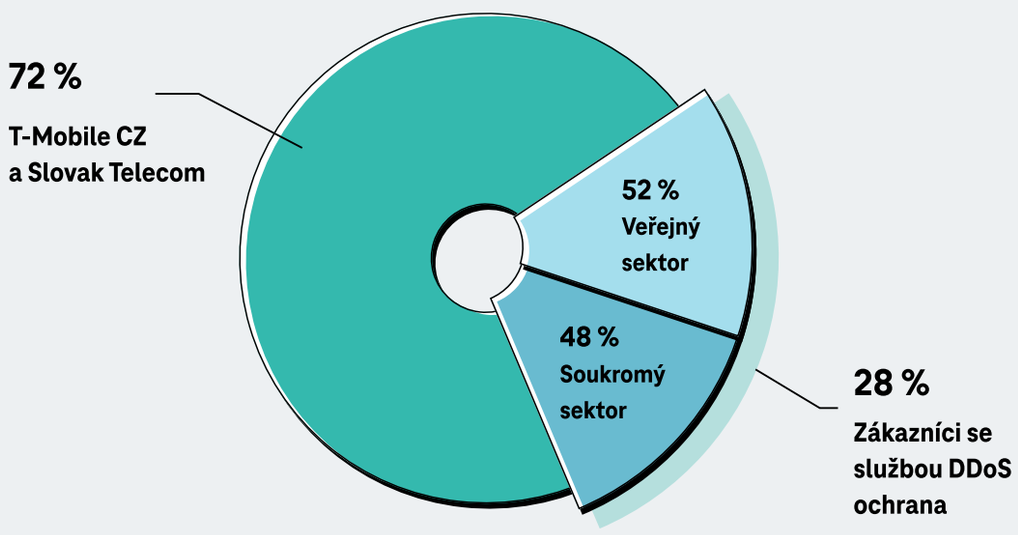




Útok typu UDP flood zahlcuje cíl velkým množstvím UDP paketů, na něž cílové zařízení odpovídá. Vedle přetížení infrastruktury dochází také často k podvržení adresy odesilatele (spoofingu) a následnému zesílení útoku (amplifikaci) na další oběť.



DDOS — CÍLE ÚTOKŮ

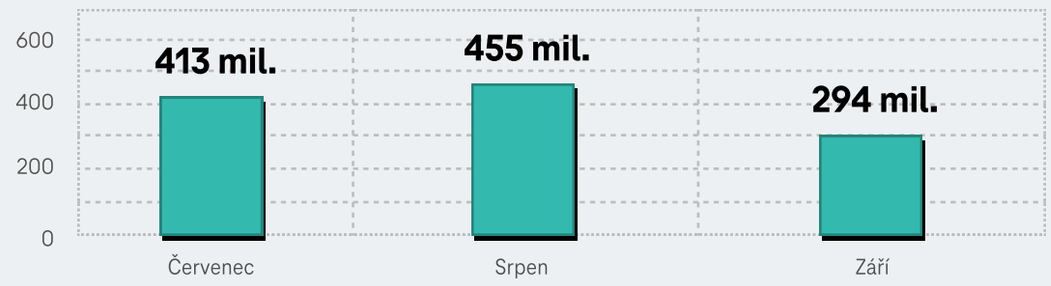


Všichni zákazníci s aktivní službou DDoS ochrana od T-Mobile, kteří se stali terčem DDoS útoku, nezaznamenali díky aktivní ochraně narušení provozu.

NEJVĚTŠÍ ÚTOK NA ZÁKAZNÍKA SE SLUŽBOU DDOS OCHRANA

Nejsilnější volumetrický **útok** v průběhu 3. čtvrtletí 2023 byl v srpnu a měl sílu 107,2Gbps. Cílem útoku byly slovenské vládní instituce.

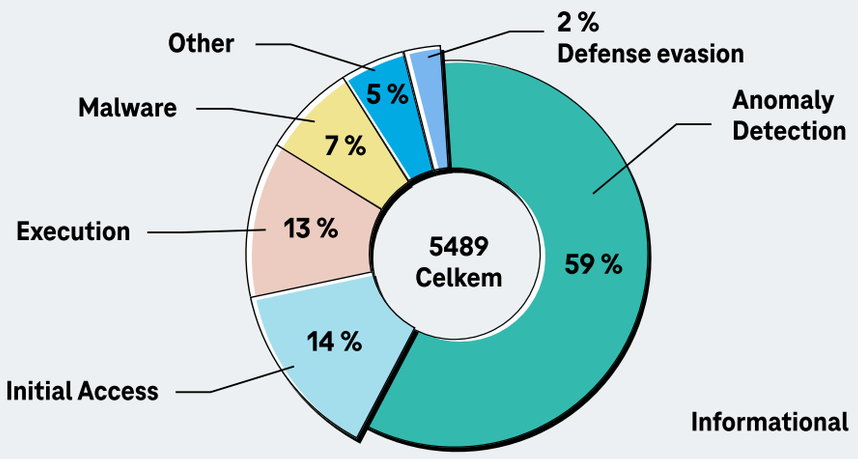
ÚTOKY NA WEBOVÉ APLIKACE



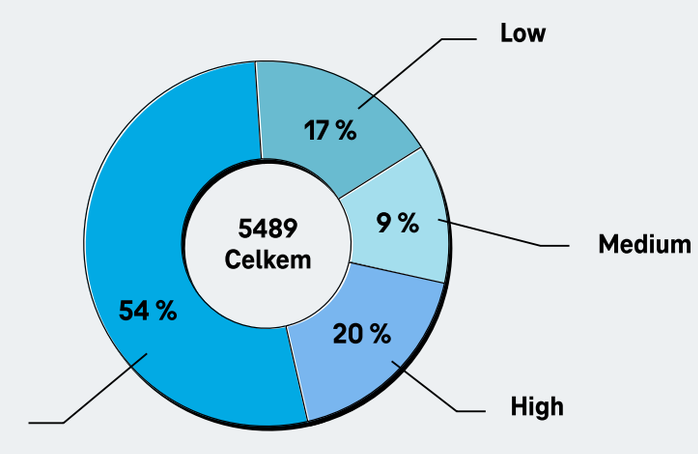
Údaje zahrnují více než 60 webových portálů, které chrání T-Mobile CZ WAF. Jedná se o jednu z největších WAF implementací v Evropě.

EDR — OCHRANA KONCOVÝCH ZAŘÍZENÍ

Aktuálně monitorujeme přes 19 600 koncových stanic jak v našem interním prostředí (T-Mobile CZ a Slovak Telekom), tak i u našich zákazníků.
EDR nástroje dokážou na koncových zařízeních zachytit a zablokovat mj. bezpečnostní události:



Zachycené typy EDR incidentů



EDR incidenty **podle závažnosti**

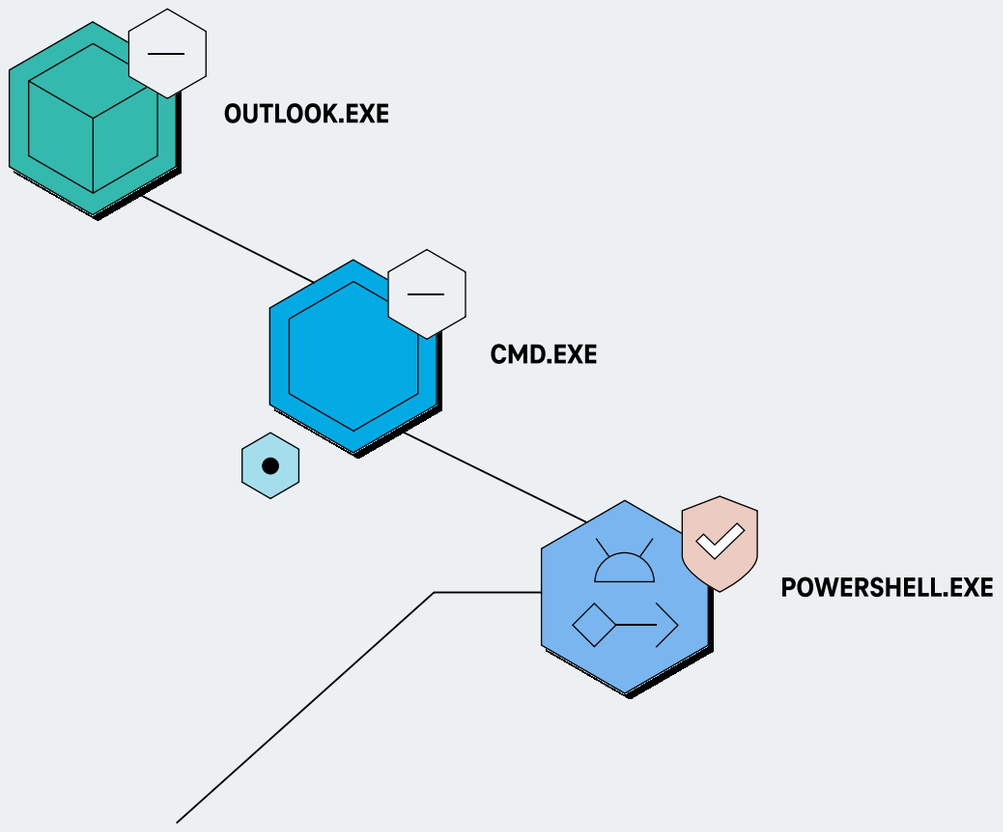
Téma čtvrtletí — Ochrana koncových zařízení (EDR)

Ochrana koncových zařízení (jako jsou počítače a servery) před kybernetickými útoky je jedním ze základních prvků pro zajištění bezpečnosti každé organizace, jejich dat. Zvyšuje schopnost organizace pokračovat ve svých klíčových obchodních aktivitách i po výskytu malware v jejím prostředí. Základní ochrana běžnými antiviry má dnes již omezenou účinnost, která nadále klesá. Antiviry jsou proto postupně nahrazovány systémy typu EDR. Ty však jsou mimo vyšší ochrany také většinou nákladnější a zejména náročnější na konfiguraci a obsluhu. K tomu potřebné specifické znalosti nezřídka překračují rámec běžných kompetencí správců IT, a požadavky na kontinuální dohled téměř vždy převyšují reálné kapacitní možnosti organizace. T-Mobile proto představil rodinu služeb pro ochranu koncových stanic – Magenta EDR a Magenta Security Shield. Tyto služby garantující pokrytí všech základních potřeb v oblasti EDR, jsou cenově dostupné a zároveň obsahují i celou řadu doplňujících modulů či služeb (např. dohled SOC v režimu 24x7, odborné poradenství, Device Control, Threat Intel atd.)

Služba **Magenta EDR** je určena pro menší organizace, které si chtějí řešit správu IT a její bezpečnost buď vlastními silami nebo se svým lokálním partnerem. Služba obsahuje balík profesionální péče včetně licence EDR technologie CrowdStrike Falcon. V průběhu úvodního workshopu provedeme prvotní konfiguraci ochrany prostředí dle potřeb zákazníka a zaškolíme jej. Následně jsme po dobu kontraktu zákazníkovu k dispozici, kdykoliv potřebuje odbornou pomoci. Zákazník tak za cenu na úrovni licence běžného antiviru získá podstatně účinnější špičkové EDR řešení, nemění správu svého prostředí, ale současně má v případě nutnosti k dispozici kapacitu a kompetence specializovaného partnera.

Modelová situace, kterou řešilo naše dohledové centrum:
Zákazníkovi jsme asistovali v nočních hodinách s incidentem vyvolaným spearphishing mailem zaslaným jednomu ze zaměstnanců. E-mail v příloze obsahoval infikovaný excel soubor, který po otevření spustil škodlivý powershell skript (downloader), který se pokusil o stažení malwaru z internetu. CrowdStrike Falcon toto detekoval a powershell proces zablokoval. Infikovaný excel soubor byl následně extrahován a prozkoumán našimi SOC analytiky – malware analýza a spuštění v kontrolovaném sandbox prostředí umožnila plné zmapování útoku. Zákazníkovi jsme následně asistovali s celkovým odstraněním infekce z jeho prostředí.

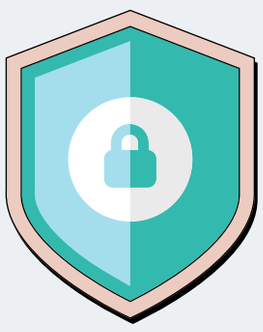
I přes dlouhodobé nasazení tradičních antivirových řešení v monitorovaných prostředích stále zaznamenáváme značné množství tzv. PUA/PUP (Potentially Unwanted Application/Potentially Unwanted Program). Tato kategorie detekcí je často podceňována, přestože může otevírat dveře dalším bezpečnostním hrozbám. Nejen že PUA/PUP shromažďují citlivé informace, ale zachytáváme i případy, kdy PUA/PUP slouží přímo k šíření malware.



ACTION TAKEN	Process blocked
SEVERITY	High
OBJECTIVE	Gain Access
TACTIC & TECHNIQUE	Initial Access via Spearphishing Attachment
TECHNIQUE ID	T1566.001

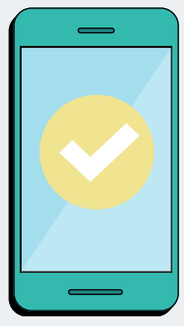
Zvýšení bezpečnosti pomocí Threat Intelligence.
Ke službě EDR nabízíme doplňkový modul, který zpřístupňuje aktuální klíčové informace o činnosti organizovaných hackerských skupin a dalších útočníků. Na základě charakteristik chráněné organizace lze vybrat právě ty skupiny, které pro organizaci představují skutečnou hrozbu. S podrobnými informacemi o útočnících – jejich motivací, využívaných taktikách, technikách, nástrojích a zranitelnostech je následně pro organizaci snazší přijmout odpovídající kroky ke zvýšení své bezpečnosti.

Služba **Magenta Security Shield** je určena pro střední a větší organizace, které chtějí přenechat péči o bezpečnost koncových stanic specializovanému partnerovi. Služba zahrnuje podobně jako u služby Magenta EDR licence technologie Crowdstrike Falcon a její nasazení. Rozdílem je, že celý následný provoz technologie, a to včetně analýzy veškerých detekcí podezřelého chování i případné reakce na incident zajišťuje naše Security Operations Center. Zákazník má detailní vhled do bezpečností situace prostřednictvím zákaznického portálu, reportů a pravidelných schůzek se dedikovanými experty SOC.



KYBERNETICKÁ BEZPEČNOST

Už od roku 2011 jsme expertem na kybernetickou bezpečnost s celosvětovou působností. Poskytujeme širokou škálu služeb od prevence přes detekci až po reakci na bezpečnostní incidenty. Provozujeme **vlastní dohledové centrum (SOC)** s 24/7 provozem a naši specialisté jsou držiteli **mezinárodně uznávaných certifikací.**



HLÁŠENÍ PODEZŘELÉ ZPRÁVY NA MOBILNÍM ZAŘÍZENÍ

Pro hlášení podezřelých textových zpráv funguje pro naše zákazníky telefonní číslo **7726**.
Náš bezpečnostní tým podezřelé zprávy zanalyzuje a následně odkaz zablokuje.