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 poslední čtvrtletí 2023. Aktuální vydání je zaměřené na Směrnici EU známou pod názvem NIS2 a její transpozici do české legislativy.

AKTUÁLNÍ TRENDY

Trendy v kybernetické bezpečnosti

Směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, která se postupně dostává do našeho povědomí pod zkratkou NIS 2, rezonuje v poslední době nejen v bezpečnostní komunitě. Směrnice NIS 2 musí být letos transponována do české legislativy, a proto byl na konci loňského roku předán návrh nového Zákona o kybernetické bezpečnosti k připomínkám Legislativní radě vlády.

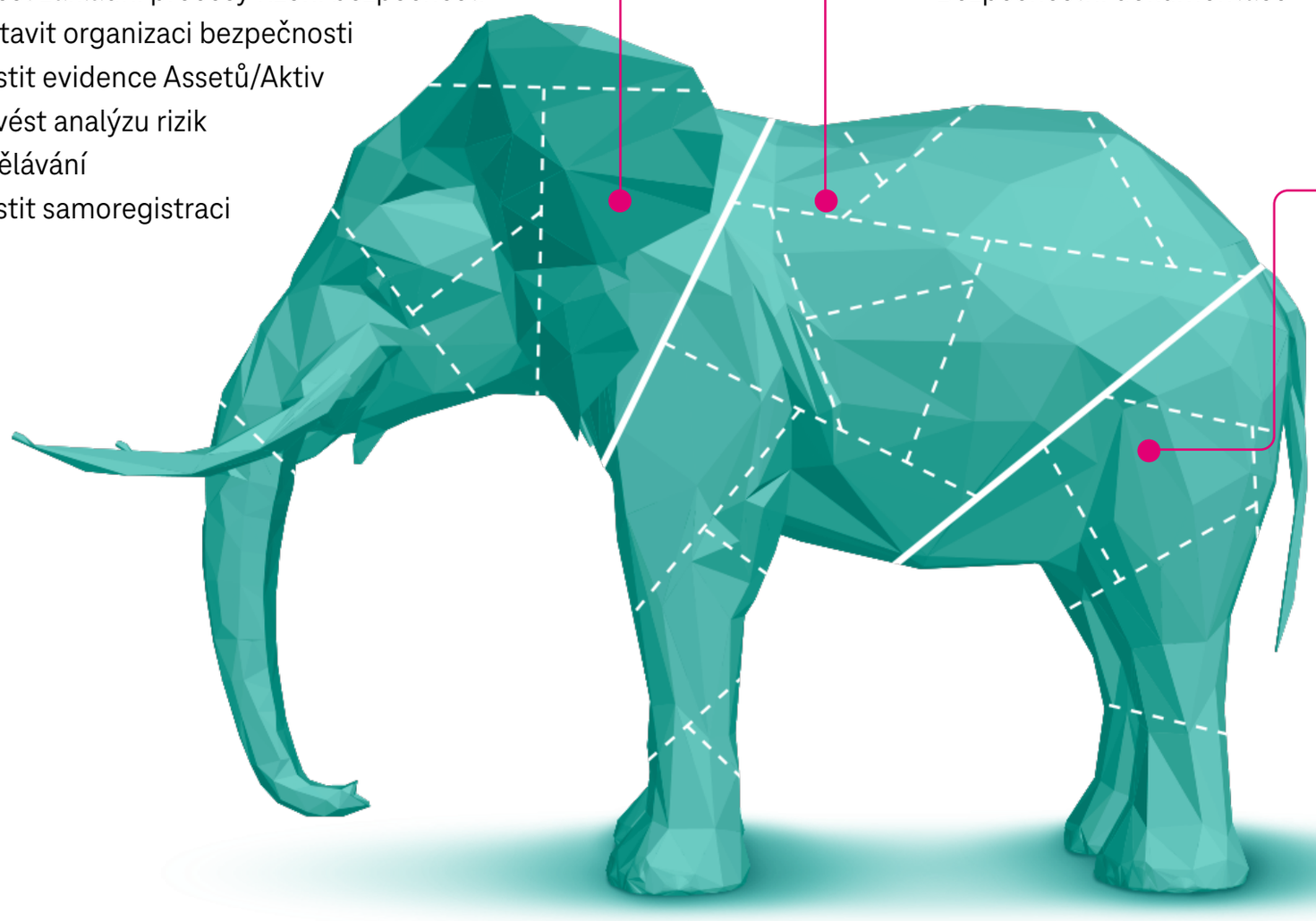
I když ještě neznáme přesné požadavky Zákona, můžeme jednotlivé oblasti rozdělit do tří skupin: strategické a plánovací činnosti, které jsou spojené s prvotním nastavením systému řízení bezpečnosti informací, provozně-technické činnosti, kdy jsou implementovány přiměřené nástroje k naplnění cílů strategie informační bezpečnosti a provozně-správní činnosti, kam řadíme operativní činnosti, které musí být průběžně zajištěny.

STRATEGICKÉ A PLÁNOVACÍ ČINNOSTI

- Zjistit aplikovatelnost ZoKB pro organizaci
- Provést rozdílovou analýzu
- Definovat plán zavedení požadavků a opatření
- Definovat strategii informační bezpečnosti
- Definovat Bezpečnostní politiku
- Zavést základní procesy řízení bezpečnosti
- Nastavit organizaci bezpečnosti
- Zajistit evidence Assetů/Aktiv
- Provést analýzu rizik
- Vzdělávání
- Zajistit samoregistraci

PROVOZNĚ-TECHNICKÉ ČINNOSTI

- Řízení a ochrana identit
- Řízení a ochrana přístupu k síti
- Ochrana koncových bodů
- Detekce incidentů
- Bezpečnostní dohled
- Bezpečnostní dokumentace



PROVOZNĚ-SPRÁVNÍ ČINNOSTI

- Řízení incidentů
- Hlášení incidentů
- Průběžné řízení rizik a Risk registr
- Business continuity plán
- Business recovery plán
- Dodavatelský řetězec
- Správa třetích stran
- Komunikace s NÚKIB
- Neustálé zlepšování

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost – NÚKIB odeslal návrh nového zákona o kybernetické bezpečnosti Legislativní radě vlády (gov.cz)

Návrh Zákona o kybernetické bezpečnosti
ODok Portál – VeKLEP – Návrh zákona o kybernetické bezpečnosti

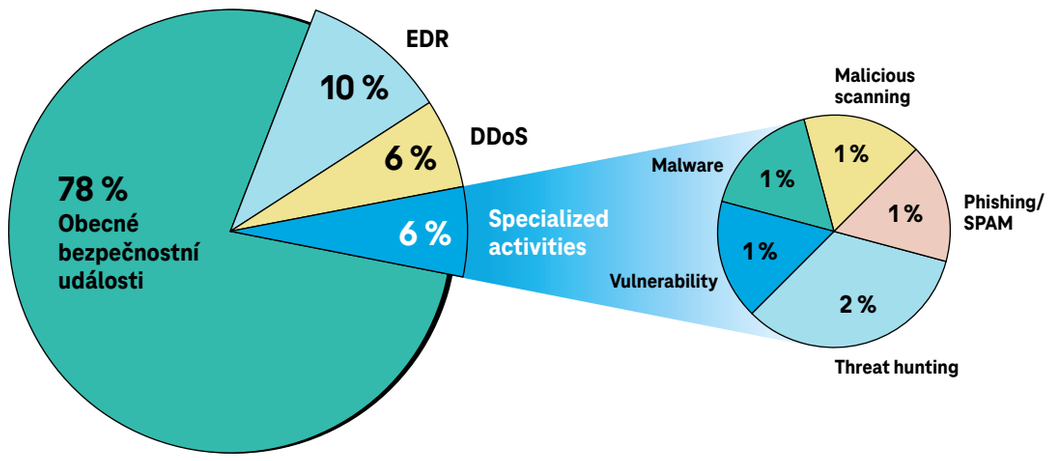
Pravidelný report

Tým bezpečnostních expertů T-Mobile (Computer Security Incident Response Team, CSIRT) se ve 4. čtvrtletí zabýval různými druhy bezpečnostních incidentů a aktivit.

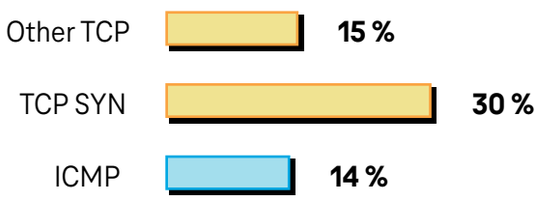
CO ŘEŠIL CSIRT T-MOBILE V Q4/2023

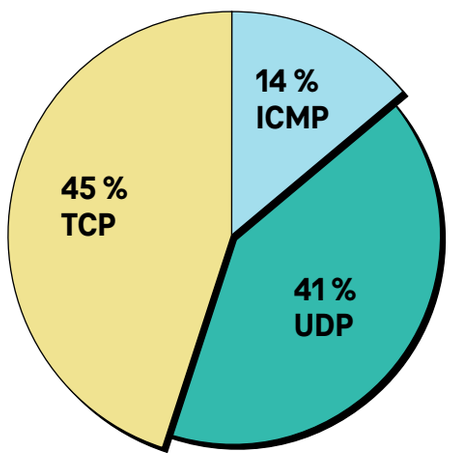
Na **CSIRT** bylo postoupeno přes 11 500 bezpečnostních událostí

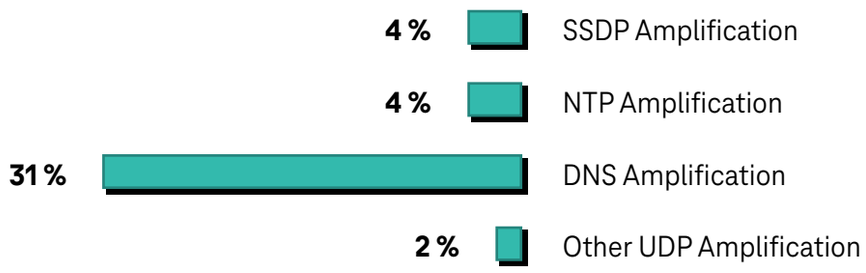
Náš 24x7 SOC zpracoval přes 27 300 bezpečnostních událostí



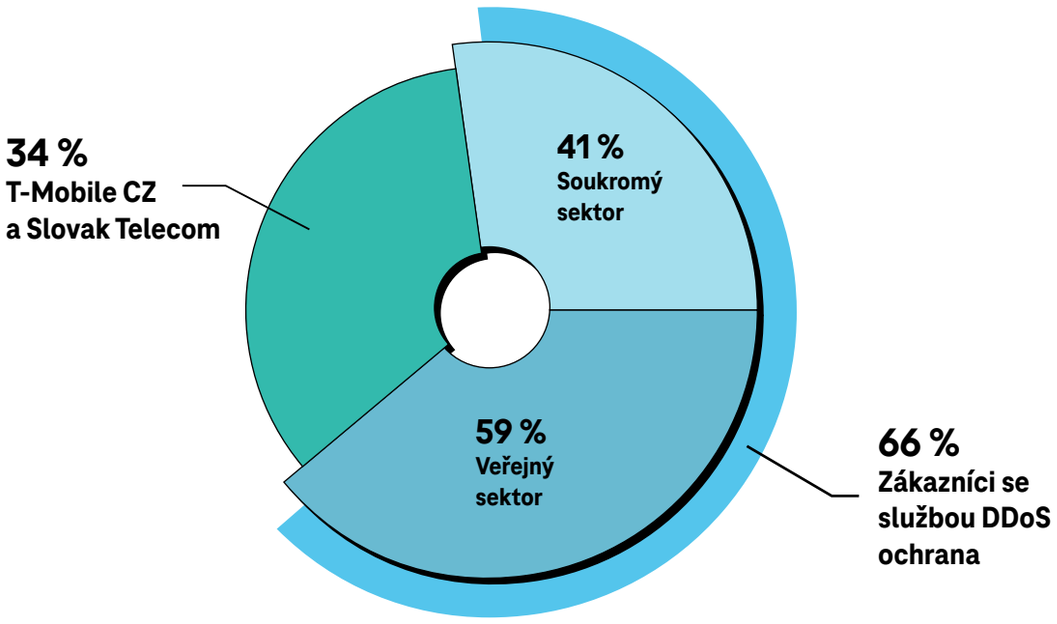
DDoS – TYPY DETEKOVANÝCH ÚTOKŮ







DDoS – CÍLE ÚTOKŮ

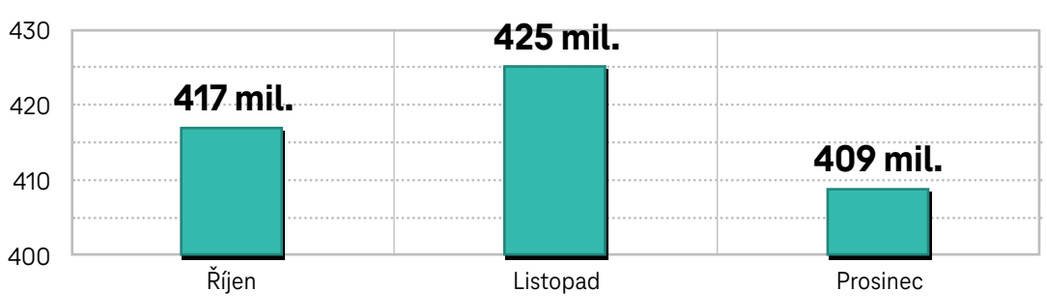


Zákazníci s aktivní službou DDoS ochrana od T-Mobile, kteří se stali terčem DDoS útoku, nezaznamenali díky aktivní ochraně narušení provozu.

NEJSILNĚJŠÍ VOLUMETRICKÝ ÚTOK

Nejsilnější volumetrický **útok** v průběhu 4. čtvrtletí 2023 byl v listopadu a měl sílu 258,7 Gbit/s. Byl součástí volumetrických útoků na slovenské instituce.

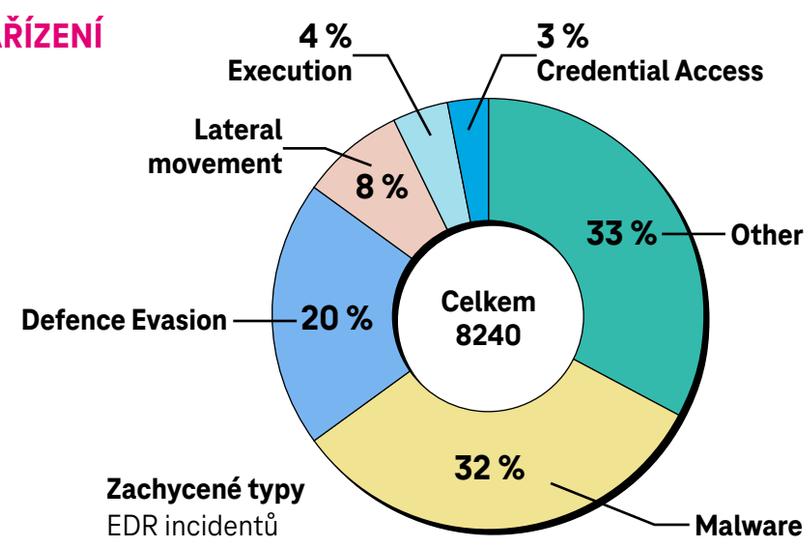
ÚTOKY NA WEBOVÉ APLIKACE

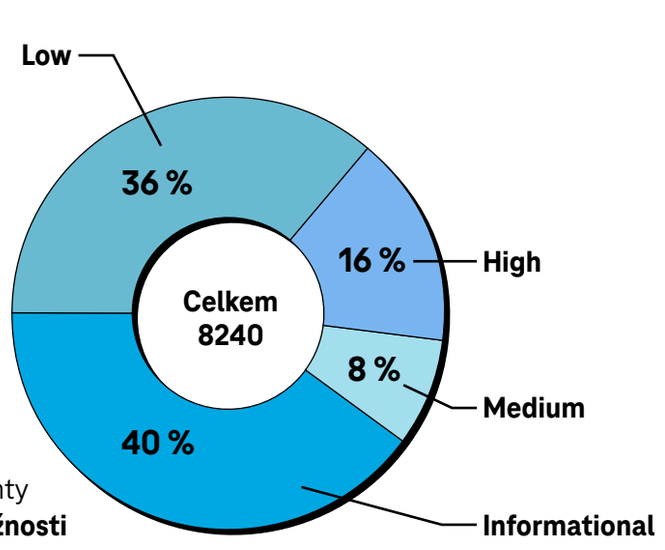


Údaje zahrnují statistiku z více než 60 webových portálů, které jsou chráněné díky T-Mobile CZ WAF. Jde o jednu z největších WAF implementací v Evropě.

EDR – OCHRANA KONCOVÝCH ZAŘÍZENÍ

Aktuálně monitorujeme přes 19 600 koncových zařízení, a to jak v našem interním prostředí (T-Mobile CZ a Slovak Telekom), tak i u našich zákazníků.





Téma čtvrtletí: NIS2 a nový Zákon o kybernetické bezpečnosti

Směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, která se postupně dostává do našeho povědomí pod zkratkou NIS 2, rezonuje v poslední době nejen v bezpečnostní komunitě. Již před rokem byl zveřejněn první návrh nového Zákona o kybernetické bezpečnosti, do kterého bude transponována. Každý se tak mohl seznámit s návrhem nových požadavků a podat k nim případně připomínky. Po zpracování připomínek od veřejnosti a jednotlivých subjektů v rámci mezirezortního připomínkového řízení byl návrh Zákona předán Legislativní radě vlády. Nyní jej čeká projednání (a úpravy) vládou a následně poslaneckou sněmovnou. Předpokládáme, že nová podoba Zákona bude jasná na konci tohoto roku. Následně budou mít dotčené subjekty přechodné období, ve kterém budou muset požadavky Zákona implementovat.

Je nutné mít na paměti, že pouhé splnění podmínek NIS 2 neznamená automaticky naplnění požadavků nového Zákona. I když přesné znění Zákona neznáme (a tím pádem není možné přesně určit, na koho a v jakém rozsahu se budou povinnosti vztahovat), není nutné pouze pasivně čekat. Lze začít s celou řadou aktivit, které zcela jistě zjednoduší následnou implementaci požadavků Zákona:

Zavedení systému řízení bezpečnosti informací

Systém řízení bezpečnosti informací je komplexní interní proces pro práci s informačními aktivy, klíčovými pro řádné fungovaní společnosti. Je nutné stanovit cíle řízení bezpečnosti informací a na jejich základě přijmout přiměřená opatření. Tato opatření je zapotřebí následně pravidelně vyhodnocovat.

V této fázi je zároveň vhodné jasně určit osoby odpovědné za kybernetickou bezpečnost.

Zavedení řízení aktiv a rizik

Řízení aktiv a rizik je jedna ze základních povinností pro společnost. Řízením aktiv má organizace zajištěno, že ví, co je pro ni klíčové a co tedy musí chránit (a co chránit nepotřebuje). Prvním krokem je komplexně zmapovat podniková aktiva, informace o fungování a firemní data. Na základě zmapovaných aktiv se provede analýza zranitelností a hrozeb, které na tyto aktiva působí (analýza rizik). Cílem je mít přehled, jaká rizika se ve společnosti vyskytují a současně mít možnost přijmout opatření k jejich snížení.

Bezpečnost dodavatelského řetězce

Každá firma bude muset mít ze Zákona přehled o svých dodavatelích a určit jejich význam pro své podnikání. Podle předmětu plnění a významnosti dodavatele budou muset smlouvy s dodavateli obsahovat ustanovení k zajištění informační bezpečnosti. Mimo to bude nutné dodavatele průběžně informovat o nových požadovaných bezpečnostních opatřeních.

Bezpečnost software, hardware a IT infrastruktury

Na základě analýzy rizik musí být přijata přiměřená opatření k ochraně software, hardware a síťové infrastruktury. Kromě implementace technických prostředků (například firewallů, EDR řešení, VPN přístupů) a nasazení kryptografických prostředků, to zahrnuje i řízení přístupů k jednotlivým systémům, procesy pro bezpečný vývoj, řízení změn a zálohování a další.

IT prostředí je potřeba monitorovat s ohledem na výskyt nových zranitelností a pravidelně je testovat (provádět penetrační testy, analýzy zdrojových kódů).

Monitoring provozu IT prostředí

Monitoring IT prostředí je klíčový pro schopnost detekce incidentů. Logy z jednotlivých systémů a síťových prvků je nezbytné kontinuálně vyhodnocovat a na nálezy adekvátně reagovat. V tomto mohou technicky pomoci SIEM nástroje, systém na řízení incidentů (ticketing tool). Ideálně jsou pak tyto nástroje dohledovány týmem bezpečnostního dohledového centra (SOC).

Vzdělávání zaměstnanců v oblasti informační bezpečnosti

Nejslabším článkem kybernetické a informační bezpečnosti je většinou člověk, respektive uživatel. Odpovídající průběžné školení zaměstnanců (včetně vrcholového managementu) je nutnou součástí jakéhokoli systému řízení informační bezpečnosti.

Hlášení incidentů

Nový zákon přináší vybraným subjektům povinnost hlásit příslušným orgánům (včetně zákazníků) incidenty ve svém prostředí. Zatímco forma hlášení není ještě finalizována, může společnost již nyní implementovat první krok, tedy schopnost incident zjistit a zajistit, že se jím bude někdo zabývat.

Kontinuita činností provozu, havarijní plány a audit

Pokud bude společnost napadena, je nutné, aby na tuto situaci dokázala adekvátně reagovat. Je vhodné mít připravené postupy, které zajistí minimalizaci následků incidentů. Havarijní plány a plány kontinuity činností umožní rychlou a efektivní reakci na krizovou situaci. Nezbytnou součástí pak jsou i plány obnovy – zásady, nástroje a postupy které zajistí včasnou obnovu provozu tak, aby společnost mohla pokračovat ve své činnosti bez ohledu na incident.

Audit

Společnost musí provádět interní audity systému řízení bezpečnosti informací, evidovat jejich nálezy a na základě závěrů z nálezů přijímat opatření pro kontinuální zlepšování.

Řízení bezpečnosti není nic komplikovaného. Je ale klíčové si uvědomit že bezpečnost má primárně chránit vaše podnikání, a proto se netýká pouze technických opatření (a IT oddělení). Dotýká se všech procesů a činností vaší společnosti. Pokud se v některých oblastech necítíte úplně jistí, rádi vám pomohou naši konzultanti.