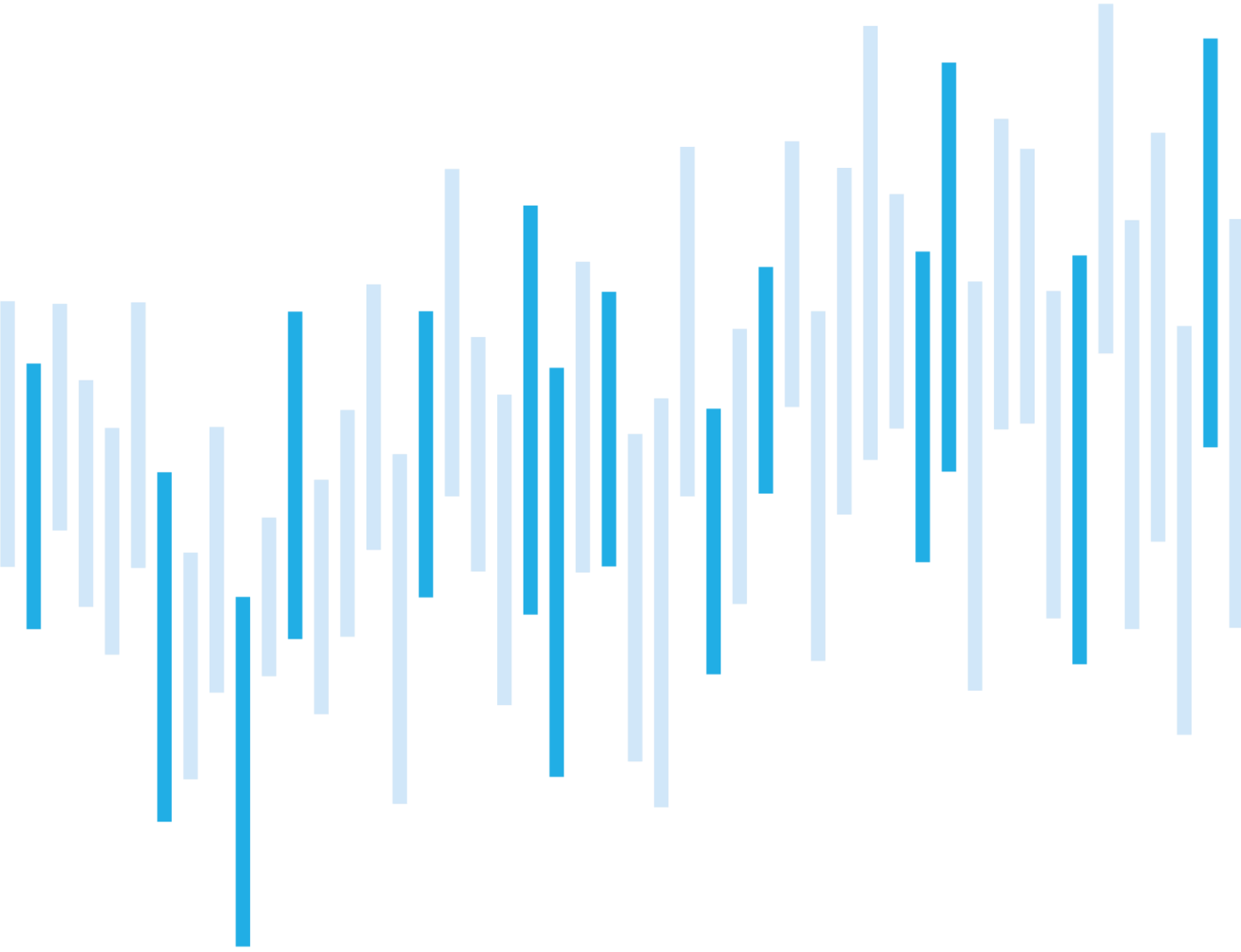
Kybernetické incidenty pohledem NÚKIB

ČERVENEC 2024



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Červenec přinesl významný nárůst evidovaných incidentů, z nichž značná část byla způsobena výpadkem nástroje společnosti CrowdStrike. Dopady tohoto celosvětového incidentu se nevyhnuly ani České republice, celkově však byly jeho implikace v tuzemsku spíše nižší. Evidovány byly taktéž DDoS útoky.

Celkový počet incidentů se vyšplhal na počet 32, z nichž bylo 27 klasifikováno jako méně významné. Zbylých 5 incidentů pak NÚKIB eviduje jako významné.

V kapitole Zaměřeno na událost shrnujeme příčiny a dopady incidentu společnosti CrowdStrike, který byl způsoben chybnou aktualizací jejich EDR (Endpoint Detection and Response) softwaru Falcon. Ta vedla k tzv. modré obrazovce smrti (Blue screen of death, BSOD) na zařízeních využívajících právě EDR Falcon a OS Windows. Celkově se incident dotkl přibližně jednoho procenta všech zařízení využívajících OS Windows, jednalo se tak o největší IT výpadek v historii se škodou dosud vyčíslenou v miliardách dolarů.

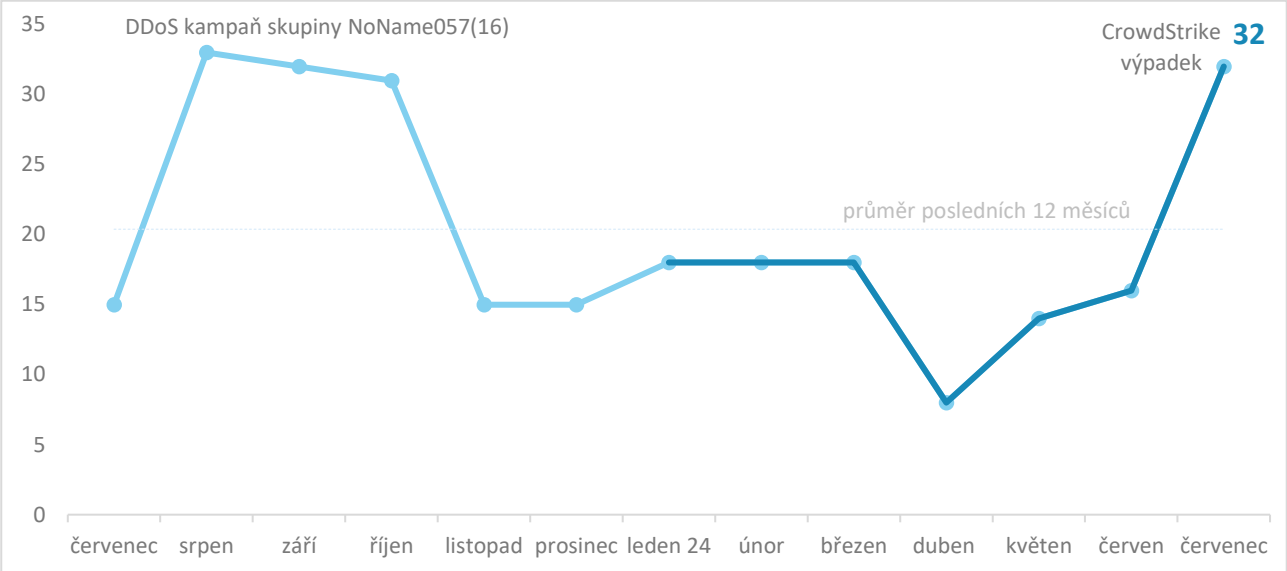
Obsah

Následující report shrnuje dění měsíce. Data, informace a závěry v něm obsažené primárně vychází z kybernetických incidentů nahlášených NÚKIB. Pokud report v některých částech obsahuje informace z otevřených zdrojů, je vždy uveden původ těchto informací.

Připomínky a náměty na zlepšení reportu můžete posílat na adresu komunikace@nukib.gov.cz.

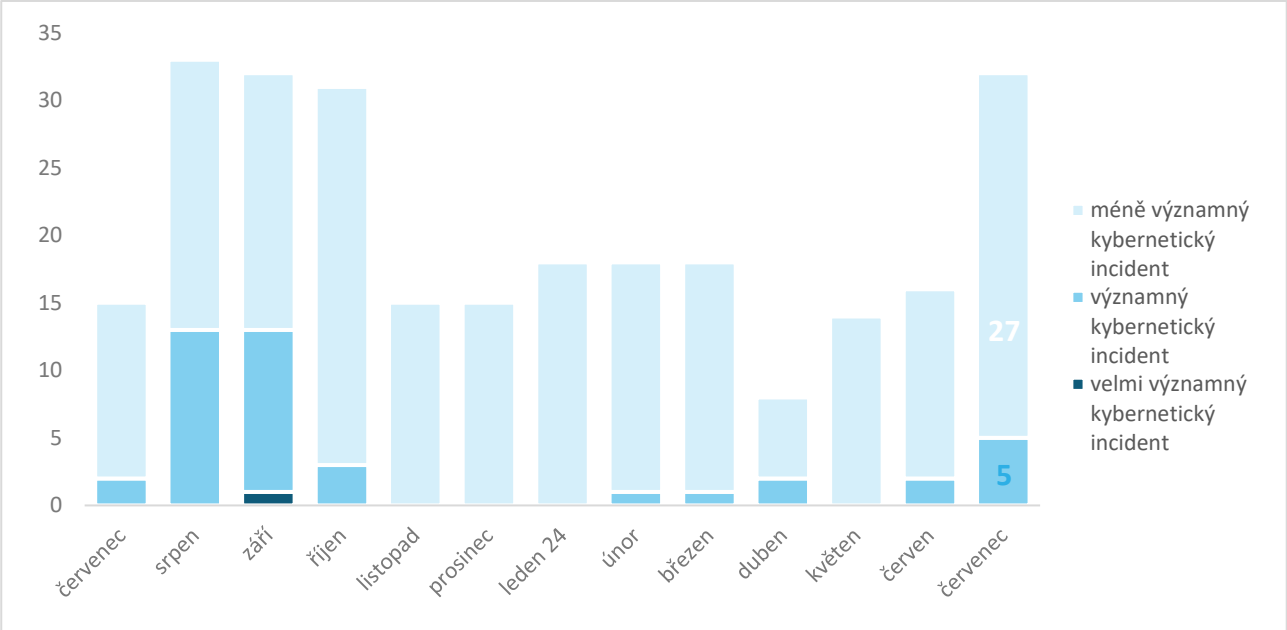
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Během července NÚKIB evidoval 32 incidentů, což představuje výrazný nárůst oproti předchozím měsícům. Důvodem jsou zejména incidenty spojené s výpadkem EDR softwaru CrowdStrike a pokračujícím výskytem DDoS útoků.



Závažnost řešených kybernetických incidentů[1]

I v kontextu závažnosti došlo k růstu počtu incidentů, které NÚKIB eviduje jako významné. Dva z nich se týkají incidentu CrowdStrike, zbylé tři se týkají různých kompromitací, v jednom případě i se značnou finanční škodou v důsledku úspěšného spear-phishingu.



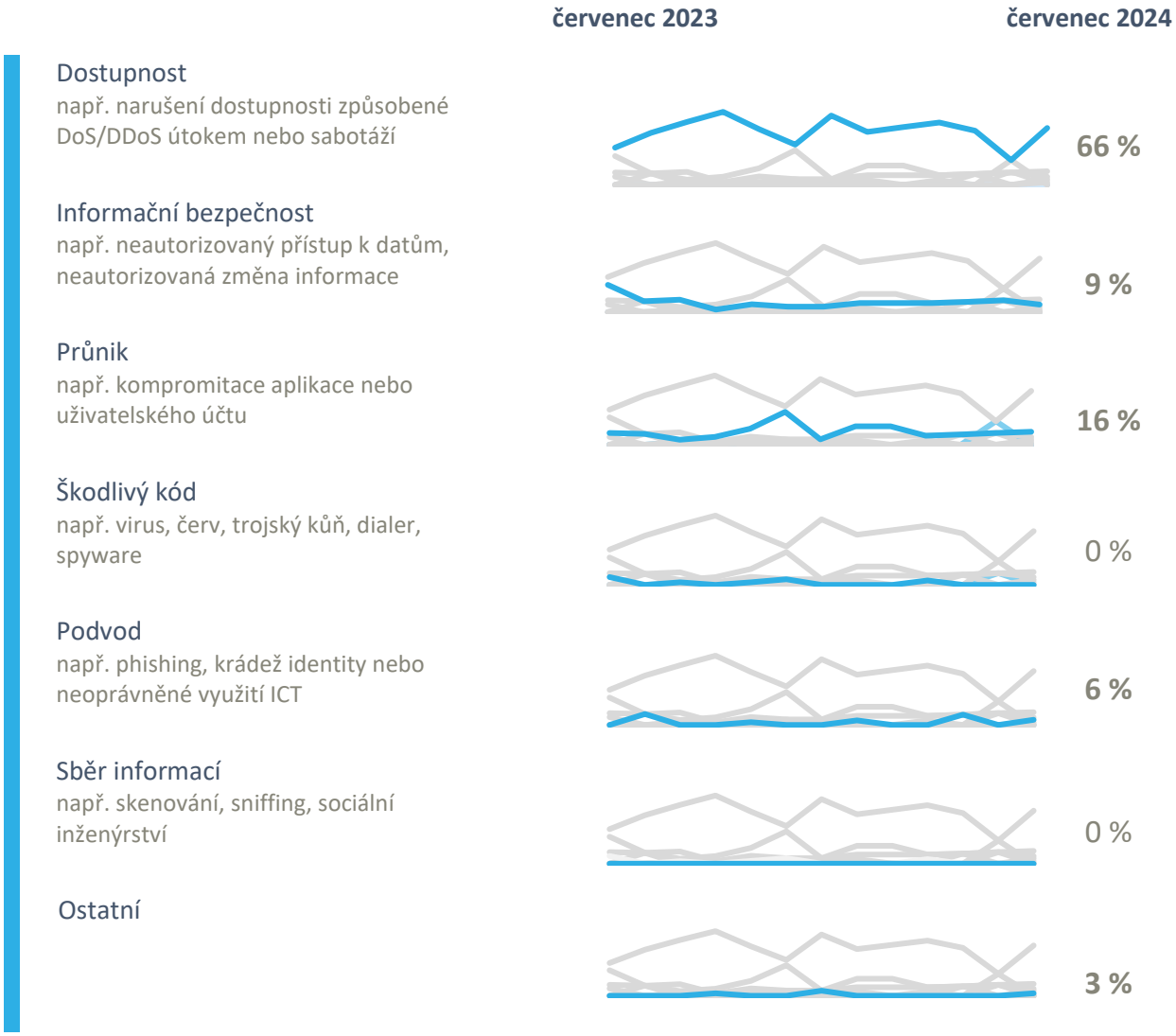
[1] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[2]

Nejpočetnější kategorii incidentů během července představuje Dostupnost, ve které NÚKIB evidoval 10 incidentů v kontextu výpadku CrowdStrike, 10 DDoS útoků a jeden výpadek způsobený technickou závadou. Pouze u dvou subjektů zasažených výpadkem CrowdStrike byly následky vyhodnoceny jako významné. Za čtyřmi DDoS útoky stála ruskojazyčná hacktivistická skupina NoName057(16).

NÚKIB dále řešil incidenty ve třech kategoriích:

- Pět incidentů spadá do kategorie Průnik, ve čtyřech případech se jednalo o kompromitované e-mailové schránky a následný phishing či spamming, v posledním případě byl kompromitován systém české státní instituce dosud neznámým útočníkem.
- Ve dvou incidentech v kategorii Podvod útočníci využívali spear-phishing, v obou případech úspěšně přesvědčili oběť k autorizaci podvodné platby.
- V rámci kategorie Informační bezpečnost eviduje NÚKIB dva úspěšné ransomwarové útoky, při kterých byl využit ransomware DragonForce a Qilin, a jeden případ úniku informací.



[2] Klasifikace kybernetických incidentů je založena na taxonomii ENISA: Reference Incident Classification Taxonomy — ENISA (europa.eu).

Trendy v kybernetické bezpečnosti za červenec pohledem NÚKIB[3]

Phishing, spear-phishing a sociální inženýrství

NÚKIB v červenci eviduje dva případy využití spear-phishingu. V obou případech povědomí útočníků o napadené organizaci vedlo k úspěšné autorizaci podvodných plateb oběťmi.

Malware

V červenci podobně jako v uplynulých měsících probíhaly kontinuální aktivity v oblasti malwarové analýzy v souvislosti s některými dříve evidovanými incidenty.

Zranitelnosti

Během července NÚKIB nevydal žádné upozornění týkající se zranitelností. Vládní CERT však pokračuje ve sdílení informací o aktuálních zranitelnostech na platformě X.
Zveřejněna byla například CVE-2024-37085 v rámci WMware ESXi, která měla být aktivně zneužívána ransomwarovými gangy i po její nápravě.
Zmíněny byly i škodlivé aktivity různých aktérů hrozeb, kteří zneužívali tematiky výpadku EDR softwaru společnosti CrowdStrike.

Ransomware

V červenci byly evidovány dva případy incidentů spojených s ransomwarem. Jeden z nich má na svědomí skupina DragonForce Ransomware, u druhého incidentu byl evidován ransomware Qilin, který je nabízen jako služba (RaaS).

Útoky na dostupnost

V červenci NÚKIB evidoval 10 útoků na dostupnost, z nichž alespoň čtyři byly provedeny ruskojazyčnou hacktivistickou skupinou NoName057(16). Všechny mířily na instituce státního a finančního sektoru.

[3] Vývoj ilustrovaný šipkou je vyhodnocován ve vztahu k předešlému měsíci.

Zaměřeno na událost: Chybná aktualizace vyřadila z provozu miliony zařízení po celém světě, v České republice byly dopady mírné

V pátek 19. července 2024 zasáhl širokou škálu zařízení s operačním systémem Microsoft Windows po celém světě problém způsobující nefunkčnost těchto zařízení, konkrétně kolaps operačního systému do tzv. „modré obrazovky smrti“ a následné neschopnosti se spustit. Za vznikem stojí chyba v aktualizaci Endpoint Detection and Response (EDR) platformy CrowdStrike Falcon. Společnost CrowdStrike během několika hodin chybnou aktualizaci stáhla a vydala návod na opravu, který zahrnoval lokalizaci a odstranění problematického souboru. Ačkoliv byla oprava principiálně jednoduchá, zasažené počítače bylo třeba manuálně spustit v nouzovém režimu. To znamenalo, že se každé zasažené zařízení muselo opravit individuálně, což výrazně prodloužilo dobu a dopady výpadku.

Zasaženi byli uživatelé platformy Falcon s OS Windows. Podle Microsoftu bylo výpadkem poznamenáno přes osm a půl milionu zařízení, což je méně než jedno procento všech zařízení s OS Windows. **I přesto se jedná o doposud největší IT výpadek v historii.** Dopady incidentu se dotkly takřka všech sektorů, s pravděpodobně nejvýznamnějšími dopady se potýkaly aerolinky. Dále byly zasaženy např. televizní stanice, objednávkové systémy k lékaři, samoobslužné pokladny, bankovní služby nebo železnice. **V rámci České republiky NÚKIB eviduje deset zasažených subjektů, přičemž u dvou z nich byly dopady výpadku hodnoceny jako závažné.**

Obrázek 1: Zasažený samoobslužný terminál

Zdroj: thesun.com

Krátce po události začali útočníci zneužívat nastalé situace k jiným škodlivým kybernetickým aktivitám. Jedná se zejména o podvodné e-maily či telefonáty, ve kterých se podvodníci vydávali za zaměstnance společnosti CrowdStrike, případně za nezávislé výzkumníky nabízející technickou pomoc. **Hlavním cílem podvodníků bylo přesvědčit oběť, aby nainstalovala malware, který poskytli pod záminkou, že se jedná o opravný nástroj nebo skript, který má pomoci vyřešit výpadek nebo jeho možné dopady.**

Před vlnou takových phishingových aktivit varovala přímo společnost CrowdStrike a její zjištění se shodují s veřejně dostupnými zdroji i informacemi od partnerů NÚKIB. Podle dostupných informací byl výpadek zneužíván jak kyberkriminálními, tak státem sponzorovanými aktéry.

Použité pravděpodobnostní výrazy

Pravděpodobnostní výrazy a vyjádření jejich procentuálních hodnot:

Výraz	Pravděpodobnost
Téměř jistě	90–100 %
Velmi pravděpodobně	75–85 %
Pravděpodobně	55–70 %
Nelze vyloučit/Reálná možnost	40–50 %
Nepravděpodobně	20–35 %
Velmi nepravděpodobně	0–15 %

Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách nukib.gov.cz). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
TLP:RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP:AMBER+STRICT	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
TLP:CLEAR	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.