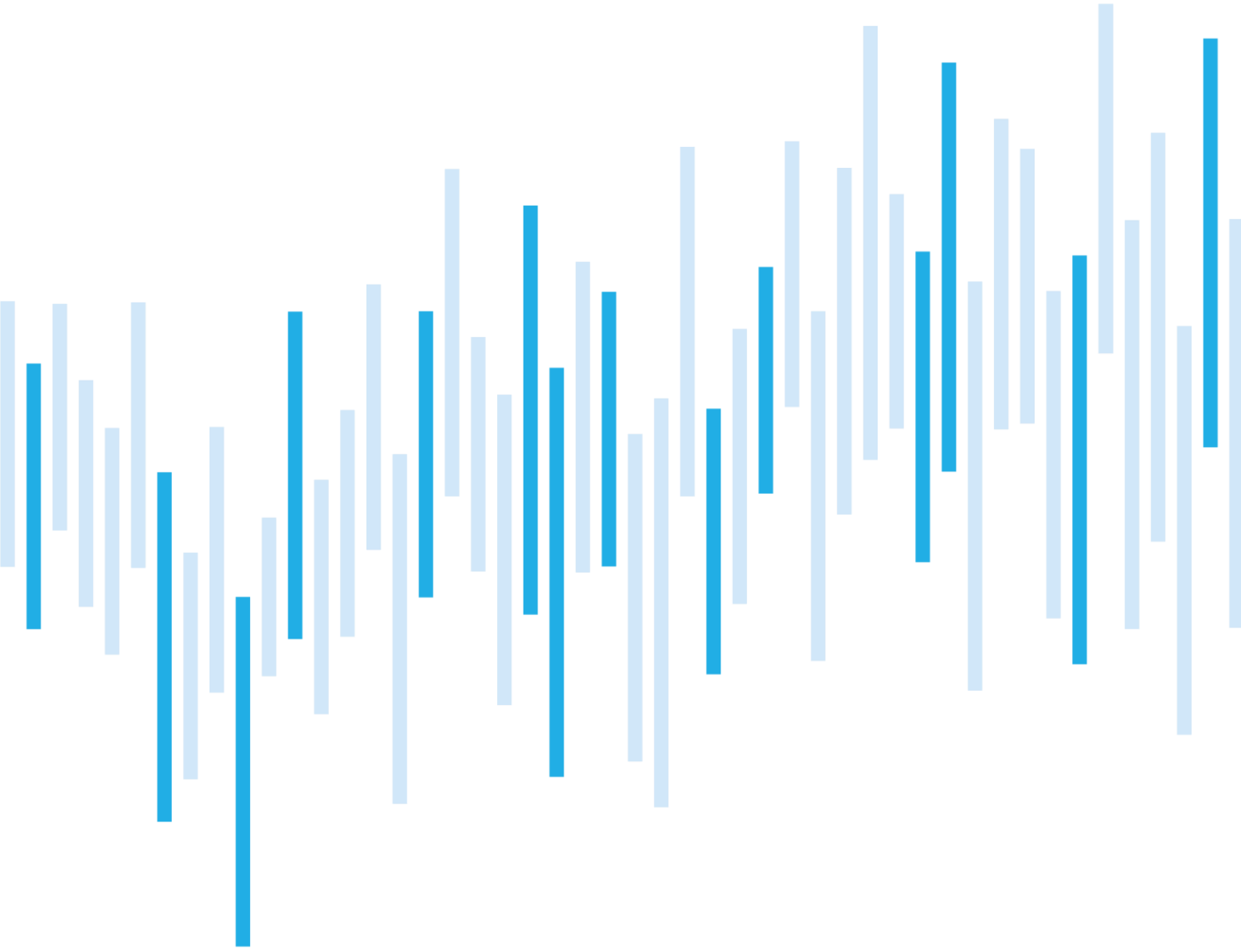
Kybernetické incidenty pohledem NÚKIB

DUBEN 2024



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Duben představuje z pohledu incidentů podprůměrný měsíc, během kterého NÚKIB evidoval pouze osm incidentů. Jedná se tak o dosavadní minimum za uplynulý rok. Pokles je dán zejména absencí útoků na dostupnost, z nichž většinu mají obvykle na svědomí ruskojazyčné hacktivistické skupiny.

Většina incidentů i přesto spadala do kategorie Dostupnost, jednalo se však o incidenty v důsledku technických závad, které vedly k výpadkům různých služeb a systémů subjektů. Dále byly evidovány jednotky incidentů v kategoriích Podvod, Informační bezpečnost a Průnik.

V kapitole Zaměřeno na trend se tentokrát věnujeme rozmachu kompromitací okrajových zařízení (tzv. edge devices), jako jsou VPN servery, firewally či routery. Kompromitace těchto zařízení nabízí útočníkům výhodnou pozici pro další škodlivé působení a snižuje riziko jejich odhalení. Specificky pak kapitola zmiňuje kampaň s názvem ArcaneDoor, která cílila na produkty společnosti Cisco. Existuje reálná šance, že podobný typ kampaní bude s rostoucí mírou evidován i v České republice.

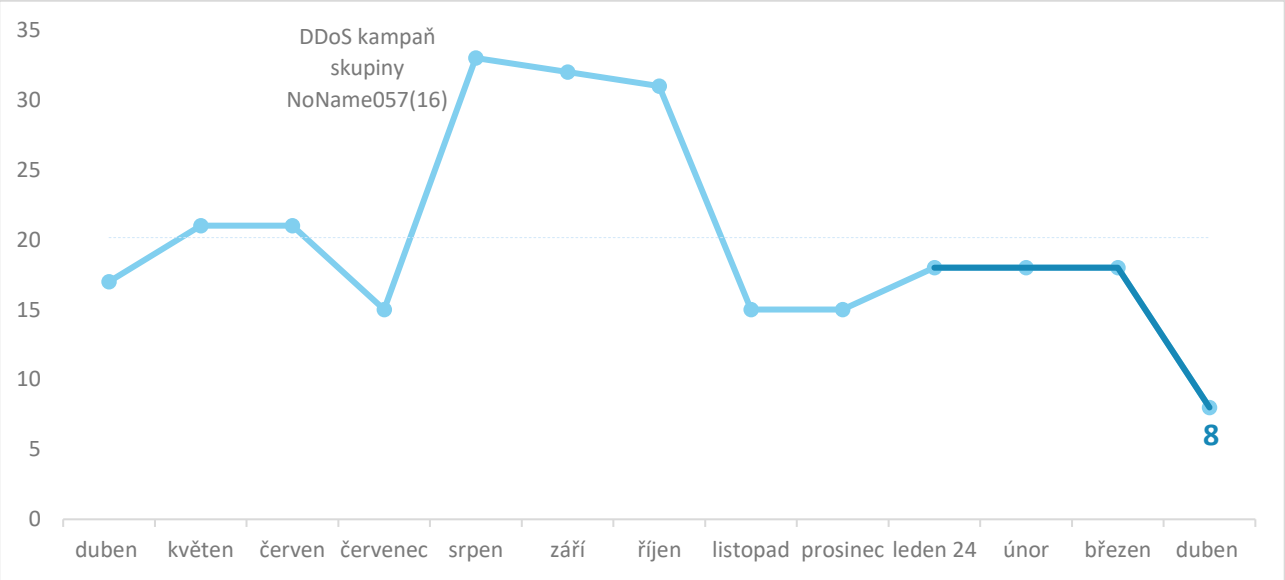
Obsah

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.

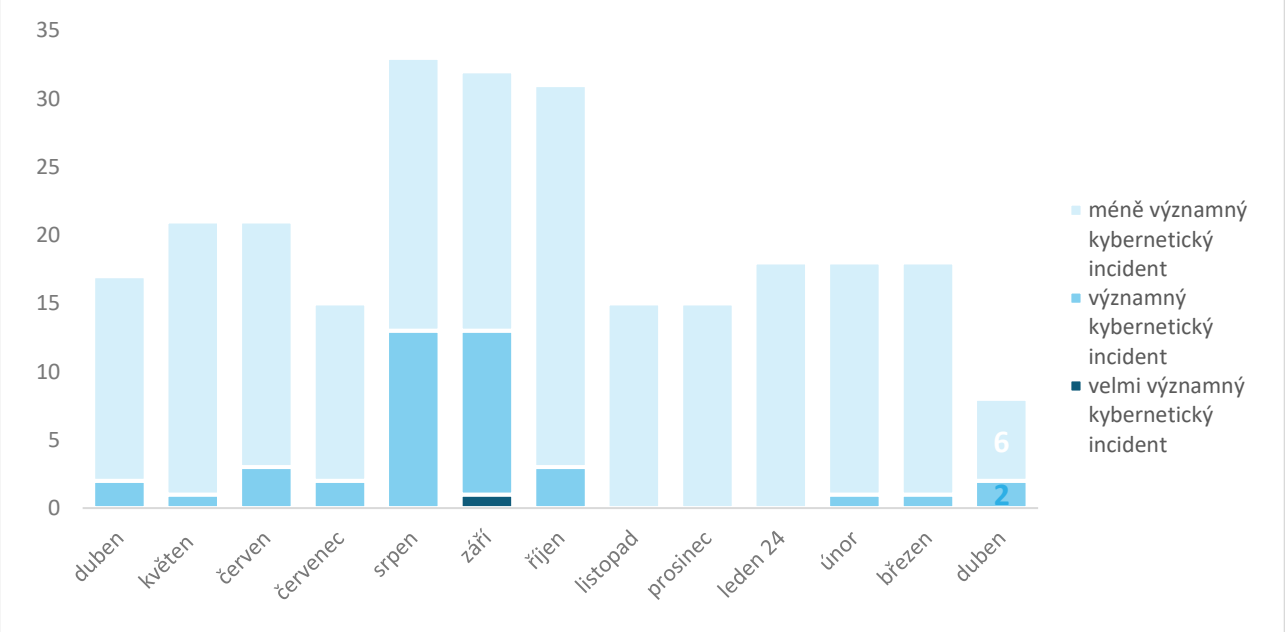
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Během dubna bylo evidováno osm kybernetických incidentů. Jedná se o výrazně podprůměrné množství, dokonce nejnižší za uplynulý rok. Pokles je dán zejména absencí škodlivé činnosti rusko-jazyčných aktérů, která je typická zejména DDoS útoky.



Závažnost řešených kybernetických incidentů[1]

Navzdory nižšímu počtu incidentů byly dva z osmi vyhodnoceny jako významné, zbylých šest pak spadalo do kategorie méně významných.



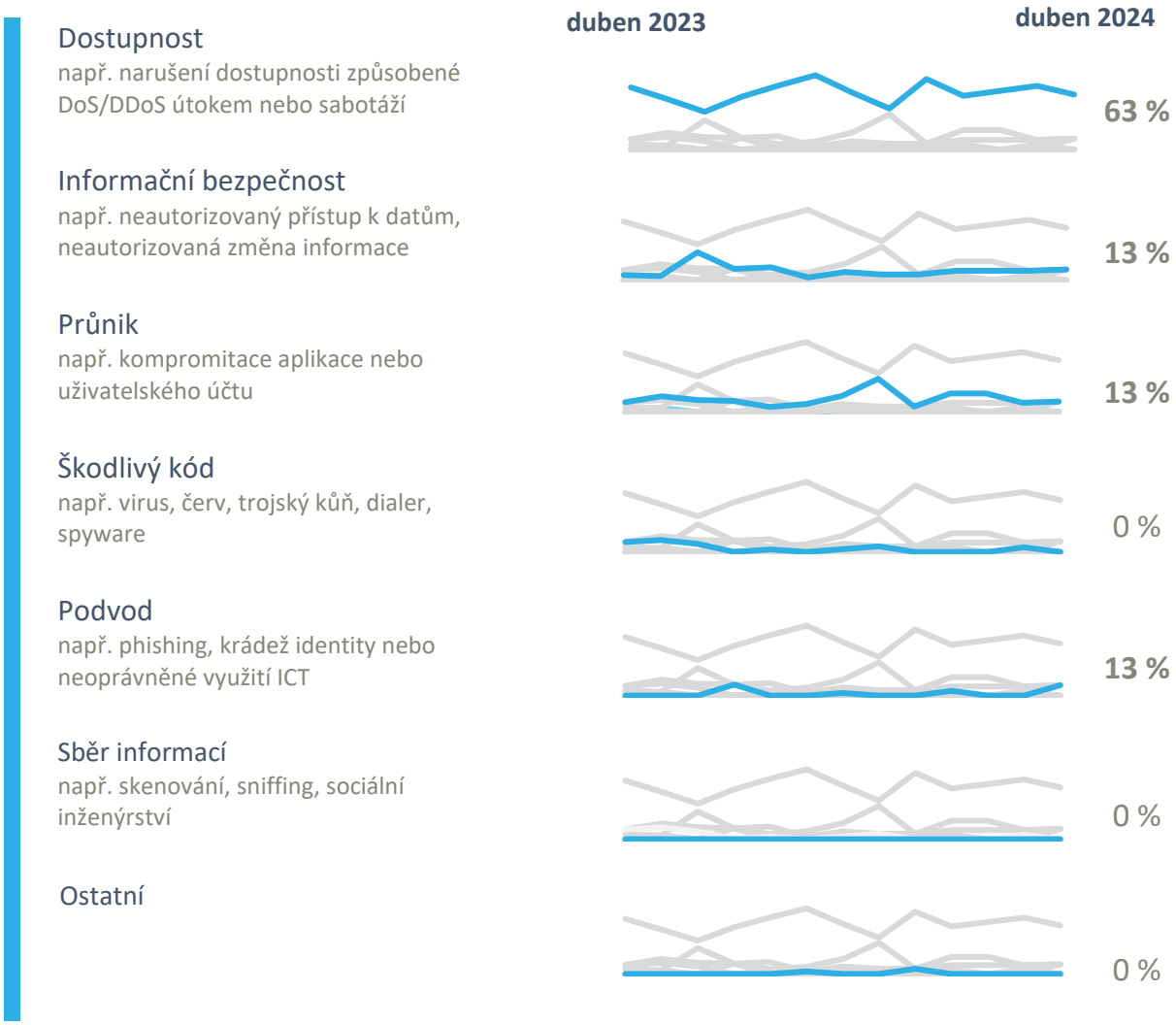
[1] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[2]

Po několika měsících v dubnu absentovaly dlouhodobě evidované DDoS útoky, nicméně i tak většina incidentů spadala do kategorie Dostupnost. Všech pět incidentů této kategorie však bylo způsobeno technickou chybou, bez vnějšího zavinění.

NÚKIB dále řešil incidenty ve třech kategoriích:

- Jeden incident spadal do kategorie Podvod, jelikož se jednalo o úspěšný phishingový útok, jehož oběť poskytla přihlašovací údaje, včetně hesla pro dvoufázové ověření. Neznámý útočník následně využil účet oběti k rozesílání dalších phishingových zpráv.
- V rámci kategorie Informační bezpečnost byl evidován jeden incident. Jednalo se však pouze o případ sdílení přístupu do informačního systému vícero osobami v rámci běžného provozu.
- Poslední kategorií byl Průnik, kdy dosud neznámý útočník kompromitoval publikační systém webu jednoho z českých médií, kde zveřejnil několik dezinformačních článků. Jeho činnost však byla odhalena v řádu desítek minut a články smazány.



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

Trendy v kybernetické bezpečnosti za duben pohledem NÚKIB[3]

Phishing, spear-phishing a sociální inženýrství

Během dubna NÚKIB registroval jeden incident zahrnující phishing. Jeho oběť poskytla útočníkovi přihlašovací údaje a následně i kód pro dvoufázové ověření. Tyto údaje byly posléze zneužity pro rozesílání dalších phishingových zpráv.

Malware

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

Zranitelnosti

Během dubna NÚKIB nevydal upozornění či varování v kontextu nově nalezených zranitelností.

Ransomware

V průběhu dubna nebyly registrovány žádné ransomwarové útoky.

Útoky na dostupnost

Přestože v dubnu absentovaly DDoS útoky rusko-jazyčných hacktivistických skupin, došlo k pěti incidentům v kategorii Dostupnost. Jednalo se však o incidenty způsobené technickou závadou.

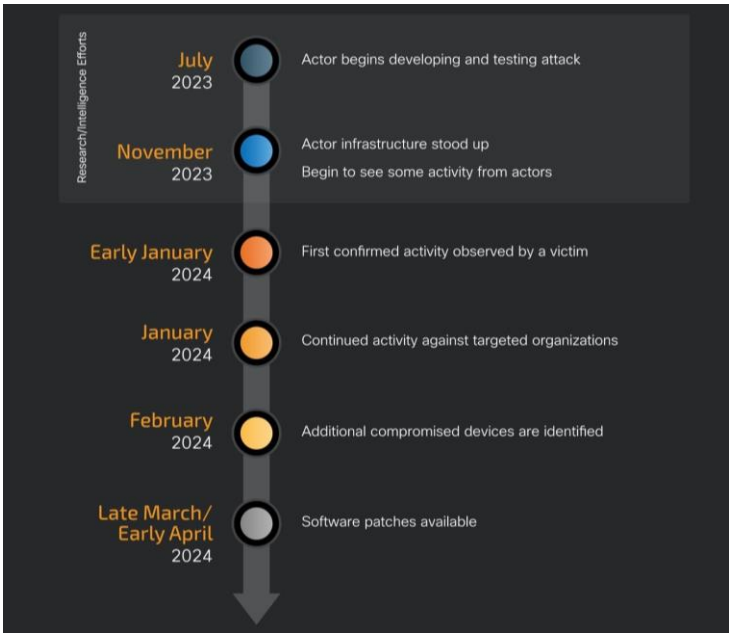
[3] Vývoj ilustrovaný šipkou je vyhodnocován ve vztahu k předešlému měsíci.

Zaměřeno na trend: Útoky vůči okrajovým zařízením (tzv. edge devices)

V této kapitole se zaměříme na vzrůstající trend kompromitace okrajových zařízení (tzv. edge devices), jakožto prvotního vektoru kybernetických útoků. Během dubna totiž došlo k vydání několika analýz rozsáhlých kampaní, při kterých byly využity zranitelnosti právě v okrajových zařízeních, jako jsou VPN servery, firewally či routery. Nárůst tohoto trendu lze vysvětlit například rostoucím zabezpečením koncových stanic vůči malwaru, či výhodnou pozicí okrajových zařízení pro další fáze útoku v rámci infrastruktury obětí.

Během dubna vydala společnost Cisco analýzu několikaměsíční kampaně s názvem ArcaneDoor, v rámci které dosud neznámý státem sponzorovaný aktér kompromitoval řadu okrajových zařízení několika různých výrobců. Cílem kampaně byla kyberšpionáž a útoky zneužívaly dvou zranitelností (CVE-2024-20353 a CVE-2024-20359).

Obrázek 1: Časová osa kampaně ArcaneDoor (větší rozlišení)



Nárůst tohoto typu útoků potvrzuje i výroční zpráva společnosti Mandiant, podle které je tato taktika pro útočníky výhodná díky nižším šancím na odhalení jejich škodlivé aktivity. Typicky je kompromitace okrajových zařízení docílena pomocí kombinace zneužití zranitelnosti a nasazení specifického malwaru, což potvrzuje i výše zmíněný případ společnosti Cisco. Podle zprávy Mandiant navíc tento trend bude akcelerovat a téměř jistě (90–100 %) se objeví další případy již během letošního roku.

NÚKIB v tomto kontextu v uplynulých měsících evidoval několik incidentů. Zejména se jednalo o zneužívání zranitelností v okrajových zařízeních Ivanti, či méně sofistikované brute-force útoky na produkty Cisco v České republice během dubna. Poslední jmenované však nebyly úspěšné a jsou evidovány pouze jako bezpečnostní události.

V kontextu mitigace potom platí tradiční přístupy spočívající zejména v udržování aktuálního softwaru dotčených zařízení a monitorování jejich nově odhalených zranitelností či dodržování zásad tzv. defense-in-depth pro případy zneužití zranitelnosti nultého dne.

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.