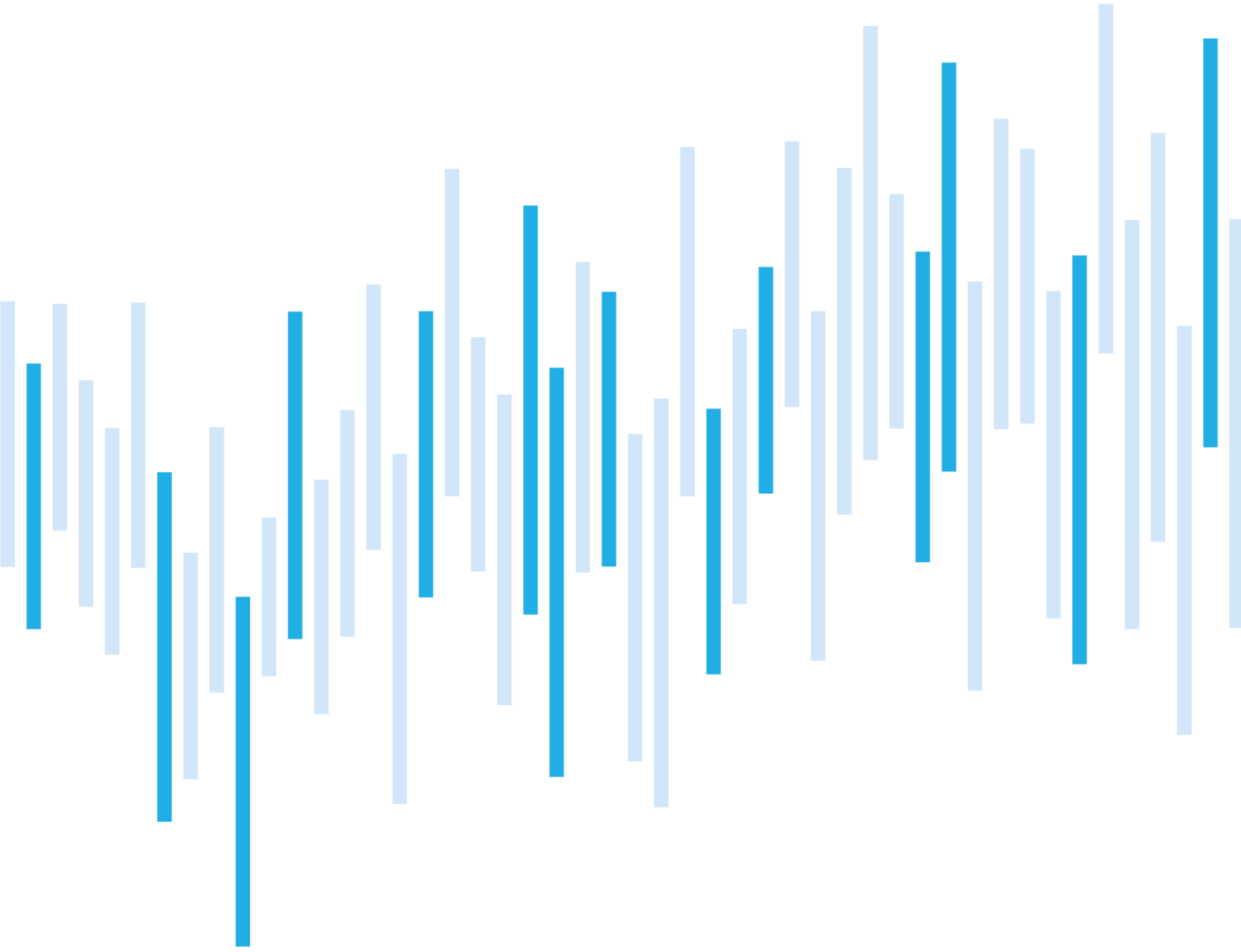
Kybernetické incidenty pohledem NÚKIB

BŘEZEN 2024



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

V březnu byl evidován totožný počet incidentů jako uplynulý měsíc. Jednalo se tak již o pátý měsíc v řadě s podprůměrnými hodnotami evidovaných incidentů. Stejně jako v únoru byl zaznamenán i jeden významný kybernetický incident. Zbylých 17 incidentů pak spadalo do kategorie méně významných.

I nadále v přehledu dominují incidenty spojené s dostupností. Evidovány byly také incidenty z kategorií Průnik a Informační bezpečnost a oproti únoru i Škodlivý kód.

V kapitole Zaměřeno na hrozbu se tentokrát věnujeme odhalení kompromitace nástroje XZ, který je využíván většinou operačních systémů Unix. Dosud neznámý aktér do něj v rámci komplexní a dlouholeté operace umístil backdoor s cílem získat přístup k vysokému počtu zařízení. V reakci na incident došlo k vydání řady varování, zejména ze strany firem distribuujících různé varianty systému Linux.

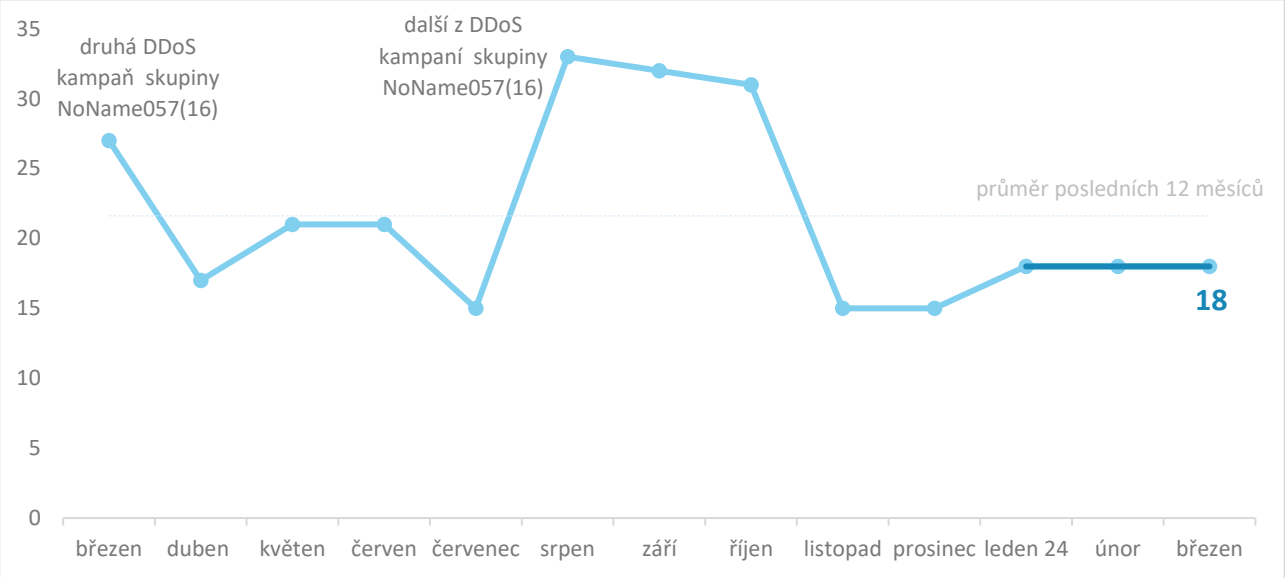
Obsah

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.cz.

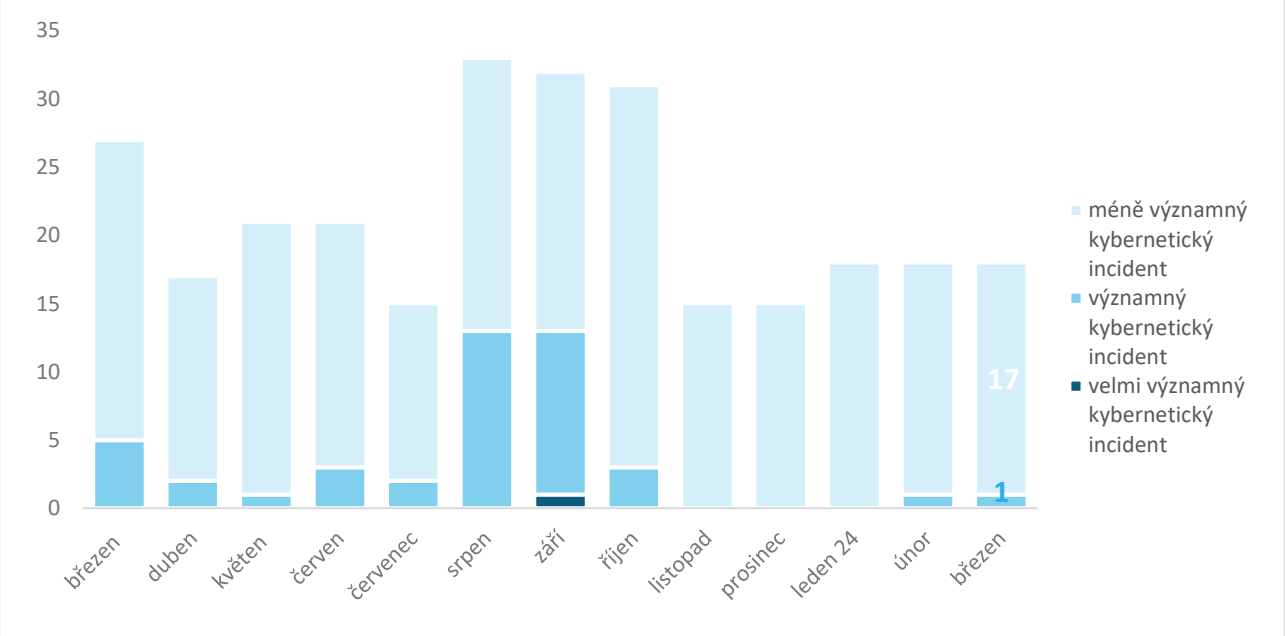
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

V březnu byl evidován totožný počet incidentů jako v předchozím měsíci. Jednalo se tak o pátý měsíc v řadě s podprůměrnými hodnotami evidovaných incidentů.



Závažnost řešených kybernetických incidentů[1]

Obdobně jako v únoru byl v březnu evidován jeden významný kybernetický incident. Zbylých 17 incidentů pak spadalo do kategorie méně významných.



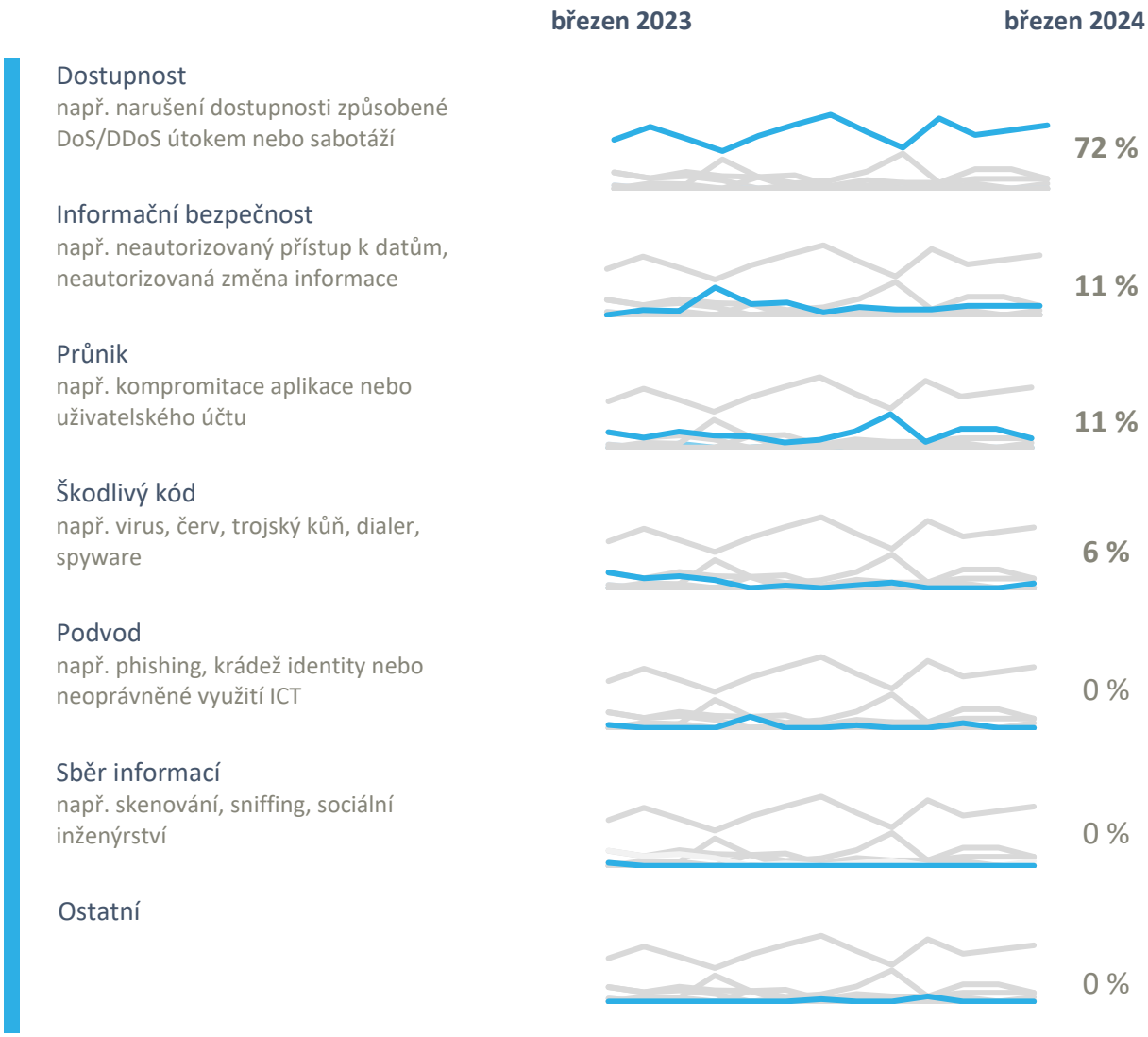
[1] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[2]

Dlouhodobý trend dominance incidentů spojených s dostupností přetrvával také během března, kdy byla tato kategorie tvořena výhradně DDoS útoky.

NÚKIB dále řešil incidenty ve třech kategoriích:

- Dva incidenty spadají do kategorie Informační bezpečnost, přičemž v obou případech se jednalo o ransomwarové útoky. Jeden z útoků má na svědomí skupina LockBit 3.0, u druhého incidentu NÚKIB nedisponuje informacemi o útočníkovi.
- V rámci kategorie Průnik evidoval NÚKIB dva incidenty prolomení uživatelských účtů. Kompromitace však nevedla k úniku dat a incidenty nezpůsobily další dopady.
- Poslední kategorií byl Škodlivý kód, přesněji se jednalo o zneužití zranitelností v produktech Ivanti, které vedly ke kompromitaci VPN a následné exfiltraci dat subjektu.



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

Trendy v kybernetické bezpečnosti za březen pohledem NÚKIB[3]

Phishing, spear-phishing a sociální inženýrství

NÚKIB v březnu zaregistroval pouze jeden incident, v rámci kterého byl prokazatelně využit phishing. Útočníkům se podařilo přimět oběť k vyplnění přihlašovacích údajů na podvodné stránce a poté zneužít tyto údaje pro přístup do dalších služeb.

Malware

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

Zranitelnosti

Během března NÚKIB nevydal žádné upozornění týkající se zranitelností. V rámci jednoho incidentu však došlo ke zneužití starší zranitelnosti v produktech Ivanti ke kompromitaci VPN a dalším škodlivým aktivitám. Zranitelnost, přesněji backdoor, v nástroji XZ však byla označena jako CVE-2024-3094 s nejvyšším hodnocením závažnosti 10.

Ransomware

V březnu byly evidovány dva případy incidentů spojených s ransomwarem. Jeden z nich má na svědomí skupina LockBit 3.0, u druhého incidentu NÚKIB nedisponuje informacemi o původcích útoku.

Útoky na dostupnost

V průběhu března NÚKIB evidoval více než desítku DDoS útoků, které cílily převážně na státní instituce. Za třemi incidenty stála ruskojazyčná hacktivistická skupina, u zbytku útočník není znám.

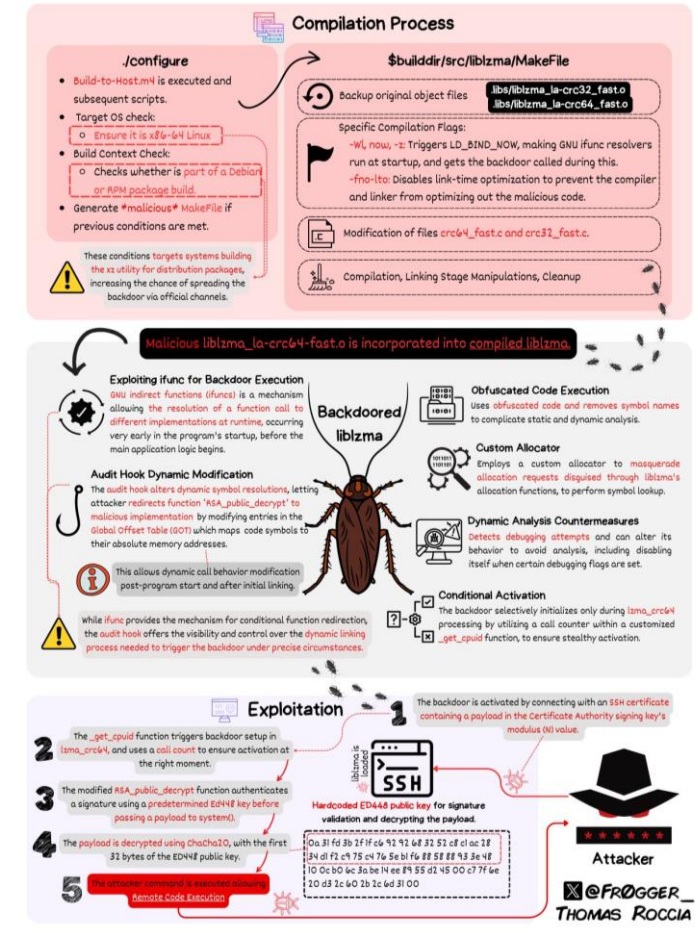
[3] Vývoj ilustrovaný šipkou je vyhodnocován ve vztahu k předešlému měsíci.

Zaměřeno na hrozbu: Kompromitace rozšířeného nástroje systémů na bázi Unix

V pátek 29. března detekoval vývojář společnosti Microsoft, že linuxový nástroj XZ (open-source nástroj pro kompresi dat) obsahuje úmyslně vložený backdoor. Útočníci měli na kompromitaci pracovat roky, přičemž backdoor se měl dostat i do produktů Debian a Fedora, což jsou jedny z největších distribucí systému Linux. S ohledem na komplexní povahu kampaně se jedná o jeden z nejlépe provedených útoků proti dodavatelskému řetězci.

XZ poskytuje bezeztrátovou kompresi dat na prakticky všech operačních systémech podobných operačnímu systému Unix, včetně systému Linux. **Zranitelnost je označována jako CVE-2024-3094, přičemž na škále CVSS dostala kritickou a nejvyšší možnou hodnotu 10.** Navzdory komplexnosti operace byl útok odhalen včas, jelikož nepronikl do stabilních, ale pouze testovacích verzí systémů. Škodlivý kód mohl v případě svého spuštění umožnit eventuální převzetí kontroly nad zařízením oběti.

Obr. 1: Schéma funkce kompromitované knihovny XZ (větší rozlišení)



Zdroj: x.com

V reakci na incident vydala řada společností, včetně Microsoft a Red Hat, varování a doporučení degradovat operační systémy na poslední známou bezpečnou verzi. Obdobně varovala i americká Agentura pro kybernetickou a infrastrukturní bezpečnost (CISA).

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	25–50 %
Nepravděpodobně	15–20 %
Velmi nepravděpodobně	0–10 %

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.