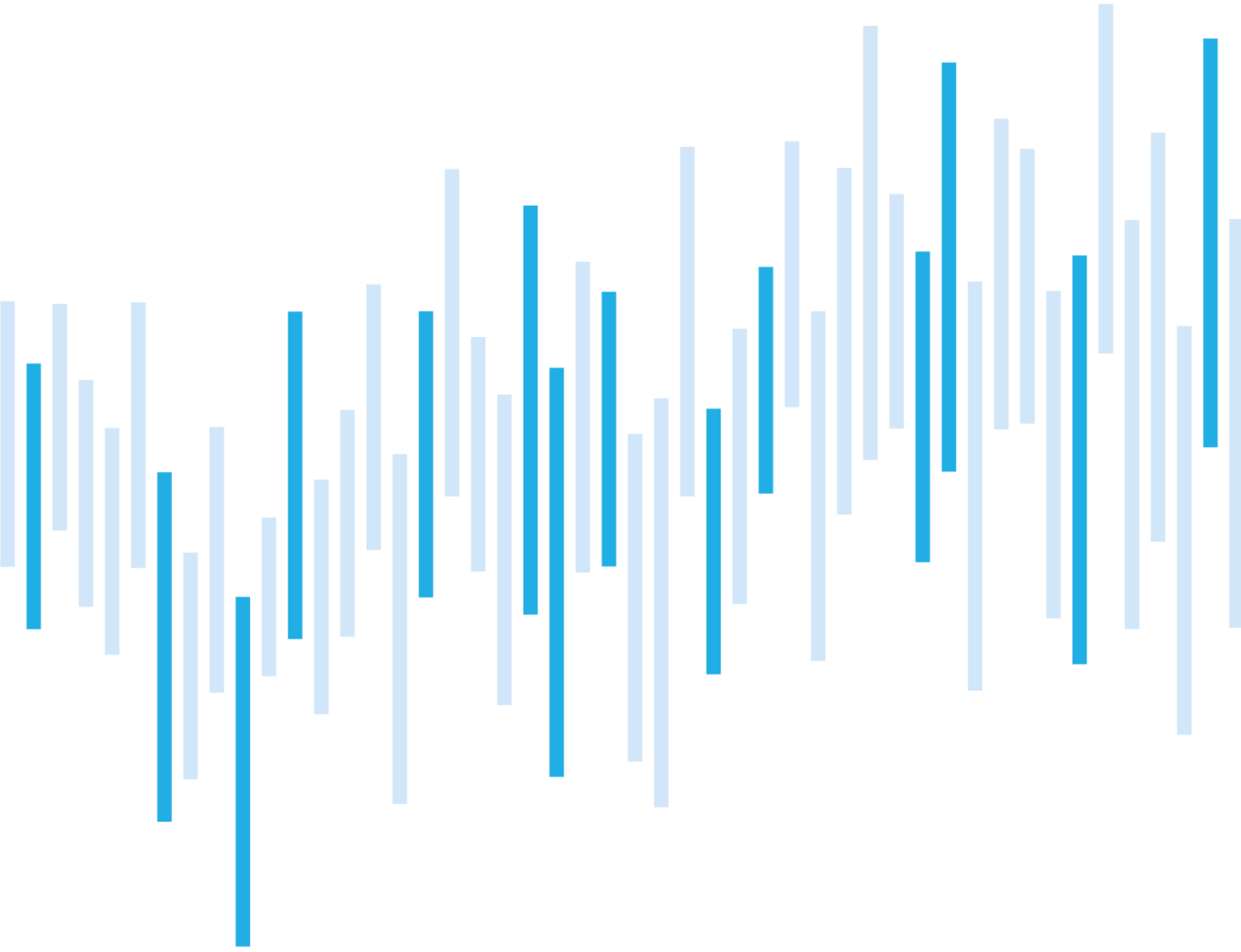
Kybernetické incidenty pohledem NÚKIB

SRPEN 2024



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Během srpna bylo evidováno 31 incidentů, o jeden méně než během července. Druhým měsícem tak pokračuje trend nadprůměrného počtu incidentů. Za vysokými čísly během srpna stojí primárně DDoS kampaň ruskojazyčné hacktivistické skupiny NoName057(16) vůči subjektům veřejného a finančního sektoru. Proběhly však i další útoky na dostupnost, u kterých se útočníka nepodařilo určit.

Většina incidentů spadala do kategorie méně významných, nicméně jeden z evidovaných ransomwarových útoků vůči instituci veřejného sektoru byl vyhodnocen jako významný.

V kapitole Zaměřeno na hrozbu se tentokrát věnujeme malwaru a podvodné kampani NGate, která byla odhalena kyberbezpečnostní společností ESET. Její původci se snaží získat citlivé údaje a finanční prostředky obětí, přičemž aktivní měli být i v rámci České republiky.

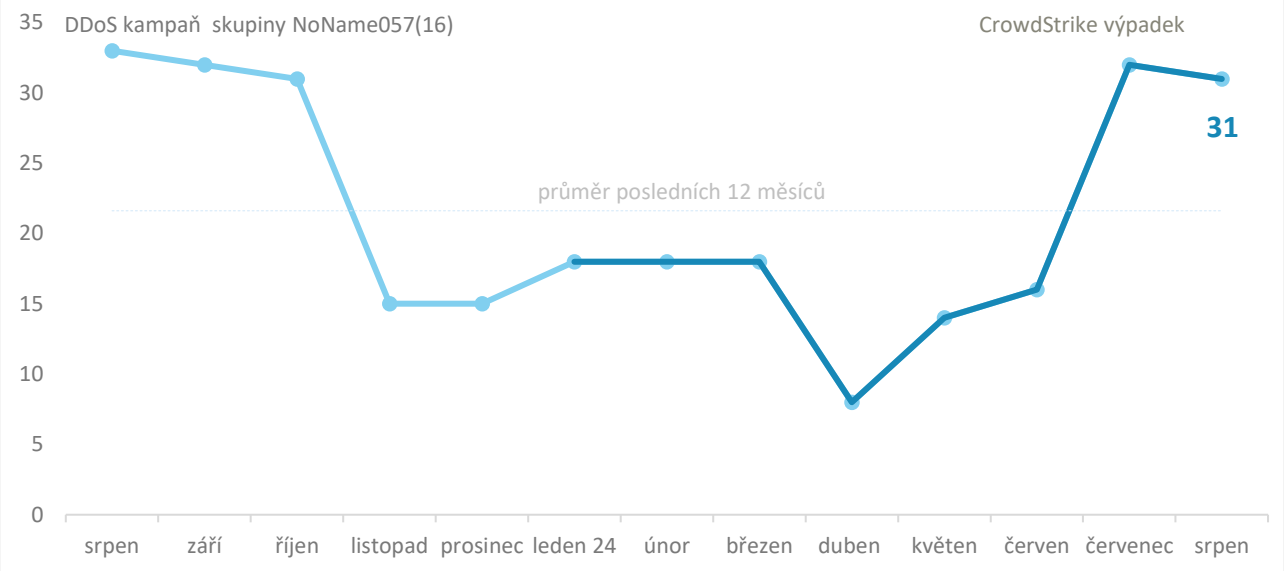
Obsah

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.

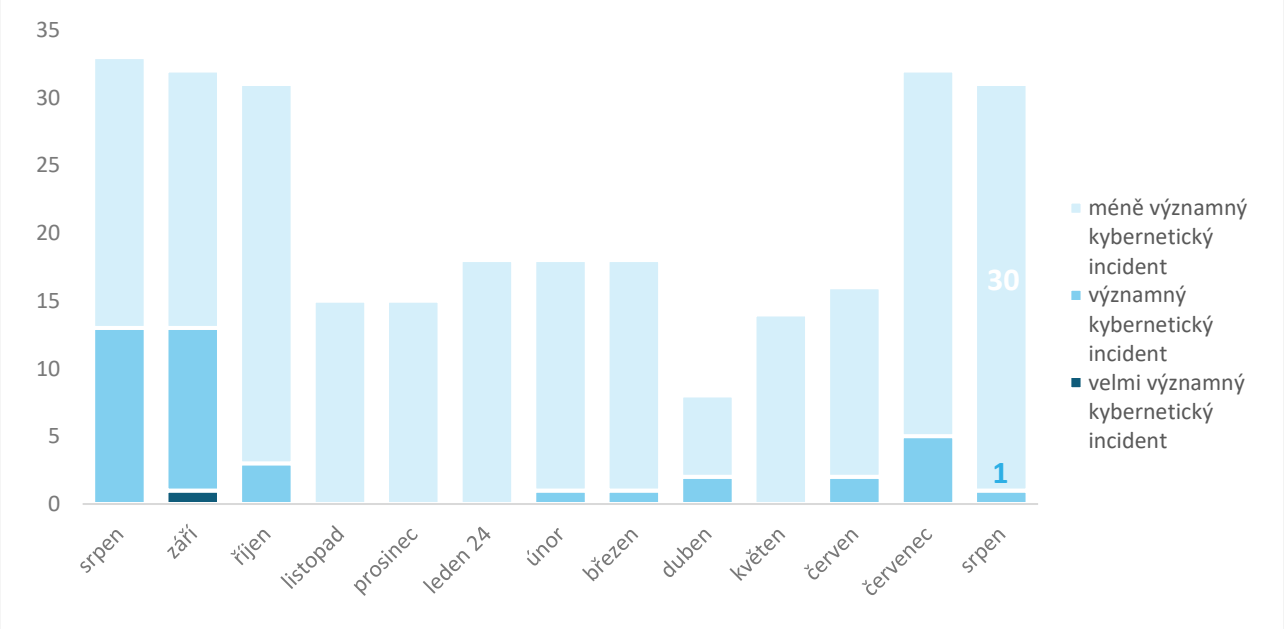
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

V srpnu bylo evidováno 31 incidentů, oba letní měsíce byly tudíž počtem incidentů výrazně nad-průměrné. Za červencový nárůst mohl výpadek EDR softwaru CrowdStrike, za srpnovým poté stojí DDoS kampaň ruskojazyčných hacktivistů.



Závažnost řešených kybernetických incidentů[1]

Pouze jeden z evidovaných incidentů byl vyhodnocen jako významný, zbylých 30 spadá do kategorie méně významných. Znovu se tak ukazuje trend, kdy navzdory vysokému počtu jednotlivých DDoS útoků se nejedná o případy s významnými dopady na jejich oběti.



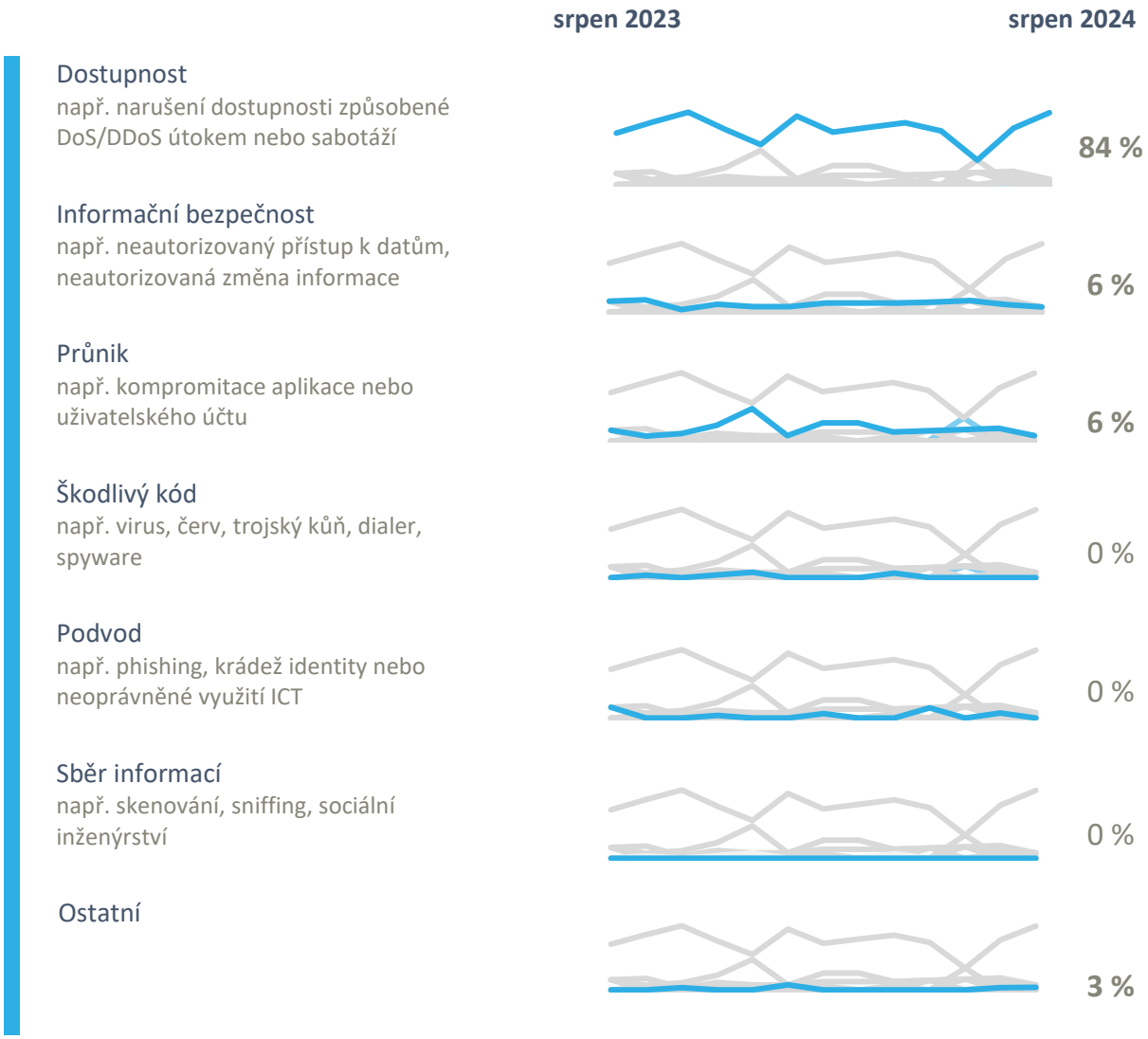
[1] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[2]

Díky vysokému množství srpnových DDoS útoků, a naopak menšímu počtu jiných incidentů, dominuje srpnovému přehledu právě kategorie Dostupnost. Ta kromě více než dvou desítek DDoS či DoS útoků obsahuje i 4 výpadky v důsledku technické závady.

NÚKIB dále řešil incidenty ve dvou kategoriích:

- Dva incidenty spadají do kategorie Informační bezpečnost, přičemž v obou případech se jednalo o ransomwarové útoky. Jeden z útoků byl veden vůči instituci veřejného sektoru a má jej na svědomí skupina White Rabbit. Druhý útok má na svědomí skupina RansomHub.
- V rámci kategorie Průnik evidoval NÚKIB dva incidenty prolomení uživatelských účtů. V jednom případě útočník úspěšně přesvědčil zahraničního klienta napadené společnosti k autorizaci platby falešné faktury, v druhém případě došlo pouze k šíření spamu.



[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 srpnu neeviduje incident, při kterém by došlo k použití phishingu.

Malware

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

Zranitelnosti

Během srpna NÚKIB pokračoval v publikaci zranitelností skrze kanál na sociální síti X, kde byly taktéž zveřejněny informace Digitální a informační agentury (DIA) o škodlivé kampani napodobování vládních webů s cílem získat citlivé informace a finanční prostředky obětí.

Kromě toho došlo i k vydání prohlášení NÚKIB ve spolupráci s Úřadem pro ochranu osobních údajů (ÚOOÚ) upozorňující na e-shopové aplikace sbírající nestandardní množství uživatelských dat.

Ransomware

V srpnu byly evidovány dva případy incidentů spojených s ransomwarem. Jeden z nich má na svědomí skupina White Rabbit a byl veden vůči instituci veřejného sektoru, za druhý incident je zodpovědná skupina RansomHub.

Útoky na dostupnost

V průběhu srpna NÚKIB evidoval více než dvacet DDoS a DoS útoků, které cílily převážně na státní instituce. Za většinou stála ruskojazyčná hacktivistická skupina NoName056(17), u zbytku útočník není znám.

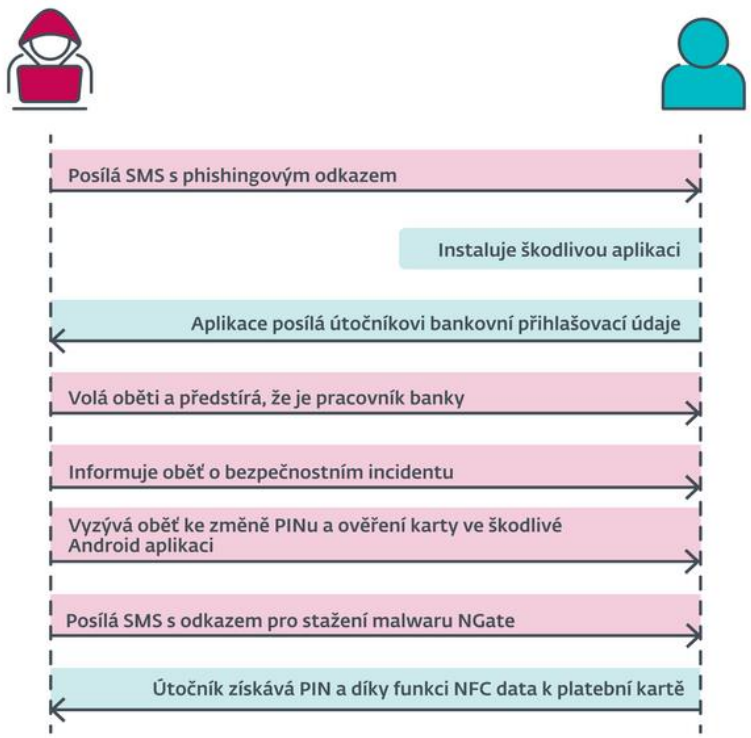
[3] Vývoj ilustrovaný šipkou je vyhodnocován ve vztahu k předešlému měsíci.

Zaměřeno na hrozbu: Malware a podvodná kampaň NGate cílila na české občany

Výzkumníci ze společnosti ESET zaznamenali nový mobilní malware NGate, který cílí na uživatele telefonů s operačním systémem Android a slouží k získání bankovních údajů oběti. **Přestože mělo po zatčení jednoho z členů skupiny dojít k zastavení kampaně, nelze vyloučit (40–50 %), že bude v budoucnu znovu obnovena či napodobena jinými aktéry.**

Tento malware byl zaznamenán v ČR, Maďarsku a Gruzii. V ČR se stali obětí klienti tří nejmenovaných bank. Útočníci přimějí oběť nainstalovat si malware do svého zařízení pomocí phishingu. Po spuštění NGate zobrazí falešnou webovou stránku, která z oběti vyláká její bankovní údaje. Co činí tento malware obzvlášť rizikovým je funkce NFCGate, která dokáže získat i další bankovní údaje skrze NFC technologii využívanou pro bezkontaktní placení v mobilním telefonu. S těmito daty dokáží útočníci kompletně napodobit oběť u bankomatů a následně vybrat hotovost z jejího účtu. Alternativně mohou napodobit NFC komunikaci pro menší bezkontaktní platby. Skrze NFC funkcionalitu může být malware použit i bez instalace do zařízení oběti jako čtečka platební karty kopírující platební data. Získaná data by umožnila jen menší bezkontaktní platby nevyžadující PIN.

Obr. 1: Schéma škodlivé kampaně NGate



Zdroj: eset.com

Podle informací ESET je součástí této kampaně sofistikovaný phishing v několika fázích, jehož cílem je přimět oběť nainstalovat škodlivou aplikaci. Nejlepší cestou, jak se proti tomuto malwaru bránit, je stahovat aplikace pouze z ověřených a legitimních zdrojů. Dále je třeba být obezřetný při zadávání svých bankovních či jiných přihlašovacích údajů. V neposlední řadě je pak vhodné mít nastavené nízké limity na výběr z bankomatu či platbu kartou, které omezí množství peněz, které může útočník odcizit. Je rovněž vhodné hlídat si své bezkontaktní platební karty, aby nemohlo dojít k jejich oskenování, jelikož NFC nefunguje na větší vzdálenosti než 5 cm.

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.