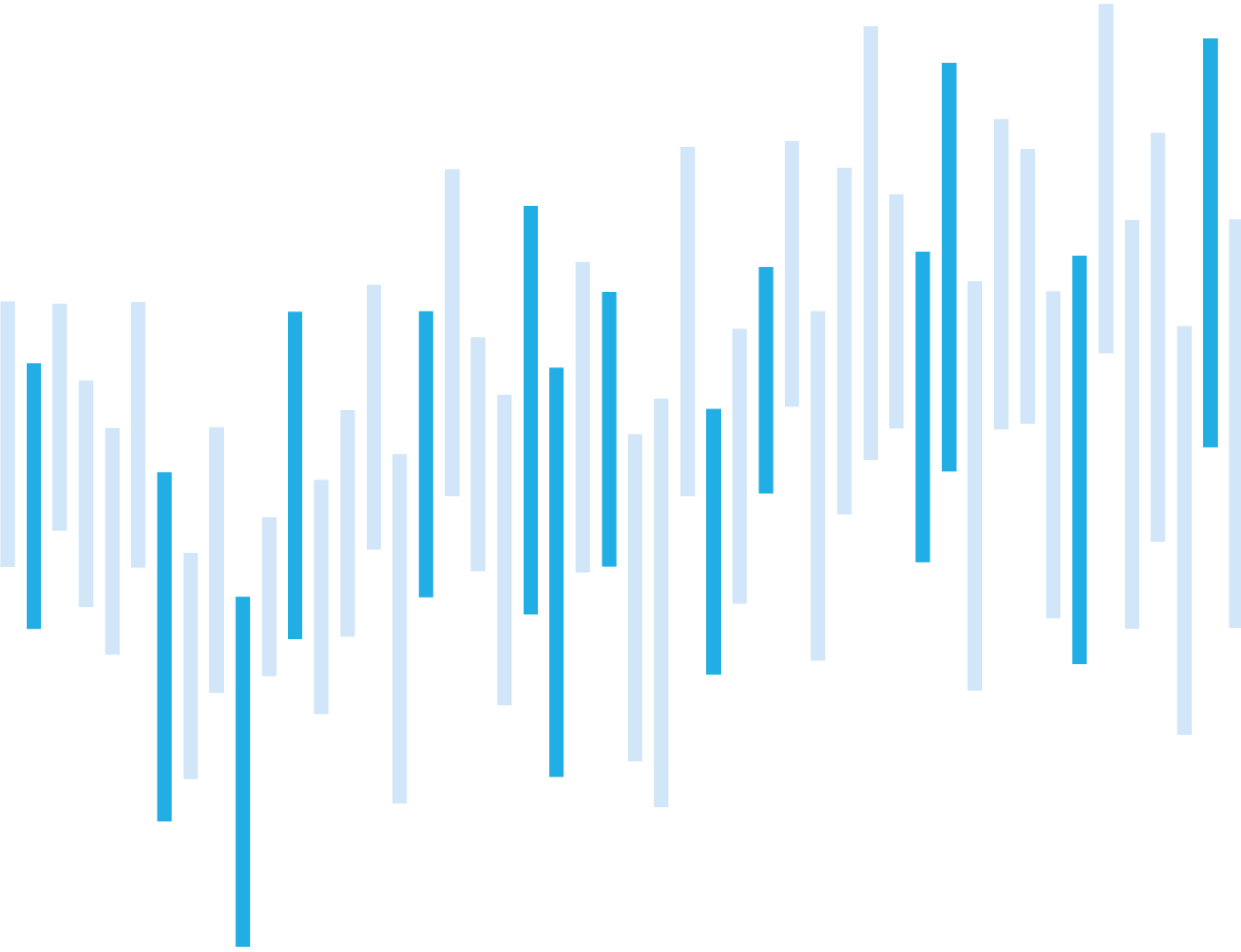
Kybernetické incidenty pohledem NÚKIB

KVĚTEN 2026



Národní úřad
pro kybernetickou
a informační bezpečnost

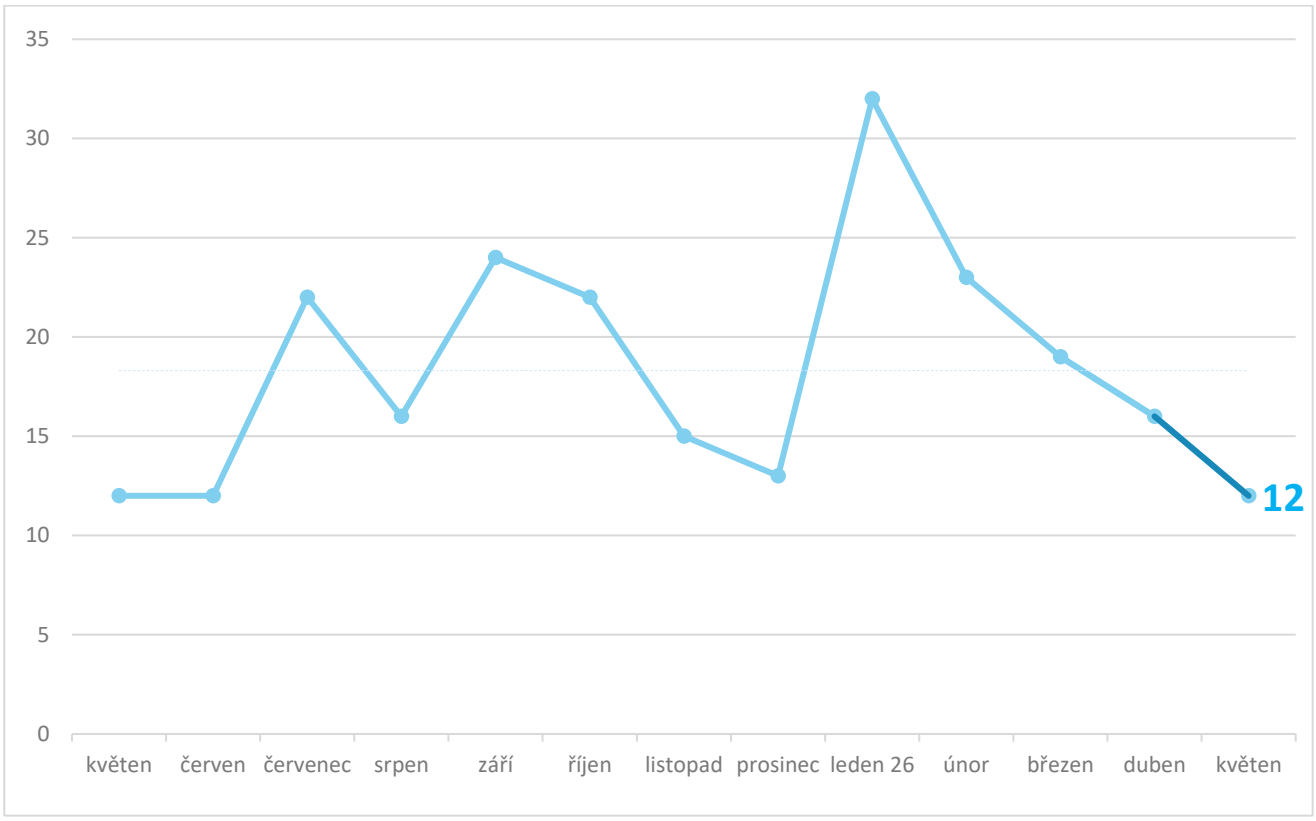
Shrnutí měsíce

Během května NÚKIB zaznamenal celkem 12 kybernetických bezpečnostních incidentů. Květen tak pokračoval v pozitivním trendu setrvalého poklesu incidentů, který trvá již od ledna. Leden byl v tomto ohledu nadprůměrný zejména díky vlně DDoS útoků proruských hacktivistů, kterých však v následujících měsících výrazně ubylo.

Ačkoli DDoS útoky byly za měsíc květen nejčastějším typem incidentu, již několik měsíců se pohybují na úrovni nižších jednotek případů. Vyjma útoků na dostupnost byly incidenty poměrně rozloženy napříč jednotlivými kategoriemi. NÚKIB evidoval případy phishingu, ransomwaru, průniku, škodlivého kódu či úniku informací. Podobně pak kybernetické události zahrnovaly jednotlivé neúspěšné případy phishingu, sociálního inženýrství, pokusu o přihlášení či DDoS útoku. Nejvíce zasaženými subjekty byly instituce z veřejného sektoru.

Květen přinesl nejen pozitivní trend klesajícího počtu incidentů, ale také nižší závažnost. Tento měsíc byl prvním za rok 2026, kdy NÚKIB nezaznamenal žádný významný či velmi významný incident.

Počet kybernetických bezpečnostních incidentů evidovaných NÚKIB



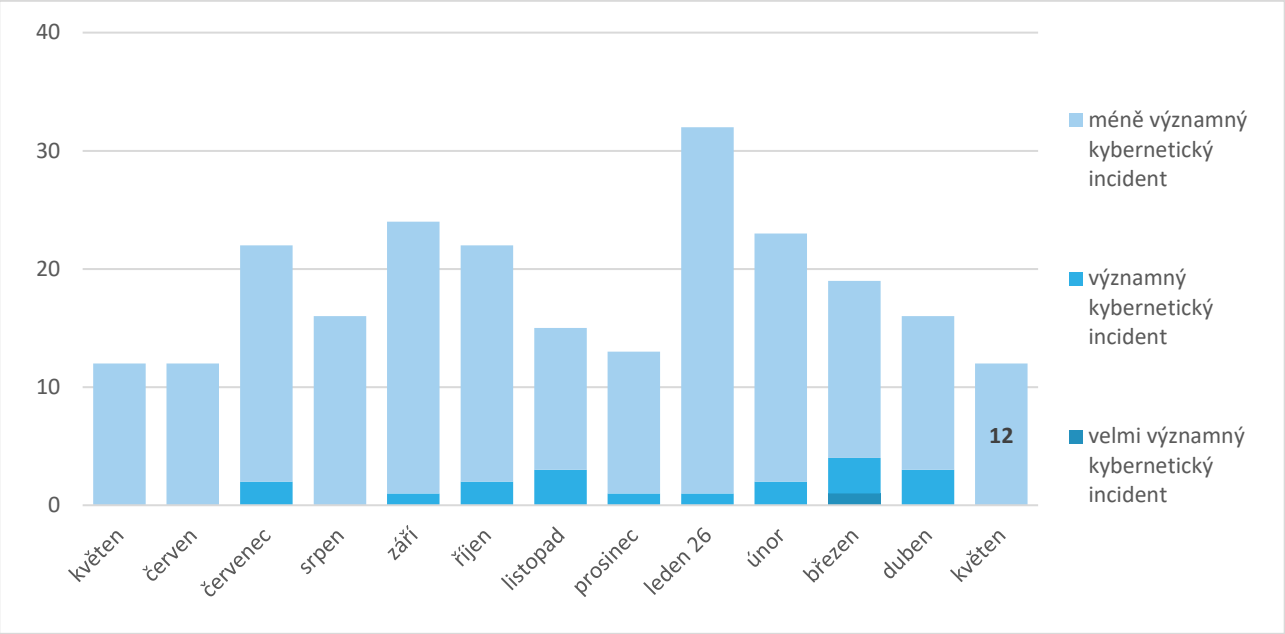
Následující přehled shrnuje dění za daný měsíc. Data, informace a závěry v něm obsažené primárně vychází z evidence NÚKIB. Pokud přehled v některých částech obsahuje informace z otevřených zdrojů, je původ těchto informací vždy uveden.

V některých případech může zpětně docházet k rekvalifikaci hodnot v rámci evidence incidentů, může tedy dojít ke změně historických údajů v zobrazovaných grafech.

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

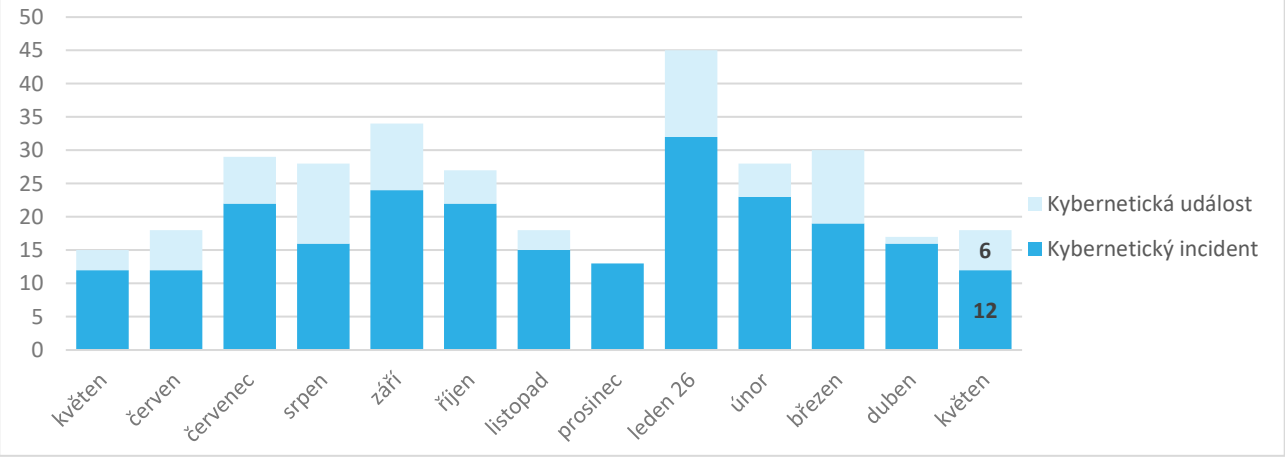
Závažnost evidovaných kybernetických incidentů

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



Poměr evidovaných kybernetických incidentů a kybernetických událostí[2]

NÚKIB v rámci své činnosti přijímá, zpracovává a vyhodnocuje hlášení kybernetických incidentů. Na základě provedené analýzy může být hlášení klasifikováno jako kybernetický incident, kybernetická událost nebo jako nerelevantní podnět. Graf níže ukazuje poměr kybernetických incidentů a kybernetických událostí.



[1] Ve spojení s přechodným ustanovením § 71 odst. 1 zák. č. 264/2025 Sb., zákon o kybernetické bezpečnosti.
[2] Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.
Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.
Oba pojmy definuje Zákon o kybernetické bezpečnosti.

Klasifikace incidentů nahlášených NÚKIB

Klasifikace kybernetických incidentů je založena na taxonomii ENISA: Reference Incident Classification Taxonomy — ENISA (europa.eu). Grafy zobrazují procentuální zastoupení jednotlivých kategorií v daných měsících za uplynulý rok. Procentuální číselná hodnota zobrazuje poměr dané kategorie vůči ostatním v tomto měsíci.

2025 **2026**

Dostupnost – např. narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží

Informační bezpečnost – např. neautorizovaný přístup k datům, neautorizovaná změna informace

Průnik – např. kompromitace aplikace nebo uživatelského účtu

Škodlivý kód – např. virus, červ, trojský kůň, dialer, spyware

Podvod – např. phishing, krádež identity nebo neoprávněné využití ICT

Pokus o průnik

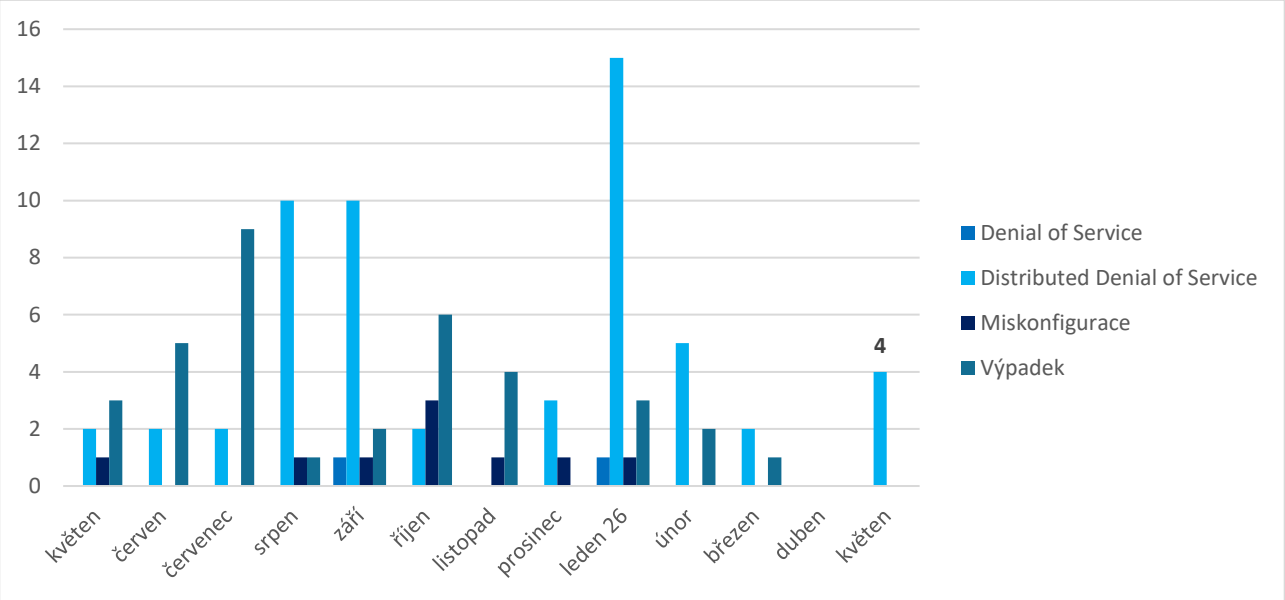
Ostatní

Počet evidovaných incidentů ve vybraných kategoriích

Níže uvedené kategorie jsou vybrány zejména z důvodu jejich dlouhodobé četnosti (Dostupnost) či závažnosti (Informační bezpečnost).

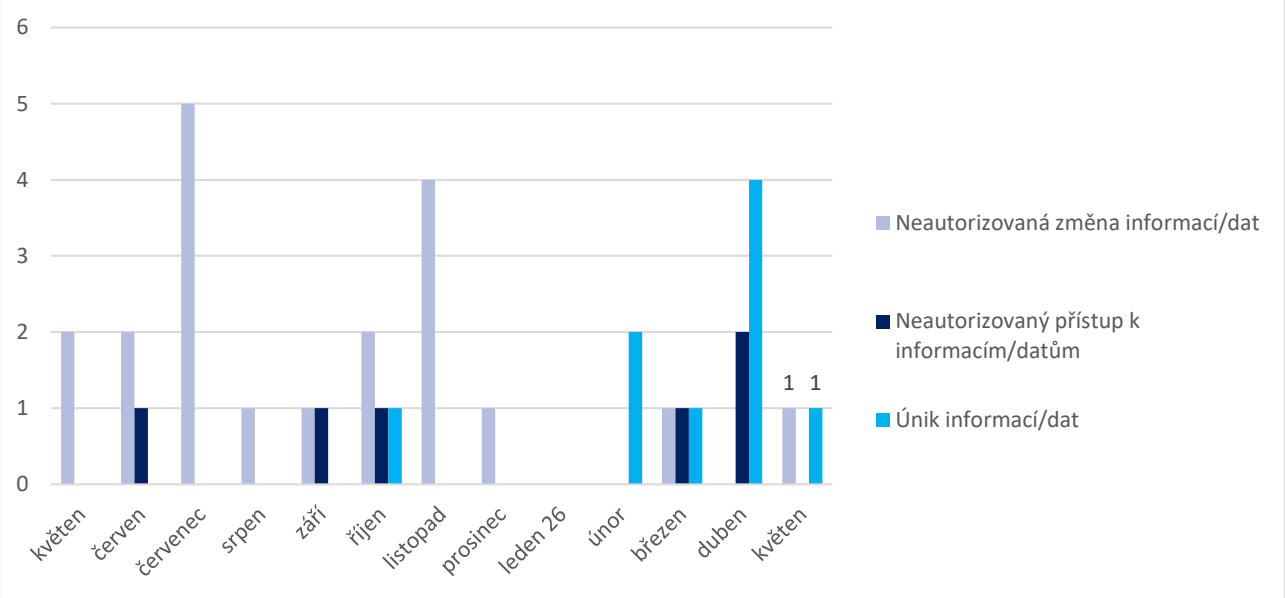
Dostupnost

Kategorie Dostupnost je primárně tvořena DDoS a DoS útoky, nicméně obsahuje i výpadky dostupnosti způsobené technickou závadou či miskonfigurací a neoprávněnou manipulací.



Informační bezpečnost

Kategorie Informační bezpečnost je tvořena primárně ransomwarovými útoky (zpravidla řazenými do podkategorie Neautorizovaná změna informací/dat), nicméně obsahuje také podkategorie Neautorizovaný přístup k datům a systémům či Únik informací.



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 NÚKIB). 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.[i]
TLP:AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují zásady need-to-know.
TLP:GREEN	Informace může být sdílena 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.

[i] need-to-know — princip, který tvrdí, že k informaci mají mít přístup pouze osoby, které danou informaci nutně potřebují ke svojí práci