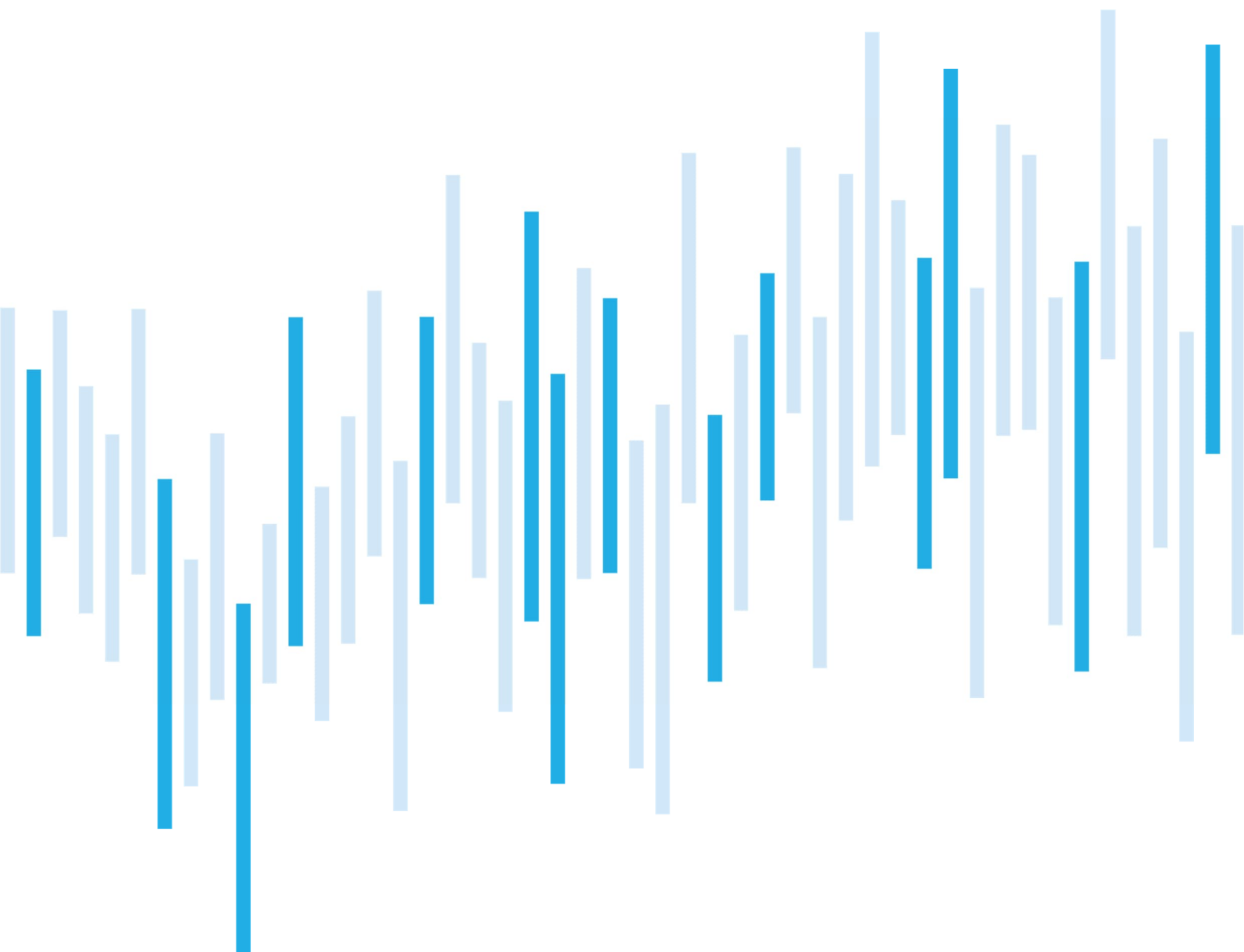


Kybernetické incidenty pohledem NÚKIB

LISTOPAD 2025



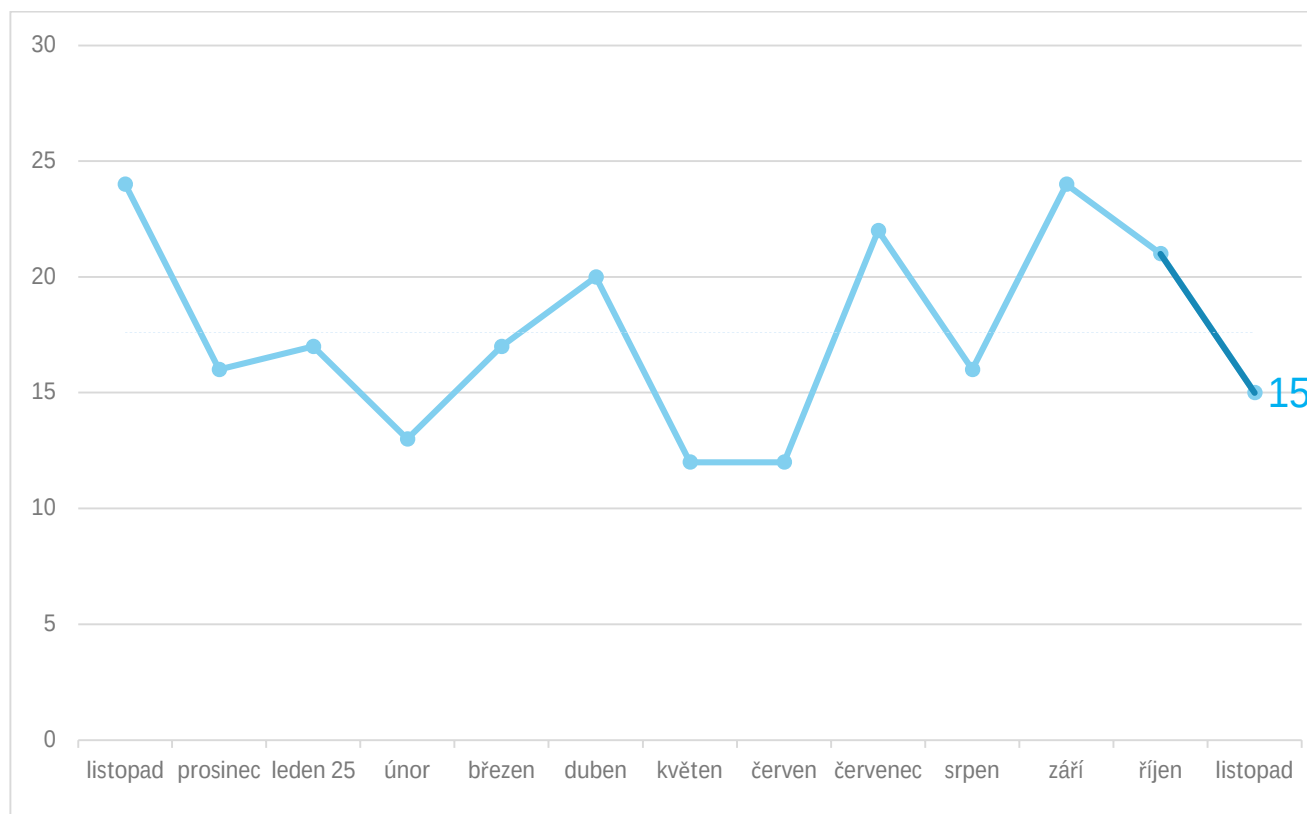
Shrnutí měsíce

V listopadu se počet evidovaných kybernetických bezpečnostních incidentů snížil na podprůměrné hodnoty. Nicméně mírně narostla závažnost – z celkových 15 incidentů NÚKIB zařadil 3 mezi významné. Ty byly tvořeny úspěšnými průniky v rámci státního sektoru.

Co se klasifikace incidentů týče, dominovaly tři kategorie: Dostupnost, Průnik a Informační bezpečnost. V rámci Dostupnosti převažovaly zejména výpadky, přičemž DDos útok NÚKIB neevidoval žádný. Aktivita hacktivistických skupin z pohledu evidovaných incidentů tak zůstaly již druhý měsíc v řadě minimální. Naopak 4 úspěšné ransomwarové útoky představují mírný nárůst oproti předešlým měsícům. Zaznamenány byly například ransomwary Warlock či INC Ransom. V rámci průniků byly evidovány kompromitace VPN, administrátorských účtů, či e-mailových schránek. Nad rámec již výše zmíněných evidoval NÚKIB jeden případ škodlivého kódu u zdravotnického subjektu.

Během listopadu NÚKIB evidoval také podprůměrný počet kybernetických událostí tvořených podezřelou komunikací, pokusem o kompromitaci či neúspěšným DDos útokem.

Počet kybernetických bezpečnostních incidentů evidovaných NÚKIB



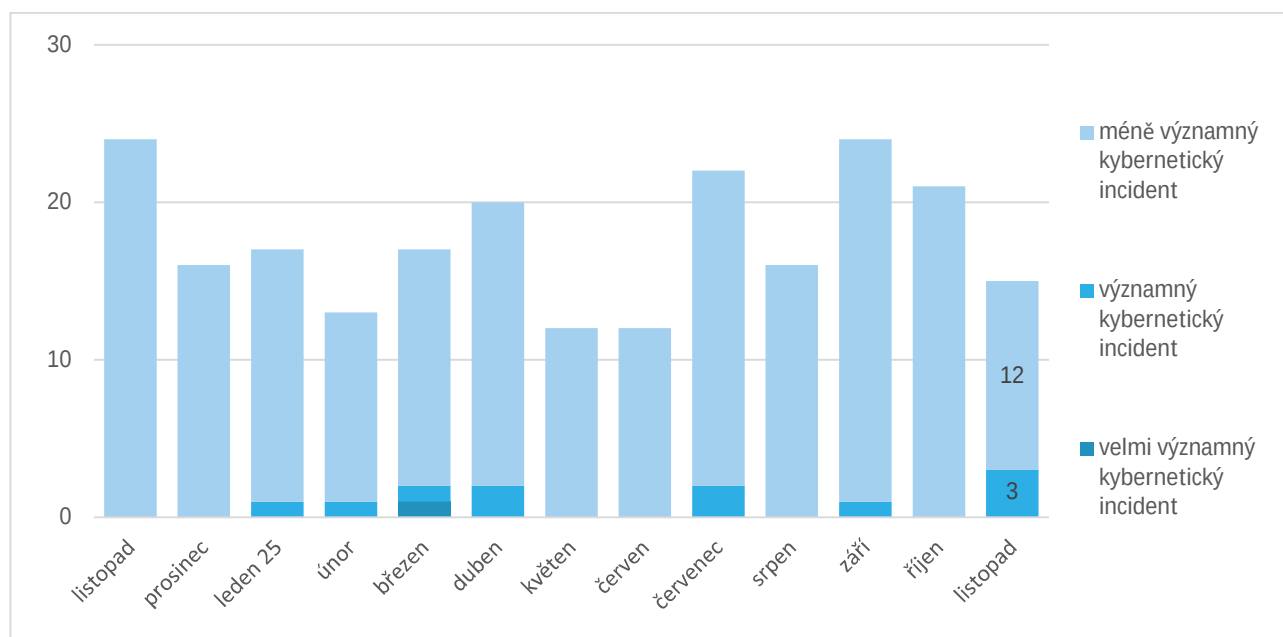
Následující přehled shrnuje dění za daný měsíc. Data, informace a závěry v něm obsažené primárně vychází z evidence NÚKIB. Pokud přehled v některých částech obsahuje informace z otevřených zdrojů, je původ těchto informací vždy uveden.

V některých případech může zpětně docházet k reklasifikaci 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.

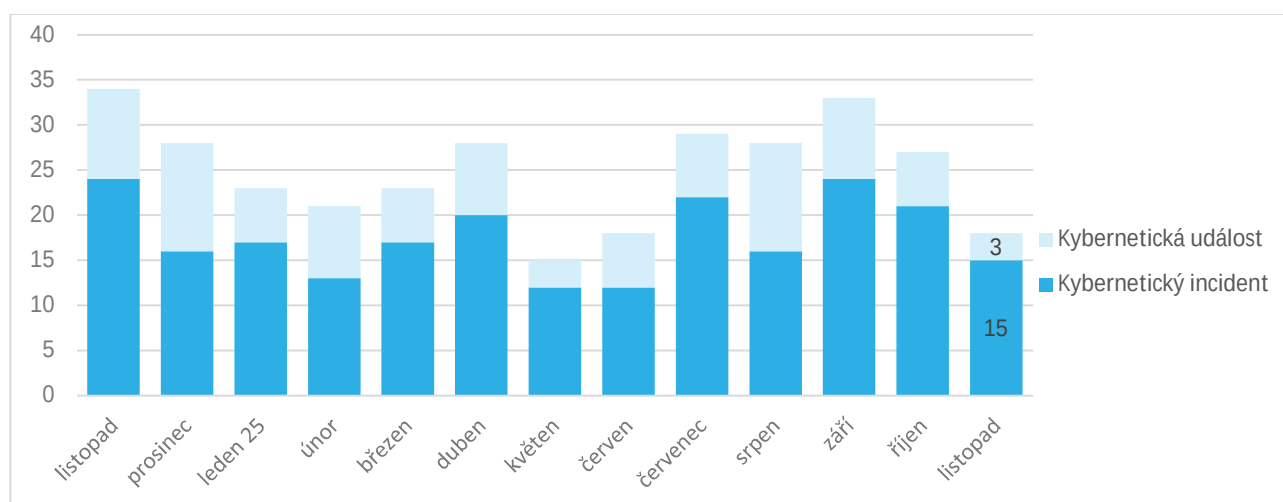
Závažnost evidovaných kybernetických incidentů

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



Poměr evidovaných kybernetických incidentů a kybernetických událostí¹

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 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.

2024

2025

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

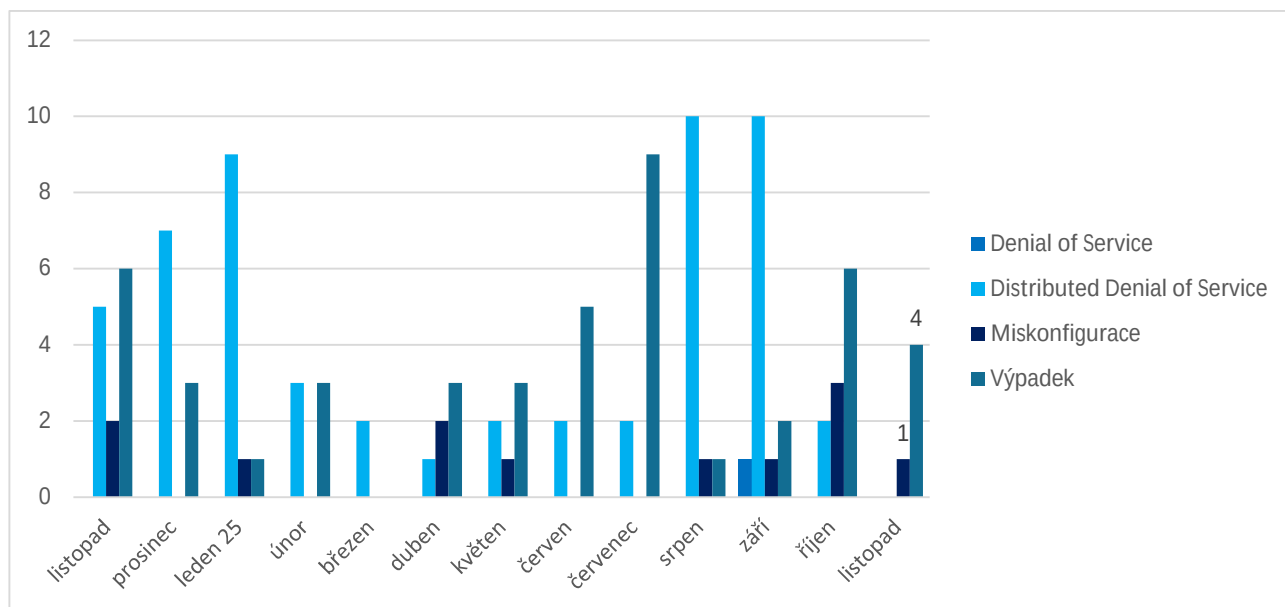


Počet evidovaných incidentů ve vybraných kategoriích

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

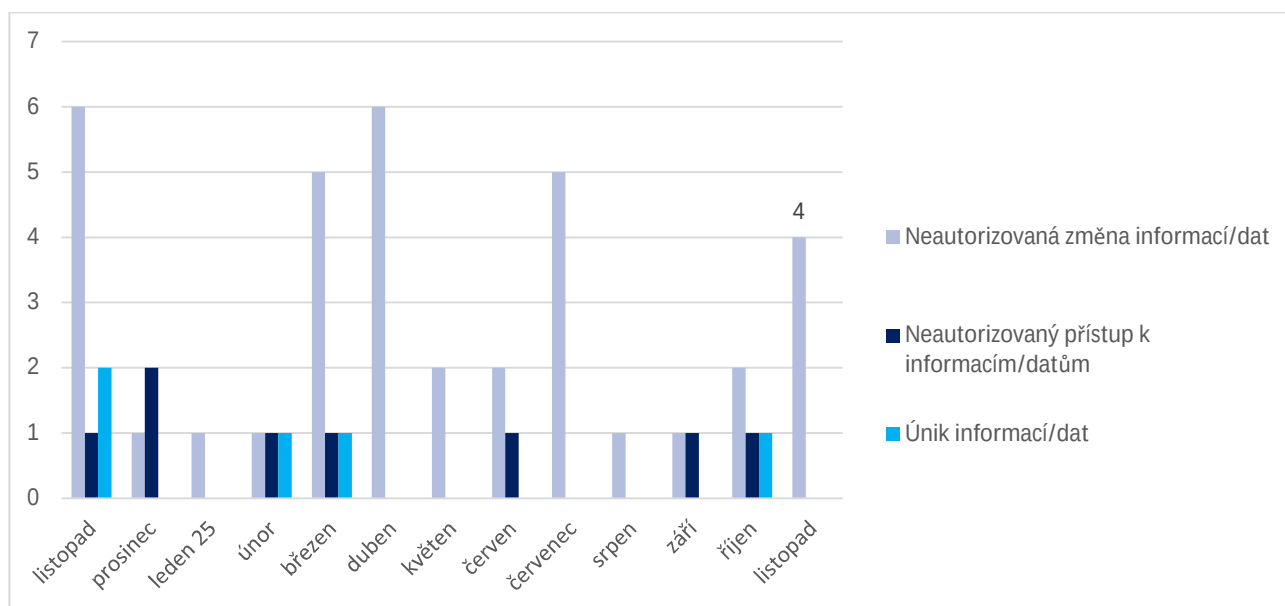
Dostupnost

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 i 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