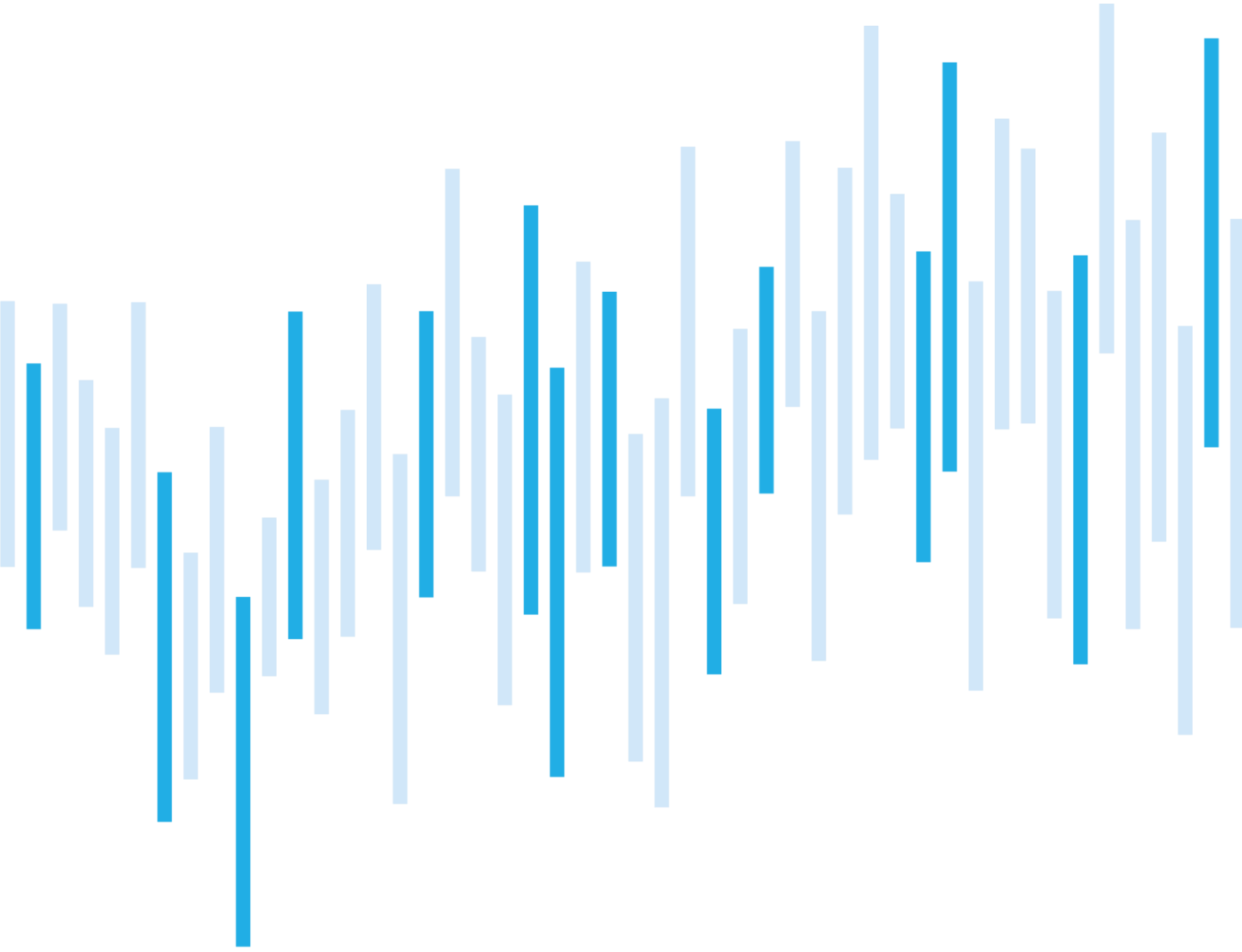
Kybernetické incidenty pohledem NÚKIB

ŘÍJEN 2024



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

V říjnu NÚKIB evidoval 47 incidentů, což je nejvyšší měsíční hodnota za celou dobu evidence. Tři incidenty byly klasifikovány jako významné, zbylých 44 bylo méně významných.

Hlavní kategorií zůstává Dostupnost. V říjnu ji tvořilo 30 DDoS útoků a čtyři výpadky spojené s technickou závadou. Došlo též k evidenci 9 ransomwarových útoků, taktéž nejvyšší historická hodnota.

V kapitole Zaměřeno na hrozbu se tentokrát věnujeme phishingové kampani vůči českým vládním institucím. Útočníci zneužívali identitu společností Amazon a Microsoft, v jednom případě i falešnou doménu české vládní instituce, k šíření škodlivých e-mailů se souborem RDP (Remote Desktop Protocol). Jeho spuštění potenciálně umožňovalo vzdálený přístup do kompromitovaného zařízení. Ačkoliv NÚKIB v tuzemsku evidoval nižší stovky těchto e-mailů, nezaznamenal úspěšnou kompromitaci některého z cílů.

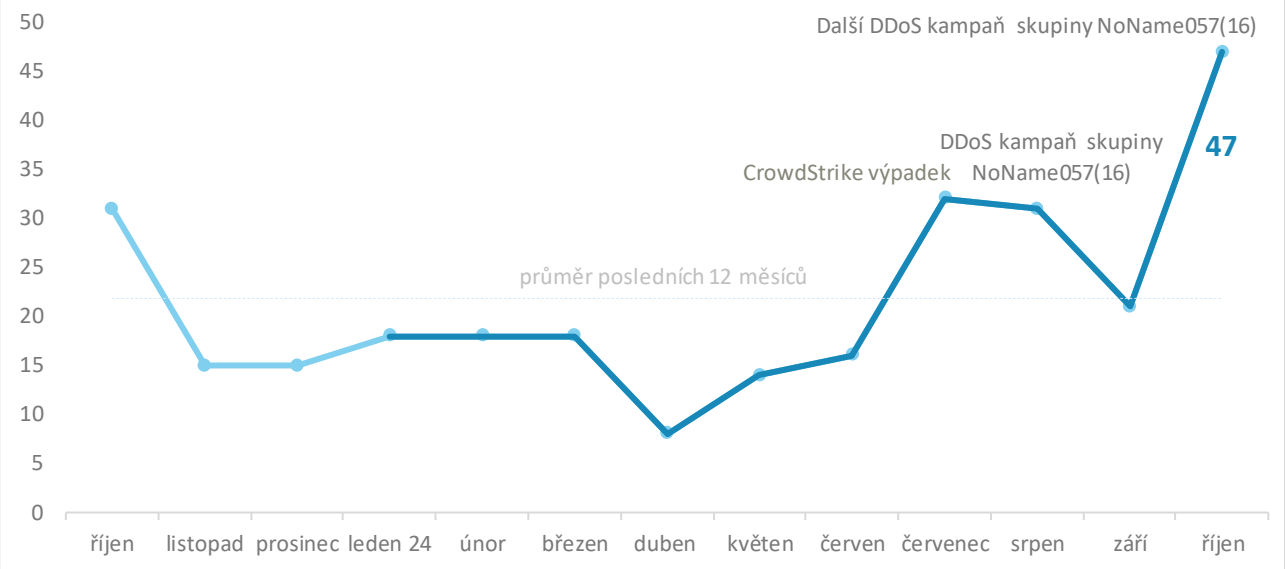
Obsah

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.

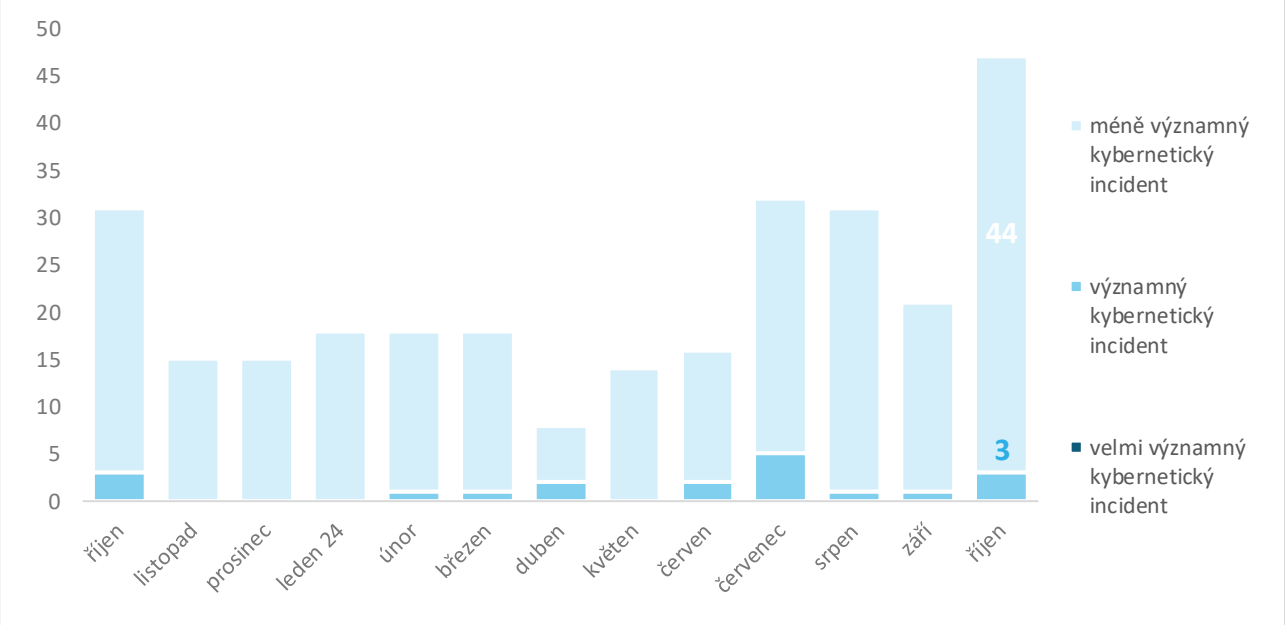
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

V říjnu NÚKIB evidoval 47 incidentů, což je nejvyšší hodnota za uplynulý rok. Vysoký počet byl tentokrát výsledkem zejména další vlny DDoS útoků.



Závažnost řešených kybernetických incidentů[1]

V kontextu závažnosti byly 3 incidenty vyhodnoceny jako významné, zbylých 44 potom spadalo do kategorie méně významných.



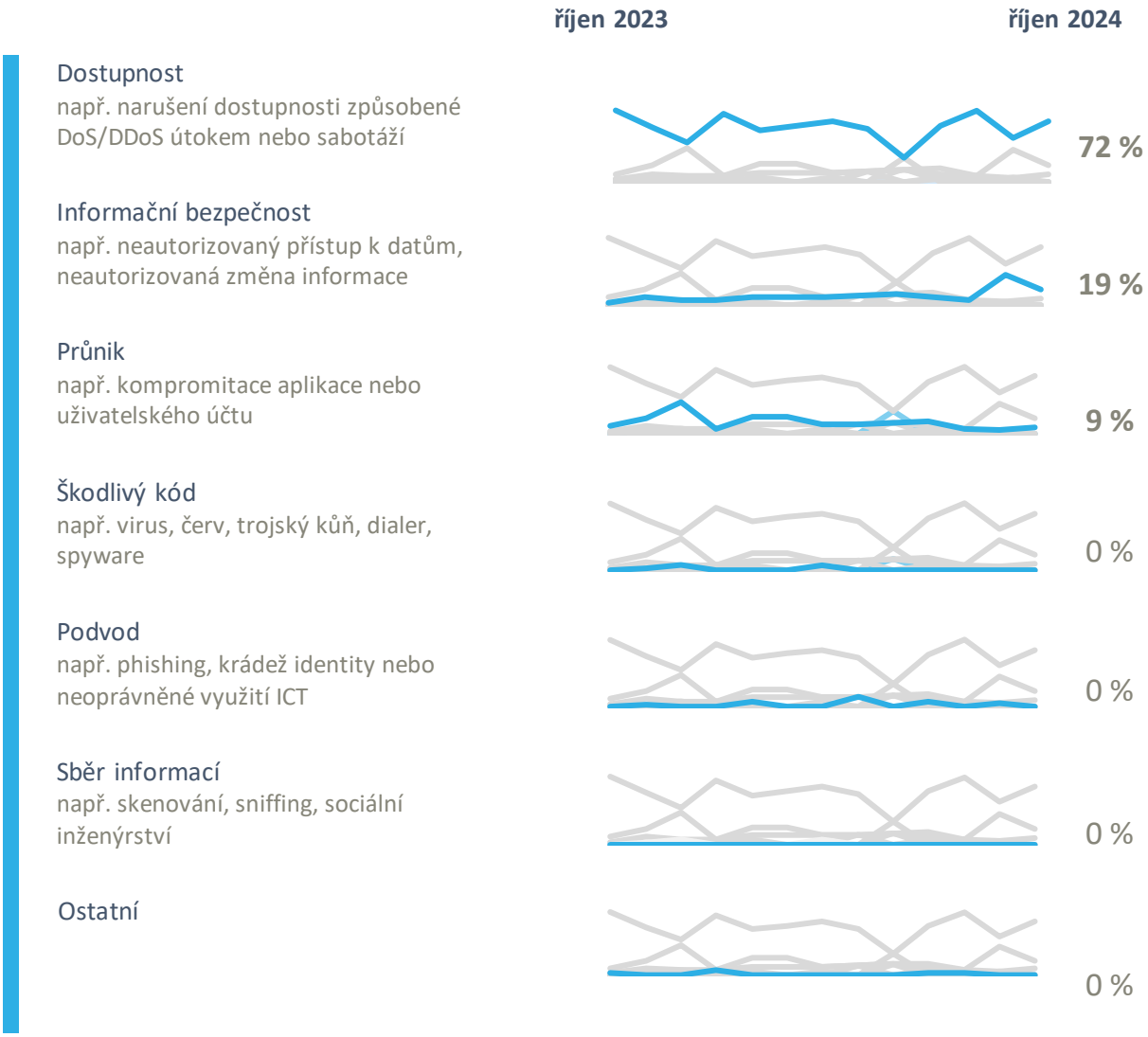
[1] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[2]

Obdobně jako v minulých měsících zůstává nejpočetnější kategorií incidentů Dostupnost. Během října NÚKIB evidoval dosud největší počet DDoS útoků (30) v rámci jednoho měsíce, za většinou stojí ruskojazyčná hacktivistická skupina NoName057(16). Zbytek v rámci kategorie Dostupnosti tvoří 4 výpadky služeb v kontextu technické závady.

NÚKIB dále řešil incidenty ve dvou kategoriích:

- Devět incidentů spadá do kategorie Informační bezpečnost, všechny představují ransomwarové útoky, což je nejvyšší zaznamenaný počet za uplynulý rok. Evidován byl například ransomware Akira, Inc Ransom a C3RB3R. Cílem byly primárně soukromé společnosti, v jednom případě se však jednalo o samosprávu menšího města.
- V rámci kategorie Průnik evidoval NÚKIB 4 incidenty zahrnující prolomení uživatelských účtů. Ve dvou případech se jednalo o kompromitace uživatelských účtů a následné šíření spamu. V dalších případech šlo o kompromitaci systému a webu.



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

Trendy v kybernetické bezpečnosti za září pohledem NÚKIB[3]

Phishing, spear-phishing a sociální inženýrství

NÚKIB v říjnu neevidoval žádný incident s využitím phishingu.

Malware

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

Zranitelnosti

Během října NÚKIB pokračoval v publikaci zranitelností skrze sociální síť X.

Jednalo se například o kritickou zranitelnost ve FortiNetManager CVE-2024-47575 se skórem závažnosti 9,8. Dále bylo upozorněno na sérii zranitelností v produktu Splunk či aktivně zneužívané zranitelnosti FortiOS, která byla odhalena již v únoru.

Ransomware

V říjnu bylo evidováno devět případů ransomwarových útoků. Jednalo se o ransomware Akira, Inc Ransom a C3RB3R. Skupina Inc Ransom přitom útočila na dva české subjekty. U zbylých útoků je druh ransomwaru neznámý.

Útoky na dostupnost

V průběhu října NÚKIB evidoval 30 DDoS útoků. Většina z nich byla provedena ruskojazyčnou skupinou NoName057(16). Přestože stále platí, že dopady těchto útoků jsou nízké, jedná se o největší dosud evidovaný počet v rámci jednoho měsíce.

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

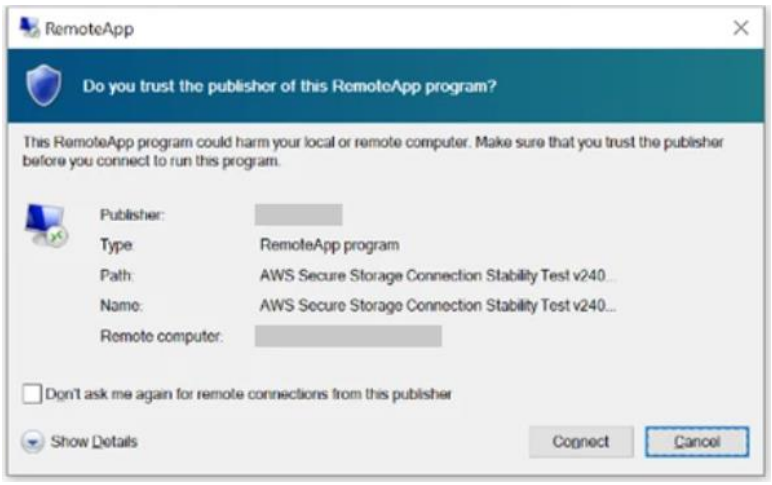
Zaměřeno na hrozbu: Phishingová kampaň cílila na státní instituce, zneužívala identitu společností Amazon, Microsoft a alespoň jedné české instituce

Během 23. října NÚKIB obdržel informace od partnerů o aktivní phishingové kampani neznámého útočníka. **Útoky byly potvrzeny v několika partnerských zemích, včetně nižších stovek zachycených e-mailů v České republice.** NÚKIB evidoval zacílení výhradně na státní instituce, oproti očekávání nedošlo k evidenci útoků na soukromé společnosti.

Kampaň byla založena na rozesílání phishingových e-mailů, které naváděly oběť k otevření škodlivé přílohy ve formátu RDP (Remote Desktop Protocol). Ta měla sloužit k nastavení služby AWS Secure Data Exchange společnosti Amazon pro vzdálenou správu zařízení a odkazoval taktéž na zavádění politiky nulové důvěry (Zero Trust), jakožto bezpečnostního opatření. Reálně však tento soubor, po potvrzení výzvy v dialogovém oknu, spouštěl zdálenou správu mezi kompromitovaným zařízením a infrastrukturou útočníka.

Spuštění škodlivého souboru mělo útočníkům zajistit přístup nejen k úložišti a síťovým zařízením, ale potenciálně i možnost spouštět programy třetích stran či vlastních skriptů. **V případě kompromitace tak útočník mohl získat takřka plnou kontrolu nad napadeným zařízením, které mohlo být využito pro další škodlivé aktivity.** Po otevření souboru se oběti taktéž otevřelo dialogové okno právě s nastavením RDP, které pro zvýšení důvěry v jednom z polí zobrazovalo cílovou doménu, připomínající v případě České republiky jednu z vládních institucí.

Obr. 1: Dialogové okno nastavení RDP. Cenzurovaná pole podle informací NÚKIB mohla obsahovat celou řadu variant různých škodlivých domén, alespoň v jednom případě i doménu zneužívající identitu české vládní instituce.



Zdroj: microsoft.com

V návaznosti na kampaň vydaly společnosti Amazon i Microsoft analýzu kampaně. Oba dokumenty se shodují v širokém zacílení jednotlivých útoků. Cílem měly být tisíce jednotlivých osob ve více než sto organizacích v západních státech, včetně Ukrajiny, a kromě vládních institucí měly být zasaženy i akademické a nevládní organizace. Obě společnosti zároveň přisuzují kampaň ruské APT29 (též známé jako Midnight Blizzard), která podléhá ruské Službě civilní rozvědky (SVR). Cílem útoků měl být sběr zpravodajsky cenných informací a dat.

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.