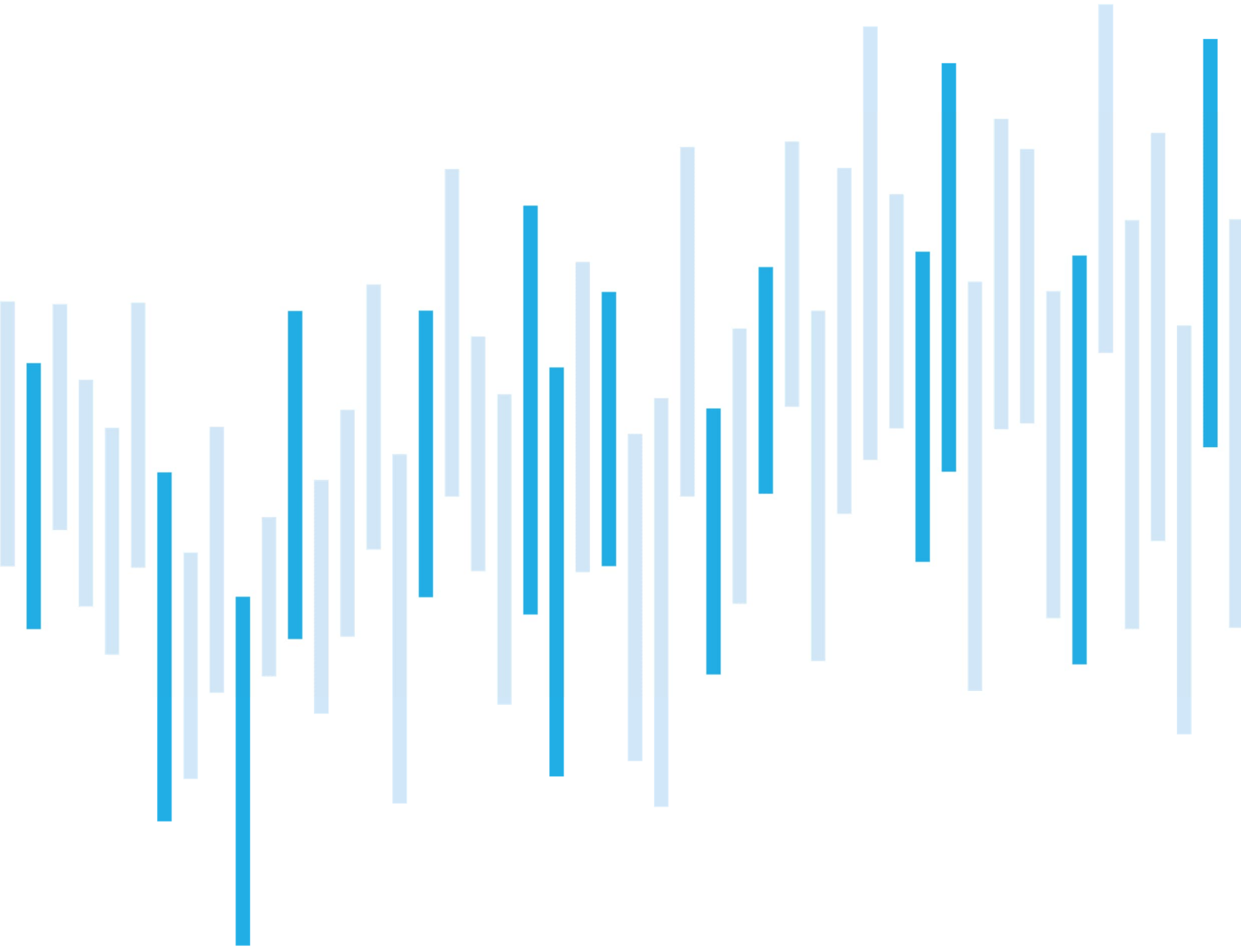
Kybernetické incidenty pohledem NÚKIB

LISTOPAD 2023



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

V listopadu došlo k výraznému poklesu registrovaných incidentů. Ačkoli oproti minulým měsícům nedošlo ke snížení DDoS útoků skupiny NoName057(16), většina z nich nenaplnila kritéria kybernetického bezpečnostního incidentu. Pozitivní trend bylo možné sledovat také v rámci závažnosti incidentů, kdy za celý listopad byly registrovány pouze méně významné kybernetické incidenty.

I když došlo oproti minulým měsícům ke značnému poklesu incidentů z kategorie Dostupnost, v poměrovém výsledku se jednalo opět o kategorii nejpočetnější. Stejně jako v minulých měsících sem spadaly DDoS útoky a některé provozní výpadky. Dále pak NÚKIB řešil incidenty z kategorií Informační bezpečnost a Průnik.

V rámci kapitoly Zaměřeno na hrozbu se tentokrát věnujeme aktérům využívajícím ransomware Phobos, který byl v minulosti již mnohokrát zaznamenán v rámci evidence kybernetických incidentů NÚKIB.

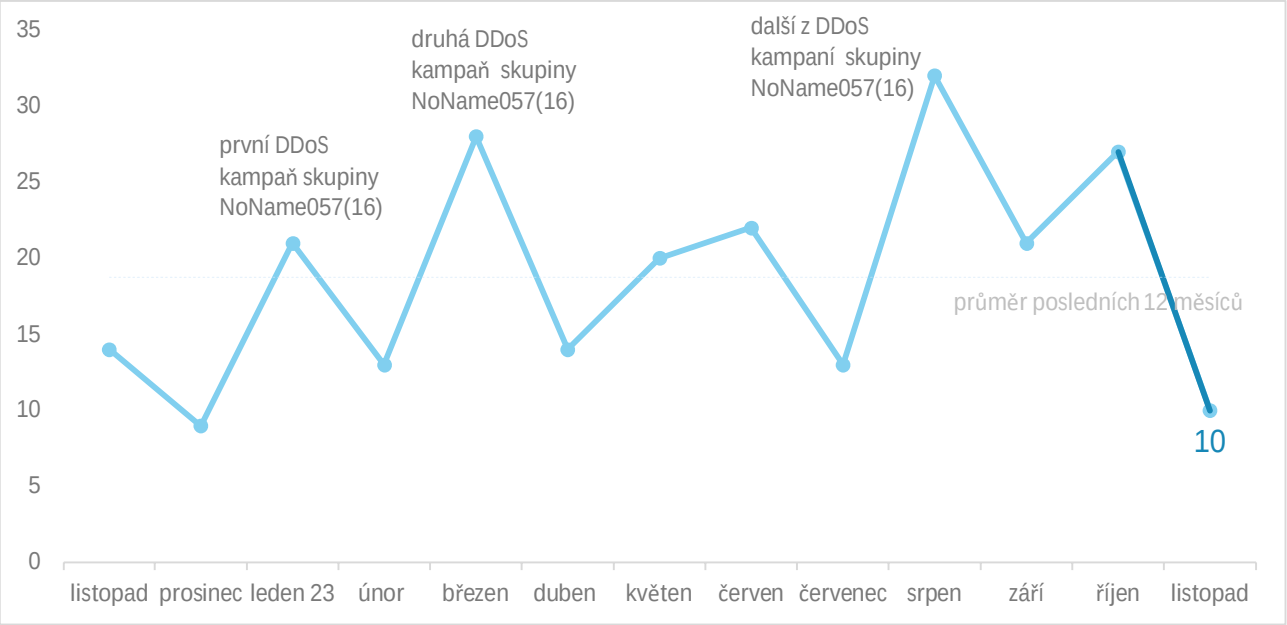
Obsah

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.

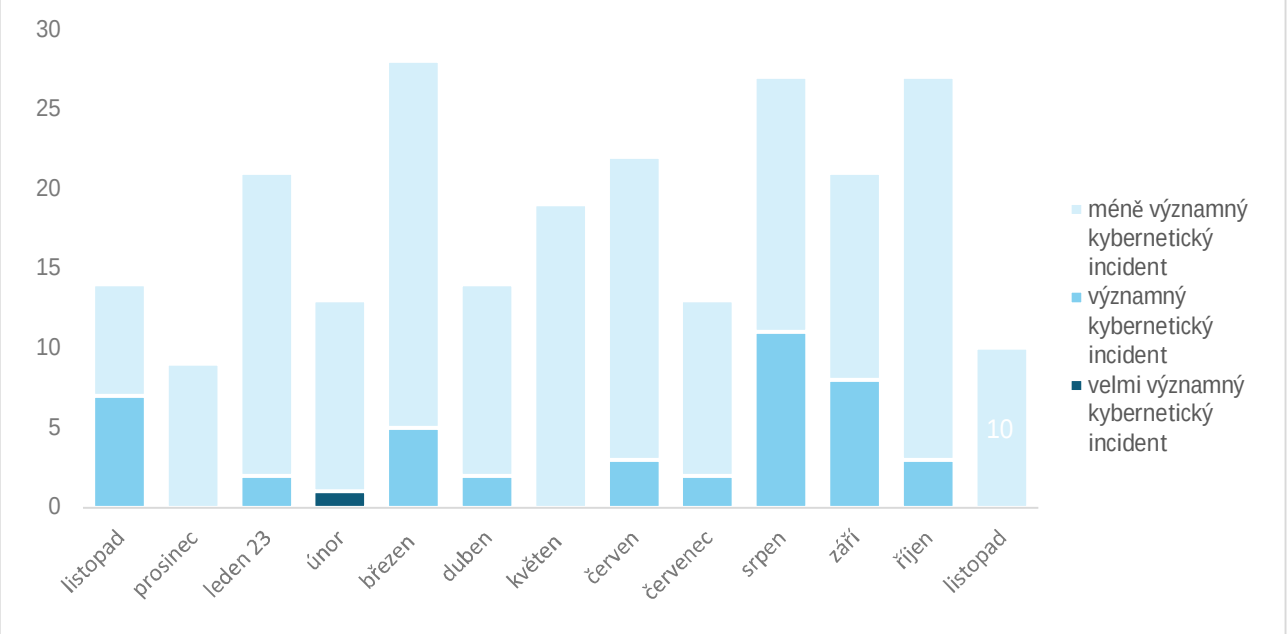
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB[1]

V listopadu došlo k výraznému poklesu registrovaných incidentů. Ačkoli oproti minulým měsícům nedošlo ke snížení počtu DDoS útoků skupiny NoName057(16), většina z nich nenaplnila kritéria kybernetického bezpečnostního incidentu.



Závažnost řešených kybernetických incidentů[2]

NÚKIB během listopadu neevidoval jediný významný či velmi významný incident a v tomto roce se tak jedná teprve o druhý měsíc, kdy byly registrovány pouze méně významné kybernetické incidenty.



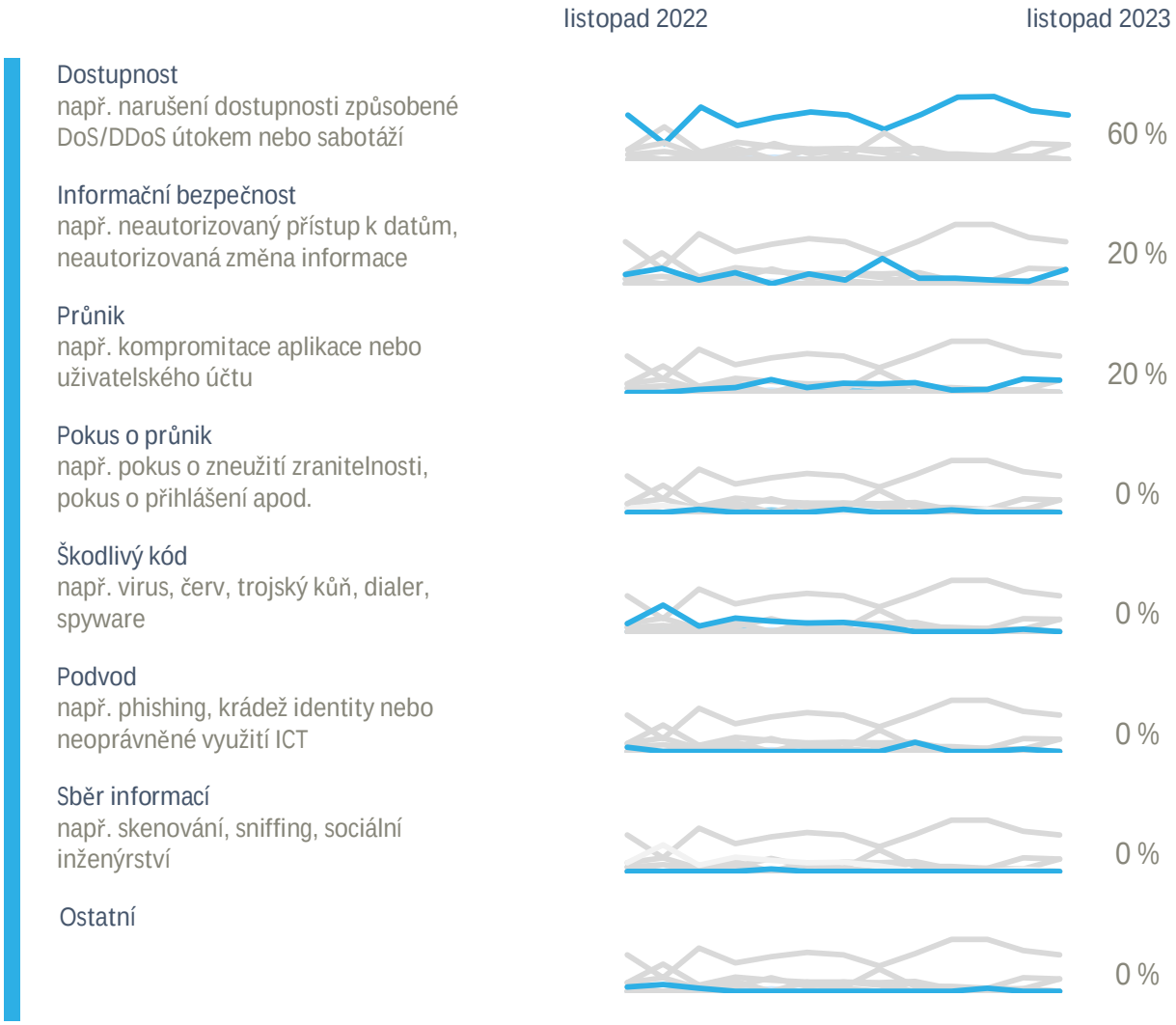
[1] NÚKIB evidoval všech 10 incidentů u povinných osob dle zákona o kybernetické bezpečnosti.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Ačkoli oproti minulým měsícům došlo ke značnému poklesu incidentů z kategorie Dostupnost, v poměrovém výsledku se jednalo opět o kategorii nejpočetnější. Stejně jako v minulých měsících sem spadaly DDoS útoky a některé provozní výpadky.

NÚKIB v průběhu listopadu řešil incidenty v dalších dvou kategoriích:

- NÚKIB během listopadu zaznamenal celkem dva průniky, které zahrnovaly využití nepříliš sofistikovaného phishingu s řadou rozpoznatelných prvků typických pro sociální inženýrství. Navzdory tomu byli útočníci v obou případech úspěšní a podařilo se jim kompromitovat zacílené účty.
- V rámci kategorie Informační bezpečnost došlo ke dvěma úspěšným ransomwarovým útokům u regulovaných subjektů (viz kapitola níže).



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

Trendy v kybernetické bezpečnosti za listopad pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

NÚKIB v listopadu zaregistroval pouze dva incidenty, v rámci kterých bylo potvrzeno využití phishingu. Oba případy vedly k následné kompromitaci účtů a získaný přístup byl následně využit k dalšímu rozesílání phishingových e-mailů z kompromitovaného účtu.

Malware

V listopadu probíhaly kontinuální aktivity v oblasti malwarové analýzy, a to nejen v návaznosti na evidované incidenty, ale také v rámci proaktivní činnosti NÚKIB.

Zranitelnosti

Během listopadu NÚKIB nevydal žádné upozornění týkající se nových zranitelností. Vydal nicméně upozornění na hrozbu spojenou s používáním mobilní aplikace WeChat a její čínské verze Weixin.

Ransomware

NÚKIB evidoval celkem dva incidenty, v rámci kterých byly využity ransomwary Phobos a Cuba. Zatímco Phobos v minulosti cílil na české cíle již mnohokrát, ransomware Cuba byl zaznamenán vůbec poprvé.

Útoky na dostupnost

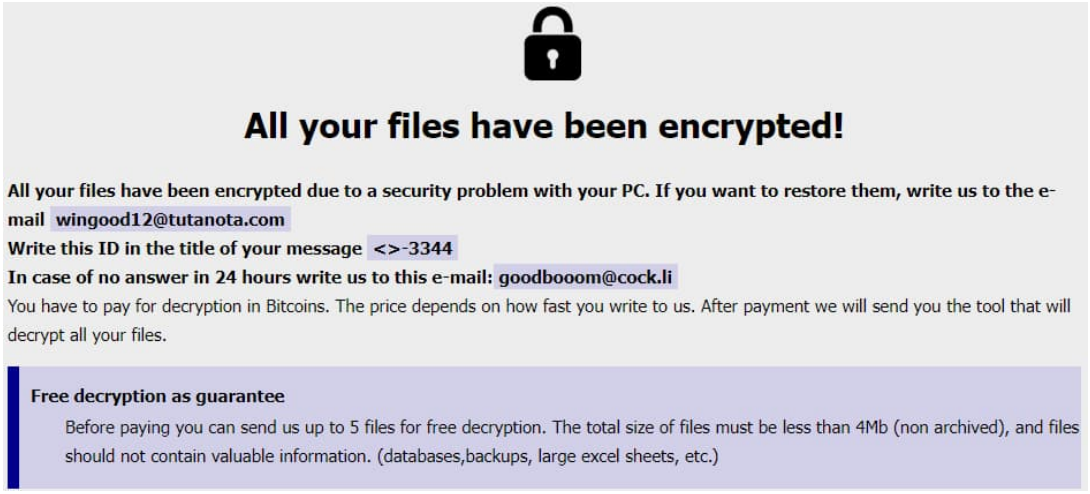
Útoky proruské hacktivistické skupiny NoName057(16) nadále pokračovaly i v listopadu. Ačkoli NÚKIB zaznamenal téměř tři desítky těchto útoků, v kybernetický incident vyústilo jen minimum z nich.

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

Zaměřeno na hrozbu: Analýza aktérů využívajících ransomware Phobos

NÚKIB v listopadu zaregistroval incident spojený s ransomwarem Phobos. Jedná se o ransomware, jehož varianty se v rámci evidovaných incidentů v minulosti vyskytly už mnohokrát. Ransomwarová rodina Phobos je v komunitě poměrně dobře známá a přinejmenším od roku 2019 byla využívána celou řadou aktérů. Bezpečnostní tým Cisco Talos Intelligence Group (CTIG) přišel s novou analýzou zaměřující se právě na aktéry využívající ransomware Phobos.

Obr. 1: Screenshot ransom note ransomwaru Phobos



Zdroj: blog.talosintelligence.com

Dle zjištění CTIG je pravděpodobné, že přinejmenším 5 nejčastěji využívaných variant ransomwaru Phobos (jmenovitě Eking, Eight, Elbie, Devos a Faust) je spravováno jedním aktérem. Napovídají tomu zejména dvě skutečnosti. Phobos se běžně vyhýbá šifrování souborů, které byly již dříve zašifrovány tímto ransomwarem, a to na základě blocklistů přítomných v jeho konfiguračním nastavení. Tyto blocklisty jsou průběžně aktualizovány v návaznosti na proběhlé útoky využívající výše uvedené varianty ransomwaru Phobos. To značí, že dané varianty mohou být spravovány centrální autoritou, která sleduje využívání variant ransomwaru a snaží se zabránit jejich vzájemné kolizi.

Druhým faktorem naznačujícím centrální správu výše zmíněných variant Phobos je pak využití stejného veřejného klíče v konfiguračních datech v rámci analyzovaných vzorků. CTIG usuzuje, že privátní klíč k daným vzorkům drží pouze jeden aktér a že se může jednat o vývojáře daného ransomwaru nabízejícího jej jako službu (Ransomware-as-a-Service, RaaS). Této hypotéze nasvědčuje také vysoké množství kontaktních e-mailů a jiných kontaktních údajů využívaných v rámci útoků ransomwaru Phobos, což naznačuje existenci rozšířené partnerské základny aktérů typické právě pro RaaS. Výše uvedená zjištění mohou mít značný význam pro pochopení činnosti aktérů využívajících ransomware Phobos a pomoci tak ve snaze o prevenci a mitigaci jejich útoků.

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 www.nukib.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, které byla informace poskytnuta.
TLP: AMBER	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám než výše uvedeným, nesmí být informace poskytnuta.
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.