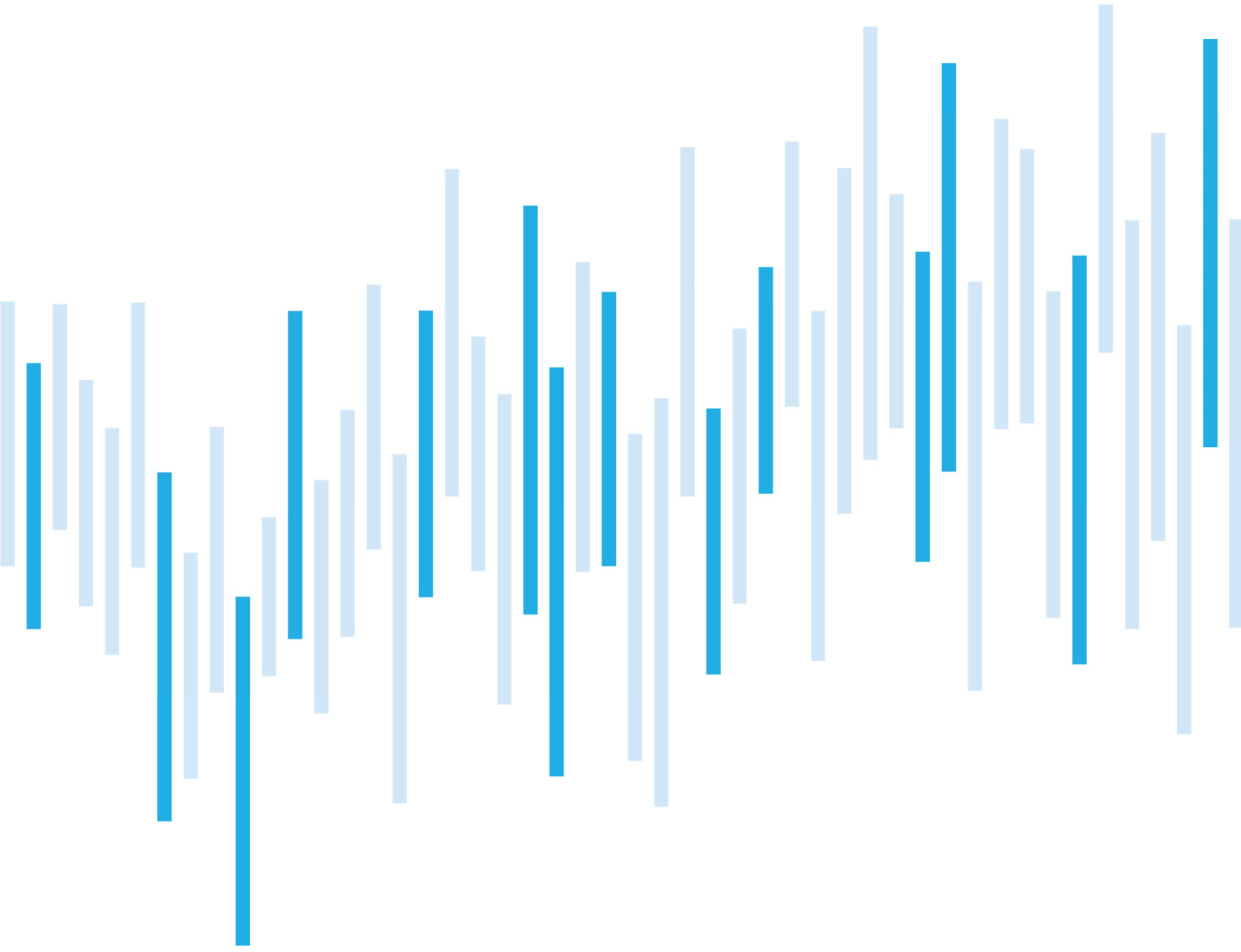
Kybernetické incidenty pohledem NÚKIB

LEDEN 2024



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

V lednu 2024 došlo k mírnému navýšení incidentů oproti prosinci 2023. Navzdory tomu jich NÚKIB již třetí měsíc v řadě evidoval podprůměrný počet. Co se týče závažnosti registrovaných incidentů, kopíroval leden hodnoty předešlých dvou měsíců. Třetí měsíc v řadě tak NÚKIB nezaznamenal žádný významný či velmi významný incident.

Incidenty spojené s dostupností tvořily jednoznačně nejpočetnější kategorii roku 2023, přičemž tento trend pokračoval také v lednu 2024. Dále pak NÚKIB evidoval incidenty v kategoriích Průnik, Informační bezpečnost a Podvod.

Společnost Ivanti v průběhu ledna varovala před několika zranitelnostmi týkajícími se produktů Connect Secure (ICS) a Policy Secure (IPS). Vzhledem k aktivnímu zneužívání ze strany státem podporovaných či jiných aktérů doporučuje NÚKIB okamžitou aktualizaci u dostupných verzí zranitelných produktů či alespoň aplikaci mitigačních opatření u verzí, kde patch prozatím není dostupný.

Obsah

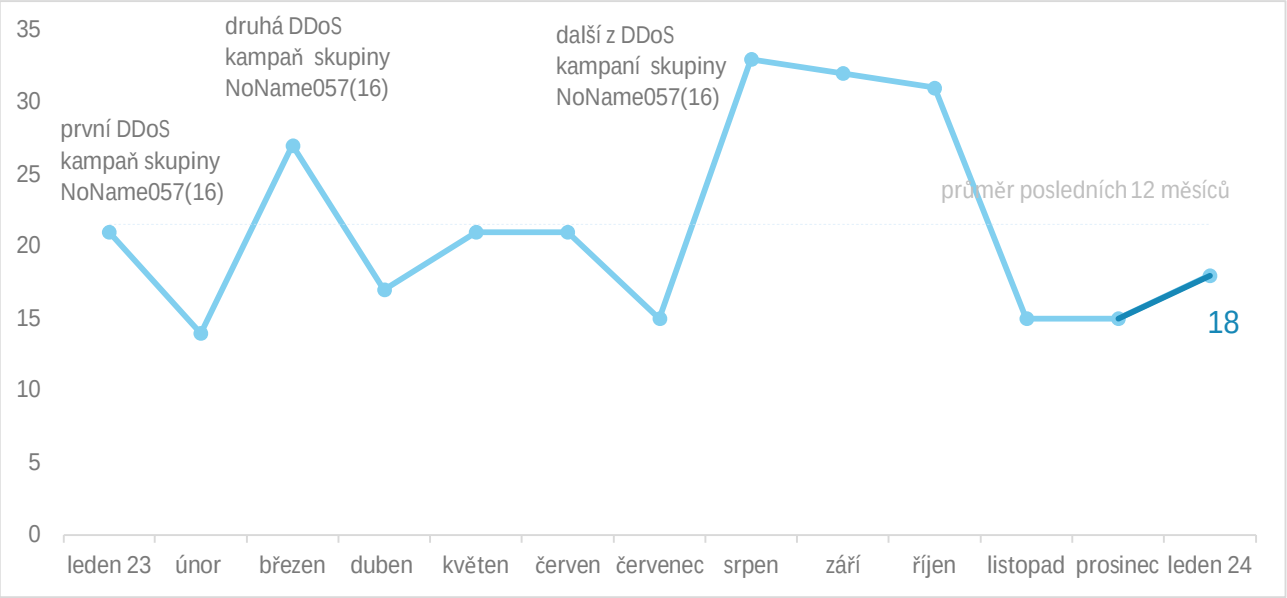
Následující report shrnuje dění měsíce. Data, informace a závěry v něm obsažené primárně vychází z kybernetických incidentů nahlášených NÚKIB. Pokud report v některých částech obsahuje informace z otevřených zdrojů, je vždy uveden původ těchto informací.

Některá data uvedená v tomto přehledu se mohou lišit od přehledů z minulých měsíců. NÚKIB na přelomu roku přistoupil k některým změnám v rámci evidence incidentů, které mírně pozměnily dosavadní statistiky evidovaných incidentů.

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

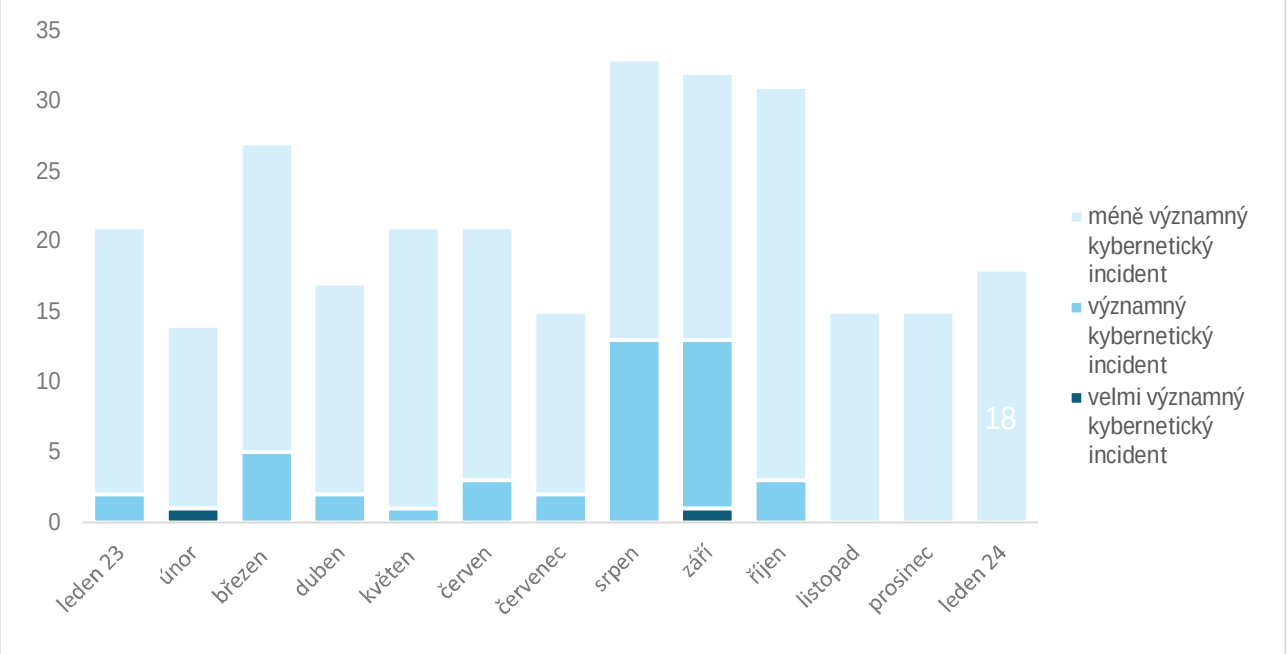
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB[1]

V lednu 2024 došlo k mírnému navýšení incidentů oproti prosinci 2023. Navzdory tomu jich NÚKIB již třetí měsíc v řadě evidoval podprůměrný počet.



Závažnost řešených kybernetických incidentů[2]

Leden co do závažnosti evidovaných incidentů kopíroval hodnoty předešlých dvou měsíců. Již třetí měsíc v řadě tak NÚKIB nezaznamenal žádný významný či velmi významný incident.



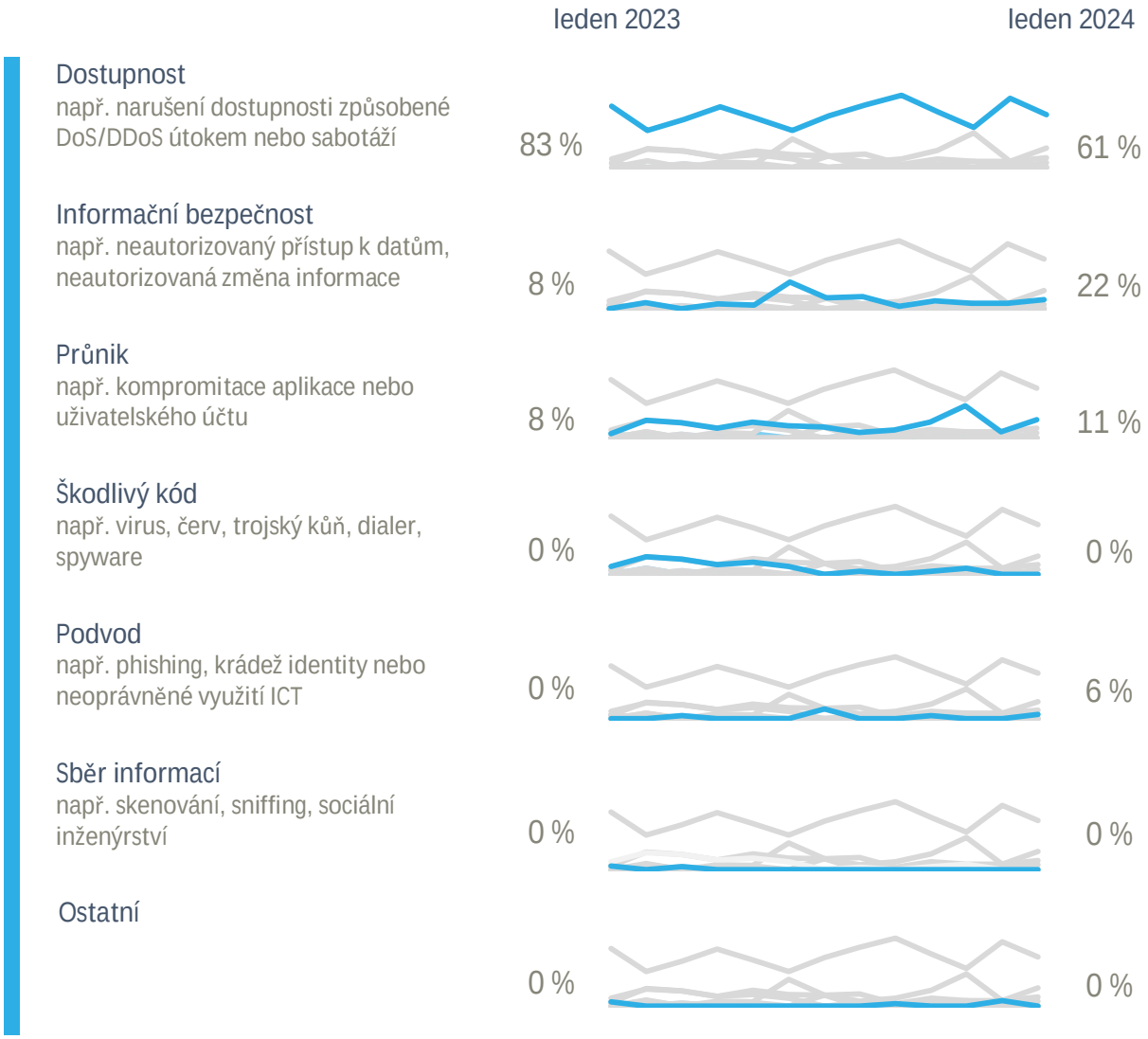
[1] NÚKIB evidoval 14 incidentů u povinných osob dle zákona o kybernetické bezpečnosti. Zbývající 4 incidenty nahlásily NÚKIB neregulované subjekty.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Incidenty spojené s dostupností tvořily jednoznačně nejpočetnější kategorii roku 2023. Tento trend pokračoval také v lednu 2024, ačkoli oproti předešlému měsíci došlo k jejich poměrnému úbytku (viz grafy níže). NÚKIB v rámci kategorie Dostupnost evidoval jak DDoS útoky, tak řadu technických výpadků.

NÚKIB pak v lednu řešil incidenty v dalších třech kategoriích:

- Během ledna byly zaregistrovány celkem 4 případy průniku. Pouze jeden zaregistrovaný případ souvisel se zranitelnostmi produktů Ivanti (viz kapitola Zaměřeno na hrozbu).
- NÚKIB v rámci kategorie Informační bezpečnost zaznamenal jeden ransomwarový útok a dále jeden specifický případ, v rámci kterého měli útočníci zcizit a následně nabízet data subjektu skrze kompromitaci jejího dodavatele.
- Jeden registrovaný případ podvodu zahrnoval phishingový e-mail se škodlivým odkazem cílený na vyšší desítky zaměstnanců regulovaného subjektu.



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

Trendy v kybernetické bezpečnosti za leden pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

NÚKIB v lednu zaregistroval několik případů phishingu, během kterých se útočníkům podařilo kompromitovat zacílené účty, či alespoň získat přihlašovací údaje obětí.

Malware

V lednu podobně jako v uplynulých měsících probíhaly kontinuální aktivity v oblasti malwarové analýzy se zaměřením na vybrané incidenty.

Zranitelnosti

NÚKIB na začátku ledna upozornil na hrozbu Terrapin útoku mířícího na SSH protokol a využívajícího zranitelnost CVE-2023-48795. Většina vývojářů SSH klientů již vydala bezpečnou verzi, na kterou doporučujeme aktualizovat server i klienta.

Do obecného povědomí se do velké míry zapsaly také zranitelnosti produktů Ivanti, kterým se věnuje kapitola Zaměřeno na hrozbu.

Ransomware

V lednu byl stejně jako v prosinci evidován pouze jeden incident spojený s ransomwarem, a to u neregulovaného subjektu. NÚKIB se prozatím nepodařilo ověřit, o jaký typ ransomwaru se jednalo.

Útoky na dostupnost

V průběhu ledna NÚKIB evidoval vyšší jednotky DDoS útoků. Za některými útoky stály proruské hacktivistické skupiny, nicméně u většiny útoků nebyl jejich původce známý.

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

Zaměřeno na hrozbu: Zneužívání zranitelností VPN produktů Ivanti

Společnost Ivanti 10. ledna 2024 varovala před dvěma zero-day zranitelnostmi týkajícími se produktů Connect Secure (ICS) a Policy Secure (IPS). Kombinací obou zranitelností může neautentizovaný útočník spouštět příkazy na všech podporovaných verzích ICS VPN a IPS network access control řešeních. Zranitelnosti s označením CVE-2023-46805 a CVE-2024-21887 měly být již v době oznámení aktivně zneužívány vůči více než desítce zákazníků Ivanti. Podle společnosti Volexity měl za touto aktivitou stát prozatím neznámý čínský aktér.

Krátce po zveřejnění bylo zaznamenáno masivní zneužívání těchto zranitelností po celém světě. Již 15. ledna měla společnost Volexity podezření na nejméně 1700 kompromitovaných zařízení. Americká Agentura pro kybernetickou a infrastrukturní bezpečnost (CISA) později upozornila na rozsáhlé zneužívání zranitelností řadou aktérů. V průběhu vyšetřování společnost navíc objevila další dvě zranitelnosti CVE-2024-21888 a CVE-2024-21893, přičemž druhá zmíněná již měla být zneužita vůči některým zákazníkům.

Obr. 1: Lednový vývoj reakcí společnosti Ivanti týkající se zveřejněných zranitelností

Edit 1: January 10 - fixed linking to XML instructions

Edit 2: January 11 - Update to XML mitigation impacts

Edit 3: January 12 - Update to reflect factory reset recommendation for impacted appliances.

Edit 4: January 13 - New ICT Version for 22.x R2 to address a bug preventing ICT from running on certain Microsoft Azure appliances.

Edit 5: January 14 - Updated patch version and timing information for Ivanti Policy Secure

Edit 6: January 15 - Update to customer impact FAQ and NEW Recovery Guidance linked HERE

Edit 7: January 20 - Update workaround section about known race condition when pushing device configurations.

Edit 8: January 26 - Updated patch timing information

Edit 9: January 31 – Patch availability update and disclosure of CVE-2024-21888 and CVE-2024-21893

Edit 10: January 31 – Known issue with downloads portal is addressed. Please clear your cache and retry if errors persist. Corrected CVE# in description. Added new FAQs

Zdroj: forums.ivanti.com

Bezpečnostní patch ke všem zmíněným zranitelnostem poskytla společnost Ivanti se zpožděním až 31. ledna, a to pouze pro vybrané verze. Další patche mají být vydávány postupně v následujících týdnech. Aktuálně je pro tyto verze dostupný alespoň návod pro mitigaci zranitelností.

Vzhledem k aktivnímu zneužívání ze strany státem podporovaných či jiných aktérů doporučuje NÚKIB okamžitou aktualizaci u dostupných verzí zranitelných produktů či alespoň aplikaci mitigačních opatření u verzí, kde patch prozatím není dostupný.

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.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.