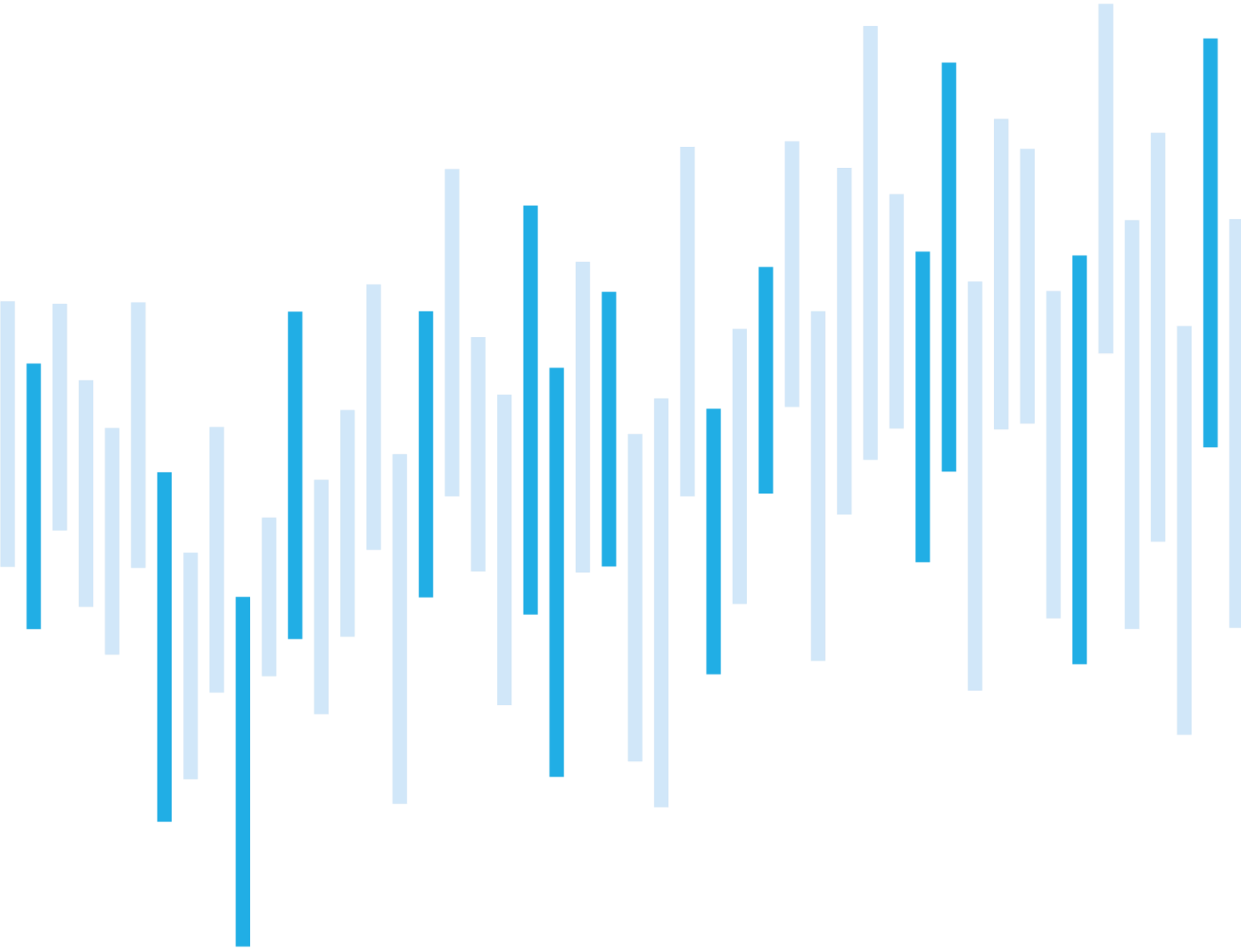
Kybernetické incidenty pohledem NÚKIB

ČERVEN 2024



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

V červnu NÚKIB evidoval 16 incidentů, o dva více než během května. Pokračuje tedy pozvolný nárůst incidentů, přestože celková hodnota se stále drží pod průměrem uplynulého roku. Dva incidenty byly klasifikovány jako významné, zbylých 14 incidentů pak spadalo do kategorie méně významných.

Po dvou měsících se opět objevily i DDoS útoky, kterých NÚKIB za měsíc červen eviduje pět, všechny mířily vůči bankovnímu sektoru. Dále NÚKIB evidoval například dva ransomwarové útoky, spear-phishingovou kampaň či únik interních dat.

V kapitole Zaměřeno na hrozbu se tentokrát věnujeme osvětovému tématu v kontextu nejmladších uživatelů. Během letních prázdnin totiž obvykle roste počet útoků vůči této cílové skupině. Je to dáno zejména zvýšenou aktivitou dětí v kyberprostoru během prázdnin, přičemž jako jeden z hlavních vektorů lze označit například falešné aplikace, které mohou obsahovat různé druhy malwaru. Kapitola proto obsahuje sadu obecných tipů, jak se těmto hrozbám vyvarovat, spolu s odkazy na vzdělávací materiály NÚKIB i pro nejmladší uživatele.

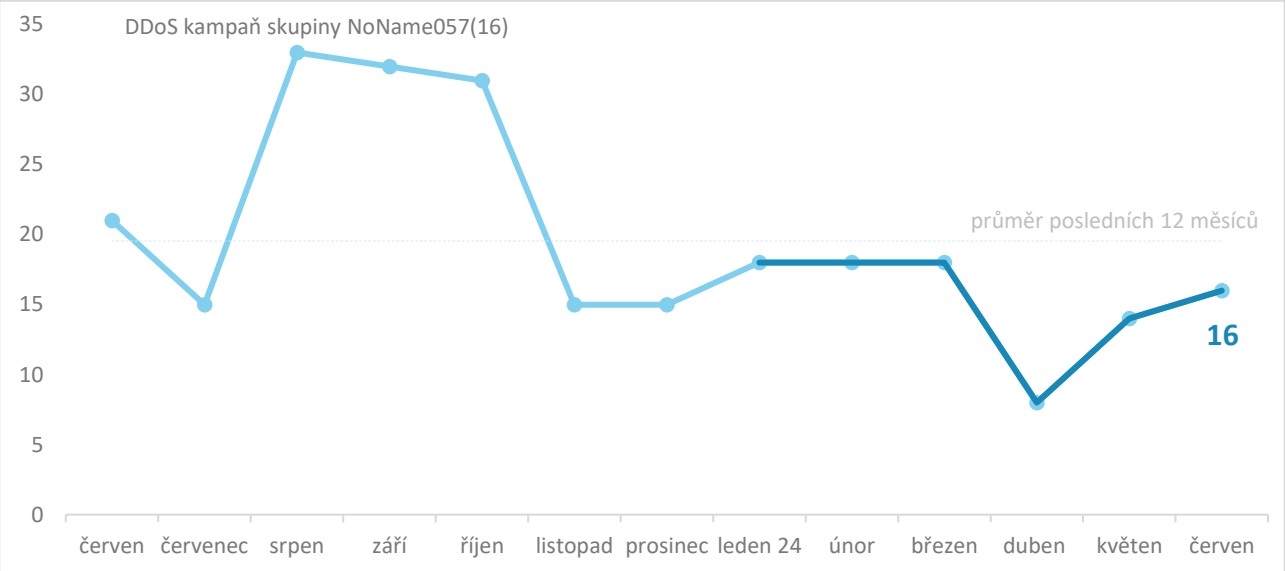
Obsah

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.

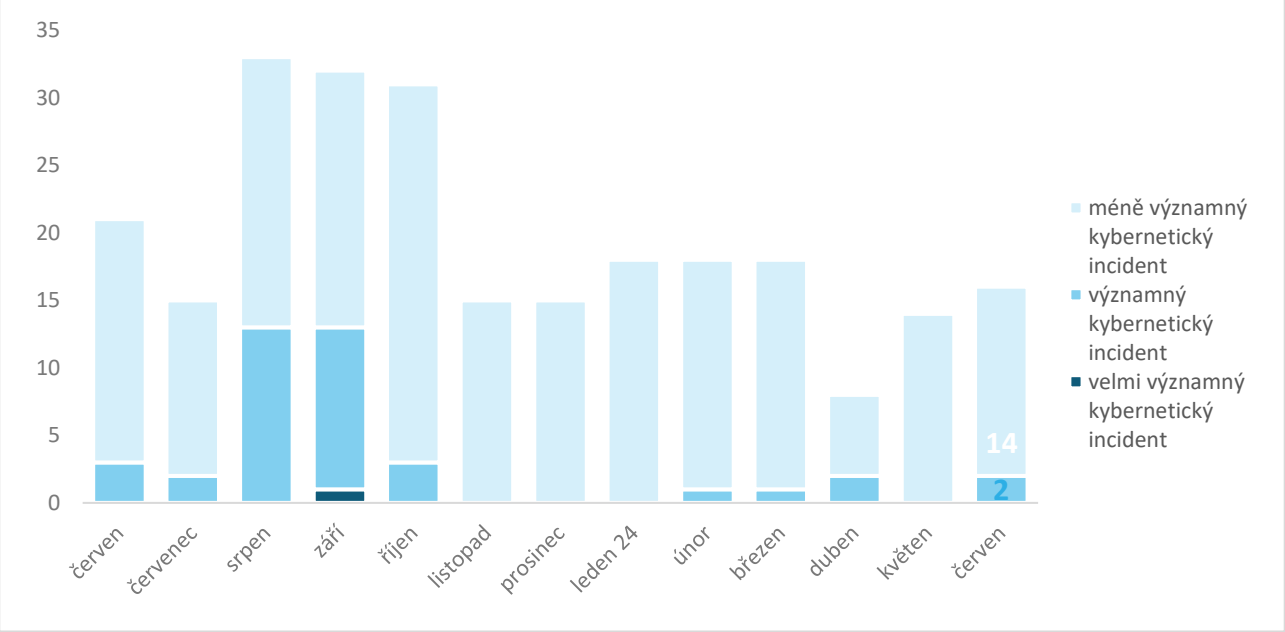
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

V červnu bylo evidováno 16 incidentů, což ukazuje na pokračování pozvolného růstu jejich počtu na úroveň ročního průměru. Po krátké odmlce se během června opět objevilo i pět incidentů spojených s DDoS útoky, které směřovaly na subjekty bankovního sektoru.



Závažnost řešených kybernetických incidentů[1]

Pohledem závažnosti evidovaných kybernetických incidentů spadala většina do kategorie méně významných, NÚKIB však v červnu evidoval i dva významné.

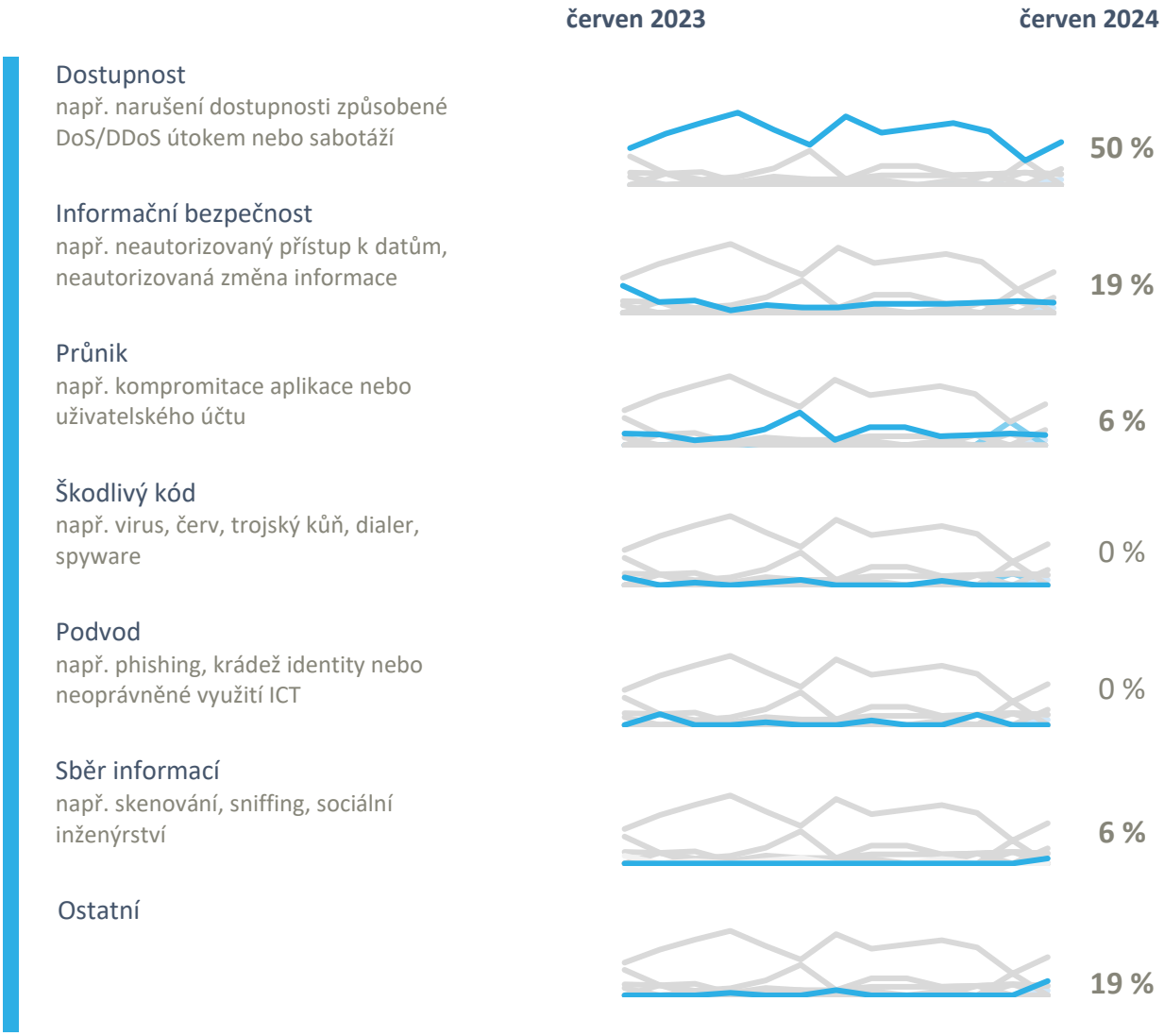


[1] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[2]

Během června NÚKIB evidoval incidenty ve třech kategoriích. Nejpočetnější kategorií byla Dostupnost, kde se kromě pěti DDoS útoků objevily i tři výpadky dostupnosti vlivem technické závady.

- V kategorii Dostupnost se po několika měsících objevil opět větší počet DDoS útoků. NÚKIB v rámci těchto incidentů nedisponuje informacemi o útočnících, nicméně všechny útoky směřovaly vůči organizacím bankovního sektoru.
- V rámci kategorie Informační bezpečnost NÚKIB během června evidoval dva ransomwarové útoky. V obou případech došlo k zašifrování části interních systémů napadených subjektů, ani v jednom případě však nedisponujeme informacemi o útočnících.
- Dále NÚKIB evidoval například spear-phishingovou kampaň, průnik do uživatelského účtu a následné rozesílání spamu či únik uživatelských údajů z neregulovaného systému.



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

Trendy v kybernetické bezpečnosti za červen pohledem NÚKIB[3]

Phishing, spear-phishing a sociální inženýrství

NÚKIB v červnu zaregistroval jeden incident zahrnující využití spear-phishingu. Útočníci při něm zneužili identitu jednoho z vysoce postavených představitelů organizace k zaslání falešných e-mailů s tematikou navýšení platů. E-mail dále obsahoval škodlivý odkaz vedoucí na stránku uzpůsobenou ke krádeži přihlašovacích údajů.

Malware

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

Zranitelnosti

Během června došlo k obnovení činnosti informování o zranitelnostech vládního CERT na sociální síti X. Za daný měsíc se zde objevila řada příspěvků, ať už v kontextu zranitelností či aktuálních hrozeb. Ze zranitelností lze zmínit například CVE-2024-37882 v nástroji Nextcloud či CVE-2024-23110 v OS Fortigate, která byla vyhodnocena jako závažná.

Ransomware

V červnu byly evidovány dva případy incidentů spojených s ransomwarem. Ani u jednoho z nich však NÚKIB nedisponuje informacemi o útočnících.

Útoky na dostupnost

V průběhu června NÚKIB evidoval pět DDoS útoků. Všechny mířily výhradně na subjekty bankovního sektoru, nicméně jejich původce se nepodařilo určit.

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

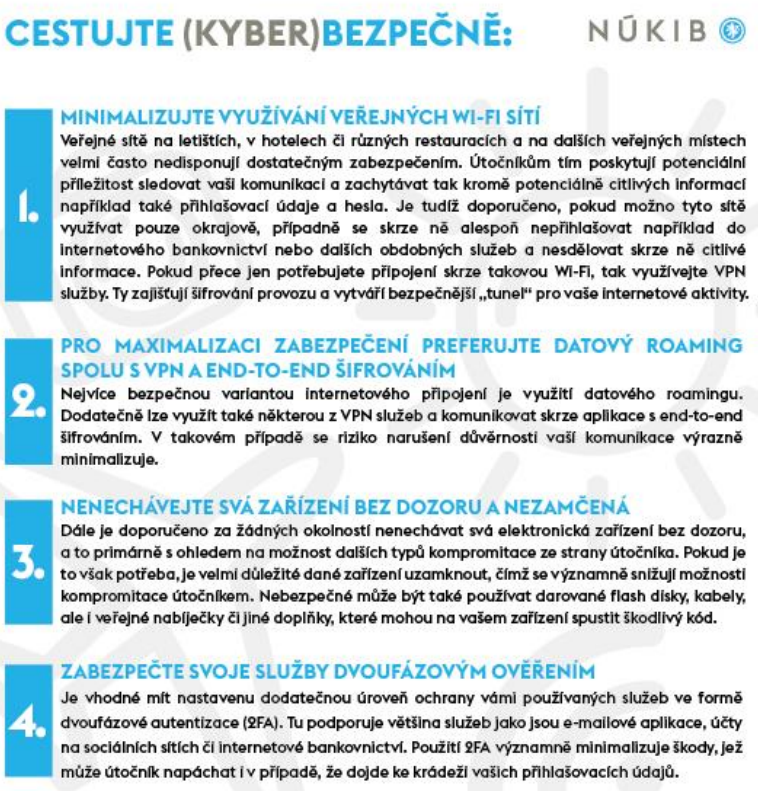
Zaměřeno na hrozbu: útočníci využívají letního období, cílí mimo jiné i na nejmladší uživatele

S příchodem letních měsíců a prázdnin vystupují do popředí i kybernetické hrozby, jejichž původci mohou zneužívat například snížené pozornosti uživatelů či naopak jejich zvýšenou aktivitu v online prostředí. Přestože toto může platit pro všechny uživatele, výše zmíněné se ve větší míře může týkat zejména nejmladších uživatelů. Varování v tomto ohledu zveřejnila například slovenská kyberbezpečnostní společnost ESET, jež v současnosti registruje nárůst hrozeb mířených primárně právě vůči této zranitelné skupině.

V jejich tiskové zprávě identifikují tři hlavní druhy malwaru, který může být pro dětské uživatele hrozbou. Jedná se o různé druhy adwaru, spywaru či různé varianty tzv. trojských koňů. Častým vektorem pak zůstávají i falešné aplikace, včetně mobilních her, které mohou ve zvýšené míře zasáhnout právě nejmladší uživatele.

Dalším rizikem mohou být například veřejné sítě. Ty bývají obvykle slabě zabezpečené a útočníci jich mohou zneužít k tzv. man-in-the-middle útokům, při kterých se snaží zachytit síťový provoz mezi zařízením oběti a zbytkem internetu. Tímto způsobem může dojít k zachycení přihlašovacích údajů či hesel a potenciálně tudíž opět k finanční ztrátě. V letních měsících, zejména v kontextu cestování, je potom toto riziko pro uživatele opět vyšší. Pro případy, kdy je použití veřejných sítí nutné, lze pak doporučit použití VPN, která uživatelskou aktivitu na internetu šifruje.

Jako seznam základních jednoduchých tipů pro všechny uživatele lze použít například obrázek níže. Pro zvýšení povědomí o hrozbách a zásadách bezpečného pohybu v online prostředí nejen nejmenších uživatelů lze potom využít vzdělávacích materiálů volně dostupných na vzdělávacím portálu NÚKIB.



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.