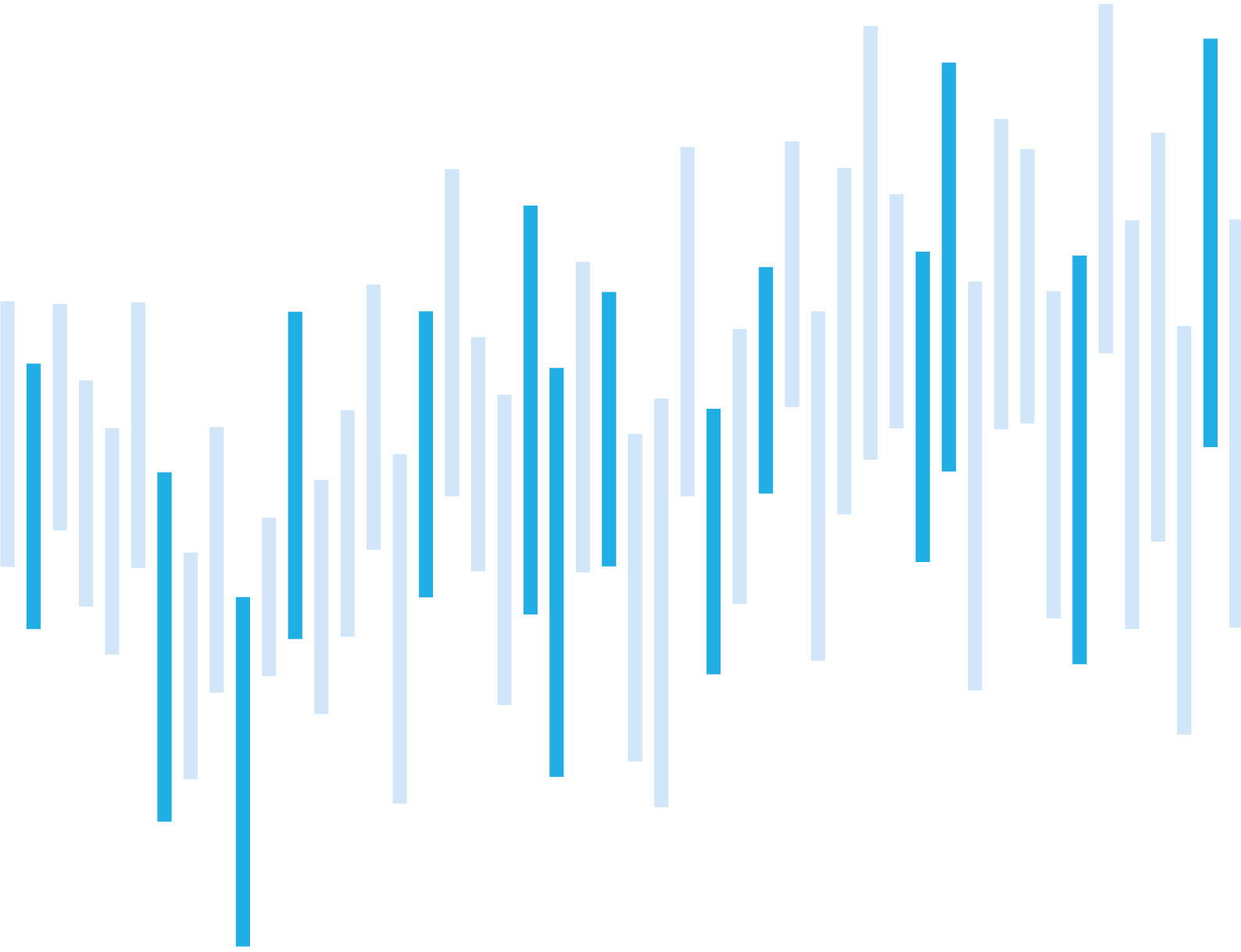
Kybernetické incidenty pohledem NÚKIB

ŘÍJEN 2023



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Během října došlo opět k nárůstu registrovaných incidentů, jejichž počet se již třetí měsíc v řadě držel nad průměrem posledních dvanácti měsíců. Průměrná měsíční hodnota se tak od loňského října zvýšila o zhruba šest incidentů.

Stejně jako v minulých měsících v rámci klasifikace incidentů dominovala kategorie Dostupnost, kde i nadále převažovaly DDoS útoky. Více než třetina incidentů v této kategorii však zahrnovala primárně provozní výpadky. NÚKIB zaregistroval také případy průniků, podvodu, škodlivého kódu či incident z kategorie Informační bezpečnosti.

V rámci kapitoly Zaměřeno na hrozbu se tentokrát zaměřujeme na zranitelnost ve WinRAR s označením CVE-2023-38831. Ačkoli tato zranitelnost byla zveřejněna již v srpnu 2023, k jejímu výraznějšímu zneužívání začalo docházet až během září a října.

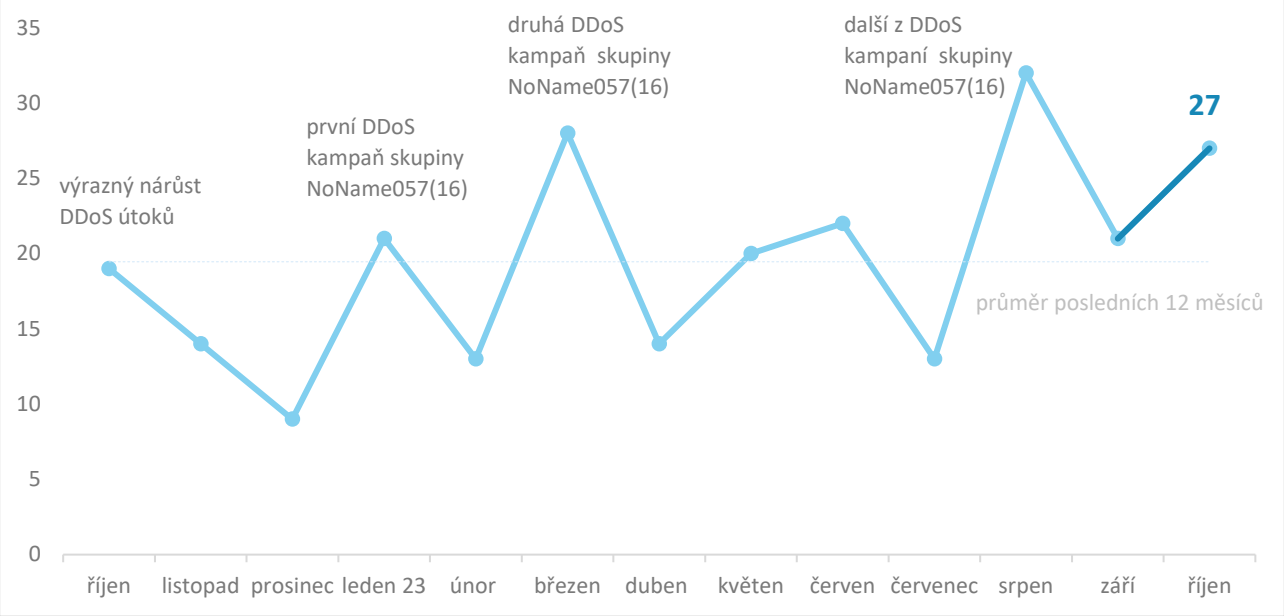
Obsah

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.

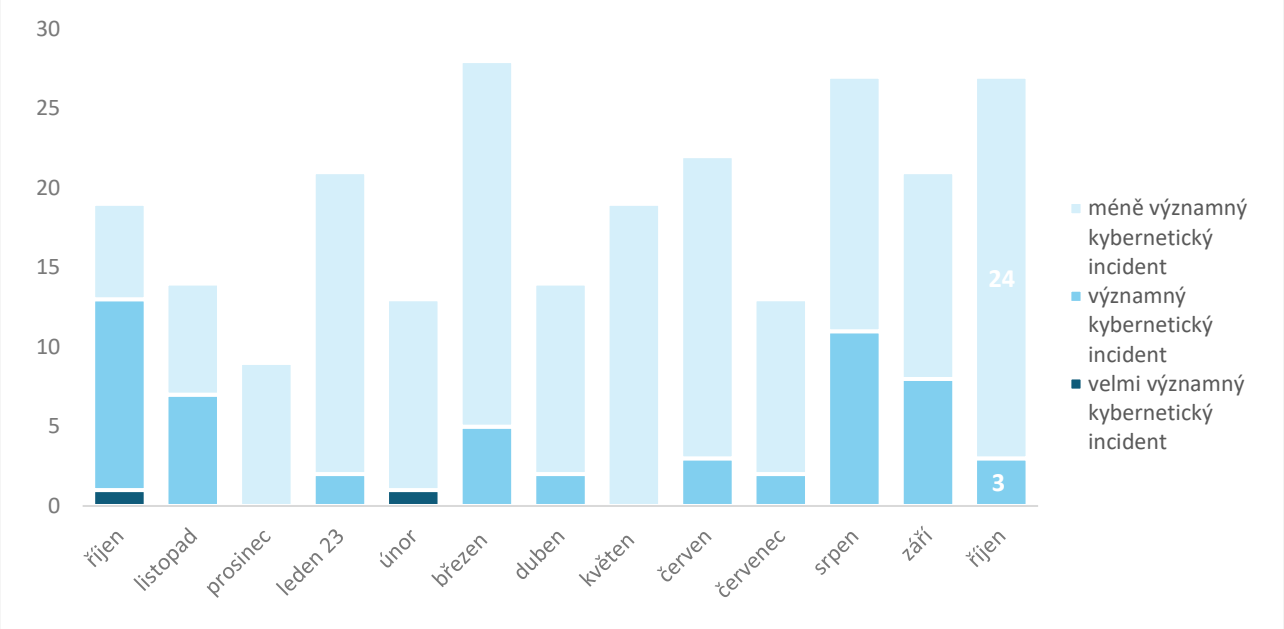
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB[1]

Během října došlo opět k nárůstu registrovaných incidentů, jejichž počet se již třetí měsíc v řadě držel nad průměrem posledních dvanácti měsíců. Průměrná měsíční hodnota se tak od loňského října zvedla zhruba o šest incidentů. NÚKIB tak za poslední rok eviduje v průměru přes 19 incidentů měsíčně.



Závažnost řešených kybernetických incidentů[2]

Vyšší počet registrovaných incidentů se nijak nepromítl do statistik závažnosti. Během října naopak došlo k poklesu evidovaných významných incidentů.



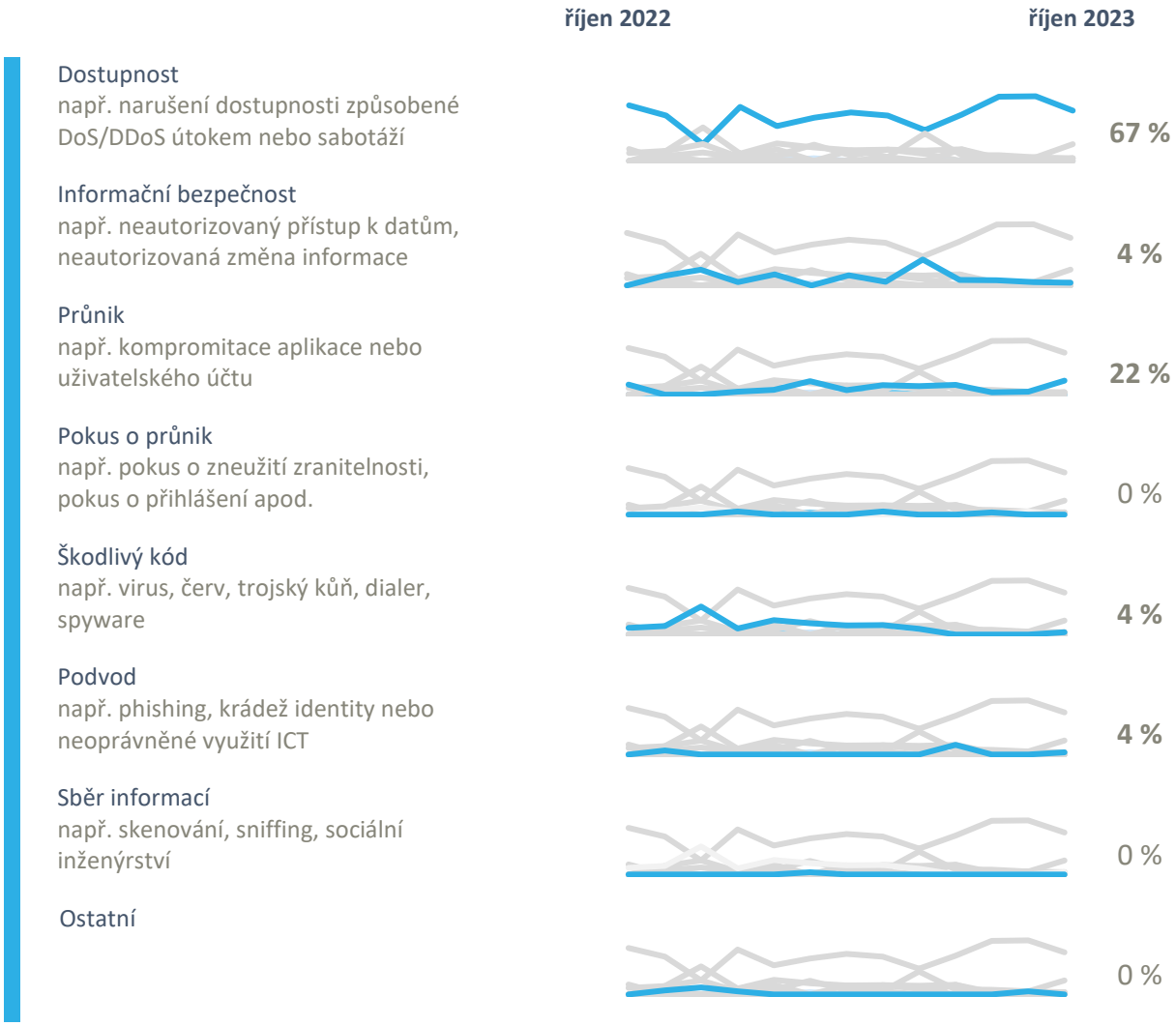
[1] NÚKIB evidoval 24 incidentů u povinných osob dle zákona o kybernetické bezpečnosti. Zbývající 3 incidenty nahlásily NÚKIB neregulované subjekty.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Stejně jako v minulých měsících v rámci klasifikace incidentů dominovala kategorie Dostupnosti, kde i nadále převažovaly DDoS útoky. Více než třetina incidentů v této kategorii však zahrnovala primárně provozní výpadky.

Vedle toho NÚKIB řešil incidenty v celkem čtyřech kategoriích:

- NÚKIB během října zaregistroval několik průniků, v rámci kterých se útočníkům podařilo získat nejen přístupy k některým uživatelským účtům, ale v některých případech také přístupy přímo do interních systémů a provádět v nich neoprávněné akce.
- V rámci kategorie Informační bezpečnost došlo ke kompromitaci jedné z e-mailových schránek subjektu, z níž byly následně rozesílány phishingové e-maily.
- Regulovaný subjekt zachytil ve svém systému malware, jehož analýza v současnosti probíhá.
- Do kategorie Podvod spadá jeden úspěšný phishing, který byl nicméně včas detekován a nevedl tak ke kompromitaci subjektu.



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

Trendy v kybernetické bezpečnosti za říjen pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

NÚKIB v říjnu zaregistroval několik incidentů, které zahrnovaly využití phishingu. V rámci některých dalších evidovaných incidentů bylo využití phishingu jako prvotního vektoru útoku pravděpodobné, nelze je však přímo potvrdit.

Malware

Během října NÚKIB zaregistroval několik různých typů malwaru, jejichž analýza aktuálně probíhá.

Zranitelnosti

Během října NÚKIB upozornil na dvě nové zranitelnosti. Obě se týkají webového rozhraní operačního systému Cisco IOS XE. Obě zranitelnosti jsou aktivně zneužívány a NÚKIB proto doporučuje aktualizaci zranitelných zařízení a případně využití mitigačních a detekčních opatření, které lze nalézt v upozorněních na stránkách NÚKIB a přiložených odkazech.

Ransomware

Po delší době NÚKIB neeviduje žádný incident spojený s ransomwarem.

Útoky na dostupnost

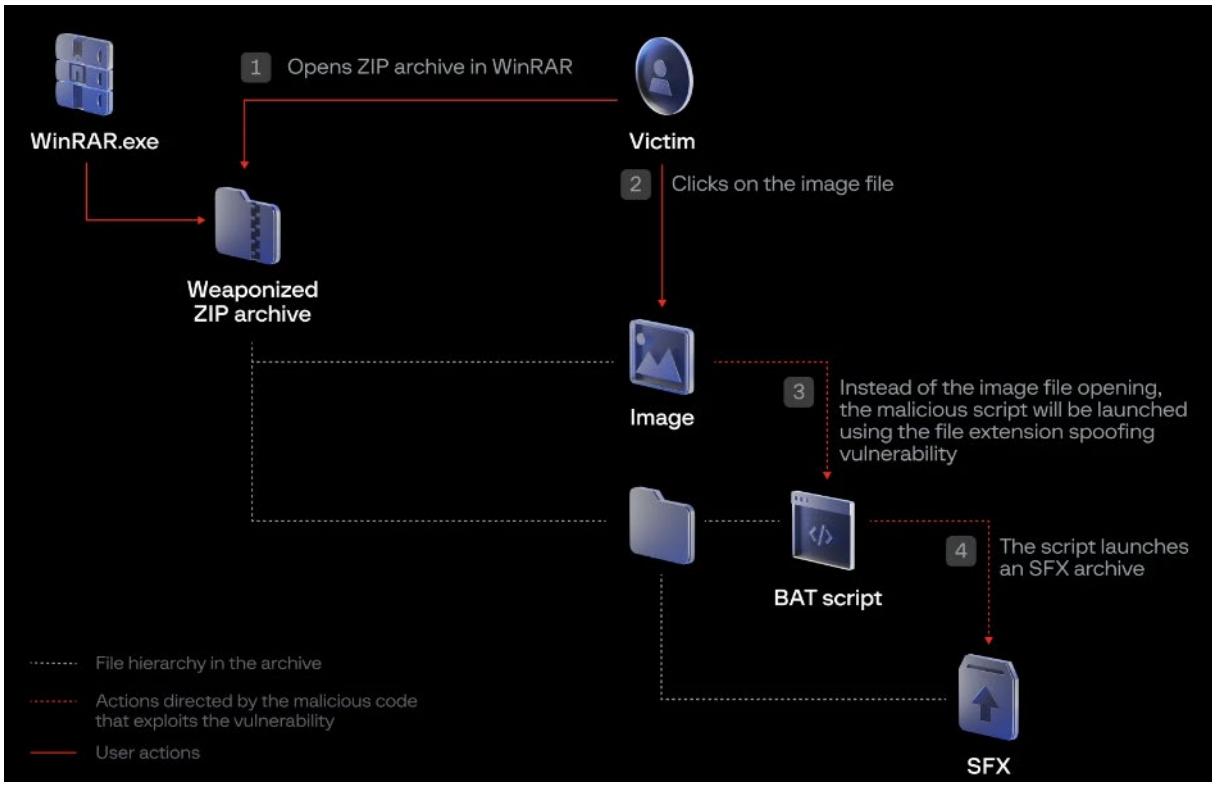
Podobně jako v uplynulých měsících i v říjnu nadále pokračovaly útoky proruské hacktivistické skupiny NoName057(16). Útokům této skupiny, včetně možností mitigace vůči nim, jsme se věnovali v zářijovém přehledu incidentů.

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

Zaměřeno na hrozbu: Aktivní zneužívání závažné zranitelnosti ve WinRAR

V rámci kapitoly zaměřeno na hrozbu se tentokrát zaměřujeme na zranitelnost ve WinRAR s označením CVE-2023-38831. Ačkoli tato zranitelnost byla zveřejněna již v srpnu 2023, k jejímu výraznějšímu zneužívání začalo docházet až během září a října. Dle společnosti Google tuto zranitelnost zneužívají v rámci svých útoků někteří státem zaštítění aktéři, přičemž v minulosti byly zaznamenány také útoky ze strany kyberkriminálních skupin. NÚKIB zaregistroval zneužívání této zranitelnosti také v rámci ČR.

Obr. 1: Grafické znázornění postupu útočníků zneužívajících zranitelnost ve WinRAR zveřejněné společností Group-IB



Zdroj: group-ib.com

Zranitelnost se týká WinRAR 6.22 a starších verzí, ve kterých lze spustit škodlivý kód v okamžiku, kdy se uživatel pokusí zobrazit soubory v ZIP archivu, které stáhnul z doručeného e-mailu. Nejčastěji se jedná o sadu souborů JPEG a PNG, mezi kterými se nachází soubor napodobující obrazový formát obsahující libovolný kód, například „poc.png .cmd“ (mezera je zde záměrná). Alternativně se lze setkat s variantou napodobující PDF soubor.

Bezpečnostní aktualizace řešící danou zranitelnost je již k dispozici a NÚKIB proto doporučuje všem, kteří tak doposud neučinili, aktualizovat WinRAR na nejnovější verzi.

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.