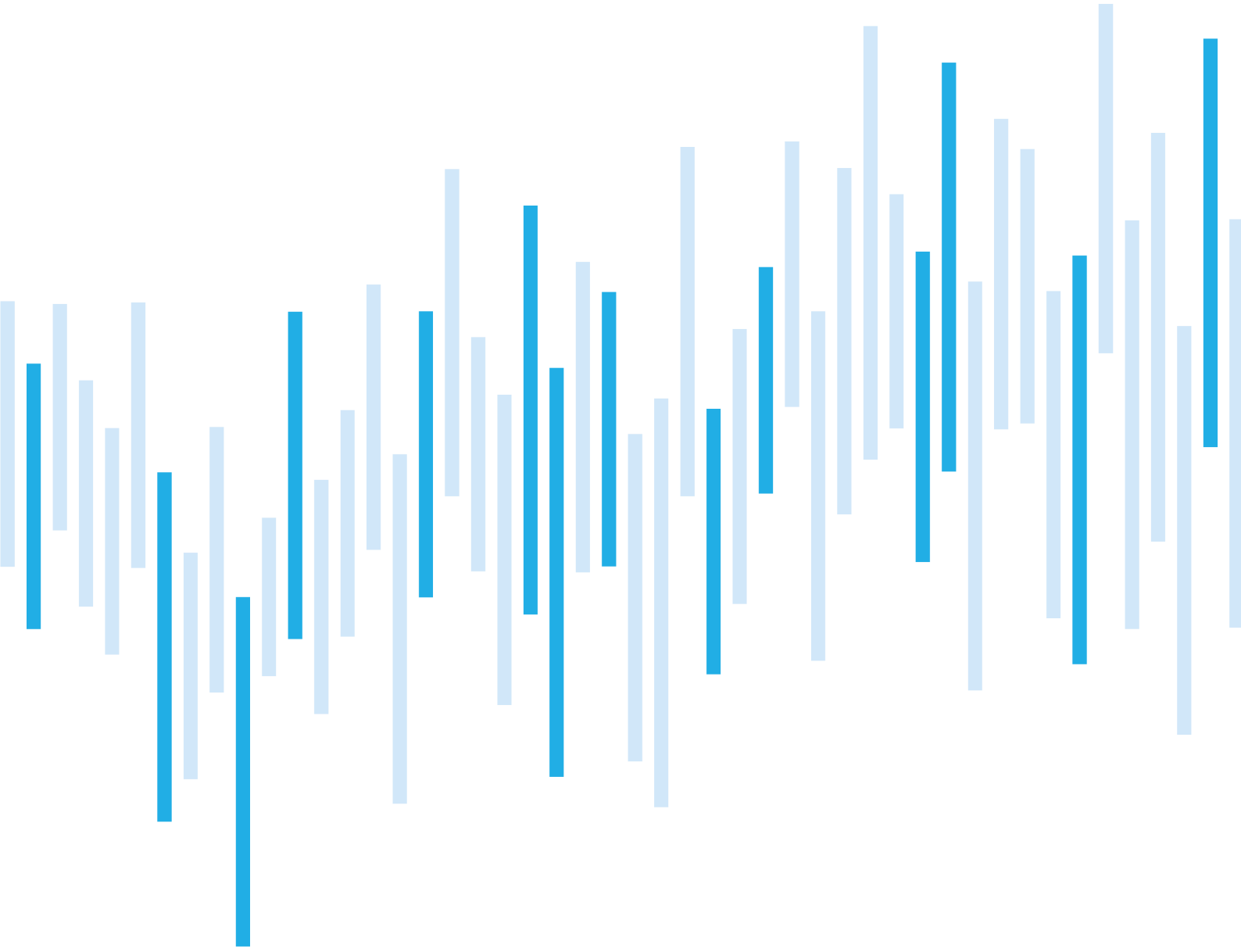
Kybernetické incidenty pohledem NÚKIB

ZÁŘÍ 2023



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Navzdory tomu, že počet evidovaných incidentů v září oproti minulému měsíci klesl, nadále se pohyboval nad průměrem posledních dvanácti měsíců. Většina incidentů byla součástí kampaně NoName057(16), která cílila primárně na český bankovní sektor a proběhla na přelomu srpna a září.

Tato kampaň se vzhledem ke svému významu propsala nejen do počtu registrovaných incidentů, ale také do statistik závažnosti. DDoS útoky v září tvořily téměř čtyři pětiny všech evidovaných incidentů a převážná většina z nich se zařadila do kategorie významných.

Skupině NoName057(16) se tentokrát věnujeme blíže v kapitole *Zaměřeno na hrozbu*. Kapitola popisuje nejen výše zmíněnou kampaň této skupiny, ale zaměřuje se také na její dosavadní modus operandi, technický popis jejích útoků a možnosti mitigace.

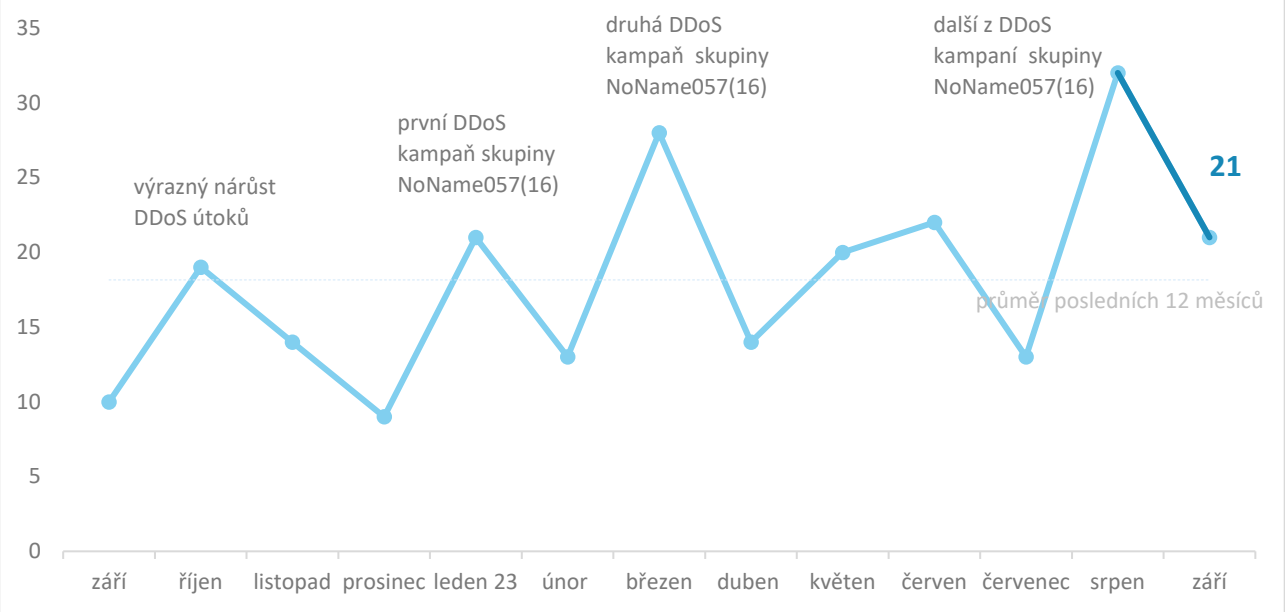
Obsah

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.

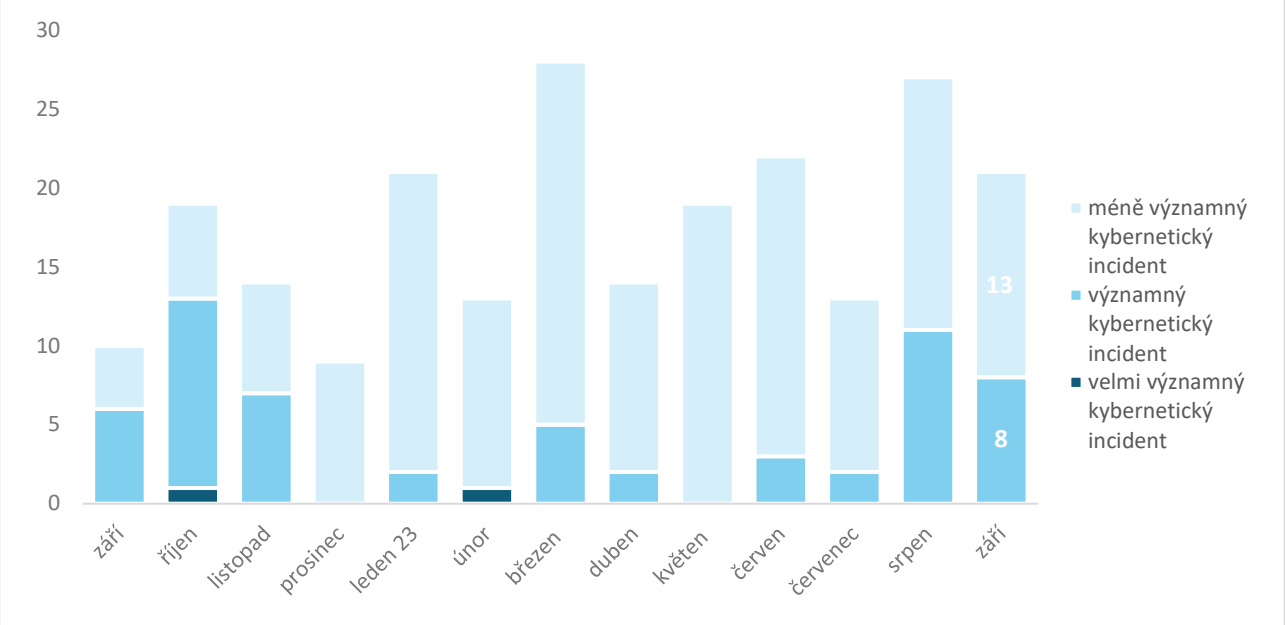
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Ačkoli počet evidovaných incidentů v září oproti minulému měsíci klesl, i nadále se pohyboval nad průměrem posledních dvanácti měsíců. Většina incidentů byla součástí kampaně NoName057(16), která proběhla na přelomu srpna a září.[1]



Závažnost řešených kybernetických incidentů[2]

Zvýšený počet významných kybernetických incidentů zaznamenaný během září byl spojen s pokračováním výše zmíněné kampaně NoName057(16) vůči českým bankám, která se promítla také do srpnových statistik.



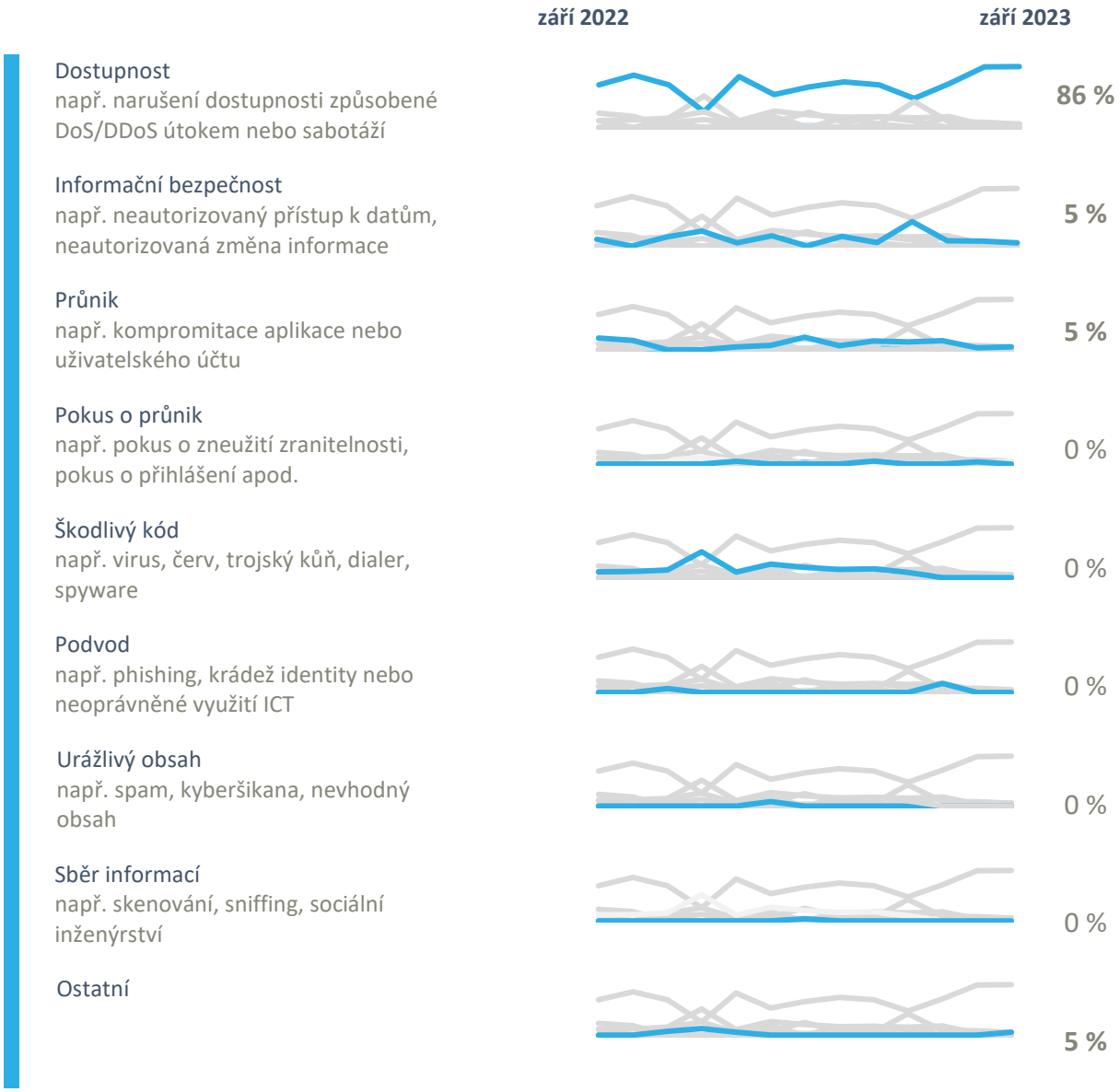
[1] NÚKIB evidoval 18 incidentů u povinných osob dle zákona o kybernetické bezpečnosti. Zbývající 3 incidenty nahlásily NÚKIB neregulované subjekty.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Klasifikaci incidentů již devátý měsíc v řadě dominuje kategorie dostupnosti. Během září vedly k omezení dostupnosti více než čtyři pětiny všech evidovaných incidentů . Převážná část z nich byla opět způsobena DDoS útoky.

Vedle toho NÚKIB řešil incidenty v těchto třech kategoriích:

- Jeden případ v rámci kategorie Informační bezpečnost byl spojen s ransomwarovým útokem skupiny Monti (viz kapitola níže).
- Během září došlo k jednomu incidentu spadajícímu do kategorie průnik. Jednalo se o útok velmi sofistikovaného aktéra, kterému se povedlo získat přístup do systémů regulovaného subjektu.
- V rámci kategorie ostatní došlo ke specifickému incidentu, který vznikl ztrátou tabletu uživatele.



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

Trendy v kybernetické bezpečnosti za září pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

Ačkoli phishing dlouhodobě patří mezi trvalé hrozby, které se objevují v rámci incidentů NÚKIB, během září byl počet registrovaných phishingových útoků výrazně nižší než v předchozích měsících.

Malware

Podobně jako v srpnu NÚKIB v září nezaznamenal žádný malware s výjimkou níže uvedeného ransomwaru.

Zranitelnosti

V září NÚKIB nevydal žádné upozornění na nově objevené zranitelnosti.

Ransomware

NÚKIB během září zaznamenal incident, v rámci kterého skupina Monti využila ransomware k napadení neregulovaného subjektu a jeho následnému vydírání. Tato skupina vznikla v polovině roku 2022 několik měsíců po úniku interních dat ransomwarového gangu Conti. Monti adoptovala nejen taktiky a techniky tohoto gangu, ale také zdrojový kód ransomwaru Conti, který následně využila pro tvorbu vlastního. Dle společnosti Zscaler ThreatLabz začala tato skupina nedávno využívat novou variantu ransomwaru Monti zvanou BIDON.

Útoky na dostupnost

Trend uplynulých měsíců, kdy proruská hacktivistická skupina NoName057(16) ve vlnách útočí na vybrané české cíle, nadále pokračoval. Bližší informace o dosud poslední kampani této skupiny nabízí kapitola Zaměřeno na hrozbu.

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

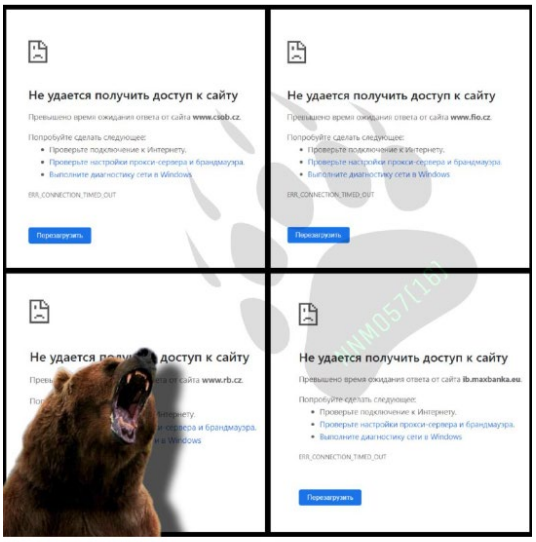
Zaměřeno na hrozbu: DDoS kampaň skupiny NoName057(16) vůči českým subjektům

Na přelomu srpna a září došlo k další vlně DDoS útoků skupiny NoName057(16), která mířila primárně na český bankovní sektor. Několik českých bank se v důsledku útoků potýkalo s problémy ohledně nedostupnosti služeb. Klienti bank se v důsledku útoků nemohli přihlásit do bankovnictví, nicméně vzhledem k typu útoku nebyla narušena důvěrnost nebo integrita jejich dat a jejich finanční prostředky nebyly žádným způsobem ohroženy. Útoky pak pokračovaly i v následujících dnech, kdy kromě bankovních institucí došlo k napadení subjektů z průmyslového a vojenského sektoru. Aktivita skupiny cílená na české subjekty po několika dnech ustala a žádný z útoků neměl dlouhodobější následky.

NoName057(16) svými útoky často reaguje na geopolitické či jiné události nebo výroky spojené s děním na Ukrajině či v Rusku. V současnosti však není zcela jisté, zda a případně jaký impuls měla vlna útoků na české bankovní instituce. Vzhledem k dlouhodobému zacílení českých subjektů nelze vyloučit, že v dohledné době dojde k dalším útokům. NÚKIB skupinu NoName057(16) dlouhodobě monitoruje a proaktivně kontaktuje subjekty označené jako cíle a poskytuje relevantní doporučení.

Česká republika není jediným cílem skupiny NoName057(16). Během minulého týdne útočila proti finančním institucím v Polsku a dále převážně proti dopravním společnostem v Dánsku, Norsku a Nizozemsku. Poslední tři jmenované státy byly zacíleny po oznámení dodávek letounů F-16 na Ukrajinu.

Obr. 1: Telegramový příspěvek skupiny NoName057(16)



Today we decided to return to the Czech Republic and check how things are going in the banking sector😏

Zdroj: t.me

Technický popis útoků a možnosti mitigace

DDoS útoky skupiny NoName057(16) spadají pod typ HTTP GET/POST flood. Útoky běžně probíhají tak, že si jednotliví členové do DDoS klienta nahrají konfigurační JSON soubor obsahující URL a IP adresu cíle a poté celý HTTP GET/POST požadavek. Tento požadavek míří na velmi specifickou URL např. náhodná záložka v tiskových zprávách, specifické nastavení půjčky v online formuláři nebo vyhledávání konkrétních bankomatů v databázi. Toho lze využít při mitigaci, kdy se správce webu může rozhodnout o zablokování specifických požadavků nebo méně důležitých částí webu. JSON soubor je aktualizován průměrně 2x denně, ale mění se jen cíle, nikoli dané požadavky. NÚKIB všem označeným cílům posílá část konfiguračního souboru s těmito požadavky.

Z interních analýz NÚKIB je doporučena blokace na základě user agenta. DDoS klient používá Go-http-agent/1.1, Go-http-agent/2 nebo prázdného user agenta (-). Toto mitigační opatření však s sebou nese riziko nefunkčnosti některých služeb využívajících jazyk GO.

Jako další způsoby mitigace lze využít například tzv. geofencing či omezování přístupu na základě počtu požadavků z konkrétní IP adresy za minutu.

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.