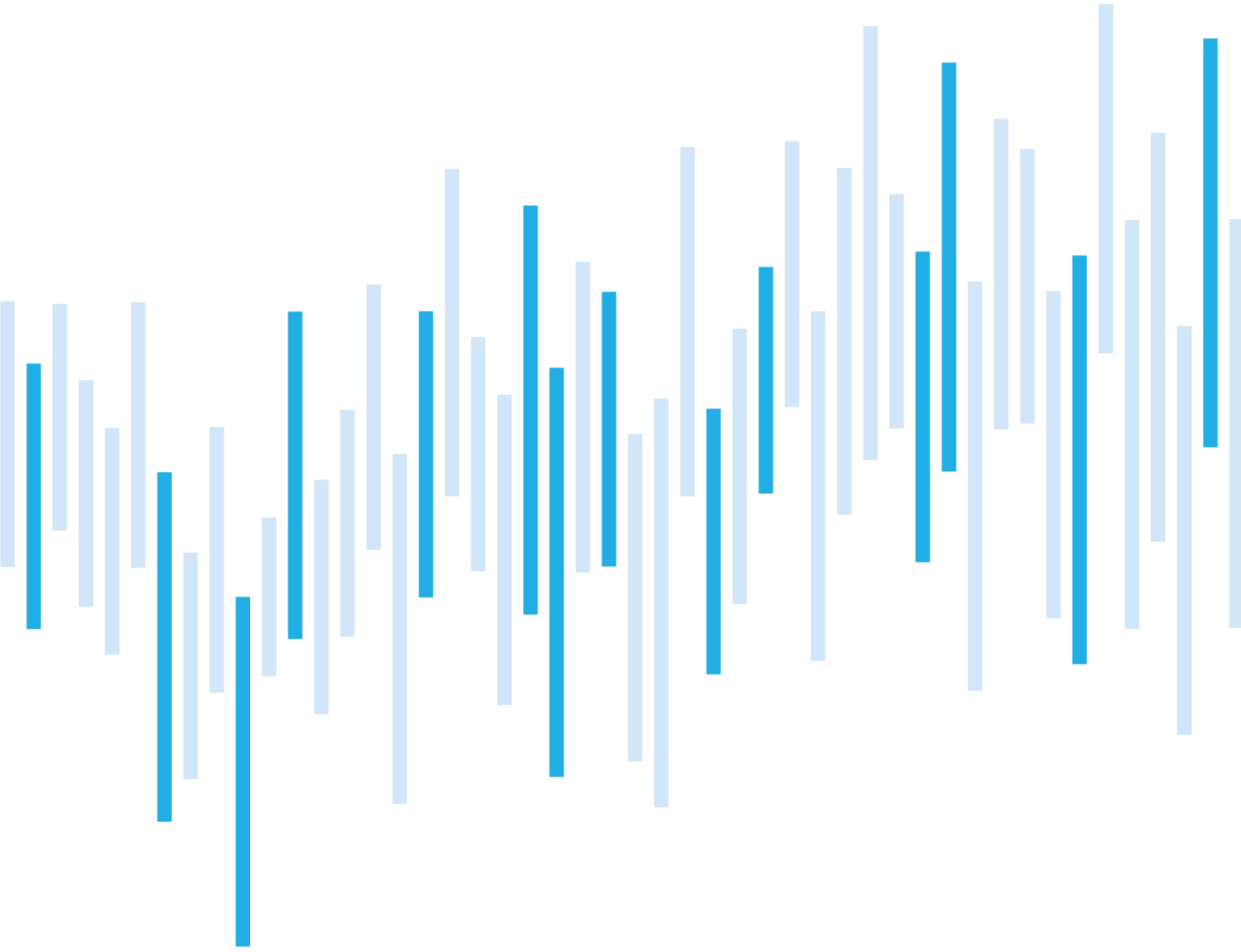
Kybernetické incidenty pohledem NÚKIB

Prosinec 2024



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Poslední měsíc roku 2024, prosinec, přinesl 16 incidentů, jednalo se tak o početně podprůměrný měsíc. Podobně jako v listopadu NÚKIB evidoval pouze méně významné incidenty.

Hlavní kategorií s počtem 10 evidovaných incidentů zůstává Dostupnost. Většinu z nich tvořily DDoS útoky. Počet ransomwarových útoků v závěru roku klesl pouze na jeden evidovaný incident.

V kapitole Zaměřeno na trend se tentokrát věnujeme rekapitulaci roku 2024 z pohledu incidentů, trendů a dalších významných událostí. Celkový roční počet evidovaných incidentů se vyšplhal na 268, což je o šest více než za rok 2023. Drobný rozdíl oproti počtu uváděnému v předchozích měsíčních přehledech je vysvětlen v dané kapitole níže.

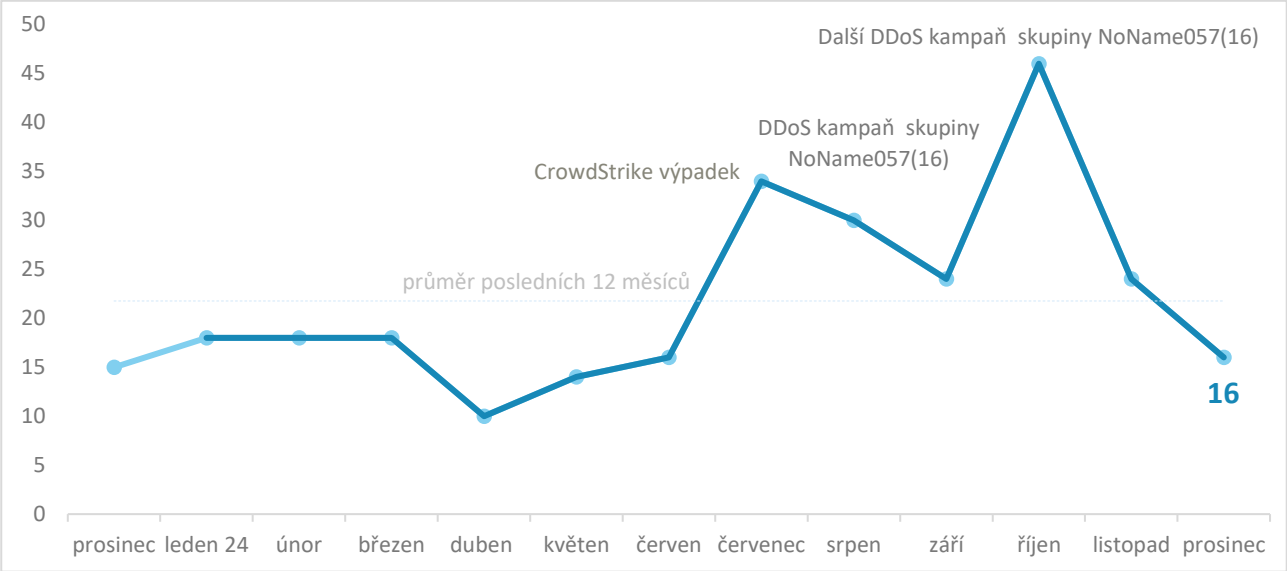
Obsah

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 původ těchto informací vždy uveden.

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

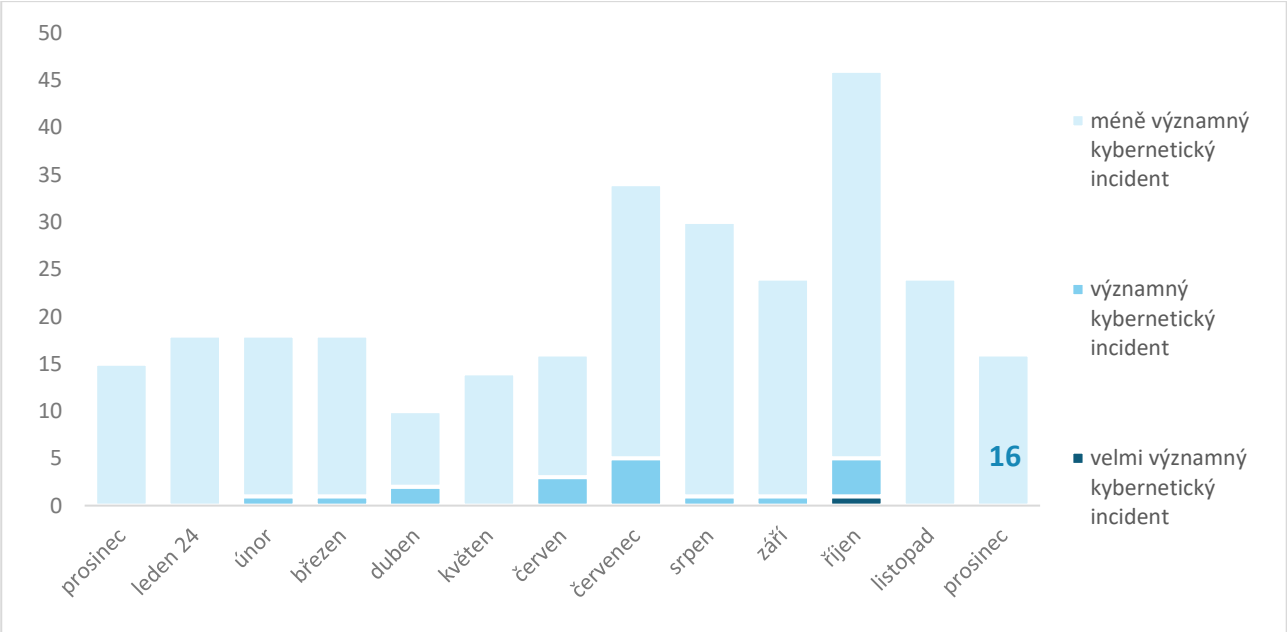
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

V prosinci NÚKIB evidoval 16 kybernetických incidentů. Závěr roku byl tudíž v podprůměrných hodnotách.



Závažnost řešených kybernetických incidentů[1]

Závažnost evidovaných incidentů zůstala i v prosinci nízká, všechny prosincové incidenty byly klasifikovány jako méně významné.



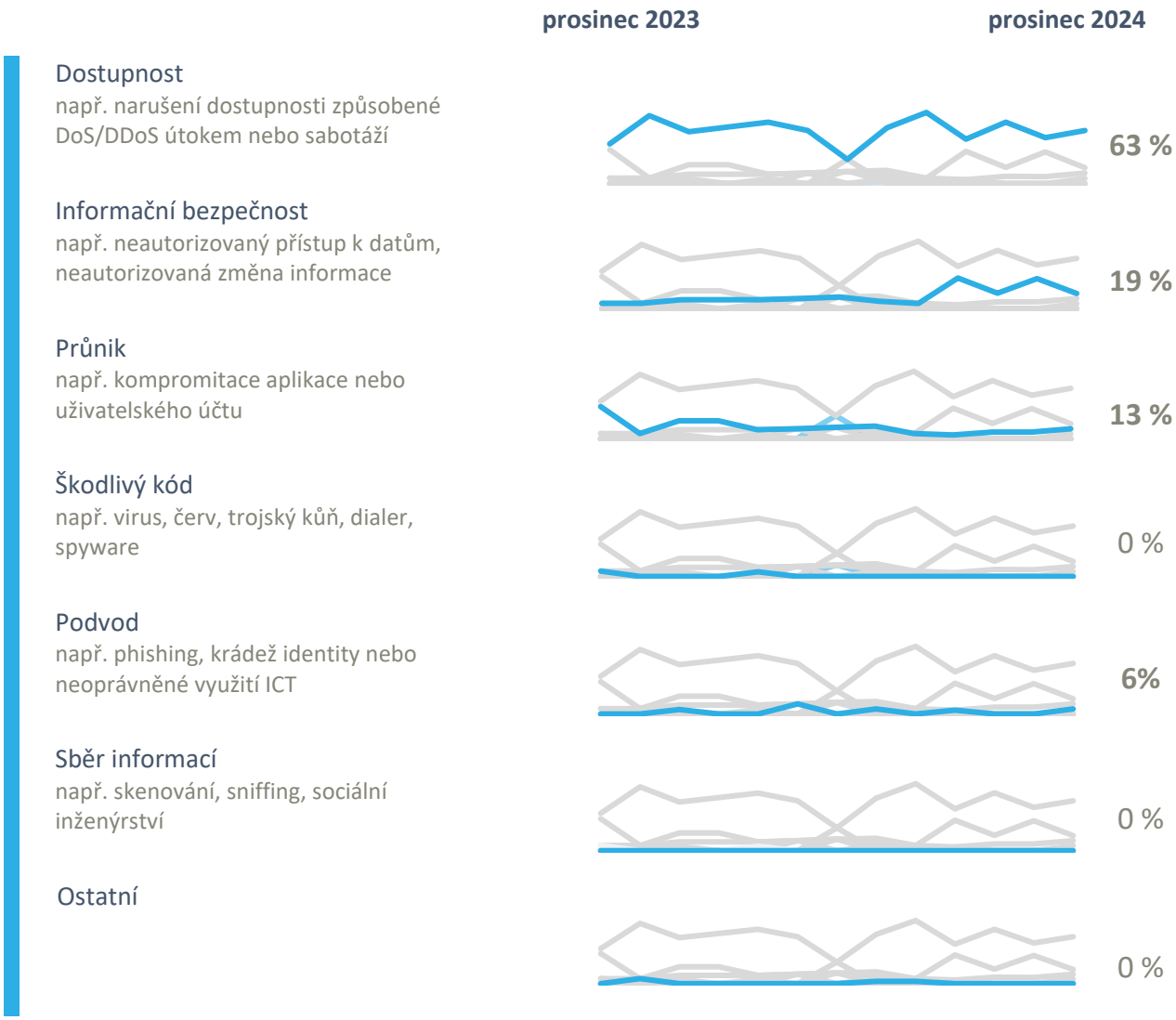
[1] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[2]

Obdobně jako v minulých měsících zůstává nejpočetnější kategorií incidentů Dostupnost. V prosinci ji tvořilo sedm DDoS útoků a tři výpadky služeb v důsledku technické závady.

NÚKIB dále řešil incidenty ve třech kategoriích:

- Tři incidenty spadají do kategorie Informační bezpečnost, jeden z nich představoval ransomwarový útok, konkrétně se jednalo o skupinu Ransomhub. Ve dvou zbylých případech šlo o neautorizovaný přístup k systémům.
- V rámci kategorie Průnik evidoval NÚKIB dva incidenty zahrnující kompromitaci serveru a prolomení jednoho uživatelského účtu.
- Poslední evidovanou kategorií byl Podvod, kdy došlo prostřednictvím spear-phishingu k zaslání falešné faktury a jejímu proplacení obětí. Celková škoda přesáhla milion korun.



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

Trendy v kybernetické bezpečnosti za prosinec pohledem NÚKIB[3]

Phishing, spear-phishing a sociální inženýrství

NÚKIB v prosinci evidoval jeden incident s využitím spear-phishingu. Konkrétně se jednalo o zaslání falešné faktury pod podvrhnutou identitou zákazníka a následné zaplacení obětí.

Malware

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

Zranitelnosti

Během prosince NÚKIB pokračoval v publikaci zranitelností skrze sociální síť X.

Ransomware

V prosinci byl evidován pouze jeden ransomwarový útok.

Útoky na dostupnost

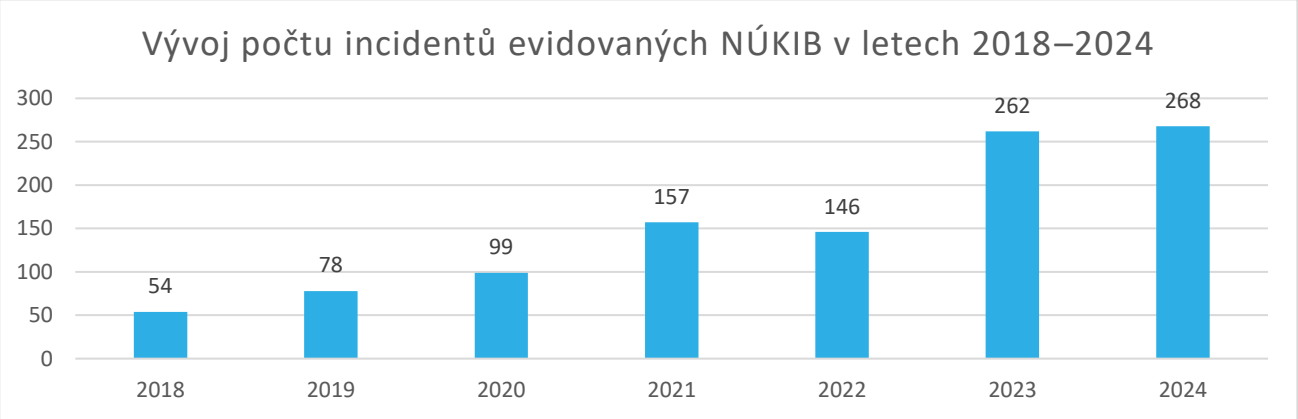
V průběhu prosince NÚKIB evidoval sedm DDoS útoků.

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

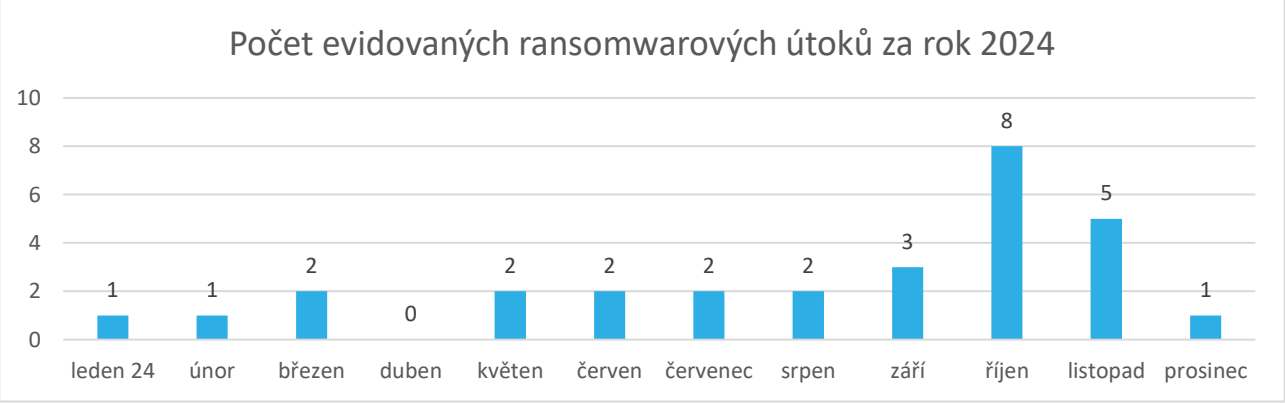
Zaměřeno na trend: Rekapitulace incidentů roku 2024 pohledem NÚKIB

NÚKIB v roce 2024 evidoval celkem 268 kybernetických bezpečnostních incidentů, což je dosud nejvyšší zaregistrovaná hodnota. Oproti roku 2023, kdy bylo evidováno 262 incidentů, se jedná o pouze drobný nárůst. Skladba incidentů je velmi podobná té z minulého roku, kdy největší podíl, 43 %, tvoří DDoS útoky ze strany ruskojazyčných hacktivistů. Částečně byla evidována i škodlivá činnost aktérů blízkovýchodního regionu . I nadále však jejich škodlivé aktivity nepůsobily zasaženým cílům větší dopady nad rámec krátkodobých výpadků napadených webů.

Rozdíl finálního počtu, závažnosti či kategorií oproti předchozím měsíčním přehledům je dán pravidelným každoročním vyhodnocováním celé evidence a s tím spojenou rekategorizací. Dalším důvodem může být i zpětné zanesení později nahlášených či odhalených incidentů.



Po celý rok též přetrvávala hrozba ransomwarových útoků, kterých NÚKIB evidoval nižší jednotky každý měsíc, reálný počet útoků v ČR mimo viditelnost NÚKIB je přitom téměř jistě (90–100 %) vyšší. **Ačkoli ransomwarové útoky stály za necelými 11 % všech evidovaných incidentů, jejich dopady dokazují, že jde o velmi závažnou hrozbu.** Kromě úniku citlivých informací (občanů či klientů) mohou vést k zašifrování dat, což může vyústit až v dočasné pozastavení výroby či poskytování služeb. Vše zmíněné s sebou samozřejmě nese reputační nebo finanční újmu. Během podzimu NÚKIB evidoval více než dvojnásobný nárůst těchto útoků oproti průměrným hodnotám – nejednalo se však nejspíš o koordinovanou kampaň, ale o vyšší aktivitu různých útočníků.



Specifickou událostí s celosvětovým dopadem byl výpadek EDR softwaru společnosti CrowdStrike, který skrze chybnou aktualizaci způsobil v červenci rozsáhlé výpadky systémů napříč sektory a následnou nedostupnost různých služeb. V tuzemsku byly dopady události menší než v jiných západních státech, přesto však NÚKIB v této souvislosti evidoval celkem devět incidentů.

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.