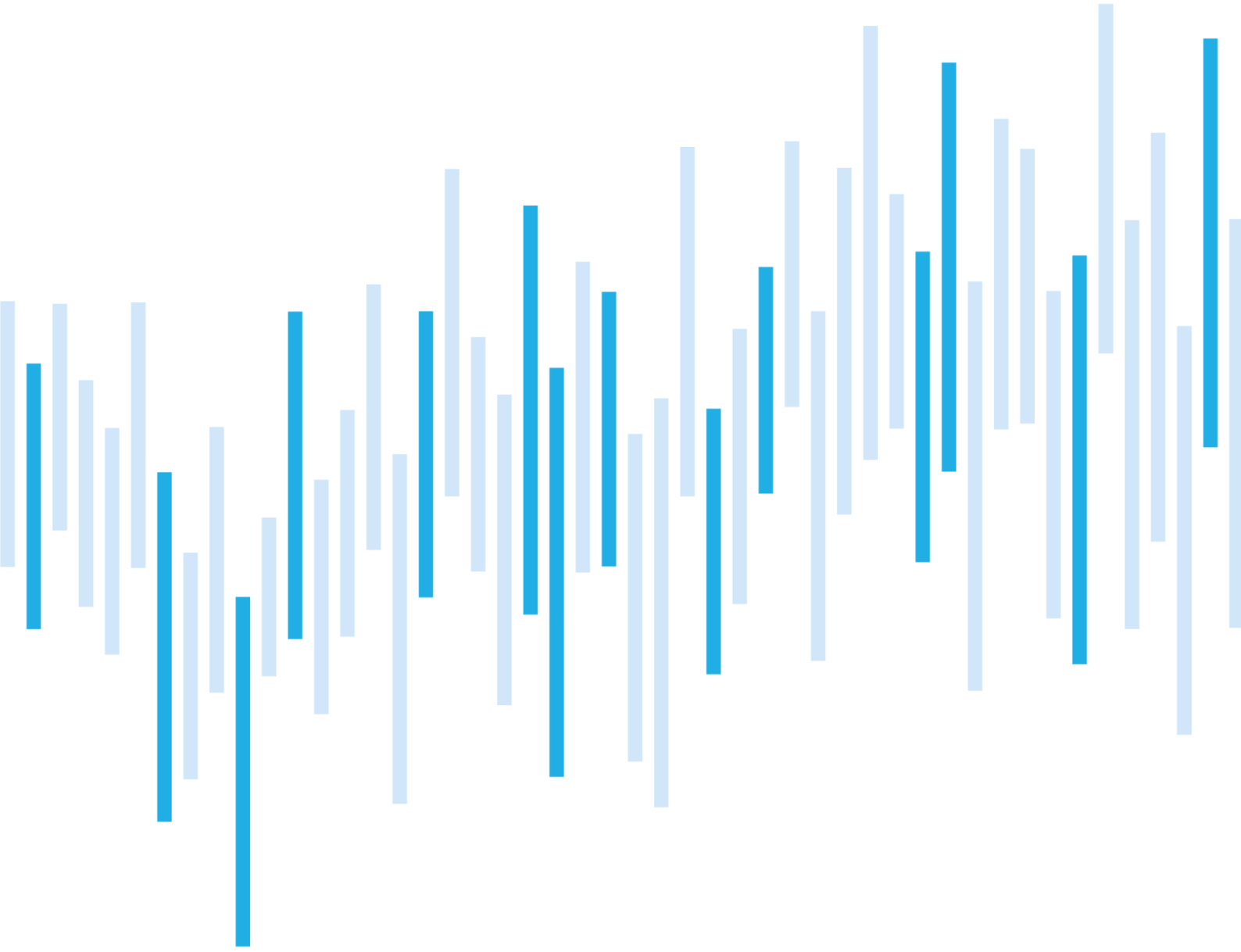
Kybernetické incidenty pohledem NÚKIB

Listopad 2024



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

V listopadu NÚKIB evidoval 24 kybernetických bezpečnostních incidentů, všechny byly klasifikovány jako méně významné. Oproti rekordnímu říjnu se tak počet incidentů přiblížil k průměrným hodnotám uplynulého roku.

Hlavní kategorií nadále zůstává Dostupnost. V listopadu ji však převážně tvořily incidenty spojené s technickými závadami, přičemž DDoS útoků NÚKIB eviduje pouze 5. Stejný počet byl zaznamenán také u ransomwarových útoků, u kterých se však jedná o nadprůměrnou hodnotu.

V kapitole Zaměřeno na hrozbu se tentokrát věnujeme přetrvávající hrozbě ransomwarových útoků. V posledních měsících je frekvence těchto útoků nadprůměrná a přestože podle dostupných informací nejde o ucelenou kampaň, ale spíše zvýšenou aktivitu jednotlivých útočníků, jejich útoky mohou obětem způsobit značné finanční škody.

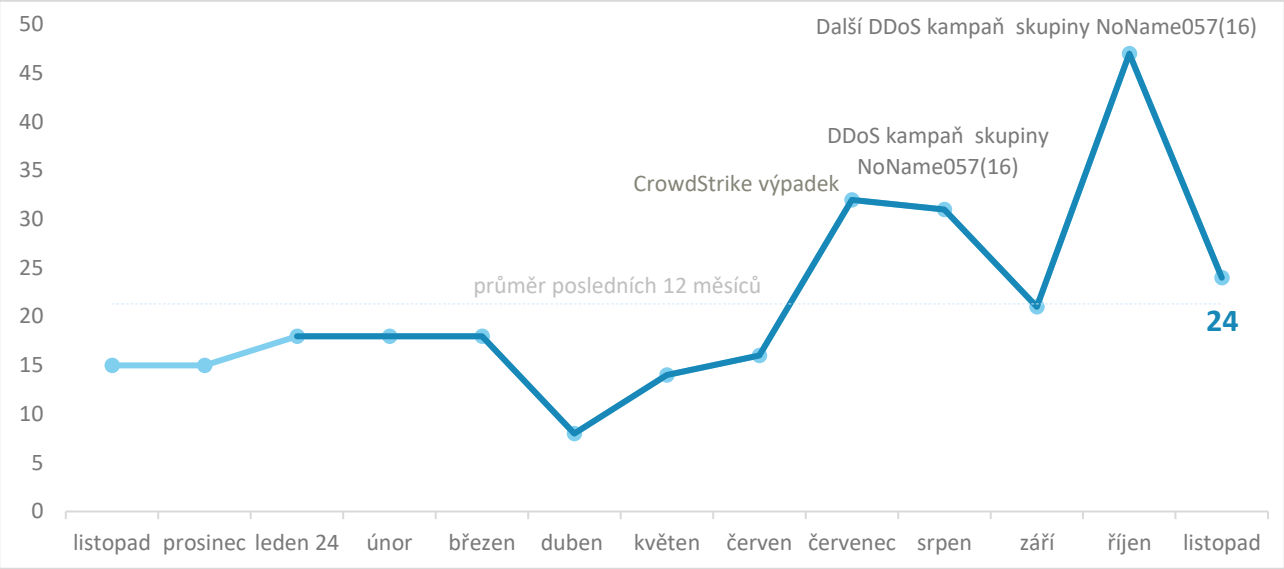
Obsah

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.

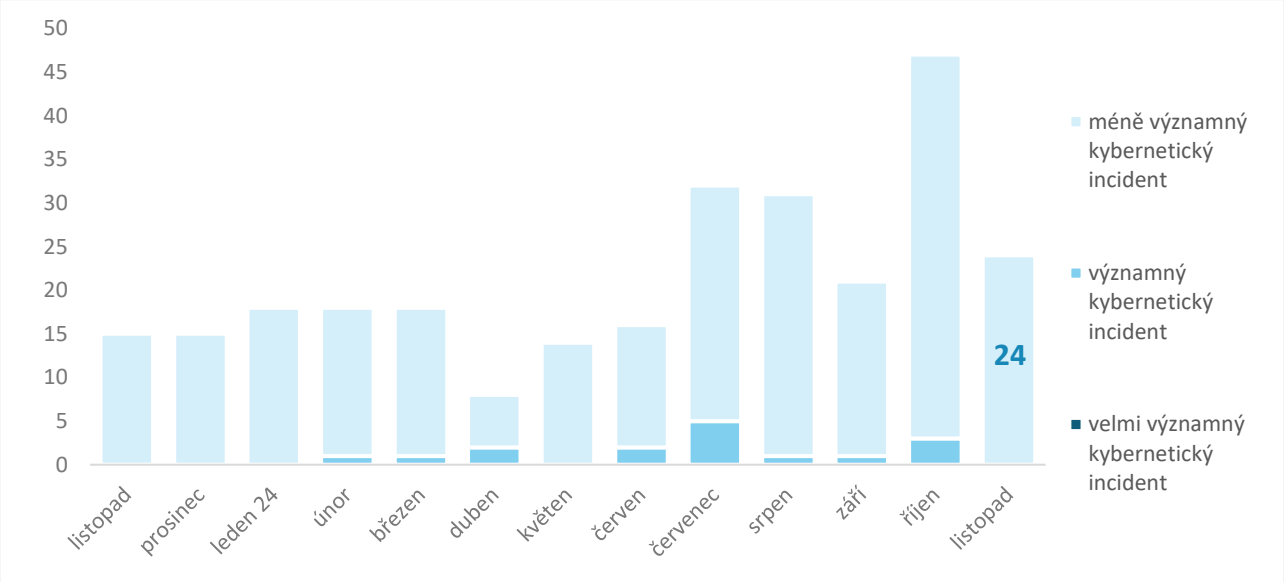
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

V listopadu NÚKIB evidoval 24 kybernetických incidentů. Po rekordním říjnu se tak jedná o návrat k průměrným hodnotám za uplynulý rok.



Závažnost řešených kybernetických incidentů[1]

Závažnost evidovaných incidentů zůstává nadále nízká, všechny listopadové incidenty byly klasifikovány jako méně významné.



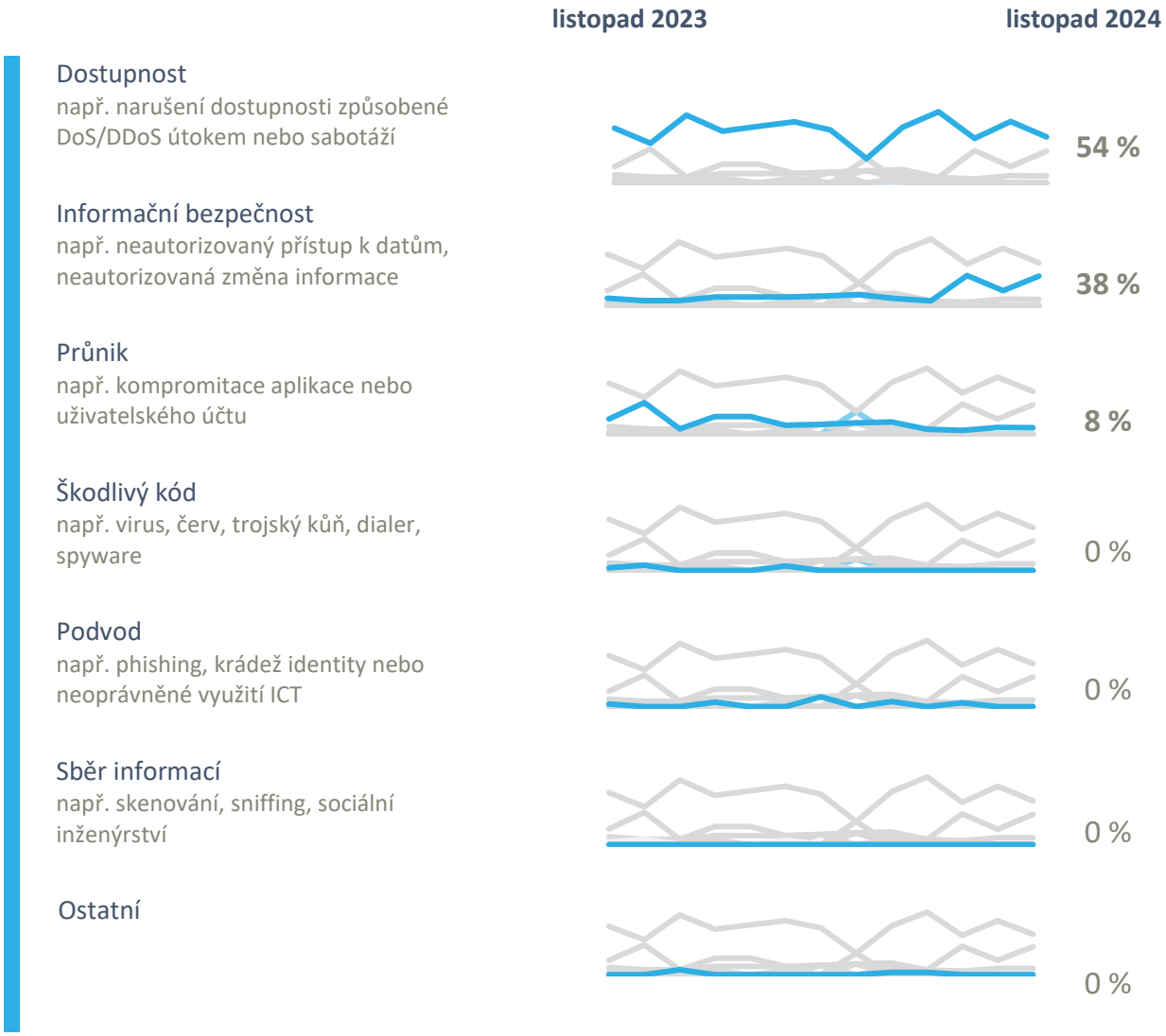
[1] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[2]

Obdobně jako v minulých měsících zůstává nejpočetnější kategorií incidentů Dostupnost. Oproti říjnu však většina incidentů v této kategorii představovala technické závady či miskonfigurace. DDoS útoků bylo v listopadu evidováno pouze pět.

NÚKIB dále řešil incidenty ve dvou kategoriích:

- Devět incidentů spadá do kategorie Informační bezpečnost, pět z nich představovaly ransomwarové útoky a ve zbylých případech šlo o úniky dat či neautorizovaný přístup k systémům.
- V rámci kategorie Průnik evidoval NÚKIB dva incidenty zahrnující prolomení uživatelských účtů. V jednom případě se jednalo o kompromitace uživatelských účtů a následné šíření spamu. Druhý incident se týkal neoprávněné snahy dvou studentů změnit známky svých spolužáků v rámci školního systému za pomoci zcizeného hesla.



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

Trendy v kybernetické bezpečnosti za září pohledem NÚKIB[3]

Phishing, spear-phishing a sociální inženýrství

NÚKIB v listopadu evidoval jeden incident s využitím phishingu. Zasažena byl instituce zdravotnického sektoru, přičemž došlo ke kompromitaci e-mailových schránek dvou jejích zaměstnanců. Útočník z kompromitovaných schránek rozesílal spam.

Malware

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

Zranitelnosti

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

Ransomware

V listopadu bylo evidováno pět případů ransomwarových útoků. Více informací naleznete v kapitole Zaměřeno na hrozbu.

Útoky na dostupnost

V průběhu listopadu NÚKIB evidoval 5 DDoS útoků. Po rekordním říjnu tak frekvence těchto útoků výrazně klesla.

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

Zaměřeno na trend: Ransomware zůstává přetrvávající hrozbou

Uplynulé čtvrtletí ukázalo, že ransomwarové útoky nadále zůstávají významnou hrozbou, a to nejen z pohledu závažnosti, ale i jejich četnosti. V daném období totiž byly zaznamenány nadprůměrné hodnoty incidentů spojených s ransomwarem.

V říjnu NÚKIB dokonce zaregistroval rekordní počet ransomwarových útoků mířených vůči státním i soukromým subjektům. Zatímco se běžně počet tohoto typu incidentů pohybuje v nižších jednotkách, během října jich NÚKIB zaregistroval osm, v listopadu potom pět. **Dle dosavadních poznatků NÚKIB nešlo o koordinovanou kampaň, ale pouze o jednotlivé útoky ze strany řady různých ransomwarových gangů.** V rámci evidovaných ransomwarových útoků bylo zaznamenáno několik typů využitých ransomwarů. Nižší jednotky byly zaznamenány u ransomwarů Ransom Inc a Akira, které v současnosti patří mezi nejaktivnější také napříč celou Evropou.

U řady obětí taktéž NÚKIB eviduje úspěšnou kompromitaci s dopady na chod subjektu. **Neodpovídající či neexistující systém záloh mnohdy vede k tomu, že oběti se s incidentem potýkají řadu dnů až týdnů, což působí i značné finanční škody, nemluvě o reputačních rizicích plynoucích z případného zveřejnění citlivých interních či klientských informací útočníky.**

NÚKIB v kontextu této hrozby již v minulosti vydal podpůrnou analýzu Ransomware: Doporučení pro mitigaci, prevenci a reakci, která shrnuje základní doporučená opatření. Na dokumentu se taktéž podílela AFCEA a NAKIT.

NÚKIB kromě poskytování metodické podpory českým subjektům tuto hrozbu řeší také na mezinárodní úrovni. V říjnu taktéž zástupci NÚKIB, náměstek ředitele pro řízení Sekce strategických agend a spolupráce Pavel Štěpáník a Cyber Attachée pro spolupráci s USA a Kanadou Berta Jarošová, zastupovali Českou republiku na čtvrtém ročníku International Counter Ransomware Summit. V rámci Summitu zástupci na vysoké úrovni z celkem 68 států a organizací, vč. např. Interpolu, diskutovali o nárůstu ransomwarových útoků proti strategickým institucím a subjektům, posílení sdílení informací nebo aktivním narušování činnosti ransomwarových skupin. Summit byl zároveň příležitostí pro diskusi o dalších strategických tématech jako například využívání umělé inteligence v boji s kybernetickými hrozbami, posilování odolnosti či bezpečnosti dodavatelského řetězce v oblasti energetiky.

Obrázek 1: Webové stránky CRI, kde lze nalézt další infromace v kontextu této iniciativy a ransomwaru.

Letošní summit opět potvrdil, že ransomware zůstává jednou z klíčových hrozeb pro národní bezpečnost, kterým čelí státy napříč kontinenty. Podobně jako v předchozích letech, bylo na Summitu přijato obecné společné prohlášení a zároveň prohlášení vyzývající k odpovědnému chování států v kyberprostoru a využívání všech dostupných nástrojů a prostředků v boji proti ransomware. K oběma prohlášením se připojila i ČR.

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.