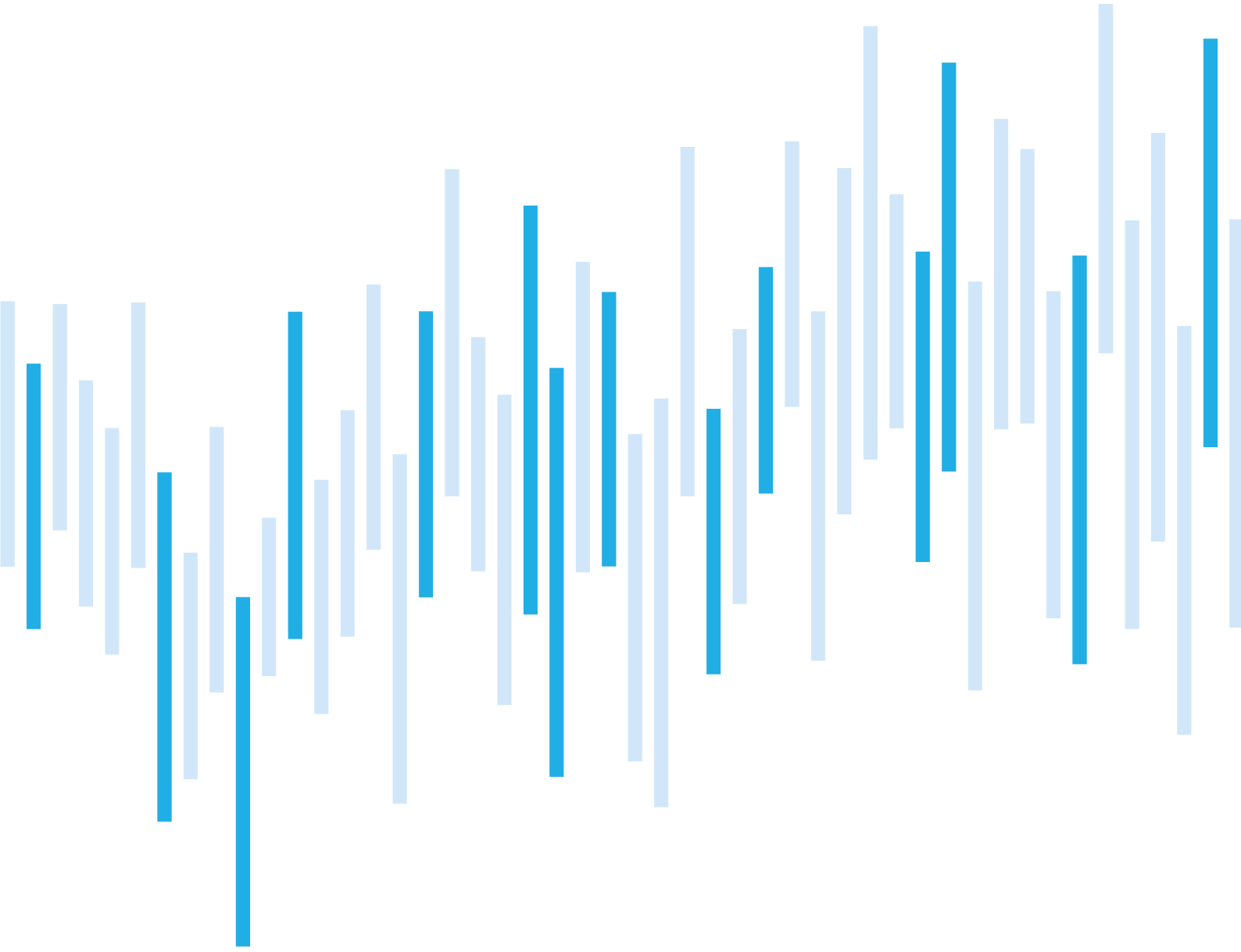
Kybernetické incidenty pohledem NÚKIB

SRPEN 2023



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

V srpnu došlo k více než dvojnásobnému nárůstu registrovaných kybernetických incidentů oproti červenci. Tento nárůst byl ovlivněn další novou vlnou DDoS útoků vedených skupinou NoName057(16). Převážná část těchto útoků mířila na stránky českých bank, jejichž nedostupnost mohla ovlivnit velkou část široké veřejnosti.

V kapitole *Zaměřeno na hrozbu* se věnujeme jednomu z aktuálně nejaktivnějších ransomwarových gangů LockBit. Dle zjištění experta Joe DiMaggia je fungování tohoto gangu v posledních měsících výrazně ovlivněno řadou interních problémů.

Jedním z nich mají být například problémy se zveřejňováním zcizených dat kvůli nedostačující infrastruktuře. Tato zjištění mj. napovídají, že zaplacení výkupného gangu LockBit se nemusí příliš vyplatit. NÚKIB přitom placení výkupného obecně nedoporučuje, a to z celé řady důvodů.

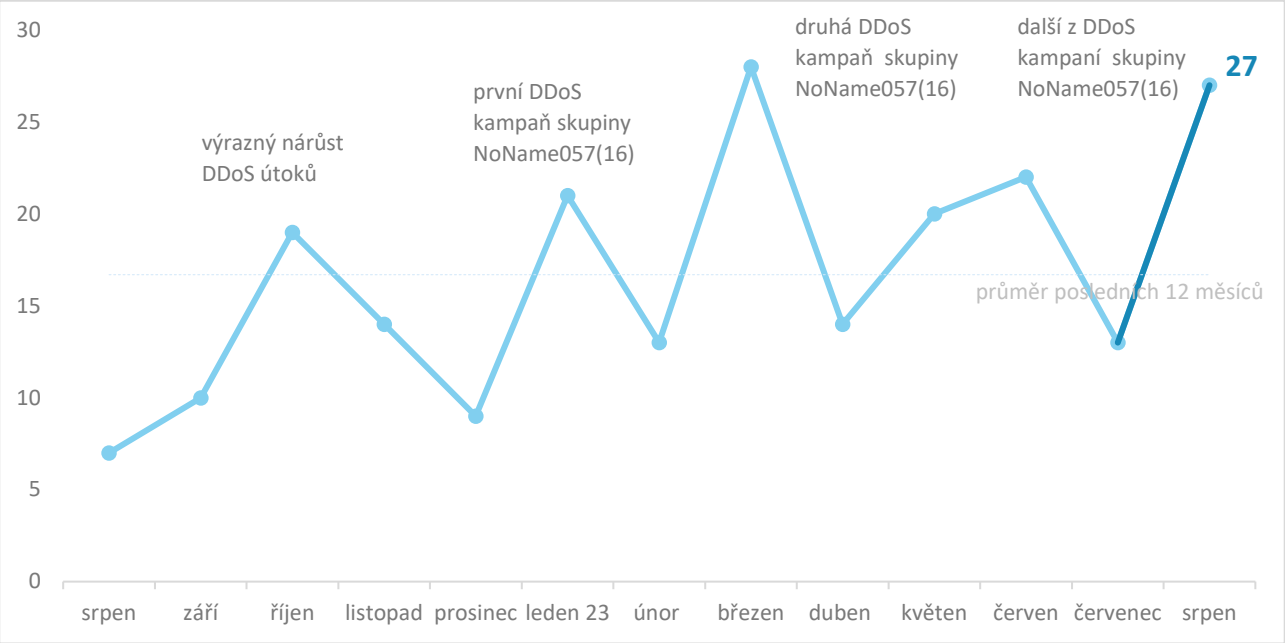
Obsah

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.

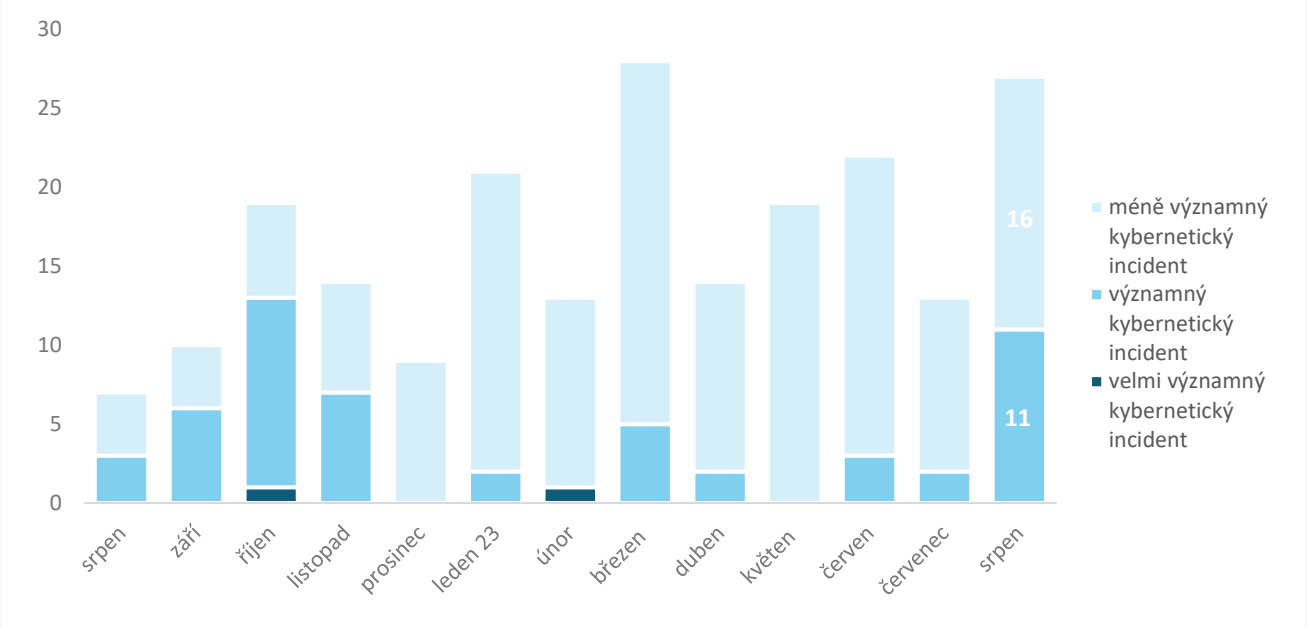
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

V srpnu došlo k více než dvojnásobnému nárůstu registrovaných kybernetických incidentů oproti červenci. Tento nárůst byl ovlivněn další novou vlnou DDoS útoků vedených skupinou No-Name057(16).[1]



Závažnost řešených kybernetických incidentů[2]

Ačkoli v srpnu i nadále převažovaly méně významné kybernetické incidenty, došlo k výraznému nárůstu incidentů významných. Sem spadaly zejména DDoS útoky na stránky českých bank, jejichž nedostupnost mohla ovlivnit velkou část široké veřejnosti.



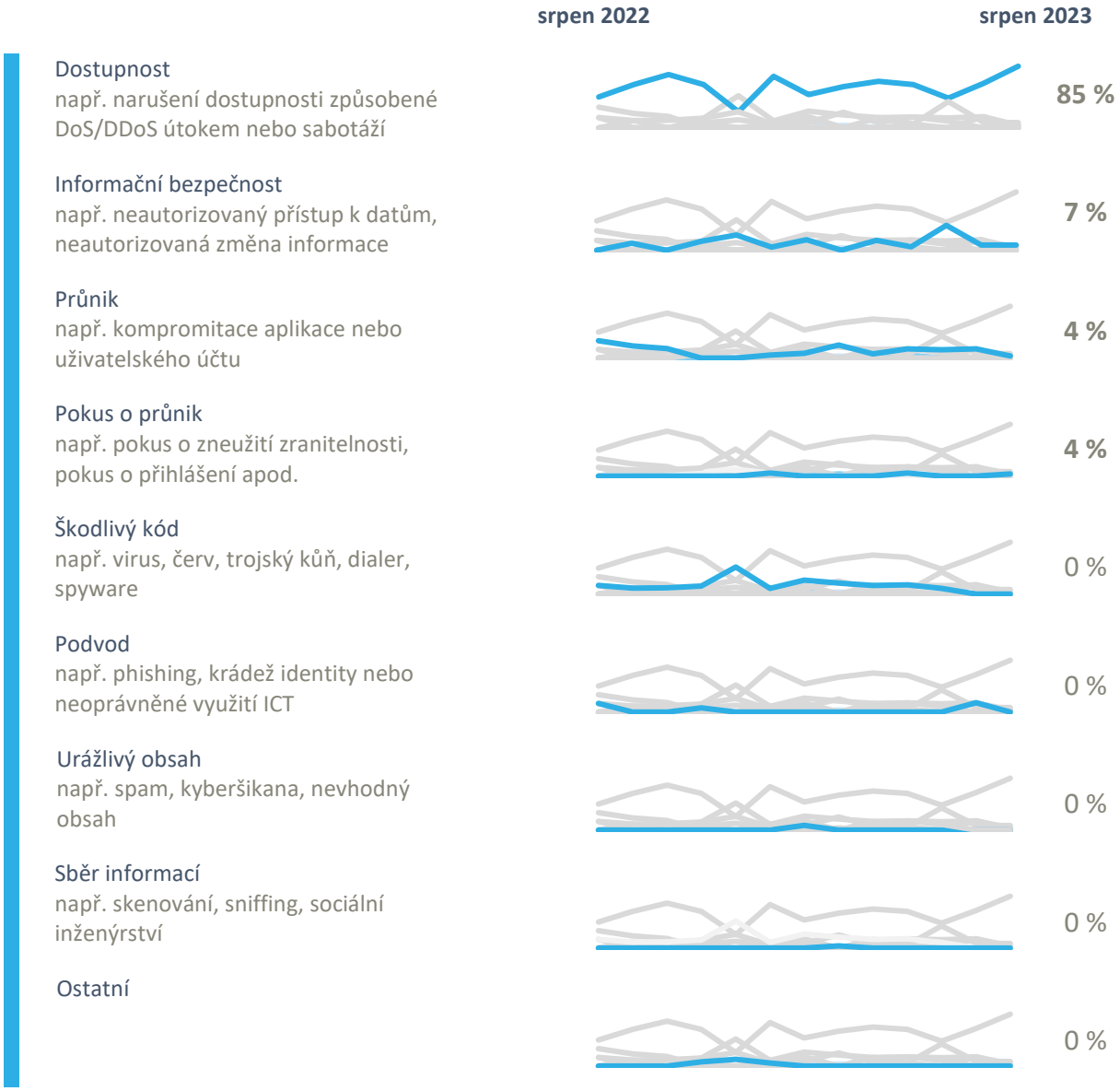
[1] NÚKIB evidoval 18 incidentů u povinných osob dle zákona o kybernetické bezpečnosti. Zbývajících 9 incidentů nahlásily NÚKIB neregulované subjekty.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

V srpnu, podobně jako v uplynulých měsících, převažovaly incidenty spadající do kategorie omezení dostupnosti služeb, které tentokrát tvořily více než čtyři pětiny veškerých incidentů. Převážná část z nich byla způsobena DDoS útoky.

Vedle toho NÚKIB řešil incidenty v těchto třech kategoriích:

- V rámci kategorie Informační bezpečnost byly evidovány dva ransomwarové útoky u neregulovaných subjektů.
- V srpnu došlo k jednomu případu průniku, kdy neznámý útočník kompromitoval účet uživatele na vybraném portálu a posléze na základě získaného přístupu prováděl další škodlivé aktivity.
- NÚKIB evidoval také jeden incident z kategorie pokus o průnik, jehož jediným potvrzeným dopadem byla dočasná nedostupnost služeb.



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

Trendy v kybernetické bezpečnosti za srpen pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

NÚKIB v srpnu upozornil na vishingovou kampaň cílenou na širokou veřejnost. V rámci této kampaně se neznámí útočníci vydávající se za pracovníka banky snaží pod nátlakem a s odkazem na NÚKIB či jeho zaměstnance přinutit oběť k převodu finančních prostředků na „rezervní účet“, aby se tak vyhnula fiktivní hrozbě odcizení těchto prostředků útočníkem.

NÚKIB vyzývá k maximální obezřetnosti a na svých stránkách zveřejnil doporučení, jak se podvodným telefonátům bránit.

Malware

Po delší době NÚKIB v rámci evidence incidentů nezaznamenal žádný malware vyjma dvou níže zmíněných ransomwarů.

Zranitelnosti

V srpnu NÚKIB nevydal žádné upozornění na nově objevené zranitelnosti.

Ransomware

NÚKIB během srpna evidoval celkem 2 ransomwarové útoky. V prvním případě byl neregulovaný subjekt napaden ransomwarem Cryptolocker, ve druhém případě nebyl použitý ransomware dosud identifikován.

Útoky na dostupnost

Již po několikáté v tomto roce provedla proruská hacktivistická skupina NoName057(16) sérii DDoS útoků na české subjekty. Hlavním cílem další vlny útoků, která proběhla na konci srpna, se tentokrát staly bankovní instituce. Více informací o skupině NoName057(16) lze nalézt v lednovém přehledu kybernetických incidentů.

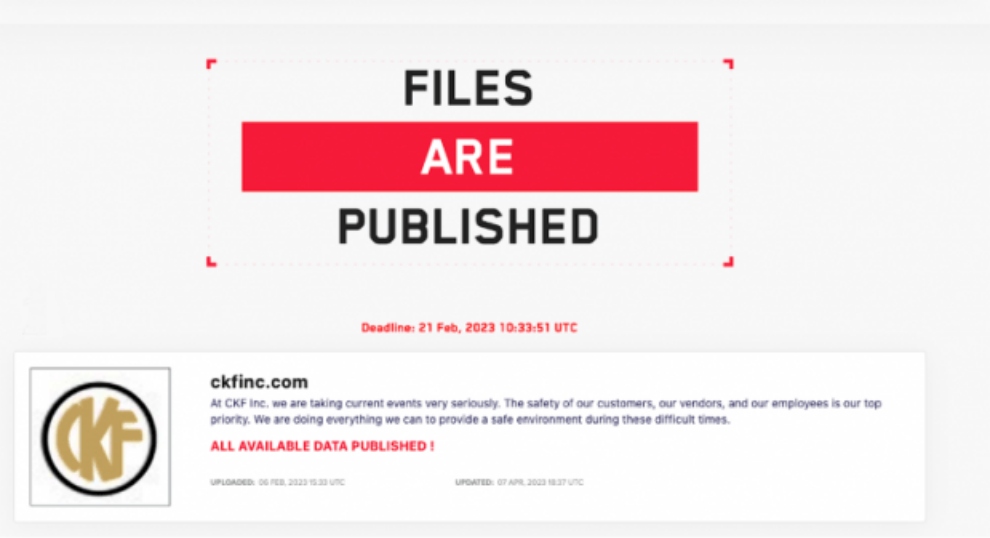
[4] Vývoj ilustrovaný šipkou je vyhodnocován ve vztahu k předešlému měsíci.

Zaměřeno na hrozbu: Problémy ransomwarového gangu LockBit

Ransomwarový gang LockBit je aktuálně jedním z nejaktivnějších kyberkriminálních aktérů na světě. Funguje na bázi modelu ransomware jako služba (tzv. Ransomware-as-a-service, Raas), v rámci kterého nabízí ransomware svým společníkům (tzv. affiliates) za podíl na zisku z výkupného. Ransomware LockBit se v různých variantách již několikrát objevil v rámci incidentů evidovaných NÚKIB a vzhledem k dosavadní úspěšnosti je pravděpodobné (55–70 %), že se některé české subjekty stanou cílem tohoto gangu i v budoucnu.

Ačkoli je LockBit často považován za velmi efektivního a poměrně sofistikovaného aktéra, kyberbezpečnostní expert Jon DiMaggio přišel s překvapivými zjištěními, které odhalují závažné interní problémy tohoto gangu. Jedním z nejvýznamnějších a pro oběti nejvíce relevantních zjištění je skutečnost, že LockBit má od začátku roku 2023 problémy se zveřejňováním zcizených dat. Podle DiMaggia nedostačující infrastruktura gangu vede k tomu, že LockBit často pouze oznámí zveřejnění dat na svých stránkách, aniž by data reálně zveřejnil. Daný stav pak spolu s některými dalšími interními problémy vede k tomu, že řada společníků gangu raději přechází ke konkurenci. Kompletní verzi článku se všemi zjištěními týkajícími se gangu LockBit lze nalézt na stránkách společnosti Analyst1.

Obr. 1: Příklad oběti zveřejněné na stránkách LockBit, jejíž data zveřejněna nebyla



Zdroj: analyst1.com

Výše uvedená zjištění napovídají, že zaplacení výkupného gangu LockBit nemusí být příliš výhodné, jelikož má gang problém naplnit své hrozby. Navíc NÚKIB placení výkupného obecně nedoporučuje, a to z mnoha důvodů. Co se týče kybernetické bezpečnosti obecně, přispívá placení výkupného k posilování útočníků, a to jak po stránce finanční, tak po stránce sebevědomí spojeného s úspěchem útoku. Úspěšné útoky mohou zvyšovat množství a intenzitu dalších útoků stejných i jiných útočníků a nelze vyloučit riziko opakovaného útoku na oběť, která výkupné již zaplatila. Dalším důvodem pro neplacení výkupného je pak také absence faktické záruky, že budou data po zaplacení dešifrována nebo že útočníci data posléze dále neprodají či nezveřejní.

NÚKIB v červnu 2023 vydal aktualizovanou verzi dokumentu, který uvádí nejen doporučení týkající se platby výkupného, ale zejména doporučení zahrnující preventivní a mitigační opatření proti ransomwaru.

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.