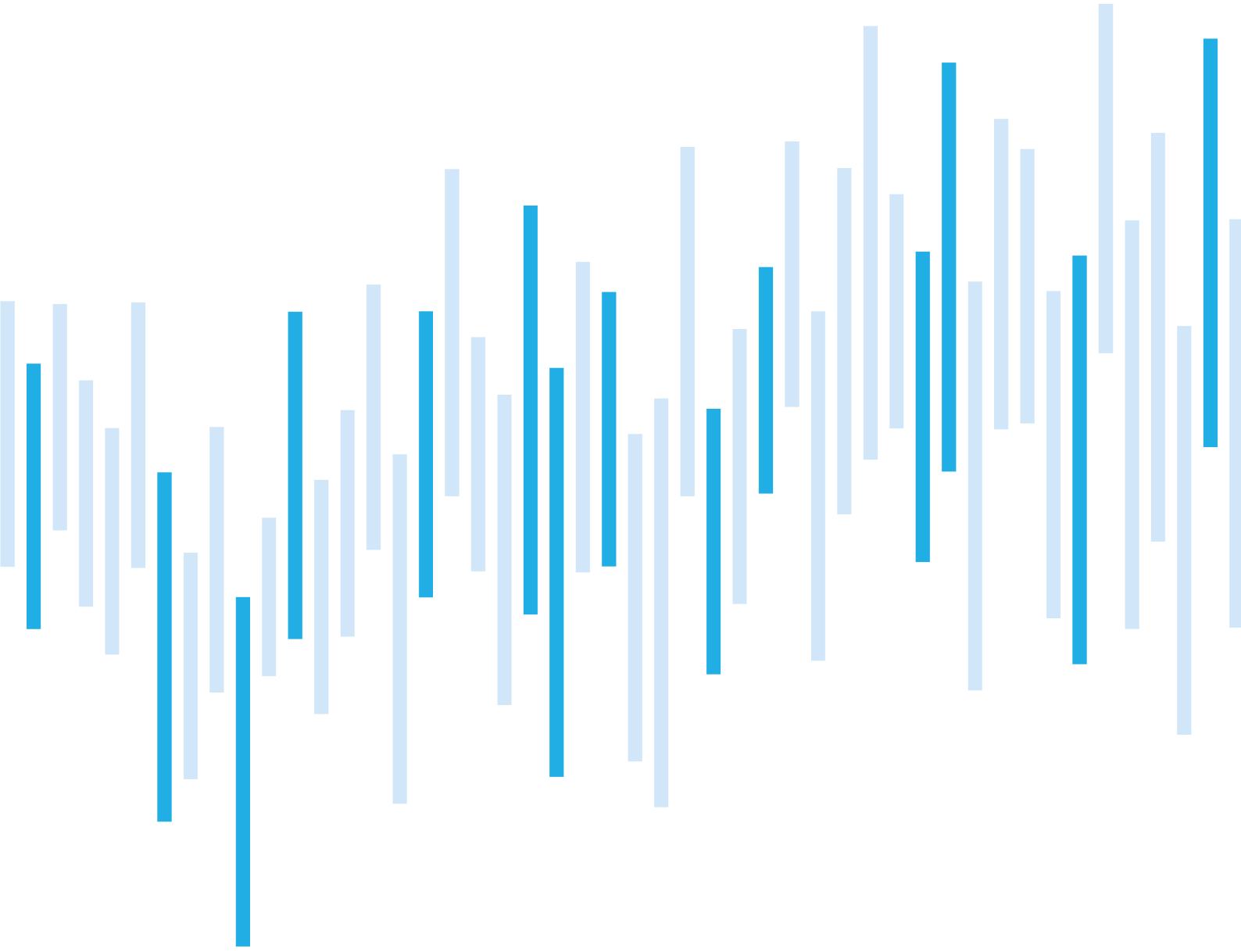
Kybernetické incidenty pohledem NÚKIB

PROSINEC 2023



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Ačkoli v prosinci došlo k mírnému nárůstu evidovaných incidentů oproti předešlému měsíci, i nadále byla výsledná hodnota poměrně nízko pod ročním průměrem, který se pohyboval okolo 19 incidentů měsíčně. Stejně jako v listopadu NÚKIB registroval během prosince pouze méně významné kybernetické incidenty, které v roce 2023 tvořily více než čtyři pětiny všech evidovaných incidentů.

Podobně jako v průběhu celého roku, také v prosinci v rámci klasifikace incidentů dominovala kategorie Dostupnosti. Incidenty z této kategorie v roce 2023 tvořily téměř dvě třetiny všech evidovaných incidentů. Mimo to NÚKIB řešil také incidenty z kategorií Informační bezpečnost a Průnik.

V rámci kapitoly Zaměřeno na hrozbu se tentokrát věnujeme zranitelnosti CVE-2023-42793 v softwarovém řešení TeamCity od společnosti JetBrains, která je aktivně zneužívána ruskou skupinou APT29 (též známá jako CozyBear či NOBELIUM/Midnight Blizzard).

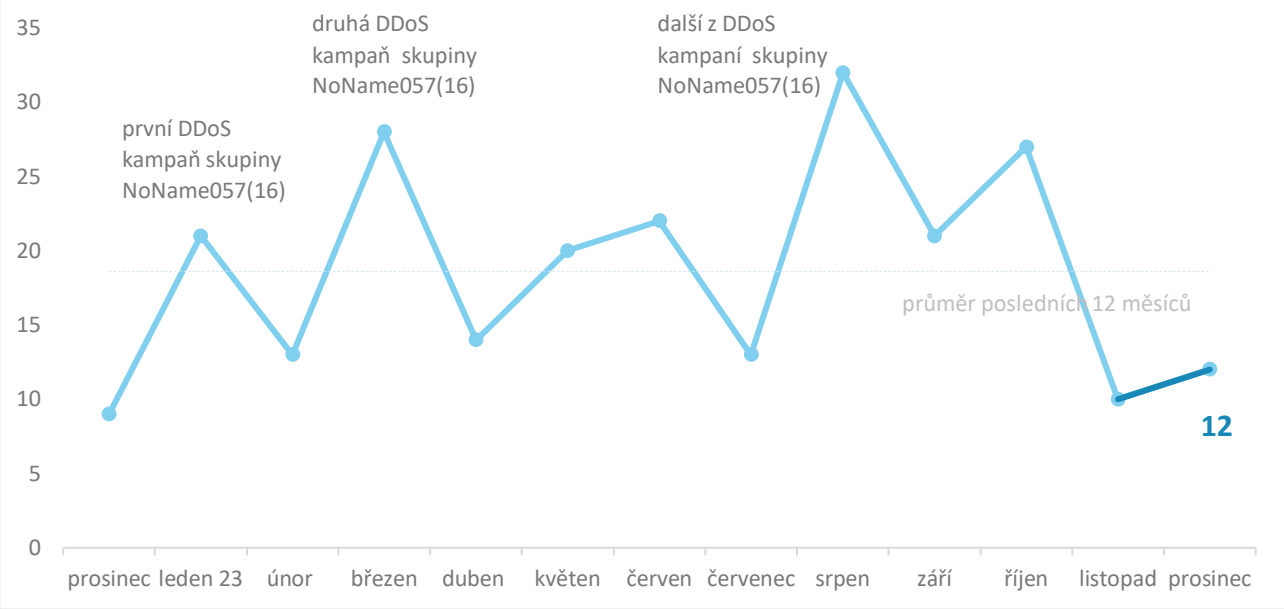
Obsah

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.

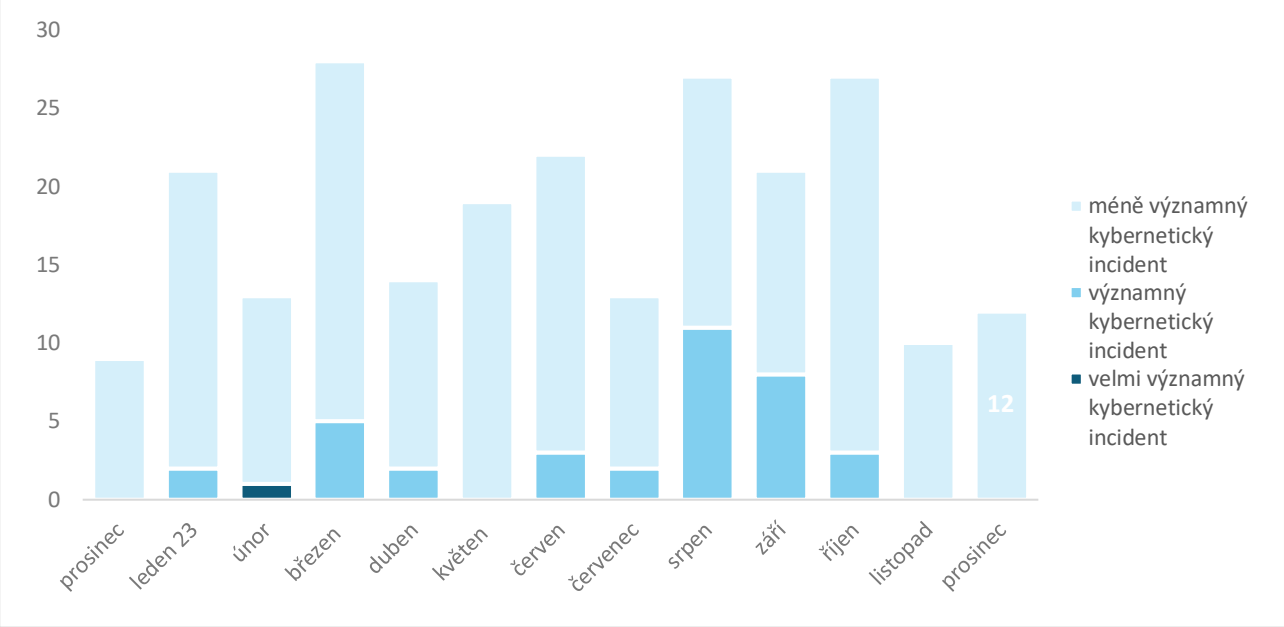
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB[1]

Ačkoli v prosinci došlo k mírnému nárůstu evidovaných incidentů oproti předešlému měsíci, i nadále byla výsledná hodnota poměrně nízko pod ročním průměrem, který se pohyboval okolo 19 incidentů měsíčně.



Závažnost řešených kybernetických incidentů[2]

Stejně jako v listopadu NÚKIB registroval během prosince pouze méně významné kybernetické incidenty, které v roce 2023 tvořily více než čtyři pětiny všech evidovaných incidentů.



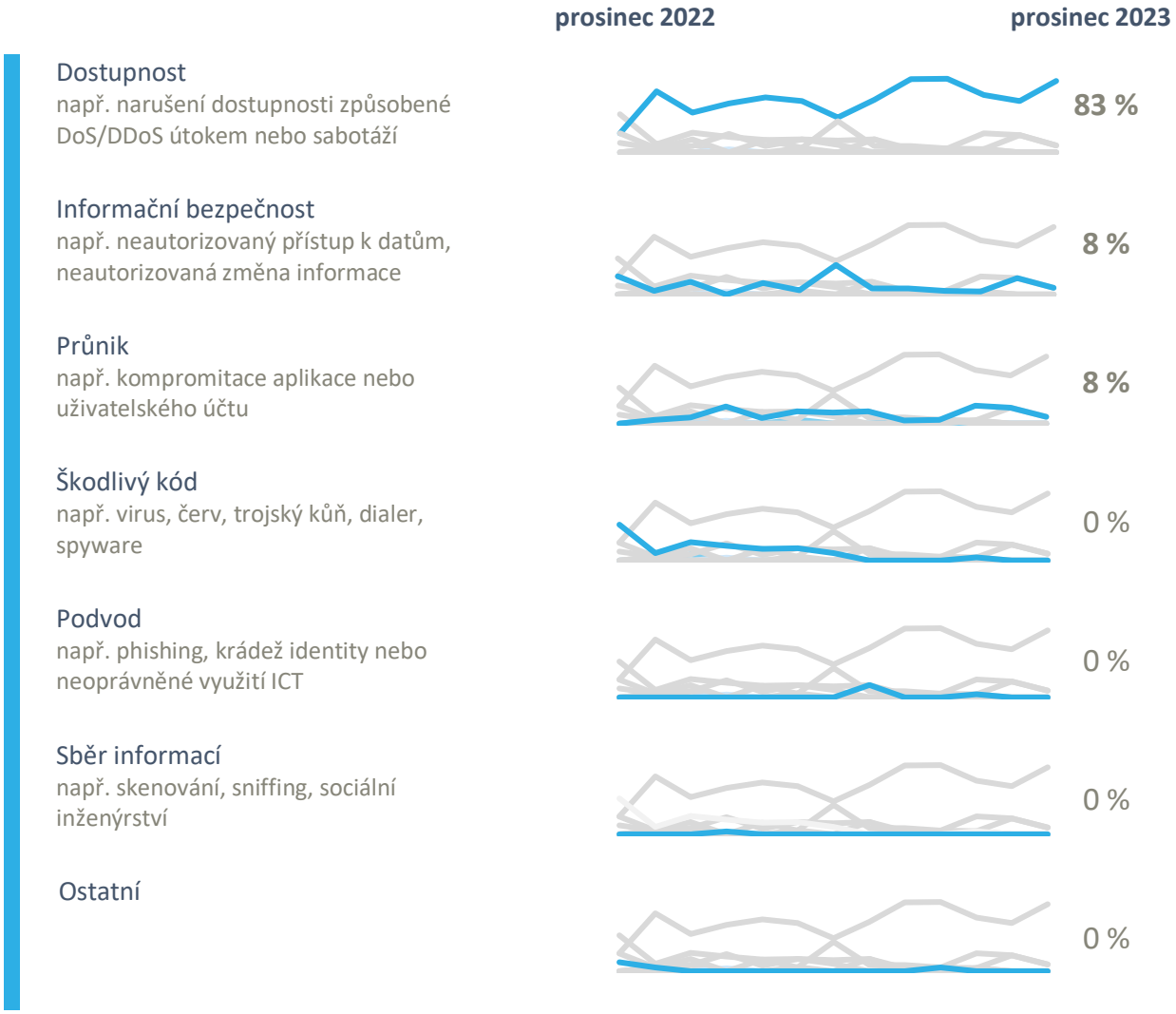
[1] NÚKIB evidoval 9 incidentů u povinných osob dle zákona o kybernetické bezpečnosti. Zbývající 3 incidenty nahlásily NÚKIB neregulované subjekty.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Stejně jako v průběhu celého roku, také v prosinci v rámci klasifikace incidentů dominovala kategorie Dostupnosti. Incidenty z této kategorie v roce 2023 tvořily téměř dvě třetiny všech evidovaných incidentů. Stejně jako v uplynulých měsících byly vyšší počty incidentů vedoucí k narušení dostupnosti spojeny s DDoS útoky.

NÚKIB v průběhu prosince řešil incidenty v dalších dvou kategoriích:

- Během prosince byl evidován průnik do systému regulovaného subjektu, který vedl k úniku identifikačních a kontaktních údajů zákazníků a některých dalších údajů. Prvotní vektor útoku je prozatím neznámý.
- NÚKIB v rámci kategorie Informační bezpečnost zaznamenal útok dosud neznámého ransomwaru, během kterého útočníci zašifrovali data subjektu a následně také smazali jejich zálohy.



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

Trendy v kybernetické bezpečnosti za prosinec pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

NÚKIB v prosinci nezaregistroval žádný případ, v rámci kterého by bylo využito phishingu či jiných metod sociálního inženýrství.

Malware

V prosinci probíhaly kontinuální aktivity v oblasti malwarové analýzy se zaměřením na vybrané incidenty.

Zranitelnosti

Během prosince NÚKIB nevydal žádné plošné upozornění týkající se nových zranitelností.

Ransomware

NÚKIB evidoval pouze jeden incident spojený s ransomwarem. Útočníci získali přístup skrze do internetu otevřený protokol RDP (Remote Desktop Protocol) a posléze zašifrovali soubory a databáze daného subjektu, včetně jejich záloh.

Útoky na dostupnost

V prosinci došlo k mírnému nárůstu DDoS útoků vedených různými aktéry. Za útoky stála například skupina NoName057(16), ale také skupina Anonymous Russia, která se na české cíle zaměřila po více než půl roce. U několika DDoS útoků pak jejich původce není prozatím známý.

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

Zaměřeno na hrozbu: Upozornění na zranitelnost v aplikaci TeamCity

Dne 13. prosince vydala americká kyberbezpečnostní agentura CISA (Cybersecurity & Infrastructure Security Agency) spolu s dalšími americkými, polskými a britskými bezpečnostními institucemi společné varování před zranitelností v softwarovém řešení TeamCity společnosti JetBrains. Konkrétně upozorňují na zranitelnost CVE-2023-42793, která při zneužití umožňuje útočníkovi vzdáleně spouštět škodlivý kód. Podle CISA je tato zranitelnost aktivně zneužívána skupinou APT29 (též známá jako CozyBear či NOBELIUM/Midnight Blizzard) spojovanou s ruskou Službou vnější rozvědky (SVR). Útočníci ji využívají jako prvotní vektor útoku za účelem získání přístupu do infrastruktury oběti, kdy následně provádí hlubší průzkum sítě a pokouší se o zajištění dlouhodobé perzistence.

Obr. 1: Logo softwarového řešení TeamCity

Zdroj: twitter.com

Softwarové řešení TeamCity je převážně CI/CD (continuous integration & continuous delivery) platformou. CI/CD platformy jsou obvykle využívány programátory a DevOps specialisty pro psaní kódu, jeho verzování a následné testování a integraci. Jeden z hlavních důvodů, proč vývojářské společnosti nasazují podobná řešení, je ten, že umožňuje automatizovat velké množství procesů a aktivit spojených s vývojem software.

NÚKIB v kontextu této kampaně chce upozornit na nutnost kontroly dodavatelského řetězce. Pro možnost kontroly dodavatelské řetězce je nutné, aby si každý dodavatel vedl tzv. SBOM (software bill of materials). V rámci tohoto seznamu jednotlivých softwarových komponent lze následně jednoduše dohledat zranitelnou komponentu, identifikovat její zařazení v infrastruktuře a sjednat nápravu.

Při probíhajícím vyhodnocování aktuální kampaně NÚKIB nezaznamenal vysoké riziko zneužívání konkrétní zranitelnosti v softwarovém řešení TeamCity v rámci své konstituence, nicméně i přes to NÚKIB upozorňuje na potřebu kontroly dodavatelského řetězce a při detekování zranitelné verze softwarového řešení TeamCity mitigovat jeho zneužití, v lepším případě aktualizovat tuto komponentu.

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.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, 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.