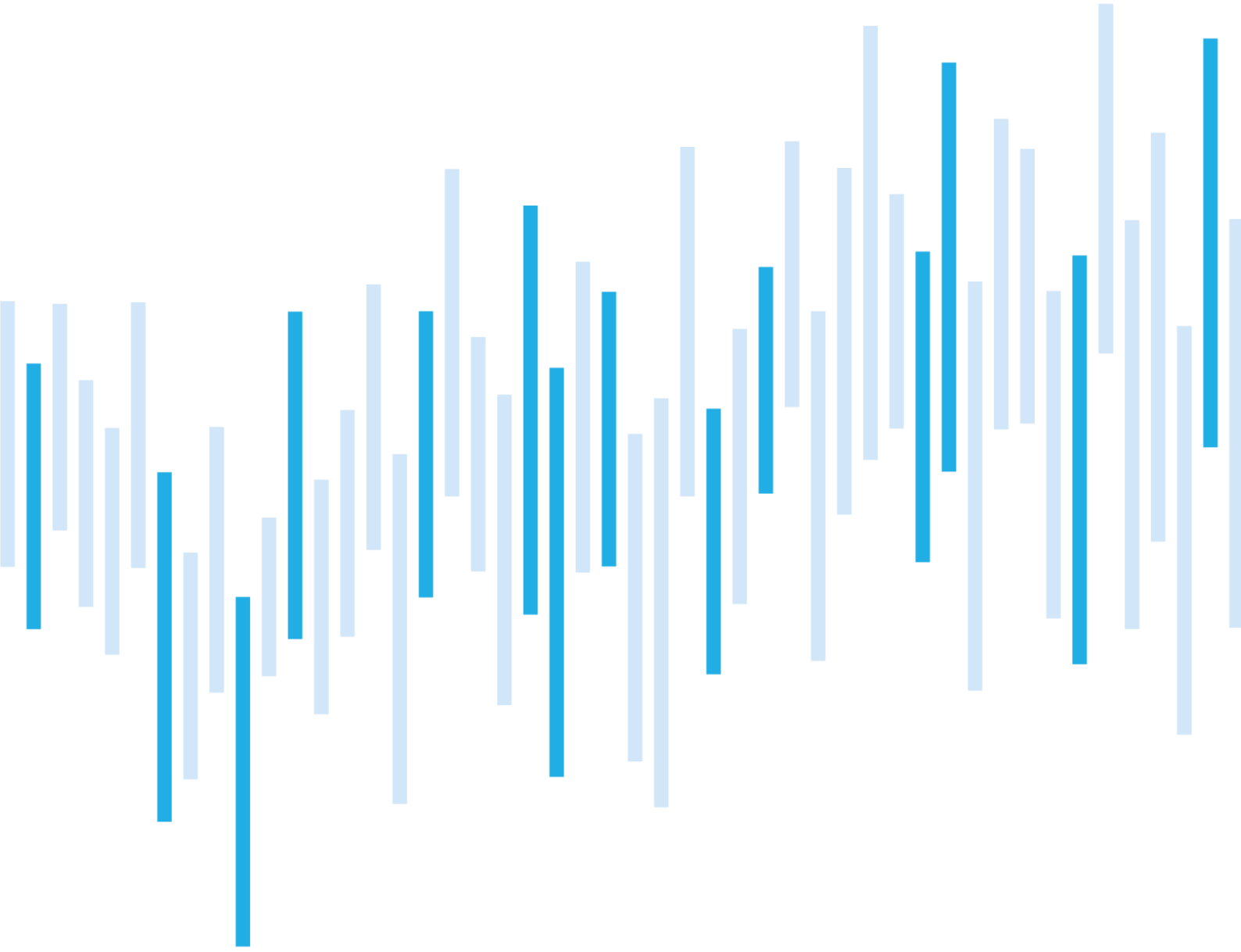
Kybernetické incidenty pohledem NÚKIB

LEDEN 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Leden byl z hlediska počtu kybernetických incidentů průměrným měsícem. NÚKIB poprvé od zveřejnění zranitelnosti Log4Shell zaznamenal incident, ve kterém její zneužití předcházelo ransomwarovému útoku. Útočníci objevili tuto zranitelnost v programu pro správu virtualizací jedné soukromé společnosti. Přes ní se jim podařilo proniknout do jejich systémů a tam spustit ransomware NightSky. Jedná se o nový ransomware, který se poprvé objevil v druhé polovině prosince, tedy chvíli po zveřejnění zranitelnosti Log4Shell.

Veřejnost také informovala NÚKIB o zranitelnostech systémů patřících dvěma regulovaným subjektům. Za všechny podněty k prověření děkujeme. Slabá místa a zranitelnosti v systémech vystavených do internetu patří k nejčastějším vektorům útoků, a i proto se oběma případy v současné době zabýváme.

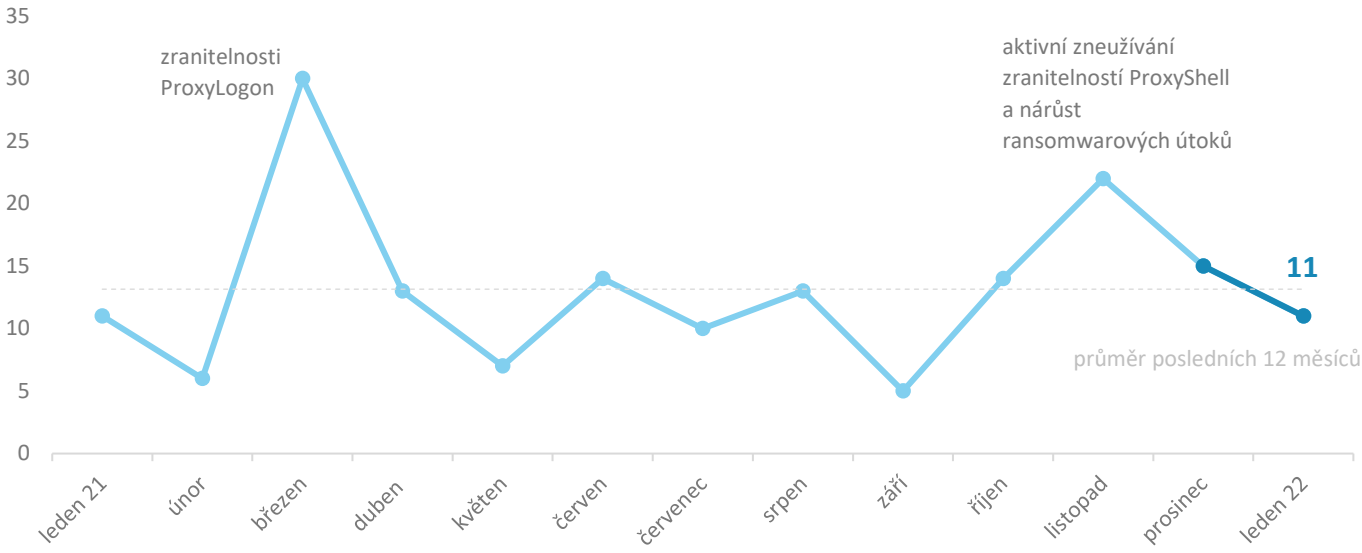
Obsah

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.

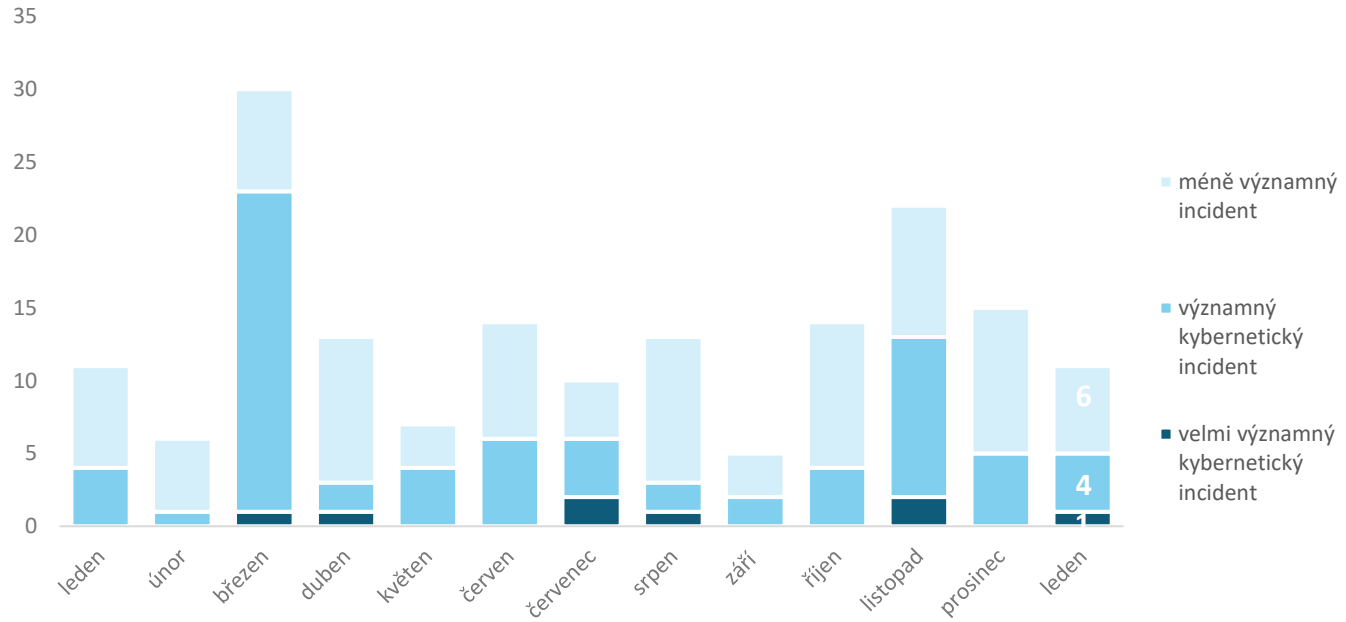
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Z hlediska počtu byl leden s 11 incidenty lehce pod průměrem posledního roku.[1]



Závažnost řešených kybernetických incidentů[2]

NÚKIB eviduje jeden z lednových incidentů jako velmi významný. Způsobila ho vadná komponenta v infrastruktuře postižené organizace, nicméně dopady byly natolik závažné, že incident dostal nejvyšší možnou významnost. Jednalo se o výpadek prvku kritické infrastruktury, který měl plošný dopad na celou zemi.

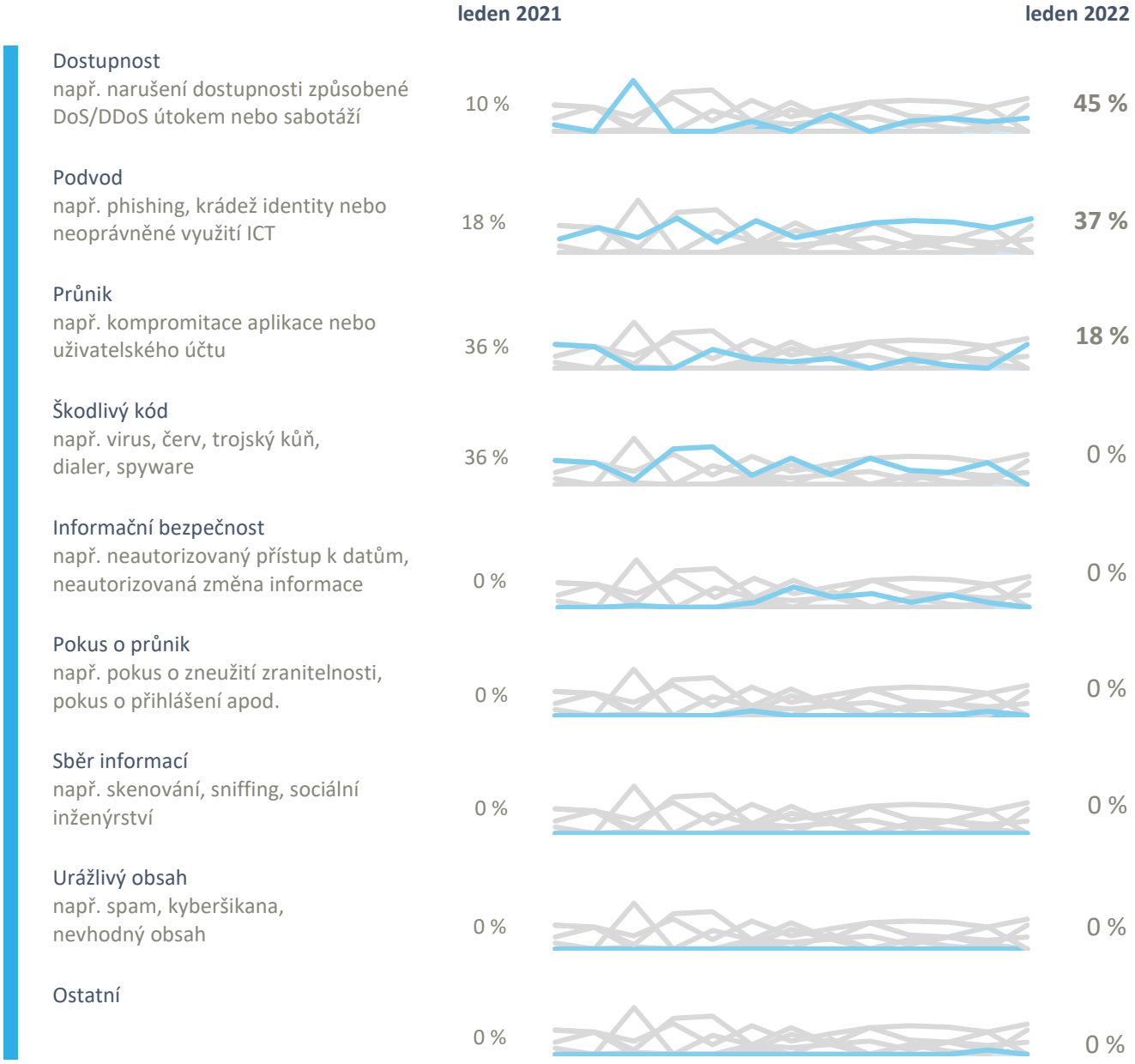


[1] Sedm incidentů nahlásily NÚKIB povinné osoby dle zákona o kybernetické bezpečnosti. O zbylých čtyřech incidentech NÚKIB informovaly subjekty, které pod tento zákon nespadají.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb. a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Lednové incidenty byly rozloženy do tří kategorií:

- Pět incidentů vyústilo v nedostupnost služeb. Ve dvou z těchto případů ovlivnil fungování organizací ransomware, který vedle dat zašifroval i zálohy obětí. Ve zbylých třech případech nedostupnost způsobila technická chyba;
- Druhou nejčastější kategorií byly se čtyřmi incidenty podvody, za kterými stály především phishingové kampaně ve státní správě. Jedním incidentem v této oblasti byl také finanční podvod v soukromé společnosti. Útočníci se neznámým způsobem dostali do e-mailové schránky uživatele zodpovědného za zasílání faktur obchodním partnerům a na fakturách změnili platební údaje. Podvržené číslo účtu následně poslali minimálně dvěma zahraničním firmám a tímto způsobem od nich dostali tisíce eur;
- Poslední dva incidenty NÚKIB klasifikoval jako průnik, jelikož se u nich útočníci dostali do sítí svých obětí skrze zneužití zranitelnosti, včetně zranitelnosti Log4Shell.



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

Trendy v kybernetické bezpečnosti za leden pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

NÚKIB na začátku roku evidoval dvě phishingové kampaně, které se dotkly českých veřejných institucí. V obou případech se útočníkům podařilo kompromitovat uživatelské účty a z nich rozesílat další phishing na různé domény, včetně dalších veřejných institucí. V jedné z kampaní útočník použil tzv. thread hijacking, kdy navázal na již existující komunikaci své oběti a zprávy se škodlivými odkazy poslal v odpovědi na tato vlákna. Napadené organizaci se podařilo situaci během 24 hodin od kompromitace vyřešit, ale v tuto chvíli nevíme, kolik uživatelů z dalších organizací se následně nakazilo.

Malware

Kromě níže zmíněných ransomwarů se v lednových incidentech neobjevil žádný jiný škodlivý kód.

Zranitelnosti

V lednu pokračovalo zneužívání zranitelnosti Log4Shell. Tato zranitelnost způsobila dva z incidentů, které NÚKIB řešil. Útočníci v prvním případě kompromitovali server pro správu mobilních zařízení v jedné instituci veřejné správy, ale žádné další škody nenapáchali. Ve druhém případě, popsaném ve vedlejší části „ransomware“, útočníci po zneužití zranitelnosti ve VDI VMware Horizon nainstalovali do systémů české soukromé společnosti ransomware a zašifrovali její systémy.

Veřejnost také informovala NÚKIB o nedostatcích domén patřících dvěma regulovaným subjektům. NÚKIB se v současnosti oběma případy zabývá.

Ransomware

NÚKIB v lednu řešil dva případy ransomwaru, což je oproti předchozím dvěma měsícům z hlediska jejich počtu pokles. První byl ransomware Jigsaw ve státní organizaci, druhý ransomware NightSky v soukromé společnosti.

Případ ransomwaru NightSky je zajímavý, jelikož se pravděpodobně jedná o první český případ, kdy útočníci nejdříve zneužili zranitelnosti Log4Shell, aby se dostali do sítě oběti, a následně zašifrovali její systémy. NightSky je nový ransomware, který začal poprvé útočit ve druhé polovině prosince 2021, tedy chvíli po zveřejnění zranitelnosti. Podle společnosti Microsoft ho ve své kampani používá čínská skupina, kterou pojmenoval DEV-0401. Nelze ale vyloučit ani použití ze strany jiného aktéra.

Útoky na dostupnost

Téměř polovina lednových incidentů sice skončila nedostupností služeb, ale žádný z nich nebyl zapříčiněn DoS nebo DDoS útokem.

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

Technika měsíce: User Execution

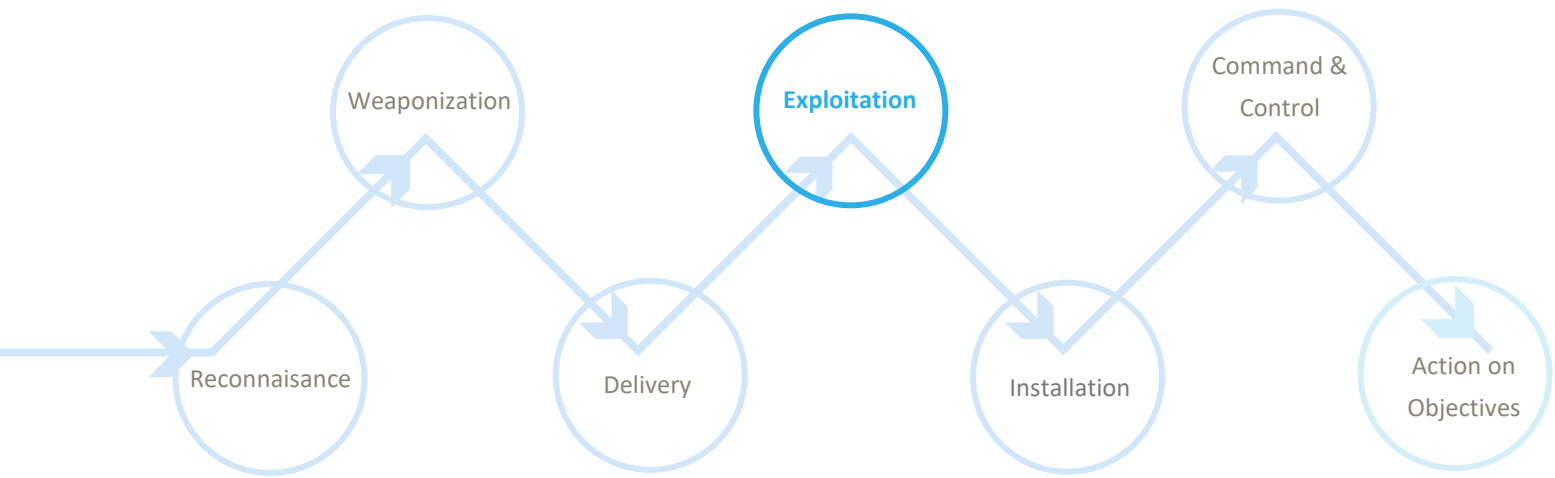
V lednových incidentech se nejčastěji objevila technika, kterou MITRE ATT&CK nazývá „Exploit Public-Facing Application“ a která se pojí především se zneužíváním zranitelností a slabých míst v infrastruktuře vystavené do internetu. Tuto techniku jsme blíže přiblížili v srpnovém reportu. Budeme se proto věnovat technice „User Execution“, která byla v lednu druhou nejpoužívanější a která se objevila u incidentů spojených s phishingem.

User Execution je technika, při níž se útočníci spoléhají na to, že jim sami uživatelé pomůžou s kompromitací systému. Často proto volí formu sociálního inženýrství, kdy se snaží uživatele oklamat tak, aby nevědomky spustili škodlivý kód nebo jim poskytli své přihlašovací údaje do systému. Typickým příkladem jsou phishingové zprávy, ve kterých se útočníci snaží přimět své oběti, aby otevřeli nakaženou přílohu e-mailu nebo vyplnili své údaje do podvržených přihlašovacích stránek. V lednových incidentech jsme zaznamenali především snahu vylákat z uživatelů jejich přihlašovací údaje.

MITRE ID: T1204

Mitigace: Mitigace této útočné taktiky běží ve dvou rovinách. Na technické úrovni lze značné množství phishingu spoléhajícího na podvrženou identitu odesílatele odfiltrovat, pokud poštovní server podporuje a provádí kontrolu příchozí pošty dle ochranného opatření NÚKIB. Vhodným protiopatřením je také sandboxing příloh, alespoň u potenciálně problematických typů souborů (zip, exe, ps1, js), a varování v případě zaheslovaných archivů. Nejčastěji zneužívanou metodou k doručení malwaru jsou stále makra v Office dokumentech. Tomuto vektoru útoku lze technickým opatřením nejsnáze zamezit zablokováním makro funkcí uživatelům, kteří je nezbytně nepotřebují ke své práci, pomocí doménových politik. Tyto technické kroky ale samy o sobě nestačí. Je potřeba neustále školit uživatele, upozorňovat je na rizika spojená se sociálním inženýrstvím a posledními trendy v oblasti phishingu, aby ho byli schopni sami odhalit.

Znázornění „User Execution“ v kill chainu, který ukazuje, ve které fázi útočníci techniku používají:



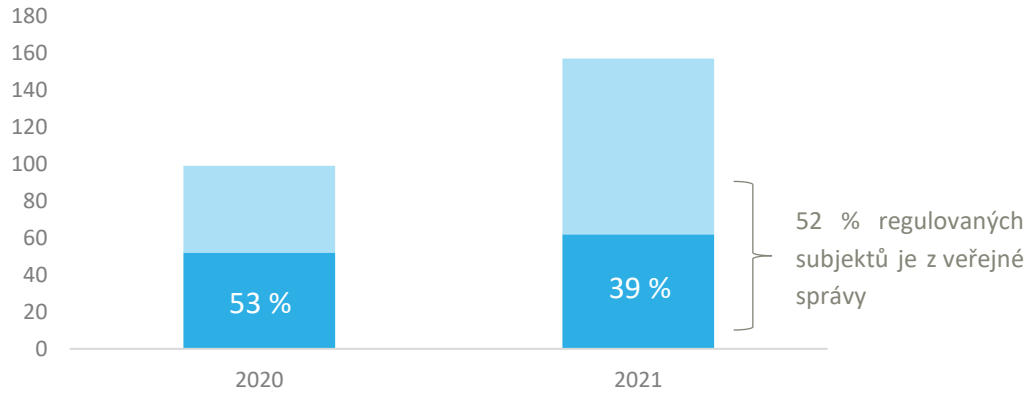
Zaměřeno na sektor: Veřejná správa

Téměř dvě třetiny lednových incidentů zasáhly veřejný sektor. Jednalo o úspěšné phishingové kampaně, ransomware, ale také kompromitaci skrze zneužití zranitelnosti Log4Shell.

7 kybernetických incidentů | **64% zastoupení v lednových incidentech**

Útoky na veřejný sektor patří v incidentech NÚKIB k těm nejčastějším. V posledních dvou letech byl veřejný sektor nejvíce zasaženým sektorem. Podíl kybernetických incidentů v roce 2021 dosáhl téměř 40 % všech řešených incidentů. Jedním z hlavních důvodu vysokého podílu incidentů ve veřejném sektoru je, že více jak polovina regulovaných osob, tedy organizací, které musí dle zákona o kybernetické bezpečnosti hlásit NÚKIB incidenty, jsou právě instituce veřejné správy.

Podíl incidentů ve veřejném sektoru na celkovém počtu incidentů



Veřejný sektor je obecně lákavým cílem pro útočníky, a to jak pro APT skupiny sponzorované cizími státy, tak kyberkriminální uskupení.

APT skupiny provádí sofistikovanější útoky především proti ministerstvům a dalším institucím centrální státní správy, které jsou pro ně zdrojem zpravodajsky, vojensky, politicky i ekonomicky významných informací. Kybernetické špionážní operace usilující o získání podobných informací jsou dlouhodobého charakteru a vyžadují po útočnících pokročilé schopnosti dlouhodobě se vyhýbat odhalení a nepozorovaně z napadeného systému exfiltrovat data. Takovou úrovní know-how disponují zejména státní aktéři nebo jimi sponzorované skupiny. Tyto útoky se nevyhýbají ani ČR, NÚKIB už jich v minulosti několik řešil.

V incidentech NÚKIB se také často objevují útoky na samosprávu. V roce 2020 to byl především ransomware (70 % incidentů v samosprávě). V roce 2021 pak případů ransomwarových útoků v samosprávě ubylo (17 %) a dominovaly kompromitace skrze zneužívání zranitelností (58 %). Pro útočníky je samospráva lákavým cílem především kvůli možnosti finančního zisku. Z naší zkušenosti jsou ohrožena jak velká města, kde existuje možnost vyššího zisku, tak menší obce, kde často bývá kybernetická bezpečnost podfinancovaná a útočníci pravděpodobně neočekávají silné zabezpečení.

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	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. Původce informace může rozsah sdílení dále omezit.
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:WHITE	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.