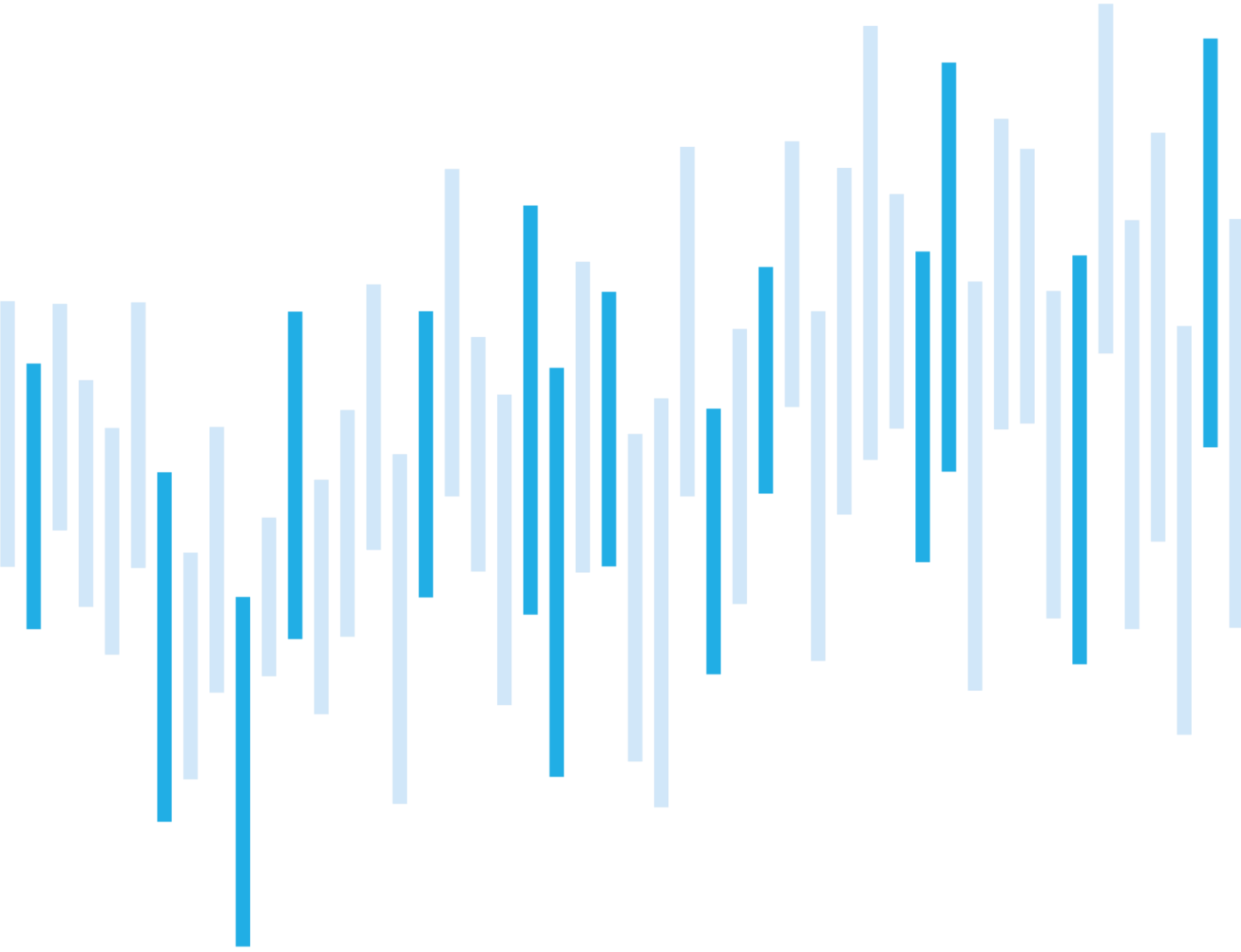
Kybernetické incidenty pohledem NÚKIB

KVĚTEN 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Počet kybernetických incidentů se po předchozím rušném měsíci vrátil do průměrných hodnot. Jejich závažnost nicméně byla relativně vysoká.

Květnové incidenty poznamenalo špatné zabezpečení na straně dodavatelů, kterého útočníci zneužili jako vstupní bod do sítí obětí. Proto jsme se na řízení dodavatelů v tomto reportu více zaměřili. V technice měsíce nastiňujeme, jak mohou útočníci jejich špatného zabezpečení zneužít a v poslední kapitole přibližujeme řízení dodavatelů jako bezpečnostní opatření.

Z květnových událostí je potřeba vyzdvihnout novou kritickou zranitelnost CVE-2022-30190, známou jako „Follina“. Follina činí phishingové útoky mnohem jednoduššími. Zranitelnost se dotýká balíku Microsoft Office a útočníci skrze ni mohou spustit škodlivý kód, aniž by oběť povolila makra. Zranitelnost začaly po celém světě ihned zneužívat hackerské skupiny. NÚKIB ji v posledních květnových incidentech neevidoval, nelze ale vyloučit, že se situace v následujících dnech změní. Vzhledem k jejímu relativně jednoduchému zneužití a doposud neexistující opravné aktualizaci nelze vyloučit, že budeme pozorovat podobnou vlnu kybernetických útoků, jako tomu bylo v případě zneužívání zranitelností MS Exchange v roce 2021.

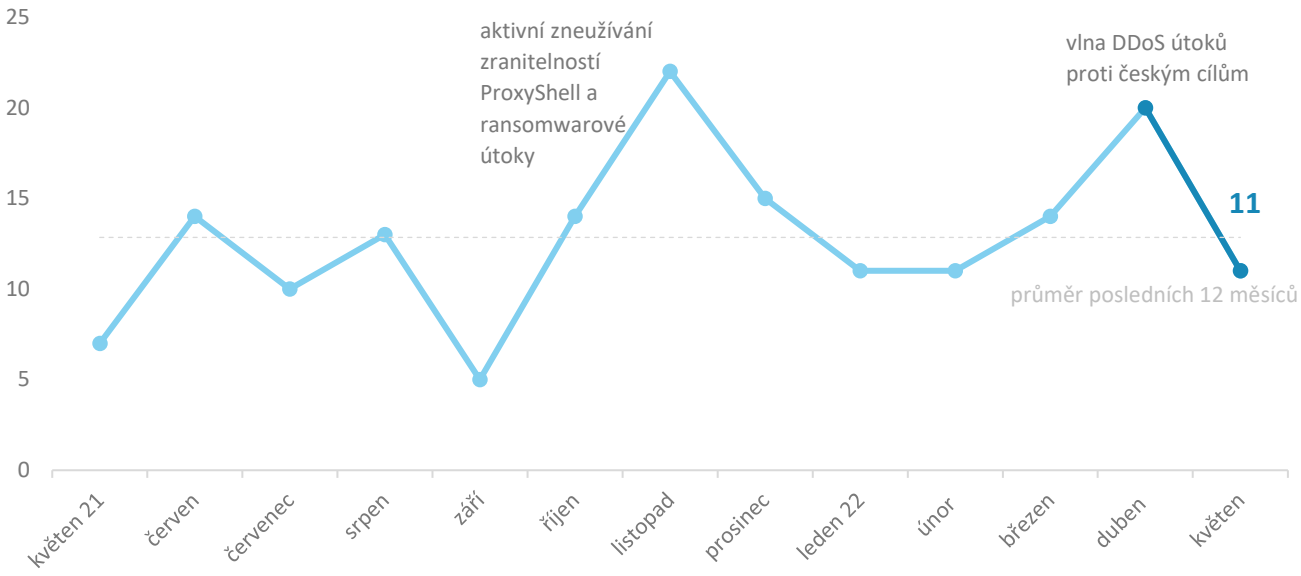
Obsah

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.

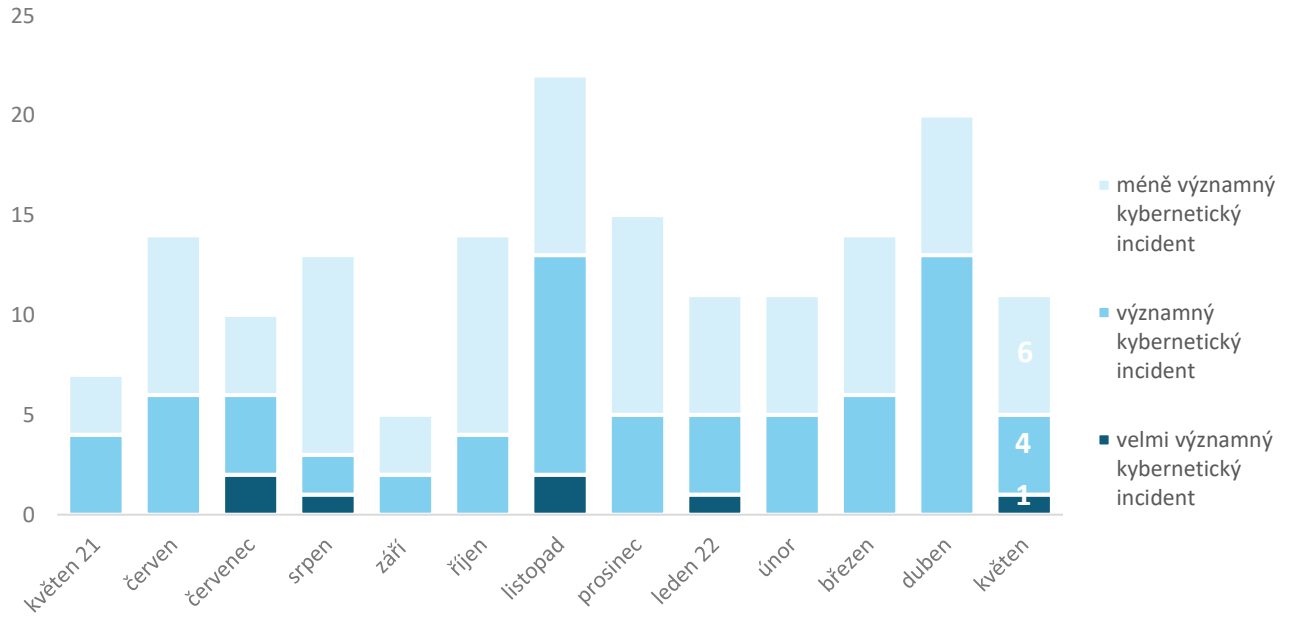
Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Po předchozím rušném měsíci se v květnu počet incidentů vrátil přibližně na průměr posledních dvanácti měsíců.[1]



Závažnost řešených kybernetických incidentů[2]

Po třech měsících se v kybernetických incidentech znovu objevil velmi významný incident. Útočníkům se podařilo kompromitovat síť s kritickými systémy, znemožnit napadené organizaci vykonávat svou funkci a způsobit jí plošné škody.

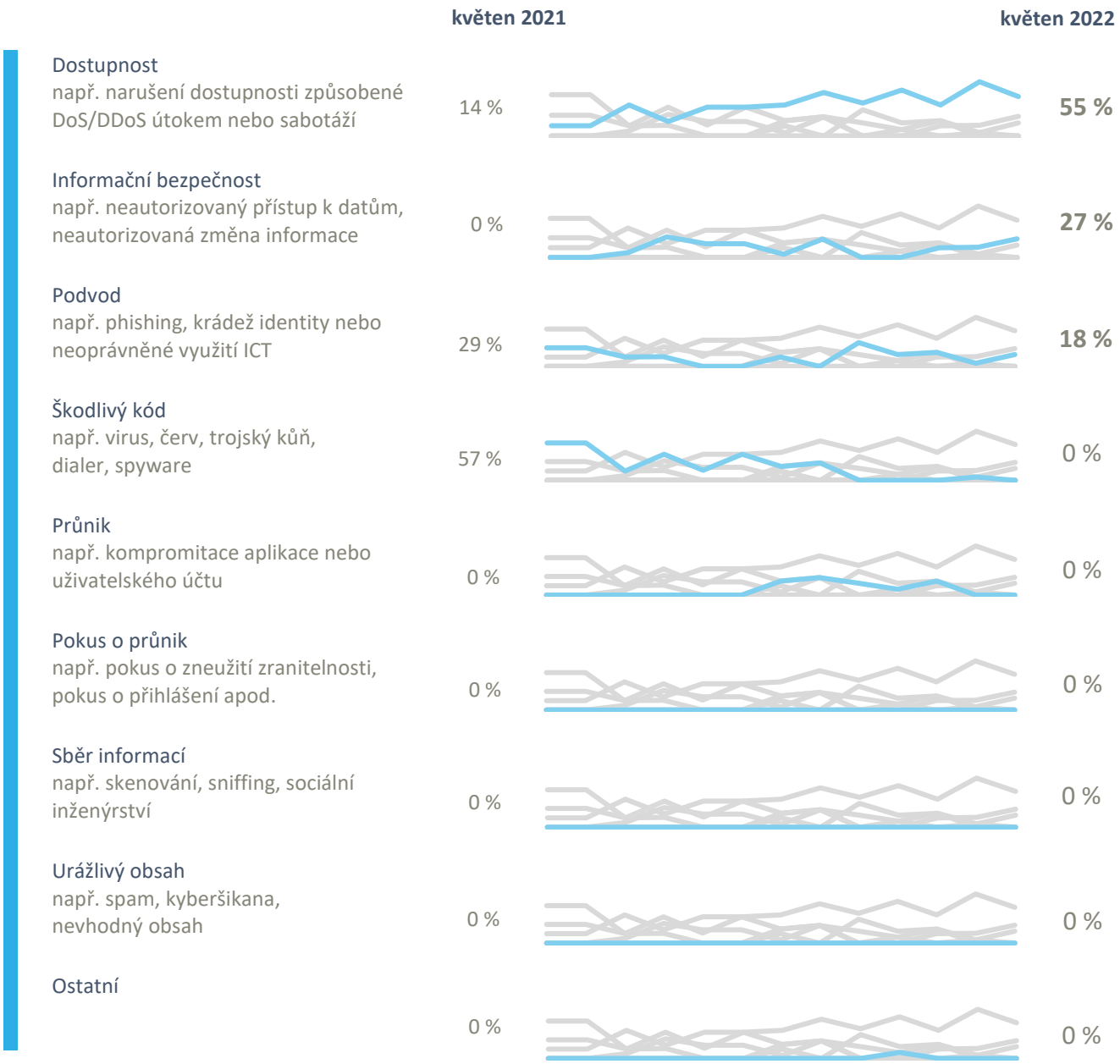


[1] Devět incidentů nahlásily NÚKIB povinné osoby dle zákona o kybernetické bezpečnosti. O zbylých dvou incidentech NÚKIB informovaly subjekty, které pod tento zákon nespadají.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb. a v interní metodice NÚKIB.

Klasifikace incidentů nahlášených NÚKIB[3]

Květnové kybernetické incidenty NÚKIB zařadil do tří kategorií:

- Více jak polovina kybernetických incidentů vyústila v nedostupnost služeb. Až na jeden případ stály za nedostupnostmi technické chyby. Jedinou výjimkou byl kybernetický incident způsobený ransomwarem, při kterém útočníci zašifrovali data oběti.
- Druhou nejčastější kategorií byly incidenty, při nichž došlo k neoprávněnému přístupu k informacím. Do této kategorie se propsal také ransomwarový útok, při kterém útočníci před zašifrováním data napadené organizace exfiltrovali;
- Dva incidenty NÚKIB zařadil do kategorie podvodů. Oba se týkaly phishingu. První byla rozsáhlá phishingová kampaň zacílená na klienty jedné z komerčních bank. Snahou útočníků bylo získat přihlašovací údaje do internetového bankovnictví a následně z něj převést peníze. Druhý phishing byl odhalen ve chvíli, kdy z domény napadené vzdělávací instituce odcházely phishingové e-maily na další adresy.



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

Trendy v kybernetické bezpečnosti za květen pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

Phishingové útoky nebo pokusy o ně se v hlášeních NÚKIB objevují pravidelně (viz graf ke kategorii podvod na předchozí straně). Nejzávažnější z květnových útoků byla rozsáhlá a cílená kampaň proti klientům jedné z českých komerčních bank. Útočníci se skrze podvodné sms a e-maily snažili získat přístup do jejich internetového bankovnictví a z něj pak převést peníze. Útočníci přesvědčovali klienty banky k otevření škodlivého odkazu tvrzením, že jejich účet byl zablokován a pro odblokování se musí znovu přihlásit.

Malware

NÚKIB na základě dat z květnových incidentů žádný malware kromě níže zmíněných ransomwarů neanalyzoval.

Zranitelnosti

Koncem května se objevila nová kritická zranitelnost CVE-2022-30190, také známá jako „Follina“, která se dotýká kancelářského balíku Microsoft Office. Útočníci skrze ni mohou spustit škodlivý kód i bez toho, aniž by oběť povolila makra. To činí phishingové útoky mnohem jednodušší. Zranitelnosti začaly ihned zneužívat hackerské skupiny, včetně APT skupin podporovanými vládami třetích zemí. NÚKIB proto na svých webových stránkách na zranitelnost upozornil a poskytl několik doporučení, jak zranitelnost mitigovat do doby, než bude dostupná opravná aktualizace.

Ransomware

Ransomwarové útoky od začátku roku stabilně tvoří přibližně pětinu incidentů, které NÚKIB eviduje, a stejně tomu bylo i v květnu. Dva z květnových incidentů byly způsobeny právě ransomwary, které jsou nabízeny jako služba a v kybernetickém prostoru je útočníci celosvětově nasazují od léta 2021.

Útoky na dostupnost

Po předchozím měsíci, který charakterizovaly vlny DDoS útoků proti českým cílům, nastal s ohledem na útoky na dostupnost klid. Ani jeden z incidentů, který NÚKIB v květnu řešil, nezpůsobil DDoS útok.

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

Technika měsíce: Trusted Relationship

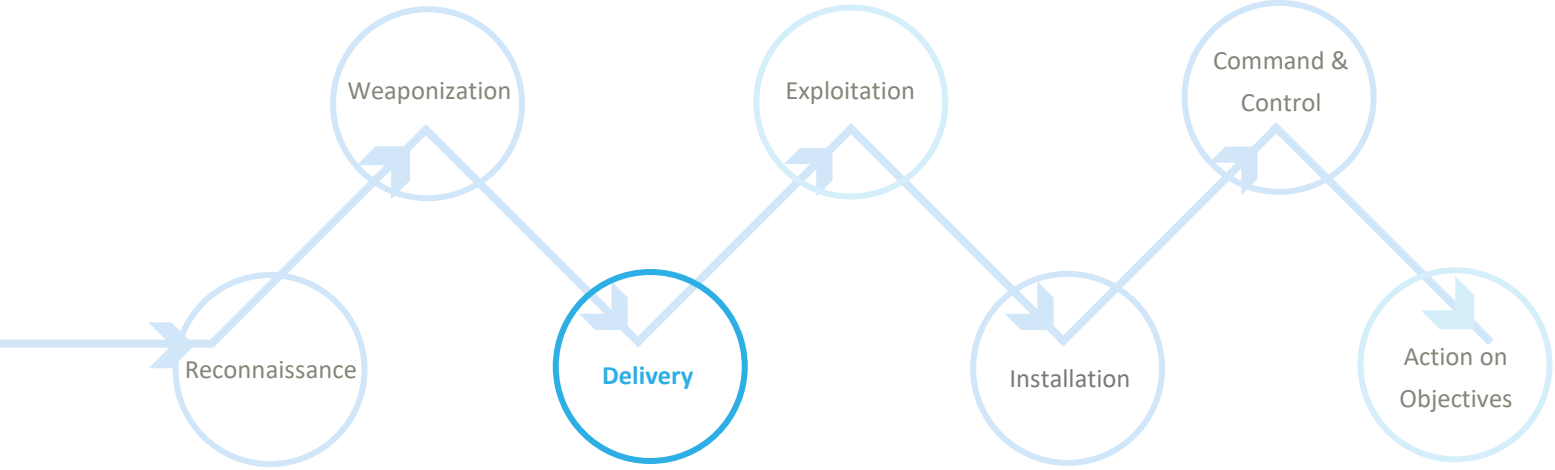
NÚKIB kybernetické incidenty vyhodnocuje mimo jiné na základě rámce MITRE ATT&CK, který slouží jako přehled známých technik a taktik používaných při kybernetických útocích. V květnových incidentech převažovala technika „Malicous File“. Tři ze závažných kybernetických incidentů a událostí, které NÚKIB v květnu řešil, byly ale způsobeny nedostatečným zabezpečením na straně dodavatele. Proto je technika měsíce tentokrát zaměřena na toto téma.

Organizace často poskytují dodavatelům přístup do svých systémů, aby je mohli spravovat. Dodavatelé mohou mít přístup do sítí zákazníků například skrze VPN. **Trusted Relationship** je technika, při níž útočníci těchto přístupů zneužívají, aby přes ně kompromitovali systémy zamýšlených obětí – tedy jejich klientů. Pokud dodavatel přístupy do sítí svých klientů nezabezpečí nebo je zabezpečí hůře než přístupy, které si jejich klientská organizace spravuje sama, pro útočníky to může být nejsnadnější cesta dovnitř. Útočníci mohou tuto techniku také zneužít k útokům na dodavatelský řetězec.

MITRE ID: T1199

Mitigace: Prvním krokem k mitigaci této techniky je správné zabezpečení účtů, které dodavatelé používají pro přístup do sítí obětí. Čím robustněji bude mít dodavatel přístupy do sítí obětí zabezpečeny, tím menší bude riziko jejich zneužití. Proto by organizace pro všechny vzdálené přístupy měly vyžadovat dvoufaktorovou autentizaci, princip nejnižšího možného oprávnění a u nejdůležitějších systémů i whitelisting. Dalším preventivním krokem je segmentace sítě tak, aby komponenty v infrastruktuře, které nevyžadují plošné přístupy, byly izolovány. Organizace by také měly pamatovat na organizační bezpečnostní opatření v podobě řízení dodavatelů, které je blíže popsáno na straně 6.

Znázornění techniky Trusted Relationship v kill chainu, který ukazuje, ve které fázi útočníci techniku používají:



Zaměřeno na bezpečnostní opatření: Řízení dodavatelů

NÚKIB v květnu řešil několik závažných případů, které zdůrazňují potřebu procesu řízení dodavatelů. V jednom z kybernetických incidentů, který napadené organizaci způsobil značné škody, se útočník dostal do sítě své oběti skrze kompromitovaný VPN účet její servisní firmy. V tuto chvíli není jasné, jak servisní společnosti přihlašovací údaje k tomuto účtu unikly, ani jak se k nim útočník dostal. Útočník je použil jako vstupní bod do napadené organizace, odkud se pak laterálně rozšířil do dalších systémů.

Na další dva případy špatného zabezpečení přišly organizace samy, pravděpodobně ještě před tím, než slabého místa stačili zneužít útočníci. Organizace zjistily, že dodavatel informačního systému jejich citlivá data, mimo jiné prohřešky proti bezpečnosti, ukládá na webové uložiště bez potřeby autentizace. Podle dosavadních poznatků s daty nikdo neoprávněně nemanipuloval a NÚKIB proto oba případy vede jako kybernetickou událost. Téměř neexistující zabezpečení dat by ale pro útočníky bylo velmi pravděpodobně tou nejsnazší cestou k jejich získání a dalšímu zneužití.

Povinnosti k řízení dodavatelů vyplývající z legislativy

Řízení dodavatelů je jedním z organizačních bezpečnostních opatřeních, k jejichž provádění jsou povinny vybrané osoby spadající do působnosti zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Proces řízení dodavatelů slouží především k identifikaci rizik spojených s využíváním služeb třetích stran a jejich následné mitigaci.

V rámci řízení všech svých dodavatelů jsou uvedené osoby povinny stanovit pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací, seznamovat své dodavatele s těmito pravidly a vyžadovat jejich plnění a řídit rizika spojená s dodavateli. V rámci řízení bezpečnosti lidských zdrojů povinné osoby zajistí poučení dodavatelů o jejich povinnostech a o bezpečnostní politice a v rámci zvládání kybernetických bezpečnostních incidentů zajistí oznamování neobvyklého chování systému a podezření na jakékoliv zranitelnosti.

Uvedené osoby jsou také povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém (tzv. významného dodavatele) a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. V rámci výběrových řízení a před uzavřením smlouvy je potřeba provádět hodnocení rizik souvisejících s plněním předmětu výběrového řízení. Dále je potřeba v rámci uzavíraných smluvních vztahů stanovit způsoby a úrovně realizace bezpečnostních opatření a určit obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření, provádění pravidelného hodnocení rizik a pravidelné kontroly zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany (a v reakci na rizika a zjištěné nedostatky zajistí jejich řešení). A v neposlední řadě též zajistit, aby smlouvy, které jsou s nimi uzavírány, obsahovaly relevantní oblasti uvedené v příloze č. 7 vyhlášky o kybernetické bezpečnosti, a pravidelně plnění smluv s významnými dodavateli přezkoumávat z hlediska systému řízení bezpečnosti informací.

Řízení dodavatelů je kontinuální proces, do něhož vstupuje mnoho proměnných. Velcí dodavatelé jsou mnohdy v pozici, kdy si mohou určovat podmínky poskytování svých služeb a zákazník má jen omezené možnosti včlenění svých bezpečnostních požadavků do smluv. Stejně tak není vždy snadné zkontrolovat, jakým způsobem dodavatel v praxi přistupuje k zajištění bezpečnosti jím dodávaných

služeb a zda dodržuje všechna opatření, která deklaruje. Ani v takovém případě však povinné osoby nemohou rezignovat na své povinnosti zajistit bezpečnost svých systémů a dat v nich obsažených a dbát na dodržování základních bezpečnostních zásad, pravidel pro ochranu dat a nejlepší praxe v oblasti kybernetické bezpečnosti. Je tak potřeba s dodavateli aktivně a pravidelně komunikovat, vyžadovat informace o způsobu poskytování nasmlouvaných služeb, požadovat okamžitou nápravu nedostatků, důsledně vymáhat plnění smluv, nebát se odejít od dodavatele, který neposkytuje kvalitní služby, neuzavírat smlouvy s lock-in efektem apod.

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.