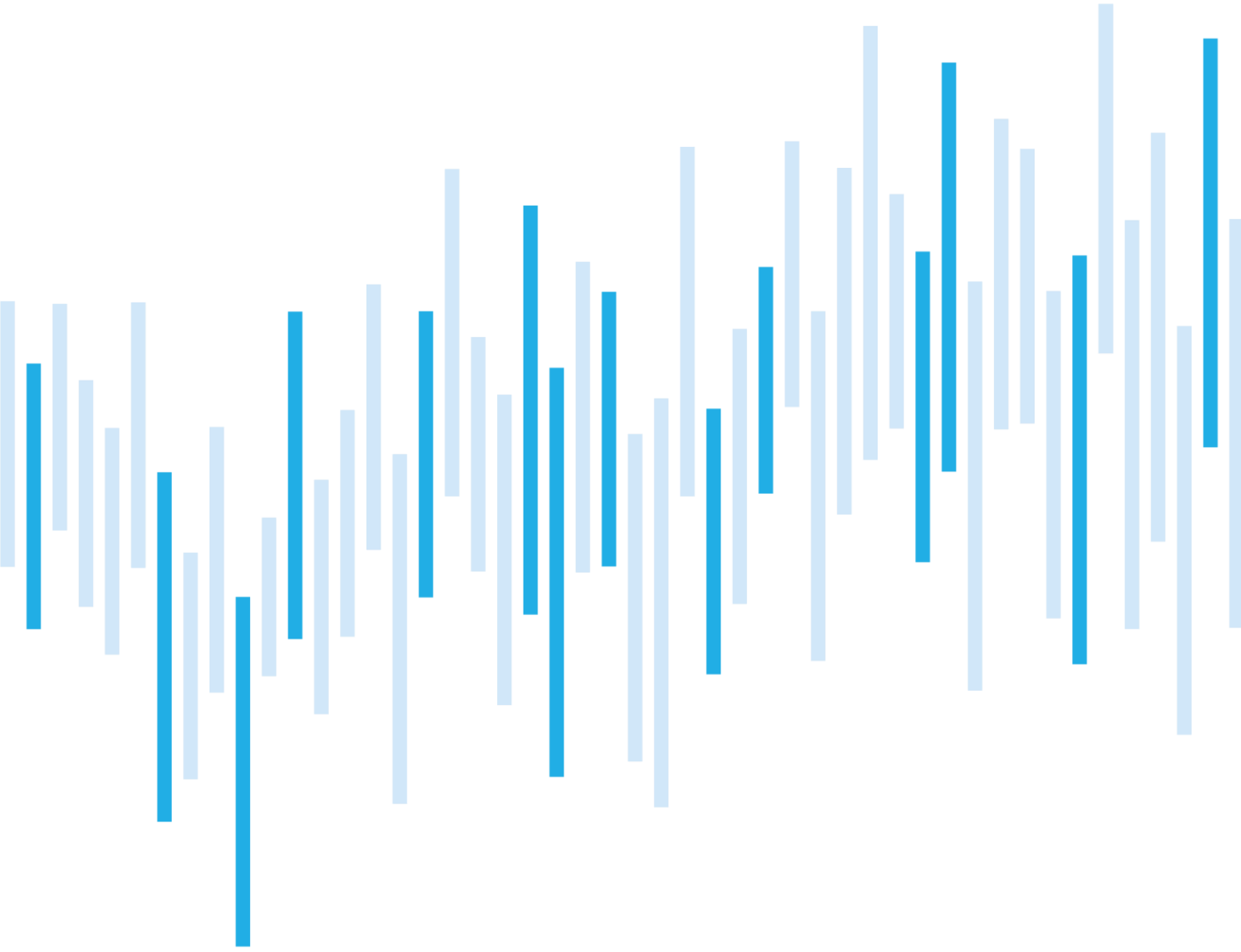
Kybernetické incidenty pohledem NÚKIB

Červenec 2021



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Počet kybernetických incidentů nahlášených NÚKIB byl v červenci mírně pod průměrem posledního roku. Z dlouhodobého hlediska se jedná o předvídatelný stav, jelikož NÚKIB o letních prázdninách eviduje nižší počet incidentů pravidelně. V porovnání s červencem minulého roku je počet incidentů přesto dvojnásobný.

V červenci se do popředí kybernetických incidentů nahlášených NÚKIB dostaly ransomwarové útoky. Představovaly polovinu všech nahlášených incidentů. Některé z obětí po útoku nedokázaly obnovit svá data ze zálohy a zcela je ztratily. Další oběti útočníci data exfiltrovali.

Ve dvou případech stojí za útoky ransomware REvil, což je vyděračský software poskytovaný jako služba. Jeho autoři ho pronajímaný jiným útočníkům a následně si berou podíl ze zisku. REvil byl použit i při masivním červencovém útoku na americkou softwarovou společnost Kaseya. Podle informací dostupných NÚKIB ale tyto incidenty s útokem na software Kaseya nesouvisí.

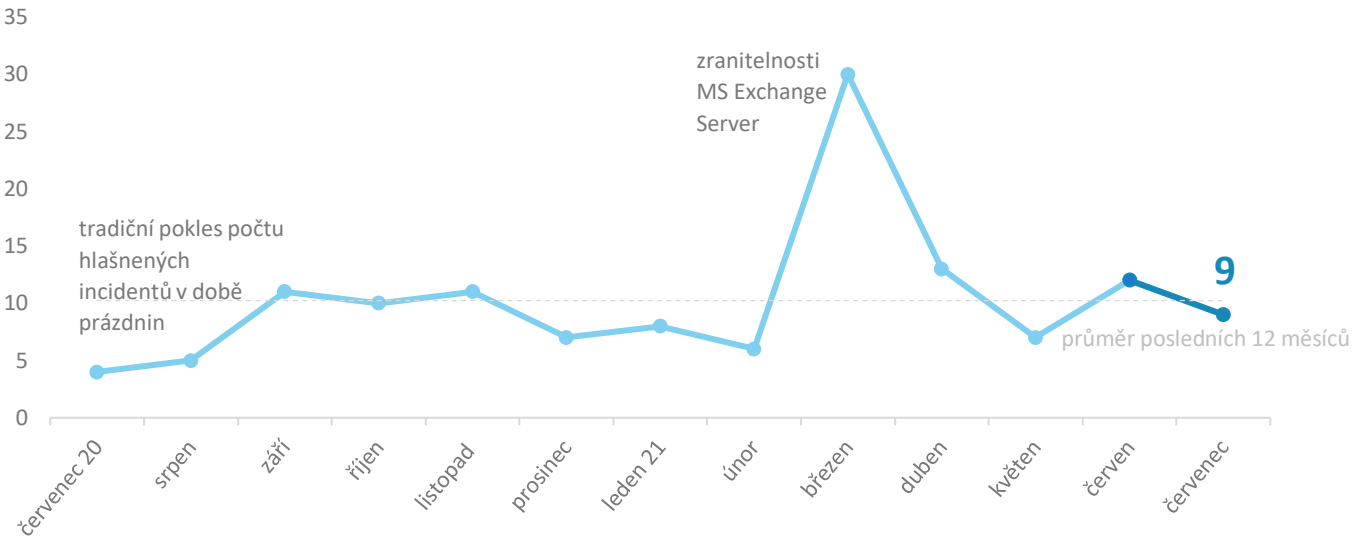
Obsah

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.

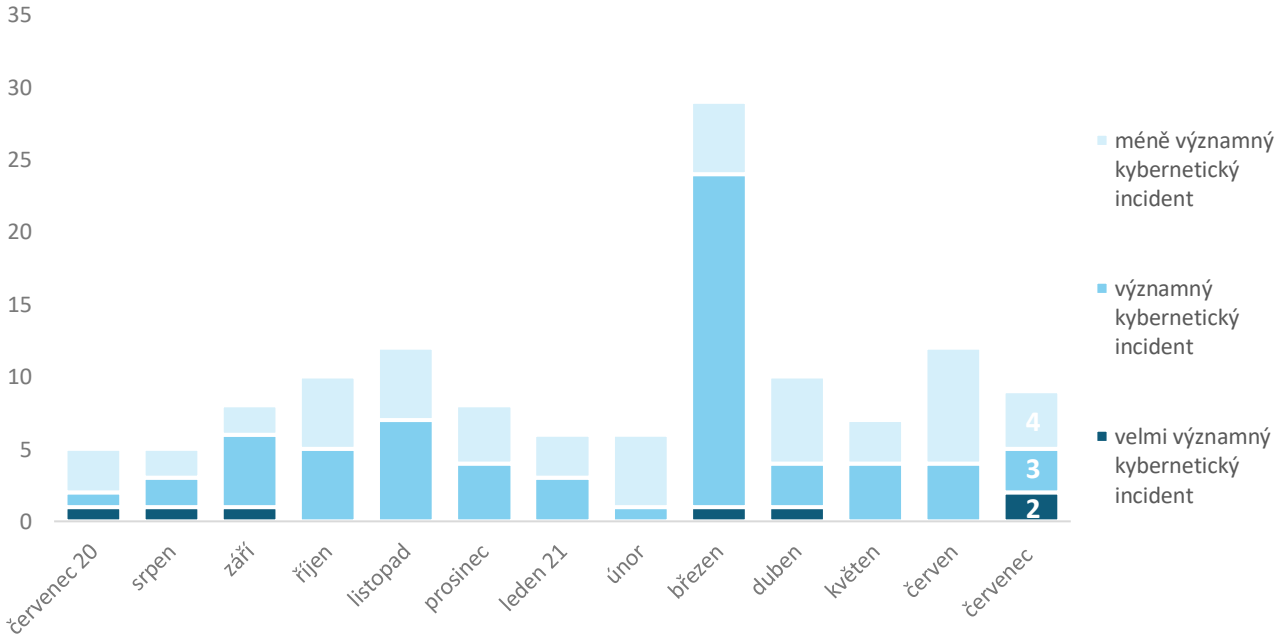
Počet kybernetických incidentů nahlášených NÚKIB

Počet kybernetických incidentů byl v červenci mírně pod průměrem posledních 12 měsíců.[1] NÚKIB v prázdninových měsících zaznamenává pokles incidentů pravidelně a z dlouhodobého hlediska se tak jedná o běžnou věc. V porovnání s červencem minulého roku je počet incidentů přesto dvojnásobný.



Závažnost řešených kybernetických incidentů[2]

Více než polovina červencových incidentu měla vážné dopady na dostupnost a integritu dat a NÚKIB je eviduje jako významné či velmi významné.

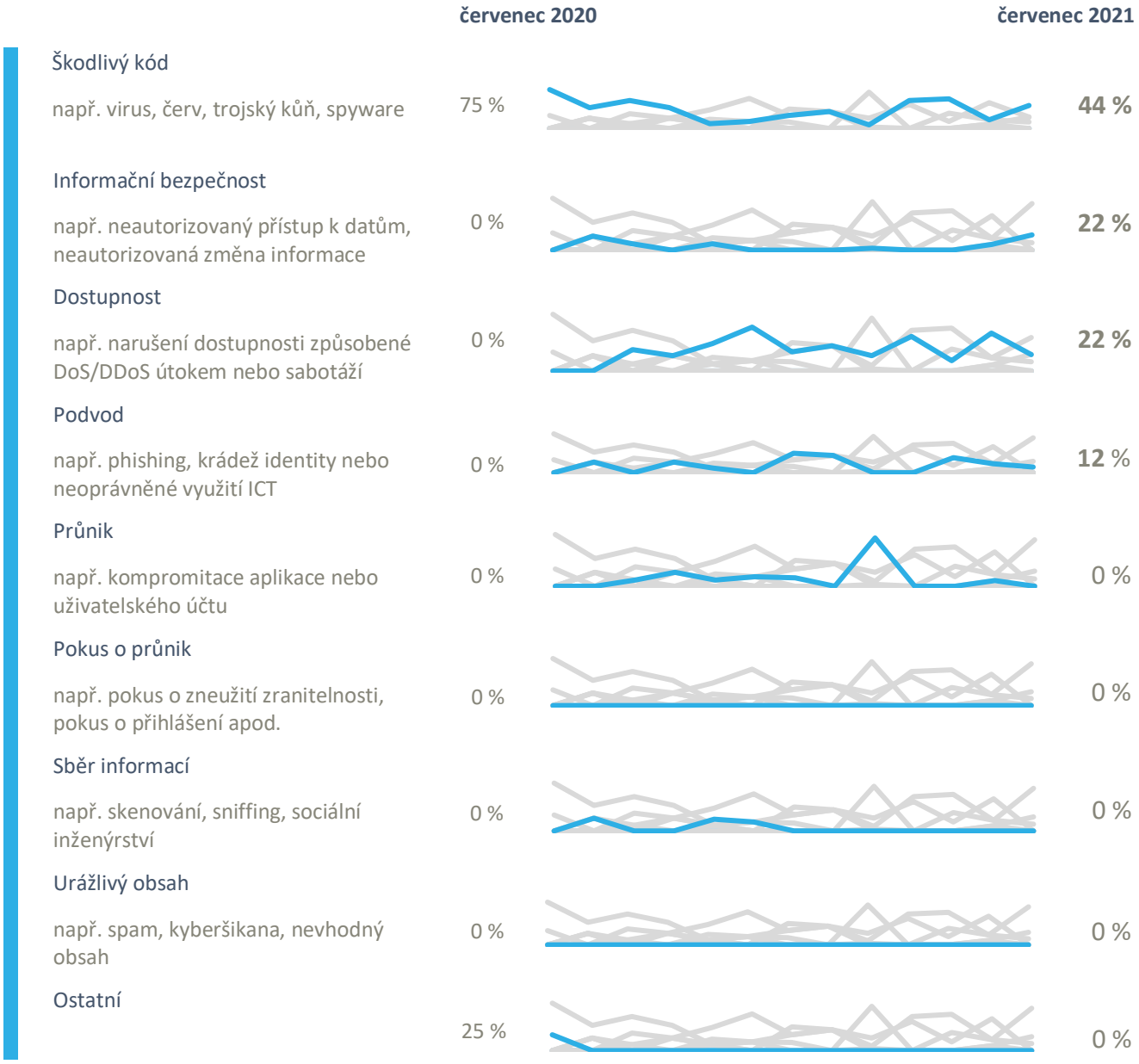


[1] Jeden z červencových incidentů nahlásila osoba povinná dle zákona o kybernetické bezpečnosti. Osm incidentů NÚKIB oznámily nepovinné osoby.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb.

Klasifikace incidentů nahlášených NÚKIB[3]

Podobně jako v předchozích měsících převažují v červencových statistikách NÚKIB kybernetické incidenty zapříčiněné škodlivým kódem. Promítl se do nich nález kontrolního (C2) serveru TrickBotu (více informací na straně 4) a ransomwarové útoky.

NÚKIB v červenci řešil pět ransomwarových útoků. Jelikož měl každý z útoků rozdílné dopady, spadají tyto incidenty do několika kategorií. Dva z ransomwarových útoků NÚKIB eviduje jako škodlivý kód, protože se obětem podařilo zašifrovaná data obnovit ze záloh. V dalších dvou případech oběti při útoku ztratily i zálohy a data nemohly obnovit. Tyto incidenty jsou proto klasifikovány jako narušení dostupnosti. Při posledním z ransomwarových útoků došlo k exfiltraci dat a NÚKIB ho tudíž eviduje jako narušení informační bezpečnosti.



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

Trendy v kybernetické bezpečnosti za červenec pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

V červenci byl odhalen kompromitovaný e-mailový účet jednoho z povinných subjektů dle zákona o kybernetické bezpečnosti. Útočník z kompromitovaného účtu dále rozesílal phishingové e-maily a snažil se proniknout do dalších organizací.
Phishing je jedním z nejčastějších vektorů útoků. Odpovídá tomu i pravidelnost, se kterou se objevuje v incidentech hlášených NÚKIB. Za posledních 12 měsíců byly jen tři měsíce, kdy phishingové, spear-phishingové nebo vishingové kampaně v hlášeních kybernetických incidentů chyběly.

Malware

NÚKIB svou činností zjistil aktivitu malwaru TrickBotu, který hostoval své C2 servery na infrastruktuře českých společností.
TrickBot je pokročilý bankovní trojan, který sbírá citlivá data jako například přihlašovací jména a hesla, data z internetových prohlížečů nebo e-maily. TrickBot patří k nejaktivnějším malwarům posledních měsíců a jeho autoři ho neustále aktualizují o nové funkce a schopnosti.

Zranitelnosti

NÚKIB v červenci upozornil na tři závažné zranitelnosti. První upozornění se týkalo aktivního zneužívání zranitelnosti Cisco ASA. Druhé a třetí odkazovalo na zranitelnosti v prostředí Windows – na zranitelnosti PrintNightmare a HiveNightmare.
Počet upozornění na závažné zranitelnosti oproti červnu narostl.

Ransomware

V porovnání s červnem, kdy NÚKIB řešil jediný incident spjatý s ransomwarem, se vyděračské malwary opět vrátily do popředí. Pět z červencových incidentů (56 %) způsobil ransomware a v jednom případě došlo i ke ztrátě dat klientů oběti (blíže v útocích na dodavatele ICT služeb na straně 6).
Ve dvou případech napadl české organizace ransomware REvil, který je spojován s masivním červencovým útokem na americkou společnost Kaseya. NÚKIB nemá informace, že by tyto dva incidenty souvisely.

Útoky na dostupnost

Oproti předchozímu měsíci, kdy 50 % všech nahlášených incidentů vyústilo v nedostupnost služeb, se situace zmírnila. NÚKIB v červenci DoS nebo DDoS útok nenahlásila žádná organizace, což se stalo naposledy v srpnu minulého roku.
Dlouhodobě ale počet i síla DoS a DDoS útoků proti cílům v Česku roste. Jak ukazuje graf na předchozí straně, útoky na dostupnost v posledních 12 měsících několikrát dominovaly všem incidentům. V dubnu tohoto roku také došlo k velmi silnému DDoS útoku (160 Gbps).

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

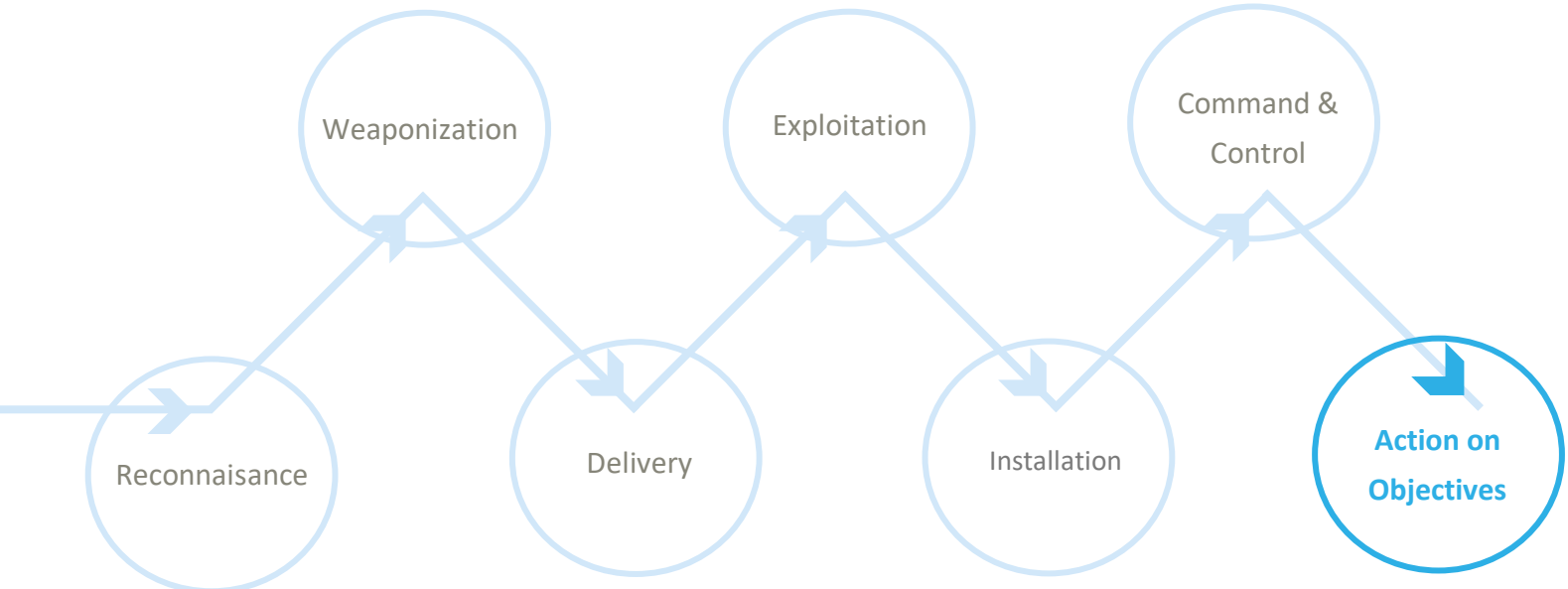
Nejpoužívanější technika měsíce: Data Encrypted for Impact

NÚKIB kybernetické incidenty vyhodnocuje také na základě metriky MITRE ATT&CK, která slouží jako přehled všech známých technik a taktik používaných při kybernetických útocích. NÚKIB na jejím základě mimo jiné určuje četnost využívání technik/taktik.

V červencových incidentech útočníci nejčastěji šifrovali data svých obětí, což je technika, která se v metrice MITRE nazývá „Data Encrypted for Impact“.

> **Data Encrypted for Impact** je technika, při které útočníci zašifrují data v systému své oběti a tím zabrání uživatelům k jejich přístupu. Ve většině případů poté od svých obětí za dešifrování dat požadují zaplacení určité částky. V posledním roce se stalo trendem, že útočníci data kromě zašifrování také exfiltrují a obětem hrozí, že pokud nedojde k zaplacení výkupného, data zveřejní. Jelikož útočník chce po své oběti výkupné, jsou takové útoky známé jako ransomwarové útoky.
>
> **MITRE ID: T14686**
>
> **Mitigace:** Zásadní pro minimalizaci dopadů ransomwaru je pravidelné zálohování a jeho správná implementace. Základní pravidla pro zálohování NÚKIB popisuje v manuálu Ransomware: Doporučení pro mitigaci, prevenci a reakci. V případě některých starších nebo špatně napsaných ransomwarů je možné data dešifrovat dekryptorem. Takových případů ale v současnosti není mnoho a oběti by se proto na dekryptor neměly spoléhat.

Znázornění „Data Encrypted for Impact“ v cyber kill chainu, který ukazuje, ve které fázi útoku útočníci techniku používají:



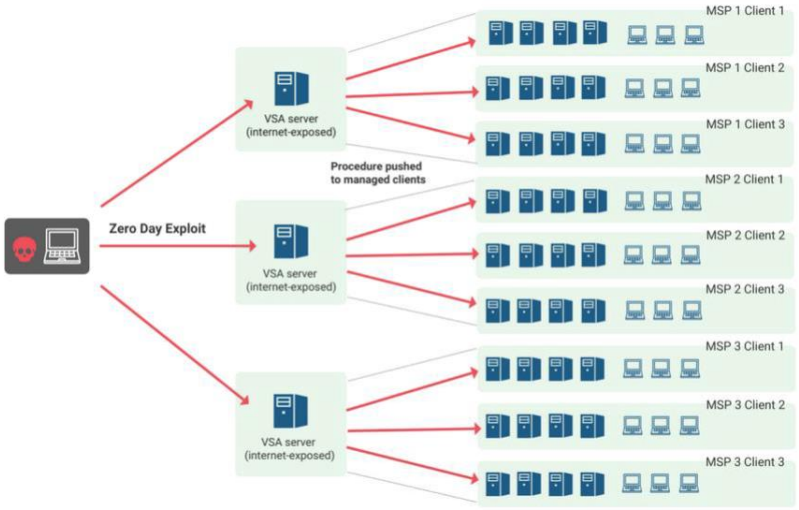
Zaměřeno na sektor: Dodavatelé ICT řešení

NÚKIB v červenci evidoval kybernetický incident, během něhož došlo k ransomwarovému útoku na server české společnosti, která svým zákazníkům poskytuje ICT řešení. Napadený server využívalo více než tucet jejich klientů a data, která na něm byla uložena, ztratili všichni z nich. Z dostupných informací nemůžeme určit, zda útočník cílil přímo na data klientů společnosti nebo jen na server dodavatele a jeho klienti se stali vedlejším produktem útoku.

Podobné útoky zatím NÚKIB ve svých incidentech neeviduje často. V roce 2021 se jedná teprve o druhý případ, kdy byli po útoku na dodavatele služeb postiženi i jeho klienti.

V zahraničí kybernetické útoky na dodavatele ICT služeb probíhají v masivních rozměrech. V pátek 2. července oznámila americká softwarová společnost Kaseya, že došlo k útoku na její software Virtual System Administrator (VSA), který využívají poskytovatelé ICT služeb (přesněji Managed Service Providers) pro vzdálenou správu a monitoring systémů svých klientů. Útočníci zneužili zranitelnosti nultého dne ve VSA a jejím prostřednictvím dokázali kompromitovat desítky serverů poskytovatelů, ze kterých byl následně šířen ransomware k jejich koncovým zákazníkům. V tomto případě tak konečnými obětmi nebyli poskytovatelé, kteří službu Kaseya využívali, ale koncoví zákazníci, kteří se službou samotnou neměli nic společného. To dělá z kompromitace Kaseya VSA útok, kterému se koncový zákazník mohl jen těžko bránit.

Obr. 1: Schéma útoku na společnost Kaseya



Zdroj: Truesec

Přesný rozsah útoku není znám. Ředitel firmy Kaseya Fred Voccola prohlásil, že jen méně než 40 klientů má kompromitované servery, které byly zneužity k rozeslání ransomwaru. Napadených koncových zákazníků je ale podle odhadů až 1500 a většinou se jedná o malé a střední podniky. NÚKIB v současné době nemá informace o tom, že by mezi oběťmi útoku na Kaseya byly i české organizace.

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.