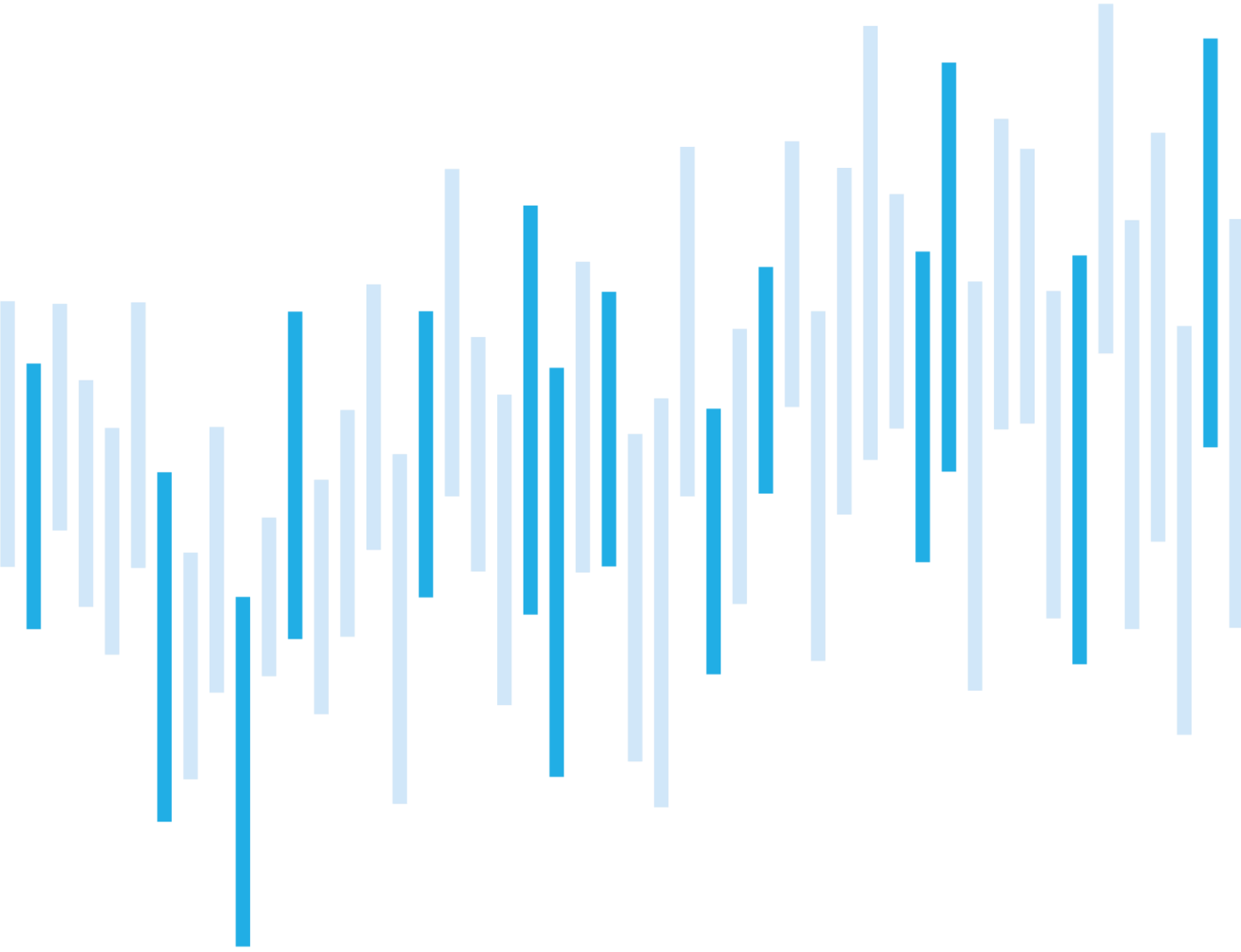
Kybernetické incidenty pohledem NÚKIB

Srpen 2021



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Počtem kybernetických incidentů se srpen řadí k nadprůměrným měsícům roku, většina z nich však neměla vážné dopady a NÚKIB je eviduje jako méně závažné.

NÚKIB v srpnu řešil nedostupnosti služeb, kompromitace aplikací, aktivitu malwaru TrickBot nebo phishing a vishing.

Ransomware na rozdíl od předešlého měsíce v srpnových incidentech chyběl. Téměř jistě (90–100 %) to ale neznamená, že hrozba ransomwaru pominula. S ohledem na výnosnost útoků a jejich rostoucí sofistikovanost očekáváme, že ransomware bude představovat jednu z největších kybernetických hrozeb i v následujících měsících. Riziko ransomwaru zvyšuje i nová série zranitelností MS Exchange, kterou v srpnu začali útočníci používat jako vstupní bod pro ransomware, např. LockFile.

Tato série zranitelností Microsoft Exchange Server se nazývá ProxyShell. Přestože žádná organizace incident spojený s ProxyShellem NÚKIB v srpnu nenahlásila, riziko, které tyto zranitelnosti pro české subjekty představují, je vysoké. Vzhledem k počtu zranitelných serverů v ČR a dění v zahraničí, je velmi pravděpodobné (75–85 %), že některé servery již kompromitovány byly, nebo se tak stane v blízké budoucnosti.

Obsah

Počet kybernetických incidentů nahlášených NÚKIB

Závažnost řešených kybernetických incidentů

Klasifikace incidentů nahlášených NÚKIB

Trendy v kybernetické bezpečnosti za srpen

Nejpoužívanější technika měsíce:
Exploit Public-Facing Application

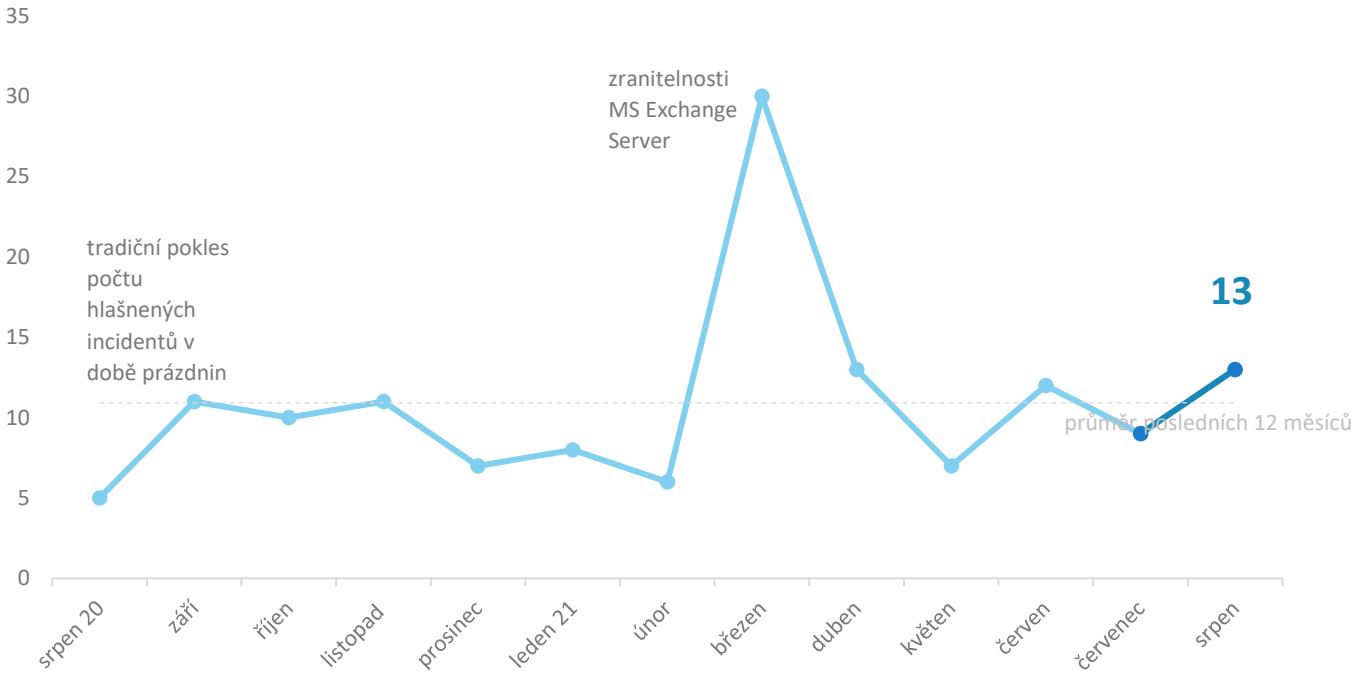
Zaměřeno na zranitelnost:
Microsoft Exchange Server - Proxyshell

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.

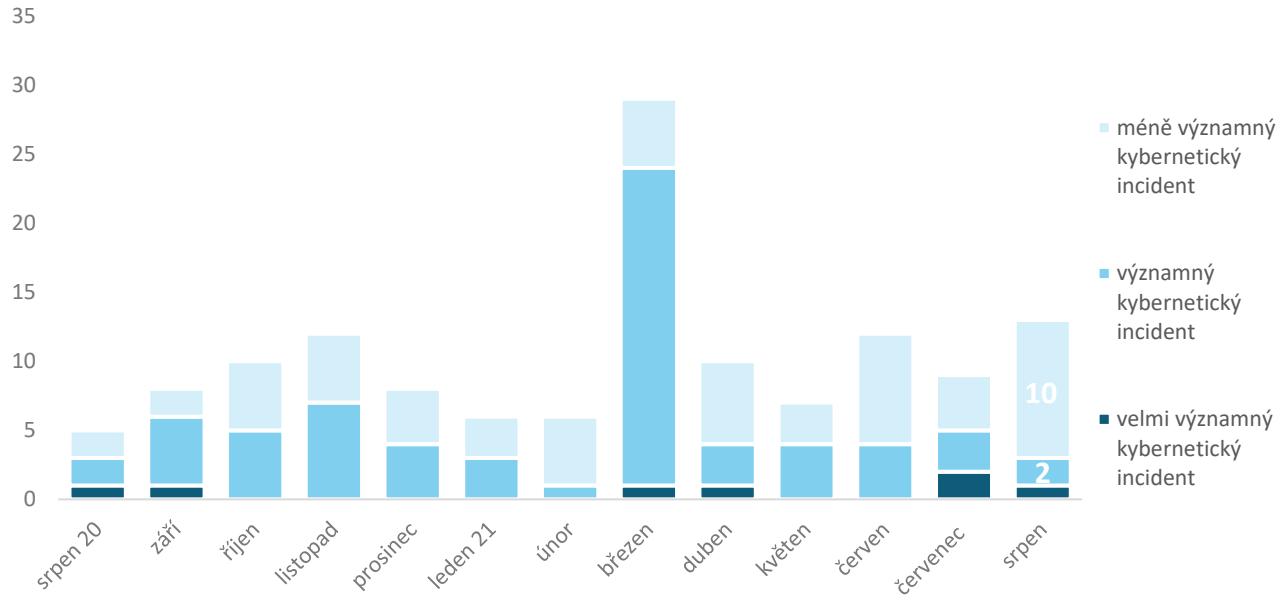
Počet kybernetických incidentů nahlášených NÚKIB

NÚKIB v srpnu subjekty nahlásily 13 incidentů. Vzhledem k počtu se srpen řadí k nadprůměrným měsícům, což se vymyká trendu posledních let, kdy letní měsíce bývaly nejklidnějším obdobím roku.[1]



Závažnost řešených kybernetických incidentů[2]

Většina z řešených incidentů neměla závažné dopady a NÚKIB je tak eviduje jako méně významné. Jeden incident, při kterém došlo k exfiltraci velkého množství dat, vedeme jako velmi významný.

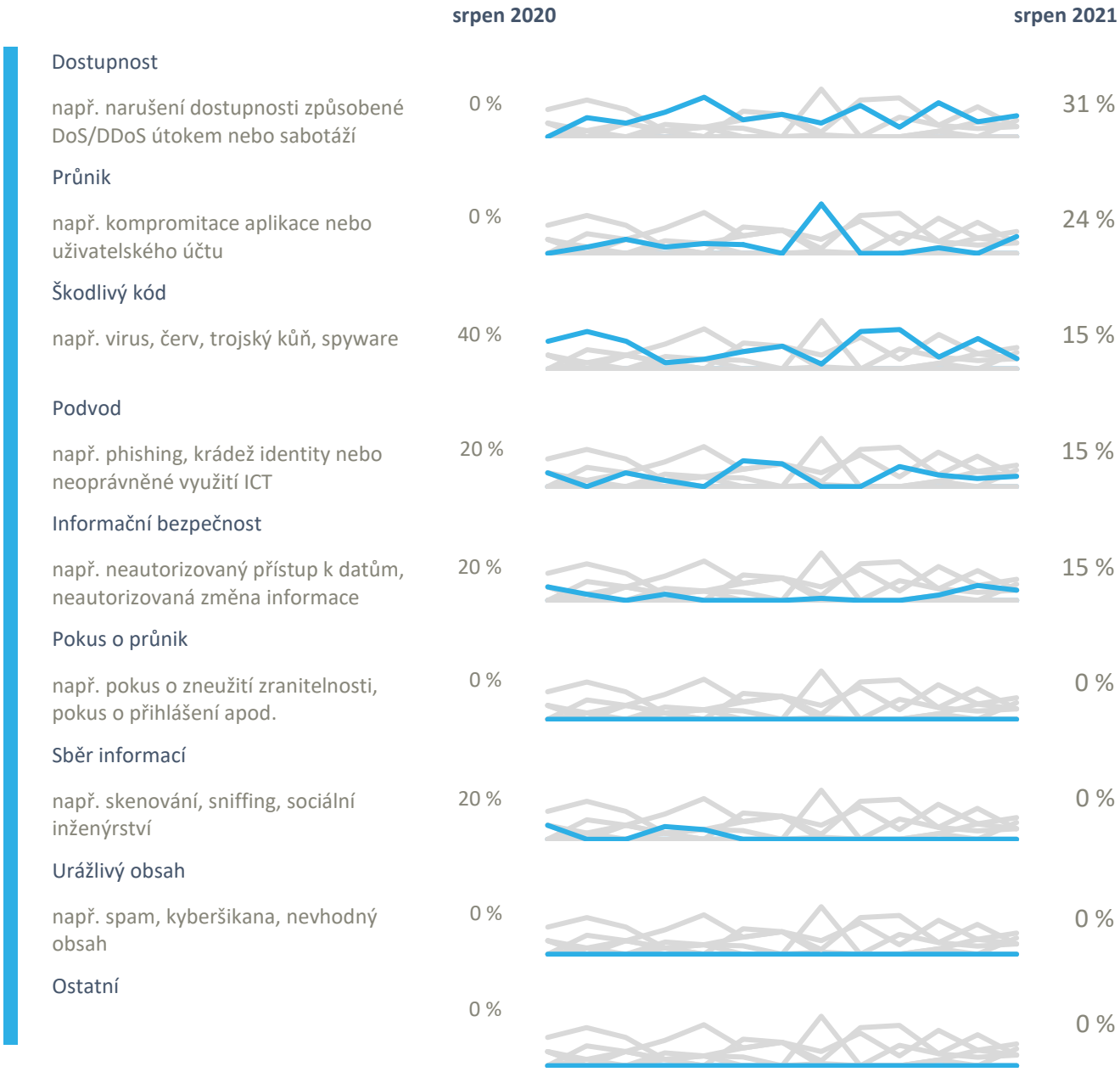


[1] Osm srpnových incidentů nahlásily povinné osoby dle zákona o kybernetické bezpečnosti. Pět incidentů osoby, které pod zákon nespadají.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb.

Klasifikace incidentů nahlášených NÚKIB[3]

Nejvíce srpnových incidentů (čtyři) vyústilo v nedostupnost služeb. Ani v jednom případě ale tyto incidenty nebyly zapříčiněné kybernetickými útoky, nýbrž technickými chybami.

NÚKIB dále řešil průniky do serverů nebo aplikací, tradiční kódy, podvody ve formě phishingu a vishingu či incidenty, ve kterých došlo k narušení bezpečnosti informací skrze exfiltraci dat.



[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 evidoval pokračující vishingovou kampaň proti klientům českých komerčních bank. Stejnou kampaň už zaznamenal na podzim 2020 a upozornil na ni také na jaře tohoto roku.

Vedle vishingu se v incidentech několikrát objevil i phishing. Ve dvou organizacích se útočníkům podařilo kompromitovat e-mailové účty jejich zaměstnanců. Další instituce pak několik phishingových e-mailů zadržela dřív, než se dostaly k jejím zaměstnancům.

Malware

NÚKIB svou činností odhalil další aktivitu malwaru TrickBot, který hostoval své kontrolní (C2) servery na infrastruktuře české společnosti. V předchozím měsíci C2 servery TrickBotu objevil u dvou organizací.

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 13. srpna upozornil na sérii tří zranitelností Microsoft Exchange Serveru, která se nazývá ProxyShell. Přestože žádná organizace v srpnu incident spojený s ProxyShellem NÚKIB nenahlásila, riziko, které tato série zranitelností pro české společnosti a instituce představuje, je vysoké. Vzhledem k počtu zranitelných serverů v ČR a dění v zahraničí, je velmi pravděpodobné (75–85 %), že některé servery již kompromitovány byly, nebo se tak stane v blízké budoucnosti. Více informací ke zranitelnosti je k dispozici na straně 6.

Ransomware

V souvislosti s ransomwarovými útoky se situace oproti předchozímu měsíci uklidnila. NÚKIB poprvé od prosince 2020 nenahlásila ransomware žádná organizace.

Téměř jistě (90–100 %) to ale neznamená, že hrozba ransomwaru vůči povinným osobám pominula. S ohledem na výnosnost ransomwarových útoků a jejich rostoucí sofistikovanost očekáváme, že ransomware bude představovat jednu z největších kybernetických hrozeb i v následujících měsících. Jeho riziko se v srpnu navíc navýšilo i zranitelnostmi MS Exchange Server ProxyShell, které útočníci začali zneužívat jako vstupních bodů pro nový ransomware LockFile.

Útoky na dostupnost

Stejně jako v červenci nenahlásila NÚKIB DoS nebo DDoS útok žádná organizace. Tři srpnové incidenty sice vyústily v nedostupnost služeb, ale ve všech případech je zapříčinila technická chyba, ne kybernetický útok.

Incidenty posledních 12 měsíců nicméně stále ukazují rostoucí trend DoS a DDoS útoků na české cíle a stejně jako v případě ransomwaru hrozba útoků na dostupnost téměř jistě (90–100 %) nepominula.

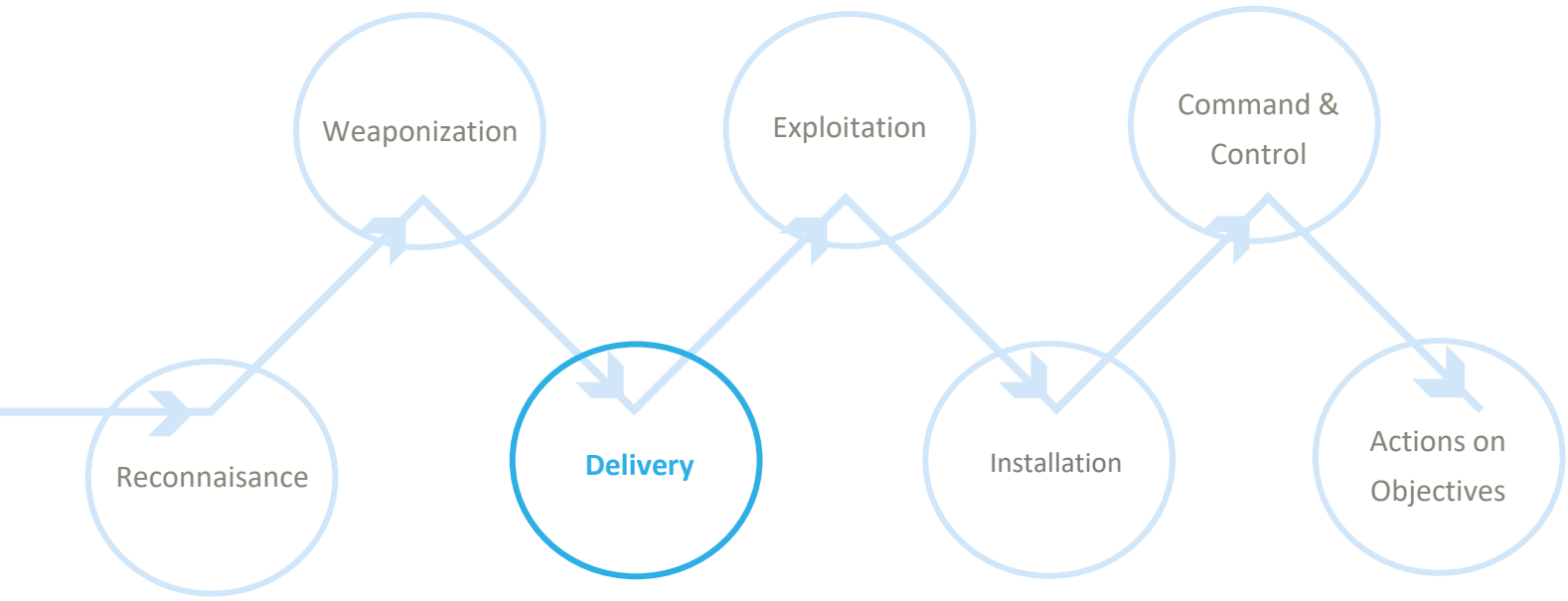
[4] Vývoj ilustrovaný šipkou je vyhodnocován ve vztahu k předešlému měsíci.

Nejpoužívanější technika měsíce: Zneužití aplikací otevřených do internetu [5]

Útočníci v srpnových incidentech nejčastěji zneužívali aplikací otevřených do internetu (Exploit public-facing application). Do systémů obětí pronikli skrze nedostatečně zabezpečené webové servery, VPN nebo Remote Desktop Protocol (RDP), který se používá pro vzdálenou správu počítače.[6]

> **Exploit public-facing application** je technika, kterou útočníci zneužívají slabých míst v systémech otevřených do internetu. Takovým slabým místem může být například nevhodné nastavení zabezpečení ze strany oběti nebo chyba, která vznikla při psaní programu.
>
> **MITRE ID: T1190**
>
> **Mitigace:** Organizace mohou zmírnit riziko úspěšného zneužití této techniky tím, že do internetu otevřou jen služby nezbytně nutné k provozu, budou pravidelně kontrolovat zranitelnosti systémů a aplikací a při jejich nasazení provedou penetrační testování. Pro služby vzdáleného přístupu (VPN, RDP, SSH) doporučujeme používat vícefaktorovou autentizaci, případně i whitelisting, a u webových služeb nasadit Web Application Firewall (WAF).

Znázornění v cyber kill chainu, který ukazuje, ve které fázi útoku útočníci aplikací otevřených do internetu zneužívají:



[5] NÚKIB kybernetické incidenty vyhodnocuje také na základě metriky MITRE ATT&CK, která slouží jako přehled všech známých technik používaných při kybernetických útocích. Na základě metriky mimo jiné určuje četnost jejich využívání.

[6] Tato technika se vztahuje také na sérii zranitelností Microsoft Exchange ProxyShell, kde jsou servery přístupné na portu 443 a tudíž jsou otevřené do internetu (více k zranitelnosti na straně 6).

Zaměřeno na zranitelnost: Microsoft Exchange Server–ProxyShell

NÚKIB 13. srpna upozornil na sérii tří zranitelností Microsoft Exchange Server, která se nazývá ProxyShell.[7] Microsoft všechny tři zranitelnosti opravil již v dubnu a květnu. Nově je lze ale v jejich kombinaci využít k ProxyShell útoku. Tento útok umožňuje nahrát na server webshell, přes který může útočník vzdáleně spouštět kód s nejvyšším oprávněním a zcela tak kompromitovat daný server. ProxyShell prezentoval v srpnu na konferenci BlackHat v USA jeden z řečníků.

Útočníci ProxyShellu brzy zneužili a na zranitelné servery začali ještě v průběhu srpna útočit. Společnost Huntress Labs nalezla více než 140 různých webshellů na téměř dvou tisících serverech po celém světě. Zasažené entity zahrnují například stavební firmy, zpracovatele mořských produktů, průmyslová zařízení, autoservisy či jedno malé letiště. Útočníci také začali používat ProxyShell jako vstupní bod pro nový ransomware LockFile, který se poprvé objevil nyní v srpnu.

Zranitelnosti MS Exchange ProxyShell představují vysoké riziko i pro Českou republiku. NÚKIB v srpnu žádná organizace zneužití těchto zranitelností nenahlásila a NÚKIB nyní nezná počet kompromitovaných serverů na našem území. Nicméně vzhledem k počtu zjištěných českých zranitelných serverů (806 podle nástroje Shodan) a dění ve světě je velmi pravděpodobné (75–85 %), že některé české servery již byly kompromitovány nebo v blízké budoucnosti budou.

Na závažnost situace v ČR ukazuje také březnové dění. Poté, co Microsoft v březnu 2021 upozornil na čtyři zranitelnosti nultého dne u MS Exchange Server (také známé jako ProxyLogon), nahlásilo NÚKIB související incident 19 českých společností a institucí. Zranitelných serverů na českém území přitom v březnu bylo méně než nyní.

Březen

609 zranitelných serverů

8.března 2021 NÚKIB prostřednictvím nástroje Shodan zachytil 609 českých serverů, které byly zranitelné vůči sérii čtyř zranitelností nazývané jako ProxyLogon.

19 incidentů

19 organizací nahlásilo NÚKIB v březnu kybernetický incident, při kterém došlo ke kompromitaci jejich systému na základě zranitelností MS Exchange Server. Březen se tak s celkovými 30 incidenty stal početně rekordním měsícem na NÚKIB.

Srpen

865 zranitelných serverů

K 13. srpnu, dni vydání upozornění, NÚKIB zachytil 865 českých serverů, které byly zranitelné vůči útoku ProxyShell.

0 incidentů

Přestože je nyní počet zranitelných serverů vyšší než březnu, související incident zatím NÚKIB nenahlásila žádná organizace. Pohled na březnové dění ale ukazuje, že organizace buď pravděpodobně (55-70 %) kompromitaci ještě neodhalily nebo útoky teprve přijdou.

[7] Bližší informace ke zranitelnostem a doporučením, jak eliminovat riziko útoku ProxyShellem, jsou dostupné v upozornění NÚKIB.

Útoky na e-mailové servery Microsoft Exchange představují pro útočníky lákavý cíl. MS Exchange Server patří k nejrozšířenějším poštovním serverům na světě. Používají ho jak velké společnosti, tak státní organizace. Z povahy věci obsahují mnoho citlivých informací a útočníci je v případě napadení mohou zneužít nejen pro účely špionáže, ale i jako vstupní bod do sítě organizace.

České organizace své zranitelné servery sice aktualizují, ale ne v dostatečném počtu. Tři týdny poté, co NÚKIB publikoval upozornění na MS Exchange Server ProxyShell, se počet zranitelných serverů snížil jen o necelých sedm procent, což stále dává útočníkům široké pole k zneužití.

865

Zranitelných serverů v ČR k 13. srpnu

NÚKIB k 13. srpnu detekoval prostřednictvím nástroje Shodan 865 českých serverů, které měly všechny tři zranitelnosti potřebné k útoku ProxyShell.

806

Zranitelných serverů v ČR k 3. září

Tři týdny po publikování upozornění na webových stránkách NÚKIB se počet zranitelných serverů snížil na 806.

6,8 %

Procento aktualizovaných serverů

Počet zranitelných serverů se od vydání upozornění snížil pouze o necelých sedm procent.

Podle našich zjištění navíc některé organizace své poštovní servery neaktualizovaly ani po březnové sérii zranitelností MS Exchange Server ProxyLogon a jsou tak zranitelné hned dvakrát, na starší útoky ProxyLogon i na nový ProxyShell. K 3. září jich je 118. Pravděpodobně (55–70 %) mezi nimi ale bude i několik honeypotů, které pro své potřeby nasadili výzkumníci.

NÚKIB proto všem správcům doporučuje zkontrolovat, zda nejsou jejich Exchange servery zranitelné a případně bezodkladně nainstalovat poslední dostupné bezpečnostní aktualizace pro Exchange Server dle dokumentace Microsoft. Dále také doporučuje prověřit indikátory potenciálního zneužití, které naleznete v publikovaném upozornění.

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.