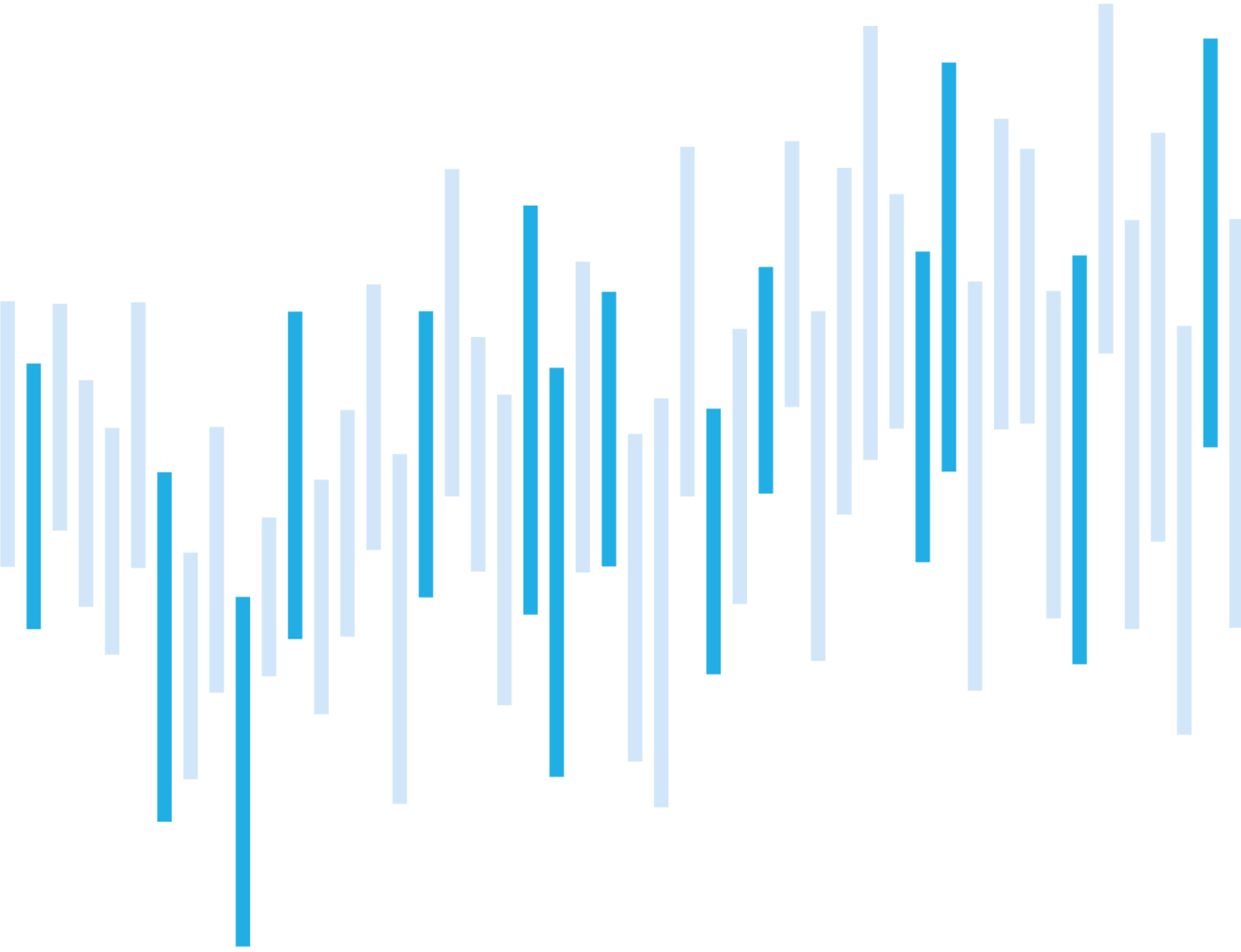
Kybernetické incidenty pohledem NÚKIB

ŘÍJEN 2021



Národní úřad
pro kybernetickou
a informační bezpečnost

Shrnutí měsíce

Říjen se co do počtu incidentů stal druhým nejrušnějším měsícem tohoto roku. NÚKIB evidoval 14 kybernetických incidentů. Většina z nich nicméně neměla vážné následky a podařilo se je rychle vyřešit.

Podobně jako v předchozích měsících se v hlášeních objevovaly DDoS útoky, phishingové kampaně nebo škodlivé kódy v sítích českých organizací. Mezi incidenty byl také jeden ransomware, který zašifroval část infrastruktury oběti a následně na svých stránkách vyhrožoval zveřejněním jejích dat.

Tři z říjnových incidentů se týkaly zdravotnického sektoru. Pohled na statistiky ukazuje, že české zdravotnictví čelí i rok a půl po vypuknutí pandemie COVID-19 zvýšenému tlaku hackerů. Počet incidentů neustále narůstá a zároveň se zvyšuje i jejich sofistikovanost.

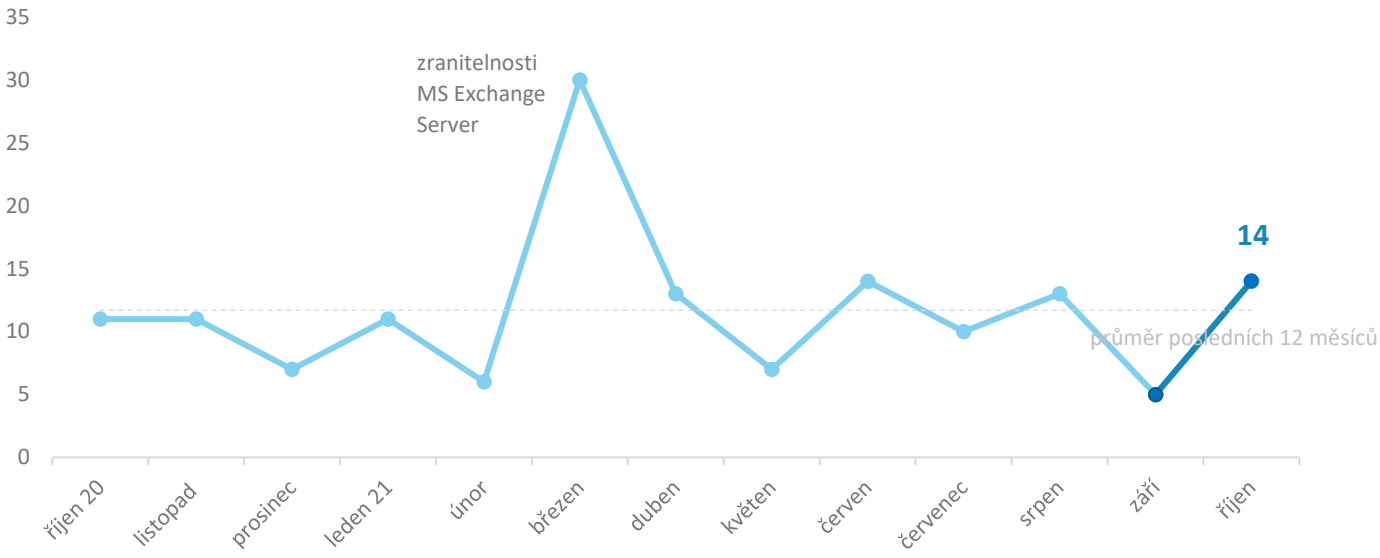
Obsah

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.

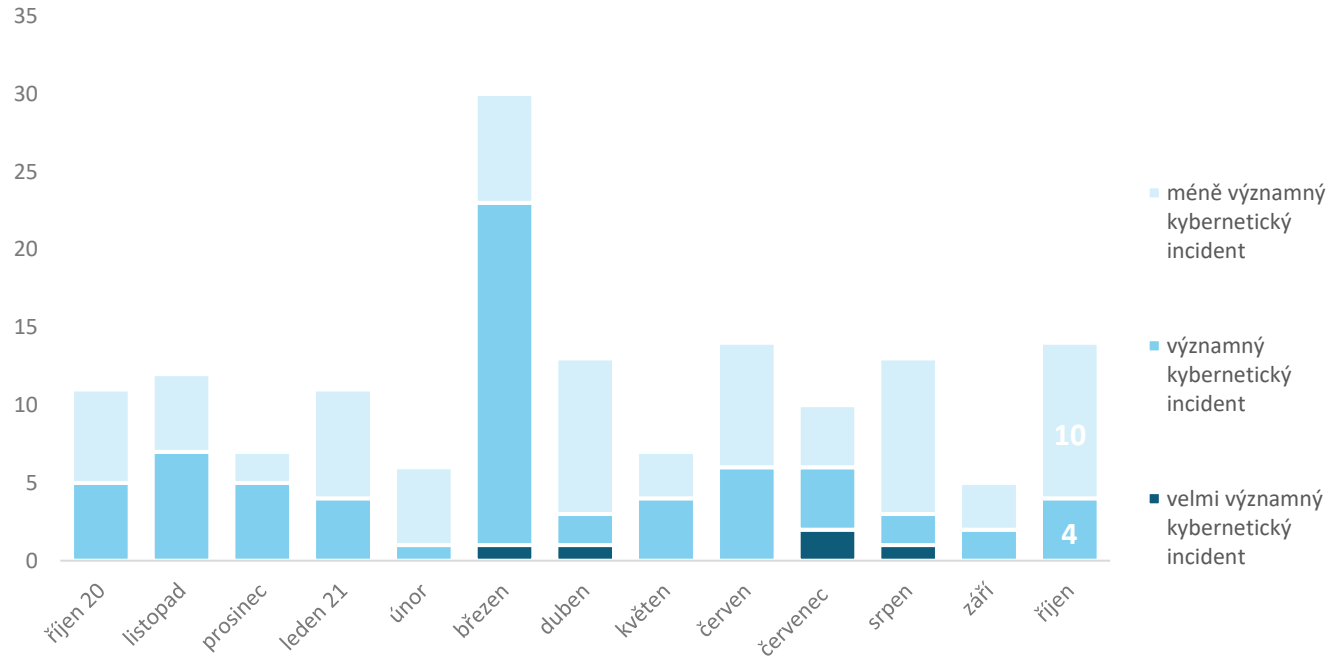
Počet kybernetických incidentů nahlášených NÚKIB

NÚKIB v říjnu evidoval 14 incidentů, což je druhý nejvyšší počet za poslední rok. Předčil ho pouze březen se 30 incidenty, z nichž většinu zapříčinily zranitelnosti MS Exchange Server.[1]



Závažnost řešených kybernetických incidentů[2]

Žádný říjnový incident neměl natolik vážné dopady, aby ho NÚKIB klasifikoval jako velmi významný. Ve více než dvou třetinách případů se jednalo o incident, který se podařilo rychle vyřešit.

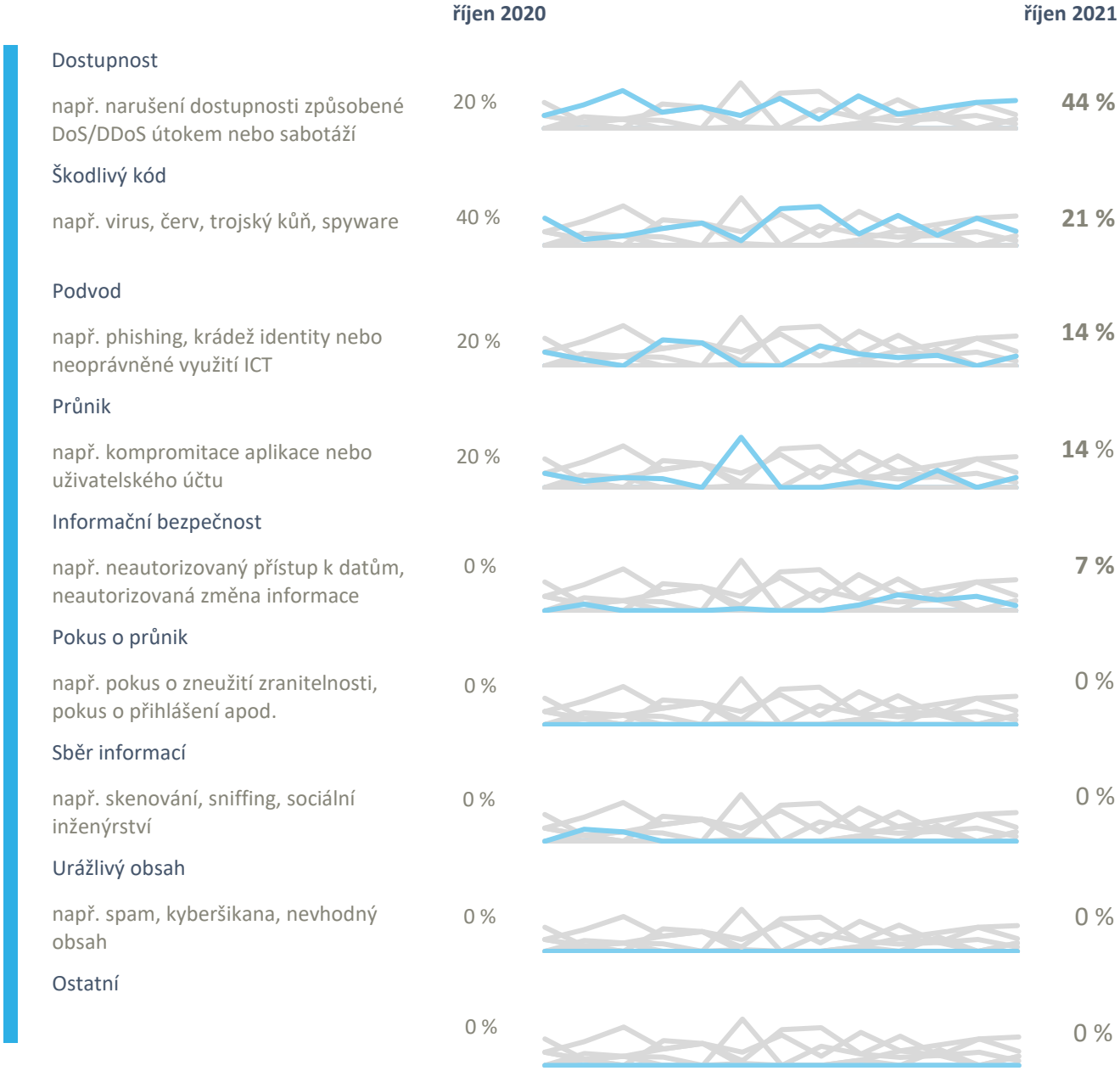


[1] Deset incidentů NÚKIB nahlásily povinné osoby dle zákona o kybernetické bezpečnosti. O zbylých čtyřech incidentech NÚKIB informovaly subjekty, které pod tento zákon nespadají.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb.

Klasifikace incidentů nahlášených NÚKIB[3]

Většina incidentů (6) vyústila v nedostupnost služeb. U poloviny organizací tuto nedostupnost způsobily DDoS útoky, za druhou polovinou stojí technické chyby na straně dotčených organizací. Vedle narušení dostupnosti NÚKIB dále řešil škodlivé kódy, které organizace objevily ve svých sítích, phishingové kampaně, při kterých došlo ke kompromitaci uživatelských účtů, a dva případy průniků, kdy podezřelé chování napadených systémů ukázalo na jejich kompromitaci.

Jeden z incidentů pak NÚKIB eviduje jako narušení informační bezpečnosti. Jednalo se o ransomwarový útok na českou společnost. Útočníkům se pravděpodobně podařilo exfiltrovat data společnosti, jelikož vyhrožovali jejich zveřejněním.



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

Trendy v kybernetické bezpečnosti za říjen pohledem NÚKIB[4]

Phishing, spear-phishing a sociální inženýrství

Podobně jako v předchozím měsíci NÚKIB v říjnu řešil phishingové kampaně. Dva povinné subjekty dle zákona o kybernetické bezpečnosti v říjnu odhalily kompromitované e-mailové účty svých uživatelů, kteří po prokliku z phishingové zprávy zadali přihlašovací údaje do falešného formuláře. Útočníci z jejich účtů dále rozesílali phishingové e-maily a snažili se tak proniknout do dalších organizací.

Malware

V říjnových incidentech se objevily tři škodlivé kódy - Dridex, RemCom a jeden coinminer.
První z nich, Dridex, NÚKIB objevil v rámci vlastního šetření na serverech jedné české společnosti, kde malware hostoval svou C2 infrastrukturu. Dridex může mít několik funkcionalit. Může detekovat bankovní aplikace, získávat k nim přihlašovací údaje, stahovat další škodlivé kódy nebo zaznamenávat úhozy na klávesnici. Kyberbezpečností společnosti Dridex připisují skupině známé jako Evil Corp, která cílí na organizace napříč sektory. V posledních dvou měsících aktivita spojená s malwarem Dridex roste.

Zranitelnosti

NÚKIB se v říjnu aktivně zabýval novou zranitelností CVE-2021-41773, která cílí na Apache HTTP Server. Ten je jedním z globálně nejvíce používaných webových serverů v prostředích Windows i Unix. Zneužití zranitelnosti umožňuje útočníkovi instalovat malware, kontrolovat systém a stahovat přihlašovací údaje.

NÚKIB o této zranitelnosti sice neinformoval veřejně na svých stránkách, ale upozornil povinné subjekty, jejichž servery byly zranitelné, a poslal jim doporučení pro řešení situace.

Ransomware

NÚKIB v říjnu řešil jeden případ ransomwaru. Jednalo se o ransomware LockBit, který zašifroval část infrastruktury soukromé společnosti a na svých stránkách vyhrožoval zveřejněním jejích dat.

LockBit je ransomware poskytovaný jako služba (RaaS). Podle dat RansomWatch se jedná o velmi rozšířený kód. V roce 2021 je zatím druhým nejrozšířenějším ransomwarem, který napadá organizace po celém světě.

Útoky na dostupnost

Oproti minulému měsíci, kdy ve statistikách NÚKIB nebyl žádný DoS nebo DDoS útok, se v říjnu objevily tři. Žádný z nich ale neměl vážné dopady. Všechny ovlivnily dostupnost služeb maximálně do 15 min a napadené organizace se s nimi vypořádaly pomocí vlastních prostředků.

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

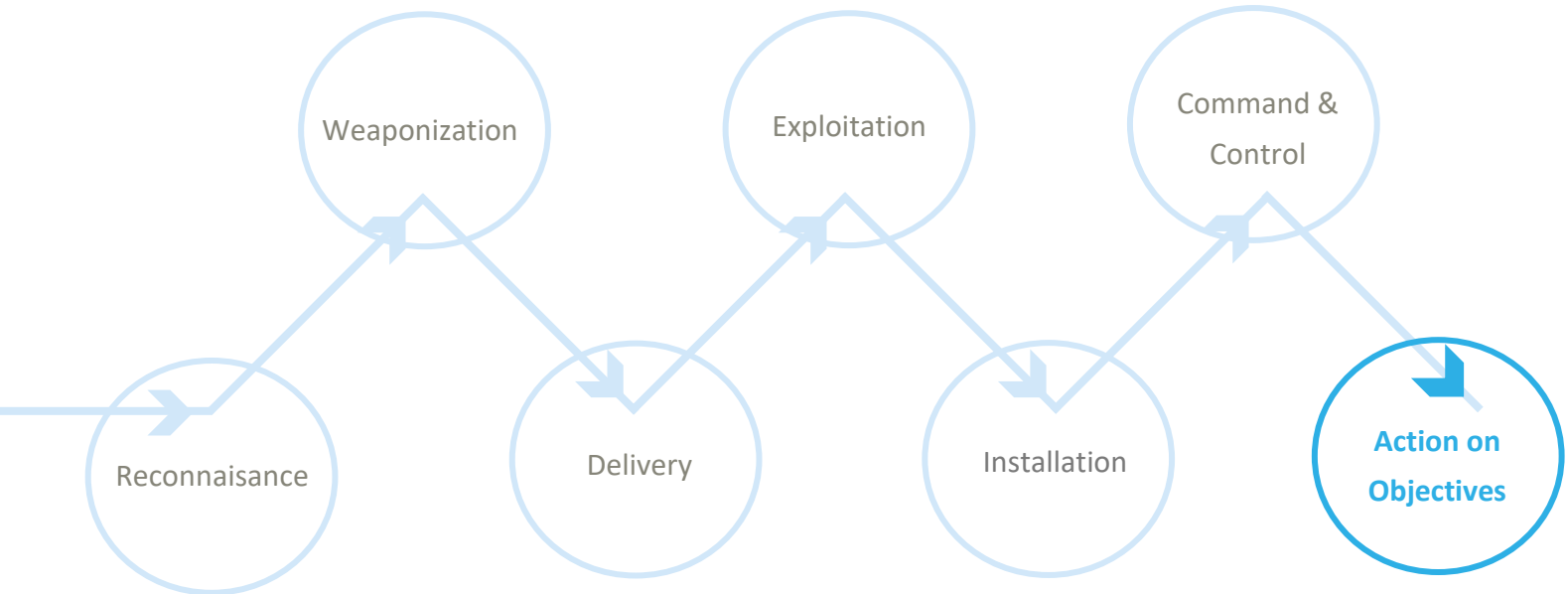
Nejpoužívanější technika měsíce: Endpoint Denial of Service: Application or System Exploitation

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

V říjnových incidentech se nejčastěji objevoval „Endpoint Denial of Service: Application or System Exploitation“.

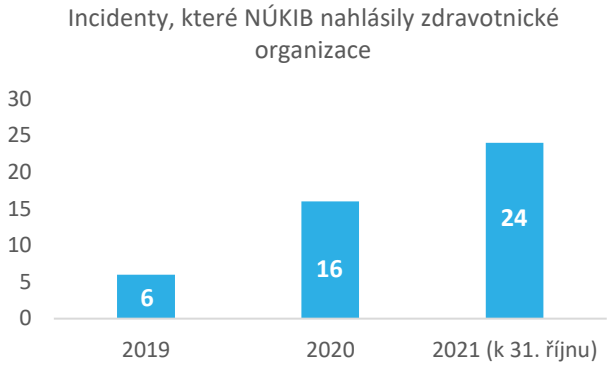
> **Endpoint Denial of Service: Application or System Exploitation** je technika, při které útočníci zneužívají softwarových zranitelností k tomu, aby způsobili výpadek systému nebo aplikací a tím narušili jejich dostupnost. Některé systémy se sice po výpadku mohou samy restartovat, útočníci ale dokáží zranitelnost zneužívat stále dokola a tím způsobit dlouhotrvající nedostupnost. Mezi služby, na které útočníci takto často cílí, patří webové stránky, DNS, e-mailové služby nebo webové aplikace.
>
> **MITRE ID: T1499.004**
>
> **Mitigace:** Útoky podobného typu se mitigují na síťové vrstvě zablokováním komunikace z IP adres útočníka, blokováním portů, na které útočník cílí, anebo protokolů, kterých útočník pro škodlivou komunikaci používá.

Znázornění „Endpoint Denial of Service“ v cyber kill chainu, který ukazuje, ve které fázi útoku útočníci techniku používají:



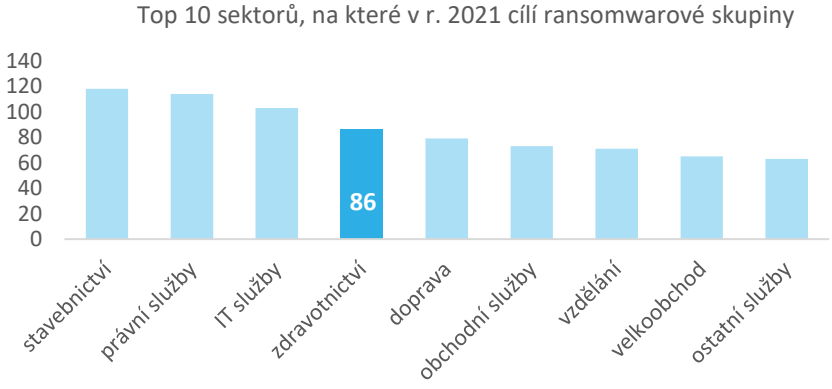
Zaměřeno na sektor: Zdravotnictví

Více než rok a půl po prvním vyhlášení nouzového stavu čelí české zdravotnictví stále zvýšenému tlaku hackerů. Tři z říjnových incidentů se týkaly zdravotnického sektoru a při srovnání s posledními dvěma lety je zjevný rostoucí trend útoků na toto odvětví. V roce 2020 narostl oproti roku 2019 počet incidentů, které NÚKIB nahlásily zdravotnické organizace, o 167 %. Letos trend pokračuje, jelikož NÚKIB už ke konci října eviduje 24 takových incidentů, což je o 8 více než za celý minulý rok.



Do nárůstu hlášení se promítá i fakt, že s novelou vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby se změnila určující kritéria ve zdravotnictví, a tak došlo k rozšíření počtu nemocnic, které jsou určeny jako provozovatelé základních služeb a jsou tak mimo jiné povinny tyto incidenty hlásit.

S příchodem pandemie COVID-19 zesílily především ransomwarové útoky.[5] Útočníci začali využívat skutečnosti, že nemocnice jsou přetížené. Předpokládají proto, že budou ochotnější zaplatit za dešifrování dat a znovuzprovoznění svých systémů, které se může jevit v porovnání s reinstalací všech nakažených stanic a serverů rychlejší.



I přes to, že se tentokrát v incidentech spojených se zdravotnickým sektorem žádný ransomware neobjevil, aktuální zahraniční dění ukazuje, že zvýšená opatrnost je stále na místě. Za poslední měsíc se v otevřených zdrojích často objevovalo jméno skupiny FIN12. Podle bezpečností společnosti Mandiant, která se jejími aktivitami zabývá, je FIN12 „agresivní“ a své ransomwarové útoky směřuje především na zdravotnické organizace. Přístup do sítí svých obětí si skupina nezajišťuje sama. Kupuje si ho od jiných kyberkriminálních skupin v pravděpodobné snaze o větší efektivitu útoků. Zároveň jí to dává možnost vybrat si ze seznamu obětí ty, u kterých je pravděpodobnost nejvyššího zisku. Většina útoků skupiny FIN12 se zatím soustředila na Severní Ameriku. Nicméně svou pozornost začala v posledních dnech upírat i na Evropu, a tak nelze vyloučit (25–50 %), že si jako další z obětí vybere některou českou zdravotnickou organizaci.

[5] Data v grafu vychází ze stránky RansomWatch, jejíž správci monitorují darkweb a na základě informací ze stránek ransomwarových skupin vytváří hromadné statistiky. Do jejich dat se dostanou pouze informace těch skupin, které své útoky zveřejnují. Ty, které své útoky nepublikují, se do statistik nedostanou.

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.