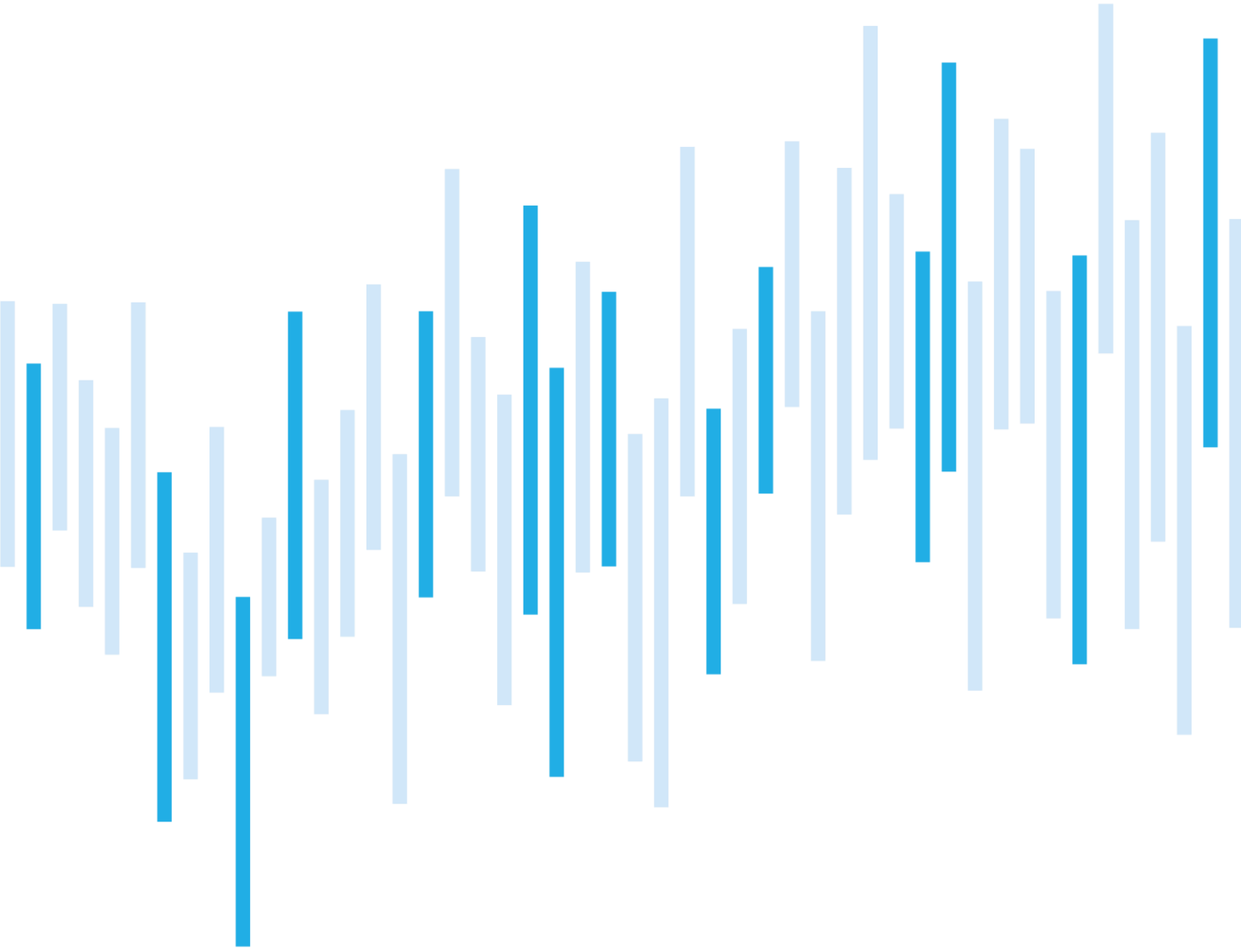
Kybernetické incidenty pohledem NÚKIB

# ČERVENEC 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

## Shrnutí měsíce

Počet kybernetických incidentů se během července pohyboval na velmi podprůměrných hodnotách. NÚKIB obvykle v letních měsících eviduje nižší počet incidentů, nicméně i na poměry klidných letních měsíců jde o nízké číslo. Přesto byla většina z nich z hlediska závažnosti označena jakožto významný incident.

V měsíci červenci byly incidenty u povinných i nepovinných osob téměř v rovnováze. Nelze také určit častěji zasažený sektor.

Vzhledem ke skutečnosti, že během července byla zasažena místní samospráva, tak jsme se nyní zaměřili na útoky vůči obcím, městům a krajům. Ty pro útočníky představují lákavý cíl nejenom kvůli možnému finančnímu zisku, nýbrž také kvůli často slabšímu zabezpečení.

## Obsah

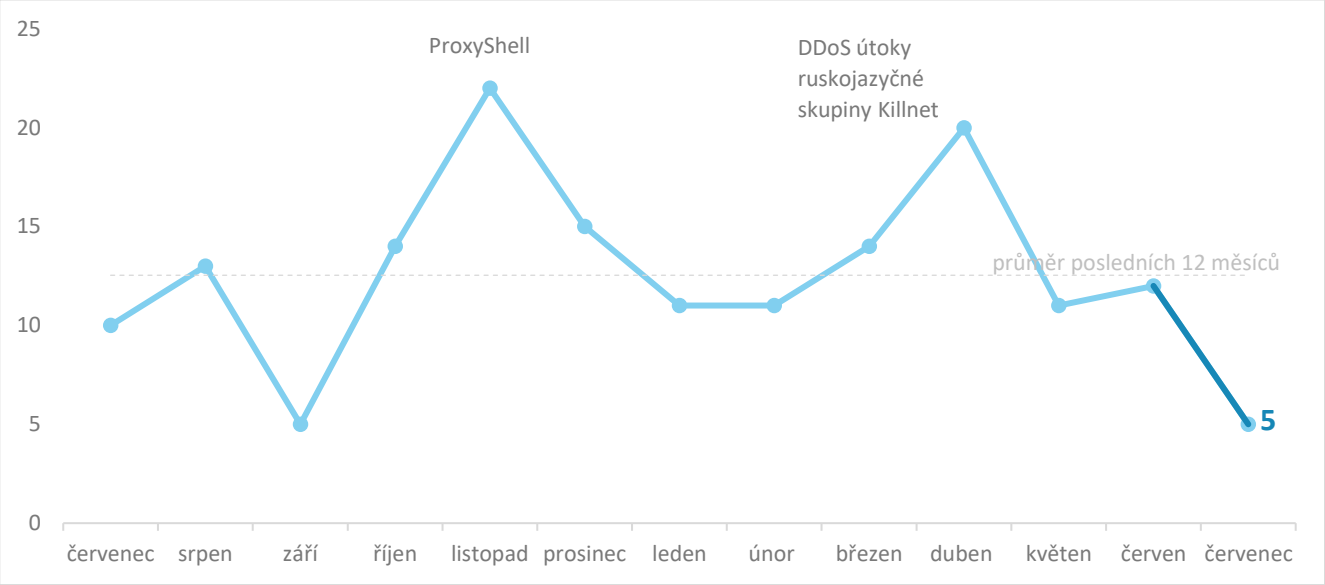


Následující report shrnuje dění měsíce. Data, informace a závěry v něm obsažené primárně vychází z kybernetických incidentů nahlášených NÚKIB. Pokud report v některých částech obsahuje informace z otevřených zdrojů, je vždy uveden původ těchto informací.

Připomínky a náměty na zlepšení reportu můžete posílat na adresu komunikace@nukib.cz

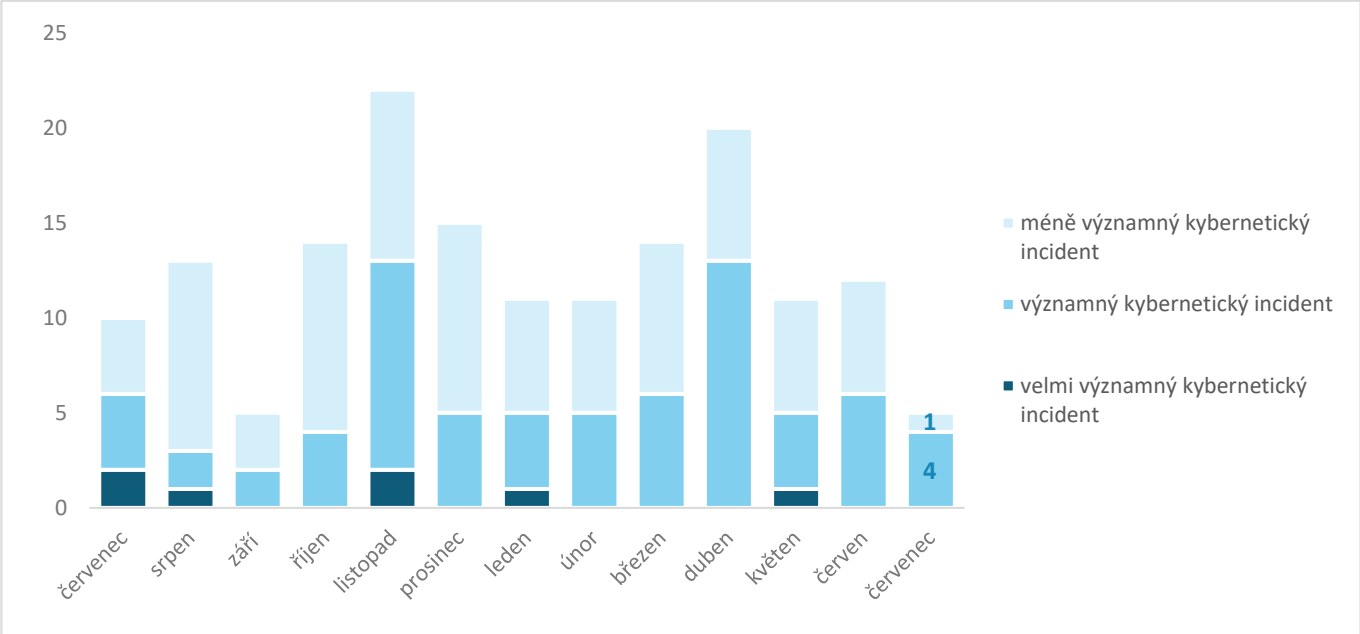
## Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

Počet incidentů se v měsíci červenci držel na velmi podprůměrných hodnotách. I na poměry jinak klidných letních měsíců se však jedná o nízké číslo.[1]




## Závažnost řešených kybernetických incidentů[2]

Během měsíce července výrazně převažovaly incidenty klasifikované jako významné. Stejně jako v červnu ani v minulém měsíci nedošlo k velmi významnému incidentu.

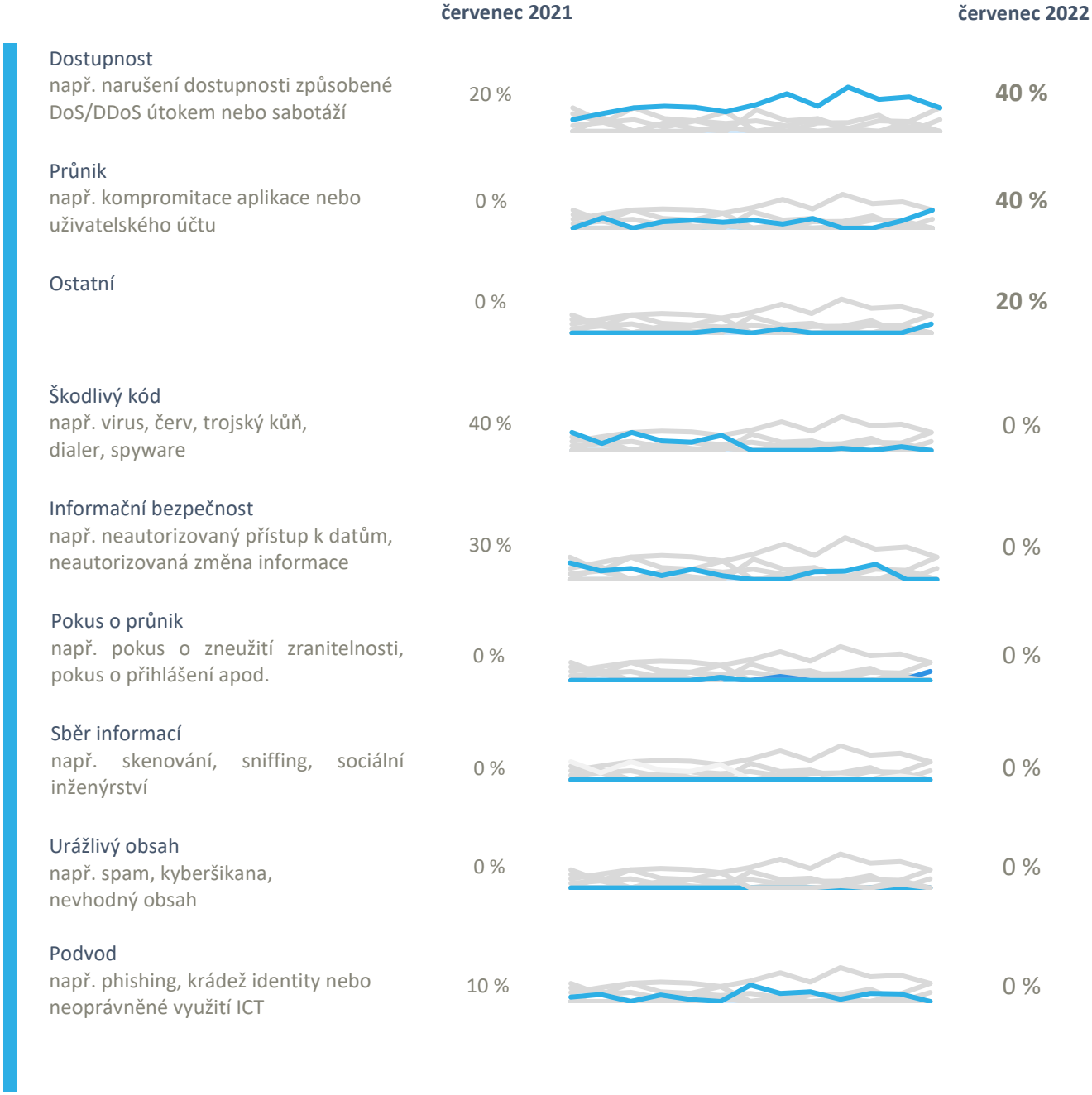



[1] Tři incidenty nahlásily NÚKIB povinné osoby dle zákona o kybernetické bezpečnosti. O zbylých dvou incidentech pak NÚKIB informovaly zákonem neregulované subjekty.
[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

## Klasifikace incidentů nahlášených NÚKIB[3]

Červencové kybernetické incidenty NÚKIB zařadil do třech kategorií:

- Nadále docházelo k útokům na dostupnost, které jsou trvalým trendem. V obou případech šlo o útoky ransomwaru proti neregulovaným subjektům. Druh ransomwaru není ani v jednom případě známý, přičemž obětmi byly i orgány samospráv.
- Podobně jsou trvalým trendem také průniky. Jejich počet zůstal na stejné úrovni jako v červnu, přestože lze pozorovat jejich větší závažnost.
- Jeden incident z kategorie ostatní se týkal krátkodobé nedostupnosti aplikace nasazené regulovaným subjektem. Vzhledem k jeho charakteru byl incident klasifikován jako významný.




[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

Phishing nebo pokusy o něj mají permanentní trend. Během července sice nebyl evidován žádný takový incident, nicméně vzhledem k útokům pomocí ransomwaru nelze vyloučit, že vektorem pro jejich provedení bylo právě sociální inženýrství.

### Malware

NÚKIB na základě dat z červencových incidentů žádný malware neanalyzoval.

### Zranitelnosti

Během července NÚKIB nevydal upozornění na nové zranitelnosti, ani nedetekoval výraznější zneužívaní konkrétních dosud známých zranitelností.

### Ransomware

Přestože podíl ransomwaru na celkovém počtu všech incidentů byl v červnu spíše nízký, trend vyděračských útoků pokračoval.

### Útoky na dostupnost

Podobně jako v předchozím měsíci nezpůsobil žádný incident DDoS útok.

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

## Technika měsíce: Deobfuscate/Decode Files or Information

NÚKIB kybernetické incidenty vyhodnocuje mj. na základě rámce MITRE ATT&CK, jenž slouží jako přehled známých technik a taktik používaných při kybernetických útocích. V tomto měsíci jsme se zaměřili na techniku T1140: Deobfuscate/Decode Files or Information.

**MITRE ID: T1140**

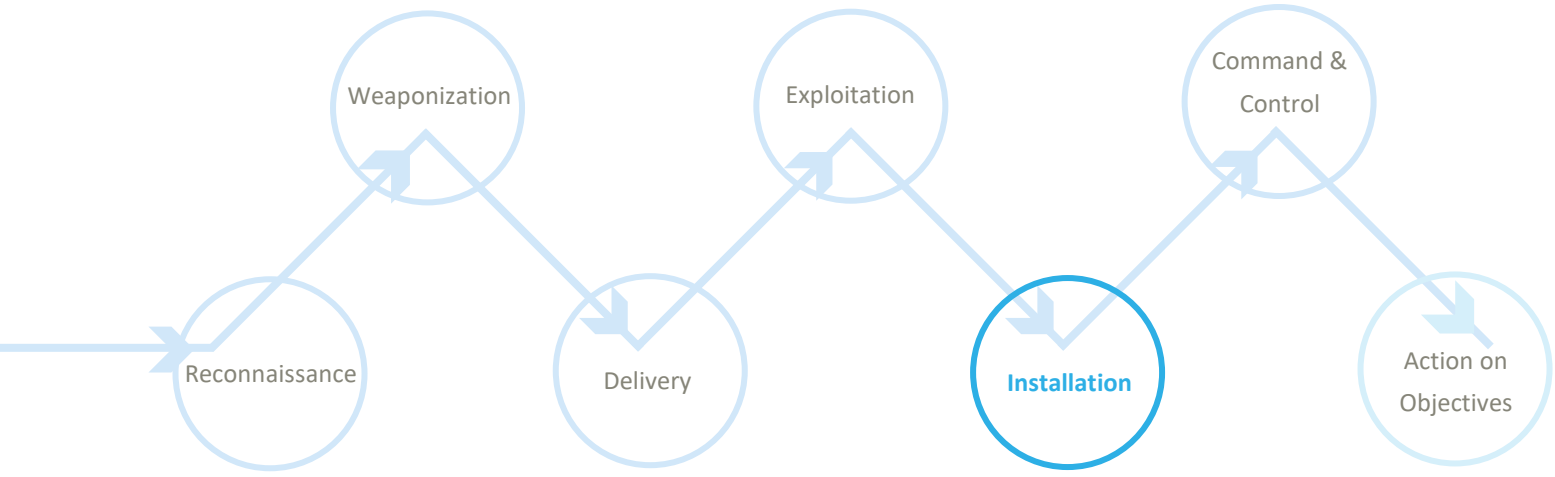
Tato technika je využívána k obcházení ochran a detekčních systémů. Malware je útočníkem do systému doručen zašifrovaný, zakódovaný do jiného formátu nebo rozdělený na více částí, což následně komplikuje efektivní kontrolu a soubor může být vyhodnocen jako neškodný. Posléze je malware dešifrován a sestaven do původní podoby jiným procesem, akcí uživatele či legitimním nástrojem (např. certutil). K dalšímu ztížení detekce je často dešifrování a následné spuštění provedeno pouze v paměti.

Metody praktického využití se mohou lišit od prostého zakódování škodlivého kódu do Base64 až po sofistikované typy využívající vícestupňovou asymetrickou kryptografii. Častým případem je také kombinace s technikou T1204: User Execution, kdy uživatel obdrží malware v archivu, k němuž zadá heslo.

**Mitigace:** Techniku nelze z její podstaty efektivně mitigovat, avšak lze podniknout kroky k účinnější detekci. Klíčové je především auditovat spouštění procesů a modifikace souborů, zejména takových, kde je rodičovským procesem kryptografický nástroj. Uživatelům je dále doporučeno věnovat zvýšenou pozornost u zaheslovaných archivů stažených z internetu nebo v přílohách e-mailu.

U vysoce citlivých systémů může být také pro včasnou detekci vhodná TLS inspekce provozu.

Znázornění techniky T1140 v kill chainu ukazujícím, kdy útočníci techniku používají:



## Zaměřeno na trend: útoky na místní samosprávy

V červenci byl NÚKIB informován o incidentu, kdy ransomware cílil na místní samosprávu. Jenom během roku 2022 je evidováno několik incidentů směřovaných vůči obecním a krajským úřadům, potažmo subjektům, které pod ně spadají. V tomto měsíci se proto zaměřujeme na útoky cílící na samosprávy.

**Samosprávy jsou lákavý cíl kvůli možnosti finančního zisku a v důsledku toho je jedním z nejčastějších druhů útoku ransomware.** Ten zablokuje systémy, čímž se základní služby poskytované městy a kraji stávají nedostupnými. Ze zkušeností jsou ohrožena jak velká města či samosprávy vyšších územních celků, kde lze očekávat možnost vyššího finančního zisku, ale též malé obce, u nichž naopak útočník neočekává silné zabezpečení.

Obr 1: Ilustrativní obrázek radnice

Hlavním problémem je nejen často nedostatečné IT zabezpečení, nýbrž i málo proškolení zaměstnanci. **Specifickým případem pak může být útok insidera, kdy zaměstnanec disponující širokými oprávněními z nějakého důvodu úmyslně poškodí vlastního zaměstnavatele nebo provádí činnosti, jež nejsou v souladu s jeho standardní pracovní náplní.**

**Doporučení:**

**NÚKIB vydal množství doporučení, jež mohou implementovat samosprávy.** Obecní, městské či krajské úřady mohou využít Minimální bezpečnostní standard, jehož cílem je napomoci subjektům nespadajícím pod zákon o kybernetické bezpečnosti. Pro výše postavené představitele samospráv jsou využitelná Základní bezpečnostní opatření pro vrcholové vedení. Pro základní proškolení zaměstnanců lze doporučit kurz „Dávej kyber“, případně pak pro manažery kybernetické bezpečnosti kurz „Šéfuj kyber“.

NÚKIB též představil dokument obsahující doporučení pro ochranu před spear-phishingem, jenž představuje častý vektor pro napadení. Dále byla vydána analýza upozorňující na hrozbu ransomwaru, který zůstává jednou z hlavních hrozeb pro samosprávy.

## 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. |