RANSOMWARE: DOPORUČENÍ PRO MITIGACI, PREVENCI A REAKCI

Verze 1.1, platná ke dni 26. listopadu 2020

NÚKIB

AFCEA

Na přípravě Ransomware: Doporučení pro mitigaci, prevenci a reakci dále spolupracovali:

AFCEA

NAKIT

Národní agentura pro komunikační a informační technologie, s. p.

NÚKIB

AFCEA

Obsah

1 Úvod

Ransomware je druh škodlivého kódu (malware), který zašifrováním zabrání uživateli v přístupu k datům. Ve většině případů poté útočník vyžaduje zaplacení určité částky za obnovení (dešifrování) dat. Motivace útočníků je tedy zejména finanční zisk, nicméně existují i případy, kdy útočník data jednoduše zničil a nepožadoval žádné výkupné (angl. ransom). Čím dál častější motivací je i hrozba zveřejnění dat, zejména při napadení firem, jejichž data obsahují citlivé informace o jejich zákaznících. Více o hrozbě ransomwaru naleznete na https://nukib.cz/download/publikace/analyzy/Analyza_hrozby_ransomware.pdf.

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

2 Vektory útoku

Mezi hlavní způsoby, jakými se ransomware dostane na počítač, patří:

- **Phishing**
  - Phishingová zpráva (e-mail, zpráva na sociálních sítí či messengerech) se adresáta snaží přesvědčit, že se jedná o legitimní komunikaci od společnosti, organizace nebo jednotlivce. V případě spear-phishingu jde o vysoce cílenou zprávu namířenou na konkrétního zaměstnance nebo skupinu zaměstnanců. V obou případech je účelem přesvědčit adresáta, aby stáhl a otevřel škodlivou přílohu nebo odkaz. Tím dojde k nakažení zařízení malwarem. Více o rizicích spear-phishingu a phishingu naleznete na https://nukib.cz/cs/infoservis/doporuceni/1514-spear-phishing-a-jak-se-pred-nim-chranit/.
- **Nezabezpečené služby otevřené do internetu**
  - Pokud má vaše organizace otevřené služby do sítě internet, útočníci se mohou pokusit prolomit jejich autentizaci pomocí bruteforce útoku. Pokud uspějí, mohou se přes tyto otevřené služby dostat dále do sítě.
- **Zneužití zranitelného zařízení nebo služby**
  - V případě neaktualizovaných aplikací a systémových služeb se na zařízení může nacházet jedna či více zranitelností, které mohou útočníkům umožnit přístup do systému i bez jakékoli aktivity uživatele (zranitelnost různých protokolů jako např. RDP, SMB, nebo webového serveru aj.).
- **Zneužití odcizených přihlašovacích údajů**
  - Ročně dojde k úniků stovek milionů přihlašovacích údajů jednotlivých uživatelů, kteří o tom často ani nevědí. S ukradenými údaji se pak často obchoduje na černých trzích, kde je hackeři mohou koupit. V případě, že takto uniknou údaje někoho z vaší organizace, je možné, že se toho útočníci pokusí zneužít, a pokud nedojde ke změně přihlašovacích údajů, může se jim to podařit.

Kroky k zabezpečení vaší sítě před ransomwarem:

- aktualizovat OS, programy a aplikace;
- zablokovat služby otevřené do veřejné sítě, vyjma těch nejnutnějších, ty dostatečně zabezpečit;
- omezit administrátorské účty pouze pro administrátory;
- nastavit skrze bezpečnostní politiky povinnost používat silná a bezpečná hesla;
- segmentovat síť vaší organizace dle bezpečnostních možností a potřeb;
- ukládat síťové logy na nezávislém serveru mimo podnikovou síť;
- vytvářet bezpečné zálohy a testovat jejich použití;
- zvyšovat povědomí uživatelů o hrozbě ransomware a jeho vektorech;
- mít připraven krizový plán a trénovat jeho nasazení.

- **Kompromitace skrze poskytovatele služeb**
  - Výjimečné nejsou ani infekce skrze třetí stranu, kterou může být např. dodavatel software, hardware či jiných služeb (včetně služeb typu Software as a Service (SaaS)). V případě, že dojde ke kompromitaci sítě třetí strany, vaše síť může být následně infikována skrze datové médium (USB disk) či stroj třetí strany ať už připojovaný vzdáleně nebo lokálně.

3 Preventivní opatření

Zásadním krokem pro minimalizaci dopadů ransomware je pravidelné bezpečné zálohování a jeho správná implementace.

Nedávné kybernetické útoky na české instituce ukázaly dva typy strategií, které útočníci při svých útocích využívají.

První a v minulosti nejvíce využívanou strategií je ta, kdy útočník infikuje škodlivým kódem libovolnou stanici a vzápětí začne šifrovat všechna připojená média, lokální a síťové disky aj., ke kterým má v danou chvíli přístup.

Druhá strategie, kterou v posledních měsících útočníci hojně využívají, je ta, kdy po několik dnů až týdnů operují nepozorovaně v síti napadené instituce a snaží se získat přístupové údaje pro správu celé domény. Jakmile se jim to podaří, zahájí útok na síť celé instituce. Ten se skládá z několika fází, ne všechny ale musí být bezpodmínečně součástí útoku. První je odcizení záloh či případně citlivých dat. Ve druhé fázi dochází ke smazání všech dostupných záloh (lokální zálohy (VSS), online zálohy apod.). Ve třetí fázi je zahájeno šifrování na všech stanicích v doméně, kam má útočník v danou chvíli přístup.

Základní pravidla pro zálohování:

1. Pravidlo 3 – 2 – 1
   - Nejméně 3 kopie na 2 různých zařízeních, z toho 1 mimo organizaci.
2. Neaktivní záloha
   - Minimálně jedna nebo více záloh musí být neaktivní (off-line) v jednom okamžiku.
   - V případě záloh v cloudu důsledně nasadit správu identit a řízení přístupu.
3. Obnovitelnost
   - Plán obnovy
   - Zálohy jsou testovány a jsou použitelné k obnově.
4. Pravidelnost
   - Plán zálohy
   - Zálohy musí být vytvářeny pravidelně.

Z výše uvedeného je vidět, že špatně nastavené zálohování může mít pro instituci stejné následky jako v případě, že není prováděna žádná záloha. Proto zde uvedeme několik základních doporučení/rad, kterých by se měl administrátor při zálohování držet. Nejdříve ale uvedeme, s jakými typy záloh se můžeme setkat.

V praxi se setkáváme s třemi typy záloh online, off-line a vzdálená záloha.

Online záloha: Jedná se o zálohu, která je dostupná v síti instituce pro okamžité zálohování/obnovu dat z poslední zálohy. U tohoto typu se nejčastěji provádí tři typy zálohy tzv. plná záloha, inkrementální záloha a rozdílová záloha.

- **Plná záloha** – je zdlouhavější a zpravidla prováděna v době, kdy je provoz instituce na nižší úrovni např.
  v nočních hodinách, případně o víkendech a je vhodné ji provádět minimálně jednou za měsíc.
- **Inkrementální záloha** – je pořizována oproti plné záloze a jsou ukládány pouze soubory, které se změnily oproti předešlé plné nebo inkrementální záloze. Jedná se o velmi rychlý typ zálohy, který klade menší nároky na úložný prostor. Lze provádět každý den, v závislosti na důležitosti dat, která jsou zálohována. K obnově dat z této zálohy je potřeba plná záloha a celý řetězec inkrementálních záloh, až po zálohu, ze které chceme obnovu provádět.
- **Rozdílová záloha** – jedná se o podobný typ jako je záloha inkrementální. Rozdíl je pouze v tom, že se vytváří rozdíl oproti plné záloze a nebere se tak v potaz žádná jiná předtím vytvořená záloha. K obnově dat z této zálohy je tak potřeba mít pouze poslední plnou zálohu.

Obrázek 1: Dle ideálního modelu je vhodné vytvořit tři zálohy, které budou na dvou různých typech úložišť, přičemž jedno z nich bude mimo pracoviště.

U online záloh je také důležitým pojmem retence dat. V překladu – doba uchování záloh. Jelikož jsme na začátku zmínili, že se útočník může v síti pohybovat dny až týdny je vhodné dobu retence nastavit s ohledem na tyto informace. Pokud bychom tak neučinili, může se stát, že si stanice obnovíme do stavu, kdy je již ovládána útočníkem a problém s ransomware by se mohl opakoval. Tento parametr se často nastavuje na 1, 2, 3 nebo 12 měsíců.

Off-line záloha: Jedná se o datovou zálohu, která je uložena nejčastěji na off-line úložišti, kterým může být externí disk, datové pásky apod. Obnova z takové kopie zabere mnohem více času než obnova z tzv. online zálohy a zpravidla se nejedná o poslední verzi zálohy, ale o zálohy starší. Z praxe to může být měsíc, častěji ale více. Doporučujeme tuto zálohu provádět pravidelně, jelikož v nejhorším scénáři se může jednat o poslední záchranu kritických dat instituce.

Vzdálená záloha: Jedná se o typ zálohy, která se fyzicky nachází v jiné lokalitě (off-line), případně na cloudovém úložišti. Pokud se rozhodnete takovou zálohu vytvořit, je dobré pamatovat na to, že tyto zálohy je vhodné šifrovat, aby se zamezil přístup k datům nepovolané osobě.

Doporučení/rady pro bezpečné zálohování:

- mít zpracovaný plán záloh a plán obnovy;
- pravidelně zálohovat;
- zálohovací server/uložiště by se měl nacházet mimo produkční síť, zpravidla v oddělené síti nebo jiné VLAN;
- záloha by měla probíhat tak, že zálohovací server přistupuje k zálohovanému médiu, nikoliv naopak
- zálohovací server je spravován prostřednictvím speciálních administrátorských účtů (mimo Active Directory), nikoliv těmi běžně používanými, zejména ne účtem doménového administrátora;
- doporučujeme zálohovací server nemít připojený do domény a spravovat jej pomocí lokálních účtů;
- využívá-li zálohovací server diskové úložiště, doporučujeme u něj zvolit vytvoření RAIDového pole, které zajistí, že data ze záloh bude možné obnovit i v případě, že dojde k poruše některého z disků;
- udržovat operační systém se softwarem aktualizovaný a podporovaný;
- provádět pravidelné testování funkčnosti vytvářených online i off-line záloh;
- současně doporučujeme provádět zálohy doménového řadiče (politiky, účty apod.) pro případ, že bude potřeba provést obnovu celé domény;
- ověřovat čitelnost a obnovitelnost zálohovaných dat;
- mít k dispozici záložní hardware pro obnovu produkčního systému.

Obrázek 2: Zásadním krokem pro minimalizaci dopadů ransomware je pravidelné bezpečné zálohování a jeho správná implementace.

3.1 Segmentace sítě

Segmentace sítě většinou není vnímána jako bezpečnostní opatření, avšak z pohledu současných útoků správně nakonfigurovaná segmentace dokáže zkomplikovat rozšíření malware po síti vaší organizace. A bezpochyby patří mezi základní bezpečnostní opatření.

Segmentovaná síť je opakem tzv. "ploché" sítě, která je nevhodnějším prostředí pro šíření malware. V ploché síti se nachází všechna zařízení (koncové stanice, servery, tiskárny, BYOD) ve stejném segmentu a mohou mezi sebou napřímo komunikovat. Rozdělení vaší sítě do více segmentů je pouze prvním krokem. Řízení přístupu do jednotlivých segmentů je to, co ztěžuje život malware a brání jeho rozšíření.

Segmentaci sítě lze realizovat například na:

- linkové vrstvě – rozdělení sítě do jednotlivých VLAN dle určení

Řízení přístupu lze realizovat na několika úrovních ISO/OSI modelu, například na:

- linkové vrstvě – nasazení ACL mezi jednotlivé VLANy
- síťové vrstvě – filtrace na základě IP
- transportní vrstvě – filtrace na základě portů
- aplikační vrstvě – filtrace na základě aplikace

Doporučení:

- Rozdělit síť vaší organizace do jednotlivých segmentů s ohledem na důležitost poskytovaných služeb a dat.
- Rozdělit síť do jednotlivých segmentů s cílem ochránit a být schopen detekovat pokus o neoprávněný přístup ke kritickým službám a datům.
- Vytvořit jednotlivé VLANy pro izolaci daných segmentů.
- Vytvořit VLANy pro správu sítě (administrace síťových prvků, serverů, zálohování).
- Definovat pravidla (filtrace VLAN, IP, portů, aplikací) pro přístup do jednotlivých segmentů s ohledem na poskytované služby a data.
- Zakázat přímou komunikaci mezi koncovými stanicemi (i v rámci stejné VLAN) pomocí privátních VLAN, u wifi pomocí client isolation, případně úpravou lokálního firewallu.
- Definovat služby a zařízení, se kterými koncové stanice mohou komunikovat, vše ostatní zakázat.
- Definovat služby a zařízení, se kterými servery mohou komunikovat.

3.2 Aktualizace

Udržujte všechny aplikace i operační systém aktuální. Staré nebo zranitelné verze často bývají terčem útočníků. Zároveň se ujistěte, že vaše zařízení jsou správně nakonfigurována a bezpečnostní funkce zapnuty.

Pozornost věnujte i otevřeným službám a portům, které nutně nepotřebujete k vaší práci, více v další kapitole.

Velmi důležité jsou aktualizace antivirových řešení a jejich databází. V jejich případě je nejlepší možností automatická aktualizace.

3.3 Otevřené služby

Doporučujeme kontrolovat otevřené porty na stanicích a blokovat služby otevřené do veřejné sítě včetně služeb pro vzdálený přístup. Cílem opatření je minimalizovat riziko průniku útočníka do systému za využití zranitelností v systému nebo útoku hrubou silou. Ponechte otevřené pouze ty služby, které jsou nutné pro běh vaší organizace.

Často zneužívanými službami jsou protokoly RDP, SMB, telnet a SSH s heslem. Je vhodné výrazně omezit jejich použití a dostupnost na všech stanicích včetně serverů. Pokud uvedené služby potřebujete, povolte přístup k nim pouze z interní sítě nebo přes VPN.

Doporučujeme ověřit, jak je spravovaná síť a její služby reálně viditelné z internetu (provést skenování sítě, možnost nahlédnout do výstupů internetových skenovacích nástrojů jako např. Shodan apod.).

Vládní CERT (kontakt na konci dokumentu) nabízí možnost oskenování otevřených služeb v rámci programu průběžného skenování zranitelností. Zapojené subjekty jsou na základě podepsané smlouvy dlouhodobě monitorovány nejen z hlediska otevřených služeb, ale i z hlediska přítomnosti nejznámějších zranitelností, a to zejména za pomoci automatizovaných skenovacích nástrojů.

3.4 Uživatelé a hesla

Uživatel často bývá nejslabší článek řetězce, dbejte proto na školení zaměstnanců. Dbejte na to, aby uživatelé dodržovali základní kyberbezpečnostní hygienu. **Je nesmírně důležité používat pro různé služby různá hesla.** Ať už se jedná o heslo k zálohám, online službám (Facebook, Google), logovacímu nebo doménovému serveru. V případě kompromitace jedné služby budou ostatní v pořádku. Pokud se registrujete do různých soukromých online služeb, v žádném případě nepoužívejte pro tyto účely služební či firemní e-mail. Bezpečnostní návyky zaměstnanců lze otestovat například simulovanými phishingovými e-maily.

Doporučená minimální délka hesla dle vyhlášky 82/2018, § 19 je alespoň 12 znaků pro uživatele, 17 znaků pro administrátory. Jako krok navíc můžete volit hesla se zvýšenou složitostí, kombinovat různé druhy znaků, neodvozovat je z jiných hesel, jmen, dat narození apod. Tyto nároky jsou přirozeně náročné na lidskou paměť, proto můžete pro zapamatování hesel použít tzv. password manager s využitím hlavního hesla, např. Keepass.

Pro co nejvyšší úroveň zabezpečení je vhodné nasadit i vícefaktorovou autentizaci (MFA) v podobě hardwarových či softwarových tokenů, která může výrazně snížit možnost útočníka pohybovat se v síti.

K předejití zneužití uniklých databází přihlašovacích údajů je rovněž doporučeno hesla periodicky měnit.

3.5 Uživatelské účty

Pro běžnou práci uživatele na jeho stanici (e-mail, prohlížeč, dokumenty) přidělte uživateli pouze běžná práva. Běžné a základní úkony by uživatelé v žádném případě neměli provádět s administrátorskými právy. To samé platí pro doménového administrátora – v žádném případě by tento účet neměl provádět běžnou činnost, ani samotné přihlašování se na klientské stanice nebo jiné servery. Tento účet používejte pouze pro správu domény a k žádným jiným činnostem.

Pokud se útočníkovi podaří získat přístup k účtu doménového administrátora, např. právě při jeho použití pro běžnou činnost, může tato kompromitace vést k ovládnutí celé sítě.

3.6 E-maily a přílohy

Zvýšenou pozornost si zaslouží zejména práce s dokumenty a přílohami e-mailů. V případě, že makra ve vaší organizaci nepoužíváte, technicky vynuťte jejich zákaz. Pokud je využíváte a je to možné, zaveďte ve vaší organizaci podepisování maker a technicky vynuťte spuštění pouze podepsaných maker nebo alespoň poučte uživatele, že makra se v dokumentech povolují pouze pokud jsou si zcela jisti původem a účelem dokumentu.

Přílohy emailů otevírejte opět pouze v případě, že jste si zcela jisti původem a účelem e-mailu, který Vám přišel. Pokud můžete ovlivnit nastavení e-mailového serveru, doporučujeme blokovat přílohy obsahující spustitelné soubory, popř. skripty. Počet podvržených, a tedy potenciálně nebezpečných e-mailů je možné snížit pomocí kontroly záznamu SPF, DKIM a DMARC u přijatých e-mailů na straně e-mailového serveru.

Pro omezení dopadu případu, kdy uživatel otevře závadný email, doporučujeme zvážit nastavení restrikce spouštění souborů na klientských stanicích, případně nasadit technické prostředky sloužící k prověření škodlivosti příloh před doručením uživateli (např. sandboxing).

Doporučujeme rovněž uživatelům opakovaně zdůrazňovat, že veškerou podezřelou komunikaci mají hlásit, a jasně definovat autoritu, na kterou tato hlášení mají být směřována.

3.7 Logy

Pro efektivní reakci na incidenty jsou důležité logy, které je potřeba bezpečně ukládat. V případě incidentu jsou důležitým zdrojem informací a pomohou odhalit mj. i stupeň rozšíření nákazy. Regulované subjekty mají z vyhlášky definovanou dobu uchováni logů minimálně 12 nebo 18 měsíců, dle druhu regulovaného subjektu. Tuto dobu však doporučujeme všem správcům.

Nejlepší možností logování je ukládat logy na jiný stroj, než ze kterého pochází, ideálně mimo doménu, tj. využít log management. V případě napadení některé stanice se útočník může pokusit smazat po sobě logy a stopy z napadeného operačního systému. Pokud jsou tyto informace zkopírované na jiném, nezávislém

serveru, budou při vyšetřování dostupné. Zároveň je vhodné tyto logy zabezpečit proti smazání či manipulaci s nimi i ze strany administrátorů, jejichž účtů se může útočník zmocnit. Pro další zefektivnění práce vyšetřování je vhodné správně nastavit logování na klientských stanicích a serverech, a to následujícím způsobem:

Povolit zejména tyto události:

- Úspěšné/neúspěšné přihlášení
  - Audit logon: success, failure
- Odhlášení
  - Audit logoff: success
- Přihlášení privilegovaného uživatele
  - Audit special logon: success
- Auditování Powershellu (je nutné mít Powershell 5)
  - Cesta: Administrative Templates\Windows Components\Windows Powershell
  - Nastavení: Turn on Powershell Script Block Logging
- Auditování příkazové řádky
  - Cesta: Administrative Templates\System\Audit Process Creation
  - Nastavení: Include command line in process creation events
- Manipulace s účty
  - Audit user account management: success
- Manipulace se skupinami
  - Audit security group management: success
- Změna politiky autentizace
  - Audit authentication policy change: success
- Spuštěné procesy
  - Audit process creation: success

Více doporučení lze nalézt v oficiálním dokumentu firmy Microsoft (https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations).

V žádném případě nemažte jakákoli data bez svolení Policie ČR nebo NÚKIB.

3.8 Proaktivní monitoring infrastruktury

V případě, že dojde k infikování infrastruktury, je třeba co nejrychleji tento stav detekovat a umožnit tak mitigaci hrozby. Pro tento účel je třeba využívat prostředků detekujících anomální chování, podezřelou komunikaci.

3.9 Krizový plán

Pro případ, že selžou všechna opatření a vaše síť a systémy budou napadeny ransomwarem, doporučujeme vytvořit krizový plán. Jeho součástí by měl být nejen postup reakce na úspěšný ransomwarový útok a obnovu systémů (**Disaster Recovery Plan**), ale pozornost by měla být věnována i minimalizaci dopadů útoku na chod vaší organizace (**Business Continuity Plan)**. Potřeby každé organizace se mohou lišit, nicméně doporučujeme nastavit procesy pro případ, že zaměstnanci nebudou mít přístup k počítačům a dalším zařízením v síti vaší organizace. Na takovou situaci lze reagovat vytvořením paralelních krizových „off-line procesů“ a dále dostatečných zásob psacích potřeb a papíru (a dát zaměstnancům vědět, kde je najdou) nebo mít k dispozici záložní počítače a další zařízení, která nebyla napojena na kompromitovanou síť.

Každá organizace by měla mít stanovené alespoň následující:

- Plán obnovy, který obsahuje zejména: systémy, které budou obnovovány vč. priorit; časové plány obnovy; odpovědné osoby; dodavatele vč. kontaktů apod., tedy konktrétně Disaster Recovery Plan, který obsahuje:
    - Minimální úroveň poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního a komunikačního systému.
    - Doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního a komunikačního systému.
    - Bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání.
- Plán komunikace, který bude pokrývat alespoň následující:
    - kdo s kým a co bude komunikovat, zejména kdo komunikaci schvaluje, kdo komunikuje vně organizace (např. směrem k médiím, zákazníkům, úřadům apod.) a kdo dovnitř (např. směrem k zaměstnancům).
- Plán zajištění kontinuity provozu (Business Continuity Plan), který pomůže zajistit provoz organizace a její fungování i v případě, že je zásadním způsobem ohrožena kybernetická bezpečnost firmy. Plán by měl obsahovat např.:
    - krizová opatření a organizační pokyny pro udržení chodu organizace i případě rozsáhlého kybernetického incidentu;
    - pokyny pro zaměstnance v případě krizové situace, včetně alokace lidí, nástrojů a dalších zdrojů.

Každý plán by měl zahrnovat odpovědné osoby za jednotlivé činnosti, potřebné zdroje, kontakty na dodavatele apod. Tyto plány by měly být uloženy mimo systém tak, aby byla zajištěna jejich dostupnost i v případě incidentu.

4 Reakce na ransomwarový útok

Dále naleznete seznam úkonů, které je potřeba vykonat po zjištění ransomware útoku na vaši organizaci. Záměrně je koncipován do seznamu, kterého se můžete v případě incidentu držet a umožnit tak efektivnější řešení incidentu.

4.1 Neprodleně po zjištění útoku

- Odpojte zálohovací server od sítě, popř. jej odpojte od elektřiny.
- Maximálně omezte síťovou komunikaci mezi stroji (např. panic mode na firewallech).
- Pokud nejste zařízení v síti schopni vypojit na síťové úrovni, odpojte je od zdroje elektrické energie.
- Odpojte komunikaci do veřejné sítě.
- Zjistěte rozsah napadení a napadené systémy izolujte, dokumentujte zjištění.
- Pozastavte virtuální stroje, pokud je to možné, jinak pořiďte snapshot a vypněte.
- Kontaktujte manažera kybernetické bezpečnosti (MKB), vedení vaší organizace, NÚKIB, Policii ČR.
- Požádejte o logy ze sondy/firewallu/od poskytovatele internetu.

4.2 Další doporučení

- Vytvořte seznam klíčových lidí z organizace a decision makerů (MKB, DPO, vedoucí/ředitel/náměstek IT, ředitel organizace) a stanovte komunikační plán v případě takového incidentu.
- Vytvořte dostatečný rozpočet pro obnovu infrastruktury.
- Neplaťte výkupné
    - V případě napadení ransomwarem jsou organizace vystaveny silnému tlaku veřejnosti. Postižené organizace proto mohou být nakloněny zaplacení výkupného. NÚKIB I Světová bezpečnostní komunita se shodují, že by výkupné nemělo být za žádných okolností placeno z těchto důvodů:
        1. Zaplacení utvrdí útočníka v ziskovosti jeho jednání a motivuje jej k dalším útokům.
        2. Neexistuje záruka, že útočník data skutečně odblokuje.
        3. Odblokování dat neodstraní samotný ransomware ani další potenciální malware; situace se tak může i přes zaplacení výkupného rychle opakovat.
        4. Z právního hlediska může představovat zaplacení výkupného porušení zásad péče řádného hospodáře.

4.3 Před zahájením obnovy

- Definujte nejdůležitější služby, systémy a aktiva pro chod instituce
- Pro rychlejší a efektivnější komunikaci připravte nalepovací jmenovky pro každého, kdo se bude účastnit obnovy
- Zajistěte dostatečně velkou místnost pro analytiky, dodavatele a další zúčastněné, ideálně vybavenou tabulemi (whiteboard, flipchart)

4.4 Postup při obnově dat/sítě

- Zjistěte stav online a off-line záloh.
- Zajistěte alternativní internetové připojení.
- Navrhněte novou architekturu sítě.
- Definujte segmentaci sítě.
- Vytvořte čistou VLAN, ve které se začne budovat nová infrastruktura.
- Audit administrátorských účtů a reset všech administrátorských hesel v celé infrastruktuře.
- Připravte čisté administrátorské stanice, kterým můžou administrátoři plně důvěřovat.

NÚKIB

AFCEA

5 Další informace

- FireEye, 2016, Greater Visibility Through PowerShell Logging, https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html
- Microsoft, 2017, Command line process auditing, https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing
- NÚKIB, 2020, Vyděračské útoky ransomwarem jsou čím dál cílenější, https://nukib.cz/cs/infoservis/aktuality/1644-vyderacske-utoky-ransomwarem-jsou-cim-dal-cilenejsi/
- NÚKIB, 2020, Poskytované služby, https://nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/poskytovane-sluzby/
- NÚKIB, 2020, Analýza hrozby ransomware, https://nukib.cz/download/publikace/analyzy/Analyza_hrozby_ransomware.pdf
- NÚKIB, 2020, Spear-phishing a jak se před ním chránit, https://nukib.cz/cs/infoservis/doporuceni/1514-spear-phishing-a-jak-se-pred-nim-chranit/
- NÚKIB, 2019, Bezpečnostní doporučení NÚKIB pro administrátory 4.0, https://www.nukib.cz/download/publikace/vzdelavani/Admin%204.0%20brozura.pdf
- NÚKIB, 2020, Spear-phishing – doporučneí pro personál nemocnic, https://nukib.cz/download/publikace/doporuceni/Doporuceni_spear_phishing_pro_personal_nemocnic_modre.pdf

6 Kontakty

GovCERT.cz

- Hlášení incidentů: cert.incident@nukib.cz
- Obecný komunikační kanál: cert@nukib.cz
- Mimo pracovní dobu: pohotovostní telefonní číslo +420 725 502 878
- Během pracovní doby: telefonní číslo +420 541 110 777

CSIRT.cz

- Hlášení incidentů: abuse@csirt.cz

PČR

- Místně příslušné oddělení Policie ČR
- Postup pro podání trestního oznámení naleznete na https://www.policie.cz/clanek/oznameni-trestneho-cinu.aspx

7 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách www.nukib.cz/cs/infoservis/doporuceni/1593-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci/). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená 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.
Oranžová 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.
Zelená 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.
Bílá 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.

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
23.11.2020	1.0	NÚKIB, AFCEA	Vytvoření dokumentu
26.11.2020	1.1	NÚKIB, AFCEA	Zapracování připomínek AFCEA