RANSOMWARE: DOPORUČENÍ PRO MITIGACI, PREVENCI A REAKCI

Verze 1.2, platná ke dni 22. května 2023

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 jejich obnovení (dešifrování). Motivací pro použití této praktiky je tedy zejména finanční zisk, nicméně existují i případy, kdy útočník data jednoduše zničí a žádné výkupné (angl. ransom) nepožaduje. Čím dál častější je i hrozba jejich zveřejněním, zejména pak při napadení firem, které uchovávají a zpracovávají data obsahující citlivé informace o 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 autorům dokumentu.

2 Vektory útoku

Mezi hlavní způsoby, jakými se ransomware dostane do počítače, patří:

- **Phishing**
  - Phishingová zpráva (e-mail, zpráva na sociálních sítích či komunikačních aplikacích) 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 určitou skupinu. V obou případech je účelem přesvědčit adresáta, aby stáhl a otevřel škodlivou přílohu nebo klikl na 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 Internetu, útočníci se mohou pokusit prolomit jejich autentizaci pomocí útoku hrubou silou, tzv. bruteforce útoku. Pokud uspějí, mohou se přes tyto otevřené služby dostat dále do vaší 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).
- **Zneužití odcizených přihlašovacích údajů**
  - Ročně dojde k úniků stovek milionů přihlašovacích údajů jednotlivých uživatelů, kteří o tom často ani nevědí. Obvykle se s daty obchoduje na černých trzích, kde je mohou koupit hackeři či další zájemci. V případě, že takto uniknou údaje z vaší organizace, je možné, že se toho útočníci pokusí zneužít a nedojde-li k včasné změně přihlašovacích údajů, může se jim to i podařit.
- **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.

Kroky k zabezpečení vaší sítě před ransomwarem

- Aktualizovat operační systém (OS), programy a aplikace.
- Zablokovat služby otevřené do veřejné sítě, vyjma těch nejnutnějších. Ty dostatečně zabezpečit.
- Omezit přístup k administrátorským účtům.
- 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.

NÚKIB

AFCEA

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 nejčastěji využívají.

První, a v minulosti nejvíce využívanou, 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.

V rámci druhé strategie, útočníci 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 celou její síť. Ten se skládá z několika fází, všechny ale nemusí bezpodmínečně proběhnout. V první fázi jsou odcizeny zálohy čicitlivá data. Ve druhé pak 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 (offline) 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 lze vydedukovat, že špatně nastavené zálohování může mít pro instituci stejné následky jako v případě, že není prováděna záloha žádná. Proto zde uvádíme několik základních doporučení/rad, kterých by se měl administrátor při zálohování držet. Nejdříve ale představíme tři základní typy záloh, s jakými se lze v praxi setkat: online, offline a vzdálenou.

Online záloha je dostupná v síti instituce pro okamžité zálohování a případnou obnovu dat z posledního zálohování. V rámci ní lze rozlišovat tzv. plnou, inkrementální a rozdílovou zálohu.

- **Plná záloha** – Jelikož její provedení probíhá po delší dobu, bývá zpravidla prováděna v době, kdy je provoz instituce na nižší úrovni např. v nočních hodinách, případně o víkendech. Je vhodné ji provádět minimálně jednou za měsíc.
- **Inkrementální záloha** – Dochází k ukládání pouze těch souborů, které se změnily oproti předešlé plné nebo inkrementální záloze. Jedná se o velmi rychlý typ, jenž klade menší nároky na úložný prostor. Lze provádět každý den, v závislosti na důležitosti zálohovaných dat. K jejich případné obnově je potřeba plná záloha a celý řetězec inkrementálních záloh.

- **Rozdílová záloha** – Je podobná inkrementální záloze. Liší se pouze v tom, že oproti plné záloze se vytváří rozdíl a nebere se v potaz žádná jiná předtím vytvořená záloha. K obnově dat 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 důležité zmínit pojem **retence dat**. V překladu – doba uchování záloh. Jelikož se útočník může v síti pohybovat dny až týdny, je vhodné dobu retence nastavit s ohledem na tuto skutečnost. Pokud bychom tak neučinili, může se stát, že stanice obnovíme do stavu, kdy již byla ovládána útočníkem, a problém s ransomware by se tak mohl opakoval. Tento parametr se povětšinou nastavuje na 1, 2, 3 nebo 12 měsíců.

Offline záloha je uložena nejčastěji na offline úložišti, kterým může být externí disk, datové pásky apod. Obnova z takové kopie zabere mnohem více času než obnova z online zálohy a zpravidla se nejedná o poslední verzi, ale o zálohy starší. Z praxe to může být měsíc, častěji ale více. Doporučujeme ji provádět pravidelně, jelikož při nejhorším scénáři se může jednat o poslední záchranu kritických dat instituce.

Vzdálená záloha se fyzicky nachází v jiné lokalitě (offline), případně na cloudovém úložišti. Pokud se rozhodnete takovou zálohu vytvořit, je vhodné ji šifrovat, aby se zamezil přístup k datům nepovolané osobě.

Doporučení/rady pro bezpečné zálohování:

- Mějte zpracovaný plán záloh a plán obnovy.
- Pravidelně zálohujte.
- Mějte zálohovací server/uložiště umístěn mimo produkční síť (zpravidla v oddělené síti nebo jiné VLAN).
- Při záloze má zálohovací server přistupovat k zálohovanému médiu, nikoliv naopak.
- Spravujte zálohovací server prostřednictvím speciálních administrátorských účtů (mimo Active Directory), nikoliv těmi běžně používanými a zejména ne účty doménového administrátora.
- Nemějte zálohovací server připojený do domény a nespravujte jej pomocí lokálních účtů.
- Využívá-li zálohovací server diskové úložiště, zvolte vytvoření RAIDového pole, které zajistí, že data ze záloh bude možné obnovit i v případě, kdy dojde k poruše některého z disků.
- Udržujte operační systém se softwarem aktualizovaný a podporovaný.
- Provádějte pravidelné testování funkčnosti vytvářených online i offline záloh.
- Provádějte zálohy doménového řadiče (politiky, účty apod.) pro případ, že bude potřeba provést obnovu celé domény.
- Ověřujte čitelnost a obnovitelnost zálohovaných dat.
- Mějte 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

Přestože segmentace sítě většinou není vnímána jako bezpečnostní opatření, z pohledu současných útoků dokáže správně nakonfigurovaná segmentace zkomplikovat rozšíření malware po síti vaší organizace. Bezpochyby tak mezi základní bezpečnostní opatření patří.

Segmentovaná síť je opakem tzv. „ploché“ sítě. Ta je nevhodnějším prostředím pro šíření malware, přičemž se v ní nachází všechna zařízení (koncové stanice, servery, tiskárny, BYOD) ve stejném segmentu a mohou mezi sebou napřímo komunikovat.

Rozdělení vaší sítě do více segmentů představuje pouze první krok. Až následné řízení přístupu do jednotlivých segmentů je to, co ztěžuje fungování a brání rozšíření malware.

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:

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

3.2 Aktualizace

Udržujte všechny aplikace i operační systém aktuální. Staré nebo zranitelné verze bývají často 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 viz další kapitola.

Velmi důležité jsou aktualizace antivirových řešení a jejich databází. V jejich případě nejlepší možnost představuje nastavení automatické 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 nebo útoku hrubou silou.

Ponechte otevřené pouze ty služby, které jsou nutné pro chod vaší organizace.

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

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

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, proto věnujte patřičnou pozornost pravidelnému školení zaměstnanců. Dbejte na to, aby dodržovali základní kyberbezpečnostní hygienu.

Je nesmírně důležité používat pro různé služby různá hesla. Ať už se jedná o heslo k zálohám, online službám (např. 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 je dle vyhlášky 82/2018, §19 alespoň 12 znaků pro uživatele a 17 znaků pro administrátory. Volte hesla se zvýšenou složitostí, kombinujte různé druhy znaků, neodvozujte je z jiných hesel, jmen, dat narození apod. Tyto nároky jsou přirozeně náročné na lidskou paměť, můžete proto pro jejich zapamatování použít tzv. password manager (např. Keepass) s využitím jednoho hlavního superhesla.

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) mu přidělte pouze běžná práva. Základní úkony by pak v žádném případě neměli provádět s administrátorskými právy. To samé platí pro doménového administrátora – tento účet by nikdy neměl provádět běžnou činnost, ani samotné přihlašování se na klientské stanice nebo jiné servery. Tento účet používejte pouze pro správu domény, k žádným jiným činnostem.

Pokud se útočníkovi podaří získat přístup k účtu doménového administrátora, např. právě během jeho použití při běžné činnosti, 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 jejich podepisování. Technicky pak vynuťte spuštění pouze podepsaných maker nebo alespoň poučte uživatele, že se v dokumentech povolují jen pokud jsou si zcela jisti původem a účelem dokumentu.

Přílohy e-mailů 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 e-mail, 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. Je třeba také jasně definovat autoritu, na kterou tato hlášení mají být směřována.

3.7 Logy

Pro efektivní reakci na incidenty jsou důležité tzv. logy, jež je potřeba bezpečně ukládat. V případě incidentu představují důležitý zdroj informací a pomáhají odhalit mj. i stupeň rozšíření nákazy.

Nejlepší možností je ukládat logy na jiný stroj, než ze kterého pochází, ideálně mimo doménu, tedy využít log management. V případě napadení některé stanice se útočník může po sobě pokusit smazat logy a stopy z napadeného operačního systému. Pokud se tyto informace nachází zkopírované na jiném, nezávislém serveru, budou při vyšetřování dostupné. Zároveň je důležité 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:

povolte 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

Regulované subjekty mají na základě Vyhlášky 82/2018 sb. o kybernetické bezpečnosti §22 (bod 3, 4) definovanou dobu uchování logů minimálně 12 nebo 18 měsíců, dle druhu regulovaného subjektu. Tuto dobu však doporučujeme všem správcům. 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 využívejte prostředky detekující anomální chování a podezřelou komunikaci, například síťovou sondu, SIEM, Proxy, Centrální Antivirové řešení, Firewall logy.

3.9 Krizový plán

Pro případ, že selžou všechna opatření a vaše síť a systémy budou napadeny ransomwarem, doporučujeme mít vytvořený krizový plán, který aktivujete. Jeho součástí by měl být nejen postup reakce na úspěšný ransomwarový útok a obnovu systémů (**Disaster Recovery Plan**), ale pozornost věnujte i minimalizaci dopadů útoku na chod vaší organizace (**Business Continuity Plan)**. Potřeby každé instituce se mohou lišit, nicméně doporučujeme nastavit jasné 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 „offline procesů“. Disponujte dostatečnými zásobami psacích potřeb a papíru (také dejte zaměstnancům vědět, kde je najdou) nebo mějte k dispozici záložní počítače a další zařízení, která nebyla napojena na kompromitovanou síť.

Každá organizace by měla mít stanoveno alespoň následující:

- Plán obnovy obsahující zejména informace, které systémy budou obnovovány, stanoví priority, časové plány obnovy, odpovědné osoby, dodavatele vč. kontaktů apod., tedy konktrétně Disaster Recovery Plan, jenž bude obsahovat:
    - minimální úroveň poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního a komunikačního systému,
    - dobu obnovení chodu, během níž má být po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního a komunikačního systému,
    - dobu obnovení dat jako časového období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání systému.
- Plán komunikace pokrývající alespoň následující:
    - kdo s kým a co bude komunikovat, zejména kdo komunikaci řídí, vede a 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. Měl by obsahovat např.:
    - krizová opatření a organizační pokyny pro udržení chodu organizace i v případě rozsáhlého kybernetického incidentu,
    - pokyny pro zaměstnance v případě krizové situace včetně alokace lidí, nástrojů a dalších zdrojů.

Každý plán by měl zahrnovat seznam odpovědných osob 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. Ideální je také plány průběžně aplikovat, zkoušet jejich reálnost a proveditelnost, např. při cvičeních.

4 Reakce na ransomwarový útok

Dále naleznete seznam úkonů, jež je potřeba vykonat po zjištění ransomware útoku na vaši organizaci. V případě incidentu jej lze následovat a umožnit tak efektivnější řešení problému.

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). Po kompromitaci mohou aktéři monitorovat aktivitu nebo komunikaci vaší organizace, aby zjistili, zda byly jejich akce provedeny. Ujistěte se, že jste systémy koordinovaným způsobem izolovali a pro komunikaci používáte metody mimo kompromitovanou síť, jako jsou telefonní hovory nebo jiné prostředky. Nechcete aktéry nijak upozornit, že byli odhaleni a jsou přijímána bezpečnostní opatření (tento bod dává smysl, pokud útočníka odhalíte před destruktivními/šifrovacími aktivitami).
- Zařízení v síti odpojte na síťové úrovni. Pouze v případě, že tak nelze učinit, vypněte je, abyste zabránili dalšímu šíření infekce ransomware. Zabráníte tak zničení potenciálních důkazů uložených v dočasné paměti.
- Odpojte komunikaci do veřejné sítě.
- Zjistěte rozsah napadení a infikované systémy izolujte.
- Dokumentujte zjištění.
- Pokud je to možné, pozastavte virtuální stroje, jinak pořiďte snapshot a vypněte je.
- Pořiďte bitovou kopii zasažených systémů a zařízení (např. pracovních stanic a serverů). Kromě toho shromážděte všechny relevantní logy, vzorky jakýchkoli binárních souborů malwaru a indikátory kompromitace (např. podezřelé IP adresy a položky registrů, spuštěné příkazy nebo jiné zjištěné relevantní soubory).
- Aby se zabránilo ztrátě dočasných důkazů nebo manipulaci s nimi, dbejte na jejich uchování. Týká se to např. systémové paměti, protokolu Zabezpečení Windows a dat ve vyrovnávacích pamětech protokolu brány firewall.
- Kontaktujte manažera kybernetické bezpečnosti (MKB), vedení vaší organizace, NÚKIB a Policii ČR.
- Požádejte o logy ze sondy/firewallu od poskytovatele internetu.

4.2 Další doporučení

- Vytvořte seznam klíčových osob 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.
- Pokud je požadováno výkupné, neplaťte jej.

- V případě napadení ransomwarem jsou organizace vystaveny silnému tlaku veřejnosti i útočníka, který organizaci může vydírat samotnými ukradenými daty, případně jejich zveřejněním, utlačováním zákazníků organizace nebo situaci vyostří DDoS útoky na stále funkční část infrastruktury. Oběti útoku proto mohou být nakloněni zaplacení výkupného. NÚKIB i Světová bezpečnostní komunita se ovšem shodují, že by výkupné nemělo být za žádných okolností placeno, jelikož:
    1. zaplacení utvrdí útočníka v ziskovosti jeho jednání a motivuje jej k dalším útokům,
    2. neexistuje záruka, že útočník data skutečně odblokuje, nebo smaže (v případě odcizení),
    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.
- Zajistěte dostatečně velkou místnost pro analytiky, dodavatele a další zúčastněné, ideálně vybavenou tabulemi (whiteboard, flipchart), občerstvením (jídlo a pití), případně zjistěte/zajistěte nejbližší ubytování.
- Pro rychlejší a efektivnější komunikaci připravte jmenovky pro každého, kdo se bude účastnit obnovy.

4.4 Postup při obnově dat/sítě

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

5 Časté dotazy

Může ransomware ukrást vaše data?

Ano. Některé typy ransomwaru mohou před zašifrováním souborů ukrást všechna osobní data, která se na napadeném počítači nachází.

Může antivirus opravit ransomware?

Ne. Antivirus může zabránit mnoha typům ransomwaru ve spuštění, nedokáže ale zašifrované soubory opravovat. Antivirové programy se ovšem vyvíjejí, aby hrozbu překonaly.

Může resetování počítače odstranit ransomware?

Záleží na typu ransomware, obecně lze ale říct, že pouhý restart vás ransomware nezbaví, pouze přeruší šifrování souborů, ale po opětovném zapnutí počítače se spustí znovu. Většina ransomwarů totiž využívá funkcionalit operačního systému, které je ochrání před restartem zařízení a opětovně je po načtení operačního systému automaticky spustí.

Může se ransomware šířit přes Wi-Fi?

Ano. Ransomware se může pohybovat přes Wi-Fi sítě a infikovat počítače. Technologie Wi-Fi nemá žádnou přidanou ochranu oproti komunikaci po kabelu, proto je ideální omezit nepoužívané služby např. pomocí firewallu případně nějakého jiného omezení. Nejdůležitější a nejúčinnější obrana však spočívá v offline zálohách svých dat.

Mohou hackeři prolomit VPN?

Prolomení šifrování u služeb VPN ze strany útočníka není pravděpodobné. Většina prémiových VPN používá šifrované protokoly, které je téměř nemožné dešifrovat pomocí útoků hrubou silou.

Můžete zakázat ransomware?

Škodlivé soubory můžete odstranit ručně nebo automaticky pomocí antivirového softwaru. Ruční odstranění se doporučuje pouze počítačově zdatným uživatelům. Pokud je váš počítač infikován ransomwarem, který šifruje vaše data, budete k opětovnému získání přístupu potřebovat vhodný dešifrovací nástroj.

Zastaví VPN ransomware?

VPN nemůže zastavit ransomware.

Odstraní tovární nastavení ransomware?

Obnovení zařízení do továrního nastavení je možné, pokud ransomware neodstranil nebo nepoškodil tyto zálohy. Většina z nich totiž před započetím šifrování tyto zálohy odstraní. Současně je potřeba myslet i na to, že uvedením zařízení do továrního nastavení přijdeme bez provedení zálohy o všechna osobní data.

Tovární nastavení dává uživatelům šanci začít znovu s čistým štítem. Podniky, které spravují svá zařízení Windows pomocí Microsoft Endpoint Manager (MEM), mohou jednoduše resetovat zařízení a nechat MEM automaticky znovu nainstalovat aplikace, čímž se počítač okamžitě vrátí do plného produkčního režimu. Jelikož je resetování zařízení dnes takto snadné, zůstává otázkou, zda obnovení továrního nastavení skutečně zařízení před ransomwarem ochrání.

6 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 – doporučení pro personál nemocnic, https://nukib.cz/download/publikace/doporuceni/Doporuceni_spear_phishing_pro_personal_nemocnic_modre.pdf
- CISA, 2023, https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

7 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

8 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách https://www.nukib.cz/cs/infoservis/doporuceni/1862-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci-2/). 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+STRICT	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
Oranžová TLP: AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
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
24.4.2023	1.2	NÚKIB, AFCEA	Zapracování doporučení k problematice od CISA, přidání kapitoly nejčastější dotazy, Aktualizace TLP protokolu