Jak se bránit ransomware – základní bezpečnostní opatření a doporučení

Autor dokumentu	Dominik Marek, marek.dominik@kr-vysocina.cz
Verze	1.0 – nový dokument
Datum vydání verze	1. 6. 2018
Cílová skupina	Správci ICT
Účel	Definice základních bezpečnostních opatření pro prevenci a detekci ransomware
Ověřil/schválil	Dominik Marek

Obsah

1. Úvod 2
2. Bezpečnostní opatření a doporučení 2
   Zálohování 2
   Bezpečnost klienta 3
   Bezpečnost serveru (sítě) 4
3. Závěr 7

Revize	Strana	Změna	Odkaz

1. Úvod

Ransomware je škodlivý kód, který na cílovém systému šifruje uživatelská či systémová data a požaduje po oběti, aby zaplatila výkupné. Útočníci slibují po zaplacení výkupného poskytnout nástroj na dešifrování dat.

Níže jsou uvedena základní technická bezpečnostní opatření, doporučení a metody detekce, které by měly pomoci snížit riziko nákazy pomocí ransomware či snížit dopady při infekci.

2. Bezpečnostní opatření a doporučení

Zálohování

- Pravidelné zálohování – data by měla být pravidelně zálohována.
- Ochrana záloh – zálohy musí být adekvátně chráněny, aby také nedošlo k jejich zašifrování.
    - Oddělení záloh od provozních systémů
        - Zálohovací server/zařízení slouží pouze pro zálohy, pro nic jiného
    - Provádění offline nebo read-only záloh
    - Provádění tzv. archivace – nespoléhat se pouze na provozní zálohy, ale provádět nepřepsatelnou archivaci vybraných důležitých dat (např. pomocí optických disků či nějaké cloudové služby)
    - Pozn.: ransomware je natolik sofistikovaný, že dokáže najít připojené síťové disky, není tedy vhodné mít médium pro zálohování on-line v provozu
    - Oddělení oprávnění/účtů, které slouží pro provoz a pro správu záloh. Provozním administrátorským účtem (DOMAIN\Administrator či jiný provozní privilegovaný účet) by nemělo být možné přistupovat k zálohám
- Kvalitní testování obnovy záloh – schopnost obnovit zálohy by měla být kvalitně a pravidelně testována, aby nedošlo k situaci, že zálohovaná data nebude možné obnovit
- Model zálohování 3-2-1 – nasadit zálohovací model: minimálně 3 kopie záloh na 2 typech médií (např. 2x HDD, 1x páska) a 1 kopie dat mimo geografické úložiště organizace
    - Výše zmíněná zásada archivace není zahrnuta v tomto modelu, měla by stát vedle samotného zálohování

Bezpečnost klienta

- Endpoint security
    - Aktuální a funkční antivirový program je základ ochrany klienta.
    - Ransomfree od společnosti Cybereason (https://ransomfree.cybereason.com/)
        - Jedná se o klientskou aplikaci, která detekuje činnost ransomware a zabraňuje v jejím pokračování. Aplikace ve své klientské neplacené verzi nemá možnost centrální správy (jako např. deployment či aktualizace), ale v menších organizacích by mohla být bez problémů nasazena.
- Patch management
    - Bezpečnostní aktualizace instalovat neprodleně a minimalizovat tak riziko samovolného šíření některých typů ransomware.
- Zvyšování povědomí uživatelů
    - Školit uživatele, nabádat k obezřetnosti při otevírání souborů a upozorňovat na nestandardní hlášení a požadavky aplikací (různá vyskakovací okna s požadavky na spuštění nějakého obsahu či připojení k URL).
- Zobrazení známých typů přípon souborů
    - Průzkumník Windows by měl být nastavený tak, aby byly zobrazeny přípony souborů.
    - Spojit se vzděláváním uživatelů ohledně typů souborů a jejich chování.
- Pro soubory .js(e) a .vbs nastavit výchozí program pro spouštění na poznámkový blok
    - Běžný uživatel nepotřebuje tyto soubory většinou spouštět, vývojář (či zaměstnanec IT) si dokáže systém přenastavit sám nebo dočasně spustit pomocí jiného programu.
- Zakázat spouštění aplikací z %TEMP% (případně z %APPDATA%, ale nutno otestovat, jestli není potřeba)
    - GPO se nastavuje zde:
        - Group Policy Management > GPO > Computer Configuration > Windows settings > Security Settings > Software Restriction Policies
    - Příklady způsobu nastavení např. zde:
        - https://blog.brankovucinec.com/2014/10/24/use-software-restriction-policies-to-block-viruses-and-malware/

        - http://thesolving.com/server-room/how-to-software-restriction-policy-for-ad-domain-users/
        - http://www.itingredients.com/how-to-deploy-software-restriction-policy-gpo/

- Na klientovi nepracovat pod privilegovaným účtem
    - Oddělit běžný uživatelský účet od privilegovaného účtu na pracovní stanici.
- V MS Office dokumentech povolit pouze podepsaná makra nebo zakázat makra celkově
    - https://blogs.technet.microsoft.com/diana_tudor/2014/12/02/microsoft-project-how-to-control-macro-settings-using-registry-keys/
    - Nevýhoda: bohužel, většinou ani legitimní (potřebná) makra v MS Office dokumentech nebývají el. podepsaná.
- V PDF prohlížeči vypnout spouštění javascriptu
    - [HKCU\Software\Adobe\<product name>\<version>\JSPrefs]
      "bEnableJS"=dword:00000000
    - Toto nastavení se chová jako v MS Office dokumentech nastavení maker - uživatelsky lze toto nastavení změnit.

Bezpečnost serveru (sítě)

- Ochrana
    - Oprávnění pro operaci write do sdíleného adresáře na file serveru přidělovat pouze těm, kteří to opravdu potřebují.
    - Patch management
        - Instalovat bezpečnostní aktualizace neprodleně a minimalizovat tak riziko samovolného šíření některých typů ransomware.
    - Zabezpečení vzdáleného připojení
        - RDP
            - Používat RDP over SSL/TLS
            - Zakázat připojení k RDP z WAN, omezit pouze na LAN
            - Pro připojení do LAN používat VPN (ideálně ne MS VPN RAS)
            - Omezit zdrojovou adresu, ze které je možné se k RDP přihlásit

- Zapnout logování nejen úspěšného přihlášení, ale i neúspěšných pokusů o přihlášení na cílovém stroji
- Nastavit RDP tak, aby naslouchal na jiném než standardním portu č. 3389.
- Na server nasadit aplikaci typu fail2ban, která zabraňuje brute-force či slovníkovým útokům na RDP

▪ SSH

- Zakázat přihlášení uživatele root přes SSH
- Používat RSA autentizaci (RSA klíče se silnou passphrase)
- Omezit zdrojovou adresu, ze které je možné se přihlásit k SSH
  - Např. pomocí iptables nebo tcp wrappers
- Zakázat X11 forwarding
- Na server nasadit aplikaci typu fail2ban, která zabraňuje brute-force či slovníkovým útokům na SSH

▪ WMI

- Zakázat vzdálené připojení přes WMI z prostředí Internetu

o Privilegované účty

▪ Nastavit kvalitní heslovou politiku

▪ Nastavit rozumnou lock-out politiku pro zamykání účtů

▪ Nepoužívat implicitní účet Administrator.

- Vytvořit jiného privilegovaného uživatele s odlišným jménem pro správu.

▪ Privilegovaný účet (např. lokální administrátor) nepoužívat pro běžnou práci na pracovní stanici.

o PowerShell

▪ Zabezpečit spouštění powershellových skriptů

- Prezentace zabývající se obecnějším zabezpečením PowerShell s podrobnými komentáři ke stažení - https://blogs.msdn.microsoft.com/powershell/2013/12/16/powershell-security-best-practices/

        - Nastavení execution policy pomocí GPO - https://blogs.technet.microsoft.com/poshchap/2015/01/02/execution-policy-and-group-policy/

    - Privilegovaný účet (např. lokální administrátor) nepoužívat pro běžnou práci na pracovní stanici.
    -

- Detekce
    - Filescreening pomocí FSRM - služba MS Windows File Serveru File Server Resource Manager (automatická detekce)
        - Jedná se o filtrování souborů dle jejich názvu a typu (na file server nelze uložit soubory, které jsou vydefinované v zakázaných skupinách).
        - Př.: šifrovací virus Locky se bude snažit uložit na file server zašifrované soubory *.locky, FSRM mechanizmus tuto akci nepovolí a notifikuje odpovědnou osobu o porušení tohoto pravidla.
        - V příloze jsou uvedeny přípony nejčastějších typů ransomware.
    - Honeypot na úrovni file serveru (automatická detekce)
        - Detekce je založena na principu hlídání integrity souborů, které slouží jako návnada pro škodlivý kód.
        - Falešné soubory
            - Jde o vytvoření jednoúčelového síťového disku a jeho namapování všem uživatelům (označení svazku písmenem co nejblíže k písmenu A).
            - Tento síťový disk bude obsahovat falešné soubory (reálné soubory se smyšleným obsahem) různých typů (např. doc(x), xls(x), pdf, txt, mdb, cer, jpg, apod.).
        - Integrita těchto souborů by se neměla měnit, protože jde o falešné soubory, které by nikdo neměl měnit (v podstatě ani otevírat).
        - Nástroj pro hlídání integrity - např. File Checksum Integrity Verifier (resp. script používající tento nástroj).
        - Nevýhoda: u MS Office souborů se změní jejich integrita pouhým jejich otevřením, zvědaví uživatelé tak generují false positive.
            - Řešení - přijmout false positive nebo seznámit uživatele.

        - V příloze je uveden příklad konfigurace honeypotu a nástroje pro hlídání integrity.
    - Ruční kontrola zašifrovaných souborů na file serveru:
        - Výčet všech typů souborů v adresářích (rekurzivně):
            - Get-Childitem C:\MyDirectory -Recurse | WHERE { -NOT $_.PSIsContainer } | Group Extension -NoElement | Sort Count -Desc > FileExtensions.txt
        - Lze využít pro ruční kontrolu, zda neexistují na serveru již zašifrované soubory
    - V případě inkrementální/rozdílové zálohy - velký nárůst velikosti zálohy oproti trendu
        - Lze detekovat pouze u jednoduchých systémů zálohování

3. Závěr

Několik poznámek na závěr:

- I pravidelné a zabezpečené zálohy nám nepomohou, pokud nejsme schopni detekovat činnost ransomware v našem prostředí. Hrozí totiž situace, kdy dojde k retenci záloh a budou přepsané již zašifrovanými daty.
- Ransomware již necílí pouze na uživatelská data, ale šifruje i systémové soubory a útočí tak na dostupnost či použitelnost služeb, systémů či infrastruktury.
- Existují úspěšně provedené útoky (stále „in-the-wild“), prostřednictvím kterých byl instalován ransomware na citlivé systémy bez interakce uživatele.

Příloha č. 1 – Nejčastější typy souborů používaných ransomware

Masky přípon souborů, které používá známý ransomware, lze automatiky naimportovat do připravené skupiny souborů FSRM pomocí power shell příkazu. Přípony je potřeba překopírovat do samostatného souboru (např. .csv). Pro import stačí spustit tento příkaz:

Set-FsrmFileGroup -Name "name_of_groupt" -IncludePattern (Get-Content -Path "path_to_file.csv")

!satana!.*
*.0x0
*.1999
*.73i87A
*.777
*.7h9r
*.8lock8
*.AFD
*.CCCRRRPPP
*.CRRRT
*.CRYPTENDBLACKDC
*.CRYPTOSHIELD
*.CTB2
*.CrySiS
.CryptoTorLocker
*.EnCiPhErEd
*.FuckYourData
*.H3LL
*.HeroesOftheStorm
*.JUST
*.KEYH0LES
*.KEYZ
*.LOL!
*.LeChiffre
*.MKJL
*.OMG!
*.PoAr2w
*.PzZs
*.R4A
*.R5A
*.RAD
*.RADAMANT
*.RDM
*.RRK
*.RSNSlocked
*.Rsplited
*.SUPERCRYPT
.Sarah_G@ausicom
*.SecureCrypted
*.Silent
*.Where_my_files
*.XRNT
*.Z81928819
*.abc
*.aesir
*.aga
*.amba
*.bart
*.better_call_saul
*.bitstak
*.bleep
*.bleepYourFiles
*.bloc
*.blocatto

*.btc
*.btc-help-you
*.btcbtcbtc
*.cbf
*.ccc
*.cerber
*.cerber3
*.chifrator@qq_com
*.clf
*.code
*.coverton
*.crime
*.crinf
*.criptiko
*.criptoko
*.criptokod
*.cripttt
*.crjoker
*.crptrgr
*.cry
*.cryp1
*.crypt
*.crypt38
*.crypted
*.crypto
*.cryptolocker
*.cryptz
*.crypz
*.ctbl
*.czvxce
*.da_vinci_code
*.darkness
*.ded
*.diablo6
*.dxxd
*.dyatel@qq_com_ryp
*.ecc
*.enc
*.encedRSA
*.encrypt
*.encrypted
*.encryptedAES
*.encryptedRSA
*.enigma
*.epic
*.evillock
*.exx
*.ezz
*.fileiscryptedhard
*.frtrss
*.fuck
*.fucked
*.fun
*.good
*.gruzin@qq_com
*.gws
*.ha3
*.helpdecrypt@ukr
*.herbst
*.infected
*.isis
*.iwanthelpuuu
*.justbtcwillhelpyou
*.keybtc@inbox_com
*.kimcilware

*.kk
*.kkk
*.korrektor
*.kraken
*.kratos
*.locked
*.locky
*.magic
*.micro
*.nalog@qq_com
*.net
*.nochance
*.nuclear
*.odcodc
*.odin
*.only-we_can-help_you
*.oor
*.oplata@qq_com
*.oshit
*.ozyzig
*.p5tkjw
*.padcrypt
*.paybtcs
*.payms
*.paymst
*.payransom
*.pizda@qq_com
*.porno
*.protect
*.pzdc
*.rapid
*.relock@qq_com
*.remind
*.rokku
*.sanction
*.scl
*.se
*.sport
*.stn
*.surprise
*.szf
*.thor
*.toxcrypt
*.troyancoder@qq_com
*.trun
*.ttt
*.tzu
*.unavailable
*.vault
*.vscrypt
*.vvv
*.wcry
*.wflx
*.windows10
*.work
*.xort
*.xrtn
*.xtbl
*.xxx
*.xyz
*.ykcol
*.zcrypt
*.zepto
*.zyklon
*.zzz

.~HL
*.已加密
*_luck
.Xcri

Příloha č. 2 – Příklad konfigurace honeypotu

- Je vytvořen share s různými falešnými soubory a je namapován uživatelů jako síťový disk (co nejblíže písmenu A, ideálně před všechny ostatní namapované disky)
- Na file serveru je adresář C:\FCIV s tímto obsahem:
    - Stažený a rozbalený nástroj FCIV.exe (http://download.microsoft.com/download/c/f/4/cf454ae0-a4bb-4123-8333-a1b6737712f7/windows-kb841290-x86-enu.exe)
    - Vytvořený XML soubor, který obsahuje vypočítané hashe všech falešných souborů na vytvořeném sharu. Proti tomuto souboru se kontroluje integrita falešných souborů.
        - Vytvoření XML souboru lze provést tímto příkazem:
            - *fciv.exe FilesToCheck -r -md5 -xml db.xml*
    - Adresář fciv_log v případě použití skriptu pro automatickou kontrolu integrity. Skript ukládá do tohoto adresáře své logy.
- Popis skriptu:
    - Obecně:
        - Skript používá nástroj fciv.exe, pomocí kterého se kontroluje integrita vybraných souborů oproti vygenerované XML databázi souborů.
        - Skript lze spouštět různými způsoby – např. pomocí naplánovaných úloh v časových intervalech nebo pomocí jiného nástroje (např. nástroj SIEM dokáže spouštět skript v případě, že se v logách file serveru objeví, že bylo přistupováno (read nebo write) k adresáři, kde jsou hlídané soubory umístěny).
    - Příklad obsahu skriptu:

```
@echo off
SET filename=%date%-%time%
SET filename=%filename: =%
SET filename=%filename:.=_%
SET filename=%filename::=_%
SET filename=%filename:/=_%

cmd /C "c:\FCIV\fciv.exe -v g:\share_name\ -xml c:\FCIV\db.xml > c:\FCIV\fciv_log\%filename%.txt"
IF EXIST c:\FCIV\fciv_log\%filename%.txt (for /f "delims=" %%i in ('FIND /C "All files verified successfully" c:\FCIV\fciv_log\%filename%.txt') do set result=%%i) ELSE (CALL :notify_error)
SET _result=%result:~-1%
IF %_result% lss 1 (CALL :notify_warning) ELSE (CALL :notify_information)
GOTO :eof

:notify_error
ECHO File %filename%.txt does not exist!>>c:\FCIV\fciv_log\errors.log
EXIT /B
```

```
:notify_information
eventcreate /ID 999 /L APPLICATION /T INFORMATION  /SO FCIV_SCRIPT /D "Everything should by OK."
ECHO %filename% not changed!>>c:\FCIV\fciv_log\ok.log
EXIT /B

:notify_warning
eventcreate /ID 999 /L APPLICATION /T WARNING  /SO FCIV_SCRIPT /D "Files changed! Look at c:\FCIV\fciv_log\%filename%.txt"
ECHO %filename% - found changed files!>>c:\FCIV\fciv_log\modified.log
EXIT /B
```

- Tento skript ukládá výsledky jak do jednoduchého textového logu, tak do aplikačních událostí (Event Viewer>Windows logs>Applications).