Jak se bránit ransomware/malware – základní bezpečnostní opatření a doporučení

Autor dokumentu	Dominik Marek, marek.dominik@kr-vysocina.cz
Verze	1.1
Datum vydání verze	1. 9. 2020
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
1.1		Aktualizace opatření	

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 nejen pomocí ransomware, ale obecně malware jako takového, 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
        - Je vhodné zálohovací server oddělit i síťově a přístup řídit rovněž pomocí FW
    - 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 běžný provoz a pro správu záloh. Pro přístup k zálohám a jejich správu by měl sloužit samostatný - dedikovaný - účet, kterým se nelze hlásit jinde než na backup infrastruktuře.
- 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.
- 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), [.]vbs a [.]iqy 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 je možné)
    - GPO se nastavuje zde:
        - Group Policy Management > GPO > Computer Configuration > Windows settings > Security Settings > Software Restriction Policies
    - Příklady způsobu nastavení např. zde:
        - 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 (a sítě)

- Ochrana
    - Servery
        - Omezit oprávnění pro operaci write do sdílených adresářů na (file) serveru.
            - Vyvarovat se např. write oprávnění pro skupinu Everyone.
        - 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
            - https://rdpguard.com/
            - https://github.com/glasnt/wail2ban
            - https://github.com/DigitalRuby/IPBan
    - 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
            - https://www.fail2ban.org/
    - WMI
        - Zakázat vzdálené připojení přes WMI z prostředí Internetu
- 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.
    - Používat pojmenované privilegované účty na osobu.
        - Nepoužívat sdílené admin účty pro běžnou správu.
    - Privilegovaný účet (např. lokální administrátor) nepoužívat pro běžnou práci na pracovní stanici.
    - Zavést tierový model správy

        - rozdělit IT do 3 vrstev a do každé vrstvy se hlásit dedikovaným účtem pro danou vrstvu /např. domain admins mají práva přihlášení pouze na doménové kontrolery, server admins pouze na member servery a Workstation admins pouze na pracovní stanice/).

    - PowerShell

        - Zabezpečit spouštění powershellových skriptů

            - Informace a prezentace zabývající se obecnějším zabezpečením PowerShell s podrobnými komentáři ke stažení - https://docs.microsoft.com/cs-cz/mem/configmgr/apps/deploy-use/learn-script-security

            - 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.

- Sítě

    - Segmentovat síť a řídit přístupy mezi jednotlivými segmenty

        - Segmenty oddělovat jak na základě důvěryhodnosti zón, tak na základě logického členění prvků v nich obsažených

    - Oddělit WIFI síť pro veřejnost od LAN, od WIFI sítě pro zaměstnance a případně jiných segmentů

    - Oddělit segment infrastruktury/managementu od segmentu běžných uživatelů, zamezit přístupu z uživatelského segmentu

- Detekce

    - Filescreening pomocí FSRM - služba MS Windows File Serveru s názvem 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.

    - 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 (aby nedošlo k zálohování zašifrovaných dat), např. při podezření z nákazy, apod.
        - Pozor, příkaz je celkem náročný na zdroje RAM!
    - 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 necílí pouze na uživatelská data, ale šifruje hlavně systémové soubory a útočí tak na dostupnost či použitelnost služeb, systémů či infrastruktury.
- Provedené útoky bez interakce uživatele, prostřednictvím kterých byl instalován ransomware na citlivé systémy, jsou běžné, nikoliv výjimečné.

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")

Přípony jsou uvedeny v samostatném souboru.