Ransomvér v infraštruktúre

Ako sa chrániť?

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CSIRT.SK

Hrozba preniknutia útočníkov do IT infraštruktúry organizácie zneužitím rôznych ciest je veľmi reálnym ohrozením chodu celej organizácie. Následná krádež a zašifrovanie dôležitých informácií a systémov môžu vyradiť služby a spôsobiť rozsiahle reputačné a finančné škody. V najhorších prípadoch môžu viesť ku ohrozeniu zdravia a životov, či fyzickým škodám. Zo skúseností Vládnej jednotky CSIRT s ransomvérovými incidentmi v poslednom období vyplýva, že ako najlepšia prevencia stále platia nasledujúce opatrenia.

Pred kompromitáciou

- Poznajte detailne topológiu svojej siete – neexistencia jej mapy sťažuje identifikáciu vektora útoku a pohybu útočníka v infraštruktúre. Vďaka mape siete tiež poznáte, ktoré jej prvky predstavujú najslabší článok.
- Majte vytvorené a pravidelne v praxi testované procesy pre zamedzenie šírenia a mitigáciu kybernetických bezpečnostných incidentov a obnovu služieb po incidente.
- Nastavte si upozornenia pri zaznamenaní mazania dôležitých logov. Útočníci sa tak niekedy snažia zabrániť odhaleniu a rekonštrukcii udalostí incidentu.
- Nastavte si upozornenia na prihlásenia administrátorských účtov, resp. účtov s vyššími oprávneniami do vašej infraštruktúry mimo pracovných hodín, resp. v časoch s nízkou pravdepodobnosťou legitímnych prihlásení a tiež z podozrivých IP adries (napr. zahraničie). Ideálne monitorujte takéto prihlásenia aj pre bežné účty.
- Zakážte nepoužívané kontá. Dôraz kladťe na kontá s vysokými oprávneniami (administratívne). Riešením je zavedenie riadenia prístupu a správa používateľov. Používateľské konto by malo v systéme existovať len kým je potrebné a používané. Nezabudnite na testovacie kontá.
- Pre získanie oprávnení typu root nastavte povinné zadanie hesla pre každého používateľa.
- Obmedzte oprávnenia účtov na minimálne potrebné, aby útočník v prípade prieniku nemohol vykonávať činnosti, ktoré dovoľujú iba vyššie oprávnenia.
- Aby ste znížili riziká útokov hrubou silou (brute force):
    - Používajte/vynúťte silné heslá pre všetky účty, vrátane testovacích. Minimálna odporúčaná dĺžka hesla je 16 znakov pri dodržaní jeho komplexnosti (postupovať môžete v zmysle štandardu NIST Special Publication 800-63B).
    - Na prístup k rôznym službám je vhodné používať rôzne heslá (s výnimkou Single-Sign-On). Použitie rôznych hesiel je potrebné pre prístupy k službám s rôznymi bezpečnostnými požiadavkami (security level).
    - Používajte správcov hesiel so šifrovanou databázou (napr. KeePass). Pre prístup k šifrovaným databázam hesiel používajte jedinečné a silné heslo. Zabezpečte zálohu databázy hesiel.

  - Implementujte v organizácii povinné používanie viacfaktorovej autentifikácie (MFA) pri prístupoch k dôležitým systémom a zariadeniam v sieti. Použitie komplikovaného hesla už dnes nie je dostatočnou ochranou. Pri uniknutí alebo odcudzení hesiel následne útočníkovi nebráni nič v procese autentifikácie voči danému systému a má voľnú cestu ku kompromitácii systému a ďalšej škodlivej činnosti v sieti.
  - Deaktivujte štandardné, testovacie, verejne známe (dokumentácia) a nepoužívané účty (admin, test a pod.).
  - Nastavte obmedzenia neúspešných pokusov o prihlásenie (rate-limiting) a dočasné alebo trvalé zamykanie účtov po ich vyčerpaní – aj pre pokusy o prihlásenie zvnútra siete (napríklad po kompromitácii).
- Nepoužívajte v konzole príkazy, ktoré obsahujú heslo. V prípade že nie je možné heslo zadať ináč ako priamo v príkaze, vymažte daný príkaz z histórie príkazového riadka.
- Nepoužívajte heslá v čitateľnej podobe v konfiguračných súboroch.
- Pre zabezpečenie vzdialeného prístupu k bežne používaným protokolom:
  - Nastavte upozornenia pri podozrivo vysokom množstve úspešných/neúspešných prihlásení cez protokoly ako RDP, SSH, SMB a podobne.
  - Monitorujte spojenia na SSH, RDP, SMB, ... Ideálne ich obmedzte na vybrané dôveryhodné IP adresy. Pre vyššiu ochranu použite pre vzdialený prístup VPN s multifaktorovou autentifikáciou.
  - Zakážte protokoly SSH, RDP, SMB, ... pokiaľ ich na danom zariadení nepotrebujete využívať.
  - Pre vzdialený administrátorský prístup používajte neprivilegované kontá. Až následne po prihlásení a ak je to potrebné, zvýšte svoje privilégiá (napr. „sudo“ spolu so zadaním hesla). Keď vaši zamestnanci používajú na prihlásenie cez SSH normálny používateľský účet a následne prejdú na root pomocou príkazu „sudo“, je možné efektívnejšie auditovať ich činnosť a logovať aktivity. Týmto spôsobom je oveľa jednoduchšie identifikovať, ktorý používateľ vykonal akciu ako root a zabezpečiť, že prístup je obmedzený len na skutočne oprávnených používateľov.
- Ak používate prostredie Office 365, zaveďte politiku podmieneného prístupu.
- Monitorujte dopyty protokolu HTTP/S, najmä typu POST, na podozrivé súbory vo Vašej infraštruktúre (možný webshell).
- Nastavte monitoring a upozornenia na odchádzajúce dáta z infraštruktúry pri stanovenom objeme a v stanovených časoch, prípadne do stanovených krajín podľa geoIP.
- Monitorujte neoprávnené spustenie nástrojov ako pkexec, Nmap, balík Sysinternals, AnyDesk, ScreenConnect, TeamViewer, prípadne PowerShell a príkazový riadok CMD (pre Linux Bash shell a pod.).
- Pokiaľ máte nasadený monitoring (SIEM a pod.) je nevyhnutné, aby ste mali dostupných zamestnancov, ktorí budú analyzovať výstupy. Nasadenie monitorovacej technológie bez aktívnej analýzy jej výstupov ľudským faktorom neumožní v reálnom čase reagovať na

prebiehajúce incidenty, a tým výrazne obmedzuje užitočnosť tejto technológie. Pri vyhodnotení ako tzv. „true positive“ musia byť pre rôzne typy varovaní stanovené postupy opatrení, ktoré je nutné bezodkladne vykonať vrátane prípadnej eskalácie na iné tímy alebo subjekty.

- Implementujte centrálne antimalvérové riešenie pre servery, resp. rozšírte existujúce riešenie o zariadenia poskytujúce sieťové služby (servery).
- Segmentujte svoju podnikovú sieť
    - Nedostatočná segmentácia siete zvyšuje pravdepodobnosť, že útočník kompromituje ďalšie zariadenia, keďže môže útočiť na akúkoľvek službu dostupnú v danej sieti.
    - Rozdeľte sieť do virtuálnych sietí (VLAN) podľa účelu a bezpečnostných požiadaviek. Zariadenia, ktoré majú služby dostupné z internetu, by nemali byť v rovnakej sieti ako lokálne servery. Segmenty siete by mali obsahovať iba zariadenia s rovnakou úrovňou zabezpečenia.
    - Nakonfigurujte sieťový firewall, ktorý filtruje komunikáciu medzi jednotlivými VLAN, podľa princípu najnižších nutných privilégií.
    - Pre správu infraštruktúry je vhodné implementovať Out-Of-Band manažment (OOBM).
    - Kdekoľvek je to možné, implementujte technológiu privátnych lokálnych sietí (private VLAN). Napríklad pre prípad manažmentu sieťových prvkov a manažmentu fyzických serverov.
    - Pri sieťových službách určených pre externých používateľov prijmite nutné bezpečnostné opatrenia – použite firewall a umiestnite servery do demilitarizovanej zóny.
- Vytvorte a implementujte do praxe proces zálohovania dát. Citlivé údaje zálohujte tiež offline, mimo infraštruktúru.
- Na pravidelnej báze overujte dostupnosť a obnoviteľnosť záloh.
- Opravujte bezpečnostné zraniteľnosti systémov a softvéru, ktoré používate vo svojej infraštruktúre. Útočník ich môže zneužiť pre prienik, ale aj po prieniku napr. na nahratie a aktiváciu webshellu.
- Pravidelne sa informujte o nových bezpečnostných zraniteľnostiach používaného softvéru a systémov.
- Vytvorte si a implementujte do praxe proces bezodkladnej aplikácie bezpečnostných aktualizácií/záplat.
- Prejdite na podporovanú verziu softvéru a hardvéru, pokiaľ niektoré prvky vašej infraštruktúry prešli do fázy „end-of-support“. Prvky s ukončenou podporou odstráňte z infraštruktúry, pretože sa stávajú závažným rizikom prieniku do systému.
- Pokiaľ využívate skener zraniteľností (službu Achilles od CSIRT.SK, a pod.), bezodkladne vykonajte potrebné opatrenia pri nájdení vážnych zraniteľností. Ak aktualizácia nie je dostupná alebo možná, mitigujte možný dopad zneužitia zraniteľnosti (vypnutie, zakázanie služby, mitigácia podľa odporúčaní výrobcu, zamedzenie prístupu z internetu, a pod.).

V priebehu incidentu

- Spustite proces pre zabránenie šírenia kybernetického bezpečnostného incidentu. Využite pritom existujúce prostriedky (firewall, ...).
- Pre zmiernenie dopadu odpojte od centrálnej časti všetky bočné vetvy a menej dôležité služby.
- Odpojte dotknuté zariadenia od internetu.
- Odpojte infraštruktúru od externým prepojov (partnerské organizácie, GOVNET) a bezodkladne informujte zainteresované organizácie pre prípad, že by sa infekcia stihla rozšíriť.
- Znefunkčnite certifikáty potrebné pre komunikáciu s dotknutými službami.

Po incidente

- Zasiahnuté zariadenia nevypínajte, ale odpojte od počítačovej siete, vrátane Wi-Fi. Ponechanie živých systémov umožní forenzným analytikom získať volatilné dáta (obsah pamäte RAM, otvorené relácie, a pod.), ktoré môžu pomôcť pri odhalení útočníka, no tiež pri obnove systémov.
- Nemanipulujte s napadnutými zariadeniami, aby analytici pri zaistení obrazov ich diskov získali tieto dáta bez nežiaducich zmien.
- V neposlednom rade si nezabudnite splniť legislatívnu povinnosť a nahláste incident jednotkám SK-CERT (NBÚ) a CSIRT.SK. Naši technici a analytici vám pomôžu v najťažších chvíľach.