ČO JE TO RANSOMVÉR A AKO SA CHRÁNIŤ?

TIPY/OPATRENIA PRED-POČAS-PO ZASIAHNUTÍ RANSOMVÉROM

Čo je to ransomvér?

Ide o slovný novotvar, ktorý vznikol spojením dvoch anglických slov: „ransom" a „software". Čo znamená „software", to už dnes vedia aj malé deti - slovo bolo už prevzaté aj do slovenského jazyka, píše sa tak, ako sa vyslovuje v angličtine: „softvér".

Výraz „ransom" znamená v angličtine výkupné. Výraz „ransomware" (po slovensky „ransomvér") vznikol príchodom nového typu škodlivého softvéru, ktorý vydiera používateľa o výkupné.

V prvom kroku útočníci na diaľku infikujú počítač a následne, pomocou tohto špeciálneho typu počítačového kódu, postupne zašifrujú alebo ukradnú dáta. Za ich vrátenie, sprístupnenie alebo nezverejnenie žiadajú, aby používateľ zaplatil.

Stratégia obrany proti ransomvéru

- ✓ Zaraďte ransomvér medzi vysoké riziká v katalógu hrozieb a rizík, vykonajte analýzu dopadov (BIA) a odhadnite možné finančné straty z výpadku vašej činnosti, straty údajov, zverejnenia údajov, nákladov na obnovu infraštruktúry a nákladov na nápravu poškodenej reputácie.
- ✓ Na úrovni najvyššieho vedenia organizácie prijmite zásadné strategické rozhodnutie neplatiť výkupné. Platenie výkupného nemusí zaručiť návrat a nezverejnenie dát, vôbec nezníži náklady na obnovu infraštruktúry a zároveň financuje skupiny, vykonávajúce trestnú činnosť.
- ✓ Zaveďte technické a organizačné bezpečnostné opatrenia.
- ✓ Zvážte možnosť poistenia proti kybernetickým rizikám, ak je také poistenie pre vás dostupné.

Pre dosiahnutie primeranej ochrany pred ransomvérom je potrebné venovať čas a finančné zdroje na zaručenie kybernetickej hygieny organizácie, na zvyšovanie bezpečnostného povedomia používateľov a na implementáciu preventívnych bezpečnostných opatrení.

Ako prebieha ransomvérový útok?

Pochopenie priebehu ransomvérového útoku môže poskytnúť štruktúrovaný spôsob, ako odhaliť, alebo zmariť útok v jeho skorších štádiách a ako je možné zabrániť útočníkom dosiahnuť ich cieľ. Keď už sú dáta zašifrované a útočníci požadujú výkupné, vaše možnosti riešenia sú obmedzené.

PRÍPRAVA

PRIESKUM

- *Aktívne skenovanie*
- *Analýza otvorených zdrojov*
- *Prehľadávanie neverejných informácií*

PRÍPRAVA PROSTRIEDKOV

- *Infraštruktúra (stránky skupiny na dark webe, phishingové stránky)*
- *Útočné nástroje*
- *Softvér na šifrovanie a exfiltráciu*

PRVOTNÝ ÚTOK

PRVOTNÝ PRÍSTUP

- *Phishing*
- *Útok na dodávateľský reťazec*
- *Zneužitie existujúceho účtu*
- *Verejne prístupná zraniteľná aplikácia*
- *Vzdialený prístup (RDP, TeamViewer, ...)*
- *Škodlivé aplikácie na stiahnutie*

VYKONANIE

- *Príkazový riadok*
- *API rozhranie*
- *Interakcia používateľa*

USADENIE

TRVÁCNOSŤ

- *Vytváranie účtov*
- *Manipulácia existujúcich účtov*
- *Využitie funkcie „autoštart"*

ESKALÁCIA PRIVILÉGIÍ

- *Zneužitie zraniteľnosti*
- *Manipulácia s prístupovými tokenmi*
- *Únik z obmedzeného prostredia (z virtualizácie, kontajnerov, ...)*

VYHNUTIE SA OBRANE

- *Vypnutie obrany (AV, logovania, firewallu, zmena doménových politík)*
- *Skrývanie artefaktov (skryté súbory, používatelia, partície), obfuskácia*
- *Rootkity*

ŠÍRENIE

ZÍSKANIE PRÍSTUPOV

- *Útok hrubou silou*
- *Man-in-the-middle útoky*
- *Výber hesiel z úložísk*
- *Zachytávanie sieťovej komunikácie*
- *Kradnutie tokenov a cookies*
- *Slabé a nezabezpečené heslá*

OBJAVOVANIE

- *Účty (AD/LDAP, mail, cloud ...)*
- *Zaujímavé súbory a adresáre*
- *Postupy a technológie zálohovania*
- *Záložky v prehliadačoch*
- *Aplikácie a sieťové spojenia*
- *Skupinové politiky, heslové politiky, ...*

POSTRANNÝ POHYB

- *Zraniteľné sieťové služby*
- *Vnútorný spear phishing*
- *RDP, SSH, VNC, zdieľaný disk*
- *Replikácia cez pamäťové médiá*
- *Prevzatie existujúcej otvorenej session*
- *Zneužitie nástrojov na správu siete*

DOSIAHNUTIE CIEĽOV

KRÁDEŽ ÚDAJOV

- *Dokumenty, tabuľky, súbory*
- *Duševné vlastníctvo*
- *Obchodné a finančné záznamy*
- *E-maily, kontakty, osobné údaje*
- *Kryptomeny a kryptopeňaženky*
- *Uložené heslá*

ŠIFROVANIE A ZNEHODNOTENIE

- *Zmazanie záloh*
- *Šifrovanie celých súborov alebo prvej časti súboru (väčšia rýchlosť útoku)*
- *Zmazanie súborov tak, aby ich nebolo možné obnoviť*

ZANECHANIE SPRÁVY

- *Súbor na ploche*
- *Oznam cez celú obrazovku*
- *Papier vytlačený z tlačiarne*

VYDIERANIE

- *Výkupné za odšifrovanie*
- *Výkupné za nezverejnenie*
- *Aukcia ukradnutých dát*
- *Vyhrážanie poškodením reputácie*
- *Výkupné za nenahlásenie autoritám*
- *Eskalácia požiadaviek počas komunikácie*

Plánovanie ochrany pred ransomvérom

- Stanovte hodnotu kritických informačných aktív organizácie.
- Navrhnite proces reakcie na kybernetické bezpečnostné incidenty, vrátane jasných pravidiel eskalácie informácií v rámci organizácie a pokynov pre vykonávanie internej komunikácie.
- Navrhnite a vopred schváľte pravidlá externej komunikácie, informovania médií a informovania tretích strán potenciálne dotknutých incidentom.
- Aktívne vyhľadávajte a získavajte informácie o hrozbách, zraniteľnostiach, technikách útočníkov a zapojte sa do technických platforiem na výmenu takýchto informácií.
- Navrhnite a schváľte plán kontinuity činností (BCP) a plán havarijnej obnovy prevádzky po kybernetickom bezpečnostnom incidente (DRP).
- Vopred identifikujte možných poskytovateľov služieb a dodávateľov, ktorí vám môžu pomôcť v skoršom zotavení sa po incidente.
- Vykonávajte overovanie účinnosti implementovaných bezpečnostných opatrení.
- Neustále pracujte na zvýšení vyspelosti procesov riadenia zraniteľností, hrozieb a rizík.

Pamätajte, že procesy riešenia incidentov majú vždy dva hlavné ciele:

1) Napraviť nežiaduci stav a obnoviť prevádzku (s cieľom pokračovať v štandardnej činnosti)

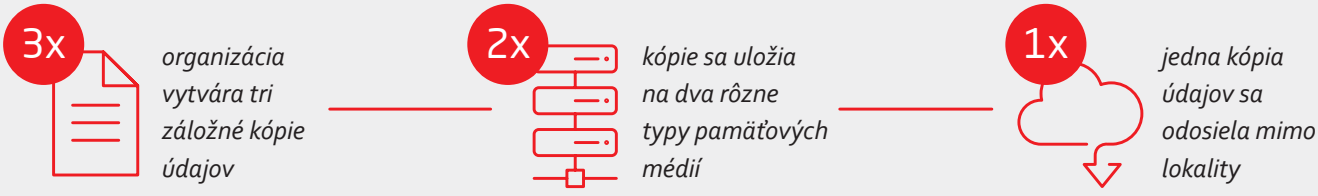
2) Získať digitálne stopy použiteľné v dôkaznom konaní (s cieľom vyšetriť incident a potrestať páchateľov)

Preventívne bezpečnostné opatrenia

- Obvyklou súčasťou ransomvérového útoku je škodlivý softvér (malvér). Zaveďte detekciu škodlivého kódu a anomálneho správania na pracovných staniciach a serveroch. Zabezpečte tiež, aby do skenovania možného výskytu malvéru boli zahrnuté všetky komunikačné kanály, vrátane zobrazovania obsahu webstránok, USB portov, e-mailu, protokolov na prenos súborov, služieb okamžitých správ, kanálov určených na výmenu údajov s tretími stranami atď.
- Zaveďte zásadu najnižších privilégií, podľa ktorej sú každému používateľovi obmedzené systémové právomoci iba na rozsah potrebný na splnenie pridelených úloh (Principle of least privilege).
- Zaveďte procesy manažmentu identít a prístupov a pravidelnú kontrolu prístupových účtov a oprávnení. Detegujte a následne trvalo blokujte nepoužívané prístupové účty.
- Zaveďte proces riadenia softvérových vydaní a zaveďte pravidlá pre inštaláciu softvéru. Softvér sťahujte a inštalujte iba z overených a povolených zdrojov.
- Zaveďte proces nasadzovania softvérových aktualizácií a záplat.
- Zaveďte proces zálohovania kritických údajov na základe pravidla 3-2-1. Pravidelne zálohujte kritické dáta a poznajte umiestnenie záloh kritických dát. Vykonávajte pravidelné preverenie záloh, testujte obnovu dát zo záloh a precvičujte zavedené plány kontinuity činností a plánov havarijnej obnovy. Do testovania BCP a DRP zapojte aj členov vedenia organizácie.
- Zálohovaciu infraštruktúru prevádzkujte úplne oddelene od produkčnej infraštruktúry (technológia, heslá).
- Implementujte segmentáciu počítačovej siete tak, aby sa informačné systémy so službami priamo prístupnými z externých sietí nachádzali v samostatných sieťových segmentoch a aby v rovnakom segmente boli umiestnené vždy iba informačné systémy s rovnakými bezpečnostnými požiadavkami, rovnakej kategórie a s podobným účelom.
- Vzdelávajte zamestnancov, neustále zvyšujte ich bezpečnostné povedomie.
- Interne, alebo prostredníctvom vopred zazmluvnených dodávateľov si zabezpečte spôsobilosť vykonať analýzu škodlivého kódu.

Zálohovanie 3-2-1 je rokmi overená metodika zálohovania a obnovy údajov, ktorou sa zabezpečí, že údaje sú primerane chránené a že v prípade potreby sú k dispozícii aktuálne záložné kópie údajov.

Koncept stratégie zálohovania 3-2-1:



Reakcia na incident

Ak už v organizácii zistíte prítomnosť ransomvéru, vykonajte prvotné kroky plánu reakcie na incident:

- ✓ Infikované koncové zariadenia umiestnite do karantény, čím zabránite laterálnemu šíreniu infekcie a izolujete ich na forenzné účely
- ✓ Ak plánujete vykonať právne kroky voči útočníkom, k tzv. neopakovateľným úkonom odporúčame prizvať súdneho znalca.
- ✓ V rámci aktivácie plánu reakcie na incident:
  a) transparentne, efektívne a bez paniky komunikujte so všetkými zainteresovanými stranami,
  b) bezodkladne zvolajte tím reakcie na bezpečnostné počítačové incidenty a informujte externé tímy CSIRT (ak ide o incident u prevádzkovateľa základnej služby, nezabudnite kontaktovať aj národnú jednotku CSIRT a SK-CERT),
  c) identifikujte potenciálny dopad incidentu,
  d) o incidente informujte vedenie organizácie,
  e) do riešenia incidentu zapojte právne oddelenie a ďalšie relevantné subjekty (napr. poisťovňu),
  f) informujte vašich zákazníkov a v prípade, že sa incident týka osobných údajov, informujte aj konkrétne dotknuté osoby,
  g) členom tímu reakcie na bezpečnostné incidenty umožnite nerušene vykonať všetky opatrenia potrebné na zotavenie z incidentu.

Zotavenie z incidentu

- ✓ Nepripájajte infikované koncové zariadenia k sieti. S ohľadom na možnú stratu volatilných dát ich nevypínajte.
- ✓ Detailne si premyslite nasledujúce kroky a celý proces obnovy tak, aby nemohlo dôjsť k poškodeniu zálohy dát.
- ✓ Vykonajte obnovu infraštruktúry, systémov a aplikácií z čistých, vopred pripravených bitových obrazov.
- ✓ Neplaťte výkupné za ransomvér. Ani zaplatenie výkupného vám totiž nezaručí, že svoje dáta získate naspäť.
- ✓ Využite existujúce znalosti na dešifrovanie škodlivého softvéru a obnovu dát. Pokiaľ nedisponujete potrebnými znalosťami, neváhajte k riešeniu prizvať expertov zvonka.
- ✓ Zaznamenávajte si všetky podrobnosti zistené počas obnovy (čas, odchýlky, zmeny atď.).

Post-incidentné aktivity

- ✓ Ak plánujete vykonať právne kroky voči útočníkom, objednajte si znalecký posudok od súdneho znalca. Zoznam znalcov nájdete na stránke Ministerstva spravodlivosti SR.
- ✓ Zapojte do ďalšieho riešenia incidentu oddelenie, ktoré (ak tak rozhodne vedenie organizácie) bude zodpovedné za ďalšie právne pokračovanie.
- ✓ Zapojte do ďalšieho riešenia incidentu právne oddelenie komunikácie a oddelenie zodpovedné za vzťahy so zákazníkmi.
- ✓ Venujte čas spoločnému preskúmaniu poznatkov získaných počas obnovy dát a zotavenia sa z incidentu s cieľom zlepšiť procesy reakcie na budúce incidenty.
- ✓ Ošetrite všetky zraniteľnosti, ktoré viedli alebo napomohli k vniknutiu ransomvéru.
- ✓ Implementujte dodatočné bezpečnostné opatrenia, a v prípade potreby zmeňte informačnú architektúru.
- ✓ Udržujte všetky záznamy, poznámky a artefakty pre potreby ďalšieho vyšetrovania.

Znalecké odvetvia relevantné pri riešení ransomvéru

- 10 10 00 Bezpečnosť a ochrana informačných systémov
- 10 11 00 Kybernetická bezpečnosť
- 10 02 00 Elektronika
- 10 04 00 Riadiaca technika, výpočtová technika (hardvér)
- 10 09 00 Počítačové programy (softvér)
- 49 20 00 Kriminalistická informatika

Spolufinancovaný Európskou úniou

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

SK CERT NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberajú žiadnu zodpovednosť.

ISBN 978-80-69011-33-5
Verzia V.1

www.cybercompetence.sk