

## 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.
- ✓ Ošetrte 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 04 00 Riadiaca technika, výpočtová technika (hardvér) |
|  10 11 00 Kybernetická bezpečnosť                    |  10 09 00 Počítačové programy (softvér)                   |
|  10 02 00 Elektronika                                |  49 20 00 Kriminalistická informatika                     |



## 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 neznižuje náklady na obnovu infraštruktúry a zároveň financuje skupiny, vykonávajúce trestnú činnosť.
- ✓ Zavedzte 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 zmať 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.



## Plánovanie ochrany pred ransomvérom

- ✓ Stanovte hodnotu kritických informačných aktív organizácie.
- ✓ Navrhňte proces reakcie na kybernetické bezpečnostné incidenty, vrátane jasných pravidiel eskalácie informácií v rámci organizácie a pokynov pre vykonávanie internej komunikácie.
- ✓ Navrhňte 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.
- ✓ Navrhňte a schváľte plán kontinuity činnosti (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 páchatelov)

## Preventívne bezpečnostné opatrenia

- ✓ Obvyklou súčasťou ransomvérového útoku je škodlivý softvér (malvér). Zavedte 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.
- ✓ Zavedte zásadu najnižších privilégii, podľa ktorej sú každému používateľovi obmedzené systémové právomoci iba na rozsah potrebný na splnenie pridelených úloh (Principle of least privilege).
- ✓ Zavedte procesy manažmentu identít a prístupov a pravidelnú kontrolu prístupových účtov a oprávnení. Detegujte a následne trvalo blokujte nepoužívané prístupové účty.
- ✓ Zavedte proces riadenia softvérových vydání a zavedte pravidlá pre inštaláciu softvéru. Softvér sťahujte a inštalujte iba z overených a povolených zdrojov.
- ✓ Zavedte proces nasadzovania softvérových aktualizácií a záplat.
- ✓ Zavedte 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 činnosti 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:

