IstroSec

Data Sheet

Reakcia na útok ransomvérom

V prípade, že Vaša organizácia bola zasiahnutá útokom typu ransomvér alebo iným typom útoku, je na minimalizáciu jeho dopadov kriticky dôležitá rýchla reakcia. Prosím kontaktujte nás 24/7 na čísle +421 917 699 002 alebo v pracovných hodinách na email incident@istrosec.com. Experti IstroSec Vám pomôžu s vykonaním reaktívnych aktivít na rýchle a efektívne vyriešenie tohto incidentu.

Reakcia na útok ransomvérom

- Prvotné posúdenie situácie
- Izolovanie ransomvéru (tzv. containment) na zabránenie jeho ďalšieho šírenia v organizácií
- Identifikácia konkrétnej vzorky ransomvéru a skupiny útočníkov, rozsahu útoku ako aj pomoc s analýzou nutnosti kontaktovať útočníka a prípadne zaplatiť výkupné
- Zaistenie digitálnych stôp pre potreby forenznej analýzy resp. pre potreby OČTK alebo poisťovní
- Bezpečnostný dohľad na DarkWebe na prítomnosť uniknutých dát
- Implementácia ochranných nástrojov do siete klienta a zabezpečenie bezpečnostného dohľadu počas trvania bezpečnostného incidentu
- Zabezpečenie nenapadnutej časti siete pred pokračovaním kybernetického útoku
- V prípade, že sa klient rozhodne komunikovať s útočníkmi:
  - Komunikácia a vyjednávanie s útočníkom s cieľom znížiť výkupné a vyhnúť sa chybám, ktoré môžu spôsobiť, že aj v prípade zaplatenia výkupného útočník neposkytne dešifrovacie kľúče.
  - Pomoc s použitím a validáciou dešifrovacieho nástroja poskytnutého útočníkmi
  - Analýza poskytnutého dešifrovacieho nástroja
- Identifikácia spôsobu kompromitácie organizácie vrátane forenzných analýz použiteľných pre poistenie alebo orgány činné v trestnom konaní
- Identifikácia sekundárnych infekcií v organizácií
- Identifikácia uniknutých dát
- Zabezpečenie organizácie aby sa rovnaký typ útoku neopakoval

Prečo IstroSec?

Kombinované skúsenosti expertov viac ako 70 rokov

Prístup k odborníkom na všetky oblasti informačnej bezpečnosti, vrátane audítorov, penetračných testerov, forenzných analytikov, analytikov malvéru, školiteľov a ďalších

Systematické zlepšenie informačnej bezpečnosti v zmysle štandardov a na základe skúseností s riešením pokročilých bezpečnostných incidentov

Certifikovaní odborníci a zaistenie súladu s bezpečnostnými štandardmi a legislatívou - skúsenosti z verejnej správy (zákon o kybernetickej bezpečnosti, zákon o ITVS a iné) ako aj zo súkromného sektora (ISO 27001, NIST, HIPAA a iné)

Prečo práve my?

Experti IstroSec majú dlhoročné skúsenosti s reakciou na útoky ransomvérom, identifikáciou problému a jeho efektívnym riešením. Využívajú v praxi overenú proprietárnu metodiku a nástroje na efektívnu reakciu na ransomvér (vrátane súvisiacich hrozieb), minimalizáciu škôd na strane klienta a zaistenie digitálnych stôp pre potreby OČTK, regulátora alebo poisťovne.

Sprostredkovanie platieb prostredníctvom kryptomien

V prípade, že sa klient rozhodne zaplatiť vie IstroSec sprostredkovať komunikáciu s útočníkom prostredníctvom vyškolených vyjednávačov s psychologickým tréningom a zabezpečiť, aby:

- nedošlo k nedorozumeniam, ktoré v takejto situácií môžu viesť k trvalej strate údajov;
- v prípade nutnosti platba výkupného prebehla tak, aby bola čo najväčšia pravdepodobnosť poskytnutia dešifrovacieho nástroja útočníkom;
- bola čo najviac znížená pravdepodobnosť zverejnenia uniknutých dokumentov.

Efektívna reakcia

Keď je v organizácií spustený ransomvér, je potrebné reagovať v rádoch hodín, identifikovať momentálne prioritné úlohy a vykonať potrebné aktivity okamžite. Špecialisti IstroSec majú skúsenosti s krízovým manažmentom v takýchto situáciách a podľa požiadaviek klienta koordinujú aktivity reakcie na incidenty alebo priamo tento proces riadia.

Podpora cieľovej organizácie

Nie všetky organizácie majú implementované nástroje, ktoré im umožnia efektívne riešiť takýto útok. IstroSec má k dispozícií proprietárne nástroje, ktoré implementuje v rámci organizácie umožní tak efektívne izolovanie (containment) útoku a jeho analýzu.

Expertíza v riešení kybernetických útokov, v analýze malvéru a forenznej analýze

Špecialisti IstroSec majú expertízu v oblasti reakcie na incidenty, forenznej analýzy a analýzy malvéru na svetovej úrovni, ktorú viackrát preukázali pri riešení štátmi sponzorovaných kybernetických útokov, útokov vedených voči organizáciám FORTUNE 500 ako aj účasťou 4 expertov spoločnosti IstroSec vo víťaznom tíme cvičenia LockedShields 2016.

Experti IstroSec sú súčasne držiteľmi medzinárodne uznávaných certifikátov v týchto oblastiach. Držíme certifikáty, ako napríklad GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE), Certified Reverse Engineering Analyst (CREA) a ďalšie.