IstroSec

Data Sheet

Posúdenie pripravenosti na incident

Pravdepodobnosť výskytu incidentov kybernetickej bezpečnosti ako aj ich dopady sa neustále zvyšujú. Implementáciou vhodných preventívnych, detekčných a reakčných opatrení je možné toto riziko znížiť z hľadiska pravdepodobnosti ako aj z hľadiska dopadu. Ako však zistiť, ktoré procesné, organizačné či technické opatrenia vlastne potrebujete? Experti zo spoločnosti IstroSec majú dlhoročné skúsenosti s riešením kybernetických bezpečnostných incidentov v organizáciách každého zamerania a veľkosti a sú pripravení pomôcť Vám s posúdením pripravenosti Vašej organizácie odolávať bezpečnostným incidentom a spôsobilosti na ich rýchle a efektívne riešenie.

V rámci posúdenia pripravenosti sa zameriame na nasledovné oblasti:

Ľudské zdroje

- zodpovednosť za riešenie incidentov vo Vašej organizácii
- veľkosť, spôsobilosť a pripravenosť vášho tímu na riešenie incidentov
- tretie strany a ich rola v procese riešenia incidentov

Procesy

- prevencia incidentov
- identifikácia incidentov
- prvotná analýza incidentov
- obmedzenie, odstránenie a obnova (Containment, Eradication a Recovery)
- digitálne stopy a forenzná analýza
- zlepšovanie
- Incident prevention
- Incident identification
- Initial incident analysis
- Containment, Eradication and Recovery
- Digital evidence and forensic analysis
- Continual improvement

Technológie

- Architektúra infraštruktúry
- Nastavenia sieťových prvkov – routery, switche
- Nastavenia bezpečnostných prvkov – firewally, UTM, IPS/IDS, NBA, aplikačné firewally
- Nastavenia bezpečnostného dohľadu a systému detekcie a reakcie na bezpečnostný incident
- Nastavenia Serverov – Windows, Linux, Unix
- Nastavenia pracovných staníc
- Nastavenia doménových politík GPO
- Nastavenia cloudových systémov – O365, Azure, AWS
- Nastavenia kritických aplikácií
- Nastavenia zálohovania

Informácie a dokumentácia

- Inventár aktív a dáta o aktívach
- dáta o incidente
- threat intelligence
- sieťová topológia
- bezpečnostné politiky a smernice
- plány reakcie na incident
- eskalačné postupy
- kontakty a komunikačné schémy

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)

IstroSec

Data Sheet

Naša metodológia

Posudzovanie pripravenosti na riešenie incidentu je založené na odporúčaných postupoch, dlhoročnej skúsenosti s riešením bezpečnostných incidentov a znalosti aktuálnych zraniteľností, techník a postupov, ktoré útočníci používajú v rámci kybernetických útokov.

Na čo najefektívnejšie posúdenie pripravenosti organizácie na kybernetický bezpečnostný incident požívajú experti z IstroSec unikátnu metodológiu. Dosahujú ňou pokrytie relevantných bezpečnostných potrieb zákazníka implementáciou opatrení tak, aby mali čo najväčší dosah voči kybernetickým útokom a bola minimalizovaná ich časová, technická a finančná náročnosť.

Naša metodológia stojí na týchto pilieroch:

Threat Landscape

- Vytvorení „Threat landscape“ pre organizáciu. V rámci tejto časti analytici IstroSec analyzujú relevantné hrozby pre organizáciu na základe Threat Intelligence, typu, veľkosti a sektoru organizácie, prípadných minulých prienikov, OSINT, dostupných informácií o organizácií na clear a dark webe, geopolitickej situácie, a špecifík organizácie a threat score vypočítaného na základe používaných technológií.

TTP

- Identifikácia TTP, ktoré používajú útočníci, ktorí sú príslušní vypracovanej „threat landscape“

Dokumentácia, rozhovory a konfigurácia

- Posúdenie procesov, technológie a spôsobilostí relevantných k identifikovaným hrozbám.
  - Preskúmanie relevantnej dokumentácie
  - Preskúmanie pripravenosti formou rozhovorov s personálom
  - Preskúmanie pripravenosti overením konfigurácie implementovaných technológií
  - Vykonanie posúdenia zraniteľností

Analýza a návrh opatrení

- Analýza zisteného stavu a návrh opatrení.

Report

- Vyhodnotenie pripravenosti, príprava záverečnej správy a odporúčaní

Implementácia a cvičenia

- (Optional) Implementácia navrhnutých opatrení a implementácia zodpovedajúcich procesov
- (Optional) Po implementácií navrhnutých opatrení prebehne procesné a technické cvičenie za účelom preverenia efektivity implementovaných opatrení na procesnej a technickej úrovni prostredníctvom:
  - Tabletop cvičenia
  - Red Team cvičenia
  - Purple Team cvičenia

IstroSec

Data Sheet

Prečo my?

Skúsenosti a znalosti

Experti **Istro**Sec majú dlhoročné skúsenosti so zvyšovaním odolnosti na kybernetické útoky v organizáciách rôznych veľkostí a zameraní. Majú prehľad o aktuálnych hrozbách, taktikách, technikách a procedúrach používaných útočníkmi. Kombinácia týchto znalostí s bohatými skúsenosťami s reakciami na incidenty umožňujú našim špecialistom navrhnúť na mieru pre Vašu organizáciu sadu administratívnych aj technických opatrení na vytvorenie odolnej a robustnej kybernetickej imunity.

Expertíza v riešení incidentov

IstroSec má expertízu v posudzovaní pripravenosti svojich klientov odolávať kybernetickým bezpečnostným incidentom, s forenznou analýzou a analýzou 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 **Istro**Sec vo víťaznom tíme cvičenia Locked Shields 2016.

Certified professionals

Experti **Istro**Sec sú držiteľmi medzinárodne uznávaných certifikátov v mnohých oblastiach. Držíme certifikáty, ako napríklad Certified Information Systems Security Professional (CISSP), Certified Information system Auditor (CISA), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE), Certified Reverse Engineering Analyst (CREA) a ďalšie.

Prípadová štúdia

Typ organizácie: Väčšia firma z fintech sektora

Poskytnutá služba: Posúdenie pripravenosti na incident

Riešenie: Posúdenie vyspelosti riešenia incidentov a simulácia útoku

Veľká organizácia z fintech sektora sa na nás obrátila so žiadosťou o posúdenie úrovne vyspelosti svojich schopností reagovať na incidenty relevantné pre túto organizáciu. Organizácia má certifikovaný svoj systém riadenia informačnej bezpečnosti podľa štandardu ISO 27001 a tiež je držiteľom certifikácií PCI DSS.

IstroSec systematicky analyzoval profil hrozieb organizácie a zistil, že okrem štandardných hrozieb, ako je napríklad ransomvér, by sa na túto organizáciu mohli zamerať aj sofistikovanejšie útočné skupiny kvôli jej pozícii na trhu, počtu inštitúcií a organizácií, ktoré používajú jej softvér, a tiež kvôli jej dobrým finančným výsledkom. Následne bol zostavený zoznam schopností útočníkov a ich TTP, aby sa vytvoril základ, voči ktorému sa vykonalo samotné posúdenie pripravenosti.

IstroSec použil svoju metodológiu na posúdenie dokumentácie, procesov a technológií. Organizácia má implementované ISO 27001 a systematicky dodržiava všetky požadované postupy. Tiež má kompetentný bezpečnostný tím, ktorý štandardne postupuje v zmysle interných predpisov. Počas hodnotenia sa však zistilo, že bezpečnosť organizácie sa zameriava na dodržiavanie predpisov a noriem, chýbali však kľúčové komponenty, ktoré umožňujú rýchlo a efektívne reagovať na skutočné incidenty.

IstroSec navrhol 283 konfiguračných zmien v active directory, cloudovom prostredí, koncových bodoch, sieťových a bezpečnostných riešeniach, v správe protokolov a v SIEM systéme. Každá z nich bola zameraná na detekciu, narušenie, odmietnutie, znehodnotenie alebo oklamanie konkrétneho použitého TTP útočníka relevantného pre organizáciu. Tiež sa zistilo, že organizácia nemá efektívne procesy týkajúce sa riešenia bezpečnostných incidentov a zistili sa aj niektoré medzery v eskalácii incidentov. Ďalej boli odporučené zmeny procesov a bola podporená implementácia týchto zmien.

Po implementácii odporúčaní bola vykonaná simulácia útoku na testovanie účinnosti implementovaných opatrení.