IstroSec

Data Sheet

Implementácia procesov riadenia informačnej bezpečnosti

Špecialisti zo spoločnosti ISTROSEC majú dlhoročné skúsenosti v oblasti riadenia informačnej bezpečnosti vo verejnej správe i v súkromnom sektore. Z našich skúseností preto vieme, že požiadavky na informačnú bezpečnosť sa v organizáciách rôznych typov a zamerania rôznia a neexistuje univerzálne riešenie, ktoré by umožnilo adekvátne tieto požiadavky plniť za primeranú cenu vzhľadom na hodnotu aktív.

Náš prístup k zavádzaniu informačnej bezpečnosti:

- Súlad cieľov informačnej bezpečnosti s obchodnými cieľmi a ich podpora
- Implementácia opatrení na základe analýzy rizík
- Individuálny prístup
- Implementácia efektívnych opatrení na základe skúseností s mnohými pokročilými bezpečnostnými incidentmi

Prečo IstroSec?

Kombinované skúsenosti expertov viac ako 70 rokov

Prístup k odborníkom na všetky oblasti informačnej bezpečnosti, vrátane 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

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)

„Sme pripravení zaviesť procesy riadenia informačnej bezpečnosti v súlade s regulačnými a normatívnymi požiadavkami"

- ISO / IEC 27001 and ISO / IEC 27002
- NIST Cybersecurity Framework
- IASME
- 69/2018 Z.z. - Zákon o kybernetickej bezpečnosti
- Zákon o informačných technológiách vo verejnej správe
- GDPR
- HIPAA
- FISMA

Postup implementácie:

- Identifikácia všetkých bezpečnostných požiadaviek
- Určenie rozsahu implementácie
- Posúdenie existujúcich bezpečnostných opatrení
- Posúdenie rizík
- Vytvorenie implementačného plánu
- Implementácia bezpečnostných opatrení a procesov
- Meranie, monitorovanie, preskúmavanie a neustále zlepšovanie
- Príprava na certifikáciu

IstroSec

Data Sheet

Prečo práve my?

Skúsenosti a znalosti

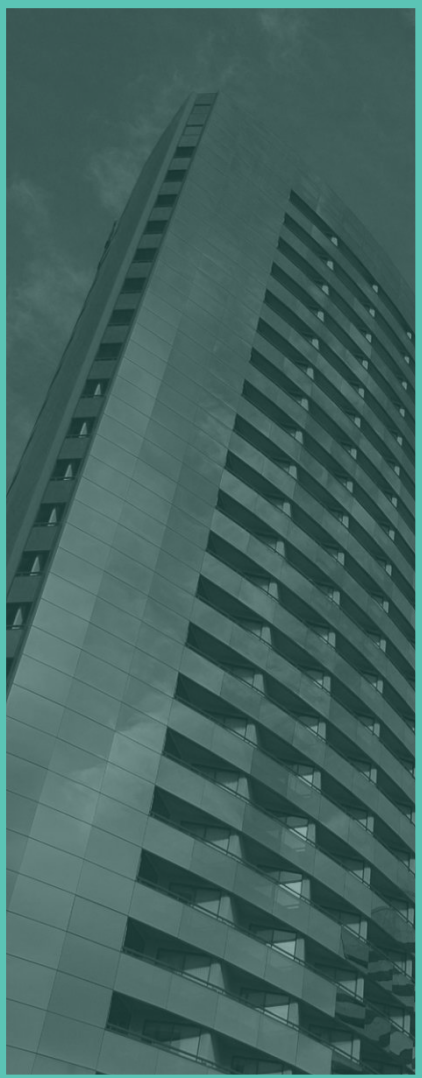
Špecialisti **Istro**Sec majú skúsenosti s implementáciou a riadením informačnej bezpečnosti podľa väčšiny bezpečnostných frameworkov, poznajú taktiky, techniky a postupy útočníkov a majú znalosti potrebné na efektívnu a plynulú implementáciu procesov informačnej bezpečnosti do vašich biznis procesov.

Expertíza v manažmente

Expertíza v oblasti riadenia informačnej bezpečnosti a mnohých ďalších oblastiach, ako napr. reakcia na incidenty, forenzná analýza a analýza 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 LockedShields 2016.

Certifikovaní profesionáli

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.



Prípadové štúdie

Typ organizácie: Stredne veľká spoločnosť na vývoj softvéru

Poskytnutá služba: Implementácia procesov riadenia informačnej bezpečnosti

Riešenie: Implementácia procesu riadenia rizík

Spoločnosť zaoberajúca sa vývojom ekonomického softvéru potrebovala implementovať procesy riadenia rizík, aby mohla pravidelne hodnotiť svoje riziká. Keď spoločnosť nedávno začala svoju implementáciu ISO 27001, bola potrebné preukázať jej schopnosť odhaľovať, posudzovať a zmierňovať riziká v oblasti informačnej bezpečnosti. Bola preto pre ňu vyvinutá metodika riadenia rizík založená na ISO 27005. Následne sa začala prvá iterácia analýzy rizík. Bol vypracovaný inventár informačných aktív na základe identifikácie a ohodnotenia informačných aktív. Potom boli identifikované zraniteľné miesta a hrozby súvisiace s týmito aktívami. Vypočítali sa riziká informačnej bezpečnosti a boli mitigované tie, ktoré prekročili hranicu prijateľného rizika.

Typ organizácie: Poskytovateľ základnej služby v sektore elektronické komunikácie

Poskytnutá služba: Implementácia procesov riadenia informačnej bezpečnosti

Riešenie: Rozdielová analýza a implementácia procesov riadenia incidentov

Poskytovateľ základnej služby podľa zákona o kybernetickej bezpečnosti potreboval splniť svoju regulačnú povinnosť implementovať procesy na detekciu kybernetických bezpečnostných incidentov, získavanie a uchovávanie digitálnych stôp, riešenie incidentov a ich hlásenie regulátorovi. Na začiatku bolo vykonané hodnotenie pripravenosti na incidenty, ktoré odhalilo nedostatky v ľudských zdrojoch, procesoch a technológiách potrebných na riešenie incidentov. Následne bol navrhnutý a implementovaný plán reakcie na incidenty a súvisiace postupy. Tieto boli potom testované uskutočnením tabletop cvičenia, ktoré tieto procesy ešte posilnilo a validovalo.

IstroSec | Černyševského 10 | 851 01 Bratislava | Slovensko | +421 917 699 002 | info@istrosec.com | www.istrosec.com