IstroSec

Data Sheet

Audit informačnej bezpečnosti

Audit bezpečnosti informačných systémov je kľúčovým prvkom v procese zaisťovania a overovania súladu s bezpečnostnými požiadavkami. Je to nástroj na overenie toho, že bezpečnostné opatrenia sú adekvátne, efektívne a fungujú tak, ako sa od nich očakáva. Je to tak isto spôsob, ako zaistiť neustále zlepšovanie, resp. adaptáciu opatrení na dynamicky meniace sa prostredie a bezpečnostné hrozby.

Audítori zo spoločnosti IstroSec dodržiavajú nasledovné princípy:

- Nestrannosť, nezávislosť a objektivita
- Due dilligence a odborná starostlivosť
- Dôvernosť a mlčanlivosť
- Prístup na základe analýzy rizík
- Profesionálna etika
- Kompetencia a profesionálny rozvoj

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

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)

"Vykonávame audity bezpečnosti podľa mnohých legislatívnych a normatívnych požiadaviek"

- 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

Spoločnosť IstroSec vykonáva externé audity podľa Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. Naši certifikovaní audítori spĺňajú kvalifikačné požiadavky dané vyhláškou NBÚ č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora.

Interný audit od spoločnosti **IstroSec** Vám umožní:

- Pripraviť sa na externý alebo certifikačný audit
- Splnenie legislatívnych povinností a požiadaviek štandardov na výkon interného auditu
- Identifikovať nezhody aktuálneho stavu s bezpečnostnými požiadavkami
- Identifikovať príležitosti na zlepšenie opatrení
- Stanoviť priority v investíciách do bezpečnosti

IstroSec

Data Sheet

Pri výkone auditov postupujeme v týchto krokoch

Plánovanie

- Stanovenie predmetu auditu
- Identifikácia cieľov auditu
- Určenie rozsahu auditu
- Pre-audit
- Identifikácia zdrojov informácií

Výkon auditu

- Preskúmanie dokumentácie
- Riadené rozhovory
- Zber a vyhodnocovanie dôkazov

Reportovanie

- Vyhodnotenie auditu
- Tvorba záverečnej správy
- Prezentácia výsledkov
- Následné činnosti a vyhodnotenie implementácie opatrení

Poskytujeme tieto typy auditov

Audit bezpečnostnej dokumentácie

Preskúmanie adekvátnosti a účinnosti dokumentácie súvisiacej s informačnou bezpečnosťou umožní odhaliť nedostatky v riadení informačnej bezpečnosti. Bezpečnostná dokumentácia zahŕňa predovšetkým bezpečnostné stratégie, projekty, politiky, smernice, pracovné postupy, príručky, ale aj záznamy o prevádzke systému informačnej bezpečnosti. V rámci auditu okrem vrcholovej dokumentácie preskúmame aj riadenie aktív, rizík, schémy klasifikácie informácií, riadenie prístupu a akúkoľvek bezpečnostnú dokumentáciu.

Audit procesov

V rámci systému informačnej bezpečnosti prebiehajú mnohé procesy, ako napr. riadenie rizík tretích strán alebo proces riadenia incidentov informačnej bezpečnosti. Naši audítori preskúmajú ako tieto procesy fungujú a posúdia mieru plnenia interných a externých požiadaviek. Počas rozhovorov so zamestnancami zodpovednými za tieto procesy sa preverí aktuálny stav a zhodnotí sa či je tento proces dostatočne jasne definovaný, dokumentovaný a či všetky zainteresované strany vedia aká je ich rola. V rámci záverečnej správy z auditu poskytneme aj odporúčania pre vyriešenie zistených nedostatkov.

Audit zhody so štandardom

Tento typ auditu má za cieľ preskúmať, do akej miery sú splnené požiadavky bezpečnostných štandardov a legislatívy (napr. zákon o kybernetickej bezpečnosti). Rozsah auditu závisí od štandardu, voči ktorému ma byť audit vykonaný. V rámci auditu zhody so štandardom audítori skúmajú vnútorné predpisy, dokumentované postupy, a rôzne záznamy preukazujúce, že systém bezpečnosti funguje tak, ako má.

Technický bezpečnostný audit

V rámci tohto typu bezpečnostného auditu sa preverujú bezpečnostné konfigurácie serverov, koncových zariadení, siete, sieťových a bezpečnostných zariadení. Rovnako sa skúma hardening zariadení a implementácie technických bezpečnostných opatrení. V rámci auditných činností sa audítori zameriavajú aj na bezpečnostné logy, FW pravidlá, šifrovanie, zálohovanie a podobne.

IstroSec

Data Sheet

Prečo práve my?

Skúsenosti a znalosti

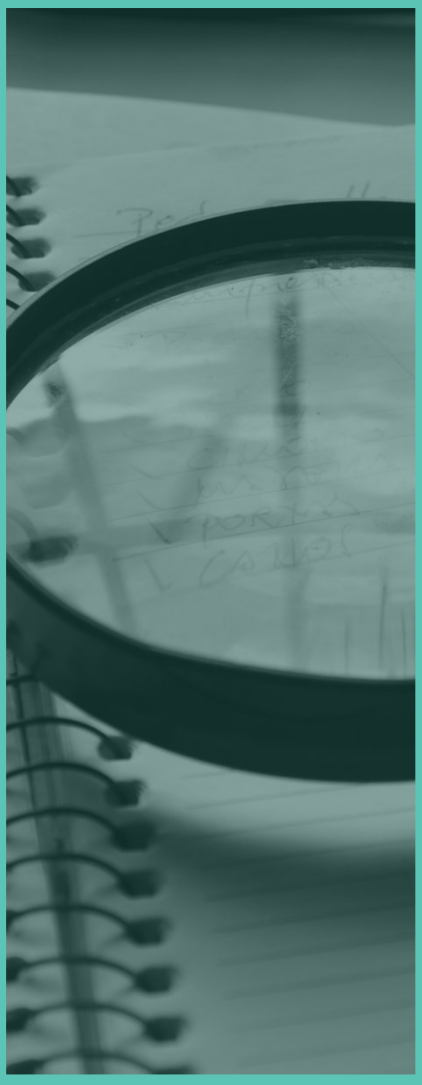
Špecialisti **Istro**Sec majú skúsenosti s implementáciou a riadením a auditom informačnej bezpečnosti podľa väčšiny bezpečnostných frameworkov, poznajú taktiky, techniky a postupy útočníkov a majú znalosti potrebné na efektívnu a plynulú implementáciu procesov informačnej bezpečnosti do vašich biznis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

Expertíza v oblasti auditu

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: Poskytovateľ logistických služieb

Poskytnutá služba: Audit informačnej bezpečnosti

Riešenie: Vnútorný audit zhody so štandardom ISO 27001

Spoločnosť zaoberajúca sa poskytovaním logistických a zasielateľských služieb potrebovala vykonať vnútorný audit systému riadenia informačnej bezpečnosti. Táto spoločnosť nedávno implementovala štandard ISO 27001 a bolo potrebné preukázať, že má nezávislú a efektívnu funkciu vnútorného auditu. Keďže v tejto spoločnosti nebol zamestnaný interný audítor, spoločnosť sa preto rozhodla túto funkciu outsourcovať. Bola preto pre ňu vyvinutá interná metodika na vykonávanie auditov a bol vypracovaný program auditov na tri roky. Následne sa začala prvá iterácia vnútorného auditu v zmysle ISO 27001. Bola preskúmaná interná riadiaca dokumentácia, boli vykonané rozhovory so zamestnancami, boli zozbierané a analyzované dôkazy a následne boli vyhodnotené zistenia. Závery z auditu spolu s odporúčaniami boli zhrnuté v záverečnej správe z auditu. Bolo identifikovaných niekoľko nezhôd so štandardom a viacero príležitostí na zlepšenie.

Typ organizácie: Spoločnosť zameraná na vývoj softvéru

Poskytnutá služba: Audit informačnej bezpečnosti

Riešenie: Technický bezpečnostný audit

Spoločnosť zameraná na vývoj softvéru potrebovala preveriť účinnosť svojich sieťových bezpečnostných prvkov a ich súlad so súčasnými bezpečnostnými štandardmi. Bol preto vykonaný komplexný technický audit konfigurácie firewallov, systémov prevencie prienikov (IPS), webaplikačných firewallov a proxy serverov. Boli preskúmané firewall pravidlá, logovanie, patch management a v neposlednom rade aj hardening sieťových a bezpečnostných prvkov. Záverečná správa obsahovala prioritizovaný zoznam zistení spolu s odporúčaniami na ich mitigáciu.

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