IstroSec

Arkusz danych

Audyt bezpieczeństwa teleinformatycznego

Audyt bezpieczeństwa systemów teleinformatycznych jest kluczowym elementem w procesie zapewnienia i weryfikacji zgodności z wymaganiami bezpieczeństwa. Jest to narzędzie do weryfikacji, czy środki bezpieczeństwa są odpowiednie, skuteczne i działają zgodnie z oczekiwaniami. To także sposób na ciągłe doskonalenie i dostosowywanie zabezpieczeń do dynamicznie zmieniającego się środowiska i zagrożeń bezpieczeństwa.

Audytorzy IstroSec przestrzegają następujących zasad:

- Bezstronność, niezależność i obiektywność
- Należyta zawodowa staranność
- Poufność i nieujawnianie
- Podejście oparte na ryzyku
- Etyka zawodowa
- Kompetencje i rozwój zawodowy

Dlaczego IstroSec?

Łącznie ponad 70 lat doświadczenia

Dostęp do ekspertów ze wszystkich dziedzinach bezpieczeństwa informacji, w tym testerów penetracyjnych, analityków kryminalistycznych, analityków złośliwego oprogramowania, trenerów i nie tylko

Systematyczna poprawa bezpieczeństwa informacji według frameworków wzbogaconych doświadczeniem ekspertów IstroSec z zaawansowanymi incydentami bezpieczeństwa

Zapewniając zgodność z normami i przepisami bezpieczeństwa, eksperci IstroSec działają zarówno w administracji publicznej (dyrektywa NIS, RODO i inne) jak i w sektorze prywatnym (ISO 27001, NIST, HIPAA i inne)

Wykonujemy wewnętrzne audyty bezpieczeństwa zgodnie z wieloma wymogami legislacyjnymi i normatywnymi

- ISO / IEC 27001 oraz ISO / IEC 27002
- Ramy cyberbezpieczeństwa NIST
- IASME
- Ustawa nr 69/2018 (Zbiór Praw) - Ustawa o cyberbezpieczeństwie
- Ustawa o technologiach informacyjnych w administracji publicznej
- RODO
- HIPAA
- FISMA

IstroSec nie przeprowadza obecnie audytów zewnętrznych ani certyfikacyjnych. Obecnie pracujemy nad rozszerzeniem naszego portfolio usług o tego typu audyty.

Audyt wewnętrzny IstroSec pozwoli Ci:

- Przygotować się do audytu zewnętrznego lub certyfikacyjnego
- Spełnić obowiązki regulacyjne i wymagania standardów dotyczących prowadzenia audytu wewnętrznego
- Zidentyfikować niezgodności między aktualnym stanem a wymaganiami bezpieczeństwa
- Zidentyfikować możliwości poprawy
- Nadać priorytet inwestycjom w bezpieczeństwo

IstroSec

Arkusz danych

Podczas przeprowadzania audytów postępujemy zgodnie z tymi krokami

Planowanie

- Ustalenie przedmiotu i zakresu oraz identyfikacja celów audytu
- Audyt wstępny
- Identyfikacja źródeł informacji

Przeprowadzenie audytu

- Przegląd dokumentacji
- Rozmowy z personelem
- Gromadzenie i ocena dowodów

Sprawozdawczość

- Ocena audytu
- Tworzenie raportu końcowego
- Prezentacja wyników
- Kontynuacja i ocena działań naprawczych

Wykonujemy następujące audyty

Audyt dokumentacji bezpieczeństwa teleinformatycznego

Badanie adekwatności i skuteczności dokumentacji dotyczącej bezpieczeństwa informacji pozwoli zidentyfikować luki w zarządzaniu bezpieczeństwem informacji. Dokumentacja bezpieczeństwa składa się głównie ze strategii bezpieczeństwa, polityk, wytycznych, procedur, instrukcji, ale także zapisów dotyczących funkcjonowania systemu bezpieczeństwa informacji. Oprócz dokumentacji wysokiego poziomu dokonamy również przeglądu zarządzania aktywami, zarządzania ryzykiem, schematów klasyfikacji informacji, kontroli dostępu i wszelkiej innej dokumentacji dotyczącej bezpieczeństwa.

Audyt procesów

W ramach systemu bezpieczeństwa teleinformatycznego zachodzi wiele procesów, takich jak zarządzanie ryzykiem stron trzecich czy proces zarządzania incydentami bezpieczeństwa teleinformatycznego. Nasi audytorzy badają działanie tych procesów i oceniają stopień spełnienia wymagań wewnętrznych i zewnętrznych. W trakcie rozmów z pracownikami odpowiedzialnymi za te procesy zostanie zweryfikowany stan obecny. Następnie zostanie ocenione, czy procesy te są jasno zdefiniowane, udokumentowane i czy wszystkie zainteresowane strony znają swoją rolę. W ramach końcowego raportu z audytu przedstawimy również rekomendacje dotyczące usunięcia zidentyfikowanych luk.

Audyt zgodności z normą

Ten rodzaj audytu ma na celu zbadanie, w jakim stopniu spełnione są wymagania norm bezpieczeństwa i ustawodawstwa. Zakres audytu w dużej mierze zależy od standardu odniesienia. W ramach audytu zgodności audytorzy badają polityki wewnętrzne, udokumentowane procedury i różne zapisy wykazujące, że system bezpieczeństwa działa zgodnie z przeznaczeniem.

Audyt bezpieczeństwa technicznego

Ten rodzaj audytu bezpieczeństwa bada konfiguracje bezpieczeństwa serwerów, punktów końcowych, sieci i urządzeń zabezpieczających. Badane są również zabezpieczenia sprzętu i wdrażanie technicznych środków bezpieczeństwa. W ramach działań audytowych nasi audytorzy koncentrują się na logach bezpieczeństwa, regułach zapory, szyfrowaniu, kopiach zapasowych i innych aspektach bezpieczeństwa teleinformatycznego.

IstroSec

Arkusz danych

Dlaczego my?

Doświadczenie i wiedza

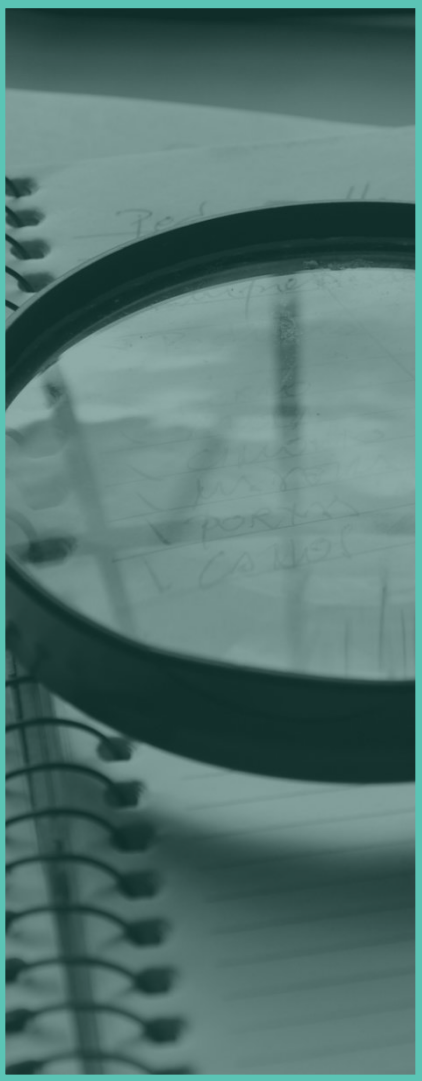
Specjaliści **Istro**Sec mają doświadczenie we wdrażaniu bezpieczeństwa teleinformatycznego, zarządzaniu nim i jego kontroli zgodnie z większością ram bezpieczeństwa teleinformatycznego. Znają taktykę, techniki i procedury atakujących oraz posiadają niezbędną wiedzę, aby skutecznie i płynnie wdrażać procesy bezpieczeństwa teleinformatycznego do twoich procesów biznesowych.

Specjalistyczna wiedza z zakresu audytów

Specjalistyczna wiedza w zakresie zarządzania bezpieczeństwem teleinformatycznym i jego kontroli oraz wielu innych obszarach, takich jak reakcja na zdarzenia, analiza kryminalistyczna czy światowej klasy analiza złośliwego oprogramowania, którą wielokrotnie wykazali się nasi specjaliści podczas radzenia sobie z cyberatakami wspieranymi przez państwo, atakami na organizacje z listy Fortune 500, a także udział czterech ekspertów IstroSec w zwycięstudniaskim zespole ćwiczenia Locked Shields 2016.

Certyfikowani profesjonaliści

Eksperci **Istro**Sec są również posiadaczami uznanych na całym świecie certyfikatów w tych dziedzinach. Posiadamy certyfikaty takie jak 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) i inne.



Studium przypadku

Rodzaj firmy: Dostawca usług logistycznych

Świadczone usługi: Audyt bezpieczeństwa teleinformatycznego

Rozwiązanie: Audyt wewnętrzny zgodności z normą ISO 27001

Firma świadcząca usługi logistyczne i spedycyjne potrzebne do przeprowadzenia audytu wewnętrznego systemu zarządzania bezpieczeństwem teleinformtycznym. Firma niedawno wdrożyła normę ISO 27001 i konieczne było wykazanie, że posiada niezależną i skuteczną funkcję audytu wewnętrznego. Ponieważ firma nie posiadała audytora wewnętrznego, firma zdecydowała się na outsourcing tej funkcji. W związku z tym opracowano wewnętrzną metodologię przeprowadzania audytów oraz opracowano program audytów na kolejne trzy lata. Następnie rozpoczęto pierwszą iterację audytu wewnętrznego zgodnie z ISO 27001. Dokonano przeglądu dokumentacji wewnętrznej, przeprowadzono rozmowy z pracownikami, zebrano i przeanalizowano dowody, a następnie dokonano oceny wyników. Wyniki audytu wraz z zaleceniami zostały podsumowane w końcowym sprawozdaniu z audytu. Zidentyfikowano kilka rozbieżności ze standardem i kilka możliwości poprawy.

Rodzaj firmy: Firma zajmująca się tworzeniem oprogramowania

Świadczone usługi: Audyt bezpieczeństwa teleinformatycznego

Rozwiązanie: Audyt bezpieczeństwa technicznego

Firma tworząca oprogramowanie musiała zweryfikować skuteczność swoich funkcji bezpieczeństwa sieci i ich zgodność z aktualnymi standardami bezpieczeństwa. W związku z tym przeprowadzono kompleksowy audyt techniczny konfiguracji zapór sieciowych, systemów zapobiegania włamaniom (IPS), zapór sieciowych aplikacji internetowych oraz serwerów proxy. Zbadano reguły zapory, logowanie, zarządzanie poprawkami oraz wzmocnienie sieci i urządzeń zabezpieczających. Raport końcowy zawierał uporządkowaną według priorytetów listę ustaleń wraz z zaleceniami dotyczącymi ich złagodzenia.