IstroSec

Arkusz danych

Wdrażanie procesów bezpieczeństwa teleinformatycznego

Specjaliści ds. zarządzania bezpieczeństwem teleinformatycznym z IstroSec posiadają wieloletnie doświadczenie w zarządzaniu bezpieczeństwem teleinformatycznym zarówno w administracji publicznej, jak i w sektorze prywatnym. Z naszego doświadczenia wiemy, że wymagania dotyczące bezpieczeństwa teleinformatycznego w różnych typach organizacji są różne. Dlatego nie ma jednego uniwersalnego rozwiązania, które pozwoliłoby odpowiednio spełnić wszystkie te wymagania przy rozsądnych kosztach, biorąc pod uwagę wartość aktywów.

Nasze podejście do wdrażania bezpieczeństwa teleinformatycznego

- Dopasowanie celów bezpieczeństwa teleinformatycznego do celów biznesowych i ich wsparcie
- Wdrażanie kontroli bezpieczeństwa w oparciu o ryzyko
- Indywidualne podejście
- Wykorzystanie doświadczenia z wieloma zaawansowanymi incydentami bezpieczeństwa podczas wdrażania kontroli bezpieczeństwa

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)

„Jesteśmy gotowi na wdrożenie procesów zarządzania bezpieczeństwem teleinformatycznym zgodnie z wieloma wymaganiami regulacyjnymi i normatywnymi"

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

Proces wdrożenia

- Identyfikacja wszystkich wymagań bezpieczeństwa
- Ustalenie zakresu wdrożenia
- Ocena istniejących środków bezpieczeństwa
- Ocena ryzyka
- Tworzenie planu wdrożenia
- Wdrażanie środków i procesów bezpieczeństwa
- Pomiar, monitorowanie, przegląd i ciągłe doskonalenie
- Przygotowanie do certyfikacji

IstroSec

Arkusz danych

Dlaczego my?

Doświadczenie i wiedza

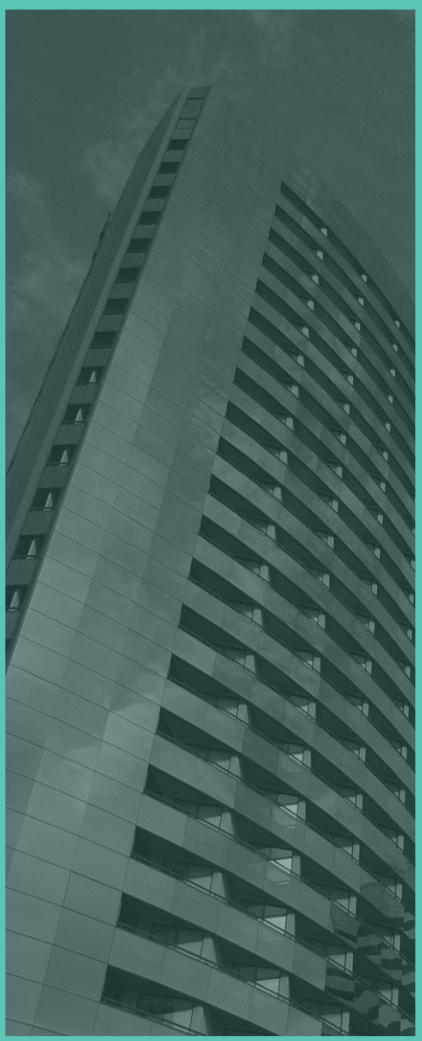
Specjaliści **Istro**Sec mają doświadczenie we wdrażaniu i zarządzaniu bezpieczeństwem informacji zgodnie z większością ram bezpieczeństwa teleinformatycznego. Znają taktykę, techniki i procedury atakujących oraz posiadają niezbędną wiedzę, aby skutecznie i płynnie wdrażać procesy bezpieczeństwa teleinformatycznego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

Specjalistyczna wiedza z zakresu zarządzania

Specjalistyczna wiedza w zakresie zarządzania bezpieczeństwem teleinformatycznym 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: Średniej wielkości firma zajmująca się tworzeniem oprogramowania

Świadczone usługi: Wdrażanie procesów zarządzania bezpieczeństwem teleinformatycznym

Rozwiązanie: Wdrożenie procesu zarządzania ryzykiem

Firma zajmująca się rozwojem oprogramowania ekonomicznego musiała wdrożyć procesy zarządzania ryzykiem, aby okresowo oceniać swoje ryzyko. Ponieważ firma niedawno rozpoczęła wdrażanie ISO 27001, musiała wykazać się umiejętnością wykrywania, rozumienia i ograniczania zagrożeń związanych z bezpieczeństwem teleinformatycznym. W związku z tym opracowano metodologię zarządzania ryzykiem opartą na normie ISO 27005. Następnie rozpoczęła się pierwsza iteracja oceny ryzyka. Opracowano listę aktywów, w ramach której zidentyfikowano i wyceniono aktywa teleinformatyczne. Następnie zidentyfikowano słabe punkty i zagrożenia związane z tymi aktywami. Obliczono zagrożenia bezpieczeństwa teleinformatycznego i ograniczono te powyżej akceptowalnego progu ryzyka.

Rodzaj firmy: Dostawca podstawowych usług w sektorze telekomunikacyjnym

Świadczone usługi: Wdrażanie procesów zarządzania bezpieczeństwem teleinformatycznym

Rozwiązanie: Ocena luk i wdrożenie procesu zarządzania incydentami

Dostawca podstawowych usług zgodnie ze słowacką ustawą o cyberbezpieczeństwie musiał wypełnić swój obowiązek regulacyjny polegający na wdrożeniu procesów wykrywania incydentów cyberbezpieczeństwa, pozyskiwania i przechowywania dowodów cyfrowych, rozwiązywania incydentów i raportowania. Początkowo przeprowadzono ocenę gotowości na wypadek incydentu, która ujawniła luki w zasobach ludzkich, procesach i technologiach potrzebnych do zarządzania incydentami. Następnie opracowano i wdrożono plan reagowania na incydenty i zbiór strategii. Zostały one następnie przetestowane za pomocą ćwiczeń symulacyjnych, które dodatkowo wzmocniły i zweryfikowały te procesy.