IstroSec

Arkusz danych

Ocena gotowości na wypadek incydentu

Prawdopodobieństwo wystąpienia incydentu w zakresie cyberbezpieczeństwa i wiążących się z nim konsekwencji stale wzrasta. Możliwe jest zmniejszenie tego ryzyka poprzez wdrożenie odpowiednich środków zapobiegawczych, detektywistycznych i reaktywnych. Ale skąd będziesz wiedzieć, jakie środki techniczne, organizacyjne lub proceduralne musisz podjąć? Eksperci z **Istro**Sec mają wieloletnie doświadczenie w rozwiązywaniu incydentów w zakresie cyberbezpieczeństwa w organizacjach z wielu dziedzin. Jesteśmy gotowi pomóc Ci w ocenie gotowości Twojej organizacji i skuteczności w radzeniu sobie z incydentami w zakresie cyberbezpieczeństwa.

W ramach Twojej oceny skupiamy się na następujących obszarach:

Zasoby ludzkie

- Odpowiedzialność za radzenie sobie z incydentami w zakresie cyberbezpieczeństwa
- Wielkość, predyspozycje i przygotowanie Twojego zespołu do rozwiązywania incydentów w zakresie cyberbezpieczeństwem
- Strony trzecie i ich rola w rozwiązywaniu incydentów

Procesy

- Zapobieganie incydentom
- Identyfikacja incydentu
- Wstępna analiza incydentu
- Powstrzymanie, eliminacja i odzyskiwanie
- Analiz dowodów cyfrowych i analiza kryminalistyczna
- Ciągłe doskonalenie

Technologia

- Architektura infrastruktury i sieci
- Ustawienie komponentów sieciowych - switche i routery
- Ustawienie komponentów bezpieczeństwa - firewalle, UTM, IPS/IDS, NBA, firewall aplikacji
- Nadzór nad bezpieczeństwem, systemy wykrywania i reagowania na incydenty
- Konfiguracja serwerów - Windows, Linux, Unix
- Ustawienie stacji roboczej
- Ustawianie zasad domeny i GPO
- Ustawienia systemu w chmurze - O365, Azure, AWS
- Krytyczne ustawienie aplikacji
- Ustawienia kopii zapasowej

Materiał i dokumentacja

- Inwentaryzacja aktywów
- Dokumentacja incydentu
- Analiza zagrożeń
- Topologia sieci
- Polityki i przepisy bezpieczeństwa
- Procedury rozwiązywania incydentów
- Procedury eskalacji
- Kontakty i schematy kontaktów

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

Certyfikowani eksperci w celu zapewnienia zgodności z normami i przepisami bezpieczeństwa - eksperci **Istro**Sec działają zarówno w administracji publicznej (dyrektywa NIS, RODO i inne) jak i w sektorze prywatnym (ISO 27001, NIST, HIPAA i inne)

IstroSec

Arkusz danych

Nasza metodologia

Nasze oceny incydentów cyberbezpieczeństwa opierają się na najlepszych praktykach i wieloletnim doświadczeniu w rozwiązywaniu incydentów cyberbezpieczeństwa, znajomości aktualnych słabych punktów, technik, taktyk i procedur stosowanych przez atakujących podczas cyberataków.

Aby móc jak najskuteczniej ocenić przygotowanie Twojej organizacji na incydenty w zakresie cyberbezpieczeństwa, nasz zespół w IstroSec opracował unikalną metodologię. Dzięki tej metodologii zaspokajamy odpowiednie potrzeby naszego klienta w zakresie bezpieczeństwa. Ponadto koncentrujemy się na wdrożeniu zestawu procedur, które mają największy wpływ na zdolność radzenia sobie z atakami cyberbezpieczeństwa, przy jednoczesnej minimalizacji czasu rozwiązania, kosztów technicznych i finansowych.

Nasza metodologia opiera się na poniższych filarach:

Specyfikacja zagrożeń

- Stworzenie „Specyfikacji zagrożeń” dla organizacji, w której eksperci IstroSec analizują istotne zagrożenia dla Twojej organizacji w oparciu o analizę zagrożeń, typ, wielkość i sektor organizacji. W tym potencjalne wcześniejsze naruszenia, OSINT (clear i darkweb), sytuacja geopolityczna, konkretna organizacja i ocena zagrożeń wyliczona na podstawie stosowanych technologii.

TTP

- Identyfikacja taktyk, technik i procedur (TTP) stosowanych przez atakujących
- Ocena procedur, technologii i zdolności istotnych dla zidentyfikowanych zagrożeń

Dokumentacja, wywiady i konfiguracja

- Sprawdzanie odpowiedniej dokumentacji
- Ocena przygotowania w formie wywiadu z pracownikami
- Ocena gotowości poprzez sprawdzenie konfiguracji wdrożonych technologii

Ocena w celu poprawy

- Ocena podatności na zagrożenia
- Analiza stanu obecnego i propozycje usprawnień

Sprawozdanie

- Ocena gotowości, stworzenie raportu końcowego i rekomendacji

Wdrażanie i ćwiczenia

- (Opcjonalnie) Wdrożenie proponowanych procedur i odpowiednich procesów
- (Opcjonalnie) Przeprowadzenie ćwiczenia technicznego w celu weryfikacji skuteczności wdrożonych procedur na poziomie technicznym i proceduralnym poprzez:
  - Ćwiczenia teoretyczne
  - Ćwiczenie Red Team
  - Ćwiczenie Purple Team

IstroSec

Arkusz danych

Dlaczego my?

Doświadczenie i wiedza

Eksperci **Istro**Sec mają wieloletnie doświadczenie w zwiększaniu odporności organizacji różnej wielkości i z różnych sektorów na cyberataki. Utrzymują aktualną wiedzę na temat cyberzagrożeń, taktyk, technik i procedur stosowanych przez atakujących. Połączenie tej wiedzy z bogatym doświadczeniem w reagowaniu na rzeczywiste incydenty pozwala naszym specjalistom dopasować odpowiedni zestaw środków administracyjnych i technicznych dla Twojej organizacji, aby stworzyć odporną i solidną cyberodporność.

Specjalistyczna wiedza w zakresie reagowania na incydenty

Specjalistyczna wiedza i doświadczenie w zakresie oceny gotowości naszego klienta do stawienia czoła cyberatakom i powiązanym obszarom, takim jak cyfrowa analiza śledcza i światowej klasy analiza złośliwego oprogramowania, którymi 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 zwycięskim 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: Duża firma fintechowa

Świadczone usługi: Ocena gotowości na wypadek incydentu

Rozwiązanie: Ocena dojrzałości IR i symulacja ataku

Duża firma fintechowa zwróciła się do nas z prośbą o ocenę ich poziomu dojrzałości i możliwości reagowania na istotne dla nich incydenty. Firma ta posiadała już certyfikat ISO 27001 oraz certyfikaty PCI DSS.

IstroSec systematycznie analizował profil zagrożeń firmy i ustalił, że oprócz standardowych zagrożeń dla firm, takich jak oprogramowanie ransomware i tym podobne, firma ta może być również celem bardziej wyrafinowanych ataków ze względu na swoją pozycję na rynku, liczbę instytucji i organizacji, które wykorzystały swoje oprogramowanie i ich wyniki finansowe. Stworzono listę transakcji handlowych i TTP atakujących, aby stworzyć punkt odniesienia, w odniesieniu do którego przeprowadzono ocenę.

IstroSec wykorzystała swoją metodologię do oceny dokumentacji, procesów i technologii. Firma wdrożyła ISO 27001 i systematycznie przestrzega wszystkich wymaganych procedur. Miała też kompetentny zespół ochrony, który rygorystycznie przestrzegał procedur. Jednak podczas oceny odkryto, że bezpieczeństwo firmy koncentruje się na zgodności z przepisami i normami, ale brakowało kluczowych elementów, które pozwoliłyby reagować na rzeczywiste incydenty.

IstroSec zaproponowała 283 zmiany konfiguracji w Active Directory, środowiskach chmurowych, punktach końcowych, rozwiązaniach sieciowych i bezpieczeństwa, zarządzaniu logami i SIEM. Każda z nich był ukierunkowana na wykrywanie, zakłócanie, degradowanie lub zmylenie konkretnego TTP używanego przez atakującego i istotnego dla firmy. Odkryto również, że firma ta nie posiada skutecznych procesów w zakresie powstrzymywania incydentów bezpieczeństwa, a także wykryto pewne luki w eskalacji incydentów w celu ułatwienia właściwej reakcji. Ponadto zarekomendowano zmiany w procesach i wspierano ich wdrażanie.

Po wdrożeniu zaleceń przeprowadzono symulację ataku w celu sprawdzenia skuteczności wdrożonych mechanizmów kontrolnych.