trecom

Kompetencje Trecom w obszarze **NIS 2 i UoKSC.**

Sprawdź, jak możemy Ci pomóc!

NIS 2
BAZA WIEDZY

Wymogi NIS 2/UoKSC

1. Opracowanie i wdrożenie polityki bezpieczeństwa systemu informacyjnego i metodyki szacowania ryzyka.
2. Opracowanie i wdrożenie procesu zarządzania incydentami i innych polityk tematycznych.
3. Opracowanie i wdrożenie planów działania oraz polityk awaryjnych umożliwiających ciągłe i niezakłócone świadczenie usługi.
4. Opracowanie i wdrożenie dokumentacji określającej bezpieczeństwo łańcucha dostaw produktów, usług i procesów, w tym polityk bezpieczeństwa stron trzecich.
5. Zapewnienie bezpieczeństwa w procesie nabywania, rozwoju i utrzymania sieci i systemów.
6. Wprowadzenie polityk i procedur służących ocenie skuteczności środków zarządzania ryzykiem
7. Zapewnienie podstawowych praktyk cyberhigieny, m.in. poprzez szkolenia z zakresu cyberbezpieczeństwa
8. Wprowadzenie polityk i procedur stosowania kryptografii.
9. Przygotowanie organizacji na zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty.
10. Monitorowanie bezpieczeństwa systemów teleinformatycznych w trybie ciągłym.

Kompetencje Trecom w obszarze NIS 2 i UoKSC

0

Podpisanie umowy NDA

Od pierwszego kroku dbamy o bezpieczeństwo wymiany informacji - z wszystkimi naszymi klientami podpisujemy umowę NDA (Non-Disclosure Agreement).

1

Audyt ~ 3 miesiące

- Audyt luki NIS 2/UoKSC
- Audyt techniczny
- Testy penetracyjne (pentesty)
- Konsulting zespołu TrecomSEC

Audyt jest niezbędny, aby poznać realny stan bezpieczeństwa organizacji. Weryfikujemy zgodność z wymogami NIS 2/UoKSC oraz analizujemy infrastrukturę IT pod kątem bezpieczeństwa. Dodatkowo możemy przeprowadzić testy penetracyjne, aby ocenić odporność organizacji na cyberataki. W trakcie audytu odbywają się również konsultacje z zespołem TrecomSEC, które pozwalają uwzględnić perspektywy wszystkich stron – działu bezpieczeństwa, compliance, IT oraz Zarządu na kolejnych etapach wdrożenia.

2

Wdrożenie dokumentacji procesów i analizy ryzyka ~ 6 miesięcy

- Analiza ryzyka
- Dokumentacja SZBI (System Zarządzania Bezpieczeństwem Informacji)
- Konsulting CISOaaS
- Wdrożenie ISO27001 oraz ISO22301

Na tym etapie identyfikujemy ryzyka specyficzne dla danej organizacji, następnie je analizujemy i opracowujemy plany ich mitygacji. Dzięki temu zarówno przygotowywana dokumentacja SZBI, jak i wdrażane technologie bezpieczeństwa są skuteczne oraz dopasowane do charakteru organizacji. W ramach SZBI tworzymy polityki i procedury bezpieczeństwa dostosowane do potrzeb firmy. Oferujemy również konsulting doświadczonego CISO w ramach usługi CISOaaS. Jeśli w organizacji nie były dotychczas wdrożone normy ISO 27001 i ISO 22301, rozpoczynamy przygotowania do certyfikacji.

3

Wdrożenie technologii na podstawie audytu i analizy ryzyka ~ 9 miesięcy

- NDR, XDR, MFA
- SIEM/SOAR/UEBA
- PAM, NAC, SASE
- Backup i Disaster Recovery
- Segmentacja sieci
- Skanery podatności
- Szyfrowanie danych i zarządzanie certyfikatami

Audyt i analiza ryzyka wskazują, jakie technologie należy wdrożyć. To etap, w którym infrastruktura IT zyskuje realną warstwę ochrony, redukując podatności i ryzyko incydentów. Czas trwania tego etapu zależy od wyników audytu i liczby wdrażanych rozwiązań.

4

Szkolenia ~ 12 miesięcy

- Cyberedukacja pracowników
- Szkolenia z zarządzania bezpieczeństwem łańcucha dostaw
- Szkolenia dla Zarządu z NIS 2
- CyberBastion

Nawet najlepsze technologie nie zapewnią ochrony, jeśli pracownicy nie będą świadomi zagrożeń. Dlatego NIS 2 i UoKSC wprost narzucają obowiązek odbywania szkoleń z obszaru cyberbezpieczeństwa. Oferujemy specjalistyczne szkolenia dopasowane do grup odbiorców oraz szkolenia w formie grywalizacji na platformie CyberBastion.

5

Wdrożenie SOC i NOC ~ 3 miesiące

- Security Operations Center (SOC)
- Cyber Threat Intelligence (CTI)
- Network Operations Center (NOC)
- Utrzymanie narzędzi (RPS)

Monitorowanie w trybie ciągłym to obowiązek w świetle NIS 2 / UoKSC. Oferujemy zarówno usługę SOC, jak i NOC, dzięki czemu nasi klienci mogą w czasie rzeczywistym reagować na incydenty oraz analizować zagrożenia nie tylko w obszarze bezpieczeństwa, ale także w zakresie infrastruktury IT. Takie podejście gwarantuje utrzymanie wysokiej dostępności systemów.

6

Audyt końcowy i certyfikacja ~ 1 miesiąc

- Certyfikacja ISO27001 i ISO22301
- Certyfikacja SIM3
- Przygotowanie organizacji do audytu państwowego NIS 2.

Ostatni etap to formalne potwierdzenie, że organizacja spełnia wszystkie wymagania. Audyt końcowy i certyfikacje są nie tylko dowodem zgodności, ale też gwarancją dla partnerów biznesowych i instytucji nadzorczych, że firma działa zgodnie z najlepszymi praktykami bezpieczeństwa.

Zespół Trecom Security

Mirosław Maj

Założyciel i Prezes Fundacji Bezpieczna Cyberprzestrzeń. Były doradca Ministra Obrony Narodowej i członek Rady ds. Cyfryzacji V kadencji. Kierował zespołem CERT Polska w NASK oraz współtworzył ComCERT SA – pierwszą polską komercyjną firmę CSIRT. Wykłada cyberbezpieczeństwo na wielu uczelniach, m.in. Politechnice Warszawskiej i Wojskowej Akademii Technicznej. Współzałożyciel i członek zarządu Open CSIRT Foundation, koordynującej współpracę setek CSIRT w ramach TF-CSIRT i Trusted Introducer. Certyfikowany audytor modelu dojrzałości zarządzania incydentami bezpieczeństwa (SIM3). Audytor kilkudziesięciu CSIRT-ów w kraju i zagranicą. Uczestnik i koordynator wielu projektów międzynarodowych, w tym NATO CLOSER - wspierających budowę CSIRT-ów w krajach CIS.

Bartłomiej Śliwiński

CISO z ponad 10-letnim doświadczeniem zdobywanym w polskich i międzynarodowych firmach, w tym w Żabce oraz Allegro. Skutecznie wspiera, doradza, wdraża i współtworzy kulturę bezpieczeństwa w organizacjach z różnych gałęzi gospodarki.

Cyprian Gutkowski

Prawnik. Ekspert w zakresie ochrony danych osobowych i miękkiego cyberbezpieczeństwa. Wykładowca akademicki na studiach podyplomowych związanych z cyberbezpieczeństwem m.in. na Wojskowej Akademii Technicznej w Warszawie oraz Uniwersytecie w Białymstoku. Posiadacz certyfikatów ITIL4 oraz ISO27001. Posiada doświadczenie w prowadzeniu testów penetracyjnych, gier socjotechnicznych, wprowadzaniu polityk bezpieczeństwa i regulaminów zarządzania bezpieczeństwem informacji.

Marcin Fronczak

Certyfikowany audytor oraz ekspert w zarządzaniu ryzykiem i bezpieczeństwem IT – CISA, CIA, CRISC czy ISO 27001 LA. Ekspert od audytów bezpieczeństwa obszaru IT/OT. Wieloletnie doświadczenie na stanowisku CISO w sektorze bankowym i ubezpieczeniowym. Założyciel polskiego oddziału Cloud Security Alliance. Pierwszy w Polsce posiadacz certyfikatu bezpieczeństwa chmur Certified Cloud Security Knowledge (CCSK).

Kamil Gapiński

Ekspert z doświadczeniem w tworzeniu zespołów SOC i CERT dla różnych klientów i sektorów. Certyfikowany audytor modelu dojrzałości zarządzania incydentami bezpieczeństwa (SIM3) oraz CISM. Wykładowca w Szkole Biznesu Politechniki Warszawiej i Wyższej Szkoły Bankowej w Warszawie. Wolontariusz Fundacji Bezpieczna Cyberprzestrzeń, która promuje dobre praktyki cyberbezpieczeństwa i zwiększa świadomość zagrożeń.

Wojciech Korus

Ekspert z zakresu Cyber Threat Intelligence (CTI) z doświadczeniem w pracy w zespołach SOC i CERT. W przeszłości zajmował się analizą incydentów, bieżących zagrożeń, ataków, podatności, wycieków danych oraz utrzymaniem i rozwojem usługi CTI. Posiada kompetencje do przeprowadzania testów Recon/OSINT oraz testów socjotechnicznych.

Maciej Wroniecki

IT & Security Engineer z 25-letnim doświadczeniem, specjalizujący się w testach penetracyjnych, etycznym hackingu i doradztwie. Pracował m.in. dla Allegro i PKP. Ekspert w ekosystemie Linuksa, wierzy w automatyzację i regularne aktualizacje jako podstawy skutecznego cybersecurity.

Artur Markiewicz

Cyber Security Consultant – doradca w zakresie rozwiązań cyberbezpieczeństwa, inicjator i koordynator projektów związanych z bezpieczeństwem. Członek Zarządu ISSA Polska - Stowarzyszenia ds. Bezpieczeństwa Systemów Informacyjnych. Specjalizuje się w obszarze cyberawareness i cyberedukacji. Działa jako operator interaktywnej gry Cyber Bastion.

Wybrane partnerstwa

Security Operations Center

- Usługi 24/7/365: detekcja, analiza, reakcja, raportowanie
- Głęboka inżynieria detekcji jako fundament efektywności SOC
- Usługi profesjonalne: Cyber Threat Intelligence, analiza śledcza, pentesty, zarządzanie podatnościami, działania proaktywne
- Możliwość pracy na technologii klienta lub własnej
- Akredytacja Trusted Introducer, certyfikat ISO 27001
- Działanie wg standardów SIM3, ISO 22301, NIST, ENISA, MITRE ATT&CK

Dlaczego warto wdrożyć wymogi NIS 2/UoKSC z Trecom?

1. Identyfikujemy realne braki i rekomendujemy wdrożenie środków wymaganych przez UoKSC.

2. Pomagamy tworzyć spójną architekturę bezpieczeństwa dopasowaną do potrzeb organizacji.

3. Wdrażamy procesy i narzędzia zgodne z wynikami szacowania ryzyka.

4. Pomagamy w doborze technologii potrzebnych w kontekście UoKSC.

5. Jesteśmy partnerem w obszarze technologii, procesów i usług (w tym SOC).

6. Zapewniamy dostęp do 70+ vendorów (30+ w obszarze bezpieczeństwa) zapweniając elastyczny wybór technologii

1700+
Klientów
Doświadczenie

115+
Inżynierów
Wiedza

70+
Vendorów
Kompetencje

Potrzebujesz pomocy w obszarze NIS 2/UoKSC?

Umów się na bezpłatną konsultację i otrzymaj konkretne rekomendacje.

Jan Bręczewski

jan.breczewski@trecom.pl

+48 727 990 111

O Trecom

Jako Trecom od ponad 25 lat rozwijamy, optymalizujemy i utrzymujemy złożone systemy IT. Jesteśmy jednym z liderów rynku polskiego w segmencie sieci, cyberbezpieczeństwa, systemów AV, UC oraz data center. Nasz zespół składa się z ponad 115 inżynierów i architektów.

Posiadamy ponad 70 partnerstw technologicznych z wiodącymi dostawcami technologii oraz obszerną ofertę szkoleń. Rozbudowane portfolio rozwiązań przekłada się na niemal nieograniczone możliwości projektowe.

Nasza oferta obejmuje audyt, doradztwo, projektowanie, wdrażanie oraz utrzymywanie infrastruktury IT oraz cyberbezpieczeństwa. Wspieramy naszych klientów również poprzez usługi zarządzane – SOC, NOC i Centrum Wsparcia.

Roadmapa wdrożenia NIS 2, UoKSC w Trecom.

Terminy podane na grafice są orientacyjne.
Całkowity orientacyjny czas wdrożenia wynosi 15 miesięcy.

4. Szkolenia

- Cyberedukacja dla pracowników
- Szkolenie z zarządzania bezpieczeństwem łańcucha dostaw
- Szkolenie dla Zarządu z NIS2
- CyberBastion

12 miesięcy

3. Wdrożenie wybranych technologii na podstawie audytu i analizy ryzyka

- NDR
- XDR
- MFA
- SIEM/SOAR/UEBA
- PAM
- Segmentacja sieci
- NAC
- Backup i DR
- SASE
- Skanery podatności
- Szyfrowanie danych i zarządzanie certyfikatami
- DLP
- Cyber Deception

9 miesięcy

3 miesiące

1. Audyt (po podpisaniu NDA)

- Audyt luki NIS2
- Audyt techniczny
- Pentesty

6 miesięcy

2. Wdrożenie dokumentacji procesów i analizy ryzyka

- Przeprowadzenie analizy ryzyka
- Wdrożenie dokumentacji SZBI (System Zarządzania Bezpieczeństwem Informacji)
- Konsulting CISOaaS
- Wdrożenie ISO27001 oraz ISO22301

3 miesiące

5. Wdrożenie SOC i NOC

- SOC
- CTI
- NOC
- Utrzymanie narzędzi (RPS)

1 miesiąc

6. Audyt końcowy

- Certyfikacja ISO27001 oraz ISO22301
- Certyfikacja SIM3
- Przygotowanie organizacji do audytu państwowego NIS2