DOSTOSOWANIE UCZELNI DO WYMOGÓW DYREKTYWY NIS 2

comCERT
We Think Cybersecurity

www.comcert.pl

Spis treści

Nowe Ramy Cyberbezpieczeństwa: Dyrektywa NIS 2 i Nowelizacja UoKSC

Dyrektywa NIS 2 (Network and Information Security Directive 2) to nowy akt prawny Unii Europejskiej, który został przyjęty w celu wzmocnienia i rozszerzenia wymagań dotyczących cyberbezpieczeństwa, wprowadzonych wcześniej przez dyrektywę NIS (Network and Information Security). Wejście w życie dyrektywy NIS 2 ma na celu zwiększenie odporności podmiotów kluczowych, takich jak instytucje publiczne, przedsiębiorstwa i infrastruktura krytyczna, na cyberzagrożenia.

Nowelizacja Ustawy o Krajowym Sysytemie Cyberbezpieczeństwa (UoKSC) dostosowuje polskie prawo do wymogów wynikających z Dyrektywy NIS 2. W szczególności nowelizacja wprowadza obowiązki w zakresie zarządzania ryzykiem w cyberbezpieczeństwie na podmioty kluczowe i podmioty ważne oraz wzmacnia kompetencje organów nadzorczych właściwych do spraw cyberbezpieczeństwa. NIS 2 nakłada obowiązki na szeroką gamę podmiotów, a nowelizacja UoKSC określa, w jaki sposób przepisy te będą realizowane w Polsce.

Kluczowe cele Dyrektywy NIS 2

Dyrektywa NIS 2 ma na celu podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w całej Unii Europejskiej. Jej główne cele obejmują:

- **Zarządzania ryzykiem:**

Dyrektywa kładzie duży nacisk na zarządzanie ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych do prowadzenia działalności lub świadczenia usług i zapobieganie wpływowi incydentów na odbiorców usług lub na inne usługi, bądź minimalizowanie takiego wpływu.

- **Rozszerzenie zakresu:**

NIS 2 obejmuje więcej sektorów niż poprzednia dyrektywa NIS, w tym jednostki sektora finansów publicznych, podmioty udzielające świadczeń zdrowotnych, organizacje badawcze i uczelnie, a także inne istotne branże.

- **Zgłaszanie incydentów:**

Podmioty kluczowe i ważne będą zobowiązane do zgłaszania incydentów za pomocą systemu teleinformatycznego S46 do właściwych zespołów CSIRT sektorowych i CSIRT poziomu krajowego.

- **Większe obowiązki zarządcze**

Dyrektywa nakłada odpowiedzialność w zakresie zarządzania ryzykiem w cyberbezpieczeństwie na organy zarządzające podmiotami kluczowymi i ważnymi, w tym organy uczelni.

Ważne terminy

17 października 2024
Upłynął termin na wdrożenie dyrektywy NIS 2 przez państwa członkowskie.

2024/25
Przyjęcie nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa.

Lipiec/Sierpień 2025
Podmioty kluczowe i ważne powinny zacząć realizować swoje obowiązki.

Kogo dotyczy NIS 2?

Dyrektywa NIS 2 ma na celu osiągnięcie wysokiego, wspólnego poziomu cyberbezpieczeństwa w całej Unii Europejskiej. Podmioty, które są objęte zakresem jej stosowania, podzielono na dwie kategorie – podmioty kluczowe i podmioty ważne.

Podmioty kluczowe

Podmioty te muszą spełniać wyższe kryteria wielkości, takie jak minimum:

250	10 mln	43 mln
Członków Personelu	Obroty (w EUR)	Bilans (w EUR)

Obejmuje sektory gospodarki, takie jak:

- Energetyka: produkcja i dystrybucja energii, w tym elektryczności, ropy i gazu.
- Transport: obejmuje różne formy transportu, jak lotniczy, kolejowy, morski i drogowy.
- Bankowość i infrastruktura finansowa: banki oraz firmy oferujące usługi finansowe, np. płatności.
- Administracja publiczna: uznana za kluczową z powodu jej krytycznego znaczenia dla ochrony przed cyberzagrożeniami.
- Opieka zdrowotna: dotyczy szpitali i prywatnych klinik.
- Dostawy wody pitnej i systemy ściekowe: obejmuje zarówno zaopatrzenie w wodę, jak i odbiór ścieków.
- Przestrzeń kosmiczna: operatorzy infrastruktury naziemnej wspierający świadczenie usług kosmicznych.
- Infrastruktura cyfrowa: np. dostawcy chmur obliczeniowych i usług teleinformatycznych, w tym rejestry DNS i TLD.

Podmioty ważne

Podmioty te muszą spełniać wyższe kryteria wielkości, takie jak minimum:

50	10 mln	10 mln
Członków Personelu	Obroty (w EUR)	Bilans (w EUR)

Obejmuje sektory gospodarki, takie jak:

- Usługi pocztowe i kurierskie: obejmuje firmy zajmujące się przesyłkami i logistyką.
- Gospodarowanie odpadami: sektor podatny na cyberzagrożenia ze względu na znaczenie dla zdrowia publicznego i środowiska.
- Przemysł chemiczny: obejmuje produkcję i dystrybucję chemikaliów kluczowych dla innowacyjności i konkurencyjności Europy.
- Przemysł spożywczy: obejmuje cały łańcuch dostaw żywności, od produkcji po sprzedaż detaliczną.
- Produkcja: dotyczy produkcji urządzeń medycznych, komputerów, elektroniki, pojazdów i maszyn.
- Usługi cyfrowe: sektor obejmujący wyszukiwarki, rynki internetowe i sieci społecznościowe.
- **Badania naukowe: sektor o znaczeniu krytycznym dla postępu technologicznego i innowacji, które obejmują m.in. organizacje badawcze i uczelnie wyższe.**

Ważne! Zgodnie z Dyrektywą NIS 2 podmiotem kluczowym, niezależnie od wielkości, jest:

- dostawca usług cyfrowych
  podmiot, który świadczy określone kategorie usług cyfrowych z sektora infrastruktury cyfrowej.
- podmiot krytyczny
  mała lub średnia organizacja, zakwalifikowana przez właściwe organy krajowe jako podmiot krytyczny, w rozumieniu dyrektywy w sprawie odporności podmiotów krytycznych.

Dyrektywa NIS 2 i nowelizacja UoKSC obejmują także małe i średnie przedsiębiorstwa (MŚP), które są częścią łańcucha dostaw podmiotów kluczowych i ważnych.

Podmioty te, aby zwiększyć swoją odporność na cyberzagrożenia, muszą wprowadzać odpowiednie środki techniczne, operacyjne i organizacyjne. Środki te mają na celu zarządzanie ryzykiem związanym z bezpieczeństwem sieci i systemów informatycznych, a szczególną uwagę zwraca się na bezpieczeństwo łańcucha dostaw.

Podmioty kluczowe i ważne mają obowiązek kontroli swoich dostawców produktów, usług i procesów ICT, nawet jeśli ci nie są bezpośrednio objęci przepisami NIS 2. W konsekwencji, firmy będące częścią ich łańcucha dostaw – w tym MŚP – muszą odpowiednio dostosować się do wymagań w zakresie cyberbezpieczeństwa. Oznacza to, że MŚP, aby zachować współpracę z firmami kluczowymi lub ważnymi, są zobowiązane do wdrażania odpowiednich środków technicznych i organizacyjnych.

Mechanizm samoidentyfikacji (self-assessment)

Organizacje muszą samodzielnie ocenić, czy ich wielkość i/lub świadczone przez nie usługi sprawiają, że podlegają obowiązkowi rejestracji jako podmiot kluczowy lub ważny. Jest to mechanizm samoidentyfikacji, co oznacza, że organizacje muszą we własnym zakresie dokonać analizy swojej działalności w kontekście wymagań NIS 2 i nowelizacji UoKSC oraz ustalić, czy nowe przepisy będą ich dotyczyć.

Jeśli organizacja uzna, że kwalifikuje się jako podmiot kluczowy lub ważny, ma obowiązek zarejestrować się w rejestrze podmiotów kluczowych i ważnych, który jest prowadzony przez ministra właściwego do spraw informatyzacji. Proces ten wymaga złożenia wniosku drogą elektroniczną w terminie wyznaczonym przez ministra odpowiedzialnego za informatyzację.

Sankcje za nieprzestrzeganie NIS 2

Brak zgodności z wymogami dyrektywy NIS 2 i implementującej ją nowelizacją UoKSC może prowadzić do surowych sankcji. Obejmują one zarówno wysokie kary finansowe (do 10 milionów euro lub 2% globalnych obrotów, w zależności od tego, która suma jest wyższa), jak i odpowiedzialność indywidualną organów zarządzających. Obejmuje ona tymczasowy zakaz zajmowania kierowniczego stanowiska przez kierownika podmiotu kluczowego w tym podmiocie lub tymczasowego zakazu pełnienia funkcji zarządczych przez przedstawiciela prawnego w tym podmiocie do czasu usunięcia uchybień lub zaprzestania naruszeń.

KARY FINANSOWE

grożą za brak odpowiednich środków, niewłaściwe zarządzanie incydentami oraz brak ciągłości działania.

KARY ADMINISTRACYJNE

- Kary administracyjne obejmują m.in. zawieszenie lub ograniczenie koncesji, cofnięcie zezwolenia na prowadzenie działalności gospodarczej, zakaz zajmowania funkcji kierowniczych.

- Podmioty ważne (które mają mniejsze znaczenie niż podmioty kluczowe, ale nadal są istotne dla infrastruktury) mogą zostać obciążone administracyjną karą do 7 milionów euro lub 1,4% globalnych obrotów (w zależności od tego, która z tych kwot jest wyższa).

- Podmioty kluczowe mogą zostać ukarane administracyjną karą pieniężną do 10 milionów euro lub 2% globalnych obrotów (w zależności od tego, która z tych kwot jest wyższa).

Odpowiedzialność organów zarządzających

Kierownicy podmiotów kluczowych lub podmiotów ważnych ponoszą odpowiedzialność za wykonywanie obowiązków w zakresie cyberbezpieczeństwa przez te podmioty. Osoby zajmujące kierownicze stanowiska lub pełniące funkcje zarządcze, w tym władze uczelni, mogą ponieść indywidualną odpowiedzialność w tym zakresie. Zgodnie z aktualną wersją projektu nowelizacji UoKSC możliwe sankcje mogą obejmować m.in. zakaz pełnienia funkcji kierowniczych oraz kary pieniężne dla kierowników podmiotów kluczowych lub ważnych w wysokości do 600% otrzymywanego przez ukaranego wynagrodzenia.

UCZELNIA WYŻSZA JAKO PODMIOT WAŻNY

Uczelnie wyższe, w związku z prowadzoną działalnością badawczo-naukową i dydaktyczną, a także zarządzaniem dużymi ilościami danych osobowych, naukowych i administracyjnych muszą spełniać szereg obowiązków wynikających z dyrektywy NIS 2 i nowelizacji UoKSC.

Dyrektywa NIS 2 oraz nowelizacja UoKSC znacząco wpływają na polskie uczelnie i organizacje badawcze. Kluczowe obowiązki obejmują:

Zarządzanie ryzykiem:
Uczelnie muszą wdrożyć środki techniczne i organizacyjne, które pozwolą skutecznie zarządzać ryzykiem cyberzagrożeń. Dotyczy to zarówno ochrony systemów informatycznych, jak i danych przetwarzanych na uczelni.

Raportowanie incydentów:
Uczelnie są zobowiązane do zgłaszania incydentów cyberbezpieczeństwa do właściwych organów, np. zespołów CSIRT. Incydenty poważne muszą być zgłoszone w ciągu w ciągu 72 godzin od momentu ich wykrycia.

Ciągłość działania:
Uczelnie muszą zapewnić nieprzerwane świadczenie usług, nawet w sytuacjach kryzysowych, oraz regularnie testować i oceniać skuteczność swoich środków technicznych i organizacyjnych.

Ochrona danych:
W szczególności, w kontekście badań naukowych i przetwarzania związanych z nimi informacji, uczelnie muszą zapewnić ich bezpieczeństwo przed nieuprawnionym dostępem i modyfikacjami.

Bezpieczeństwo łańcucha dostaw:
Jeśli uczelnie współpracują z zewnętrznymi dostawcami procesów, systemów lub usług ICT (czyli z zakresu technologii informacyjnych i komunikacyjnych),mają obowiązek sprawdzić, czy ci dostawcy spełniają wymagania bezpieczeństwa zgodnie z przepisami NIS 2 zapewniając bezpieczeństwo i ciągłość łańcucha dostaw.

Wpływ dyrektywy NIS 2 oznacza, że polskie uczelnie będą musiały lepiej zabezpieczyć swoje zasoby cyfrowe, co będzie wymagało dodatkowych inwestycji w infrastrukturę ICT oraz procedury.

Wymogi Cyberbezpieczeństwa

Zarządzenie ryzykiem w cyberbezpieczeństwie

Zgodnie z projektem nowelizacji UoKSC kierownik podmiotu kluczowego lub ważnego ponosi pełną odpowiedzialność za zarządzanie ryzykiem w cyberbezpieczeństwie. Kierownik lub organ wieloosobowy kierujący organizacją ma obowiązek formalnego zatwierdzenia środków zarządzania ryzykiem oraz nadzorowania ich wdrożenia. Niewłaściwe zarządzanie lub zaniedbania, mogą prowadzić do odpowiedzialności prawnej.

Formalne zatwierdzenie środków zarządzania ryzykiem

- Wszystkie procedury, polityki i narzędzia mające na celu zarządzanie ryzykiem związanym z cyberbezpieczeństwem muszą być zatwierdzone przez odpowiednie organy uczelni.
- Zatwierdzenie to powinno być udokumentowane, a dokumentacja powinna być dostępna na potrzeby audytów wewnętrznych i zewnętrznych oraz ewentualnych kontroli.

Regularne przeglądy i nadzór nad środkami zarządzania ryzykiem

- Zarząd powinien regularnie przeglądać i aktualizować środki zarządzania ryzykiem w cyberbezpieczeństwie, aby dostosowywać je do nowych zagrożeń i zmian technologicznych.
- Przeglądy powinny być udokumentowane i przeprowadzane w oparciu o aktualne raporty z audytów bezpieczeństwa oraz testów penetracyjnych.

Odpowiedzialność organów uczelni

- Członkowie organów uczelni muszą być świadomi, że są prawnie odpowiedzialni za skuteczność środków zarządzania ryzykiem cyberbezpieczeństwa. To oznacza, że w przypadku naruszenia zabezpieczeń członkowie organów uczelni mogą zostać pociągnięci do odpowiedzialności za niedopilnowanie swoich obowiązków.

Rekomendowane wsparcie ComCERT:

Audyty i Testy Bezpieczeństwa	**Wdrażanie Rozwiązań Zabezpieczających**	**Outsourcing SOC (Security Operations Center)**
Doradztwo Prawne i Organizacyjne	**Szkolenia i Edukacja Cyberbezpieczeństwa**	**Tworzenie Polityk i Procedur Bezpieczeństwa**

Wymogi Cyberbezpieczeństwa

Regularne Szkolenia

Zgodnie z projektem nowelizacji UoKSC, kierownicy podmiotów kluczowych i ważnych, a także osoby odpowiedzialne za zarządzanie ryzykiem w cyberbezpieczeństwie, muszą przynajmniej raz w roku przechodzić szkolenie dotyczące cyberbezpieczeństwa. Szkolenie to musi podnosić świadomość w zakresie cyberbezpieczeństwa i ustawowych obowiązków. Dokumentowanie tych szkoleń oraz ich efektywności jest kluczowe dla zapewnienia zgodności z przepisami.

Regularne szkolenia

- Szkolenia powinny być organizowane przynajmniej raz w roku, zgodnie z wymogami projektu nowelizacji UoKSC. Powinny obejmować nie tylko ogólną edukację na temat zagrożeń cybernetycznych, ale także specjalistyczne szkolenia dotyczące zarządzania ryzykiem oraz obowiązków wynikających z przepisów.

Dokumentowanie uczestnictwa i postępów

- Każde szkolenie powinno być udokumentowane, w tym w zakresie uczestników, tematyki oraz efektów nauki. Dokumentacja powinna zawierać:
  - Raporty z ewaluacji postępów uczestników,
  - Ankiety po szkoleniach, które pozwolą ocenić, na ile uczestnicy zdobyli nowe umiejętności i wiedzę.
- Udokumentowanie każdego szkolenia oraz jego wyników jest kluczowe w przypadku audytów lub kontroli przeprowadzanej przez organy nadzoru.

Dostosowanie szkoleń do zmian zagrożeń

- Tematyka szkoleń powinna być aktualizowana w miarę pojawiających się nowych zagrożeń i technologii. Należy skupić się na analizie aktualnych trendów w cyberatakach, technikach ochrony oraz strategiach minimalizowania ryzyka w cyberbezpieczeństwie.

Szkolenia dla całego personelu

- Oprócz szkoleń dla organów uczelni, ważne jest także organizowanie regularnych szkoleń dla personelu, szczególnie osób zaangażowanych w zarządzanie systemami ICT i bezpieczeństwem danych. Szkolenia te powinny być zgodne z politykami bezpieczeństwa ICT uczelni.

Rekomendowane wsparcie ComCERT:

Szkolenia

Ewaluacja i Dokumentacja

Dedykowane Ćwiczenia Cyberbezpieczeństwa

Wdrażanie środków technicznych, operacyjnych i organizacyjnych

Projekt nowelizacji UoKSC określa, że podmioty kluczowe i ważne muszą wdrażać proporcjonalne środki techniczne i organizacyjne zgodne z oszacowanym ryzykiem. Środki te powinny uwzględniać:

- Koszty wdrożenia.
- Wielkość i specyfikę podmiotu.
- Prawdopodobieństwo wystąpienia incydentów oraz ich potencjalne skutki.

Szacowanie Ryzyka i Dokumentacja

Przeprowadzenie analizy ryzyka, zdefiniowanie polityk i procedur oraz wdrożenie narzędzi do monitorowania ryzyka. Dokumentacja powinna zawierać szczegółowe raporty i analizy, które mogą być przedmiotem audytów i kontroli.

Polityki Bezpieczeństwa Informacji

Organizacja powinna opracować polityki obejmujące wszystkie aspekty bezpieczeństwa informacji i zatwierdzić je na poziomie najwyższego kierownictwa.

Zarządzanie Incydentami

Ustanowienie formalnych procedur postępowania w przypadku incydentu, w tym monitorowanie systemów IT oraz reagowanie na wykryte zagrożenia.

Monitorowanie SOC (Security Operations Center)

Ustanowienie formalnych procedur postępowania w przypadku incydentu, w tym monitorowanie systemów IT oraz reagowanie na wykryte zagrożenia.

Cyber Threat Intelligence (CTI)

Używanie narzędzi do monitorowania zagrożeń, przeprowadzanie regularnych analiz oraz aktualizowanie systemów zgodnie z najlepszymi praktykami.

Wymogi Cyberbezpieczeństwa

Wdrażanie środków technicznych, operacyjnych i organizacyjnych c.d.

Planowanie Ciągłości Działania (BCP/DRP)
Opracowanie i testowanie planów BCP (Business Continuity Plan)/DRP (Disaster Recovery Plan), które zapewniają dostępność, poufność i integralność danych.

Bezpieczeństwo Łańcucha Dostaw
Organizacja musi zapewnić bezpieczeństwo łańcucha dostaw ICT, w tym monitorowanie dostawców pod kątem cyberzagrożeń.

Bezpieczeństwo Systemów ICT
Wymagane jest wdrażanie zasad projektowania i utrzymania bezpiecznych systemów, zgodnie z normami ISO.

Środki Zapobiegawcze i Ochronne
Organizacje muszą stosować środki zapobiegające incydentom, takie jak szyfrowanie danych i aktualizacje oprogramowania.

Audyt i Ocena Skuteczności
Przeprowadzanie regularnych audytów wewnętrznych oraz analiz skuteczności wdrożonych zabezpieczeń.

Audyt i Ocena Skuteczności
Przeprowadzanie regularnych audytów wewnętrznych oraz analiz skuteczności wdrożonych zabezpieczeń.

Szkolenia i Cyberhigiena
Organizowanie regularnych szkoleń z zakresu cyberbezpieczeństwa dla wszystkich członków personelu.

Kryptografia i Szyfrowanie
Niezbędne jest stosowanie środków kryptograficznych, np. do ochrony danych.

Bezpieczeństwo Zasobów Ludzkich
Organizacje muszą wdrażać zasady bezpieczeństwa dla personelu przed jego zatrudnieniem, w trakcie i po ustaniu zatrudnienia.

Ochrona Fizyczna i Kontrola Dostępu
Wdrażanie systemów kontroli dostępu oraz monitorowanie infrastruktury.

Wdrożenie MFA (Uwierzytelnianie Wieloskładnikowe)
Uwierzytelnianie wieloskładnikowe (MFA) jest wymagane do zapewnienia bezpiecznego dostępu do zasobów organizacji.

Wymogi Cyberbezpieczeństwa

Zarządzanie incydentami i raportowanie

Projekt nowelizacji UoKSC określa, że podmioty ważne, takie jak uczelnie, muszą zgłaszać poważne incydenty do właściwego CSIRT w ciągu 72 godzin od momentu ich wykrycia. Ponadto, zobowiązane są do informowania użytkowników swoich usług o incydencie poważnym, jeżeli ma on niekorzystny wpływ na świadczenie tych usług, np. na prowadzenie zajęć lub badań.

Wprowadzenie procedur raportowania incydentów

- Podmioty muszą opracować i wdrożyć formalne procedury zarządzania incydentami, które obejmują wczesne ostrzeganie i zgłaszanie poważnych incydentów do CSIRT.
- Procedury te powinny zapewniać natychmiastową reakcję i powiadamianie odpowiednich osób oraz zespołów w momencie wykrycia incydentu.
- Zgłoszenie poważnego incydentu musi zawierać wskazanie usługi zgłaszającego oraz liczbę użytkowników i zasięg geograficzny incydentu poważnego, a także wpływ na świadczenie usługi przez inne podmioty, opis przyczyn incydentu, jego przebieg oraz skutków, informacje o podjętych działaniach zapobiegawczych i naprawczych.

Dokumentacja obsługi incydentów

- Ważne jest, aby każdy podmiot prowadził szczegółową dokumentację obsługi poważnych incydentów.

Przekazywanie sprawozdań z obsługi poważnego incydentu

- Podmioty są zobowiązane do przekazywania sprawozdań z postępu obsługi incydentu do CSIRT.

Testowanie planów zarządzania incydentami

- Organizacje powinny regularnie testować swoje plany zarządzania incydentami, aby upewnić się, że są one skuteczne i aktualne. Testy te mogą obejmować symulacje incydentów, takie jak ataki typu ransomware lub wycieki danych, które sprawdzą gotowość organizacji do szybkiego reagowania i zgłaszania incydentów.
- Testowanie umożliwia także identyfikację luk w systemie oraz ulepszanie procedur.

Rekomendowane wsparcie ComCERT:

Doradztwo w Zarządzaniu Incydentami	**Wsparcie w Raportowaniu do CSIRT**	**Outsourcing SOC (Security Operations Center)**
Testy Penetracyjne	**Zarządzanie Kryzysowe**	**Analiza Powłamaniowa**

Jak ComCERT może wesprzeć podmioty w realizacji tych obowiązków:

ISO/IEC 27001

ComCERT wspiera organizacje we wdrożeniu normy ISO 27001, która zapewnia systematyczne zarządzanie bezpieczeństwem informacji. Certyfikacja ta ułatwia także spełnienie wymogów dyrektywy NIS 2, dzięki zgodności z kluczowymi wymaganiami w zakresie ochrony danych i zarządzania ryzykiem.

ComCERT, jako ekspert w obszarze cyberbezpieczeństwa, oferuje kompleksowe usługi, które wspierają organizacje, w tym uczelnie wyższe i inne podmioty kluczowe, w spełnieniu wymagań wynikających z Dyrektywy NIS 2 oraz nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (UoKSC). Poniżej przedstawiamy kluczowe usługi, które adresują konkretne wymogi i mogą pomóc w ich skutecznej realizacji.

Bezpieczeństwo Łańcucha Dostaw

- Konsulting w zakresie umów z dostawcami i podwykonawcami
- Audyty bezpieczeństwa środowiska deweloperskiego

Zarządzanie Incydentami

- Opracowanie procedur zarządzania incydentami
- Outsourcing SOC 1,2,3 Linii
- Usługa C3TI (Cyber Threat Intelligence)

Szacowanie Ryzyka i Zarządzanie Ryzykiem

- Wsparcie w wyborze metodyki i narzędzi szacowania ryzyk
- Opracowanie Polityki Bezpieczeństwa Informacji (PBI)
- Wsparcie w opracowaniu Business Impact Analysis (BIA), oceny ryzyka oraz planów BCP/DRP

Audyty, Testy i Przeglądy Bezpieczeństwa

- Realizacja testów podatności i penetracyjnych
- Audyty bezpieczeństwa, przeglądy konfiguracji oraz testy penetracyjne

Projektowanie i Wdrażanie Systemów Cyberbezpieczeństwa

ComCERT dostarcza swoim klientom sprawdzone rozwiązania bezpieczeństwa. Dzięki współpracy i autoryzacji wiodących producentów oferujemy usługi w modelu multi-vendor, czyli wykluczające ryzyko vendor-lock. Obszar naszej specjalizacji obejmuje między innymi systemy klasy

VPN | WAF | DAM | EDR | DLP | SIEM | SOAR

comCERT
We Think Cybersecurity

Chcesz podnieść cyberbezpieczeństwo w swojej organizacji?

Opowiedz nam o swoich potrzebach, a zaproponujemy najlepsze rozwiązanie. Skontaktuj się nami!

Marcin Matusiak
Key Account Manager

+48 502 310 794

marcin.matusiak@comcert.pl

www.comcert.pl

ul. A. Branickiego 13
02-972 Warszawa