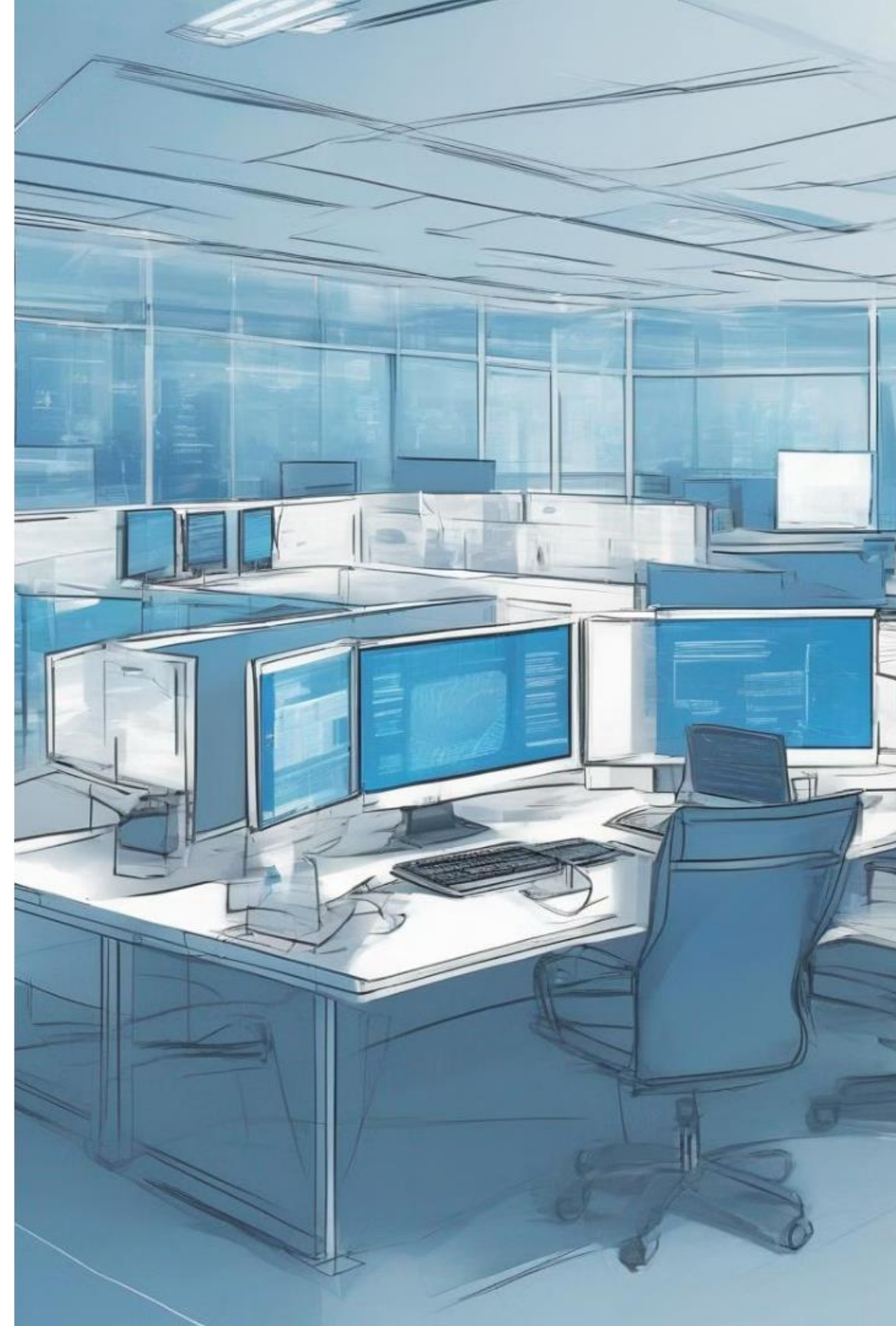


**Efektywne zarządzanie cyberbezpieczeństwem  
w jednostkach sektora finansów publicznych**



## Wprowadzenie do Dyrektywy NIS2



### Dyrektywa NIS2

Dyrektywa NIS2 to kluczowe narzędzie regulacyjne dla jednostek sektora finansów publicznych, wprowadzające szereg zmian mających na celu zwiększenie odporności na zagrożenia cybernetyczne.

### Zarządzanie ryzykiem

Jednostki sektora finansów publicznych będą zobowiązane do systematycznego monitorowania ryzyka cybernetycznego oraz wdrażania odpowiednich środków zabezpieczających.

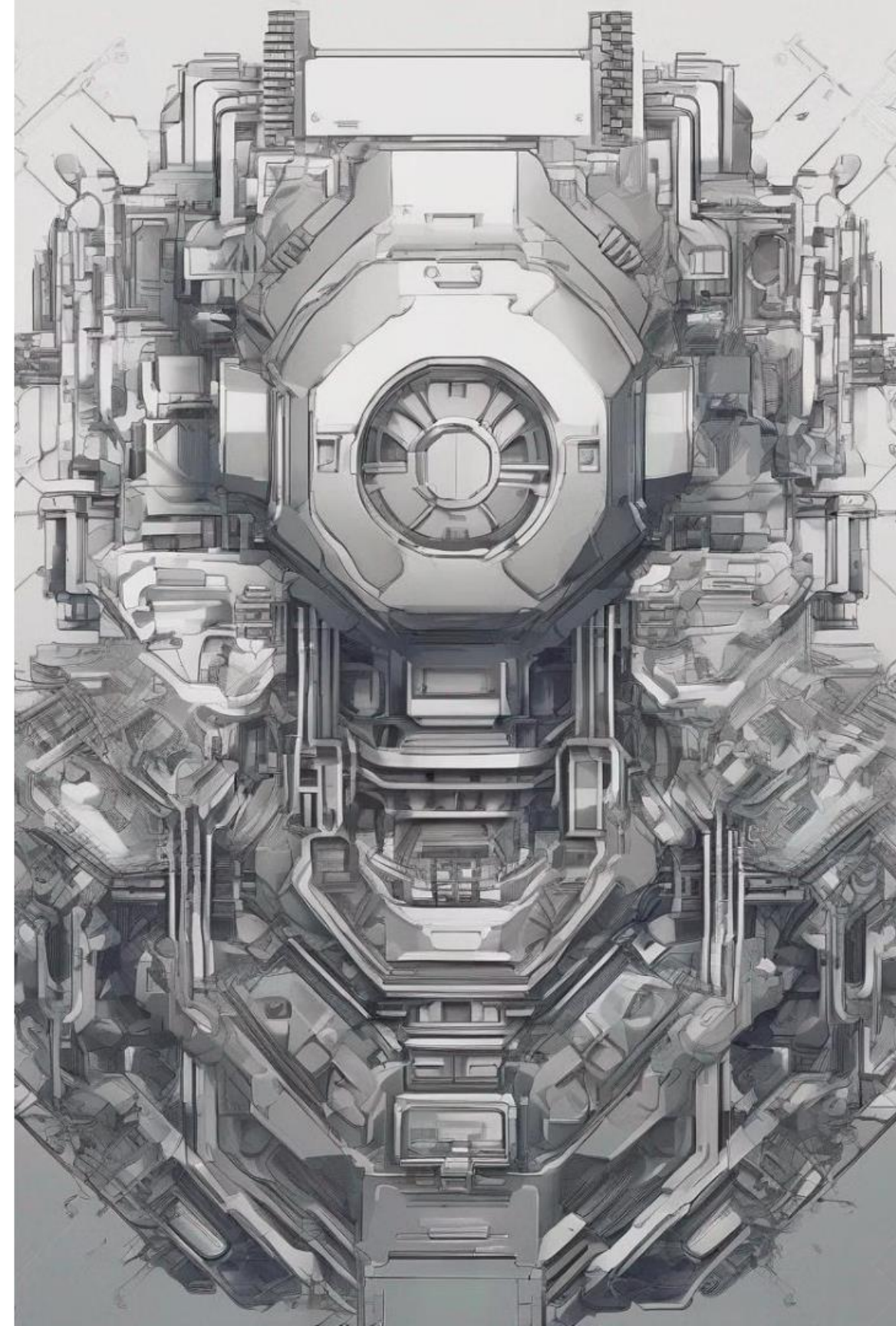
### Reagowanie na incydenty

Dyrektywa NIS2 nakłada na organizacje obowiązek posiadania skutecznych procedur reagowania na incydenty cybernetyczne.

Dyrektywa NIS2 to kluczowy element regulacyjny, który ma na celu zwiększenie odporności jednostek sektora finansów publicznych na zagrożenia cybernetyczne.

Dyrektywa ta wprowadza szereg nowych wymogów i obowiązków dla jednostki z sektora finansów publicznych, takich jak systematyczna ocena ryzyka, wdrażanie środków ochronnych, posiadanie procedur reagowania na incydenty oraz współpraca międzynarodowa w zakresie wymiany informacji o zagrożeniach.

Głównym celem Dyrektywy NIS2 jest zwiększenie cyberbezpieczeństwa w jednostkach sektora finansów publicznych, które ze względu na swoją strategiczną rolę są szczególnie narażone na zagrożenia cybernetyczne. Nowe regulacje mają zapewnić lepsze przygotowanie tych instytucji na potencjalne ataki i incydenty, a tym samym zwiększyć ich odporność na skutki takich zdarzeń.



# Dyrektywa NIS2 - Kluczowe narzędzie dla cyberbezpieczeństwa w sektorze finansów publicznych

Dyrektywa NIS2 to kluczowy element regulacyjny, który ma na celu zwiększenie odporności jednostek sektora finansów publicznych na zagrożenia cybernetyczne. Wprowadza ona szereg zmian, które znacząco wpływają na zarządzanie bezpieczeństwem informacji i ochronę danych wrażliwych.

Głównym celem Dyrektywy NIS2 jest zapewnienie wysokiego poziomu cyberbezpieczeństwa w całej Unii Europejskiej. Wymusza ona na organizacjach sektora publicznego implementację spójnych i skutecznych środków zabezpieczających infrastrukturę informatyczną, a także procedur reagowania na incydenty.

Regulacje te mają na celu zapewnienie jednolitych standardów i procedur w całym sektorze, co przyczyni się do zwiększenia ogólnego bezpieczeństwa. Dyrektywa NIS2 wymusza również ścisłą współpracę między instytucjami oraz organami nadzoru, aby umożliwić szybkie i efektywne reagowanie na zagrożenia.

# Główne cele Dyrektywy NIS2 dla sektora finansów publicznych

Głównym celem Dyrektywy NIS2 jest wzmocnienie mechanizmów bezpieczeństwa cybernetycznego w sektorze finansów publicznych poprzez ustanowienie spójnych i kompleksowych ram regulacyjnych. Dyrektywa ta dąży do stworzenia jednolitego podejścia do ochrony przed zagrożeniami cybernetycznymi, co ma kluczowe znaczenie w kontekście rosnącej liczby i złożoności cyberataków. Dzięki wprowadzeniu jednolitych standardów, instytucje finansowe w sektorze publicznym będą mogły lepiej współpracować oraz wymieniać się informacjami i najlepszymi praktykami w zakresie cyberbezpieczeństwa.

**Wzmocnienie zarządzania ryzykiem i reagowania na incydenty** - Dyrektywa NIS2 nie tylko definiuje ogólne zasady, ale również wprowadza szczegółowe wymagania dotyczące zarządzania ryzykiem oraz reagowania na incydenty cybernetyczne. Nowe standardy i procedury, które muszą zostać wdrożone, mają na celu minimalizację ryzyka ataków oraz skuteczną ochronę kluczowych instytucji finansowych przed potencjalnymi zagrożeniami.

**Promowanie kultury bezpieczeństwa i podnoszenie świadomości** - Wprowadzenie Dyrektywy NIS2 ma również na celu zwiększenie odporności sektora finansów publicznych na incydenty cybernetyczne poprzez promowanie kultury bezpieczeństwa oraz podnoszenie świadomości w zakresie zagrożeń cybernetycznych. Instytucje finansowe są zobowiązane do regularnego szkolenia swoich pracowników oraz do implementacji zaawansowanych systemów monitorowania i wykrywania zagrożeń.

**Wzmocnienie współpracy międzynarodowej** - Dodatkowo, Dyrektywa NIS2 wprowadza mechanizmy współpracy między państwami członkowskimi Unii Europejskiej, co umożliwi szybsze i bardziej efektywne reagowanie na transgraniczne zagrożenia cybernetyczne. Dzięki temu możliwe jest skoordynowane działanie w obliczu poważnych incydentów, co znacznie zwiększa poziom ochrony na poziomie międzynarodowym.



## Ocena Ryzyka

Jednostki sektora finansów publicznych muszą regularnie oceniać ryzyka cybernetyczne i wdrażać odpowiednie środki zabezpieczające.



## Reagowanie na Incydenty

Dyrektywa NIS2 określa wymagane procedury wykrywania, analizowania i naprawiania incydentów cybernetycznych.



## Środki Zabezpieczające

Instytucje są zobowiązane do wdrożenia adekwatnych środków ochrony systemów informatycznych.

# Audyty, edukacja i reagowanie na incydenty w sektorze finansów publicznych

**Częstsze audyty bezpieczeństwa** - Dyrektywa NIS2 znacząco zwiększa obowiązek przeprowadzania regularnych audytów bezpieczeństwa w jednostkach sektora finansów publicznych. Audyty mają zapewnić stałe monitorowanie ciągłości działania oraz identyfikację wszelkich słabych punktów w systemach informatycznych.

**Podniesienie świadomości pracowników** - Nowe regulacje wymagają intensywnych szkoleń oraz kampanii informacyjnych dla pracowników, aby zwiększyć ich wiedzę na temat zagrożeń cybernetycznych. Pozwoli to ograniczyć ryzyko incydentów spowodowanych błędami ludzkimi.

**Skuteczne reagowanie na incydenty** - Dyrektywa nakłada obowiązek posiadania jasnych procedur reagowania na incydenty, w tym szybkiego wykrywania, analizy i naprawiania zagrożeń. Celem jest minimalizacja skutków incydentów i przywrócenie normalnego funkcjonowania.

**Transparentność w raportowaniu** - Instytucje muszą systematycznie raportować wszelkie zidentyfikowane luki w systemach, aby umożliwić szybkie ich usuwanie i doskonalenie strategii bezpieczeństwa.

# Wymagania Dyrektywy NIS2 dla sektora finansów publicznych

Dyrektywa NIS2 nakłada na podmioty sektora finansów publicznych szereg kluczowych obowiązków w celu zwiększenia odporności na cyberzagrożenia. Kluczowe wymagania to wdrożenie zaawansowanych środków zarządzania ryzykiem, ciągłe monitorowanie środowiska IT oraz szybkie i skuteczne reagowanie na incydenty cybernetyczne.

Instytucje muszą przeprowadzać regularne oceny ryzyka, wdrażać odpowiednie środki ochronne oraz implementować systemy monitorowania aktywności w sieciach informatycznych. Szybka identyfikacja i analiza incydentów, a także przywrócenie normalnego funkcjonowania to kolejne kluczowe obowiązki.

Ponadto, podmioty zobowiązane są do regularnego raportowania incydentów i luk w zabezpieczeniach, aby zwiększyć transparentność i umożliwić doskonalenie strategii cyberbezpieczeństwa w sektorze finansów publicznych.

# Podmioty zobowiązane do stosowania Dyrektywy NIS2 w sektorze finansów publicznych

Dyrektywa NIS2 nakłada obowiązki w zakresie cyberbezpieczeństwa na instytucje finansowe, takie jak banki i fundusze inwestycyjne, **jednostki sektora finansów publicznych** oraz **dostawców usług cyfrowych** świadczących usługi na rzecz tego sektora. Te podmioty muszą wdrażać zaawansowane środki ochrony, przestrzegać rygorystycznych standardów bezpieczeństwa IT oraz regularnie raportować incydenty i związane z nimi ryzyko.

Jednostki sektora finansów publicznych jako te odpowiedzialne za zarządzanie i ochronę danych publicznych muszą stosować się do określonych wymagań Dyrektywy NIS2. Obejmuje to nie tylko środki techniczne, ale także **procedury organizacyjne** zapewniające ciągłość działania i ochronę danych przed nieuprawnionym dostępem. Podmioty te zobligowane są również do **współpracy z organami nadzoru** w przypadku incydentów cybernetycznych.

# Monitorowanie ryzyka w jednostkach sektora finansów publicznych



## Analiza ryzyka

Systematyczna identyfikacja zagrożeń i ocena ryzyka jest kluczowa dla skutecznej strategii cyberbezpieczeństwa.



## Rozwiązania zapobiegawcze

Wdrażanie zaawansowanych zabezpieczeń, takich jak zapory, systemy wykrywania włamań i mechanizmy szyfrowania, minimalizuje ryzyko.



## Szkolenia dla pracowników

Regularne szkolenia pomagają zapewnić, że wszyscy pracownicy są świadomi potencjalnych zagrożeń i wiedzą, jak reagować.

# Zarządzanie incydentami w jednostkach sektora finansów publicznych



## Identyfikacja incydentów

Zaawansowane systemy monitorowania wykrywają podejrzane działania w czasie rzeczywistym, wykorzystując technologie AI i uczenie maszynowe.



## Analiza incydentów

Specjaliści ds. bezpieczeństwa stosują narzędzia analityczne i techniki forensyczne, aby odtworzyć przebieg incydu i zidentyfikować jego przyczyny.



## Reakcja na incydenty

Jednostki mają opracowane procedury określające kroki do podjęcia, takie jak izolacja systemów i przywrócenie danych, w celu minimalizacji skutków incydu.



## Przywrócenie funkcjonowania systemów

Posiadanie planów ciągłości działania (BCP) i planów odzyskiwania danych (DRP) umożliwia szybkie przywrócenie normalnej pracy po incydencie.



## Dokumentacja i analiza po incydencie

# Definicja incydentu w kontekście Dyrektywy NIS2

Zgodnie z Dyrektywą NIS2, incydent to każde niepożądane zdarzenie, które **ma lub może mieć negatywny wpływ na bezpieczeństwo infrastruktury informacyjnej**. Incydenty te mogą obejmować różnorodne zagrożenia, zarówno **zewnętrzne, jak i wewnętrzne**, które mogą zakłócić funkcjonowanie systemów informatycznych oraz wpłynąć na **integralność, poufność i dostępność danych finansowych**.

Przykłady incydentów mogą obejmować ataki hakerskie, awarie sprzętowe, błędy ludzkie, działanie złośliwego oprogramowania lub cyberprzestępczość. Każde z tych zdarzeń ma potencjał, by naruszyć kluczowe aspekty bezpieczeństwa informacji, takie jak dostępność danych, ich integralność czy poufność. Sprawna identyfikacja i reakcja na tego typu incydenty jest kluczowa dla zapewnienia ciągłości działania jednostek sektora finansów publicznych.

Dyrektywa NIS2 nakłada na te podmioty obowiązek posiadania odpowiednich procedur oraz planów awaryjnych, które umożliwią skuteczne zarządzanie i ograniczenie skutków incydentów. Jednym z głównych celów Dyrektywy jest właśnie wzmocnienie odporności sektora na cyberataki i inne zagrożenia, które mogłyby zakłócić kluczowe usługi finansowe.



# Procedury reagowania na incydenty w jednostkach sektora finansów publicznych

Jednostki sektora finansów publicznych powinny posiadać szczegółowe procedury reagowania na incydenty, które określają kroki do podjęcia w celu zminimalizowania szkód i szybkiego przywrócenia normalnego funkcjonowania systemów informatycznych. **Te procedury są kluczowe dla skutecznego zarządzania incydentami cybernetycznymi i zapewnienia ciągłości operacyjnej.** Aby były one skuteczne, muszą być regularnie testowane i aktualizowane, uwzględniając dynamicznie zmieniające się zagrożenia oraz nowe technologie.

Pierwszy krok to **szybka identyfikacja incydentu** przy użyciu systemów monitorowania i wykrywania, takich jak systemy wykrywania włamań (IDS), zapory ogniowe (firewalle) oraz narzędzia do analizy ruchu sieciowego. Następnie **ocena i klasyfikacja incydentu** pozwala na określenie priorytetów działań oraz alokację odpowiednich zasobów.

Kolejne kroki to **izolacja incydentu** w celu zapobiegania jego rozprzestrzenianiu się, **analiza i eliminacja** zagrożenia oraz **przywrócenie normalnego funkcjonowania systemów** przy użyciu planów odzyskiwania po awarii (DRP) i planów ciągłości działania (BCP).

Na koniec ważna jest **dokumentacja i analiza po incydencie**, która pozwala na ocenę skuteczności podjętych działań oraz identyfikację obszarów do poprawy. **Regularne testowanie i aktualizowanie procedur** zapewnia ich skuteczność w obliczu nowych zagrożeń.

# Raportowanie i analiza incydentów cybernetycznych



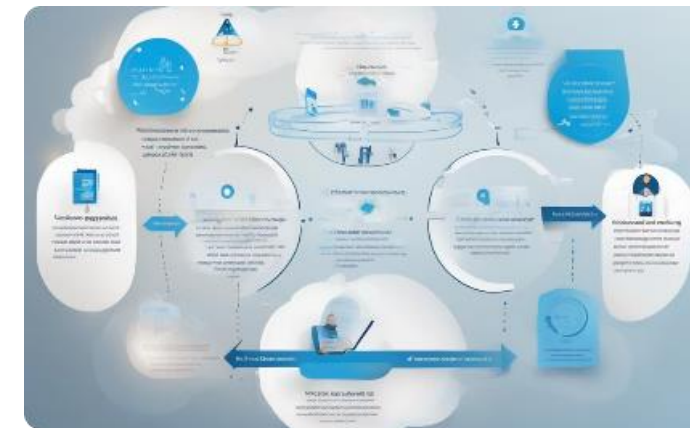
## Proces Raportowania Incydentów

Jednostki sektora muszą posiadać jasne procedury raportowania incydentów, zapewniając szybką reakcję, określone kanały komunikacji i odpowiedzialność.



## Rodzaje Incydentów

Procedury raportowania powinny uwzględniać różne rodzaje incydentów, takie jak włamania, wycieki danych, ataki DDoS czy oprogramowanie ransomware.



## Analiza i Doskonalenie

Analiza zgłoszonych incydentów pozwala na identyfikację trendów i ocenę skuteczności działań, a także podejmowanie działań prewencyjnych na przyszłość.

# Wdrażanie Środków Ochrony

- Ustanowienie **kompleksowych procedur** reagowania na incydenty cyberbezpieczeństwa w jednostkach sektora finansów publicznych
- Wdrożenie **zaawansowanych narzędzi monitorujących** i wykrywających zagrożenia, takich jak systemy IPS, firewalle i analiza ruchu sieciowego
- Zapewnienie **regularnych szkoleń** dla pracowników w zakresie cyberbezpieczeństwa i postępowania w obliczu incydentów
- Stworzenie **przejrzystych ścieżek raportowania** incydentów i odpowiedzialności za ich rozwiązywanie
- Systematyczne **testowanie i aktualizowanie** procedur reagowania na incydenty, zgodnie z nową specyfiką zagrożeń



# Współpraca międzynarodowa w cyberbezpieczeństwie sektora finansów publicznych

Dyrektywa NIS2 nakłada na organizacje sektora finansów publicznych obowiązek aktywnej międzynarodowej wymiany informacji o zagrożeniach i incydentach cybernetycznych. Wymiana danych, wspólne operacje oraz konsultacje z instytucjami międzynarodowymi są kluczowe dla budowania globalnego ekosystemu cyberbezpieczeństwa i skutecznej ochrony przed cyberatakami.

**Aktywna wymiana informacji** obejmuje regularne dzielenie się danymi o incydentach, nowych zagrożeniach oraz najlepszych praktykach bezpieczeństwa z innymi państwami członkowskimi UE i organizacjami międzynarodowymi.

**Koordinacja działań** polega na udziale w międzynarodowych ćwiczeniach, wspólnych operacjach oraz wymianie zasobów, aby zwiększyć gotowość i efektywność reagowania na incydenty.

**Współpraca z instytucjami** takimi jak ENISA, Europol czy inne agencje ds. cyberbezpieczeństwa oferuje jednostkom sektora finansów publicznych konsultacje, szkolenia oraz wsparcie w projektach badawczych.

Korzyści ze współpracy międzynarodowej to **szybsze wykrywanie zagrożeń, lepsza ochrona danych, zwiększenie odporności oraz rozwój kompetencji pracowników.**

# Wymiana informacji w ramach Dyrektywy NIS2



## Regularna wymiana informacji

Organizacje sektora finansów publicznych będą zobowiązane do raportowania incydentów i udostępniania danych o nowych zagrożeniach na dedykowanych platformach i forach.



## Analiza zebranych danych

Współpraca w zakresie analizy danych pozwoli na lepsze zrozumienie zagrożeń i opracowanie skuteczniejszych środków ochrony.



## Mechanizmy wymiany informacji

Dyrektywa NIS2 promuje różnorodne mechanizmy wymiany informacji, takie jak grupy robocze, fora i konferencje, wzmacniające współpracę i budujące zaufanie.

# Współpraca międzynarodowa w cyberbezpieczeństwie sektora finansów publicznych

Organizacje partnerskie odgrywają kluczową rolę we współpracy międzynarodowej w sektorze finansów publicznych. Współpraca z partnerami zagranicznymi, instytucjami europejskimi oraz organizacjami międzynarodowymi umożliwia wymianę know-how, najlepszych praktyk oraz wzajemne wsparcie w zakresie zapobiegania incydom cybernetycznym oraz reagowania na nie. Taka współpraca jest niezbędna do budowania silnego, globalnego ekosystemu cyberbezpieczeństwa.

**Partnerzy zagraniczni** to rządy innych krajów, instytucje finansowe oraz organizacje sektora prywatnego. Umożliwiają one *wymianę informacji o zagrożeniach, wspólne opracowywanie standardów bezpieczeństwa oraz wdrażanie zaawansowanych technologii ochrony.*

**Instytucje europejskie**, takie jak ENISA, odgrywają kluczową rolę w *koordynowaniu działań, prowadzeniu wspólnych projektów badawczych oraz wymianie informacji o incydentach.* Współpraca z nimi pozwala na lepsze przygotowanie się na cyberzagrożenia.

**Organizacje międzynarodowe**, w tym CERTs, Europol oraz ISACs, wspierają sektor finansów publicznych w *szybkiej reakcji na incydenty, analizowaniu zagrożeń oraz koordynacji działań przeciwko cyberprzestępczości.*





# Audyty cyberbezpieczeństwa w sektorze finansów publicznych

Regularne przeprowadzanie **audytów bezpieczeństwa** oraz **oceny ryzyka** są kluczowe, aby zapewnić, że systemy i procedury informatyczne sektora finansów publicznych spełniają najwyższe standardy ochrony przed **cyberzagrożeniami**. Audyty obejmują całościową weryfikację infrastruktury IT, procedur i polityk bezpieczeństwa oraz zarządzania dostępem.

Audyty przeprowadzane są **co najmniej raz w roku**, a także **po wystąpieniu incydentów** oraz **w formie audytów tematycznych**. Ich celem jest **wykrywanie słabych punktów** poprzez testy penetracyjne, analizę podatności i ocenę ryzyka. Następnie wdrażane są **środki zaradcze**, takie jak aktualizacje, zmiany konfiguracji oraz szkolenia pracowników.

# Audyty cyberbezpieczeństwa w sektorze finansów publicznych



## Planowanie i Przygotowanie

Audyty cyberbezpieczeństwa w sektorze finansów publicznych rozpoczynają się od dokładnego planowania i przygotowania. Ten etap jest kluczowy, aby zapewnić kompleksową ocenę systemów i infrastruktury IT. Obejmuje on analizę istniejących procedur, polityk bezpieczeństwa oraz zidentyfikowanie kluczowych systemów i danych.



## Testy Penetracyjne

Przeprowadzane testy penetracyjne pozwalają na identyfikację rzeczywistych słabych punktów i ocenę faktycznego poziomu zabezpieczeń. Eksperti symulują ataki, wykorzystując najnowsze techniki i narzędzia stosowane przez hakerów, aby zweryfikować skuteczność istniejących środków ochrony.



## Analiza i Raportowanie

Analiza wyników audytu i przygotowanie kompleksowych raportów to kluczowe etapy procesu. Raporty zawierają szczegółowe informacje na temat zidentyfikowanych luk w zabezpieczeniach, rekomendacje dotyczące niezbędnych środków zaradczych oraz ocenę poziomu ryzyka.



## Wdrażanie Środków Zaradczych

Po przeprowadzeniu audytu niezwłocznie należy wdrożyć odpowiednie środki zaradcze, aby podnieść poziom cyberbezpieczeństwa w sektorze finansów publicznych. Może to obejmować aktualizacje oprogramowania, zmiany konfiguracji systemów, wdrożenie nowych narzędzi ochrony oraz szkolenia pracowników.

# Przykłady incydentów

Sektor finansów publicznych stoi w obliczu różnorodnych zagrożeń związanych z cyberbezpieczeństwem. Poniżej przedstawiamy kilka przykładów poważnych incydentów, z jakimi musiały się zmierzyć instytucje publiczne:

1. Włamania do systemów IT **jednostek sektora finansów publicznych** prowadzące do kradzieży danych osobowych lub środków finansowych. Te ataki mogą mieć poważne konsekwencje, takie jak wyciek poufnych informacji, straty finansowe oraz zakłócenia w działaniu urzędów.
2. Masowe **ataki typu ransomware** paraliżujące pracę urzędów i instytucji publicznych oraz uniemożliwiające dostęp do kluczowych zasobów. Takie incydenty powodują przestoje w świadczeniu usług publicznych, co negatywnie wpływa na obywateli.
3. Wykradzenie poufnych **informacji o klientach** lub kontrahentach instytucji sektora finansów publicznych przez hakerów. Może to prowadzić do naruszeń prywatności, utraty zaufania oraz potencjalnych kar dla organizacji.
4. Awarie **krytycznej infrastruktury IT** jednostek sektora finansów publicznych, prowadzące do zakłóceń w działalności. Przestoje w systemach teleinformatycznych mogą uniemożliwić realizację kluczowych procesów w instytucjach publicznych.
5. Rozpowszechnianie **falszywych informacji** atakujących wizerunek i reputację instytucji sektora finansów publicznych. Takie działania mogą prowadzić do utraty zaufania obywateli oraz negatywnie wpływać na funkcjonowanie organizacji.

# Wytyczne dla audytów

Regularna ocena stanu cyberbezpieczeństwa jednostek sektora finansów publicznych jest kluczowa dla skutecznego wdrażania Dyrektywy NIS2. Wytyczne dotyczące audytów obejmują kompleksową analizę podatności, weryfikację zgodności z normami, ocenę skuteczności środków ochrony oraz identyfikację obszarów wymagających poprawy.

Kompleksowa analiza podatności powinna obejmować szczegółową ocenę zagrożeń i słabych punktów w infrastrukturze IT oraz procesach organizacyjnych. Pozwoli to zidentyfikować kluczowe ryzyka, które mogą negatywnie wpłynąć na bezpieczeństwo informacji w jednostkach sektora finansów publicznych.

Weryfikacja zgodności z normami jest niezbędna, aby upewnić się, że jednostka spełnia wszystkie wymogi Dyrektywy NIS2 w zakresie zarządzania ryzykiem i reagowania na incydenty. Audyt powinien sprawdzić, czy wdrożone zostały odpowiednie polityki, procedury i kontrole, zapewniające zgodność z obowiązującymi przepisami.

Ocena skuteczności środków ochrony to analiza, czy wdrożone rozwiązania techniczne i organizacyjne w zakresie cyberbezpieczeństwa faktycznie minimalizują zidentyfikowane ryzyka. Audyt powinien zweryfikować, czy zastosowane mechanizmy są skuteczne i odpowiednie do specyfiki danej organizacji.

Identyfikacja obszarów wymagających poprawy pozwoli na sformułowanie rekomendacji i planu działań naprawczych. Dzięki temu jednostki sektora finansów publicznych będą mogły wdrożyć niezbędne usprawnienia, zwiększając poziom cyberbezpieczeństwa i spełniając wymagania Dyrektywy NIS2.

# Rola personelu IT



## **Eksperci ds. cyberbezpieczeństwa**

Odpowiedzialni za ocenę ryzyka, wdrożenie środków ochrony oraz reagowanie na incydenty.



## **Podnoszenie kompetencji**

Szkolenia i podnoszenie kompetencji personelu IT to istotny element zwiększenia poziomu cyberbezpieczeństwa w organizacji.



## **Współpraca z kadłą zarządzającą**

Ścisła współpraca pomiędzy działami IT a kadłą zarządzającą pozwoli na skuteczne wdrożenie wymagań Dyrektywy NIS2.

# Rola zarządu



## Wiodąca rola w wdrażaniu wymagań

Zarząd musi zapewnić skuteczne wdrożenie środków ochrony oraz procedur reagowania na incydenty w jednostce.



## Zapewnienie odpowiednich zasobów

Zarząd powinien zagwarantować wystarczające fundusze, kompetentny personel oraz niezbędne narzędzia i technologie.



## Nadzór nad realizacją zadań

Monitorowanie przez kadrę kierowniczą procesu oceny ryzyka, audytów oraz reagowania na incydenty jest kluczowe.



## Odpowiedzialność za zapewnienie zgodności

Zarząd ponosi ostateczną odpowiedzialność za przestrzeganie przez jednostkę wszystkich wymogów Dyrektywy NIS2.

# Potencjalne skutki incydentów

Incydenty cyberbezpieczeństwa mogą mieć poważne konsekwencje dla jednostek sektora finansów publicznych. Jednym z głównych zagrożeń są **straty finansowe**, które mogą wynikać z kosztów naprawy szkód, wypłacania odszkodowań oraz utraty przychodów spowodowanej przestojami w działalności.

Innym kluczowym ryzykiem jest **naruszenie bezpieczeństwa danych**. Wycieki poufnych informacji, a także naruszona integralność danych, mogą prowadzić do poważnych konsekwencji prawnych i utraty zaufania do organizacji.

Cyber-ataki często skutkują także **przerwami w działalności** jednostki, co z kolei przekłada się na zakłócenia w świadczeniu kluczowych usług publicznych. Tego typu przestoje mogą mieć dotkliwe skutki zarówno dla pracowników, jak i obywateli korzystających z tych usług.

Jednym z najbardziej dotkliwych skutków incydentów jest **utrata zaufania** do organizacji. Negatywny wizerunek, jaki może zostać wytworzony w wyniku skutecznego ataku, znacząco utrudni dalszą współpracę z interesariuszami.

Ponadto jednostki sektora finansów publicznych narażone są na wysokie **kary i sankcje** nakładane przez organy regulacyjne w przypadku nieprzestrzegania przepisów dot. cyberbezpieczeństwa, w tym Dyrektywy NIS2. Postępowania sądowe i towarzyszące im koszty mogą mieć niekorzystny wpływ na całokształt działalności organizacji.



# Rola audytorów

Audytorzy pełnią kluczową rolę w zapewnieniu zgodności jednostek sektora finansów publicznych z wymogami Dyrektywy NIS2. Ich zadaniem jest kompleksowa ocena stanu cyberbezpieczeństwa organizacji oraz identyfikacja luk i obszarów wymagających poprawy.

Na podstawie szczegółowych analiz środków ochrony, procedur reagowania na incydenty oraz stopnia wdrożenia wymagań regulacyjnych, audytorzy doradzają kadrze zarządczej w zakresie wzmocnienia cyberochrony i minimalizowania ryzyka.

# Ocena Ryzyka w Jednostkach Sektora Finansów Publicznych

Ocena ryzyka w obszarze cyberbezpieczeństwa jest kluczowym elementem zapewnienia bezpieczeństwa infrastruktury informatycznej i danych w jednostkach sektora finansów publicznych. Proces ten obejmuje identyfikację zagrożeń, analizę prawdopodobieństwa ich wystąpienia oraz ocenę potencjalnych skutków. Dzięki temu można opracować skuteczne strategie ochrony i środki zaradcze, które minimalizują ryzyko i konsekwencje ataków cybernetycznych.

Etapy oceny ryzyka obejmują: identyfikację zagrożeń zewnętrznych i wewnętrznych, analizę podatności, ocenę wpływu na operacje i reputację, a także ocenę gotowości organizacji do reagowania na incydenty. Na tej podstawie opracowuje się strategie wzmacniania zabezpieczeń, zarządzania dostępem, szkoleń personelu oraz procedur reagowania i ciągłości działania.

Identyfikacja zagrożeń to pierwszy krok w procesie oceny ryzyka cybernetycznego. Obejmuje ona analizę potencjalnych źródeł ataków, takich jak złośliwe oprogramowanie, włamanie do systemów, wycieki danych czy ataki na infrastrukturę krytyczną. Kluczowe jest tu również zrozumienie słabych punktów organizacji, które mogą być wykorzystywane przez cyberprzestępców.

Kolejnym etapem jest analiza prawdopodobieństwa wystąpienia zidentyfikowanych zagrożeń. Uwzględnia się tutaj czynniki takie jak częstotliwość występowania podobnych incydentów w przeszłości, skuteczność istniejących zabezpieczeń oraz ogólny poziom zagrożenia w danym sektorze. Ta część oceny pozwala skoncentrować się na priorytetowych obszarach ryzyka.

Ostatnim, ale nie mniej ważnym elementem, jest ocena potencjalnego wpływu ataków cybernetycznych na kluczowe procesy, reputację oraz ciągłość działania organizacji. Obejmuje to analizę możliwych strat finansowych, opóźnień w realizacji zadań, a także obniżenie zaufania obywateli do instytucji publicznych. Ta analiza pozwala określić priorytety w zakresie wdrażania środków zaradczych.

# Sankcje za naruszenia Dyrektywy NIS2 w sektorze finansów publicznych

Organizacje sektora finansów publicznych, które naruszają przepisy Dyrektywy NIS2, będą podlegać różnorodnym sankcjom. Prawidłowe egzekwowanie tych sankcji ma na celu zwiększenie świadomości i odpowiedzialności instytucji w zakresie ochrony cybernetycznej. Sankcje te stanowią kluczowy element zapewnienia zgodności z dyrektywą i zapobiegania przyszłym naruszeniom.

Sankcje mogą obejmować kary finansowe, takie jak grzywny lub opłaty za niewdrożenie środków zaradczych. Grzywny te będą proporcjonalne do skali naruszenia i jego wpływu na bezpieczeństwo cybernetyczne. Instytucje, które nie wdrożą zaleceń lub środków naprawczych, będą musiały ponosić dodatkowe opłaty, co stanowi dodatkową presję do poprawy zabezpieczeń.

Poza karami finansowymi, instytucje mogą również doświadczać konsekwencji prawnych, takich jak postępowania administracyjne czy nawet czasowe zawieszenie określonych działań lub usług. Te sankcje prawne mają na celu zmuszenie organizacji do natychmiastowej reakcji i wdrożenia właściwych środków bezpieczeństwa.

## Przykłady:

- **Kary finansowe:** Grzywny proporcjonalne do skali naruszenia i wpływu na bezpieczeństwo, opłaty za niewdrożenie zaleceń
- **Konsekwencje prawne:** Postępowania administracyjne, czasowe zawieszenie działań lub usług
- **Inne sankcje:** Ostrzeżenia publiczne, zwiększony obowiązek raportowania

Oprócz kar finansowych i konsekwencji prawnych, instytucje mogą również podlegać innym sankcjom, takim jak ostrzeżenia publiczne lub zwiększony obowiązek raportowania. Te sankcje mają na celu zwiększenie transparentności



# Kary finansowe za naruszenia Dyrektywy NIS2 w sektorze finansów publicznych



## Wysokość Kar

Kary finansowe będą uzależnione od stopnia naruszenia oraz skali szkód wyrządzonych przez incydenty cybernetyczne.



## Cele Kar

Celem kar jest nie tylko ukaranie za złamanie przepisów, ale także zapobieganie przyszłym incydomom poprzez zachęcanie do inwestowania w skuteczne środki ochrony.



## Kryteria Kar

Kryteria ustalania wysokości kar obejmują stopień naruszenia, skalę szkód oraz stopień odpowiedzialności organizacji.

# Konsekwencje prawne za naruszenia Dyrektywy NIS2 w sektorze finansów publicznych

Konsekwencje prawne za naruszenia Dyrektywy NIS2 mają na celu zapewnienie długofalowych skutków dla organizacji sektora finansów publicznych, które nie przestrzegają wymogów związanych z cyberbezpieczeństwem. Oprócz **kar finansowych**, konsekwencje prawne mogą obejmować **zakazy działalności**, **odpowiedzialność karną** dla zarządu lub innych pracowników oraz **szkody reputacyjne**. Aby uniknąć poważnych konsekwencji prawnych, organizacje muszą wdrożyć skuteczne procedury zarządzania incydentami oraz monitorowanie ryzyka cybernetycznego.

Rodzaje konsekwencji prawnych to **czasowe zawieszenie działalności**, **ograniczenia operacyjne**, **postępowania karne** oraz **odpowiedzialność indywidualna** członków zarządu, a także **utrata zaufania publicznego** i **negatywne publikacje** w mediach. Te konsekwencje mogą mieć poważne reperkusje dla organizacji sektora finansów publicznych, wpływając na ich zdolność do prowadzenia działalności, reputację i długoterminową stabilność.

Aby uniknąć tych konsekwencji, organizacje muszą **wdrożyć skuteczne procedury zarządzania incydentami**, **monitorować ryzyko cybernetyczne** oraz **zwiększać świadomość** i **edukować pracowników** na temat cyberbezpieczeństwa. Tylko kompleksowe podejście, obejmujące zarówno techniczne, jak i organizacyjne środki ochrony, może zapewnić skuteczną ochronę przed naruszeniami Dyrektywy NIS2 i związanymi z nimi konsekwencjami prawnymi.

# Skutki braku zgodności z Dyrektywą NIS2

Brak zgodności z Dyrektywą NIS2 w sektorze finansów publicznych może pociągać za sobą poważne konsekwencje prawne i finansowe. Organizacje, które nie spełnią wymogów cyberbezpieczeństwa, mogą zostać ukarane **wysokimi karami pieniężnymi**, nawet dochodzącymi do 10 milionów euro lub 2% całkowitego rocznego światowego obrotu.

Ponadto, **jednostki sektora finansów publicznych** mogą zostać poddane **ograniczeniom operacyjnym**, takim jak czasowe zawieszenie działalności lub nakaz wprowadzenia określonych środków naprawczych. W skrajnych przypadkach, **osoby odpowiedzialne w zarządzie** mogą nawet zostać pociągnięte do **odpowiedzialności karnej**.





## **Odpowiedzialność Kierownika**

Kierownik podmiotu kluczowego lub ważnego ponosi pełną odpowiedzialność za cyberbezpieczeństwo.



## **Współpraca Wieloosobowego Organu**

Gdy podmiotem kieruje organ wieloosobowy, wszyscy członkowie ponoszą odpowiedzialność za cyberbezpieczeństwo.



## **Wypełnienie Obowiązków**

Nawet jeśli niektóre zadania zostały powierzone innej osobie, kierownik wciąż ponosi odpowiedzialność za ich prawidłowe wykonanie.

# Harmonizacja przepisów Dyrektywy NIS2 w sektorze finansów publicznych

Dyrektywa NIS2 ma na celu **zapewnienie spójności** regulacji dotyczących cyberbezpieczeństwa w Unii Europejskiej. Harmonizacja przepisów pozwala uniknąć **sprzeczności prawnych** oraz ułatwia **efektywne egzekwowanie** środków ochrony. Stosowanie **jednolitych standardów** oraz **wzajemna zgodność** przepisów zwiększa **odporność na zagrożenia** i **ułatwia współpracę** między różnymi podmiotami.

Kluczowe cele harmonizacji to **zapewnienie zgodności** Dyrektywy NIS2 z innymi dyrektywami, takich jak RODO, oraz **unikanie kolizji prawnych**. Spójne przepisy umożliwiają **zintegrowane zarządzanie ryzykiem** oraz **efektywną wymianę informacji** o incydentach, co przekłada się na **lepszą ochronę infrastruktury krytycznej** w sektorze finansów publicznych.

Ponadto, harmonizacja przepisów pozwala na **lepsze zrozumienie** i **interpretację** wymagań Dyrektywy NIS2 wśród jednostek sektora finansów publicznych. Wspólne standardy i definicje zapewniają **jednolite wdrożenie** środków cyberbezpieczeństwa, co zwiększa **skuteczność ochrony** na skalę całej Unii Europejskiej.

Wreszcie, harmonizacja ułatwia **współpracę transgraniczną** między organami nadzorczymi i jednostkami sektora finansów publicznych. Dzięki temu możliwa jest **szybsza identyfikacja** i **reagowanie** na zagrożenia, które nie znają granic administracyjnych.

# Kluczowe procedury zgodne z wymogami Dyrektywy NIS2

Wdrożenie skutecznych procedur cyberbezpieczeństwa zgodnych z Dyrektywą NIS2 jest kluczowe dla ochrony jednostek sektora finansów publicznych. Obejmuje to m.in. procedury zarządzania ryzykiem, zarządzania dostępem, zarządzania ciągłością działania oraz reagowania na incydenty.

Harmonizacja tych procesów zapewnia spójność działań i ułatwia współpracę między różnymi podmiotami. Jednolite standardy zwiększają odporność na zagrożenia i pozwalają na efektywną wymianę informacji o incydentach.





## **Procedura Zarządzania Ryzykiem**

Systematyczna identyfikacja zagrożeń, ocena ryzyka oraz wdrażanie środków minimalizujących ryzyko.



## **Procedura Raportowania Incydentów**

Mechanizmy wykrywania, zgłaszania, reagowania oraz raportowania incydentów cybernetycznych do organów nadzorczych.



## **Procedura Zarządzania Incydentami**

Wczesne wykrywanie, jasno określone kroki reagowania oraz procedury eskalacji w zależności od poziomu krytyczności.



## **Procedura Audytów i Przeglądów**

Regularne oceny zgodności z wymogami Dyrektywy NIS2 oraz aktualizacja środków zabezpieczających.

# Procedura Zarządzania Dostępem



## Kontrola Dostępu

Definiowanie i egzekwowanie zasad dostępu do systemów i danych w oparciu o role i uprawnienia.



## Planowanie Ciągłości Działania

Opracowanie i wdrożenie planów zapewniających ciągłość działalności w przypadku zakłóceń.



## Odzyskiwanie Danych

Procedury odzyskiwania danych i przywracania systemów po awarii lub incydencie.

# Procedura Zarządzania Kontynuacją Działalności i Odzyskiwania Danych po Awarii

## Planowanie Ciągłości Działania

Opracowanie i wdrożenie planów zapewniających ciągłość działalności w przypadku zakłóceń lub awarii.

## Odzyskiwanie Danych

Zdefiniowanie procedur szybkiego i bezpiecznego odzyskiwania danych oraz przywracania systemów po incydencie.

## Testy i Aktualizacje

Regularne testowanie oraz aktualizowanie planów ciągłości działania i procedur odzyskiwania danych.

## Role i Odpowiedzialności

Jasne określenie ról i obowiązków zespołów odpowiedzialnych za ciągłość działania i odzyskiwanie danych.

## Komunikacja Kryzysowa

Opracowanie planów efektywnej komunikacji z interesariuszami na wypadek zakłóceń w działalności.



# Procedury Szkoleniowe i Podnoszenia Świadomości

- **Programy Szkoleniowe:** Regularne szkolenia dla pracowników nt. bezpieczeństwa IT, rozpoznawania zagrożeń i postępowania w przypadku incydentów.
- **Podnoszenie Świadomości:** Kampanie informacyjne mające na celu zwiększenie świadomości nt. cyberbezpieczeństwa wśród personelu.

# Procedury Zarządzania Dostawcami i Partnerami

- **Ocena Ryzyka Dostawców:** Analiza i ocena ryzyka związanego z dostawcami usług IT i innymi partnerami.
- **Umowy SLA:** Definiowanie i monitorowanie umów SLA (Service Level Agreement) w zakresie wymogów bezpieczeństwa.

# Procedury Zarządzania Zmianami w Systemach IT

- **Planowanie Zmian:** Określenie procedur planowania, testowania i wdrażania zmian w systemach IT.

# Procedury Ochrony Danych i Raportowania Incydentów

**Klasyfikacja Danych:** Wdrożenie szczegółowych procedur klasyfikacji danych na podstawie ich poufności i wrażliwości, zapewniając odpowiednie środki ochrony.

**Szyfrowanie:** Implementacja kompleksowych mechanizmów szyfrowania danych zarówno podczas przechowywania, jak i transmisji, zapewniających integralność i poufność informacji.

**Bezpieczeństwo Fizyczne:** Wdrożenie zaawansowanych zabezpieczeń fizycznych chroniących infrastrukturę IT przed nieautoryzowanym dostępem i uszkodzeniem sprzętu.

**Zgłaszanie Incydentów:** Opracowanie szczegółowych procedur szybkiego i efektywnego zgłaszania incydentów cybernetycznych do właściwych organów nadzorczych, zgodnie z wymogami regulacyjnymi.

**Współpraca z Organami Nadzoru:** Utrzymywanie otwartej i stałej komunikacji z instytucjami nadzorczymi w celu wymiany informacji i koordynacji działań w zakresie cyberbezpieczeństwa.



# Procedury Raportowania i Komunikacji z Organami Nadzoru



1

## Zgłaszanie Incydentów

Jasno określone procedury szybkiego zgłaszania incydentów cybernetycznych do właściwych organów nadzoru, zgodnie z wymogami regulacyjnymi.

2

## Współpraca z Organami Nadzoru

Otwarta i stała komunikacja z instytucjami nadzorczymi w celu wymiany informacji i koordynacji działań w zakresie cyberbezpieczeństwa.

3

## Przetwarzanie Logów i Monitoring

Regularne zbieranie, przetwarzanie i analiza logów systemowych w celu wczesnego wykrywania zagrożeń. Utrzymanie ciągłego monitoringu w celu natychmiastowej reakcji.

# Procedury Przetwarzania Logów i Monitoringu

1

## Zbieranie i Analiza Logów

Regularne gromadzenie, przetwarzanie i analiza logów systemowych w celu wykrywania nietypowych wzorców aktywności, które mogą sygnalizować potencjalne zagrożenia.

2

## Monitoring Ciągły

Utrzymanie stałego monitoringu systemów i infrastruktury IT, aby umożliwić wczesne wykrycie i szybką reakcję na wszelkie oznaki zagrożeń lub naruszeń bezpieczeństwa.

3

## Proaktywne Reagowanie

Analiza zebranych logów oraz ciągły monitoring pozwalają na szybkie identyfikowanie i eliminowanie potencjalnych luk lub podatności, zanim staną się one źródłem realnego zagrożenia.

# Podsumowanie

Dyrektywa NIS2 wprowadza obowiązek **systematycznego monitorowania ryzyka cybernetycznego** oraz **efektywnego reagowania na incydenty** w jednostkach sektora finansów publicznych. Organizacje będą zobowiązane do **regularnego raportowania incydentów** do odpowiednich organów nadzoru, co zapewni **transparentność** i umożliwi **szybką reakcję** na zagrożenia na poziomie krajowym i międzynarodowym.

**Przeprowadzanie audytów** oraz **systematyczna ocena ryzyka cybernetycznego** są kluczowymi elementami efektywnego zarządzania bezpieczeństwem informacji. Wprowadzenie **sankcji za naruszenia** ma na celu zwiększenie **odpowiedzialności organizacji** oraz **motywowanie ich do inwestowania w skuteczne środki zapobiegawcze**.

Skuteczne zarządzanie incydentami w sektorze finansów publicznych to kluczowy element ochrony krytycznej infrastruktury. Jednolite procedury reagowania, współpraca międzynarodowa oraz wymiana informacji zapewniają szybkie wykrywanie i neutralizację zagrożeń. Priorytetem jest zapewnienie ciągłości działania oraz minimalizacja negatywnych skutków incydentów dla obywateli i gospodarki.

Wdrożenie wymagań Dyrektywy NIS2 wymaga kompleksowego podejścia, obejmującego ocenę ryzyka, audyty, szkolenia pracowników oraz inwestycje w nowoczesne narzędzia bezpieczeństwa. Zaangażowanie zarządu i współpraca z organami nadzoru są kluczowe dla sukcesu tych działań.

Regularne badanie luk i podatności w systemach IT jednostek sektora finansów publicznych pozwala na szybkie reagowanie na nowe zagrożenia. Wczesne wykrywanie i łatanie słabych punktów znacząco redukuje ryzyko skutecznych ataków hakerskich. Współpraca z ekspertami z innych krajów ułatwia wymianę dobrych praktyk i skutecznych narzędzi cyberbezpieczeństwa.

Szkolenia pracowników w zakresie bezpiecznych praktyk, rozpoznawania zagrożeń oraz postępowania w przypadku incydentów są niezbędne do budowania kultury cyberbezpieczeństwa w organizacji. Zaangażowanie kierownictwa w promowanie tych działań zapewnia skuteczne wdrożenie i stosowanie się do nowych wymogów.

# Autor

Dominik Kisiel

Audyt i Doradztwo Dominik Kisiel

Całość tekstu ujęta w prezentacji *Efektywne zarządzanie cyberbezpieczeństwem w jednostkach sektora finansów publicznych* jest objęta prawem autorskim i podlega ochronie na mocy „*Ustawy o prawie autorskim i prawach pokrewnych*” z dnia 4 lutego 1994 r. (t.j. Dz. U. z 2022 r. poz. 2509). Kopiowanie, przetwarzanie, rozpowszechnianie tych materiałów w całości lub w części bez zgody autora jest zabronione.

