HOLM SECURITY

NIS2
Przewodnik

NIS2 to kontynuacja prac rozpoczętych w ramach dyrektywy NIS na rzecz wspólnego wysokiego poziomu cyberbezpieczeństwa w Unii Europejskiej.

https://holmsecurity.pl/zgodnosc-z-przepisami/dyrektywa-nis

Spis treści

1 Wprowadzenie

Dyrektywa NIS2 obowiązująca od października 2024 r. ma na celu usprawnienie prac rozpoczętych wraz z dyrektywą NIS.

1

NIS2 Wprowadzenie

Dyrektywa NIS2, która obowiązuje od października 2024 r., ma na celu ustanowienie wyższego poziomu cyberbezpieczeństwa i odporności w organizacjach Unii Europejskiej. NIS2 w dużej mierze opiera się na tych samych zasadach, co NIS, ale zawiera kilka ważnych dodatków. Dyrektywa obejmuje zakresem więcej sektorów i wskazuje wytyczne w celu zapewnienia jednolitej ratyfikacji w prawie lokalnym w państwach członkowskich UE.

NIS2 - Nowości

- ✓ Uwzględnia większą liczbę podmiotów i sektorów (branż)
- ✓ Większa odpowiedzialność za zarządzanie oraz każdą osobę fizyczną
- ✓ Zmienia metoda kwalifikacji i rejestracji
- ✓ Nakłada nowe terminy powiadamiania o incydentach
- ✓ Obejmuje bezpośrednio kluczowe, ważne podmioty i pośrednio dostawców
- ✓ Obowiązkowe raporty z incydentów, również w przypadku “potencjalne zdarzenie dla cyberbezpieczeństwa”
- ✓ Wprowadza sankcje, podobne do tych zawartych w RODO

3 główne filary NIS2

Obowiązki państw członkowskich

- Organy krajowe
- Strategie krajowe
- Ramy CVD
- Ramy zarządzania kryzysowego

OBOWIĄZKI FIRMY

Zarządzanie ryzykiem

- Odpowiedzialność najwyższego kierownictwa za nieprzestrzeganie przepisów
- Kluczowe i ważne podmioty są zobowiązane do wdrożenia środków bezpieczeństwa
- Firmy są zobowiązane do zgłaszania incydentów w określonych ramach czasowych.

Współpraca oraz wymiana informacji

- Grupa współpracy
- Sieć CSIRT
- CyCLONe
- CVD i europejski rejestr podatności na zagrożenia
- Wzajemne oceny
- Dwuletni raport ENISA na temat cyberbezpieczeństwa

2 Rozszerzenie zakresu

NIS2 zwiększa liczbę zaangażowanych sektorów i redefiniuje organizacje objęte zakresem jako kluczowe i ważne podmioty.

2

Kluczowe i ważne podmioty

Poprzednie rozróżnienie między operatorami usług kluczowych i dostawcami usług cyfrowych w pierwotnej dyrektywie NIS zostało zastąpione rozróżnieniem między podmiotami kluczowymi i podmiotami ważnymi.
Rozróżnienie między nimi zależy od takich czynników, jak wielkość, sektor i krytyczne znaczenie dla społeczeństwa. Oba typy podmiotów muszą przestrzegać ram cyberbezpieczeństwa NIS2, ale podmioty kluczowe mają bardziej rygorystyczne wymogi w zakresie sprawozdawczości i nadzoru.

Kluczowe podmioty

Podmioty te podlegają nadzorowi ex ante (proaktywnemu).

Ważne podmioty

Podmioty te podlegają nadzorowi ex post (reaktywnemu).

Duże podmioty

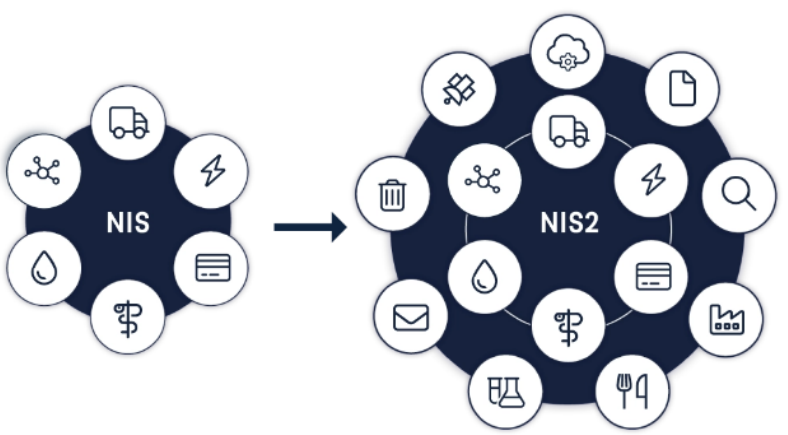
Podmioty, które zatrudniają ponad 250 pracowników lub mają ponad 50 milionów euro przychodów.

Średni podmiot

Podmioty, które zatrudniają ponad 50 pracowników lub mają ponad 10 milionów euro przychodów.

NIS2 określiła listę sektorów objętych dyrektywą i ustanawia podstawową zasadę, zgodnie z którą każdy duży lub średni podmiot z tych sektorów będzie bezpośrednio objęty zakresem. Nie musi to wykluczać podmiotów małych lub mikroorganizacji; państwa członkowskie mogą rozszerzyć te wymagania, jeśli podmiot spełnia określone kryteria jako kluczowy gracz w społeczeństwie, gospodarce, poszczególnych sektorach lub rodzajach usług.

Pierwsza wersja NIS miała wpływ na ograniczoną liczbę sektorów, ale wraz z NIS2 rozszerzono zasięg do 15 branż.



Kluczowe i ważne podmioty

Sektor	Podsektor	Duże podmioty (>250 pracowników ub >50 mln EUR przychodów)	Średnie podmioty (50-249 pracowników lub >10 mln EUR przychodów)	Małe/mikro-podmioty (S:<50 pracowników lub <> 10 mln EUR przychodów; M <10 pracowników lub <2 mln EUR przychodów)
Sektory o wysokim stopniu krytyczności				
Energetyka	W tym podsektory energii elektrycznej, ropy i gazu, systemy ciepłownicze i chłodnicze, wodór	**Kluczowe**	**Ważne**	**Nieobjęte zakresem**
Transport	W tym podsektory transportu lotniczego, kolejowego, wodnego i drogowego.	**Kluczowe**	**Ważne**	**Nieobjęte zakresem**
Opieka Zdrowotna	Obejmuje podsektor środowiska opieki zdrowotnej (w tym szpitale i prywatne kliniki).	**Kluczowe**	**Ważne**	**Nieobjęte zakresem**
Administracja publiczna	Rządów centralnych. *	**Kluczowe**	**Kluczowe**	**Kluczowe**
	Rządów regionalnych.	**Ważne**	**Ważne**	**Ważne**
Bankowość i infrastruktura rynku finansowego	Banki i infrastruktura rynku finansowego, np. usługi płatnicze.	**Kluczowe**	**Ważne**	**Nieobjęte zakresem**
Infrastruktura cyfrowa	Kwalifikowani dostawcy usług zaufania, dostawcy usług DNS i rejestry nazw TLD.	**Kluczowe**	**Kluczowe**	**Kluczowe**
	Dostawcy publicznych sieci łączności elektronicznej.	**Kluczowe**	**Kluczowe**	**Ważne**
	Dostawcy niekwalifikowanych usług zaufania.	**Kluczowe**	**Ważne**	**Ważne**
	Punkt wymiany ruchu internetowego, usługa przetwarzania w chmurze, usługa centrum danych i dostawcy sieci dostarczania treści.	**Kluczowe**	**Ważne**	**Nieobjęte zakresem**
Woda pitna i ścieki	Woda pitna i ścieki, przy czym to ostatnie ma zastosowanie **tylko wtedy**, gdy stanowi istotną część ogólnej działalności podmiotów.	**Kluczowe**	**Ważne**	**Nieobjęte zakresem**
Przestrzeń kosmiczna	Operatorzy infrastruktury naziemnej.	**Kluczowe**	**Ważne**	**Nieobjęte zakresem**

*Z wyłączeniem sądownictwa, parlamentów, banków centralnych, obrony, bezpieczeństwa narodowego lub publicznego.

Kluczowe i ważne podmioty

Sektor	Podsektor	Duże podmioty (>250 pracowników ub >50 mln EUR przychodów)	Średnie podmioty (50-249 pracowników lub >10 mln EUR przychodów)	Małe/mikro-podmioty (S:<50 pracowników lub <> 10 mln EUR przychodów; M <10 pracowników lub <2 mln EUR przychodów)
Sektory ważne				
Usługi pocztowe i kurierskie		**Ważne**	**Ważne**	**Nieobjęte zakresem**
Gospodarka odpadami	(Tylko jeśli jest główną działalnością gospodarczą)	**Ważne**	**Ważne**	**Nieobjęte zakresem**
Przemysł chemiczny	Produkcja, wytwarzanie i dystrybucja.	**Ważne**	**Ważne**	**Nieobjęte zakresem**
Przemysł spożywczy	Produkcja hurtowa i przemysłowa oraz przetwórstwo.	**Ważne**	**Ważne**	**Nieobjęte zakresem**
Produkcja	Wyroby medyczne (do diagnostyki in vitro); wyroby komputerowe, elektroniczne, optyczne; sprzęt elektryczny; maszyny; pojazdy silnikowe, przyczepy, naczepy; pozostały sprzęt transportowy.	**Ważne**	**Ważne**	**Nieobjęte zakresem**
Dostawcy usług cyfrowych	Rynki internetowe, wyszukiwarki i platformy społecznościowe	**Ważne**	**Ważne**	**Nieobjęte zakresem**
Badania	Organizacje badawcze (z wyłączeniem instytucji edukacyjnych)	**Ważne**	**Ważne**	**Nieobjęte zakresem**
Podmioty świadczące usługi rejestracji nazw domen	Wszystkie rozmiary, ale tylko z zastrzeżeniem art. 3 ust. 3 i art. 28. Dyrektywy NIS2			

Istnieją pewne wyjątki od powyższych wytycznych. Pełna i wyczerpująca lista wszystkich wyjątków znajduje się w tekście dyrektywy.

3 Zgłaszanie incydentów

Jak już ustalono dla NIS, każde państwo członkowskie będzie miało centralny punkt kontaktowy w celu zapewnienia zgodności z dyrektywą.

3

Zgłaszanie incydentów

Jak już ustalono dla NIS, każde państwo członkowskie będzie miało centralny punkt kontaktowy w celu zapewnienia zgodności z dyrektywą, a także koordynujący zespół reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) lub inny właściwy organ do zgłaszania incydentów. Na przykład w Belgii będzie to rola Centrum Bezpieczeństwa Cybernetycznego Belgii (CCB).

CSIRT lub właściwy organ musi zgłaszać takie incydenty do ENISA co trzy miesiące, wykorzystując zanonimizowane informacje. Dzięki tym danym ENISA będzie następnie co sześć miesięcy raportować o incydentach w UE. Ten proces raportowania pomoże organizacjom i państwom członkowskim UE wyciągać wnioski z takich incydentów i jest kluczową zmianą w nowej dyrektywie NIS2.

W stosownych przypadkach podmioty powiadamiają odbiorców swoich usług o istotnych incydentach. Jeśli leży to w interesie publicznym, CSIRT lub odpowiedni właściwy organ może poinformować opinię publiczną o istotnym incydencie lub może zażądać tego od podmiotu.

4 Surowsze kary i złożoność jurysdykcji

NIS2 wprowadza surowsze kary za nieprzestrzeganie przepisów niż te, które zostały określone w NIS, i kładzie nacisk na transgraniczną zgodność i współpracę.

4

Surowsze kary za nieprzestrzeganie przepisów

NIS2 wprowadza surowsze kary za nieprzestrzeganie przepisów przez kluczowe i ważne podmioty.

Sektory kluczowe

Kary administracyjne w wysokości do 10,000,000 EURO lub 2% całkowitego rocznego światowego obrotu z poprzedniego roku podatkowego, w zależności d tego, która z tych kwot jest wyższa.

Sektory ważne

Grzywny administracyjne w wysokości od 7,000,000 EURO lub 1.4% całkowitego rocznego światowego obrotu w poprzednim roku podatkowym, w zależności od tego, która kwota jest wyższa.

Złożoność jurysdykcji

Zgodnie z dyrektywą NIS2 istotne i ważne podmioty podlegają jurysdykcji państwa członkowskiego UE, w którym świadczą swoje usługi. Jeśli podmiot świadczy usługi w więcej niż jednym państwie członkowskim, jurysdykcję sprawuje każde z tych państw. W przypadku podmiotów, w których usługa jest świadczona lub zależy od działalności poza UE, muszą one zapewnić, że będą mogły kontynuować działalność w UE w przypadku zaprzestania działalności poza UE.

5 Obowiązki kierownictwa

NIS2 zobowiązuje kierownictwo wyższego szczebla do przejęcia odpowiedzialności za poziom dojrzałości cyberbezpieczeństwa swoich organizacji. Niezastosowanie się do tego wymogu wiąże się z poważnymi konsekwencjami.

5

Obowiązki kierownictwa

Odpowiedzialność kierownictwa jest kolejnym kluczowym elementem NIS2, ponieważ nowa dyrektywa zobowiązuje kierownictwo do przejęcia odpowiedzialności za poziom dojrzałości cyberbezpieczeństwa swoich organizacji. Obejmie to przeprowadzanie ocen ryzyka i zatwierdzanie planów postępowania z ryzykiem, co oznacza, że kierownictwo musi uczestniczyć w szkoleniach z zakresu cyberbezpieczeństwa. Dyrektywa zobowiązuje również organizacje do szkolenia swoich pracowników w zakresie ryzyka cyberbezpieczeństwa i reagowania na nie.

Nieprzestrzeganie przez kierownictwo wymogów NIS2 może skutkować poważnymi konsekwencjami, w tym odpowiedzialnością, tymczasowymi zakazami i grzywnami administracyjnymi przewidzianymi w krajowych przepisach wykonawczych.

Organy zarządzające kluczowych i ważnych podmiotów muszą:

- **Zatwierdzać adekwatność** środków zarządzania cyberryzykiem podejmowanych przez podmiot
- **Nadzorować wdrażanie** środków zarządzania ryzykiem
- **Przechodzić szkolenia** w celu zdobycia wystarczającej wiedzy i umiejętności, aby identyfikować zagrożenia i oceniać praktyki zarządzania ryzykiem cybernetycznym oraz ich wpływ na usługi świadczone przez podmiot
- Regularnie **oferować podobne szkolenia swoim pracownikom**
- **Ponosić odpowiedzialność** za nieprzestrzeganie przepisów

6 Środki zarządzania ryzykiem

Kluczowe i ważne podmioty muszą podejmować odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem.

6

Środki zarządzania ryzykiem

Zarządzanie ryzykiem jest kluczowym elementem zgodności z NIS i NIS2, zapewniającym systematyczne i ustrukturyzowane podejście do identyfikacji, analizy i zarządzania ryzykiem związanym z infrastrukturą IT. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) wyraźnie wymienia zarządzanie ryzykiem (podatnością) jako jeden ze sposobów poprawy bezpieczeństwa.

Artykuł 21 Dyrektywy NIS2 podsumowuje minimalne środki, jakie muszą podjąć podmioty w ramach NIS2. Środki te jasno określają potrzebę analizy ryzyka i zarządzania ryzykiem.

Artykuł 21 (2a)

Zasady dotyczące analizy ryzyka i bezpieczeństwa systemów informatycznych.

Artykuł 21 (2a)

Zasady i procedury oceny skuteczności środków zarządzania ryzykiem cyberbezpieczeństwa.

Takie środki muszą obejmować co najmniej następujące elementy:

1. Analiza ryzyka i bezpieczeństwo systemów informatycznych
2. Obsługa incydentów
3. Środki ciągłości działania (kopie zapasowe, odzyskiwanie danych po awarii, zarządzanie kryzysowe)
4. Bezpieczeństwo łańcucha dostaw
5. Bezpieczeństwo nabywania, rozwoju i utrzymania systemów
6. Zasady i procedury oceny skuteczności środków zarządzania ryzykiem cyberbezpieczeństwa
7. Podstawowa higiena komputerowa i szkolenia
8. Zasady właściwego stosowania kryptografii i szyfrowania
9. Bezpieczeństwo zasobów ludzkich, zasady kontroli dostępu i zarządzanie zasobami
10. Korzystanie z wieloskładnikowej, zabezpieczonej komunikacji głosowej/wideo/tekstowej i zabezpieczonej komunikacji awaryjnej

HOLM SECURITY

7 Zautomatyzowane i ciągłe oceny ryzyka

Zarządzanie ryzykiem jest kluczowym elementem zgodności z NIS2, a art. 21 dyrektywy NIS2 jasno określa potrzebę analizy ryzyka.

7

Zautomatyzowana i ciągła ocena ryzyka

Oceny ryzyka mają zasadnicze znaczenie w kontekście NIS i NIS2, ponieważ odgrywają podstawową rolę w identyfikowaniu, ocenie i zarządzaniu ryzykiem cyberbezpieczeństwa w ramach infrastruktury krytycznej i usług kluczowych. Dyrektywy NIS podkreślają znaczenie oceny ryzyka jako części szerszej strategii mającej na celu zwiększenie ogólnej odporności cyberbezpieczeństwa organizacji objętych dyrektywami.

Przeprowadzanie ciągłych ocen ryzyka w ramach procesu zarządzania podatnościami tworzy systematyczne podejście do cyberzagrożeń. Podejście to pozycjonuje Twoją organizację jako proaktywną, co oznacza, że skupisz się na zapobieganiu incydentom, a nie na ich usuwaniu po fakcie.

Ocena ryzyka jest niezbędna i pomaga organizacji:

- **Zidentyfikować słabe punkty**
- **Zrozumieć zagrożenia**
- **Przydzielać zasoby**
- **Ciągle się doskonalić**
- **Wykazać należytą staranność**
- **Uzyskać zgodność z wymaganiami**
- **Proaktywnie zarządzać ryzykiem**
- **Być przygotowanym na incydenty**
- **Wdrażanie zabezpieczeń już w fazie projektowania**
- **Priorytetyzuj środki bezpieczeństwa**

8 Wymogi dotyczące higieny cyberbezpieczeństwa

Ponad 90% wszystkich incydentów rozpoczyna się od czynnika ludzkiego, dlatego UE włączyła praktyki cyberhigieny i szkolenia w zakresie bezpieczeństwa cybernetycznego jako część NIS2.

8

Wymogi dotyczące cyberbezpieczeństwa

Badania pokazują, że ponad 90% wszystkich incydentów ma swój początek w czynniku ludzkim. W odpowiedzi UE włączyła praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa jako część dyrektywy NIS2. Można to znaleźć w art. 21, sekcja 2G („podstawowe praktyki higieny cyberbezpieczeństwa i szkolenia w zakresie cyberbezpieczeństwa").

Cyberhigiena odnosi się do środków, które osoby fizyczne i organizacje muszą podjąć w celu utrzymania dobrego stanu cyberbezpieczeństwa i ochrony swoich środowisk cyfrowych przed cyberzagrożeniami. Obejmuje ona podejmowanie proaktywnych i zapobiegawczych kroków w celu zmniejszenia ryzyka cyberataków i zapewnienia ogólnego bezpieczeństwa systemów informatycznych.

Kluczowe aspekty cyberhigieny:

- Zarządzanie hasłami
- Aktualizacje i patching
- Świadomość i szkolenie w zakresie obrony przed phishingiem
- Kopie zapasowe danych
- Bezpieczeństwo urządzeń mobilnych
- Najlepsze praktyki bezpiecznego Wi-Fi
- Planowanie reakcji na incydenty
- Bezpieczne przeglądanie stron internetowych
- Bezpieczeństwo IoT
- Zapora sieciowa i oprogramowanie zabezpieczające
- Kontrola dostępu
- Zgodność z przepisami

9 Holm Security pomaga w uzyskaniu zgodności z NIS2

Zapewniamy kompletne pakiety, które w pełni wspierają oparte na ryzyku wysiłki na rzecz zapewnienia zgodności z NIS2 - wszystko na jednej platformie.

9

Holm Security pomaga

Firma Holm Security pomogła setkom organizacji w całej UE w spełnieniu wymogów dyrektywy NIS, a teraz pomaga kolejnym setkom w spełnieniu wymogów dyrektywy NIS2. Zapewniamy narzędzia potrzebne do podjęcia skutecznych kroków w kierunku zapewnienia zgodności.

Narzędzia te pozwalają na:

- Przeprowadzanie zautomatyzowanych i ciągłych (systematycznych) ocen ryzyka
- Stworzenie proaktywnego podejścia do cyberbezpieczeństwa
- Wdrażanie podstawowych praktyk cyberhigieny i szkoleń w zakresie cyberbezpieczeństwa
- Zapewnienie narzędzi potrzebnych do zabezpieczenia łańcucha dostaw
- Pomoc kierownictwu w nadzorowaniu wdrażania zarządzania ryzykiem
- Wykazanie zgodności w oparciu o dane i raporty

Wymagania NIS2	Nasze rozwiązanie
Podejmuj systematyczne, analityczne, oparte na ryzyku kroki w zakresie bezpieczeństwa informacji i przeprowadzaj oceny ryzyka.	Zapewniamy wiodącą na rynku platformę do zautomatyzowanej i ciągłej oceny ryzyka (zarządzanie lukami w zabezpieczeniach).
Wdrażanie podstawowych praktyk cyberhigieny.	Pomagamy klientom wzmocnić ich ludzką obronę przed atakami phishingowymi dzięki symulacjom phishingu oraz dostosowanym i zautomatyzowanym szkoleniom uświadamiającym.
Kluczowe i ważne podmioty, a także ich dostawcy, muszą przeprowadzać oceny ryzyka.	Przeprowadzamy oceny ryzyka dla klientów i ich dostawców zarówno w fazie początkowej, jak i codziennej konserwacji.
Demonstrujemy zgodność dziś i w przyszłości.	Nasze raporty i dane wykazują zgodność już od pierwszego dnia użytkowania.
Kierownictwo nadzoruje wdrażanie zarządzania ryzykiem	Nasza platforma może w pełni zautomatyzować proces nadzorowania przez kierownictwo ciągłej oceny ryzyka w oparciu o łatwe do wykorzystania statystyki i dane.
Sankcje administracyjne, utrata zezwoleń, certyfikatów i kary.	Pomagamy zapobiegać takim scenariuszom poprzez proaktywne znajdowanie i ograniczanie ryzyka lub luk w zabezpieczeniach.

10 Często zadawane pytania

Zrozumienie NIS i NIS2 jest wyzwaniem dla większości organizacji. Jesteśmy tutaj, aby pomóc Ci zrozumieć i spełnić nowe wymagania.

10 Często zadawane pytania

Jaki jest główny cel NIS2?

Zwiększenie odporności na zagrożenia cybernetyczne
NIS2 zachęca państwa członkowskie UE i operatorów infrastruktury krytycznej do zwiększenia ich odporności w zakresie cyberbezpieczeństwa i gotowości do skutecznego reagowania na cyberincydenty i usuwania ich skutków.

Harmonizacja standardów cyberbezpieczeństwa
Ma na celu harmonizację standardów i praktyk cyberbezpieczeństwa w całej UE, aby zapewnić spójny i wysoki poziom bezpieczeństwa w całym cyfrowym krajobrazie.

Obowiązkowe zgłaszanie incydentów
NIS2 nakłada obowiązek zgłaszania istotnych incydentów cybernetycznych organom krajowym i ustanawia skoordynowany mechanizm wymiany informacji na temat zagrożeń i incydentów cybernetycznych między państwami członkowskimi.

Ochrona infrastruktury krytycznej
Dyrektywa kładzie szczególny nacisk na ochronę sektorów infrastruktury krytycznej, takich jak energetyka, transport, opieka zdrowotna i infrastruktura cyfrowa, wymagając od nich spełnienia określonych wymogów cyberbezpieczeństwa.

Egzekwowanie przepisów i kary
NIS2 wprowadza środki skutecznego egzekwowania wymogów cyberbezpieczeństwa i kar za ich nieprzestrzeganie, tym samym zachęcając organizacje do inwestowania w środki bezpieczeństwa.

Współpraca i wymiana informacji
Promuje współpracę i wymianę informacji między państwami członkowskimi oraz między sektorem publicznym i prywatnym w celu wzmocnienia zbiorowej obrony cyberbezpieczeństwa.

Kiedy dyrektywa NIS2 wejdzie w życie?

Dyrektywa NIS2 ma zostać ratyfikowana przez wszystkie państwa członkowskie UE do 17 października 2024 roku. Jest to kluczowa data dla firm, na którą należy zwrócić uwagę, ponieważ nieprzestrzeganie dyrektywy może skutkować poważnymi konsekwencjami, takimi jak kary finansowe i utrata reputacji. W związku z tym ważne jest, aby firmy przygotowały się i poczyniły niezbędne przygotowania, aby zapewnić pełną zgodność na długo przed upływem terminu. Nie czekaj, aż będzie za późno - działaj już teraz, aby uniknąć potencjalnych negatywnych konsekwencji.

10 Często zadawane pytania

Skąd mam wiedzieć, czy moja organizacja musi być zgodna z NIS2?

Kroki do osiągnięcia zgodności z NIS2 mogą się różnić w zależności od konkretnych wdrożeń krajowych lub wymagań branżowych, ale pierwszym krokiem jest ustalenie, czy Twoja organizacja wchodzi w zakres NIS2. Określ, czy jesteś kluczowym lub ważnym podmiotem zgodnie z definicjami zawartymi w dyrektywie, a następnie postępuj zgodnie z pozostałymi 10 krokami w celu zapewnienia zgodności

Jakie są kary w ramach NIS2?

Kluczowe podmioty
Grzywny administracyjne w wysokości do 10 000 000 EUR lub 2% całkowitego rocznego światowego obrotu w poprzednim roku podatkowym, w zależności od tego, która kwota jest wyższa.

Ważne podmioty
Grzywny administracyjne w wysokości do 7 000 000 EUR lub 1,4% całkowitego rocznego światowego obrotu z poprzedniego roku podatkowego, w zależności od tego, która z tych kwot jest wyższa.

Co należy wziąć pod uwagę w odniesieniu do naszych dostawców w kontekście zgodności z NIS/NIS2?

Jednym z głównych obszarów NIS2 jest zabezpieczenie łańcucha dostaw. Oznacza to, że zarówno Twoja organizacja, jak i Twoi dostawcy muszą spełniać kryteria zgodności z NIS2. Twoim obowiązkiem jest upewnienie się, że Twoi dostawcy to robią.

Jestem dostawcą dla organizacji, która musi zachować zgodność z NIS/NIS2 - co powinienem wziąć pod uwagę?

Jako dostawca dla organizacji, która musi być zgodna z NIS/NIS2, musisz upewnić się, że spełniasz wymagania bezpieczeństwa NIS/NIS2.

10 Często zadawane pytania

Jaka jest różnica między kluczowymi a ważnymi podmiotami?

Różnica między nimi nie polega na tym, jakie wymogi muszą spełniać, ponieważ pozostają one takie same dla obu podmiotów, ale raczej na tym, jakie środki nadzorcze i kary będą miały zastosowanie. \ Kluczowe podmioty będą musiały spełniać wymogi nadzorcze od momentu wprowadzenia NIS2, podczas gdy ważne podmioty będą podlegać nadzorowi ex-post, co oznacza, że działania będą podejmowane tylko wtedy, gdy organy otrzymają dowody na niezgodność.

Czy zarządzanie podatnościami jest wymagane do zapewnienia zgodności z NIS2?

Jeśli chodzi o wymogi określone przez UE i władze lokalne, skanowanie podatności lub skanowanie bezpieczeństwa jest wymogiem w ramach oceny ryzyka. Zarządzanie podatnościami jest jednym z kluczowych elementów zgodności z dyrektywą NIS2.

Jaka jest różnica między NIS/NIS2 a DORA?

Digital Operational Resilience Act (DORA) to rozporządzenie Unii Europejskiej (UE), które tworzy wiążące, kompleksowe ramy zarządzania ryzykiem w zakresie technologii informacyjno-komunikacyjnych (ICT) dla sektora finansowego UE. DORA, podobnie jak NIS i NIS2 wymaga podejścia opartego na ryzyku, ale ogranicza swoje regulacje do sektora finansowego i jego dostawców (lex specialist), podczas gdy NIS2 ma zastosowanie do wielu branż niezbędnych dla społeczeństwa.

10 Często zadawane pytania

W jaki sposób Holm Security może pomóc mojej organizacji w spełnieniu wymogów NIS2?

Wdrażanie praktyk cyberbezpieczeństwa opartych na ryzyku jest jednym z najważniejszych obszarów NIS i NIS2. Holm Security pomaga organizacjom, które muszą zachować zgodność z NIS i NIS2:

- ✓ Przeprowadzanie zautomatyzowanych i ciągłych (systematycznych) ocen ryzyka.
- ✓ Stworzenie proaktywnego podejścia do cyberbezpieczeństwa.
- ✓ Wdrożenie podstawowych praktyk cyberhigieny i szkoleń w zakresie bezpieczeństwa.
- ✓ Zapewnienie narzędzi niezbędnych do zabezpieczenia łańcucha dostaw.
- ✓ Pomoc kierownictwu w nadzorowaniu wdrażania środków ryzyka.
- ✓ Wykazanie zgodności w oparciu o dane i raporty.

Chcesz dowiedzieć się więcej?
Chcesz bezpłatnie przetestować?
Skontaktuj się z nami!

Mateusz Piątek
Product Manager Holm Security
tel. 32 259 11 67 | kom. +48 532 570 255

holmsecurity@dagma.pl
http://www.holmsecurity.pl/