softinet

Od zintegrowanego bezpieczeństwa IT/OT

do zgodności z regulacjami prawnymi

Technologie wspierające implementację Dyrektywy NIS2

Spis Treści

Dyrektywa NIS2
jednym spędza sen z powiek, inni czekają na jej wejście w życie z niecierpliwością i w pełnej gotowości.

Nowe wyzwania w zakresie cyberbezpieczeństwa, dynamiczny rozwój technologii, rosnąca złożoność infrastruktury IT/OT oraz coraz bardziej zaawansowane zagrożenia cybernetyczne wymagają od organizacji podejścia opartego na nowoczesnych i zintegrowanych rozwiązaniach.

W odpowiedzi na te wyzwania Unia Europejska wprowadziła Dyrektywę NIS2 (Network and Information Systems), która znacząco podnosi poprzeczkę w zakresie wymogów bezpieczeństwa dla operatorów usług kluczowych oraz innych podmiotów krytycznych dla funkcjonowania gospodarki i społeczeństwa.

W tej publikacji przybliżymy tematykę **zintegrowanego bezpieczeństwa IT/OT** oraz podpowiemy, jak nowoczesne technologie mogą wspierać organizacje w spełnianiu surowych wymogów Dyrektywy NIS2. Przeanalizujemy, jakie konkretne **narzędzia i rozwiązania mogą pomóc w zarządzaniu ryzykiem, monitorowaniu zagrożeń, automatyzacji procesów bezpieczeństwa oraz zapewnieniu ciągłości działania**. Wskażemy również, jakie kroki należy podjąć, aby skutecznie zintegrować technologie z politykami bezpieczeństwa, co jest niezbędne do osiągnięcia pełnej zgodności z nowymi regulacjami.

Dyrektywa NIS2 (Network and Information Security Directive 2) to europejska regulacja mająca na celu zwiększenie poziomu cyberbezpieczeństwa w krajach Unii Europejskiej. Stanowi ona rozszerzenie i aktualizację wcześniejszej dyrektywy NIS, która została przyjęta w 2016 roku. Głównym celem NIS2 jest **wzmocnienie ochrony sieci i systemów informacyjnych w kluczowych sektorach gospodarki**, takich jak energetyka, transport, finanse, zdrowie oraz dostawcy usług cyfrowych.

NIS2 Dyrektywa

Co to jest dyrektywa NIS2?

Dyrektywa NIS2 wprowadza bardziej rygorystyczne wymagania niż jej poprzedniczka, obejmując szerszy zakres organizacji oraz zaostrzając przepisy dotyczące raportowania incydentów i zarządzania ryzykiem.

Jej kluczowe elementy to:

- Zwiększenie liczby sektorów objętych regulacją, co oznacza, że więcej organizacji będzie musiało spełniać określone standardy cyberbezpieczeństwa.
- Wprowadzenie bardziej surowych wymagań dotyczących zarządzania ryzykiem i zgłaszania incydentów. Organizacje będą zobowiązane do wprowadzania odpowiednich środków technicznych i organizacyjnych w celu ochrony przed cyberzagrożeniami.
- Obowiązek zgłaszania poważnych incydentów cyberbezpieczeństwa w ciągu 24 godzin od ich wykrycia, co ma na celu zapewnienie szybkiej reakcji na zagrożenia.

Od kiedy NIS2 wchodzi w życie w Polsce?

Dyrektywa NIS2 została formalnie przyjęta przez Parlament Europejski w listopadzie 2022 roku. Kraje członkowskie Unii Europejskiej, w tym Polska, mają czas do **17 października 2024 roku** na wdrożenie jej przepisów do krajowego porządku prawnego. Oznacza to, że od tego momentu obowiązki wynikające z NIS2 staną się obowiązujące dla organizacji działających na terenie Polski.

Dyrektywa NIS2 stanowi kluczowy element w ramach strategii Unii Europejskiej na rzecz wzmocnienia cyberbezpieczeństwa

Jakich organizacji będzie dotyczyła NIS2?

Dyrektywa NIS2 obejmuje szerszy zakres organizacji niż jej poprzedniczka, co oznacza, że **więcej podmiotów będzie musiało dostosować się do nowych wymogów**.

Do głównych sektorów objętych regulacją należą:

1. Sektor energetyczny (np. operatorzy systemów elektroenergetycznych, dostawcy energii).
2. Sektor transportowy (np. operatorzy infrastruktury transportowej, przewoźnicy).
3. Sektor finansowy (np. banki, firmy ubezpieczeniowe).
4. Sektor zdrowotny (np. szpitale, laboratoria medyczne).
5. Sektor wodociągowy i ściekowy (np. przedsiębiorstwa dostarczające wodę pitną).
6. Sektor kosmiczny.
7. Infrastruktura cyfrowa (np. dostawcy usług w chmurze, dostawcy internetu).
8. Usługi administracji publicznej (np. systemy informacyjne używane przez administrację rządową i lokalną).
9. Dostawcy usług cyfrowych (np. platformy handlowe, wyszukiwarki internetowe).

Podmioty kluczowe *(11 sektorów):*
energetyka, transport, bankowość, infrastruktura rynków finansowych, opieka zdrowotna, woda pitna, ścieki, infrastruktura cyfrowa, zarządzanie usługami ICT, administracja publiczna, przestrzeń kosmiczna.

NIS2 Dyrektywa

Dyrektywa NIS2 rozszerza także obowiązki na **mniejsze podmioty, jeśli ich działalność ma kluczowe znaczenie dla bezpieczeństwa narodowego lub gospodarki**. Organizacje te będą musiały wdrożyć odpowiednie procedury zarządzania ryzykiem, zapewnić zgodność z regulacjami oraz raportować wszelkie incydenty mogące wpłynąć na bezpieczeństwo sieci i systemów informacyjnych.

Podmioty ważne *(7 sektorów):*
usługi pocztowe i kurierskie, gospodarka odpadami, produkcja chemikaliów, produkcja żywności, produkcja (w szerokim znaczeniu), usługi cyfrowe, badania naukowe.

Znaczenie cyberbezpieczeństwa w kontekście Dyrektywy NIS2

Ochrona infrastruktury krytycznej

Jednym z głównych celów NIS2 jest ochrona infrastruktury krytycznej, czyli systemów i sieci, których zakłócenie mogłoby mieć poważne konsekwencje dla funkcjonowania państw i społeczeństw. Sektory takie jak energetyka, transport, finanse, zdrowie oraz dostawcy usług cyfrowych muszą zapewnić, że ich systemy są odporne na ataki cybernetyczne.
W kontekście NIS2, cyberbezpieczeństwo oznacza nie tylko ochronę przed tradycyjnymi atakami, ale także zapewnienie ciągłości działania i szybkie reagowanie na incydenty.

Zmniejszenie ryzyka cyberzagrożeń

Dyrektywa NIS2 nakłada na organizacje obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, które minimalizują ryzyko cyberzagrożeń. W praktyce oznacza to, że organizacje muszą zainwestować w zaawansowane technologie, które umożliwiają wykrywanie, zapobieganie i reakcję na zagrożenia w czasie rzeczywistym. Wprowadzenie takich środków jest kluczowe dla zmniejszenia liczby incydentów oraz ograniczenia ich wpływu na funkcjonowanie organizacji.

Zapewnienie zgodności z przepisami

NIS2 wprowadza bardziej rygorystyczne wymogi regulacyjne, co oznacza, że organizacje muszą dostosować swoje polityki bezpieczeństwa do nowych standardów. Niezgodność z przepisami może prowadzić do poważnych sankcji, w tym wysokich kar finansowych. W związku z tym, cyberbezpieczeństwo staje się nie tylko kwestią ochrony przed zagrożeniami, ale również spełniania wymogów prawnych.
Organizacje muszą regularnie monitorować swoje systemy, przeprowadzać audyty oraz raportować o stanie bezpieczeństwa do odpowiednich organów nadzoru.

Znaczenie cyberbezpieczeństwa w kontekście Dyrektywy NIS2

Zwiększenie zaufania publicznego

W dzisiejszym świecie, zaufanie do systemów cyfrowych ma ogromne znaczenie. Ataki cybernetyczne mogą prowadzić do utraty danych, zakłóceń w działaniu usług oraz poważnych strat finansowych. Wdrożenie odpowiednich środków cyberbezpieczeństwa, zgodnych z wymogami NIS2, pomaga organizacjom budować zaufanie wśród klientów, partnerów biznesowych oraz opinii publicznej. Dzięki temu możliwe jest nie tylko utrzymanie ciągłości działania, ale również wzmacnianie reputacji na rynku.

Wzmocnienie współpracy i wymiany Informacji

NIS2 promuje ideę współpracy pomiędzy państwami członkowskimi oraz wymiany informacji na temat cyberzagrożeń. W ramach dyrektywy, organizacje są zobowiązane do zgłaszania incydentów bezpieczeństwa oraz dzielenia się informacjami o zagrożeniach z innymi podmiotami. Takie podejście pozwala na szybsze reagowanie na nowe rodzaje ataków oraz zwiększa odporność całej Unii Europejskiej na cyberzagrożenia.

Cyberbezpieczeństwo w kontekście dyrektywy NIS2 to nie tylko ochrona przed cyberatakami, ale również **kompleksowe podejście do zarządzania ryzykiem i zapewnienia ciągłości działania** w obliczu rosnących zagrożeń cyfrowych.

Organizacje muszą dostosować swoje strategie bezpieczeństwa do nowych wymogów, inwestując w **odpowiednie technologie i procedury**, które nie tylko chronią ich systemy, ale także zapewniają zgodność z regulacjami. Dyrektywa NIS2 podkreśla znaczenie cyberbezpieczeństwa jako fundamentu stabilności i zaufania w nowoczesnym, cyfrowym świecie.

Wpływ Dyrektywy NIS2 na organizacje

Dyrektywa NIS2 znacząco zwiększa odpowiedzialność organizacji za cyberbezpieczeństwo, rozszerza zakres wymagań oraz wprowadza bardziej surowe konsekwencje za ich niewypełnienie.

Rozszerzenie zakresu regulacji

Dyrektywa NIS2 obejmuje większą liczbę sektorów niż jej poprzedniczka, co oznacza, że więcej organizacji będzie musiało spełniać nowe wymogi. Do sektora operatorów usług kluczowych zalicza się m.in. energetykę, transport, finanse, zdrowie, dostawy wody, a także cyfrową infrastrukturę i administrację publiczną. Rozszerzenie zakresu oznacza, że zarówno duże, jak i mniejsze podmioty w tych sektorach będą musiały wdrożyć odpowiednie środki zabezpieczające, jeśli ich działalność ma kluczowe znaczenie dla funkcjonowania państwa lub gospodarki. Regulacja dotyczy również dostawców usług i konieczności spełnia przez nich wymagań odbiorcy podlegającego pod NIS2 (łańcuch dostaw).

Zarządzanie ryzykiem

Organizacje objęte dyrektywą NIS2 muszą wdrożyć kompleksowe mechanizmy zarządzania ryzykiem cyberbezpieczeństwa. W praktyce oznacza to, że zobowiązane są przeprowadzać regularne analizy ryzyka, identyfikować potencjalne zagrożenia, oraz opracowywać i wdrażać strategie mające na celu minimalizowanie tych zagrożeń. Operatorzy usług kluczowych będą musieli także udowodnić, że posiadają odpowiednie procedury oraz zasoby do przeciwdziałania i reagowania na incydenty cybernetyczne.

Wpływ Dyrektywy NIS2 na organizacje

Zgłaszanie incydentów

Jednym z kluczowych elementów NIS2 jest wprowadzenie bardziej surowych obowiązków związanych z raportowaniem incydentów bezpieczeństwa. Organizacje będą zobowiązane do **zgłaszania poważnych incydentów cyberbezpieczeństwa w ciągu 24 godzin od ich wykrycia**. Zgłoszenie powinno zawierać podstawowe informacje o incydencie, jego wpływie na działalność oraz podjętych krokach naprawczych. Następnie, w ciągu 72 godzin, organizacja musi dostarczyć bardziej szczegółowy raport. Ten obowiązek ma na celu szybką wymianę informacji i zminimalizowanie skutków potencjalnych ataków.

Organizacja i wymogi techniczne

Operatorzy usług kluczowych będą zobowiązani do implementacji zaawansowanych środków technicznych i organizacyjnych w celu zapewnienia wysokiego poziomu cyberbezpieczeństwa. Oznacza to m.in. konieczność inwestycji w nowoczesne technologie zabezpieczające, takie jak systemy detekcji zagrożeń (IDS/IPS), zarządzanie tożsamością (IAM), czy też automatyzację procesów bezpieczeństwa. Organizacje muszą także zapewnić odpowiednie szkolenia dla pracowników, aby zwiększyć ich świadomość w zakresie zagrożeń cybernetycznych.

Wzmożona odpowiedzialność zarządu i kary za niezgodność

NIS2 kładzie szczególny nacisk na odpowiedzialność zarządu organizacji za przestrzeganie wymogów dotyczących cyberbezpieczeństwa. Członkowie zarządów będą musieli wykazać, że nadzorują i wspierają wdrażanie polityk bezpieczeństwa. W przypadku zaniedbań, organizacje mogą zostać ukarane wysokimi karami finansowymi, a w niektórych przypadkach może to prowadzić do odpowiedzialności karnej. Dyrektywa wprowadza także mechanizmy kontroli i audytu, które mają na celu monitorowanie zgodności z przepisami.

Technologie
wspierające spełnienie wymogów NIS2

Spełnienie wymogów dyrektywy NIS2 wymaga zastosowania zaawansowanych technologii, które wspierają **zarządzanie ryzykiem, monitorowanie, log managment, wykrywanie oraz reagowanie na zagrożenia cybernetyczne**.

Zarządzanie danymi i kopie zapasowe

Zaawansowane rozwiązania do zarządzania danymi, które zapewniają automatyzację tworzenia kopii zapasowych, zarządzanie cyklem życia danych oraz szybkie odzyskiwanie danych po awarii. Technologia, która umożliwia organizacjom zabezpieczenie krytycznych danych przed utratą, co jest kluczowe dla spełnienia wymogów NIS2 dotyczących ciągłości działania i ochrony przed ransomware.

Zarządzanie tożsamością i dostępem (IAM)

Rozwiązania do zarządzania dostępem uprzywilejowanym (PAM), co jest kluczowe dla ochrony dostępu do krytycznych systemów i danych. Technologie oferujące funkcje takie jak uwierzytelnianie wieloskładnikowe (MFA), audytowanie i monitorowanie działań użytkowników oraz zarządzanie dostępem uprzywilejowanym, co wspiera organizacje w spełnianiu wymogów dotyczących zarządzania dostępem do systemów kluczowych.

Ochrona infrastruktury IT

Kompleksowe rozwiązania z zakresu zabezpieczeń sieciowych, w tym firewalle, systemy wykrywania zagrożeń (IDS/IPS) oraz narzędzia do segmentacji sieci. Te technologie pomagają organizacjom zabezpieczać swoje sieci przed atakami zewnętrznymi i wewnętrznymi, co jest niezbędne dla spełnienia wymogów NIS2 w zakresie ochrony przed zagrożeniami cybernetycznymi.

Technologie

wspierające spełnienie wymogów NIS2

Analiza ruchu sieciowego

Narzędzie do monitorowania i analizy ruchu sieciowego, które umożliwia wykrywanie anomalii, analizowanie zachowań sieciowych oraz szybkie identyfikowanie zagrożeń. Technologia ta jest kluczowa dla zapewnienia zgodności z NIS2, ponieważ umożliwia wczesne wykrywanie potencjalnych zagrożeń oraz ich szybkie neutralizowanie.

Zintegrowane bezpieczeństwo sieciowe

Rozwiązania bezpieczeństwa sieciowego, które integrują funkcje zapobiegania zagrożeniom, segmentacji sieci, ochrony przed atakami DDoS oraz zarządzania dostępem. Dzięki zaawansowanej analityce i automatyzacji, umożliwiają organizacjom skuteczne zabezpieczenie swoich systemów zgodnie z wymogami NIS2.

Systemy zapobiegania zagrożeniom

Zaawansowane systemy zapobiegania zagrożeniom, takie jak firewalle nowej generacji oraz systemy IPS. Dzięki temu organizacje mogą chronić swoje sieci przed zaawansowanymi zagrożeniami, spełniając jednocześnie wymogi NIS2 w zakresie ochrony integralności i dostępności systemów informacyjnych.

Analiza i zarządzanie zagrożeniami

Narzędzia do analizy i zarządzania zagrożeniami, w tym platformy do zarządzania podatnościami (VM), monitorowania bezpieczeństwa oraz integracji z narzędziami SIEM. Pozwalają one organizacjom na identyfikację, ocenę i zarządzanie ryzykiem cybernetycznym, co jest kluczowe dla spełnienia wymogów NIS2 związanych z analizą ryzyka i raportowaniem incydentów.

Integracja technologii

z politykami bezpieczeństwa w kontekście Dyrektywy NIS2

Tworzenie spójnych polityk bezpieczeństwa

Definiowanie polityk

Organizacje muszą opracować kompleksowe polityki bezpieczeństwa, które uwzględniają wszystkie aspekty zarządzania ryzykiem, ochrony danych, zarządzania dostępem oraz reakcji na incydenty. Polityki te powinny być zgodne z wymogami NIS2 i obejmować zasady dotyczące korzystania z technologii bezpieczeństwa.

Przykład

Zintegrowane platformy zarządzania bezpieczeństwem, które umożliwiają definiowanie polityk dostępu, segmentacji sieci oraz zarządzania zagrożeniami w jednym, centralnym systemie. Dzięki temu polityki te mogą być łatwo wdrażane i monitorowane w całej organizacji.

Automatyzacja i orkiestracja zadań bezpieczeństwa

Automatyzacja

Wdrożenie narzędzi do automatyzacji zadań związanych z bezpieczeństwem jest kluczowe dla szybkiego reagowania na zagrożenia. Automatyzacja pomaga w egzekwowaniu polityk bezpieczeństwa, takich jak automatyczne blokowanie podejrzanych działań czy automatyczne generowanie raportów zgodności.

Przykład

Rozwiązania XDR (Extended Detection and Response), które automatyzują wykrywanie i reagowanie na zagrożenia. Platforma ta integruje się z politykami bezpieczeństwa organizacji, umożliwiając natychmiastowe wdrażanie działań naprawczych zgodnie z ustalonymi procedurami.

Integracja technologii

z politykami bezpieczeństwa w kontekście Dyrektywy NIS2

Zarządzanie tożsamościami i kontrolą dostępu

Definiowanie polityk

Polityki bezpieczeństwa muszą obejmować zasady zarządzania dostępem do systemów informacyjnych, szczególnie w kontekście użytkowników uprzywilejowanych. Technologie IAM (Identity and Access Management) powinny być zintegrowane z tymi politykami, aby zapewnić kontrolę nad tym, kto i w jakim zakresie ma dostęp do krytycznych zasobów.

Przykład

Rozwiązania do zarządzania tożsamościami uprzywilejowanymi, które integrują się z politykami bezpieczeństwa, umożliwiając wdrożenie ścisłej kontroli dostępu oraz audytu działań użytkowników. Polityki te mogą obejmować wymogi dotyczące silnego uwierzytelniania i rotacji haseł.

Monitorowanie i analiza zagrożeń

Monitorowanie

Polityki bezpieczeństwa powinny zawierać zasady dotyczące monitorowania sieci i systemów w celu wykrywania anomalii oraz potencjalnych zagrożeń. Technologie takie jak SIEM (Security Information and Event Management) oraz NDR (Network Detection and Response) powinny być integralną częścią tych polityk.

Przykład

Narzędzia do zaawansowanej analizy ruchu sieciowego, które mogą być zintegrowane z politykami bezpieczeństwa, umożliwiając ciągłe monitorowanie i szybką identyfikację zagrożeń. Dzięki temu organizacje mogą reagować na incydenty zgodnie z ustalonymi procedurami.

Integracja technologii

z politykami bezpieczeństwa w kontekście Dyrektywy NIS2

Zarządzanie danymi i odzyskiwanie ich po awarii

Kopie zapasowe i odzyskiwanie

Polityki bezpieczeństwa muszą uwzględniać zarządzanie danymi, w tym strategie tworzenia kopii zapasowych i odzyskiwania po awarii. Technologie wspierające te działania powinny być zintegrowane z politykami w celu zapewnienia ciągłości działania organizacji w przypadku incydentu.

Przykład

Rozwiązania do tworzenia kopii zapasowych i odzyskiwania danych, które mogą być zintegrowane z politykami bezpieczeństwa, aby zapewnić, że dane są regularnie kopiowane i dostępne do odzyskania w razie potrzeby. Polityki te mogą również obejmować wymagania dotyczące przechowywania kopii zapasowych w wielu lokalizacjach.

Szkolenia i podnoszenie świadomości

Szkolenia

Polityki bezpieczeństwa powinny obejmować programy szkoleniowe dla pracowników, które zwiększą ich świadomość na temat cyberzagrożeń i postępowania zgodnie z procedurami bezpieczeństwa. Technologia może wspierać te działania poprzez platformy e-learningowe oraz symulacje ataków.

Przykład

Narzędzia do symulacji ataków i testowania gotowości organizacji na incydenty, co może być zintegrowane z politykami szkoleniowymi. Dzięki temu pracownicy mogą regularnie ćwiczyć scenariusze incydentów, co poprawia ich gotowość na realne zagrożenia.

Integracja technologii

z politykami bezpieczeństwa w kontekście Dyrektywy NIS2

Zgodność i audyt

Audyt

Polityki bezpieczeństwa muszą obejmować regularne audyty zgodności z wymogami dyrektywy NIS2. Technologie audytowe powinny być zintegrowane z politykami, aby umożliwić regularne sprawdzanie i raportowanie stanu bezpieczeństwa organizacji.

Przykład

Narzędzia do automatycznego audytowania polityk bezpieczeństwa, które mogą być zintegrowane z politykami wewnętrznymi organizacji, zapewniając regularne raporty zgodności oraz identyfikację obszarów wymagających poprawy.

Integracja technologii z politykami bezpieczeństwa w kontekście dyrektywy NIS2 jest kluczowa dla zapewnienia zgodności z przepisami oraz skutecznej ochrony przed cyberzagrożeniami.

Organizacje muszą **opracować i wdrożyć spójne polityki bezpieczeństwa, które są wspierane przez zaawansowane technologie w zakresie zarządzania ryzykiem, monitorowania, automatyzacji oraz reagowania na incydenty.**

Tylko takie kompleksowe podejście pozwoli na spełnienie surowych wymogów NIS2 i ochronę kluczowych zasobów organizacji.

softinet

Dlaczego z nami?

Wiedza

Kluczem do współpracy jest wiedza IT w wielu obszarach (aplikacje, bazy, sieci, serwery…), ocena zasobów i świadomość zagrożeń. Dzięki niej jesteśmy w stanie świadczyć usługi na najwyższym poziomie.

Doświadczenie

Jesteśmy ekspertami w dziedzinie bezpieczeństwa sieciowego i danych. Wieloletnie doświadczenie we wdrożeniach i zaawansowane specjalizacje technologiczne dają naszym klientom pewność kompleksowej obsługi.

Odpowiedzialność

Budujemy optymalne i bezpieczne środowiska IT. Wszechstronnie konsultujemy, wdrażamy, konfigurujemy, szkolimy i wspieramy technicznie.

Od zintegrowanego bezpieczeństwa IT/OT

do zgodności z regulacjami prawnymi

Technologie wspierające implementację Dyrektywy NIS2

softinet

Specjalistycznie skupiamy się na obszarach bezpieczeństwa IT, infrastruktury IT i OT oraz usług świadczonych w zakresie ochrony i optymalizacji działań w ramach struktury IT.

Napisz do nas i dowiedz się więcej o naszej ofercie.