INTRATEL

Dyrektywa NIS2
– istotne zmiany

Od ponad 27 lat doświadczony zespół inżynierów i specjalistów zapewnia bezpieczeństwo Twoich danych.

INTRATEL

Dyrektywa NIS2

Rozwiązania i usługi

Dyrektywa NIS2 to unijne rozporządzenie mające na celu zwiększenie poziomu cyberbezpieczeństwa w Europie. Weszła w życie 16 stycznia 2023 r., a państwa członkowskie UE mają czas do 17 października 2024 r. na jej implementację do krajowego porządku prawnego. Dotyczy szerszy zakresu podmiotów niż w poprzedniej dyrektywie NIS, obejmujący m.in. średnie firmy z sektora publicznego i prywatnego. Wymaga wprowadza szeregu nowych obowiązków dla objętych nią podmiotów, m.in.: wdrożenie minimalnych środków bezpieczeństwa, zarządzania ryzykiem cyberbezpieczeństwa, zgłaszania poważnych incydentów cyberbezpieczeństwa, regularnych testów penetracyjnych oraz stosowania szyfrowania. Jej celem jest przede wszystkim zwiększenie odporności na cyberataki infrastruktury krytycznej dla funkcjonowania społeczeństwa UE, np. w sektorach energetycznym, transportowym, wodociągowym i opieki zdrowotnej.

W Intratel doskonale zdajemy sobie sprawę z rosnących wyzwań związanych z cyberbezpieczeństwem, jakie stoją przed przedsiębiorstwami w dobie dyrektywy NIS2. Dlatego też przygotowaliśmy kompleksowe rozwiązania, które pomogą Państwu spełnić wszystkie wymagania prawne i znacząco podnieść poziom ochrony infrastruktury IT.

INTRATEL

Audyt i analiza luk w zabezpieczeniach

Dokładne zidentyfikowanie potencjalnych słabych punktów w Państwa systemach i sieciach IT

Co obejmuje audyt bezpieczeństwa i analiza luk?

- Skanowanie podatności: Automatyczne skanowanie systemów i sieci IT w celu wykrycia znanych luk w oprogramowaniu i konfiguracji.
- Testy penetracyjne: Symulowane ataki przeprowadzane przez doświadczonych testerów bezpieczeństwa w celu sprawdzenia rzeczywistej odporności systemów na włamania.
- Analiza dzienników systemowych: Przegląd dzienników systemowych w celu wykrycia podejrzanych aktywności i potencjalnych oznak włamań.
- Ocena konfiguracji: Weryfikacja konfiguracji systemów i urządzeń sieciowych pod kątem zgodności z najlepszymi praktykami bezpieczeństwa.
- Przegląd procedur bezpieczeństwa: Ocena procedur bezpieczeństwa w celu zidentyfikowania potencjalnych luk i obszarów wymagających poprawy.

Korzyści z audytu bezpieczeństwa i analizy luk:

- Poprawa widoczności cyberbezpieczeństwa: Dokładne zidentyfikowanie wszystkich potencjalnych słabych punktów w systemach i sieciach IT.
- Zmniejszenie ryzyka cyberataków: Wczesne wykrycie i usunięcie luk w zabezpieczeniach pozwala zapobiec włamaniom i wyciekom danych.
- Spełnienie wymagań dyrektywy NIS2: Audyt i analiza luk stanowią kluczowe elementy procesu zarządzania ryzykiem cyberbezpieczeństwa, wymaganego przez dyrektywę NIS2.
- Zwiększenie zaufania klientów i partnerów: Wysoki poziom cyberbezpieczeństwa buduje zaufanie i pozytywny wizerunek firmy.

Pamiętaj, że audyt bezpieczeństwa i analiza luk to inwestycja w bezpieczeństwo Twojej firmy i jej przyszłość.

INTRATEL

Wdrożenie minimalnych środków bezpieczeństwa

Wsparcie w implementacji wszystkich niezbędnych zabezpieczeń technicznych i organizacyjnych, zgodnie z wymogami

Co obejmuje wdrożenie minimalnych środków bezpieczeństwa?

- Zarządzanie ryzykiem cyberbezpieczeństwa: Wdrożenie formalnego procesu zarządzania ryzykiem, który pozwala na identyfikację, ocenę i łagodzenie zagrożeń cybernetycznych.
- Kontrola dostępu: Wdrożenie mechanizmów kontroli dostępu, które uniemożliwiają nieuprawniony dostęp do systemów i danych.
- Ochrona przed złośliwym oprogramowaniem: Wdrożenie rozwiązań antywirusowych i antyspamowych, a także regularne aktualizacje oprogramowania.
- Szyfrowanie danych: Szyfrowanie poufnych danych zarówno podczas przechowywania, jak i przesyłania.
- Kopie zapasowe danych: Regularne tworzenie kopii zapasowych danych i ich bezpieczne przechowywanie.
- Szkolenia z zakresu cyberbezpieczeństwa: Zapewnienie pracownikom niezbędnej wiedzy i umiejętności w zakresie cyberbezpieczeństwa.
- Procedury reagowania na incydenty: Opracowanie i wdrożenie procedur reagowania na incydenty cyberbezpieczeństwa.

Korzyści z wdrożenia minimalnych środków bezpieczeństwa:

- Zwiększenie odporności na cyberataki: Wdrożenie minimalnych środków bezpieczeństwa znacząco utrudnia cyberprzestępcom przeprowadzanie ataków i kradzież danych.
- Spełnienie wymagań dyrektywy NIS2: Wdrożenie minimalnych środków bezpieczeństwa jest obowiązkowe dla wszystkich podmiotów objętych dyrektywą NIS2.
- Zmniejszenie ryzyka wycieków danych: Stosowanie odpowiednich zabezpieczeń chroni dane poufne przed wyciekiem i utratą.
- Poprawa wizerunku firmy: Wysoki poziom cyberbezpieczeństwa buduje zaufanie klientów i partnerów.

INTRATEL

Zarządzanie ryzykiem cyberbezpieczeństwa

Wdrożenie efektywnego procesu zarządzania ryzykiem, który pozwoli na identyfikację, ocenę i łagodzenie zagrożeń cybernetycznych.

Proces zarządzania ryzykiem cyberbezpieczeństwa obejmuje zazwyczaj następujące etapy:

- Identyfikacja zagrożeń: Określenie wszystkich potencjalnych źródeł cyberzagrożeń, takich jak złośliwe oprogramowanie, phishing, włamania i ataki typu „odmowa usługi" (DoS).
- Ocena ryzyka: Oszacowanie prawdopodobieństwa wystąpienia poszczególnych zagrożeń oraz ich potencjalnego wpływu na działalność firmy.
- Analiza ryzyka: Określenie priorytetów dla poszczególnych zagrożeń na podstawie ich prawdopodobieństwa i potencjalnego wpływu.
- Wdrażanie środków łagodzących: Wdrożenie odpowiednich zabezpieczeń technicznych i organizacyjnych w celu zminimalizowania ryzyka.
- Monitorowanie i przegląd: Regularne monitorowanie ryzyka cybernetycznego i aktualizowanie procesu zarządzania ryzykiem w razie potrzeby.

Korzyści z wdrożenia zarządzania ryzykiem cyberbezpieczeństwa:

- Zwiększenie odporności na cyberataki: Skuteczne zarządzanie ryzykiem pozwala na proaktywne identyfikowanie i łagodzenie zagrożeń, co zmniejsza ryzyko wystąpienia poważnych incydentów cyberbezpieczeństwa.
- Spełnienie wymagań dyrektywy NIS2: Wdrożenie formalnego procesu zarządzania ryzykiem cyberbezpieczeństwa jest obowiązkowe dla wszystkich podmiotów objętych dyrektywą NIS2.
- Zmniejszenie kosztów związanych z cyberatakami: Skuteczne zarządzanie ryzykiem pozwala na uniknięcie lub ograniczenie kosztów związanych z usuwaniem skutków cyberataków, takich jak utrata danych, przestoje w działalności i kary regulacyjne.
- Poprawa podejmowania decyzji: Zarządzanie ryzykiem zapewnia ramy do podejmowania świadomych decyzji dotyczących inwestycji w cyberbezpieczeństwo.

INTRATEL

Zgłaszanie incydentów cyberbezpieczeństwa

Opracowanie i wdrożenie procedur zgłaszania incydentów cyberbezpieczeństwa, zgodnych z wymogami.

Kiedy należy zgłaszać incydenty cyberbezpieczeństwa?

Incydenty cyberbezpieczeństwa należy zgłaszać niezwłocznie po ich wykryciu, nie później niż w ciągu 24 godzin. W przypadku szczególnie poważnych incydentów, które mogą mieć istotny wpływ na bezpieczeństwo narodowe, czas ten może zostać skrócony.

Jak zgłaszać incydenty cyberbezpieczeństwa?

Sposób zgłaszania incydentów cyberbezpieczeństwa różni się w zależności od kraju. W Polsce zgłoszenia należy kierować do CSIRT NASK (Zespołu ds. Reagowania na Incydenty Bezpieczeństwa Sieci Komputerowych). Zgłoszenia można dokonać za pomocą formularza online, e-mailem lub telefonicznie.
Jakie informacje należy zawrzeć w zgłoszeniu?

Zgłoszenie incydentu cyberbezpieczeństwa powinno zawierać co najmniej następujące informacje:

- Dane identyfikacyjne zgłaszającego
- Opis incydentu, w tym datę i godzinę jego wystąpienia, rodzaj ataku, zaatakowane systemy i dane
- Skutki incydentu
- Podjęte działania w celu łagodzenia skutków incydentu
- Informacje o potencjalnych przyczynach incydentu

INTRATEL

Zgłaszanie incydentów cyberbezpieczeństwa

Opracowanie i wdrożenie procedur zgłaszania incydentów cyberbezpieczeństwa, zgodnych z wymogami.

Dodatkowe obowiązki związane ze zgłaszaniem incydentów cyberbezpieczeństwa

Oprócz obowiązku zgłaszania incydentów cyberbezpieczeństwa, dyrektywa NIS2 nakłada na podmioty objęte jej zakresem szereg innych obowiązków, m.in.:

- Przeprowadzanie regularnych testów penetracyjnych
- Stosowanie szyfrowania
- Zapewnienie szkoleń z zakresu cyberbezpieczeństwa dla pracowników

Korzyści ze zgłaszania incydentów cyberbezpieczeństwa

- Pozwala na szybsze i bardziej efektywne reagowanie na incydenty
- Umożliwia identyfikację nowych zagrożeń cybernetycznych
- Pomaga w zapobieganiu przyszłym incydentom
- Wzmacnia współpracę między podmiotami objętymi dyrektywą NIS2

Intratel – Twój partner w zgłaszaniu incydentów cyberbezpieczeństwa

Nasz zespół doświadczonych specjalistów ds. cyberbezpieczeństwa pomoże Ci w zgłoszeniu incydentu cyberbezpieczeństwa zgodnie z wymaganiami dyrektywy NIS2. Zapewnimy Ci wsparcie w zakresie:

- Identyfikacji i oceny incydentu
- Zebrania niezbędnych informacji
- Wypełnienia formularza zgłoszeniowego
- Kontaktu z właściwymi organami

INTRATEL

Szkolenia i edukacja

Zapewnienie pracownikom niezbędnej wiedzy i umiejętności w zakresie cyberbezpieczeństwa.

Dlaczego szkolenia i edukacja z zakresu cyberbezpieczeństwa są ważne?

W dobie rosnących zagrożeń cybernetycznych, szkolenia i edukacja z zakresu cyberbezpieczeństwa stają się coraz ważniejsze dla wszystkich firm i organizacji. Dyrektywa NIS2 kładzie szczególny nacisk na podnoszenie świadomości i kompetencji pracowników w zakresie cyberbezpieczeństwa, nakazując wszystkim objętym nią podmiotom zapewnienie odpowiednich szkoleń.

Szkolenia i edukacja z zakresu cyberbezpieczeństwa mogą:

- Zwiększyć świadomość pracowników na temat zagrożeń cybernetycznych i sposobów ochrony przed nimi.
- Nauczyć pracowników, jak rozpoznawać podejrzane e-maile, strony internetowe i załączniki.
- Wzmocnić hasła i stosować najlepsze praktyki bezpieczeństwa online.
- Zapobiegać przypadkowym wyciekom danych i naruszeniom bezpieczeństwa.
- Zwiększyć ogólną odporność firmy na cyberataki.

Szkolenia i edukacja

Zapewnienie pracownikom niezbędnej wiedzy i umiejętności w zakresie cyberbezpieczeństwa.

Dyrektywa NIS2 określa minimalne wymagania dotyczące szkoleń z zakresu cyberbezpieczeństwa, które muszą zostać spełnione przez wszystkie objęte nią podmioty.

Obejmują one:

- Szkolenia dla wszystkich pracowników dotyczące podstawowych zasad cyberbezpieczeństwa.
- Szkolenia dla pracowników IT z zakresu bardziej zaawansowanych zagadnień cyberbezpieczeństwa.
- Regularne aktualizacje szkoleń w celu uwzględniania nowych zagrożeń i trendów.

Intratel oferuje szeroki zakres szkoleń i usług edukacyjnych z zakresu cyberbezpieczeństwa, dostosowanych do potrzeb różnych firm i organizacji.

Nasze szkolenia prowadzone są przez doświadczonych ekspertów ds. cyberbezpieczeństwa i obejmują m.in.:

- Szkolenia z podstaw cyberbezpieczeństwa
- Szkolenia z zakresu phishingu i inżynierii społecznej
- Szkolenia z zakresu ochrony danych osobowych
- Szkolenia z zakresu zarządzania ryzykiem cyberbezpieczeństwa
- Szkolenia z zakresu reagowania na incydenty cyberbezpieczeństwa

Dostęp do najnowszych technologii

Stały monitoring i aktualizacja rozwiązań cyberbezpieczeństwa, aby zapewnić Państwu ochronę przed najnowszymi zagrożeniami.

W dynamicznie zmieniającym się świecie cyberbezpieczeństwa, dostęp do najnowszych technologii jest kluczowy dla skutecznej ochrony infrastruktury IT i danych przed coraz bardziej wyrafinowanymi cyberatakami.

Intratel, jako partner wiodących producentów rozwiązań cyberbezpieczeństwa, takich jak Dell, Lenovo, HP, VMware i Veeam, zapewnia swoim klientom dostęp do najnowocześniejszych technologii i usług, które pozwalają na:

- Skuteczne wykrywanie i zapobieganie zagrożeniom cybernetycznym: Nasze rozwiązania wykorzystują sztuczną inteligencję, uczenie maszynowe i inne zaawansowane technologie do identyfikacji i blokowania cyberataków w czasie rzeczywistym.
- Szyfrowanie danych i ochronę przed włamaniami: Zapewniamy kompleksowe rozwiązania do szyfrowania danych, zarówno podczas przechowywania, jak i przesyłania, chroniąc poufne informacje przed nieuprawnionym dostępem.
- Zarządzanie ryzykiem cyberbezpieczeństwa: Oferujemy narzędzia do zarządzania ryzykiem cyberbezpieczeństwa, które pomagają firmom identyfikować, oceniać i łagodzić zagrożenia cybernetyczne.
- Reagowanie na incydenty cyberbezpieczeństwa: Wspomagamy firmy w reagowaniu na incydenty cyberbezpieczeństwa, minimalizując ich skutki i chroniąc przed dalszymi stratami.
- Spełnienie wymagań dyrektywy NIS2: Nasze rozwiązania i usługi pomagają firmom w spełnieniu wymagań dyrektywy NIS2 w zakresie cyberbezpieczeństwa.

Wsparcie ekspertów

Zespół doświadczonych specjalistów ds. cyberbezpieczeństwa, którzy są gotowi doradzić Państwu w zakresie wszystkich aspektów ochrony infrastruktury IT.

W Intratel rozumiemy, że cyberbezpieczeństwo to nie tylko technologie, ale również ludzie. Dlatego też nasz zespół składa się z doświadczonych ekspertów ds. cyberbezpieczeństwa, z których 80% to inżynierowie z bogatym doświadczeniem praktycznym.

Nasi specjaliści posiadają certyfikaty bezpieczeństwa od renomowanych dostawców rozwiązań IT, takich jak Dell, Lenovo, HP, VMware i Veeam. Regularnie uczestniczą w szkoleniach i konferencjach, aby poszerzać swoją wiedzę i umiejętności w zakresie cyberbezpieczeństwa.

Korzyści ze współpracy z Intratel:

- Dostęp do wiedzy i doświadczenia ekspertów: Nasi eksperci posiadają bogate doświadczenie w zakresie cyberbezpieczeństwa i są na bieżąco z najnowszymi trendami i zagrożeniami.
- Indywidualne podejście: Dostosowujemy nasze usługi do specyficznych potrzeb każdego klienta.
- Szybka i skuteczna pomoc: Gwarantujemy szybką i skuteczną pomoc w przypadku wystąpienia incydentu cyberbezpieczeństwa.
- Pewność bezpieczeństwa: dzięki współpracy z nami będziesz pewny, że Twoja infrastruktura IT i dane są bezpieczne.

Intratel to Twój Partner w cyfrowej rewolucji

Od ponad 20 lat integrujemy rozwiązania informatyczne, łącząc wiedzę inżynierską z profesjonalnym doradztwem w zakresie strategii IT.

CENTRA DANYCH

OCHRONA DANYCH

DOSTAWA I DOBÓR SPRZĘTU

CHMURA

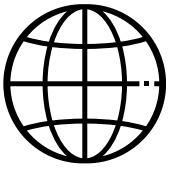
THREAT MANAGEMENT

PRZECHOWYWANIE DANYCH

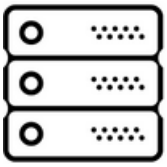
WIRTUALIZACJA

OUTSOURCING

SERWERY



USŁUGI SIECIOWE



MACIERZE

SOFTWARE HOUSE

1000+ projektów

500+ klientów

3 lokalizacje (Polska i USA)

50+ pracowników

80% to inżynierowie

2 data center

INTRATEL

Intratel to Twój zaufany partner w zakresie cyberbezpieczeństwa. Skontaktuj się z nami już dziś, aby dowiedzieć się więcej o naszych rozwiązaniach i uzyskać pomoc w spełnieniu wymagań dyrektywy NIS2.

Porozmawiajmy!

+48 85 662 30 71

www.intratel.pl

intratel@intratel.pl

Al. Tysiąclecia P.P. 39A 15-111 Białystok