GRUNDIG

Przewodnik GRUNDIG Security dotyczący zgodności z NIS2

Wersja 05/2026

Przedmowa

Dyrektywa NIS2 Unii Europejskiej[1] znacznie zaostrza wymagania dotyczące cyberbezpieczeństwa dla obiektów o znaczeniu krytycznym i ich łańcuchów dostaw. **GRUNDIG** Security, jako producent posiadający certyfikaty ISO 9001 i ISO 27001, oferuje precyzyjnie dopasowane, zgodne z prawem rozwiązania w zakresie techniki wizyjnej, aby skutecznie spełnić te surowe wymogi prawne.

Kontekst regulacji

Od stycznia 2023 r. dyrektywa NIS2 obowiązuje na poziomie UE w celu konsekwentnej harmonizacji ogólnego poziomu bezpieczeństwa systemów sieciowych i informatycznych. Wdrożenie krajowe rozszerza krąg przedsiębiorstw objętych dyrektywą w Niemczech z dotychczasowych 4500 do około 29 500 organizacji. To ogromne rozszerzenie zmusza całe gałęzie gospodarki do gruntownej reorganizacji strategii IT.

Lata 2025 i 2026 wymagają od europejskich przedsiębiorstw radykalnego zwiększenia ich cyberodporności ze względu na niestabilną sytuację geopolityczną w zakresie bezpieczeństwa. Nowa dyrektywa NIS2 rozwiązuje problem niedoskonałości rynku w zakresie bezpieczeństwa IT poprzez szeroko zakrojone i rygorystyczne wymogi regulacyjne. Jako producent sprzętu wideo, **GRUNDIG** Security aktywnie wspiera projektantów, instalatorów i operatorów w zapewnieniu wymaganego bezpieczeństwa w łańcuchu dostaw.

Główne cele dyrektywy

NIS2 ma na celu znaczne wzmocnienie gotowości obronnej całej europejskiej gospodarki przed zagrożeniami cyfrowymi i fizycznymi. W tym celu ustawa nakłada surowsze standardy w zakresie zarządzania ryzykiem cybernetycznym, utrzymania ciągłości działania oraz zarządzania słabymi punktami. Ponadto koncepcja ochrony zostaje obowiązkowo rozszerzona poza granice przedsiębiorstwa na dostawców i usługodawców.

Znaczenie dla techniki wideo w ujęciu ogólnym

Nowoczesne systemy monitoringu wizyjnego są silnie połączone w sieć i głęboko zintegrowane ze złożonymi środowiskami IT oraz OT operatorów. Dzięki temu są one uznawane za istotne dla bezpieczeństwa i stanowią potencjalną furtkę dla poważnych cyberataków.

Klasyfikacja obiektów

Dyrektywa NIS2 klasyfikuje organizacje objęte jej zakresem w oparciu o ich krytyczność w dwóch głównych kategoriach. Różnice przejawiają się przede wszystkim w wielkości przedsiębiorstwa, nadzorze administracyjnym oraz ramach sankcji prawnych.

Klasyfikacja: obiekty o znaczeniu krytycznym

Do obiektów o znaczeniu kluczowym zaliczają się duże przedsiębiorstwa z sektorów o wysokim stopniu krytyczności, takich jak energetyka, transport, bankowość, opieka zdrowotna i infrastruktura cyfrowa. Operatorzy klasycznych obiektów krytycznych (KRITIS) automatycznie należą do tej najwyższej klasy regulacyjnej. Organizacje te podlegają najsurowszemu nadzorowi administracyjnemu i muszą wykazać się najwyższymi standardami odporności.

[1] źródło: https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/raising-awareness-campaigns/network-and-information-systems-directive-2-nis2

Klasyfikacja: Obiekty ważne

Kategoria ważnych obiektów obejmuje średnie i duże przedsiębiorstwa z sektorów takich jak gospodarka odpadami, produkcja żywności, przemysł przetwórczy i chemiczny. Przedsiębiorstwa uznaje się za średnie, jeśli zatrudniają ponad 50 pracowników lub generują obroty przekraczające 10 milionów euro. Chociaż nadzór w tym przypadku ma charakter reaktywny, podstawowe wymagania bezpieczeństwa dla tych przedsiębiorstw są identyczne.

Cechy	Obiekty o znaczeniu kluczowym	Obiekty o znaczeniu kluczowym
Przynależność do sektora	Wysoce krytyczne (np. KRITIS, energetyka)	Inne sektory krytyczne (np. żywność)
Wielkość przedsiębiorstwa	Duże przedsiębiorstwa (>250 pracowników)	Średnie i duże przedsiębiorstwa (>50 pracowników)
Rodzaj nadzoru	Rygorystyczny i proaktywny	Reaktywny (w zależności od sytuacji)
Maksymalna grzywna	10 mln EUR lub 2% globalnego obrotu	7 mln € lub 1,4% globalnego obrotu

Identyfikacja i rejestracja

Przedsiębiorstwa mają obowiązek samodzielnie sprawdzić, czy dyrektywa NIS2 ich dotyczy, i zidentyfikować to zgodnie z prawem. Organizacje, których to dotyczy, muszą się zarejestrować w odpowiednim urzędzie krajowym, takim jak BSI w Niemczech. Konieczne jest też wskazanie urzędowi centralnego punktu kontaktowego ds. zarządzania bezpieczeństwem informacji.

Wykonawcy i projektanci muszą wspólnie zapewnić zgodność z przepisami.

Rygorystyczne obowiązki zgłaszania

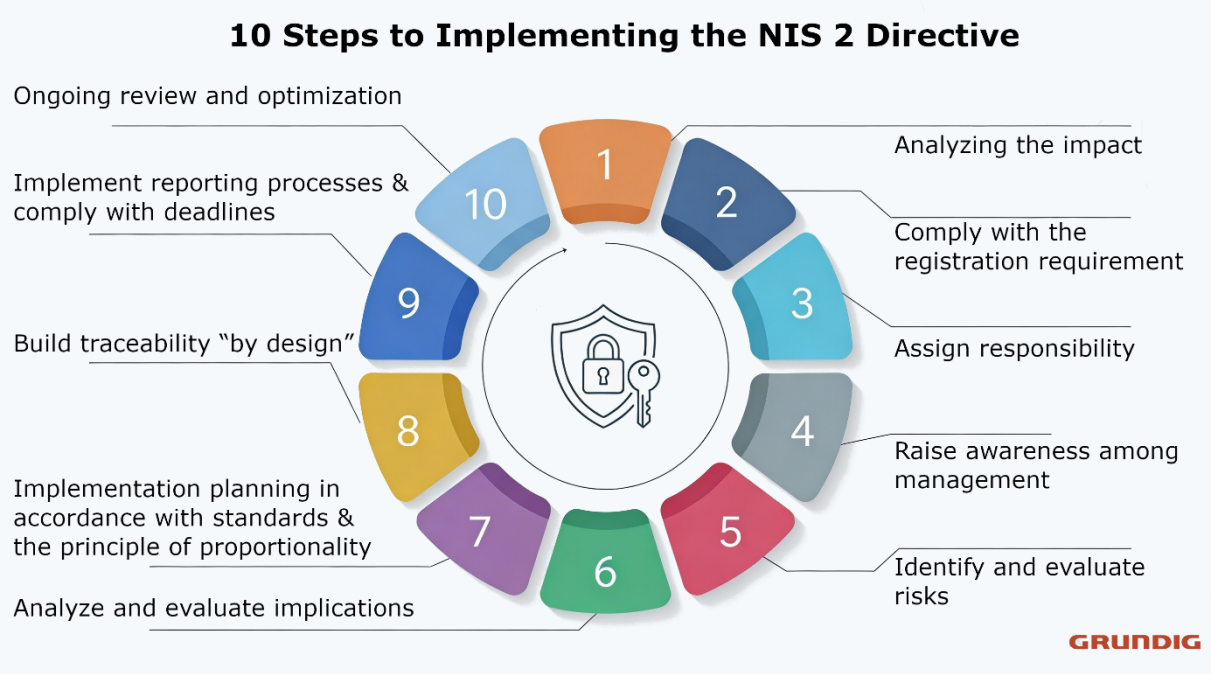
W przypadku poważnych incydentów związanych z bezpieczeństwem instytucje muszą w ciągu 24 godzin przekazać oficjalne wczesne ostrzeżenie organowi nadzorczemu. Ustawodawca wymaga szczegółowego i kompleksowego zgłoszenia incydentu najpóźniej w ciągu 72 godzin. W ciągu miesiąca organ może również zażądać szczegółowego raportu końcowego dotyczącego przyczyn i podjętych środków zaradczych.

Przedsiębiorstwa podlegające regulacjom muszą w każdej chwili wykazać się wysoką gotowością do współpracy z państwowymi organami kontrolnymi. Obejmuje to sprawne udostępnianie informacji oraz tymczasowy dostęp do systemów informatycznych na potrzeby dochodzeń urzędowych. Proaktywna współpraca ma tutaj decydujące znaczenie dla szybkiego zapobiegania zagrożeniom systemowym dla społeczeństwa.

Obowiązki dokumentacyjne

Wszystkie wdrożone środki bezpieczeństwa i procesy operacyjne muszą być dokumentowane w sposób kompletny i zrozumiały. Skuteczność tych dowodów należy weryfikować poprzez regularne,

niezależne audyty. Na żądanie organów te uporządkowane dokumenty muszą być dostępne w dowolnym momencie i w odpowiednim terminie.



Środki bezpieczeństwa cybernetycznego

Ustawa wymaga odpowiednich środków technicznych, operacyjnych i organizacyjnych w celu zminimalizowania daleko idących zagrożeń cybernetycznych. Obejmują one kompleksowe strategie tworzenia kopii zapasowych, procedury odzyskiwania danych po awarii oraz systematyczne zarządzanie reagowaniem na incydenty. W obszarach wrażliwych wyraźnie zalecane jest również stosowanie bezpiecznej komunikacji głosowej, wideo i tekstowej.

Wymagana cyberhigiena

Instytucje muszą rygorystycznie egzekwować podstawowe praktyki cyberhigieny, aby zminimalizować powierzchnię ataku. Obejmuje to obowiązkowe szkolenia pracowników, ścisłą kontrolę dostępu oraz konsekwentne zarządzanie zasobami. Ponadto konieczne jest wdrożenie uwierzytelniania wieloskładnikowego dla wszystkich krytycznych dostępów do systemów.

Grożące sankcje i odpowiedzialność kierownictwa klienta końcowego

W przypadku tzw. „niezgodności" kluczowym podmiotom grożą drastyczne kary w wysokości do 10 milionów euro lub 2 procent światowego rocznego obrotu. W przypadku ważnych podmiotów górna granica wynosi 7 milionów euro lub 1,4 procent globalnego obrotu. Te ogromne kary mają pełnić rolę odstraszającą i wymusić nadanie priorytetowego znaczenia bezpieczeństwu IT w przedsiębiorstwach.

Dzięki NIS2 cyberbezpieczeństwo awansuje strategicznie na najwyższy szczebel zarządzania i zostaje ostatecznie uznane za sprawę priorytetową. Dyrektorzy zarządzający i członkowie zarządu będą w przyszłości ponosić osobistą odpowiedzialność za naruszenia lub zaniedbania związane z nieprzestrzeganiem obowiązków prawnych. Ponadto ustawa przewiduje obowiązkowe, regularne szkolenia z zakresu bezpieczeństwa dla całego kierownictwa.

Ryzyko związane z nieprzestrzeganiem przepisów

Producenci bez udokumentowanych procesów cyberbezpieczeństwa będą systematycznie wykluczani z łańcuchów dostaw podmiotów podlegających regulacjom NIS2. Ponadto w przypadku incydentów

związanych z bezpieczeństwem mogą ponieść konsekwencje finansowe wynikające z odpowiedzialności za produkt i wysokich roszczeń regresowych. Również ryzyko geopolityczne oraz brak na międzynarodowych listach zaufanych podmiotów prowadzą do bezpośredniego wykluczenia z rynku.

GRUNDIG Security jako partner

GRUNDIG Security, jako niezawodny europejski partner, oferuje dostosowane do indywidualnych potrzeb wsparcie w zakresie zgodności z NIS2 dla swoich profesjonalnych klientów. Łączymy wydajny sprzęt z elastycznym oprogramowaniem do zarządzania obrazem C-WERK, tworząc wysoce bezpieczny, kompleksowy system. Dzięki temu zintegrowanemu podejściu operatorzy instalacji zyskują ogromne ułatwienie w wypełnianiu swoich obowiązków związanych z łańcuchem dostaw.

Stan techniki

Dyrektywa NIS2 wymaga, aby urządzenia IT odpowiadały aktualnemu stanowi techniki. Obejmuje to oczywiście wykorzystanie kamer, rejestratorów i serwerów.

Kamery, rejestratory i serwery są popularnymi celami cyberataków. Niezależnie od tego, czy chodzi o szpiegowanie zachowań, czy o tworzenie tzw. sieci botów – dostęp do oprogramowania sprzętowego i oprogramowania techniki bezpieczeństwa jest z punktu widzenia atakującego bardzo opłacalny.

Jeśli chodzi o cyberbezpieczeństwo, nasze linie produktów są wzmocnione pod kątem wersji oprogramowania sprzętowego, przetestowane pod kątem różnych wektorów ataku i podlegają ciągłym audytom wewnętrznym.

Sztuczna inteligencja i analiza wideo

Wymagany stan techniki w dziedzinie technologii wideo coraz częściej wymaga wykorzystania sztucznej inteligencji do automatycznego wykrywania zagrożeń. Linia SMART firmy **GRUNDIG** Security przetwarza analizy, takie jak rozpoznawanie twarzy, monitorowanie obwodu i wirtualna linia alarmowa, zgodnie z przepisami o ochronie danych bezpośrednio w kamerze, rejestratorze lub serwerze.

Security by Design

Zgodnie z art. 21 dyrektywy NIS2 produkty IT muszą być projektowane zgodnie z rygorystycznymi zasadami bezpieczeństwa już w pierwszej fazie rozwoju. **GRUNDIG** Security konsekwentnie wdraża filozofię „Security by Design” w systemie zarządzania obrazem C-WERK oraz we wszystkich oferowanych kamerach sieciowych. Systemy monitoringu są standardowo dostarczane klientom końcowym z bezpiecznymi ustawieniami domyślnymi (Security by Default) i zminimalizowaną powierzchnią ataku.

Innowacyjne funkcje linii SMART, takie jak „One-Click-Disable”, w razie potrzeby blokują wszelką komunikację z Internetem – nawet jeśli urządzenia otrzymają prawidłowy adres bramy sieciowej do połączenia.

Chmura i szyfrowanie

Ciągła, bezpieczna transmisja danych to podstawowy wymóg wynikający z obowiązków w zakresie zarządzania ryzykiem NIS2. **GRUNDIG** Security umożliwia płynną i silnie szyfrowaną komunikację między lokalnym sprzętem a podłączoną chmurą C-WERK. Ta architektura niezawodnie chroni wrażliwe metadane przed dostępem nieuprawnionych osób trzecich i zapewnia zgodność z przepisami prawa w przypadku projektów monitoringu obejmujących wiele lokalizacji.

Nacisk na bezpieczeństwo łańcucha dostaw

Kluczowym elementem dyrektywy NIS2 jest konsekwentne zabezpieczenie całego łańcucha dostaw zgodnie z art. 21. Objęte nią podmioty muszą ściśle monitorować i kontrolować cyberbezpieczeństwo swoich dostawców i usługodawców. Łańcuch bezpieczeństwa organizacji jest ostatecznie tak odporny, jak jej najsłabszy zewnętrzny dostawca.

Certyfikowane procesy bezpieczeństwa

Najbardziej wiarygodną odpowiedzią na wymogi NIS2 dotyczące dokumentacji w łańcuchu dostaw są niezależne i międzynarodowe certyfikaty. **GRUNDIG** Security posiada wymagające certyfikaty ISO 9001 w zakresie zarządzania jakością oraz ISO 27001 w zakresie własnego zarządzania bezpieczeństwem informacji. Te oficjalne certyfikaty gwarantują klientom, że wszystkie procesy rozwojowe i biznesowe podlegają najwyższym standardom bezpieczeństwa i są systematycznie kontrolowane przez niezależne podmioty.

Zgodność i zaufanie

Absolutna niezależność geopolityczna jest decydującym kryterium wyboru godnych zaufania dostawców technologii w ramach systemu NIS2. Wszystkie kamery i rejestratory z linii SMART firmy **GRUNDIG** Security są zatem w pełni zgodne z surowymi normami NDAA. Wyklucza to krytyczne komponenty od dostawców wysokiego ryzyka i zapewnia cyfrową suwerenność krytycznej infrastruktury europejskiej.

Nasze kamery i rejestratory z serii Smart-Line spełniają ponadto wytyczne dotyczące tzw. zgodności z NDAA. Zakaz ten uniemożliwia organom władzy w USA oraz ich wykonawcom korzystanie z technologii telekomunikacyjnych i monitoringu wizyjnego niektórych chińskich producentów w celu zminimalizowania zagrożeń dla bezpieczeństwa.

Zarządzanie lukami w zabezpieczeniach

Zwinne i proaktywne zarządzanie podatnościami jest prawnie wymagane w przypadku kluczowych obiektów. **GRUNDIG** Security wspiera swoich klientów końcowych w tym zakresie poprzez ciągłe aktualizacje oprogramowania sprzętowego i niezwykle szybkie dostarczanie poprawek bezpieczeństwa. Ścisła zgodność z otwartymi standardami, takimi jak ONVIF, zapewnia ponadto długoterminową kompatybilność systemów z produktami innych producentów.

GRUNDIG Security wraz z partnerem technologicznym Axxonsoft uczestniczy w programie „Common Vulnerabilities and Exposures (CVE)" firmy MITRE Corporation. Ten znormalizowany system identyfikacji i katalogowania publicznie znanych luk w cyberbezpieczeństwie oprogramowania i sprzętu umożliwia publikację i śledzenie wektorów ataku.

Więcej informacji można znaleźć pod następującym linkiem:
https://www.cve.org/PartnerInformation/ListofPartners/partner/AxxonSoft

Uwierzytelnianie sieciowe

Europejskie przepisy wymagają ścisłej kontroli dostępu oraz stosowania solidnych metod kryptograficznych w celu ochrony sieci zakładowych. Rejestratory i kamery IP firmy **GRUNDIG** Security obsługują złożone wejścia alarmowe oraz najnowocześniejsze mechanizmy uwierzytelniania zgodne ze standardami IEEE. W ten sposób wszystkie produkty z linii Smart-Line obsługują port-based network access control (PNAC) zgodnie z normą IEEE 802.1X.

System C-WERK VMS oferuje jednocześnie zabezpieczone pod kątem kryminalistycznym zarządzanie uprawnieniami, które całkowicie wyklucza technicznie nieuprawnioną manipulację danymi.

Wniosek

Operatorzy systemów wideo muszą bezwzględnie zapewnić, że ich infrastruktura IT bez problemu sprosta przyszłym regulacjom. Płynna integracja technologii IP i HD-TVI w portfolio **GRUNDIG** Security umożliwia skalowalną i bezpieczną pod względem inwestycyjnym migrację istniejących instalacji. Gwarantuje to ekonomicznie proporcjonalne, a jednocześnie w pełni zgodne z prawem wdrożenie wymaganych środków technicznych.

Dzięki wyłącznej współpracy z producentem posiadającym certyfikat ISO 27001, takim jak **GRUNDIG** Security, przedsiębiorstwa o znaczeniu krytycznym znacznie ograniczają własne ryzyko związane z nieprzestrzeganiem przepisów. Kompletna dokumentacja i potwierdzenie bezpieczeństwa produktów niezawodnie chronią instytucje przed sankcjami państwowymi sięgającymi milionów euro. Jednocześnie podejście to znacznie odciąża kierownictwo od zagrażających egzystencji przedsiębiorstwa ryzyk związanych z osobistą odpowiedzialnością.

www.grundig-security.com

Abetechs GmbH (**GRUNDIG** Security)

info@grundig-security.com

GRUNDIG