GRUNDIG

GRUNDIG Security NIS2 Compliance Guide

Revision 05/2026

Vorwort

Die NIS2-Richtlinie der Europäischen Union[1] verschärft die Cybersicherheitsanforderungen für kritische Einrichtungen und deren Lieferketten drastisch. **GRUNDIG** Security bietet als ISO 9001 und ISO 27001 zertifizierter Hersteller passgenaue, rechtskonforme Videotechniklösungen, um diese strengen gesetzlichen Vorgaben effizient zu erfüllen.

Hintergrund der Regulierung

Seit Januar 2023 ist die NIS2-Richtlinie auf EU-Ebene in Kraft, um das allgemeine Sicherheitsniveau von Netz- und Informationssystemen konsequent zu harmonisieren. Die nationale Umsetzung erweitert den Kreis der betroffenen Unternehmen in Deutschland von bisher 4.500 auf rund 29.500 Organisationen. Diese massive Ausweitung zwingt ganze Wirtschaftszweige zu einer grundlegenden Neuausrichtung ihrer IT-Strategien.

Die Jahre 2025 und 2026 fordern von europäischen Unternehmen eine drastische Erhöhung ihrer Cyberresilienz aufgrund einer volatilen geopolitischen Sicherheitslage. Die neue NIS2-Richtlinie adressiert das Marktversagen in der IT-Sicherheit durch weitreichende und strenge regulatorische Vorgaben. Als Hersteller von Videotechnik unterstützt **GRUNDIG** Security betroffene Planer, Errichter und Betreiber aktiv dabei, die geforderte Sicherheit in der Lieferkette sicherzustellen.

Kernziele der Richtlinie

NIS2 zielt darauf ab, die Abwehrbereitschaft der gesamten europäischen Wirtschaft gegen digitale und physische Bedrohungen massiv zu stärken. Hierfür legt das Gesetz strengere Maßstäbe an das Cyber-Risikomanagement, die Aufrechterhaltung des Geschäftsbetriebs und das Schwachstellenmanagement an. Zudem wird der Schutzgedanke über Unternehmensgrenzen hinweg verbindlich auf Zulieferer und Dienstleister ausgeweitet.

Bedeutung für Videotechnik im Allgemeinen

Moderne Videoüberwachungssysteme sind hochvernetzt und tief in komplexe IT- sowie OT-Umgebungen der Betreiber integriert. Dadurch gelten sie als sicherheitsrelevant und stellen ein potenzielles Einfallstor für schwerwiegende Cyberangriffe dar.

Klassifizierung der Einrichtungen

Die NIS2-Richtlinie klassifiziert betroffene Organisationen basierend auf ihrer Kritikalität in zwei Hauptkategorien. Die Unterschiede manifestieren sich primär in der Unternehmensgröße, der behördlichen Aufsicht und dem gesetzlichen Sanktionsrahmen.

Klassifizierung: Wesentliche Einrichtungen

Zu den wesentlichen Einrichtungen zählen große Unternehmen aus hochkritischen Sektoren wie Energie, Verkehr, Bankwesen, Gesundheit und digitaler Infrastruktur. Betreiber von klassischen kritischen Anlagen (KRITIS) fallen automatisch in diese höchste Regulierungsklasse. Diese Organisationen unterliegen der strengsten behördlichen Aufsicht und müssen höchste Resilienzstandards nachweisen.

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

Klassifizierung: Wichtige Einrichtungen

Die Kategorie der wichtigen Einrichtungen umfasst mittlere und große Unternehmen aus Sektoren wie Abfallwirtschaft, Lebensmittelproduktion, verarbeitendes Gewerbe und Chemieindustrie. Unternehmen gelten als mittelgroß, wenn sie mehr als 50 Mitarbeitende beschäftigen oder über 10 Millionen Euro Umsatz generieren. Obwohl die Aufsicht hier reaktiv erfolgt, sind die grundlegenden Sicherheitsanforderungen für diese Betriebe identisch.

Merkmal	Wesentliche Einrichtungen	Wichtige Einrichtungen
Sektoren-Zugehörigkeit	Hochkritisch (z. B. KRITIS, Energie)	Sonstige kritische (z. B. Lebensmittel)
Unternehmensgröße	Großunternehmen (>250 Mitarbeitende)	Mittlere und große Unternehmen (>50 Mitarbeitende)
Art der Aufsicht	Streng und proaktiv	Reaktiv (anlassbezogen)
Maximales Bußgeld	10 Mio. € oder 2% des globalen Umsatzes	7 Mio. € oder 1,4% des globalen Umsatzes

Identifizierung und Registrierung

Unternehmen stehen in der Pflicht, ihre Betroffenheit durch die NIS2-Richtlinie selbstständig zu prüfen und rechtskonform zu identifizieren. Betroffene Organisationen müssen sich bei der zuständigen nationalen Behörde, wie dem BSI in Deutschland, zwingend registrieren. Eine zentrale Kontaktstelle für das Informationssicherheitsmanagement ist dabei verpflichtend gegenüber der Behörde zu benennen.

Errichter und Planer müssen in Zusammenarbeit die Erfüllung sicherstellen.

Strenge Meldepflichten

Bei erheblichen Sicherheitsvorfällen müssen Einrichtungen innerhalb von 24 Stunden eine offizielle Frühwarnung an die Aufsichtsbehörde übermitteln. Eine detaillierte und umfassende Meldung des Vorfalls wird nach spätestens 72 Stunden vom Gesetzgeber verlangt. Innerhalb eines Monats kann die Behörde zudem einen ausführlichen Abschlussbericht zu Ursachen und ergriffenen Gegenmaßnahmen einfordern.

Regulierte Unternehmen müssen jederzeit eine hohe Kooperationsbereitschaft gegenüber staatlichen Prüfstellen nachweisen. Dies beinhaltet die reibungslose Bereitstellung von Informationen und den temporären Zugang zu IT-Systemen für behördliche Untersuchungen. Eine proaktive Zusammenarbeit ist hierbei entscheidend, um systemische Gefahren für das Gemeinwesen schnell abzuwenden.

Dokumentationspflichten

Sämtliche implementierten Sicherheitsmaßnahmen und operativen Prozesse müssen lückenlos und nachvollziehbar dokumentiert werden. Diese Nachweise sind durch regelmäßige, unabhängige Audits auf ihre Wirksamkeit zu überprüfen. Auf Anforderung der Behörden müssen diese strukturierten Belege jederzeit fristgerecht vorgelegt werden können.

Cybersicherheitsmaßnahmen

Das Gesetz fordert geeignete technische, operative und organisatorische Maßnahmen zur Minimierung von weitreichenden Cyberrisiken. Hierzu gehören umfassende Backup-Strategien, Disaster-Recovery-Verfahren und ein systematisches Incident-Response-Management. Auch der Einsatz sicherer Sprach-, Video- und Text-Kommunikation ist in sensiblen Bereichen explizit vorgeschrieben.

Geforderte Cyberhygiene

Einrichtungen müssen grundlegende Praktiken der Cyberhygiene rigoros durchsetzen, um Angriffsflächen zu minimieren. Dies umfasst verpflichtende Mitarbeiterschulungen, strenge Zugriffskontrollen und ein konsequent gepflegtes Asset-Management. Zudem müssen Multi-Faktor-Authentifizierungen für alle kritischen Systemzugänge zwingend etabliert werden.

Drohende Sanktionen und Haftung der Geschäftsleitung des Endkunden

Bei sogenannter „Non-Compliance“ drohen wesentlichen Einrichtungen drastische Bußgelder in Höhe von bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Jahresumsatzes. Für wichtige Einrichtungen liegt die Obergrenze bei 7 Millionen Euro oder 1,4 Prozent des globalen Umsatzes. Diese enormen Strafen sollen eine abschreckende Wirkung entfalten und die Priorisierung von IT-Sicherheit in den Betrieben erzwingen.

Die Cybersicherheit rückt durch NIS2 strategisch auf die oberste Managementebene und wird endgültig zur Chefsache erklärt. Geschäftsführer und Vorstände haften bei Verstößen oder Versäumnissen künftig persönlich für die Nichteinhaltung der gesetzlichen Pflichten. Zudem sieht das Gesetz zwingende, regelmäßige Sicherheitsschulungen für die gesamte Geschäftsleitung vor.

Risiken bei Nichtbeachtung

Hersteller ohne nachweisbare Cybersecurity-Prozesse werden systematisch aus den Lieferketten von regulierten NIS2-Einrichtungen verbannt. Darüber hinaus können sie bei Sicherheitsvorfällen durch die Produkthaftung und hohe Regressansprüche finanziell belangt werden. Auch geopolitische Risiken und das Fehlen auf internationalen Vertrauenslisten führen zum direkten Marktausschluss.

GRUNDIG Security als Partner

GRUNDIG Security bietet als verlässlicher, europäischer Partner maßgeschneiderte Unterstützung für die NIS2-Compliance seiner professionellen Kunden. Wir verknüpfen leistungsstarke Hardware mit der flexiblen Video-Management-Software C-WERK zu einem hochsicheren Gesamtsystem. Durch diesen integrativen Ansatz werden Anlagenbetreiber bei der Umsetzung ihrer Lieferkettenpflichten massiv entlastet.

Stand der Technik

Die NIS2-Richtlinie fordert von IT Geräten, dem aktuellen Stand der Technik entsprechen. Dies inkludiert natürlich den Einsatz von Kameras, Rekordern und Servern.

Kameras, Rekorder und Server sind beliebte Ziele von Cyberattacken. Egal zum Ausspionieren von Verhaltensweisen oder dem Aufbau eines sogenannten Bot-Netzwerkes – der Zugang zu der Firmware und Software von Sicherheitstechnik ist aus Sicht eines Angreifers sehr lohnenswert.

In Bezug auf Cybersicherheit sind Firmwarestände unsere Produktlinien gehärtet, gegen diverse Angriffsvektoren geprüft und werden permanent intern auditiert.

KI und Videoanalyse

Der geforderte Stand der Technik in der Videotechnik bedingt zunehmend den Einsatz künstlicher Intelligenz zur automatisierten Bedrohungserkennung. Die SMART-Linie von **GRUNDIG** Security verarbeitet Analysen wie Gesichtserkennung, Perimeterüberwachung und Virtual Tripwire datenschutzkonform direkt auf der Kamera, dem Rekorder oder dem Server.

Security by Design

Nach Artikel 21 der NIS2-Richtlinie müssen IT-Produkte bereits in der ersten Entwicklungsphase nach strengen Sicherheitsprinzipien gestaltet werden. **GRUNDIG** Security integriert diese Security by Design Philosophie konsequent in das C-WERK Videomanagementsystem und alle angebotenen Netzwerkkameras. Die Überwachungssysteme werden standardmäßig mit sicheren Voreinstellungen (Security by Default) und minimierten Angriffsflächen an die Endkunden ausgeliefert.

Innovative SMART-Line Funktionen wie „One-Click-Disable“ unterdrücken bei Bedarf jegliche Kommunikation in das Internet – selbst wenn Geräte ein gültiges Gateway zum Verbinden erhalten.

Cloud und Verschlüsselung

Eine durchgängig sichere Datenübertragung ist eine fundamentale Kernanforderung der NIS2-Risikomanagementpflichten. **GRUNDIG** Security ermöglicht eine nahtlose und hochverschlüsselte Kommunikation zwischen der lokalen Hardware und der angebundenen C-WERK Cloud. Diese Architektur schützt sensible Metadaten zuverlässig vor dem Zugriff unbefugter Dritter und sichert standortübergreifende Überwachungsprojekte rechtssicher ab.

Fokus auf Lieferkettensicherheit

Ein zentrales Element der NIS2-Richtlinie ist die konsequente Sicherung der gesamten Lieferkette nach Artikel 21. Betroffene Einrichtungen müssen die Cybersicherheit ihrer Vorlieferanten und Dienstleister streng überwachen und auditieren. Die Sicherheitskette einer Organisation ist letztlich nur so widerstandsfähig wie ihr schwächster eingesetzter Drittanbieter.

Zertifizierte Sicherheitsprozesse

Die verlässlichste Antwort auf die NIS2-Nachweispflichten in der Lieferkette sind unabhängige und internationale Zertifizierungen. **GRUNDIG** Security verfügt über die anspruchsvollen Zertifizierungen ISO 9001 für Qualitätsmanagement und ISO 27001 für das eigene Informationssicherheitsmanagement. Diese offiziellen Gütesiegel garantieren den Kunden, dass sämtliche Entwicklungs- und Unternehmensprozesse höchsten Sicherheitsstandards unterliegen und systematisch von dritten auditiert werden.

Konformität und Vertrauen

Absolute geopolitische Unabhängigkeit ist ein entscheidendes Kriterium für die Auswahl vertrauenswürdiger Technologie-Zulieferer unter dem NIS2-Regime. Sämtliche Kameras und Rekorder der SMART-Linie von **GRUNDIG** Security entsprechen daher vollumfänglich den strengen NDAA-Standards. Dies schließt kritische Bauteile von Hochrisiko-Anbietern aus und sichert die digitale Souveränität kritischer europäischer Infrastrukturen.

Unsere Smart-Line Kameras und Rekorder erfüllen zudem die Richtlinien für die sogenannte NDAA compliance. Dies verbietet US-Behörden und deren Auftragnehmern die Nutzung von Telekommunikations- und Videoüberwachungstechnik bestimmter chinesischer Hersteller, um Sicherheitsrisiken zu minimieren.

Schwachstellenmanagement

Ein agiles und proaktives Vulnerability-Management ist für wesentliche Einrichtungen gesetzlich zwingend vorgeschrieben. **GRUNDIG** Security unterstützt seine Endkunden hierbei durch kontinuierliche Firmware-Updates und die extrem schnelle Bereitstellung von Sicherheitspatches. Die strikte Kompatibilität zu offenen Standards wie ONVIF stellt zudem sicher, dass die Systeme langfristig kompatibel mit Drittherstellern bleiben.

GRUNDIG Security nimmt mit dem Technologiepartner Axxonsoft am „Common Vulnerabilities and Exposures (CVE)“ der MITRE Corporation teil. Dieses standardisierte System zur Identifizierung und Katalogisierung öffentlich bekannter Cybersicherheitslücken in Software und Hardware stellt die Veröffentlichung und die Nachverfolgung von Angriffsvektoren zur Verfügung.

Mehr Informationen unter folgendem Link:
https://www.cve.org/PartnerInformation/ListofPartners/partner/AxxonSoft

Netzwerkauthentifizierung

Das europäische Gesetz verlangt strenge Zugangskontrollen und den Einsatz robuster kryptografischer Verfahren zum Schutz der Anlagennetzwerke. **GRUNDIG** Security Rekorder und IP-Kameras unterstützen komplexe Alarm-Eingänge sowie modernste Authentifizierungsmechanismen nach IEEE-Standards. So untertsützen alle Produkte der Smart-Line port-based network access control (PNAC) entsprechend IEEE 802.1X.

Das C-WERK VMS bietet parallel eine forensisch abgesicherte Rechteverwaltung, die unberechtigte Datenmanipulationen technisch vollständig ausschließt.

Fazit

Betreiber von Videoanlagen müssen zwingend sicherstellen, dass ihre IT-Infrastruktur auch zukünftigen Regulierungen problemlos standhält. Die nahtlose Integration von IP- und HD-TVI-Technologien im Portfolio von **GRUNDIG** Security ermöglicht eine skalierbare und investitionssichere Migration bestehender Anlagen. Dies garantiert eine wirtschaftlich verhältnismäßige und dennoch vollumfänglich gesetzeskonforme Umsetzung der geforderten technischen Maßnahmen.

Durch die exklusive Zusammenarbeit mit einem ISO 27001 zertifizierten Hersteller wie **GRUNDIG** Security mindern kritische Unternehmen ihr eigenes Compliance-Risiko enorm. Die lückenlose Dokumentation und der Nachweis nachweislich sicherer Produkte schützen Einrichtungen zuverlässig vor staatlichen Sanktionen in Millionenhöhe. Gleichzeitig entlastet dieser Ansatz die Geschäftsleitung maßgeblich von existenzgefährdenden, persönlichen Haftungsrisiken.

www.grundig-security.com

Abetechs GmbH (**GRUNDIG** Security)

info@grundig-security.com

Änderungen und Fehler vorbehalten