GRUNDIG

Guide de conformité NIS2 de GRUNDIG Security

Révision 05/2026

Avant-propos

La directive NIS2 de l'Union européenne[1] renforce considérablement les exigences en matière de cybersécurité pour les infrastructures critiques et leurs chaînes d'approvisionnement. En tant que fabricant certifié ISO 9001 et ISO 27001, **GRUNDIG** Security propose des solutions de vidéosurveillance sur mesure et conformes à la législation afin de répondre efficacement à ces exigences légales strictes.

Contexte de la réglementation

Depuis janvier 2023, la directive NIS2 est en vigueur au niveau européen afin d'harmoniser de manière cohérente le niveau général de sécurité des réseaux et des systèmes d'information. La mise en œuvre nationale élargit le cercle des entreprises concernées en Allemagne, passant de 4 500 à environ 29 500 organisations. Cette extension massive oblige des secteurs économiques entiers à réorienter fondamentalement leurs stratégies informatiques.

Les années 2025 et 2026 exigeront des entreprises européennes qu'elles renforcent considérablement leur cyber-résilience en raison d'un contexte géopolitique instable. La nouvelle directive NIS2 remédie aux défaillances du marché en matière de sécurité informatique grâce à des exigences réglementaires étendues et strictes. En tant que fabricant de matériel vidéo, **GRUNDIG** Security aide activement les concepteurs, les installateurs et les opérateurs concernés à garantir la sécurité requise tout au long de la chaîne d'approvisionnement.

Objectifs principaux de la directive

La directive NIS2 vise à renforcer considérablement la capacité de défense de l'ensemble de l'économie européenne contre les menaces numériques et physiques. À cette fin, la loi impose des normes plus strictes en matière de gestion des risques cybernétiques, de continuité des activités et de gestion des vulnérabilités. En outre, le principe de protection est étendu de manière contraignante au-delà des limites de l'entreprise pour inclure les fournisseurs et les prestataires de services.

Implications pour la technologie vidéo en général

Les systèmes de vidéosurveillance modernes sont fortement interconnectés et profondément intégrés dans les environnements informatiques et opérationnels complexes des opérateurs. Ils sont donc considérés comme critiques pour la sécurité et constituent une porte d'entrée potentielle pour des cyberattaques graves.

Classification des entités

La directive NIS2 classe les organisations concernées en deux catégories principales en fonction de leur criticité. Les différences se manifestent principalement au niveau de la taille de l'entreprise, de la surveillance réglementaire et du cadre de sanctions légales.

Classification : entités essentielles

Les entités essentielles comprennent les grandes entreprises issues de secteurs hautement critiques tels que l'énergie, les transports, le secteur bancaire, la santé et les infrastructures numériques. Les opérateurs d'installations critiques classiques (KRITIS) relèvent automatiquement de cette catégorie réglementaire la plus élevée. Ces organisations sont soumises à la surveillance réglementaire la plus stricte et doivent démontrer qu'elles respectent les normes de résilience les plus élevées.

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

Classification : installations importantes

La catégorie des installations importantes comprend les moyennes et grandes entreprises issues de secteurs tels que la gestion des déchets, la production alimentaire, l'industrie manufacturière et l'industrie chimique. Les entreprises sont considérées comme de taille moyenne lorsqu'elles emploient plus de 50 personnes ou génèrent un chiffre d'affaires supérieur à 10 millions d'euros. Bien que la surveillance soit ici réactive, les exigences de sécurité fondamentales pour ces entreprises sont identiques.

Caractéristique	Installations essentielles	Installations importantes
Appartenance sectorielle	Très critiques (par ex. KRITIS, énergie)	Autres secteurs critiques (par exemple, agroalimentaire)
Taille de l'entreprise	Grandes entreprises (>250 employés)	Entreprises moyennes et grandes (>50 employés)
Type de surveillance	Stricte et proactive	Réactive (au cas par cas)
Amende maximale	10 millions d'euros ou 2 % du chiffre d'affaires mondial	7 millions d'euros ou 1,4 % du chiffre d'affaires mondial

Identification et enregistrement

Les entreprises ont l'obligation de vérifier de manière autonome si elles sont concernées par la directive NIS2 et de s'identifier conformément à la loi. Les organisations concernées doivent impérativement s'enregistrer auprès de l'autorité nationale compétente, telle que le BSI en Allemagne. Il est obligatoire de désigner auprès de l'autorité un point de contact central pour la gestion de la sécurité de l'information.

Les installateurs et les concepteurs doivent collaborer pour garantir la conformité.

Obligations de notification strictes

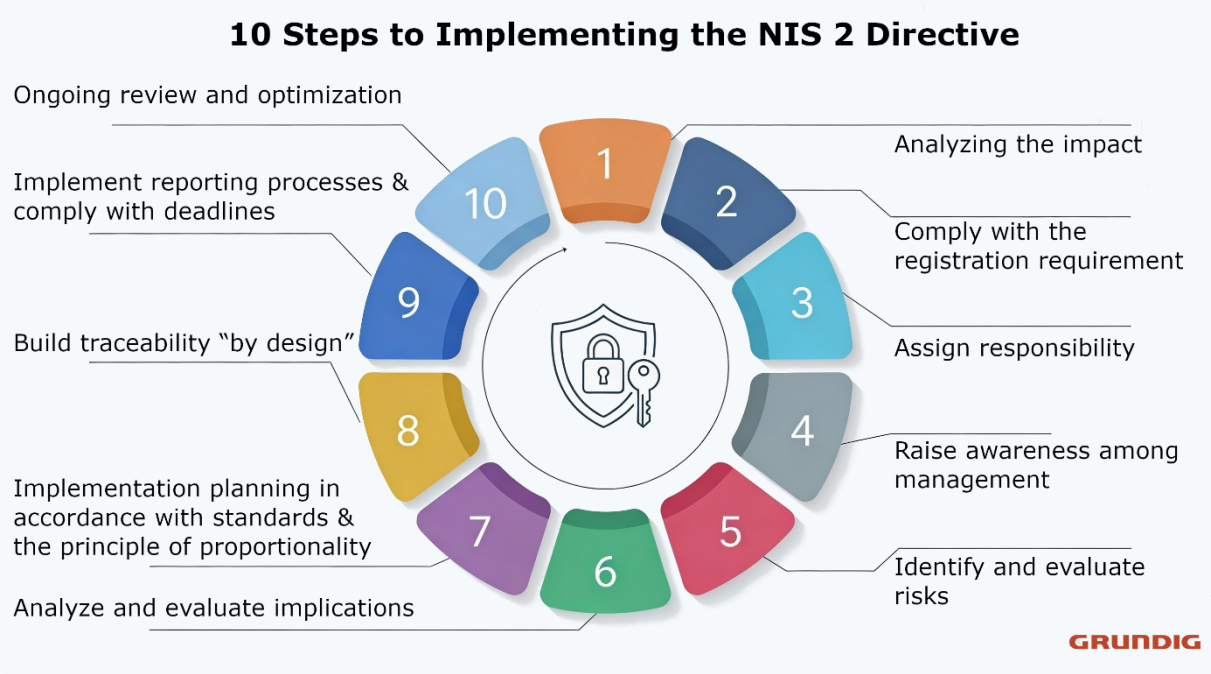
En cas d'incidents de sécurité majeurs, les établissements doivent transmettre une alerte précoce officielle à l'autorité de contrôle dans les 24 heures. Le législateur exige un rapport détaillé et complet sur l'incident au plus tard dans les 72 heures. Dans un délai d'un mois, l'autorité peut en outre exiger un rapport final détaillé sur les causes et les mesures correctives prises.

Les entreprises réglementées doivent à tout moment faire preuve d'une grande volonté de coopération envers les organismes de contrôle publics. Cela implique la mise à disposition sans difficulté d'informations et l'accès temporaire aux systèmes informatiques pour les enquêtes officielles. Une coopération proactive est ici décisive pour écarter rapidement les dangers systémiques pour la collectivité.

Obligations de documentation

Toutes les mesures de sécurité mises en œuvre et tous les processus opérationnels doivent être documentés de manière exhaustive et traçable. L'efficacité de ces preuves doit être vérifiée par des

audits réguliers et indépendants. À la demande des autorités, ces justificatifs structurés doivent pouvoir être présentés à tout moment dans les délais impartis.



Mesures de cybersécurité

La loi exige des mesures techniques, opérationnelles et organisationnelles appropriées pour minimiser les cyberrisques de grande ampleur. Cela inclut des stratégies de sauvegarde complètes, des procédures de reprise après sinistre et une gestion systématique des incidents. L'utilisation de moyens de communication vocale, vidéo et textuelle sécurisés est également explicitement prescrite dans les domaines sensibles.

Cybersécurité requise

Les établissements doivent appliquer rigoureusement les pratiques fondamentales de cyberhygiène afin de minimiser les surfaces d'attaque. Cela comprend des formations obligatoires pour les employés, des contrôles d'accès stricts et une gestion des actifs rigoureusement entretenue. De plus, l'authentification multifactorielle doit être mise en place de manière obligatoire pour tous les accès aux systèmes critiques.

Sanctions encourues et responsabilité de la direction du client final

En cas de « non-conformité », les entités importantes s'exposent à des amendes sévères pouvant atteindre 10 millions d'euros ou 2 % de leur chiffre d'affaires annuel mondial. Pour les entités essentielles, le plafond est fixé à 7 millions d'euros ou 1,4 % du chiffre d'affaires mondial. Ces sanctions colossales visent à avoir un effet dissuasif et à obliger les entreprises à faire de la sécurité informatique une priorité.

Grâce à la directive NIS2, la cybersécurité accède stratégiquement au plus haut niveau de la direction et devient définitivement une priorité absolue. À l'avenir, les dirigeants et les membres du conseil d'administration seront personnellement responsables du non-respect des obligations légales en cas d'infractions ou de négligences. En outre, la loi prévoit des formations obligatoires et régulières en matière de sécurité pour l'ensemble de la direction.

Risques en cas de non-respect

Les fabricants ne disposant pas de processus de cybersécurité vérifiables seront systématiquement exclus des chaînes d'approvisionnement des entités réglementées par la directive NIS2. De plus, en cas d'incidents de sécurité, ils s'exposent à des poursuites financières en vertu de la responsabilité du fait des produits et à d'importantes demandes de recours. Les risques géopolitiques et l'absence sur les listes de confiance internationales entraînent également une exclusion directe du marché.

GRUNDIG Security en tant que partenaire

En tant que partenaire européen fiable, **GRUNDIG** Security offre un accompagnement sur mesure pour la conformité NIS2 de ses clients professionnels. Nous combinons un matériel performant avec le logiciel de gestion vidéo flexible C-WERK pour former un système global hautement sécurisé. Cette approche intégrée allège considérablement la charge des exploitants d'installations dans la mise en œuvre de leurs obligations en matière de chaîne d'approvisionnement.

État de la technique

La directive NIS2 exige que les équipements informatiques soient conformes à l'état actuel de la technique. Cela inclut bien sûr l'utilisation de caméras, d'enregistreurs et de serveurs.

Les caméras, les enregistreurs et les serveurs sont des cibles privilégiées des cyberattaques. Qu'il s'agisse d'espionner des comportements ou de mettre en place un réseau de zombies, l'accès au micrologiciel et aux logiciels des équipements de sécurité est très intéressant pour un attaquant.

En matière de cybersécurité, les versions de micrologiciel de nos gammes de produits sont renforcées, testées contre divers vecteurs d'attaque et font l'objet d'audits internes permanents.

IA et analyse vidéo

L'état de l'art requis en matière de technologie vidéo implique de plus en plus le recours à l'intelligence artificielle pour la détection automatisée des menaces. La gamme SMART de **GRUNDIG Security** traite les analyses telles que la reconnaissance faciale, la surveillance périmétrique et le « virtual tripwire » (fil d'alerte virtuel) directement sur la caméra, l'enregistreur ou le serveur, dans le respect de la protection des données.

Sécurité dès la conception

Conformément à l'article 21 de la directive NIS2, les produits informatiques doivent être conçus selon des principes de sécurité stricts dès la première phase de développement. **GRUNDIG** Security intègre systématiquement cette philosophie de « Security by Design » dans le système de gestion vidéo C-WERK et dans toutes les caméras réseau proposées. Les systèmes de surveillance sont livrés aux clients finaux avec des paramètres de sécurité par défaut (Security by Default) et une surface d'attaque réduite au minimum.

Des fonctions innovantes de la gamme SMART-Line, telles que « One-Click-Disable », bloquent toute communication vers Internet si nécessaire, même si les appareils reçoivent une passerelle valide pour se connecter.

Cloud et cryptage

Une transmission des données sécurisée de bout en bout est une exigence fondamentale des obligations de gestion des risques NIS2. **GRUNDIG** Security permet une communication fluide et hautement cryptée entre le matériel local et le cloud C-WERK connecté. Cette architecture protège de manière fiable les métadonnées sensibles contre l'accès de tiers non autorisés et sécurise les projets de surveillance multi-sites dans le respect de la législation.

Priorité à la sécurité de la chaîne d'approvisionnement

Un élément central de la directive NIS2 est la sécurisation systématique de l'ensemble de la chaîne d'approvisionnement, conformément à l'article 21. Les entités concernées doivent surveiller et auditer rigoureusement la cybersécurité de leurs fournisseurs en amont et de leurs prestataires de services. En fin de compte, la chaîne de sécurité d'une organisation n'est aussi résistante que son prestataire tiers le plus faible.

Processus de sécurité certifiés

La réponse la plus fiable aux obligations de preuve NIS2 dans la chaîne d'approvisionnement réside dans des certifications indépendantes et internationales. **GRUNDIG** Security dispose des certifications exigeantes ISO 9001 pour la gestion de la qualité et ISO 27001 pour sa propre gestion de la sécurité de l'information. Ces labels de qualité officiels garantissent aux clients que tous les processus de développement et d'entreprise sont soumis aux normes de sécurité les plus élevées et font l'objet d'audits systématiques par des tiers.

Conformité et confiance

L'indépendance géopolitique absolue est un critère décisif pour la sélection de fournisseurs de technologies dignes de confiance dans le cadre du régime NIS2. Toutes les caméras et tous les enregistreurs de la gamme SMART de **GRUNDIG** Security sont donc pleinement conformes aux normes strictes de la NDAA. Cela exclut les composants critiques provenant de fournisseurs à haut risque et garantit la souveraineté numérique des infrastructures européennes critiques.

Nos caméras et enregistreurs Smart-Line sont également conformes aux directives de la NDAA. Ces directives interdisent aux autorités américaines et à leurs sous-traitants d'utiliser les technologies de télécommunication et de vidéosurveillance de certains fabricants chinois, afin de minimiser les risques pour la sécurité.

Gestion des vulnérabilités

Une gestion agile et proactive des vulnérabilités est légalement obligatoire pour les infrastructures essentielles. **GRUNDIG** Security soutient ses clients finaux dans ce domaine grâce à des mises à jour continues du micrologiciel et à la mise à disposition extrêmement rapide de correctifs de sécurité. La compatibilité stricte avec les normes ouvertes telles que l'ONVIF garantit en outre que les systèmes restent compatibles à long terme avec les fabricants tiers.

GRUNDIG Security participe, avec son partenaire technologique Axxonsoft, au programme « Common Vulnerabilities and Exposures (CVE) » de la MITRE Corporation. Ce système standardisé d'identification et de catalogage des failles de cybersécurité connues du public dans les logiciels et le matériel permet la publication et le suivi des vecteurs d'attaque.

Pour plus d'informations, consultez le lien suivant :
https://www.cve.org/PartnerInformation/ListofPartners/partner/AxxonSoft

Authentification réseau

La législation européenne exige des contrôles d'accès stricts et l'utilisation de procédures cryptographiques robustes pour la protection des réseaux d'installations. Les enregistreurs et caméras IP **GRUNDIG** Security prennent en charge des entrées d'alarme complexes ainsi que des mécanismes d'authentification de pointe conformes aux normes IEEE. Ainsi, tous les produits de la gamme Smart-Line prennent en charge le contrôle d'accès réseau basé sur les ports (PNAC) conformément à la norme IEEE 802.1X.

Le système de gestion vidéo C-WERK VMS offre en parallèle une gestion des droits sécurisée sur le plan légal, qui exclut techniquement toute manipulation non autorisée des données.

Conclusion

Les exploitants de systèmes vidéo doivent impérativement s'assurer que leur infrastructure informatique résiste sans problème aux réglementations futures. L'intégration transparente des technologies IP et HD-TVI dans le portefeuille de **GRUNDIG** Security permet une migration évolutive et sans risque pour l'investissement des installations existantes. Cela garantit une mise en œuvre économiquement raisonnable et pourtant pleinement conforme à la législation des mesures techniques requises.

Grâce à une collaboration exclusive avec un fabricant certifié ISO 27001 tel que **GRUNDIG** Security, les entreprises critiques réduisent considérablement leur propre risque de non-conformité. La documentation exhaustive et la certification de produits dont la sécurité est avérée protègent efficacement les établissements contre des sanctions publiques pouvant se chiffrer en millions. Parallèlement, cette approche décharge considérablement la direction des risques de responsabilité personnelle susceptibles de menacer l'existence même de l'entreprise.

www.grundig-security.com

Abetechs GmbH (**GRUNDIG** Security)

info@grundig-security.com

Sous réserve de modifications et d'erreurs.