GRUNDIG

Průvodce dodržováním normy NIS2 od společnosti GRUNDIG Security

Revize 05/2026

Předmluva

Směrnice NIS2 Evropské unie[1] výrazně zpřísňuje požadavky na kybernetickou bezpečnost pro kritická zařízení a jejich dodavatelské řetězce. Společnost **GRUNDIG** Security, jako výrobce s certifikací ISO 9001 a ISO 27001, nabízí přesně přizpůsobená řešení v oblasti video techniky, která jsou v souladu s právními předpisy a umožňují efektivní splnění těchto přísných zákonných požadavků.

Pozadí regulace

Od ledna 2023 je na úrovni EU v platnosti směrnice NIS2, jejímž cílem je důsledně harmonizovat obecnou úroveň bezpečnosti síťových a informačních systémů. Díky její implementaci na národní úrovni se okruh dotčených podniků v Německu rozšiřuje z dosavadních 4 500 na přibližně 29 500 organizací. Toto masivní rozšíření nutí celé hospodářské odvětví k zásadnímu přeorientování svých IT strategií.

Roky 2025 a 2026 vyžadují od evropských podniků drastické zvýšení jejich kybernetické odolnosti z důvodu nestabilní geopolitické bezpečnostní situace. Nová směrnice NIS2 řeší selhání trhu v oblasti IT bezpečnosti prostřednictvím rozsáhlých a přísných regulačních požadavků. Jako výrobce video techniky podporuje společnost **GRUNDIG** Security dotčené projektanty, instalatéry a provozovatele aktivně při zajišťování požadované bezpečnosti v dodavatelském řetězci.

Hlavní cíle směrnice

NIS2 si klade za cíl výrazně posílit obranyschopnost celého evropského hospodářství proti digitálním a fyzickým hrozbám. Za tímto účelem zákon stanoví přísnější standardy pro řízení kybernetických rizik, zachování provozu a řízení zranitelností. Kromě toho se princip ochrany závazně rozšiřuje i za hranice podniků na dodavatele a poskytovatele služeb.

Význam pro videotechniku obecně

Moderní video monitorovací systémy jsou vysoce propojené a hluboce integrované do komplexních IT a OT prostředí provozovatelů. Díky tomu jsou považovány za bezpečnostně relevantní a představují potenciální vstupní bránu pro závažné kybernetické útoky.

Klasifikace zařízení

Směrnice NIS2 klasifikuje dotčené organizace na základě jejich kritičnosti do dvou hlavních kategorií. Rozdíly se projevují především ve velikosti podniku, úředním dohledu a zákonném sankčním rámci.

Klasifikace: Podstatná zařízení

Mezi zásadní zařízení patří velké podniky z vysoce kritických odvětví, jako je energetika, doprava, bankovnictví, zdravotnictví a digitální infrastruktura. Provozovatelé klasických kritických zařízení (KRITIS) automaticky spadají do této nejvyšší regulační třídy. Tyto organizace podléhají nejpřísnějšímu úřednímu dohledu a musí prokázat nejvyšší standardy odolnosti.

Klasifikace: Důležité zařízení

Kategorie důležitých zařízení zahrnuje střední a velké podniky z odvětví, jako je nakládání s odpady, výroba potravin, zpracovatelský průmysl a chemický průmysl. Podniky se považují za střední, pokud zaměstnávají více než 50 zaměstnanců nebo generují obrat přesahující 10 milionů eur. Ačkoli je zde dohled reaktivní, základní bezpečnostní požadavky pro tyto podniky jsou identické.

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

Charakteristika	Zásadní zařízení	Důležité zařízení
Sektorová příslušnost	Vysoce kritické (např. KRITIS, energetika)	Ostatní kritické (např. potraviny)
Velikost podniku	Velké podniky (>250 zaměstnanců)	Střední a velké podniky (>50 zaměstnanců)
Druh dohledu	Přísný a proaktivní	Reaktivní (v závislosti na situaci)
Maximální pokuta	10 mil. EUR nebo 2 % celosvětového obratu	7 mil. € nebo 1,4 % celosvětového obratu

Identifikace a registrace

Podniky jsou povinny samostatně prověřit, zda se na ně směrnice NIS2 vztahuje, a identifikovat se v souladu s právními předpisy. Dotčené organizace se musí povinně zaregistrovat u příslušného vnitrostátního orgánu, jako je například BSI v Německu. Je povinné uvést orgánu centrální kontaktní místo pro řízení bezpečnosti informací.

Projektanti a plánovači musí ve spolupráci zajistit splnění těchto požadavků.

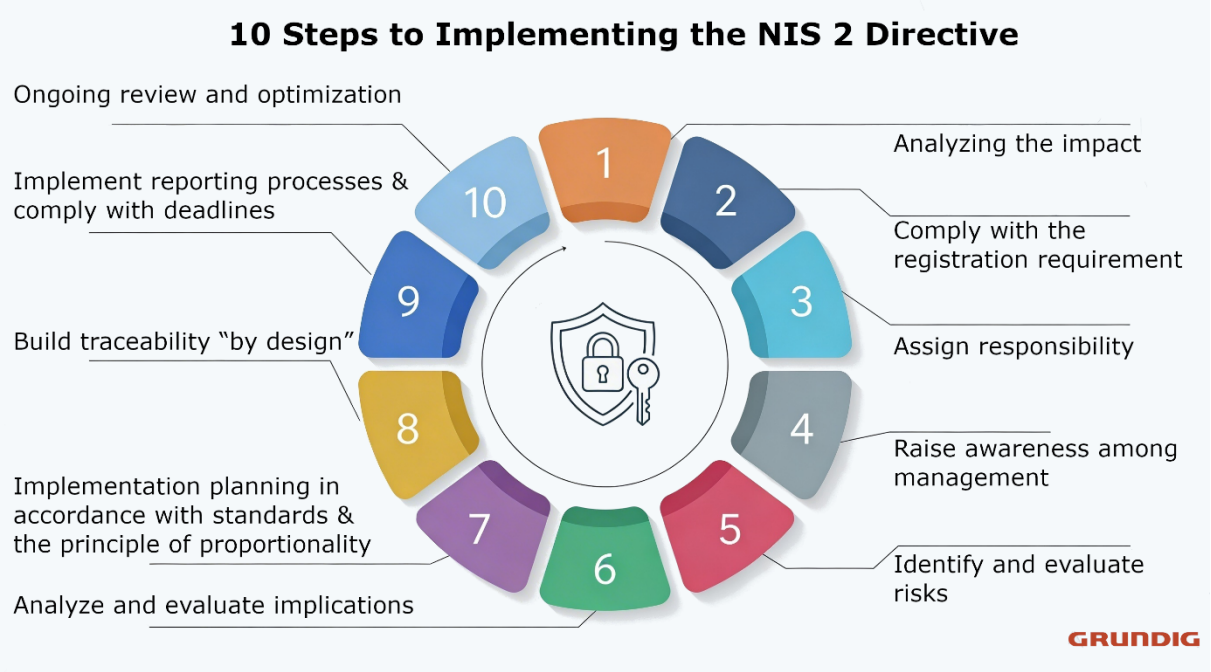
Přísné oznamovací povinnosti

V případě závažných bezpečnostních incidentů musí zařízení do 24 hodin zaslat oficiální včasné varování dozorovému orgánu. Zákonodárce vyžaduje podrobné a komplexní hlášení incidentu nejpozději do 72 hodin. Do jednoho měsíce může orgán navíc požadovat podrobnou závěrečnou zprávu o příčinách a přijatých protiopatřeních.

Regulované podniky musí kdykoli prokázat vysokou ochotu spolupracovat s státními kontrolními orgány. To zahrnuje hladké poskytování informací a dočasný přístup k IT systémům pro účely úředních vyšetřování. Proaktivní spolupráce je v tomto ohledu rozhodující pro rychlé odvrácení systémových rizik pro veřejnost.

Povinnosti v oblasti dokumentace

Všechna implementovaná bezpečnostní opatření a provozní procesy musí být bezchybně a srozumitelně zdokumentována. Účinnost těchto dokladů musí být ověřována pravidelnými nezávislými audity. Na žádost orgánů musí být tyto strukturované doklady kdykoli včas předloženy.



Opatření v oblasti kybernetické bezpečnosti

Zákon vyžaduje vhodná technická, provozní a organizační opatření k minimalizaci rozsáhlých kybernetických rizik. Patří sem komplexní strategie zálohování, postupy pro obnovu po havárii a systematické řízení reakce na incidenty. V citlivých oblastech je také výslovně předepsáno používání zabezpečené hlasové, video a textové komunikace.

Požadovaná kybernetická hygiena

Organizace musí důsledně prosazovat základní postupy kybernetické hygieny, aby minimalizovaly zranitelnost. To zahrnuje povinná školení zaměstnanců, přísné kontroly přístupu a důsledně udržovanou správu aktiv. Kromě toho musí být povinně zavedena vícefaktorová autentizace pro všechny přístupy ke kritickým systémům.

Hrozící sankce a odpovědnost vedení koncového zákazníka

V případě tzv. „nesouladu" hrozí významným subjektům drastické pokuty ve výši až 10 milionů eur nebo 2 % celosvětového ročního obratu. U důležitých subjektů činí horní hranice 7 milionů eur nebo 1,4 % globálního obratu. Tyto enormní pokuty mají působit odstrašujícím způsobem a vynutit si upřednostnění IT bezpečnosti v podnicích.

Díky směrnici NIS2 se kybernetická bezpečnost strategicky posouvá na nejvyšší úroveň řízení a definitivně se stává záležitostí nejvyššího vedení. V případě porušení nebo opomenutí budou v budoucnu generální ředitelé a členové představenstva osobně ručit za nedodržení zákonných povinností. Zákon navíc stanoví povinná pravidelná školení v oblasti bezpečnosti pro celé vedení společnosti.

Rizika v případě nedodržení

Výrobci bez prokazatelných procesů kybernetické bezpečnosti budou systematicky vyřazováni z dodavatelských řetězců regulovaných zařízení NIS2. Kromě toho mohou být v případě bezpečnostních incidentů finančně postiženi na základě odpovědnosti za výrobek a vysokých nároků na náhradu škody. Také geopolitická rizika a absence na mezinárodních seznamech důvěryhodných subjektů vedou k přímému vyloučení z trhu.

GRUNDIG Security jako partner

GRUNDIG Security jako spolehlivý evropský partner nabízí svým profesionálním zákazníkům podporu na míru pro zajištění souladu s NIS2. Propojujeme výkonný hardware s flexibilním softwarem pro správu videa C-WERK do vysoce bezpečného komplexního systému. Díky tomuto integrativnímu přístupu se provozovatelům zařízení výrazně ulehčí plnění jejich povinností v rámci dodavatelského řetězce.

Stav techniky

Směrnice NIS2 vyžaduje, aby IT zařízení odpovídala aktuálnímu stavu techniky. To samozřejmě zahrnuje i použití kamer, rekordérů a serverů.

Kamery, rekordéry a servery jsou oblíbenými cíli kybernetických útoků. Ať už jde o špehování chování nebo budování takzvané botnetové sítě – přístup k firmwaru a softwaru bezpečnostní techniky je z pohledu útočníka velmi lukrativní.

Z hlediska kybernetické bezpečnosti jsou naše produktové řady zabezpečeny na nejnovější verzi firmwaru, testovány proti různým vektorům útoku a neustále interně kontrolovány.

AI a videoanalýza

Požadovaný stav techniky v oblasti videotechniky stále více vyžaduje využití umělé inteligence pro automatickou detekci hrozeb. Řada SMART od **GRUNDIG** Security zpracovává analýzy, jako je rozpoznávání obličejů, monitorování perimetru a virtuální tripwire, v souladu s předpisy o ochraně osobních údajů přímo na kameře, rekordéru nebo serveru.

Security by Design

Podle článku 21 směrnice NIS2 musí být IT produkty již v první fázi vývoje navrženy podle přísných bezpečnostních zásad. **GRUNDIG** Security důsledně integruje tuto filozofii „Security by Design“ do systému správy videa C-WERK a do všech nabízených síťových kamer. Monitorovací systémy jsou koncovým zákazníkům dodávány standardně s bezpečnými předvolbami (Security by Default) a minimalizovanou plochou pro útoky.

Inovativní funkce řady SMART-Line, jako je „One-Click-Disable“, v případě potřeby potlačují veškerou komunikaci s internetem – i když zařízení obdrží platnou bránu pro připojení.

Cloud a šifrování

Trvale bezpečný přenos dat je základním požadavkem povinností v oblasti řízení rizik podle směrnice NIS2. **GRUNDIG** Security umožňuje plynulou a vysoce šifrovanou komunikaci mezi lokálním hardwarem a připojeným cloudem C-WERK. Tato architektura spolehlivě chrání citlivá metadata před přístupem neoprávněných třetích stran a zajišťuje právní jistotu pro monitorovací projekty napříč různými lokalitami.

Důraz na bezpečnost dodavatelského řetězce

Ústředním prvkem směrnice NIS2 je důsledné zabezpečení celého dodavatelského řetězce podle článku 21. Dotčené subjekty musí přísně sledovat a kontrolovat kybernetickou bezpečnost svých dodavatelů a poskytovatelů služeb. Bezpečnostní řetězec organizace je nakonec jen tak odolný, jak odolný je jeho nejslabší zapojený externí dodavatel.

Certifikované bezpečnostní procesy

Nejspolehlivější odpovědí na požadavky směrnice NIS2 na dokladování v dodavatelském řetězci jsou nezávislé a mezinárodní certifikace. Společnost **GRUNDIG** Security disponuje náročnými certifikacemi ISO 9001 pro řízení kvality a ISO 27001 pro vlastní řízení bezpečnosti informací. Tyto oficiální certifikáty zaručují zákazníkům, že všechny vývojové a podnikové procesy podléhají nejvyšším bezpečnostním standardům a jsou systematicky auditovány třetími stranami.

Soulad a důvěra

Absolutní geopolitická nezávislost je rozhodujícím kritériem pro výběr důvěryhodných dodavatelů technologií v rámci režimu NIS2. Všechny kamery a záznamníky řady SMART od společnosti **GRUNDIG** Security proto plně odpovídají přísným standardům NDAA. To vylučuje kritické komponenty od vysoce rizikových dodavatelů a zajišťuje digitální suverenitu kritických evropských infrastruktur.

Naše kamery a záznamníky řady Smart-Line navíc splňují požadavky na takzvanou shodu s NDAA. Ta zakazuje americkým úřadům a jejich smluvním partnerům používat telekomunikační a kamerové technologie určitých čínských výrobců, aby se minimalizovala bezpečnostní rizika.

Řízení zranitelností

Agilní a proaktivní správa zranitelností je pro klíčová zařízení zákonem povinná. **GRUNDIG** Security v tomto ohledu podporuje své koncové zákazníky prostřednictvím neustálých aktualizací firmwaru a extrémně rychlého poskytování bezpečnostních záplat. Přísná kompatibilita s otevřenými standardy, jako je ONVIF, navíc zajišťuje, že systémy zůstanou dlouhodobě kompatibilní s produkty třetích stran.

Společnost **GRUNDIG** Security se spolu se svým technologickým partnerem Axxonsoft účastní programu „Common Vulnerabilities and Exposures (CVE)“ společnosti MITRE Corporation. Tento standardizovaný systém pro identifikaci a katalogizaci veřejně známých kybernetických bezpečnostních mezer v softwaru a hardwaru umožňuje zveřejňování a sledování vektorů útoků.

Více informací naleznete na následujícím odkazu:
https://www.cve.org/PartnerInformation/ListofPartners/partner/AxxonSoft

Síťová autentizace

Evropská legislativa vyžaduje přísné kontroly přístupu a použití robustních kryptografických postupů k ochraně sítí zařízení. Záznamníky a IP kamery **GRUNDIG** Security podporují komplexní alarmové vstupy i nejmodernější autentizační mechanismy podle standardů IEEE. Všechny produkty řady Smart-Line tak podporují port-based network access control (PNAC) podle normy IEEE 802.1X.

Systém C-WERK VMS zároveň nabízí forenzně zabezpečenou správu práv, která technicky zcela vylučuje neoprávněné manipulace s daty.

Závěr

Provozovatelé video systémů musí bezpodmínečně zajistit, aby jejich IT infrastruktura bez problémů odolala i budoucím regulacím. Hladká integrace technologií IP a HD-TVI v portfoliu společnosti **GRUNDIG** Security umožňuje škálovatelnou a investičně bezpečnou migraci stávajících systémů. To zaručuje ekonomicky přiměřenou a přesto plně zákonnou implementaci požadovaných technických opatření.

Díky exkluzivní spolupráci s výrobcem certifikovaným podle normy ISO 27001, jakým je **GRUNDIG** Security, kriticky důležité podniky výrazně snižují své vlastní riziko nesouladu s předpisy. Úplná dokumentace a doklad o prokazatelně bezpečných produktech spolehlivě chrání zařízení před státními sankcemi v řádu milionů. Současně tento přístup výrazně zbavuje vedení podniku osobních rizik odpovědnosti, která by mohla ohrozit existenci firmy.

www.grundig-security.com

Abetechs GmbH (**GRUNDIG** Security)

info@grundig-security.com

S výhradou změn a chyb.