EVVA
access to security

Whitepaper

De eerste verdedigingslinie
Toegangscontrole voor kritieke infrastructuren

De eerste verdedigingslinie Toegangscontrole voor kritieke infrastructuren

Hoe moderne toegangscontrole bijdraagt aan de naleving van NIS2 en CER – en de fysieke veiligheid duurzaam verbetert.

Toegangscontrole als essentieel onderdel voor naleving van NIS2 en CER

De wereld en ook wij zijn – vooral in de afgelopen paar jaar – veranderd. Geopolitieke veranderingen zoals oorlogen, politieke instabiliteit, klimaatveranderingen en nieuwe technologieën bepalen ons dagelijks leven en vereisen een grotere weerbaarheid van vitale infrastructuur, met name een versterking van de fysieke beveiliging.

Met de Europese NIS2-richtlijn (2022/2555) en de aanvullende CER-richtlijn (2022/2557) scherpt de Europese Unie de veiligheidseisen voor exploitanten van kritieke en belangrijke voorzieningen aanzienlijk aan. Beide regelgevingen hebben tot doel de weerbaarheid tegen digitale en fysieke bedreigingen centraal te versterken – waardoor ook toegangscontrole in de schijnwerpers komt te staan binnen moderne beveiligingsarchitecturen. In deze whitepaper willen we ons vooral richten op het thema „Fysieke beveiligingsmaatregelen voor kritieke infrastructuur".

Regelgevend kader: NIS2 en CER

De begripsverklaringen

NIS2 en CER zijn EU-richtlijnen die in nationale wetgeving moeten worden omgezet; de betreffende wettelijke benamingen op de Europese markten vindt u overzichtelijk op pagina 15 van de whitepaper.

NIS2

Cyberveiligheid voor kritieke en belangrijke sectoren

- EU-richtlijn (2022/2555)
- **Doel:** het niveau van cyberbeveiliging verhogen door middel van EU-brede minimumnormen. Verplicht bedrijven en organisaties om hun IT- en cyberbeveiliging systematisch te verbeteren en incidenten te melden.
- **Geldt voor:**
  - „Essentiële" instellingen: hieronder vallen bedrijven met een hoge kriticiteit waarvan het uitvallen aanzienlijke gevolgen zou hebben voor de samenleving, de economie of de openbare veiligheid, waaronder energie, vervoer, banken, gezondheidszorg, water, telecommunicatie/IT
  - „Belangrijke" sectoren: hieronder vallen bedrijven met andere kritieke gevolgen, zoals post, afval, chemie, levensmiddelen, productie van goederen (vanaf 50 medewerkers en 10 miljoen EUR omzet)
- **Eisen** aan bedrijven die onder NIS-2 vallen, zijn onder andere:
  - Cyberbeveiligingsbeheer (risicoanalyses, beveiligingsconcepten, incidentrespons, bedrijfscontinuïteit)
  - Meldingsplicht voor beveiligingsincidenten
  - Verantwoordelijkheid van het management
  - Streng toezicht en sancties

CER

Fysieke weerbaarheid van kritieke infrastructuren

- EU-richtlijn (2022/2557)
- **Doel:** het vergroten van de fysieke weerbaarheid tegen niet-digitale bedreigingen en gevaren (all-hazard-benadering)
- **Van toepassing op:** exploitanten van kritieke infrastructuur, zoals:
  - Energie
  - Vervoer
  - Banken
  - Gezondheidszorg
  - Water
  - Telecommunicatie/IT
  - Voedingsmiddelen
  - Chemie
- **Vereisten:**
  - Risicoanalyses
  - Nood- en herstelplannen
  - Beveiligingsmaatregelen
  - Beheer van toeleveringsketens en afhankelijkheden
  - Meldingsplicht voor ernstige incidenten
  - Waarborging van de continuïteit van essentiële diensten

In het kort

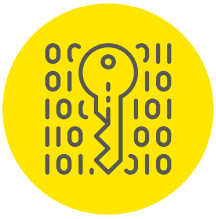
Samengevat betekent dit dat instellingen die onder NIS2 en CER vallen, na een systematische gevaren- en risicoanalyse en beoordeling ook maatregelen voor effectieve fysieke beveiliging moeten nemen. Hiertoe behoren met name toegangscontrole, bewaking en procedures voor het opsporen van incidenten. CER concretiseert dit verder: exploitanten van kritieke installaties moeten om de vier jaar risicoanalyses uitvoeren, passende fysieke beveiligingsmaatregelen nemen en onbevoegde toegang effectief voorkomen.

Cyberbeveiliging vereist ook fysieke bescherming

Relevante beveiligingskenmerken voor gebruik in een NIS2- en CER-omgeving

Fysieke toegangs-beveiliging

- Strenge toegangscontrole tot kritieke zones
- Vervalsingsbestendige toegangsmedia
- State-of-the-art-technologieën



IT-beveiliging & versleuteling

- Beveiligde communicatie volgens de nieuwste cryptografische standaarden (TLS, AES, ECDSA)
- Geen onveilige wachtwoorden

Logboekregistratie & Audits

- Volledige documentatie van alle toegangen en systeemacties
- Revisiebestendige logboeken met exportfunctie als auditdocument

Reactie op incidenten & Toegangsbeveiliging

- Snelle blokkering van gecompromitteerde toegangen
- Noodplannen voor storingen of aanvallen (offline-werking van de deuren)

Bedrijfscontinuïteit & gegevensback-up

- Geautomatiseerd concept voor gegevensback-up
- Herstelstrategie na een storing, redundantie

Beheer van kwetsbaarheden & updates

- Voortdurende monitoring door fabrikanten van softwarekwetsbaarheden (CVE)
- Tijdige, ondertekende en geverifieerde updates

Gegevens-bescherming & gegevensbeveiliging

- Privacy by Design, AVG-conformiteit
- Verwijderingsfuncties voor persoonsgegevens
- Configureerbare logboekregistratie
- Vierogenprincipe voor inzage in logboeken

EVVA-producten en hoe ze voldoen aan de wettelijke vereisten

Xesar

Toegangssysteem voor de hoogste veiligheidseisen

Fysieke en IT-beveiliging

- Op rollen gebaseerde toegangsrechten per persoon/groep
- MIFARE DESFire EV1/EV2/EV3 (EAL5+), installatiespecifieke AES-sleutels
- Versleutelde challenge-response-communicatie (geen protocollen in leesbare tekst)
- TLS ≥ 1.2 voor systeemcommunicatie
- Interne AES256-bit-versleuteling
- Wachtwoorden gehasht (Bcrypt)

Toegangs- en systeemlogboeken

- Volledige, tegen manipulatie beveiligde gebeurtenis- en systeemlogboeken
- Revisiebestendige exporten
- Audit- en incidentrapportages op elk moment mogelijk

Incidentrespons & weerbaarheid

- Realtime blokkades (online), blokkeerlijsten voor offline componenten
- Waarschuwingsmechanismen bij onzekere blokkeerstatus
- Zelfstandige offline werking bij IT- of netwerkstoringen

Updates en beheer van kwetsbaarheden

- Continue CVE-monitoring
- Cryptografisch ondertekende updates (RSA/SHA256, AES256CCM)
- Geverifieerde firmware- en software-updates

Bedrijfscontinuïteit

- Versleutelde back-ups
- Herstel in noodgevallen via het veiligheidsblad van de installatie
- Gebruik door meerdere gebruikers en 24/7 servergebruik mogelijk

Gegevensbescherming

- Privacy by Design
- Geen persoonsgegevens in de app
- Automatische verwijdering van persoonsgegevens kan worden geconfigureerd

AirKey

Mobiele toegangsoplossing volgens de hoogste normen

Fysieke en IT-beveiliging

- Toegangsmedia op basis van smartphones en RFID (JCOP SmartMX3, EAL6+)
- ECDSA256-authenticatie + AESSessionKeys
- TLS-beveiligd online beheer

Toegangs- en systeemlogboeken

- Auditbestendige logboekregistratie
- Auditbestendige exporten
- Automatische bijwerking van blokkeerlijsten en logbestanden
- Flexibele configuratie die voldoet aan de privacywetgeving

Incidentrespons & weerbaarheid

- Realtime vergrendelingen via internet
- Offline deurfunctie, ook bij serverstoringen
- Waarschuwingen bij veiligheidsrelevante situaties

Updates & werking

- Centraal, gesigneerd updatemanagement
- ISO 27001-gecertificeerde datacenters in Oostenrijk
- Redundante EVVA-servers, met HSM beveiligde sleutels

Gegevensbescherming

- AVG-conforme verwijderingsconcepten
- Privacy by Design
- Vierogenprincipe voor inzage in logbestanden kan worden geactiveerd

NORMEN EN CERTIFICERINGSSTATUS

Met succes
getest (TÜV)
EN 18031-1

VOLDOET AAN DE RED*-EISEN

*RED: Richtlijn inzake radioapparatuur

Praktijkvoorbeeld 1:

Toegangscontrole in een ziekenhuis

NIS2/CER-relevant

Uitgangssituatie

Een ziekenhuis behoort tot de „essentiële faciliteiten“ volgens NIS2 en moet voldoen aan strenge eisen op het gebied van IT- en fysieke beveiliging. Bijzonder gevoelige ruimtes, zoals serverruimtes, medicijnopslagplaatsen of intensive care-afdelingen, moeten worden beschermd tegen ongeoorloofde toegang.

Oplossing met Xesar

- Op rollen gebaseerde toegangsrechten voor verschillende medewerkersgroepen (bijv. IT, zorg, administratie)
- Toegangsmedia met individuele, uiterst veilige technologieën (MIFARE DESFire EV3)
- Volledige registratie van alle toegangen, auditbestendige logboeken voor controles
- Snelle blokkering van verloren toegangsmedia via realtime blokkeerlijsten
- Offline werking van de deuren bij serverstoringen (bedrijfscontinuïteit)
- Regelmatige, ondertekende software-updates en kwetsbaarheidsbeheer

Toegevoegde waarde

Het ziekenhuis voert de op risico’s gebaseerde maatregelen door, kan incidenten volledig documenteren en vergroot zo de fysieke weerbaarheid van deze instelling.

Praktijkvoorbeeld 2:

Productiebedrijf als toeleverancier voor kritieke infrastructuur

Toeleve-ringsketen/ CER-relevant

Uitgangssituatie

Een middelgroot machinebouwbedrijf levert aan energieleveranciers en valt daarmee indirect onder de CER-richtlijn. Het bedrijf moet aantonen dat zijn toegangssystemen en IT-infrastructuur weerbaar en veilig zijn.

Oplossing met AirKey

- Toegangsrechten worden centraal beheerd, ook voor externe dienstverleners (bijv. onderhoudspersoneel)
- Veilige cloudgebaseerde applicatie
- Toegangsmedia (smartphones, RFID) met zeer hoge versleuteling (ECDSA-256, AES-128)
- Logboekregistratie van alle toegangen, export voor audits
- AVG-conforme verwijderingsfuncties en 'Privacy by Design'
- Updates en kwetsbaarheidsbeheer centraal door EVVA

Toegevoegde waarde

Het bedrijf kan aan zijn klanten aantonen dat het de nodige maatregelen heeft genomen om de veiligheid in de toeleveringsketen met betrekking tot de toegang te waarborgen en dat het optimaal is voorbereid op audits en certificeringen.

Praktijkvoorbeeld 3:

Noodsituatiebeheer en weerbaarheid binnen een stadsbestuur

CER-relevant

Uitgangssituatie

Een gemeentebestuur beheert kritieke infrastructuur (bijvoorbeeld watervoorziening en zuiveringsinstallaties) en moet ervoor zorgen dat in geval van nood (bijvoorbeeld een cyberaanval of stroomstoring) de toegang tot belangrijke gebieden gewaarborgd blijft.

Oplossing met Xesar

- Veilige offline werking bij stroomuitval of cyberaanvallen
- Snelle blokkering van gecompromitteerde toegangsmedia, waarschuwingen bij openstaande beveiligingstaken
- Back-up- en herstelfuncties voor configuratiegegevens

Toegevoegde waarde

Het stadsbestuur blijft ook in geval van een crisis in staat om te handelen – de inwoners en de gevestigde bedrijven ondervinden geen hinder van uitval of storingen.

Praktijkvoorbeeld 4:

Gegevensbescherming en logboekregistratie in een onderzoeksinstituut

NIS2/CER-relevant

Uitgangssituatie

Een onderzoeksinstituut verwerkt gevoelige persoonsgegevens en moet voldoen aan de AVG en de NIS2-vereisten.

Oplossing met AirKey

- Privacy by Design: geen opslag van persoonsgegevens in de backend
- Configureerbare logboekregistratie, verwijderingsfuncties voor persoonsgegevens
- Implementatie in overeenstemming met de AVG

Toegevoegde waarde

Het instituut kan te allen tijde aan toezichthoudende autoriteiten en partners aantonen dat het de gegevensbescherming en transparantie waarborgt.

Veiligheidscontrole voor exploitanten van kritieke infrastructuren

1. Organisatorisch veiligheidskader

- Beschikken we over een bindend beveiligingsconcept om de fysieke veiligheid te waarborgen?
- Zijn er duidelijk omschreven rollen, bevoegdheden en verantwoordelijkheden voor beveiliging, IT, facilitaire zaken en KRITIS-relevante gebieden?
- Worden beveiligingsrichtlijnen en -processen regelmatig gecontroleerd en bijgewerkt?
- Is de naleving van de voorgeschreven meldingsplicht voor beveiligingsincidenten procedureel gewaarborgd?

2. Risicoanalyse & compliance

- Hebben we in de afgelopen 4 jaar een risicoanalyse uitgevoerd volgens de KRITIS-koepelwet/CER?
- Hebben we alle fysieke en digitale kwetsbaarheden in de hele procesketen geïdentificeerd?
- Zijn we met onze toegangsoplossingen goed gepositioneerd ten aanzien van NIS2, met name wat betreft veilige protocollen en bescherming tegen manipulatie?
- Gebruiken we uitsluitend technisch up-to-date systemen (geen onversleutelde protocollen zoals bijvoorbeeld Wiegand)?

3. Toegangsrechten & identiteiten

- Zijn alle toegangsrechten op basis van rollen en op een traceerbare manier toegewezen?
- Worden toegangsrechten regelmatig opnieuw gecertificeerd of automatisch ingetrokken wanneer ze niet langer nodig zijn?
- Hebben we duidelijke processen voor de onboarding, rolwisselingen en offboarding van medewerkers en dienstverleners?

4. Technische veiligheid van de toegangscontrole

- Zijn alle toegangsscanners, kaarten en identificatiemedia versleuteld?
- Zijn alle veiligheidsgevoelige deuren, serverruimtes en controlekamers beveiligd met elektronische toegangssystemen?
- Worden veiligheidsrelevante gegevens (bijv. logbestanden) op een auditbestendige manier opgeslagen en beschermd tegen manipulatie?

5. Monitoring, logboekregistratie & transparantie

- Worden alle toegangen en pogingen tot toegang automatisch geregistreerd?
- Zijn onze toegangslogboeken auditbestendig, beveiligd tegen manipulatie en worden ze lang genoeg bewaard?
- Gebruiken we monitoringtools die fysieke en digitale beveiligingsgebeurtenissen aan elkaar koppelen?

6. Bescherming van kritieke gebieden

- Zijn ruimtes zoals serverruimtes, controlekamers, energie- en voorzieningsinstallaties of schakelkasten extra beveiligd?
- Zijn er toegangsgebieden met verschillende niveaus en een oplopend beveiligingsniveau?
- Zijn gevoelige ruimtes extra beveiligd door middel van videobewaking, deurbewaking of alarmsystemen?
- Hebben we een plan voor noodtoegang (bijvoorbeeld bij stroomuitval of een systeemstoring)?

7. Leveranciers & dienstverleners

- Hebben externe bedrijven en dienstverleners alleen tijdelijke en duidelijk omschreven toegangsrechten?
- Worden de toegangen voor tijdelijk personeel technisch beperkt en streng bewaakt?
- Wordt het gebruik van externe toegangen regelmatig gecontroleerd?

8. Nood- en herstelcapaciteit

- ›Is er een nood- en crisisbeheersingsplan dat
- fysieke veiligheidsaspecten omvat?
- Zijn er processen vastgelegd voor:
  - Het onmiddellijk blokkeren van de toegang voor individuele gebruikers of groepen
  - Het snel herstellen van de toegangsinfrastructuur na een aanval
  - Evacuatie- of incidentresponsscenario's
- Worden deze plannen regelmatig geoefend?

9. Opleiding & bewustwording

- Krijgen alle medewerkers training in het omgaan met toegangsmedia?
- Is er een doorlopend bewustmakingsprogramma over veiligheidsrichtlijnen en correct gedrag?
- Weten medewerkers hoe ze verdachte activiteiten moeten melden?

10. Toekomstbestendigheid & verdere ontwikkeling

- Is onze toegangsoplossing schaalbaar voor nieuwe locaties of aanvullende eisen?
- Kunnen we nieuwe veiligheidsnormen (NIS2-updates, BSI-richtlijnen, uitbreidingen in de KRITIS-koepelwet) probleemloos integreren?
- Hebben we een duidelijk moderniseringsplan voor het geval technologieën verouderen of er beveiligingslekken aan het licht komen?

NIS2 en CER worden in de afzonderlijke EU-lidstaten omgezet onder de volgende nationale wettelijke benamingen

	NIS2	CER
Oostenrijk	NISG2026 (Wet inzake netwerk- en informatiebeveiliging 2026)	RKEG (Wet inzake de weerbaarheid van kritieke infrastructuur)
Duitsland	Wet inzake de tenuitvoerlegging van NIS-2 en de versterking van de cyberveiligheid (NIS2UmsuCG)	KRITIS-Dachgesetz (Wet ter versterking van de fysieke veerkracht weerbaarheid installaties)
België	Loi NIS2 (Wet van 26 april 2024 inzake cyberveiligheid van netwerk- en informatiesystemen)	Loi relative à la résilience des entités critiques (nationale CER-uitvoeringswet, 2025/26)
Nederland	Cyberbeveiligingswet (in fase van parlementaire omzetting, stand april 2026)	Wet weerbaarheid kritieke entiteiten (voorgenomen CER-wet, stand april 2026)
Zweden	Cybersäkerhetslagen (Cybersecurity Act, SFS 2025:1506)	Lag om motståndskraft hos kritiska verksamheter (CER-implementatie in voorbereiding, stand april 2026)
Italië	Decreto Legislativo n. 138/2024	Decreto Legislativo n. 134/2024
Tschechien	Zákon o kybernetické bezpečnosti (Wijziging/herziening in het kader van de omzetting van de NIS2-richtlijn)	Zákon o odolnosti kritických subjektů (CER-uitvoeringswet)
Polen	Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) – Novelle zur NIS2	Ustawa o odporności podmiotów krytycznych (in Umsetzung)
Slowakije	Zákon o kybernetickej bezpečnosti (NIS2-wijziging)	Zákon o odolnosti kritických subjektov

www.evva.com