EVVA
access to security

Whitepaper

Den första försvarslinjen
Tillträdeskontroll för kritisk infrastruktur

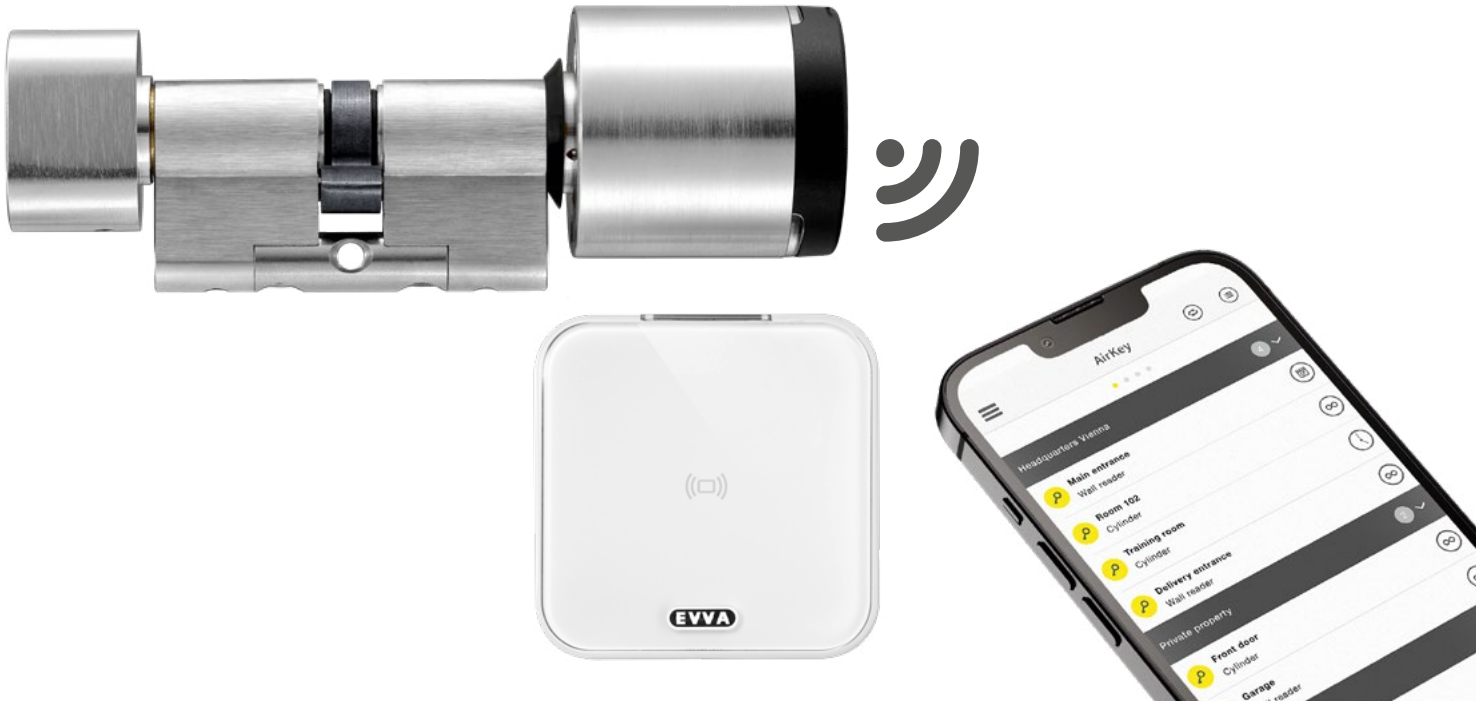
Den första försvarslinjen Tillträdeskontroll för kritisk infrastruktur

Hur modern tillträdeskontroll bidrar till att uppfylla kraven i NIS2 och CER – och på ett hållbart sätt förbättrar den fysiska säkerheten.

Tillträdeskontroll som en nyckelkomponent för efterlevnad av NIS2 och CER

Världen – och vi med den – har förändrats, särskilt under de senaste åren. Geopolitiska förändringar som krig, politisk instabilitet, klimatförändringar och ny teknik präglar vår vardag och ställer högre krav på motståndskraft hos samhällsviktig infrastruktur, framför allt genom ett förstärkt fysiskt skydd.

Med det europeiska NIS2-direktivet (2022/2555) och det kompletterande CER-direktivet (2022/2557) skärper Europeiska unionen avsevärt säkerhetskraven för operatörer av kritiska och viktiga verksamheter. Båda regelverken syftar till att stärka motståndskraften mot digitala och fysiska hot, vilket gör tillträdeskontroll till en central del av moderna säkerhetsarkitekturer. I denna vitbok fokuserar vi på ämnet ”Fysiska skyddsåtgärder för kritiska verksamheter”.



Regleringsram: NIS2 och CER

Begreppsförklaringar

NIS2 och CER är EU-direktiv som ska införlivas i nationell lagstiftning. En översikt över motsvarande lagstiftning och benämningar på de europeiska marknaderna finns på sidan 15 i denna vitbok.

NIS2

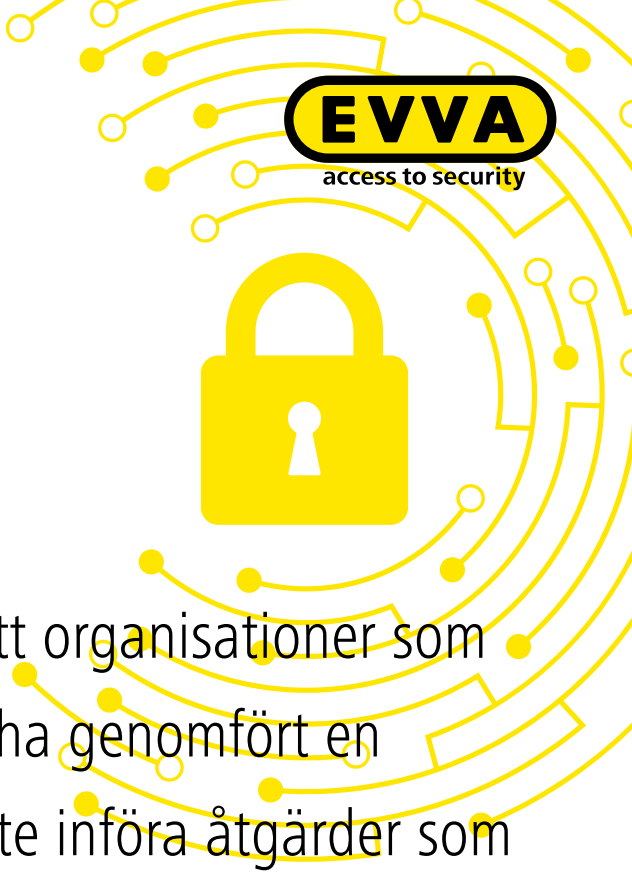
Cybersäkerhet för kritiska och viktiga sektorer

- EU-direktiv (2022/2555)
- **Syfte:** Att höja cybersäkerhetsnivån genom EU-gemensamma minimikrav. Företag och organisationer åläggs att systematiskt förbättra sin IT- och cybersäkerhet samt rapportera säkerhetsincidenter.
- Gäller för:
  - ”Väsentliga” verksamheter: Företag med hög kritikalitet vars driftstopp skulle få betydande konsekvenser för samhället, ekonomin eller den allmänna säkerheten, bland annat inom: bland annat energi, transport, bankverksamhet, hälso- och sjukvård, vattenförsörjning, telekommunikation/IT
  - ”Viktiga” sektorer: Andra verksamheter med kritisk betydelse, exempelvis, exempelvis post, avfall, kemi, livsmedel, tillverkning av varor (från 50 anställda och 10 miljoner euro i omsättning)
- **Krav** på företag som omfattar av NIS-2 är bland annat
  - Hantering av cybersäkerhet (riskanalyser, säkerhetskoncept, incidenthantering, kontinuitetsplanering)
  - Rapportering av säkerhetsincidenter
  - Ledningens ansvar
  - Strikt tillsyn och sanktioner

CER

Fysisk motståndskraft hos kritisk infrastruktur

- EU-direktiv (2022/2557)
- **Syfte:** Att stärka den fysiska motståndskraften mot icke-digitala hot och andra risker (”all hazardous”-strategi)
- **Gäller för:** Operatörer av kritisk infrastruktur exempelvis:
  - Energi
  - Trafik
  - bankverksamhet
  - Hälso- och sjukvård
  - Vattenförsörjning
  - telekommunikation/IT
  - Livsmedel
  - Kemi
- **Krav:**
  - Riskbaserat arbetssätt
  - Nöd- och återstartsplaner
  - Säkerhetsåtgärder
  - Hantering av leveranskedjor och beroenden
  - Anmälningsplikt för allvarliga incidenter
  - Säkerställande av kontinuiteten i samhällsviktiga tjänster



I korthet

Sammanfattningsvis innebär detta att organisationer som omfattas av NIS2 och CER, efter att ha genomfört en systematisk hot- och riskanalys, måste införa åtgärder som säkerställer ett effektivt fysiskt skydd.

Dessa åtgärder omfattar bland annat tillträdeskontroll, övervakning och rutiner för att upptäcka incidenter.

CER preciserar dessutom detta ytterligare: Operatörer av kritisk infrastruktur måste genomföra riskanalyser vart fjärde år, införa lämpliga fysiska skyddsåtgärder och effektivt förhindra obehörigt tillträde.

Cybersäkerhet kräver även fysiskt skydd

Relevanta säkerhetsfunktioner för användning i NIS2- och CER-miljöer

Fysisk åtkomstsäkerhet

- Strikt tillträdeskontroll till kritiska områden
- Manipulationssäkra tillträdesmedia
- Toppmodern teknik

IT-säkerhet & kryptering

- Säker kommunikation med moderna krypteringsstandarder (TLS, AES, ECDSA)
- Inga osäkra lösenord

Dokumentation & revisioner

- Fullständig dokumentation av alla tillträdeshändelser och systemaktiviteter
- Manipulationssäkra revisionsloggar med exportfunktion för revision och efterlevnads-dokumentation

Händelsehantering & tillträdesskydd

- Snabb spärrning av kompromitterade accesspunkter
- Beredskapsplaner vid driftstopp eller angrepp (offline-drift av dörrarna)

Kontinuitets-planering och säkerhetskopiering av data

- Automatiserad säkerhetskopiering
- Återställningsstrategi vid driftstopp och redundans

Sårbarhetshantering och uppdateringar

- Kontinuerlig övervakning av säkerhetssårbarheter (CVE) i tillverkarnas programvara
- Snabba, signerade och verifierade uppdateringar

Dataskydd & datasäkerhet

- Privacy by Design och GDPR-efterlevnad
- Funktioner för radering av personuppgifter
- Konfigurerbar loggning
- Fyrögonprincipen för åtkomst till loggar

EVVA:s produkter och hur de uppfyller de lagstadgade kraven

Xesar

Passersystem för högsta säkerhetskrav

Fysisk säkerhet och IT-säkerhet

- Rollbaserade tillträdesbehörigheter för personer och grupper
- MIFARE DESFire EV1/EV2/EV3 (EAL5+), ned systemspecifika AES-nycklar
- Krypterad Challenge-Response-kommunikation (inga okrypterade protokoll)
- TLS ≥ 1.2 för systemkommunikation
- Intern AES-256-bitars kryptering
- Lösenord hashas med Bcrypt

Tillträdes- och systemloggar

- Fullständig och manipulationssäker loggning av tillträdeshändelser och systemaktiviteter
- Revisionssäkra exporter
- Underlag för revisioner och incidentutredningar kan tas fram när som helst

Händelsehantering och motståndskraft

- Spärrning i realtid (online) och blocklistor för offlinekomponenter
- Varningsfunktioner vid osäker spärrstatus
- Självständig offline-drift vid IT- eller nätverksavbrott

Uppdateringar och hantering av sårbarheter

- Kontinuerlig övervakning av säkerhetssårbarheter (CVE)
- Kryptografiskt signerade uppdateringar (RSA/SHA256, AES256CCM)
- Verifierade uppdateringar av firmware och programvara

Kontinuitetsplanering

- Krypterade säkerhetskopior
- Återställning vid nödsituationer med hjälp av systemets säkerhetsdatablad
- Stöd för fleranvändardrift och serverdrift dygnet runt

Dataskydd

- Privacy by Design
- Inga personuppgifter lagras i appen
- Automatisk anonymisering av personuppgifter kan konfigureras

AirKey

Mobil tillträdeslösning med högsta standard

Fysisk säkerhet och IT-säkerhet

- Smartphone- och RFID-baserade tillträdesmedia (JCOP SmartMX3, EAL6+)
- ECDSA256-autentisering och AES-sessionsnycklar
- TLS-skyddad onlineadministration

Tillträdes- och systemloggar

- Revisionssäker loggning
- Revisionssäkra exporter
- Automatisk uppdatering av blocklistor och loggar
- Flexibel, dataskyddsanpassad konfiguration

Händelsehantering och motståndskraft

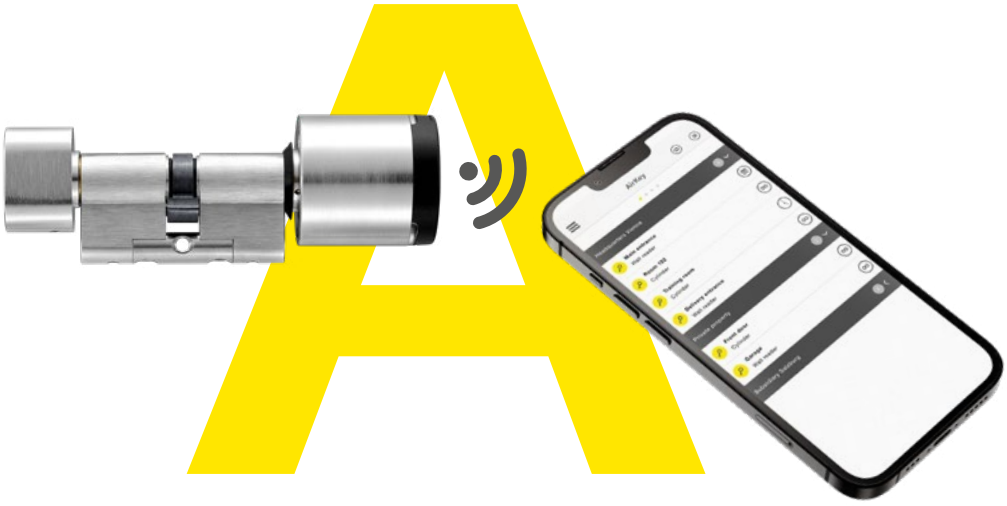
- Spärrning i realtid via internet
- Offlinefunktion för dörrar även vid serveravbrott
- Varningar vid säkerhetskritiska tillstånd

Uppdateringar och drift

- Central, signerad hantering av uppdateringar
- ISO 27001-certifierade datacenter i Österrike
- Redundanta EVVA-servrar med HSM-skyddade nycklar

Dataskydd

- GDPR-anpassade raderingskoncept
- Privacy by Design
- Fyrögonprincipen för åtkomst till loggar kan aktiveras

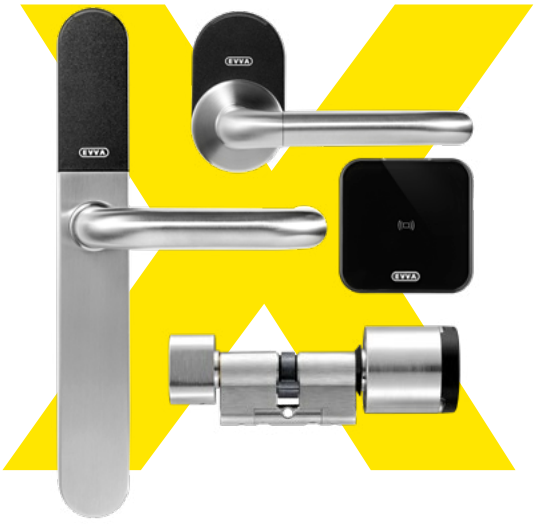


STANDARDER OCH CERTIFIERINGSSTATUS

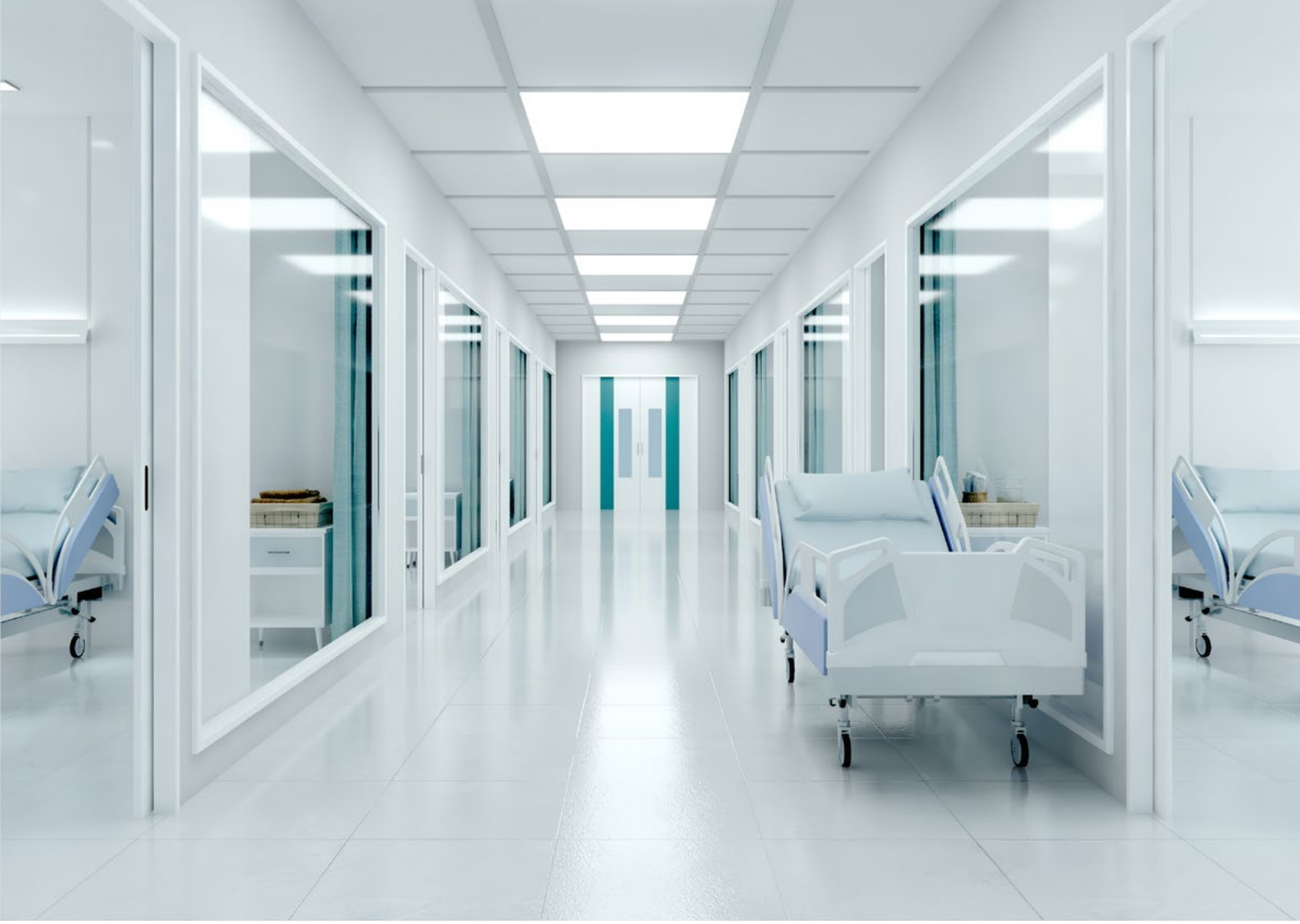
Godkänd
vid provning
(TÜV)

EN 18031-1

RED*-KRAVEN UPPFYLLDA



*RED: Direktivet om radioutrustning



Praktiskt exempel 1:

Tillträdeskontroll på ett sjukhus

NIS2/CER-relevant

Utgångsläge

Ett sjukhus räknas som en ”väsentlig verksamhet“ enligt NIS2 och omfattas av stränga krav på IT-säkerhet och fysiskt skydd. Särskilt känsliga områden som serverrum, läkemedelslager eller intensivvårdsavdelningar måste skyddas mot obehörigt tillträde.

Lösning med Xesar

- Rollbaserade tillträdesbehörigheterför olika medarbetargrupper (t.ex. IT, underhåll, administration)
- Tillträdesmedia med individuell, mycket säker teknik (MIFARE DESFire EV3)
- Fullständig loggning av alla tillträdeshändelser samt revisionssäkra loggar för revisioner
- Snabb spärrning av förlorade tillträdesmedia via blocklistor i realtid
- Offlinefunktion för dörrar även vid serveravbrott (kontinuitetsplanering)
- Regelbundna, signerade programuppdateringar och hantering av sårbarheter

Mervärde

Sjukhuset inför riskbaserade åtgärder, kan tillhandahålla fullständig dokumentation av incidenter och stärker därmed verksamhetens fysiska motståndskraft.

Praktiskt exempel 2:

Produktionsföretag som leverantör till kritisk infrastruktur

Leveranskedja/ CER-relevant

Utgångsläge

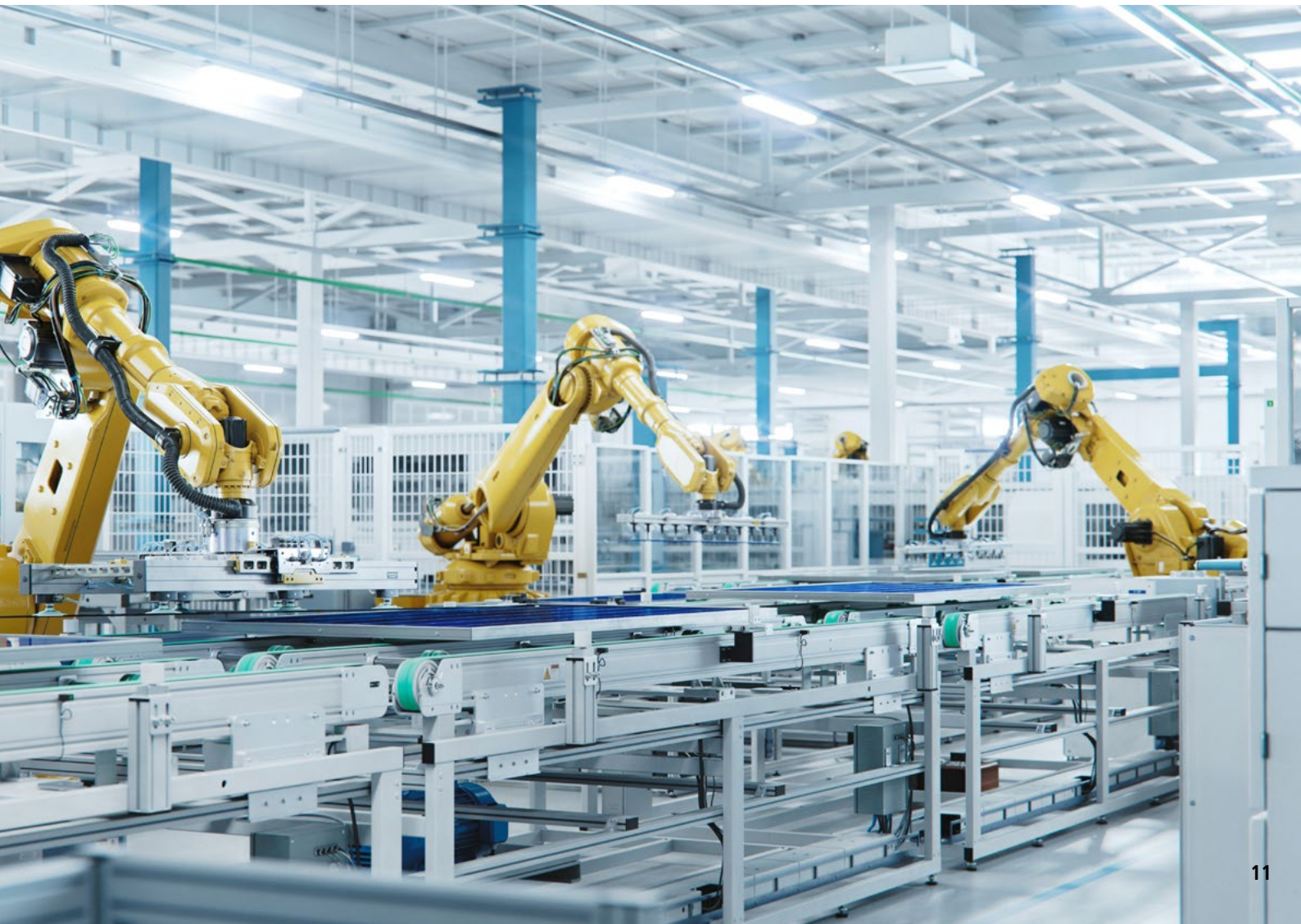
Ett medelstort företag inom maskintillverkning levererar till energibolag och omfattas därför indirekt av CER-direktivet. Företaget måste kunna visa att dess tillträdessystem och IT-infrastruktur är motståndskraftiga och säkra.

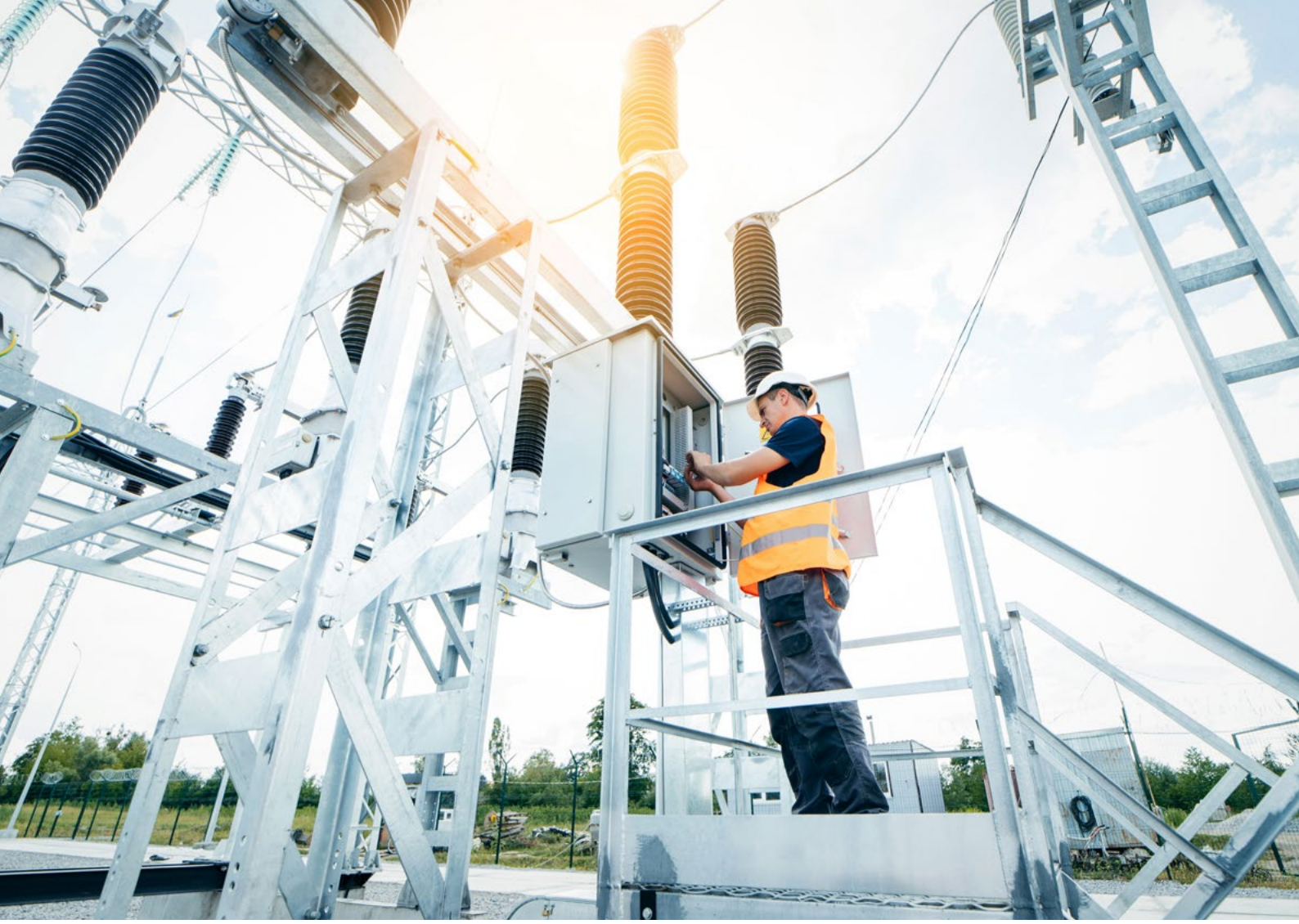
Lösning med AirKey

- Tillträdesbehörigheter hanteras centralt, även för externa tjänsteleverantörer (t.ex. underhållspersonal)
- Säker molnbaserad applikation
- Tillträdesmedia (smartphones, RFID) med mycket hög krypteringsnivå (ECDSA-256, AES-128)
- Loggning av alla tillträdeshändelser, export för revisioner
- GDPR-kompatibla raderingsfunktioner och Privacy by Design
- Uppdateringar och hantering av sårbarheter hanteras centralt av EVVA

Mervärde

Företaget kan visa sina kunder att det har infört lämpliga säkerhetsåtgärder för tillträdeskontroll i leveranskedjan och att det är väl förberett för revisioner och certifieringar.





Praktiskt exempel 3:

Krishantering och motståndskraft inom en stadsförvaltning

CER-relevant

Utgångsläge

En kommun ansvarar för kritisk infrastruktur (t.ex. vattenförsörjning och reningsverk) och måste säkerställa att tillträde till kritiska områden fortfarande är möjligt även i en nödsituation, till exempel vid en cyberattack eller ett strömavbrott.

Lösning med Xesar

- Offlinefunktion vid strömavbrott eller cyberattacker
- Snabb spärrning av komprometterade tillträdesmedia samt varningar om ej åtgärdade säkerhetsuppgifter
- Funktioner för säkerhetskopiering och återställning av konfigurationsdata

Mervärde

Kommunförvaltningen förblir handlingskraftig även i en krissituation, vilket innebär att invånare och lokala företag inte påverkas av avbrott eller störningar.

Praktiskt exempel 4:

Dataskydd och loggning vid ett forskningsinstitut

NIS2/CER-relevant

Utgångsläge

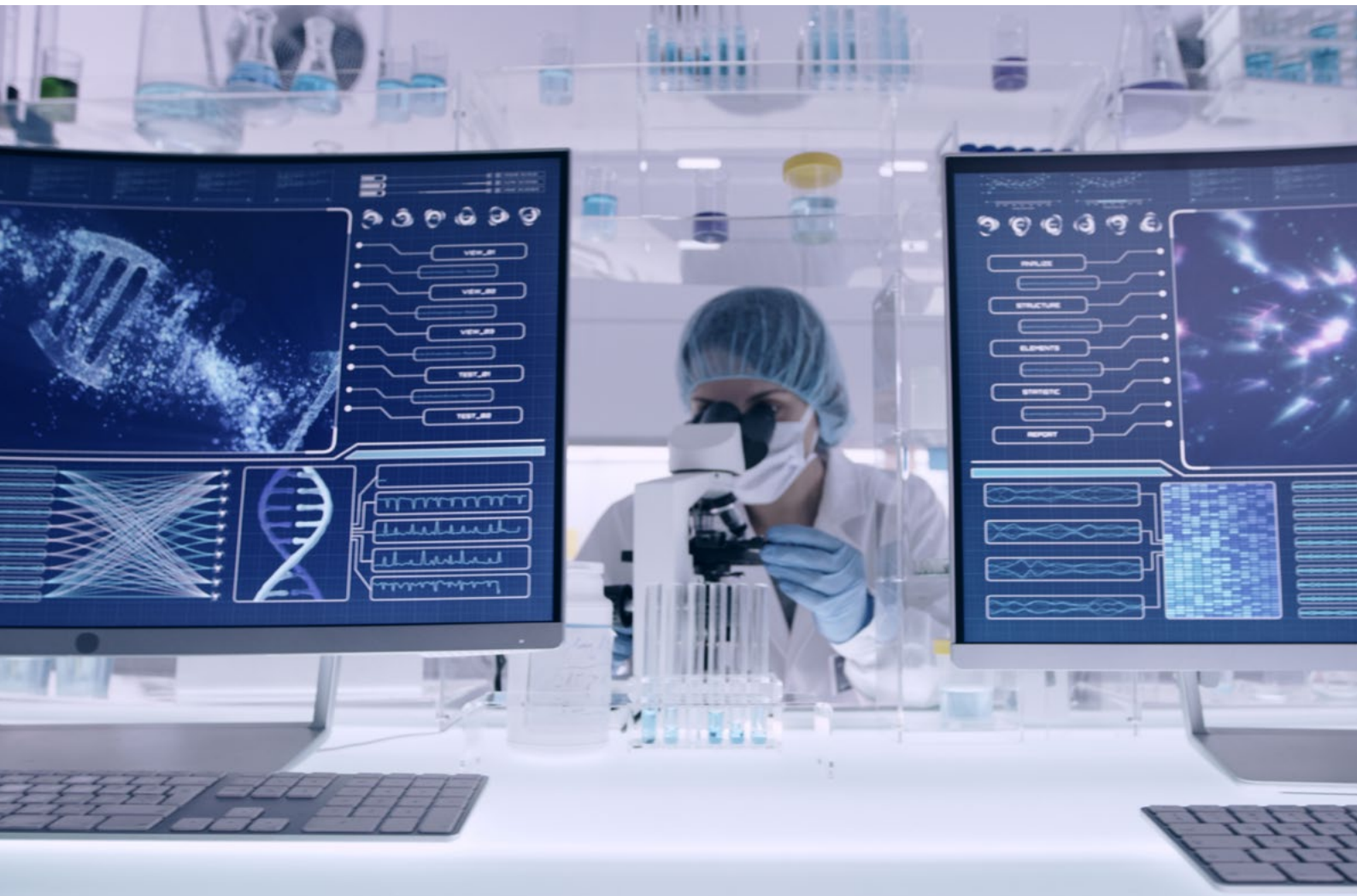
Ett forskningsinstitut behandlar känsliga personuppgifter och måste uppfylla kraven i GDPR och NIS2.

Lösning med AirKey

- Privacy by Design: Inga personuppgifter lagras i backend-systemet
- Konfigurerbar loggning och funktioner för radering av personuppgifter
- GDPR-anpassad implementering

Mervärde

Institutet kan när som helst styrka att det uppfyller kraven på dataskydd och transparens gentemot tillsynsmyndigheter och samarbetspartner.



Säkerhetskontroll för operatörer av kritisk infrastruktur

1. Organisatoriska säkerhetsramar

- Har vi ett fastställt säkerhetskoncept för att säkerställa ett effektivt fysiskt skydd?
- Finns det tydligt definierade roller, befogenheter och ansvarsområden för säkerhet, IT, fastighetsförvaltning och samhällsviktiga verksamheter?
- Granskas och uppdateras säkerhetsriktlinjer och säkerhetsprocesser regelbundet?
- Finns det tydliga rutiner som säkerställer att anmälningsplikten för säkerhetsincidenter uppfylls?

2. Riskanalys & efterlevnad

- Har vi genomfört en riskanalys enligt CER-direktivet under de senaste fyra åren?
- Har vi identifierat alla fysiska och digitala sårbarheter längs processkedjan?
- Uppfyller våra tillträdeslösningar kraven i NIS2, särskilt när det gäller säkra protokoll och skydd mot manipulation?
- Använder vi enbart moderna system och tekniker (inga okrypterade protokoll, exempelvis Wiegand)?

3. Tillträdesbehörigheter & identiteter

- Är alla tillträdesbehörigheter rollbaserade och tilldelade på ett spårbart sätt?
- Granskas och omcertifieras tillträdesbehörigheter regelbundet eller återkallas de automatiskt när de inte längre behövs?
- Har vi tydliga processer för onboarding, rollbyten och offboarding av medarbetare och tjänsteleverantörer?

4. Teknisk säkerhet vid tillträdeskontroll

- Är alla läsare, kort och tillträdesmedia krypterade?
- Är alla säkerhetskritiska dörrar, serverrum och kontrollrum skyddade med elektroniska passersystem?
- Lagras säkerhetsrelevanta data (t.ex. loggar) på ett revisionssäkert sätt och skyddas de mot manipulation?

5. Övervakning, loggning & transparens

- Loggas alla tillträdeshändelser och tillträdesförsök automatiskt?
- Är våra tillträdesloggar revisionssäkra, skyddade mot manipulation och lagras de under tillräckligt lång tid?
- Använder vi övervakningsverktyg som kopplar samman fysiska och digitala säkerhetshändelser?

6. Skydd av kritiska områden

- Är utrymmen som serverrum, kontrollcentraler, energi- och försörjningsanläggningar samt kopplingsskåp särskilt skyddade?
- Finns det tillträdesområden med flera säkerhetsnivåer?
- Finns det tillträdesområden med flera säkerhetsnivåer?
- Har vi en plan för nödåtkomst (t. ex. vid strömavbrott eller systemfel)?

7. Leverantörer & tjänsteleverantörer

- Har externa företag och tjänsteleverantörer endast tidsbegränsade och tydligt definierade tillträdesbehörigheter?
- Är tillträdet för tillfällig personal tekniskt begränsat och strikt övervakat?
- Granskas användningen av externa accesspunkter regelbundet?

8. Kris- och återställnings-förmåga

- Finns det en plan för hantering av nödsituationer och kriser som omfattar fysiska säkerhetsaspekter?
  - Finns det fastställda rutiner för: omedelbar spärrning av tillträdesbehörigheter för enskilda användare eller grupper?
  - snabb återställning av tillträdesinfrastrukturen efter en attack?
  - Evakuering eller incidenthantering?
- Övas dessa planer regelbundet?

9. Utbildning & medvetenhet

- Får alla medarbetare utbildning i hantering av tillträdesmedia?
- Finns det ett fortlöpande utbildnings- och informationsprogram om säkerhetsriktlinjer och lämpligt säkerhetsbeteende?
- Vet medarbetarna hur de ska anmäla misstänkta aktiviteter?

10. Framtidssäkerhet & vidareutveckling

- Är vår tillträdeslösning skalbar för nya anläggningar eller ytterligare krav?
- Kan vi utan problem integrera nya säkerhetsstandarder (NIS2-uppdateringar, BSI-riktlinjer, utökningar i CER-direktivet)?
- Har vi en tydlig moderniseringsplan om tekniken blir föråldrad eller om nya säkerhetssårbarheter upptäcks?

NIS2 och CER genomförs i de enskilda EU-medlemsstaterna under följande nationella lagstiftningsbeteckningar

	NIS2	CER
Österrike	NISG2026 (Lagen om nät- och informationssäkerhet 2026)	RKEG (Lagen om kritisk infrastruktur och motståndskraft)
Tyskland	NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)	KRITIS-Dachgesetz (Lag om förstärkning av den fysiska motståndskraften hos kritiska anläggningar)
Belgien	Loi NIS2 (Lag av den 26 april 2024 om cybersäkerhet för nät- och informationssystem)	Loi relative à la résilience des entités critiques (nationell lag om genomförande av CER, 2025/26)
Nederländerna	Cyberbeveiligingswet (i samband med den parlamentariska genomförandet, läget i april 2026)	Wet weerbaarheid kritieke entiteiten (planerad CER-lag, läget i april 2026)
Sverige	Cybersäkerhetslagen (Cybersecurity Act, SFS 2025:1506)	Lag om motståndskraft hos kritiska verksamheter (CER-implementering under förberedelse, läge april 2026)
Italien	Decreto Legislativo n. 138/2024	Decreto Legislativo n. 134/2024
Tjeckien	Zákon o kybernetické bezpečnosti (Ändring/ny version av genomförandet av NIS2)	Zákon o odolnosti kritických subjektů (CER-genomförandelagen)
Polen	Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) – Ändringsförslag till NIS2	Ustawa o odporności podmiotów krytycznych (under genomförande)
Slovakien	Zákon o kybernetickej bezpečnosti (NIS2-ändringen)	Zákon o odolnosti kritických subjektov

www.evva.com

I.ALLG.NIS2-CER.ID.WHPAP.SSV.LN | 26R1