EVVA
access to security

Whitepaper

Der erste Schutzwall
Zutrittskontrolle für kritische Infrastrukturen

Der erste Schutzwall Zutrittskontrolle für kritische Infrastrukturen

Wie moderne Zutrittskontrolle zur Erfüllung von NIS2 und CER beiträgt – und die physische Sicherheit nachhaltig erhöht.

Zutrittskontrolle als Schlüsselkomponente für NIS2- und CER-Compliance

Die Welt und auch wir haben uns – besonders in den letzten paar Jahren – verändert. Geopolitische Veränderungen wie Kriege, politische Instabilität, klimatologische Änderungen und neue Technologien bestimmen unseren Alltag und erfordern eine höhere Resilienz von lebensnotwendigen Einrichtungen insbesondere eine Erhöhung des physischen Schutzes.

Mit der europäischen NIS2 Richtlinie (2022/2555) und der ergänzenden CER Richtlinie (2022/2557) erhöht die Europäische Union die Sicherheitsanforderungen an Betreiber kritischer und wichtiger Einrichtungen deutlich. Beide Regelwerke verfolgen das Ziel, die Resilienz gegenüber digitalen und physischen Bedrohungen zentral zu stärken – damit rückt auch die Zutrittskontrolle in den Fokus moderner Sicherheitsarchitekturen. In diesem Whitepaper wollen wir uns vor allem dem Thema „Physische Schutzmaßnahmen für kritische Einrichtungen" zuwenden.

Regulatorischer Rahmen: NIS2 und CER

Die Begriffserklärungen

NIS2 und CER sind EU Richtlinien, die in nationale Gesetze umgesetzt werden müssen; die jeweiligen gesetzlichen Bezeichnungen in den europäischen Märkten finden Sie übersichtlich auf Seite 15 des Whitepapers.

NIS2

Cybersicherheit für kritische und wichtige Sektoren

- EU-Richtlinie (2022/2555)
- **Ziel:** Erhöhung des Cybersicherheitsniveaus durch EU-weite Mindeststandards. Verpflichtet Unternehmen und Organisationen, ihre IT- und Cybersicherheit systematisch zu verbessern und Vorfälle zu melden.
- **Gilt für:**
  - „Wesentliche" Einrichtungen: dazu zählen Unternehmen mit hoher Kritikalität deren Ausfall erhebliche Auswirkungen auf Gesellschaft, Wirtschaft oder öffentliche Sicherheit hätte, dazu zählen Energie, Verkehr, Banken, Gesundheitswesen, Wasser, Telko/IT
  - „Wichtige" Sektoren: dazu zählen Unternehmen sonstiger kritischer Auswirkung wie Post, Abfall, Chemie, Lebensmittel, Herstellung von Waren (ab 50 MA und 10 Mio. EUR Umsatz)
- **Anforderungen** an Unternehmen, welche unter NIS-2 fallen sind unter anderem
  - Cyber-Security-Management (Risikoanalysen, Sicherheitskonzepte, Incident-Response, Business Continuity)
  - Meldepflicht für Sicherheitsvorfälle
  - Verantwortung der Geschäftsleitung
  - Strenge Aufsicht und Sanktionen

CER

Physische Resilienz kritischer Infrastrukturen

- EU-Richtlinie (2022/2557)
- **Ziel:** Erhöhung physischer Widerstandsfähigkeit gegenüber nicht-digitalen Bedrohungen und Gefahren (all hazardous Ansatz)
- **Gilt für:** Betreiber kritischer Infrastruktur wie:
  - Energie
  - Verkehr
  - Banken
  - Gesundheitswesen
  - Wasser
  - Telko/IT
  - Lebensmittel
  - Chemie
- **Anforderungen:**
  - Risikoanalysen
  - Notfall- und Wiederanlaufpläne
  - Sicherheitsmaßnahmen
  - Lieferketten- und Abhängigkeitsmanagement
  - Meldepflicht für schwerwiegende Vorfälle
  - Sicherung der Kontinuität lebenswichtiger Dienste

In aller Kürze

Zusammengefasst heißt das, dass von NIS2 und CER betroffene Einrichtungen nach einer erfolgten systematischen Gefahren- und Risikoanalyse, sowie Bewertung, auch Maßnahmen für wirksamen physischen Schutz umsetzen müssen. Dazu gehören insbesondere Zugangskontrolle, Überwachung und Verfahren zur Erkennung von Vorfällen.

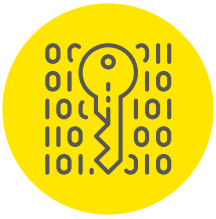
CER konkretisiert dies weiter: Betreiber kritischer Anlagen müssen alle vier Jahre Risikoanalysen durchführen, geeignete physische Schutzmaßnahmen umsetzen und unbefugte Zutritte wirksam verhindern.

Cybersecurity braucht auch physischen Schutz

Relevante Sicherheitsmerkmale für den Einsatz im NIS2- und CER-Umfeld

Physische Zugangssicherheit

- Strenge Zutrittskontrolle zu kritischen Bereichen
- Fälschungssichere Zutrittsmedien
- State-of-the-art-Technologien



IT-Sicherheit & Verschlüsselung

- Geschützte Kommunikation mit aktuellen Krypto-Standards (TLS, AES, ECDSA)
- Keine unsicheren Passwörter

Protokollierung & Audits

- Vollständige Dokumentation aller Zutritte und Systemaktionen
- Revisionssichere Logs mit Exportfunktion als Auditdokument

Vorfallsreaktion & Zugriffsschutz

- Schnelle Sperrung kompromittierter Zugänge
- Notfallpläne für Ausfall oder Angriff (Offline-Betrieb der Türen)

Business Continuity & Datenbackup

- Automatisiertes Datensicherungskonzept
- Wiederanlaufstrategie nach Ausfall, Redundanz

Schwachstellen-management & Updates

- Kontinuierliches Hersteller-Monitoring von Software-Sicherheitslücken (CVE)
- Zeitnahe, signierte und verifizierte Updates

Datenschutz & Datensicherheit

- Privacy by Design, DSGVO-Konformität
- Löschfunktionen für personenbezogene Daten
- Konfigurierbare Protokollierung
- Vier-Augen-Prinzip für Protokolleinsicht

EVVA-Produkte und ihre Antworten auf die regulatorischen Anforderungen

Xesar

Zutrittssystem für höchste Sicherheitsanforderungen

Physische & IT-Sicherheit

- Rollenbasierte Zutrittsrechte pro Person/Gruppe
- MIFARE DESFire EV1/EV2/EV3 (EAL5+), anlagenindividuelle AES-Schlüssel
- Verschlüsselte Challenge Response Kommunikation (keine Klartext-Protokolle)
- TLS ≥ 1.2 für Systemkommunikation
- interne AES256-Bit Verschlüsselung
- Passwörter gehasht (Bcrypt)

Zutritts- & Systemlogs

- Lückenlose, manipulationsgeschützte Ereignis- und Systemlogs
- Revisionssichere Exporte
- Audit und Incident-Nachweise jederzeit möglich

Vorfallsreaktion & Resilienz

- Echtzeitsperren (online), Blocklists für Offline Komponenten
- Warnmechanismen bei unsicherem Sperrstatus
- eigenständiger Offline Betrieb bei IT oder Netzwerkausfall

Updates & Schwachstellenmanagement

- Kontinuierliches CVE-Monitoring
- Kryptografisch signierte Updates (RSA/SHA256, AES256CCM)
- Verifizierte Firmware und Software-Updates

Business Continuity

- Verschlüsselte Backups
- Notfall Wiederherstellung über Anlagensicherheitsblatt
- Mehrplatz und 24/7 Serverbetrieb möglich

Datenschutz

- Privacy by Design
- Keine personenbezogenen Daten in der App
- Automatische Auflösung des Personenbezugs konfigurierbar

AirKey

Mobile Zutrittslösung mit höchsten Standards

Physische & IT-Sicherheit

- Smartphone & RFID basierte Zutrittsmedien (JCOP SmartMX3, EAL6+)
- ECDSA256 Authentifizierung + AESSessionKeys
- TLS gesicherte Online Verwaltung

Zutritts- & Systemlogs

- Revisionssichere Protokollierung
- Revisionssichere Exporte
- Automatische Aktualisierung von Blocklists & Logs
- Flexible, datenschutzkonforme Konfiguration

Vorfallsreaktion & Resilienz

- Echtzeitsperren über Internet
- Offline-Türfunktion auch bei Serverausfall
- Warnhinweise bei sicherheitskritischen Zuständen

Updates & Betrieb

- Zentrales, signiertes Update Management
- ISO 27001 zertifizierte Rechenzentren in Österreich
- Redundante EVVA-Server, HSM gesicherte Schlüssel

Datenschutz

- DSGVO konforme Löschkonzepte
- Privacy by Design
- Vier-Augen-Prinzip für Protokolleinsicht aktivierbar

NORMEN & ZERTIFIZIERUNGSSTATUS

Erfolgreich
geprüft (TÜV)
EN 18031-1

RED* ANFORDERUNGEN ERFÜLLT

*RED: Radio Equipment Directive

Praxisbeispiel 1:

Zutrittskontrolle in einem Krankenhaus

NIS2/CER-relevant

Ausgangslage

Ein Krankenhaus zählt zu den „wesentlichen Einrichtungen“ nach NIS2 und unterliegt strengen Anforderungen an IT- und physische Sicherheit. Besonders sensible Bereiche wie Serverräume, Medikamentenlager oder Intensivstationen müssen vor unbefugtem Zutritt geschützt werden.

Lösung mit Xesar

- Rollenbasierte Zutrittsrechte für verschiedene Mitarbeitergruppen (z.B. IT, Pflege, Verwaltung)
- Zutrittsmedien mit individuellen, hochsicheren Technologien (MIFARE DESFire EV3)
- Lückenlose Protokollierung aller Zutritte, revisionssichere Logs für Audits
- Schnelle Sperrung verlorener Medien über Echtzeit-Blocklists
- Offline-Betrieb der Türen bei Serverausfall (Business Continuity)
- Regelmäßige, signierte Software-Updates und Schwachstellenmanagement

Mehrwert

Das Krankenhaus setzt die risikobasierten Maßnahmen um, kann Vorfälle lückenlos nachweisen und steigert somit die physische Resilienz dieser Einrichtung.

Praxisbeispiel 2:

Produktionsbetrieb als Zulieferer für kritische Infrastruktur

Lieferkette/ CER-relevant

Ausgangslage

Ein mittelständischer Maschinenbauer beliefert Energieversorger und fällt damit indirekt unter die CER-Richtlinie. Der Betrieb muss nachweisen, dass seine Zutrittssysteme und IT-Infrastruktur resilient und sicher sind.

Lösung mit AirKey

- Zutrittsrechte werden zentral verwaltet, auch für externe Dienstleister (z.B. Wartungspersonal)
- Sichere cloudbasierte Anwendung
- Zutrittsmedien (Smartphones, RFID) mit sehr hoher Verschlüsselung (ECDSA-256, AES-128)
- Protokollierung aller Zutritte, Export für Audits
- DSGVO-konforme Löschfunktionen und Privacy by Design
- Updates und Schwachstellenmanagement zentral durch EVVA

Mehrwert

Der Betrieb kann seinen Kunden nachweisen, dass er die angemessenen Maßnahmen zur Sicherstellung in der Lieferkette in Bezug auf Zutritt umgesetzt hat und für Audits und Zertifizierungen optimal vorbereitet ist.

Praxisbeispiel 3

Notfallmanagement und Resilienz in einer Stadtverwaltung

CER-relevant

Ausgangslage

Eine Stadtverwaltung betreibt kritische Infrastrukturen (z.B. Wasserversorgung und Kläranlagen) und muss sicherstellen, dass im Notfall (z.B. Cyberangriff, Stromausfall) der Zugang zu wichtigen Bereichen weiterhin möglich ist.

Lösung mit Xesar

- Funktionsfähiger Offline Betrieb bei Stromausfall oder Cyberangriff
- Schnelle Sperrung kompromittierter Zutrittsmedien, Warnhinweise bei offenen Sicherheitsaufgaben
- Backup- und Wiederherstellungsfunktionen für Konfigurationsdaten

Mehrwert

Die Stadtverwaltung bleibt auch im Krisenfall handlungsfähig – die Bewohner:innen und ansässigen Betriebe sind von Ausfällen und Störungen nicht betroffen.

Praxisbeispiel 4

Datenschutz und Protokollierung in einem Forschungsinstitut

NIS2/CER-relevant

Ausgangslage

Ein Forschungsinstitut verarbeitet sensible personenbezogene Daten und muss die DSGVO sowie NIS2-Anforderungen erfüllen.

Lösung mit AirKey

- Privacy by Design: Keine Speicherung personenbezogener Daten im Backend
- Konfigurierbare Protokollierung, Löschfunktionen für personenbezogene Daten
- DSGVO-konforme Umsetzung

Mehrwert

Das Institut kann Datenschutz und Transparenz gegenüber Aufsichtsbehörden und Partnern jederzeit nachweisen.

Sicherheits-Check für Betreiber kritischer Infrastrukturen

1. Organisatorischer Sicherheitsrahmen

- Haben wir ein verbindliches Sicherheitskonzept, um die physische Sicherheit zu gewähren?
- Gibt es klar definierte Rollen-, Rechte- und Verantwortlichkeitsstrukturen für Sicherheit, IT, Facility und KRITIS-relevante Bereiche?
- Werden Sicherheitsrichtlinien und -prozesse regelmäßig überprüft und aktualisiert?
- Ist die Einhaltung der vorgeschriebenen Meldepflicht für Sicherheitsvorfälle prozessual gesichert?

2. Risikoanalyse & Compliance

- Haben wir innerhalb der letzten 4 Jahre eine Risikoanalyse gemäß KRITIS Dachgesetz/CER durchgeführt?
- Haben wir alle physischen und digitalen Schwachstellen entlang der Prozesskette identifiziert?
- Sind wir mit unseren Zutrittslösungen gut aufgestellt in Bezug auf NIS2, insbesondere in Bezug auf sichere Protokolle und Manipulationsschutz?
- Nutzen wir ausschließlich technisch zeitgemäße Systeme (keine unverschlüsselten Protokolle wie z. B. Wiegand)?

3. Zutrittsberechtigungen & Identitäten

- Sind alle Zutrittsberechtigungen rollenbasiert und nachvollziehbar zugeordnet?
- Werden Zutrittsrechte regelmäßig rezertifiziert oder automatisch entzogen, wenn sie nicht mehr benötigt werden?
- Haben wir klare Prozesse für Onboarding, Rollenwechsel und Offboarding von Mitarbeitenden und Dienstleistern?

4. Technische Sicherheit der Zutrittskontrolle

- Sind alle Zutrittsleser, Karten und Identifikationsmedien verschlüsselt?
- Sind alle sicherheitskritischen Türen, Serverräume und Leitstände durch elektronische Zutrittssysteme abgesichert?
- Werden sicherheitsrelevante Daten (z. B. Logs) auditfest gespeichert und vor Manipulation geschützt?

5. Monitoring, Protokollierung & Transparenz

- Werden alle Zutritte und Zugriffsversuche automatisiert protokolliert?
- Sind unsere Zutritts-Logs revisionssicher, manipulationsgeschützt und ausreichend lange gespeichert?
- Nutzen wir Monitoring-Tools, die physische und digitale Sicherheitsereignisse verknüpfen?

6. Schutz kritischer Bereiche

- Sind Bereiche wie Serverräume, Leitstellen, Energie-/Versorgungsanlagen oder Schaltschränke besonders geschützt?
- Gibt es mehrstufige Zutrittszonen mit zunehmendem Sicherheitsniveau?
- Sind sensible Räume zusätzlich durch Videoüberwachung, Türzustandsüberwachung oder Alarmtechnik gesichert?
- Haben wir einen Plan für den Notfallzugang (z. B. bei Stromausfall oder Systemstörung)

7. Lieferanten & Dienstleister

- Haben externe Firmen und Dienstleister nur zeitlich begrenzte und klar definierte Zutrittsrechte?
- Sind Zugänge für temporäres Personal technisch eingeschränkt und streng überwacht?
- Wird die Nutzung externer Zugänge regelmäßig auditiert?

8. Notfall- & Wiederherstellungsfähigkeit

- Existiert ein Notfall- und Krisenmanagementplan, der physische Sicherheitsaspekte einschließt?
- Sind Prozesse definiert für:
  - Sofortige Zugangssperrung einzelner Nutzer oder Gruppen
  - Schnelle Wiederherstellung der Zutrittsinfrastruktur nach einem Angriff
  - Evakuierungs- oder Incident Response Szenarien
- Werden diese Pläne regelmäßig geübt?

9. Schulung & Awareness

- Werden alle Mitarbeitenden im Umgang mit Zutrittsmedien geschult?
- Gibt es ein kontinuierliches Awareness Programm zu Sicherheitsrichtlinien und korrektem Verhalten?
- Wissen Mitarbeitende, wie sie verdächtige Aktivitäten melden?

10. Zukunftsfähigkeit & Weiterentwicklung

- Ist unsere Zutrittslösung skalierbar für neue Standorte oder zusätzliche Anforderungen?
- Können wir neue Sicherheitsstandards (NIS2 Updates, BSI Richtlinien, Erweiterungen im KRITIS Dachgesetz) problemfrei integrieren?
- Haben wir einen klaren Modernisierungsplan, falls Technologien veralten oder Sicherheitslücken bekannt werden?

NIS2 und CER werden in den einzelnen EU-Mitgliedstaaten unter folgenden nationalen Gesetzesnamen umgesetzt

	NIS2	CER
Österreich	NISG2026 (Netz- und Informationssicherheitsgesetz 2026)	RKEG (Resilienz kritischer Einrichtungs-Gesetz)
Deutschland	NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)	KRITIS-Dachgesetz (Gesetz zur Stärkung der physischen Resilienz kritischer Anlagen)
Belgien	Loi NIS2 (Gesetz vom 26. April 2024 zur Cybersicherheit von Netz- und Informationssystemen)	Loi relative à la résilience des entités critiques (nationales CER-Umsetzungsgesetz, 2025/26
Niederlande	Cyberbeveiligingswet (in parlamentarischer Umsetzung, Stand April 2026)	Wet weerbaarheid kritieke entiteiten (geplantes CER-Gesetz, Stand April 2026)
Schweden	Cybersäkerhetslagen (Cybersecurity Act, SFS 2025:1506)	Lag om motståndskraft hos kritiska verksamheter (CER-Umsetzung in Vorbereitung, Stand April 2026)
Italien	Decreto Legislativo n. 138/2024	Decreto Legislativo n. 134/2024
Tschechien	Zákon o kybernetické bezpečnosti (Novelle/ Neufassung zur NIS2-Umsetzung)	Zákon o odolnosti kritických subjektů (CER-Umsetzungsgesetz)
Polen	Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) – Novelle zur NIS2	Ustawa o odporności podmiotów krytycznych (in Umsetzung)
Slowakei	Zákon o kybernetickej bezpečnosti (NIS2-Novelle)	Zákon o odolnosti kritických subjektov

www.evva.com

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