EVVA
access to security

Whitepaper

La prima linea di difesa
Controllo degli accessi alle infrastrutture critiche

La prima linea di difesa Controllo degli accessi alle infrastrutture critiche

In che modo i moderni sistemi di controllo degli accessi contribuiscono al rispetto delle normative NIS2 e CER e aumentano in modo sostenibile la sicurezza fisica.

Il controllo degli accessi come elemento chiave per la conformità alle normative NIS2 e CER

Il mondo, e anche noi, siamo cambiati, soprattutto negli ultimi anni. I cambiamenti geopolitici, quali guerre, instabilità politica, cambiamenti climatici e nuove tecnologie, influenzano la nostra vita quotidiana e richiedono una maggiore resilienza delle infrastrutture essenziali, in particolare un rafforzamento della protezione fisica.

Con la direttiva europea NIS2 (2022/2555) e la direttiva complementare CER (2022/2557), l'Unione europea inasprisce notevolmente i requisiti di sicurezza a cui devono attenersi i gestori di infrastrutture critiche e importanti.

Entrambe le normative mirano a rafforzare in modo determinante la resilienza nei confronti delle minacce digitali e fisiche; di conseguenza, anche il controllo degli accessi diventa un elemento centrale delle moderne architetture di sicurezza. In questo white paper intendiamo concentrarci in particolare sul tema delle "misure di protezione fisica per le infrastrutture critiche".

Quadro normativo: NIS2 e CER

Definizioni dei termini

NIS2 e CER sono direttive dell'UE che devono essere recepite nella legislazione nazionale; le rispettive denominazioni giuridiche nei mercati europei sono riportate in modo chiaro a pagina 15 del white paper.

NIS2

Sicurezza informatica per i settori critici e strategici

- Direttiva UE (2022/2555)
- **Obiettivo:** aumentare il livello di sicurezza informatica attraverso standard minimi a livello dell'UE. Obbliga le imprese e le organizzazioni a migliorare sistematicamente la propria sicurezza informatica e a segnalare gli incidenti.
- **Valido per:**
  - Strutture «essenziali»: tra queste rientrano le imprese ad alta criticità il cui malfunzionamento avrebbe ripercussioni significative sulla società, sull'economia o sulla sicurezza pubblica, tra cui energia, trasporti, banche, sanità, risorse idriche, telecomunicazioni/IT
  - Settori «importanti»: tra questi rientrano le imprese con altre ripercussioni critiche quali servizi postali, gestione dei rifiuti, industria chimica, settore alimentare, produzione di beni (a partire da 50 dipendenti e 10 milioni di euro di fatturato)
- **Requisiti per** le aziende che rientrano nella Direttiva NIS-2, tra cui
  - Gestione della sicurezza informatica (analisi dei rischi
  - concetti di sicurezza, risposta agli incidenti, continuità operativa)
  - Segnalazione degli incidenti di sicurezza Responsabilità della direzione
  - Stretta supervisione e sanzioni

CER

Resilienza fisica delle infrastrutture critiche

- Direttiva UE (2022/2557)
- **Obiettivo:** Aumento della resistenza fisica contro le minacce non digitali e pericoli (approccio all hazardous)
- **Valido per:** Operatori di infrastrutture critiche come:
  - Energia
  - Transporti
  - Banche
  - Sanità
  - Acqua
  - Telecomunicazioni/IT
  - Alimentare
  - Chimica
- **Requisiti:**
  - Analisi dei rischi
  - Piani di emergenza e di ripristino
  - Misure di sicurezza
  - Gestione della catena di fornitura e delle dipendenze
  - Segnalazione degli incidenti gravi
  - Garantire la continuità delle attività vitali

In breve

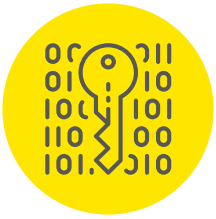
In sintesi, ciò significa che le strutture interessate dalla direttiva NIS2 e dal regolamento CER devono, a seguito di un' analisi sistematica dei pericoli e dei rischi e della relativa valutazione, attuare anche misure volte a garantire un'efficace protezione fisica. Tra queste figurano in particolare il controllo degli accessi, la sorveglianza e le procedure per l'individuazione degli incidenti. Il CER precisa ulteriormente questo aspetto: i gestori di infrastrutture critiche devono effettuare analisi dei rischi ogni quattro anni, attuare misure di protezione fisica adeguate e impedire efficacemente gli accessi non autorizzati.

La sicurezza informatica richiede anche una protezione fisica

Caratteristiche di sicurezza rilevanti per l'utilizzo in contesti NIS2 e CER

Sicurezza fisica

- Degli accessi
- Rigoroso controllo degli accessi alle aree critiche
- Supporti di accesso a prova di contraffazione
- Tecnologie all'avanguardia



Sicurezza informatica e crittografia

- Comunicazione protetta con gli standard crittografici più recenti (TLS, AES, ECDSA
- Nessuna password non sicura

Registrazione e audit

- Documentazione completa di tutti gli accessi e delle azioni del sistema
- Registri a prova di revisione con funzione di esportazione come documento di audit

Risposta agli incidenti e protezione degli accessi

- Blocco immediato degli accessi compromessi
- Piani di emergenza in caso di guasto o attacco (funzionamento offline delle porte)

Continuità operativa e backup dei dati

- Piano di backup automatizzato
- Strategia di ripristino in caso di guasto, ridondanza

Gestione delle vulnerabilità e aggiornamenti

- Monitoraggio continuo da parte dei produttori delle vulnerabilità software (CVE)
- Aggiornamenti tempestivi, firmati e verificati

Protezione dei dati e sicurezza dei dati

- Privacy by Design, conformità al GDPR
- Funzioni di cancellazione dei dati personali
- Registrazione configurabile
- Principio del doppio controllo per la consultazione dei registri

I prodotti EVVA e la loro risposta ai requisiti normativi

Xesar

Sistema di accesso per i più elevati requisiti di sicurezza

Sicurezza fisica e informatica

- Diritti di accesso basati sui ruoli per persona/gruppo
- MIFARE DESFire EV1/EV2/EV3 (EAL5+), chiavi AES specifiche per ogni impianto
- Comunicazione Challenge-Response crittografata (nessun protocollo in chiaro)
- TLS ≥ 1.2 per la comunicazione di sistema
- Crittografia interna AES a 256 bit
- Password sottoposte a hash (Bcrypt)

Registri di accesso e di sistema

- Registri degli eventi e di sistema completi e a prova di manomissione
- Esportazioni a prova di revisione
- Documentazione di audit e incidenti disponibile in qualsiasi momento

Reazione agli incidenti e resilienza

- Blocchi in tempo reale (online), liste di blocco per componenti offline
- Meccanismi di allerta in caso di stato di blocco incerto
- Funzionamento autonomo offline in caso di guasto dell'IT o della rete

Aggiornamenti e gestione delle vulnerabilità

- Monitoraggio continuo dei CVE
- Aggiornamenti firmati crittograficamente (RSA/SHA256, AES256CCM)
- Aggiornamenti verificati del firmware e del software

Continuità operativa

- Backup crittografati
- Ripristino di emergenza tramite scheda di sicurezza del sistema
- Possibilità di funzionamento multiutente e 24 ore su 24, 7 giorni su 7

Protezione dei dati

- Privacy by Design
- Nessun dato personale nell'app
- Possibilità di configurare la rimozione automatica dei riferimenti personali

AirKey

Soluzione di accesso mobile con standard di massima qualità

Sicurezza fisica e informatica

- Dispositivi di accesso basati su smartphone e RFID (JCOP SmartMX3, EAL6+)
- Autenticazione ECDSA256 + AESSessionKeys
- Gestione online protetta tramite TLS

Registri di accesso e di sistema

- Registrazione a prova di revisione
- Esportazioni a prova di revisione
- Aggiornamento automatico delle liste di blocco e dei log
- Configurazione flessibile e conforme alle norme sulla protezione dei dati

Reazione agli incidenti e resilienza

- Blocchi in tempo reale via Internet
- Funzionamento offline della porta anche in caso di guasto del server
- Avvisi in caso di condizioni critiche per la sicurezza

Aggiornamenti e funzionamento

- Gestione centralizzata e firmata degli aggiornamenti
- Data center certificati ISO 27001 in Austria
- Server EVVA ridondanti, chiavi protette da HSM

Protezione dei dati

- Procedure di cancellazione conformi al GDPR
- Privacy by Design
- Principio del doppio controllo per la consultazione dei registri attivabile

NORME E STATO DELLA CERTIFICAZIONE

Certificato
(TÜV)
EN 18031-1

REQUISITI RED* SODDISFATTI

*RED: Direttiva sulle apparecchiature radio

Esempio pratico 1:

Controllo degli accessi in un ospedale

Rilevante ai fini della direttiva NIS2/CER

Situazione iniziale

Un ospedale rientra tra le «strutture essenziali» ai sensi della direttiva NIS2 ed è soggetto a severi requisiti in materia di sicurezza informatica e fisica. Le aree particolarmente sensibili, quali le sale server, i magazzini dei farmaci o i reparti di terapia intensiva, devono essere protette da accessi non autorizzati.

Soluzione con Xesar

- Diritti di accesso basati sui ruoli per diversi gruppi di dipendenti (ad es. IT, assistenza, amministrazione)
- Supporti di accesso con tecnologie personalizzate e altamente sicure (MIFARE DESFire EV3)
- Registrazione completa di tutti gli accessi, registri a prova di revisione per gli audit
- Blocco rapido dei supporti smarriti tramite liste di blocco in tempo reale
- Funzionamento offline delle porte in caso di guasto del server (continuità operativa)
- Aggiornamenti software regolari e firmati e gestione delle vulnerabilità

Valore aggiunto

L'ospedale attua misure basate sul rischio, è in grado di documentare in modo completo gli incidenti e aumenta così la resilienza fisica della struttura.

Esempio pratico 2:

Azienda di produzione che opera come fornitore per infrastrutture critiche

Catena di fornitura/ Rilevante ai fini CER

Situazione iniziale

Un'azienda di medie dimensioni operante nel settore della costruzione di macchinari rifornisce le società di fornitura energetica e rientra quindi indirettamente nell'ambito di applicazione della direttiva CER. L'azienda deve dimostrare che i propri sistemi di accesso e la propria infrastruttura informatica sono resilienti e sicuri.

Soluzione con AirKey

- I diritti di accesso sono gestiti a livello centrale, anche per i fornitori di servizi esterni (ad es. il personale di manutenzione)
- Applicazione sicura basata su cloud
- Supporti di accesso (smartphone, RFID) con crittografia di altissimo livello (ECDSA-256, AES-128)
- Registrazione di tutti gli accessi, esportazione per gli audit
- Funzioni di cancellazione conformi al GDPR e «Privacy by Design»
- Aggiornamenti e gestione delle vulnerabilità gestiti centralmente da EVVA

Valore aggiunto

L'azienda è in grado di dimostrare ai propri clienti di aver adottato le misure adeguate per garantire la sicurezza della catena di fornitura in materia di accessi e di essere preparata al meglio per gli audit e le certificazioni.

Esempio pratico 3:

Gestione delle emergenze e resilienza in un'amministrazione comunale

Rilevante ai fini della direttiva CER

Situazione iniziale

Un'amministrazione comunale gestisce infrastrutture critiche (ad esempio, l'approvvigionamento idrico e gli impianti di depurazione) e deve garantire che, in caso di emergenza (ad esempio, un attacco informatico o un'interruzione di corrente), l'accesso alle aree importanti rimanga possibile.

Soluzione con Xesar

- Funzionamento offline garantito in caso di interruzione di corrente o attacco informatico
- Blocco rapido dei supporti di accesso compromessi, avvisi in caso di attività di sicurezza in sospeso
- Funzioni di backup e ripristino dei dati di configurazione

Valore aggiunto

L'amministrazione comunale rimane operativa anche in caso di crisi: i residenti e le aziende locali non subiscono interruzioni né disagi.

Esempio pratico 4:

Protezione dei dati e registrazione in un istituto di ricerca

Rilevante ai fini della direttiva NIS2/CER

Situazione iniziale

Un istituto di ricerca tratta dati personali sensibili e deve rispettare il GDPR e i requisiti della direttiva NIS2.

Soluzione con AirKey

- Privacy by Design: nessuna memorizzazione di dati personali nel backend
- Registrazione configurabile, funzioni di cancellazione dei dati personali
- Implementazione conforme al GDPR

Valore aggiunto

L'istituto è in grado di dimostrare in qualsiasi momento il rispetto della protezione dei dati e della trasparenza nei confronti delle autorità di vigilanza e dei partner.

Verifica di sicurezza per i gestori di infrastrutture critiche

1. Quadro organizzativo di sicurezza

- Disponiamo di un piano di sicurezza vincolante per garantire la sicurezza fisica?
- Esistono strutture chiaramente definite in termini di ruoli, diritti e responsabilità per la sicurezza, l'IT, la gestione delle strutture e i settori rilevanti ai fini KRITIS?
- Le linee guida e i processi di sicurezza vengono regolarmente verificati e aggiornati?
- Il rispetto dell'obbligo di segnalazione previsto per gli incidenti di sicurezza è garantito a livello procedurale?

2. Analisi dei rischi e conformità

- Negli ultimi 4 anni abbiamo effettuato un'analisi dei rischi ai sensi della legge quadro KRITIS/CER?
- Abbiamo identificato tutte le vulnerabilità fisiche e digitali lungo l'intera catena di processo?
- Le nostre soluzioni di accesso sono adeguate ai requisiti della direttiva NIS2, in particolare per quanto riguarda i protocolli sicuri e la protezione contro le manomissioni?
- Utilizziamo esclusivamente sistemi tecnicamente all'avanguardia (senza protocolli non crittografati come ad esempio Wiegand)?

3. Autorizzazioni di accesso e identità

- Tutte le autorizzazioni di accesso sono assegnate in base ai ruoli e in modo tracciabile?
- I diritti di accesso vengono ricertificati regolarmente o revocati automaticamente quando non sono più necessari?
- Disponiamo di procedure chiare per l'inserimento, il cambio di ruolo e l'uscita dal servizio di dipendenti e fornitori di servizi?

4. Sicurezza tecnica del controllo degli accessi

- Tutti i lettori di accesso, le tessere e i supporti di identificazione sono crittografati?
- Tutte le porte critiche per la sicurezza, le sale server e le sale di controllo sono protette da sistemi di accesso elettronici?
- I dati rilevanti per la sicurezza (ad es. i log) vengono archiviati in modo conforme ai requisiti di audit e protetti da eventuali manomissioni?

5. Monitoraggio, registrazione e trasparenza

- Tutti gli accessi e i tentativi di accesso vengono registrati automaticamente?
- I nostri registri di accesso sono a prova di revisione, protetti da manomissioni e conservati per un periodo di tempo sufficientemente lungo?
- Utilizziamo strumenti di monitoraggio che collegano gli eventi di sicurezza fisici e digitali?

6. Protezione delle aree critiche

- Aree quali sale server, centri di controllo, impianti energetici/di approvvigionamento o quadri elettrici sono protette in modo particolare?
- Esistono zone di accesso a più livelli con un livello di sicurezza crescente?
- I locali sensibili sono ulteriormente protetti tramite videosorveglianza, monitoraggio dello stato delle porte sistemi di allarme?
- Disponiamo di un piano per l'accesso di emergenza (ad es. in caso di interruzione di corrente o malfunzionamento del sistema)?

7. Fornitori e prestatori di servizi

- Le aziende e i fornitori di servizi esterni dispongono solo di diritti di accesso limitati nel tempo e chiaramente definiti?
- Gli accessi per il personale temporaneo sono limitati dal punto di vista tecnico e sottoposti a stretta sorveglianza?
- L'utilizzo degli accessi esterni viene sottoposto a regolari verifiche?

8. Capacità di gestione delle emergenze e di ripristino

- Esiste un piano di gestione delle emergenze e delle crisi che includa gli aspetti relativi alla sicurezza fisica?
- Sono state definite procedure per:
  - il blocco immediato dell'accesso a singoli utenti o gruppi
  - il ripristino rapido dell'infrastruttura di accesso a seguito di un attacco
  - scenari di evacuazione o di risposta agli incidenti
- Questi piani vengono messi in pratica regolarmente?

9. Formazione e sensibilizzazione

- Tutti i dipendenti ricevono una formazione sull'uso dei dispositivi di accesso?
- Esiste un programma di sensibilizzazione continuo sulle linee guida di sicurezza e sul comportamento corretto da tenere?
- I dipendenti sanno come segnalare attività sospette?

10. Sostenibilità e sviluppo continuo

- La nostra soluzione di controllo degli accessi è scalabile per nuove sedi o requisiti aggiuntivi?
- Siamo in grado di integrare senza problemi i nuovi standard di sicurezza (aggiornamenti NIS2, linee guida BSI, estensioni della legge quadro KRITIS)?
- Disponiamo di un piano di modernizzazione chiaro nel caso in cui le tecnologie diventino obsolete o vengano individuate delle vulnerabilità di sicurezza?

La direttiva NIS2 e il regolamento CER sono recepiti nei singoli Stati membri dell'UE con le seguenti denominazioni legislative nazionali

	NIS2	CER
Austria	NISG2026 (Legge sulla sicurezza delle reti e dell'informazione del 2026)	RKEG (Legge sulla resilienza delle infrastrutture critiche)
Germania	NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)	KRITIS-Dachgesetz (Legge sul rafforzamento della resilienza fisica delle infrastrutture critiche)
Belgio	Loi NIS2 (Legge del 26 aprile 2024 sulla sicurezza informatica delle reti e dei sistemi informativi)	Loi relative à la résilience des entités critiques (Legge nazionale di attuazione del CER, 2025/26)
Paesi Bassi	Cyberbeveiligingswet (in fase di attuazione parlamentare, aggiornato ad aprile 2026)	Wet weerbaarheid kritieke entiteiten (progetto di legge CER, aggiornato ad aprile 2026)
Svezia	Cybersäkerhetslagen (Cybersecurity Act, SFS 2025:1506)	Lag om motståndskraft hos kritiska verksamheter (Attuazione della CER in fase di preparazione, aggiornato ad aprile 2026)
Italia	Decreto Legislativo n. 138/2024	Decreto Legislativo n. 134/2024
Repubblica Ceca	Zákon o kybernetické bezpečnosti (Emendamento/Nuova versione relativa all'attuazione della direttiva NIS2)	Zákon o odolnosti kritických subjektů (Legge di attuazione della CER)
Polonia	Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) – Emendamento alla direttiva NIS2	Ustawa o odporności podmiotów krytycznych (in fase di attuazione)
Slovacchia	Zákon o kybernetickej bezpečnosti (Emendamento alla direttiva NIS2)	Zákon o odolnosti kritických subjektov

www.evva.com

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