EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

CER & NIS-2

Resilienz in Luxemburg

Zutrittskontrolle in
kritischen Infrastrukturen

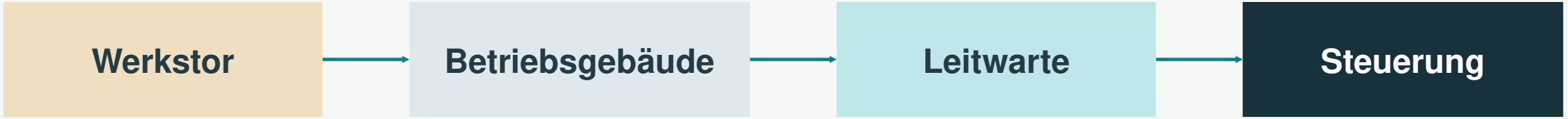
CRA ergänzt die Sicherheit digitaler Produkte



Klaus Wollscheid **CEO EIWTC SARL** CSO BEWENG S.A.

Unser Beispiel: ein kritisches Wasserwerk

Trinkwasser muss verfügbar bleiben.



Besucher werden empfangen und begleitet.

Techniker erhalten auftragsbezogene Rechte.

Betriebspersonal hält die Versorgung aufrecht.

Wartung erfolgt nur nach Freigabe.

Zusätzlich: abgelegene Pumpstation mit zeitweise unterbrochener Netzverbindung.

Fiktives Beispiel: Die förmliche Benennung als kritische Einrichtung wird angenommen.

Eine offene Tür kann die Versorgung treffen

Unbefugter Zutritt → **Eingriff in Steuerung** → **Ausfall der Versorgung**

Verlorener Ausweis bleibt gültig

Schrank oder Netzwerk ist erreichbar

Trinkwasserleistung wird beeinträchtigt

Weitere Ursachen

Hochwasser · Stromausfall · Personalausfall
Lieferengpass · Cyberangriff · Sabotage

Gemeinsam bewerten: Eintrittswege, Abhängigkeiten, Folgen und Wiederanlauf.

Luxemburgs acht Resilienzsäulen

ZIVILE VORBEREITUNG

1	2	3 CER	4	MILITÄRISCHE VORBEREITUNG
Demokratie, Rechtsstaat und Regierung	Resiliente Gesellschaft	**Wesentliche Dienste und kritische Infrastrukturen**	Resiliente Wirtschaft	8 Schutz und Verteidigung des eigenen Territoriums und der Verbündeten

5 Strategische und logistische Ressourcen

6 Cyberresilienz **NIS-2**

7 Zivile Verteidigung

CER: Versorgung sichern · NIS-2: Systeme schützen · CRA: Produkte absichern.

Verkürzte Bezeichnungen. Hervorhebung und regulatorische Zuordnung: fachliche Einordnung.

Welche Bereiche sind erfasst?

12 CER-Sektoren

Auch Sektoren im NIS-2-Anwendungsbereich

Energie	Abwasser
Verkehr	Digitale Infrastruktur
Bankwesen	Öffentliche Verwaltung
Finanzmarktinfrastrukturen	Weltraum
Gesundheit	Lebensmittel
Trinkwasser	Abfallbewirtschaftung

6 weitere NIS-2-Sektoren

- IKT-Dienste (B2B)
- Post- und Kurierdienste
- Chemikalien
- Bestimmte Herstellungsbereiche
- Digitale Anbieter
- Forschung

Beispiele: Stromnetzbetreiber, Krankenhaus, Wasserversorger, Rechenzentrum.

Die Sektorzugehörigkeit ist der erste Schritt. Einrichtungsart und Einstufung entscheiden.

Kritisch, wesentlich oder wichtig?

CER

Kritisch

Förmliche Benennung nach Bedeutung des Dienstes und möglichen Störungsfolgen.

Beispiel: benanntes Wasserwerk.

NIS-2

Wesentlich

In der Regel große Einrichtungen aus Anhang I. Zusätzlich gelten gesetzliche Sondertatbestände.

Beispiel: großes Krankenhaus oder DNS-Anbieter.

NIS-2

Wichtig

In der Regel mittlere aus Anhang I sowie mittlere und große aus Anhang II, ohne Sonderstatus.

Beispiel: mittelgroßer Maschinenbauer.

Unser CER-benanntes Wasserwerk gilt unter NIS-2 als wesentlich, unabhängig von der Größe.

Wesentliche und wichtige Einrichtungen haben beide Sicherheits- und Meldepflichten.

Zutrittskontrolle verbindet CER und NIS-2

CER

Luxemburg: Art. 12 Abs. 1 № 2 und 5

EU: Art. 13 Abs. 1 Buchst. b und e

Physischer Schutz sowie Personal- und Zutrittsberechtigungen.

NIS-2

Luxemburg: Art. 12 Abs. 2 № 8–10

EU: Art. 21 Abs. 2 Buchst. h, i und j

Kryptografie, Zugriffskontrolle und angemessene Authentifizierung.

Im Wasserwerk **Freigegebene Personen erreichen die Leitwarte. Zutrittsserver, Rechteentzug und Notbetrieb sind abgesichert.**

Nachweise: Zonenplan, Rechtefreigabe, Sperrtest und Wiederanlauftest.

Beide nationalen Gesetze nennen Art. 12. Die EU-Artikelnummern unterscheiden sich.

Leitungsverantwortung wird konkret

1	**Billigen**	Schutzbedarf, Zutrittskonzept und Restrisiken freigeben
2	**Ermöglichen**	Verantwortliche, Budget und Ersatzversorgung benennen
3	**Überwachen**	Sperrzeiten, Wartungsrechte und Ausfalltests prüfen
4	**Lernen**	Leitung schulen und Abweichungen nachverfolgen

NIS-2 · wesentlich
10 Mio. € / 2 %*

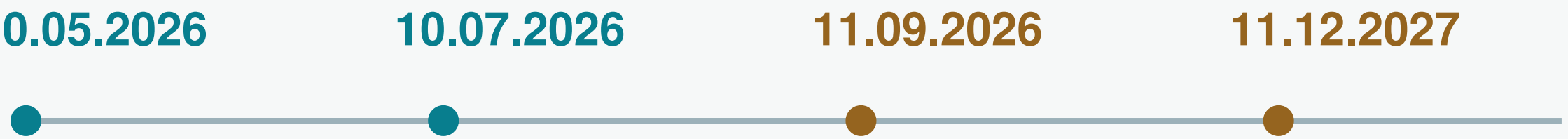
NIS-2 · wichtig
7 Mio. € / 1,4 %*

CER · Geldbuße bis
250.000 €

* Jeweils höherer Betrag aus Festbetrag und weltweitem Jahresumsatz.

Die Umsetzung läuft bereits

Stand 13. Oktober 2026



CER & NIS-2

Luxemburgische Gesetze in Kraft

NIS-2

Frist zur erstmaligen Selbstregistrierung

CRA

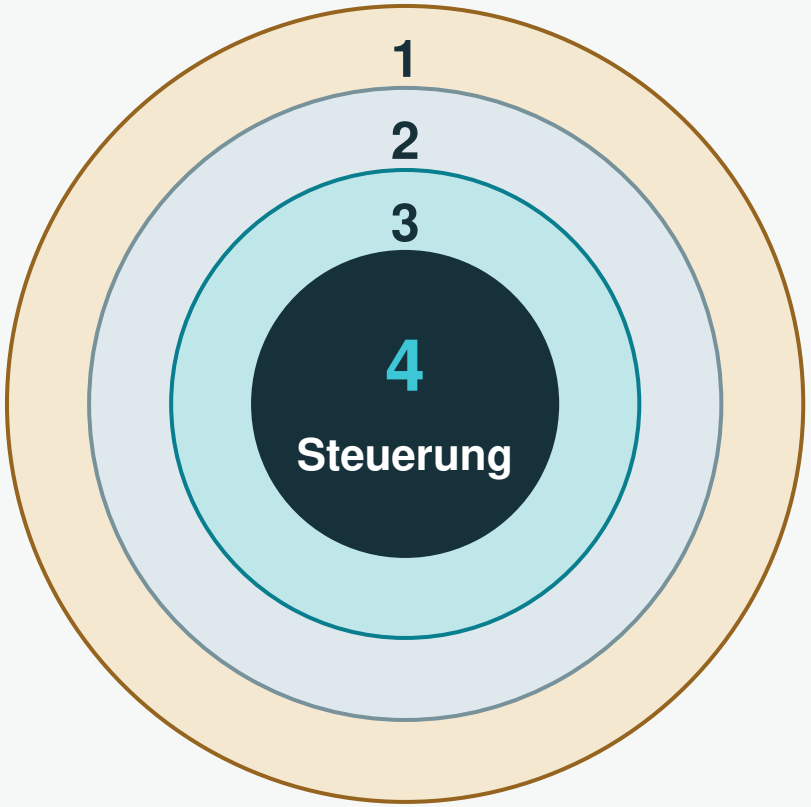
Hersteller müssen relevante Vorfälle und Schwachstellen melden

CRA

Hauptpflichten für digitale Produkte gelten

CER-Fristen für einzelne Einrichtungen knüpfen an die Benennung an.

Das Zwiebelschalenprinzip



1 Gelände / äußerer Perimeter

Zaun, Tor und Besucherführung begrenzen den Zugang zum Betriebsstandort.

2 Gebäude / innerer Perimeter

Kontrollierte Außentüren lassen nur freigegebene Personen in das Gebäude.

3 Sensible Räume

Leitwarte und Serverraum erhalten eigene rollenbezogene Zutrittsrechte.

4 Kritische Komponenten

Steuerschrank oder Rack nur mit Freigabe für die konkrete Aufgabe öffnen.

Jede Schale schützt den nächsten Bereich. Der Kreis zeigt Schutzgrenzen, keinen Gebäudeplan.

Vier Zonen als Planungsbeispiel. EN 50600-2-5 behandelt Sicherungssysteme von Rechenzentren.

Ein Wartungsauftrag führt durch vier Freigaben

Ein externer Techniker wartet heute die Steuerung. Sein Auftrag bestimmt den erlaubten Weg.

1 · Werkstor	2 · Gebäude	3 · Leitwarte	4 · Steuerung
Identität und Termin prüfen	Zugang nur für das Zeitfenster	Betrieb gibt den Zutritt frei	Konkreten Eingriff gesondert freigeben
Anmeldung beim Empfang	Berechtigung befristen	Begleitung nach Schutzbedarf	Auftrag und Öffnung belegen

Nach der Wartung **Rechte enden, Komponenten sind verschlossen, der Auftrag ist dokumentiert.**

Berechtigungen folgen der Aufgabe

Eintritt	Änderung	Austritt
Identität prüfen Rolle freigeben	Alte Rechte entziehen Neue Aufgabe prüfen	Ausweis sperren Wirksamkeit bestätigen

Wartungsauftrag

Externer Techniker erhält Zugang zur Pumpstation: nur zur freigegebenen Zeit und für den benötigten Bereich. Leitwarte und Steuerung bleiben ohne Auftrag gesperrt.

Sensible Funktionen: CER-Personalüberprüfung vor Freigabe prüfen. Details in R10.

Die Schalen müssen gemeinsam funktionieren

Eine äußere Barriere fällt aus.

Innere Grenzen sollen den Zugang weiter begrenzen und eine Reaktion ermöglichen.

Umgehungen schließen	Lieferzugang, Seitentür und Fremdfirmen erhalten dieselben klaren Freigaberegeln.
Ereignisse bearbeiten	Eine zu lange offene Leitwartentür wird erkannt. Ein benannter Verantwortlicher reagiert.
Ausfälle beherrschen	Lokaler Betrieb, Notzugang und sichere Flucht sind festgelegt und gemeinsam getestet.

Prüffall: Trotz geöffnetem Werkstor bleibt die Leitwarte für Unberechtigte gesperrt.

Die Grenzen rein mechanischer Schlüssel

Wer kann die Leitwarte nach einem Schlüssel-verlust öffnen?

Die Antwort braucht einen wirksamen Entzugsprozess.

Nachvollziehbarkeit

Das Schloss selbst liefert kein Ereignisprotokoll. Ausgabe und Rückgabe müssen nachweisbar sein.

Verlust und Kopien

Einzelne Schlüssel lassen sich nicht digital sperren. Betroffene Zylinder und Ersatzmaßnahmen prüfen.

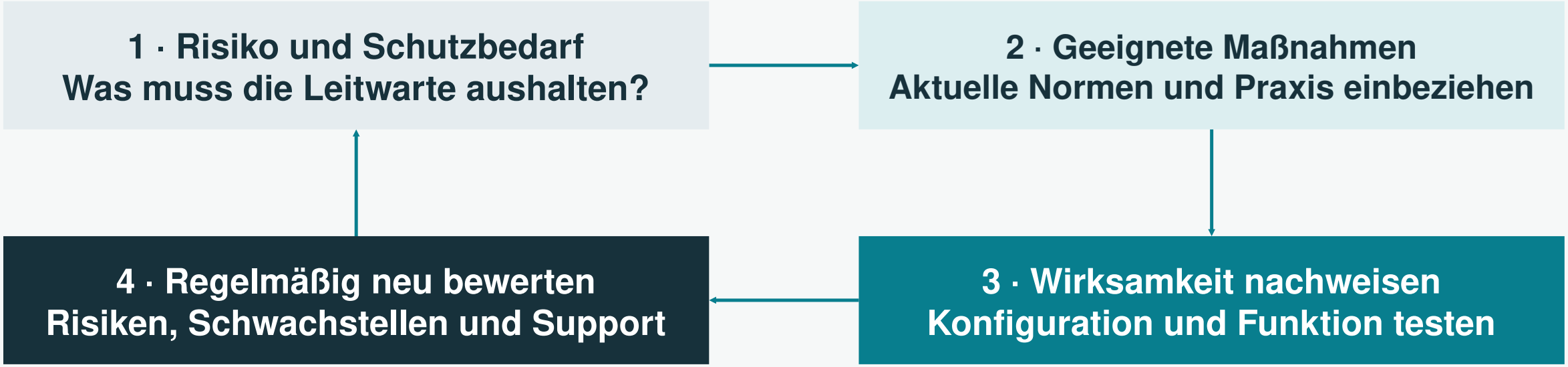
Zeit und Rolle

Rein mechanische Schlüssel setzen keine zeitabhängigen Rechte automatisch um.

Mechanik kann geeignet sein. Bei hohen Anforderungen können ergänzende Maßnahmen nötig werden.

Was bedeutet „Stand der Technik“?

Schutzmaßnahmen auf aktuellem technischem Entwicklungsstand, die für das konkrete Risiko geeignet und praktisch wirksam sind.



Aufwand und Kosten fließen in die Verhältnismäßigkeit ein. Das erforderliche Schutzniveau bleibt maßgeblich.

Vier Entwicklungsstufen der Zutrittskontrolle

01

Reaktiv

Mechanik

Schlüssel vergeben und zurückfordern.

Vergabe belegen. Bei Verlust ggf. Schloss austauschen.

02

Identifiziert

Elektronik

Individuelles Medium und Zutrittsereignisse.

Ausweis gezielt sperren. Sperrzeit hängt von der Systemarchitektur ab.

03

Dynamisch

Rechteverwaltung

Rollen und Zeitfenster je Wartungsauftrag.

Bei Austritt sperren. Änderungen mit HR abstimmen.

04

Proaktiv

Überwachung

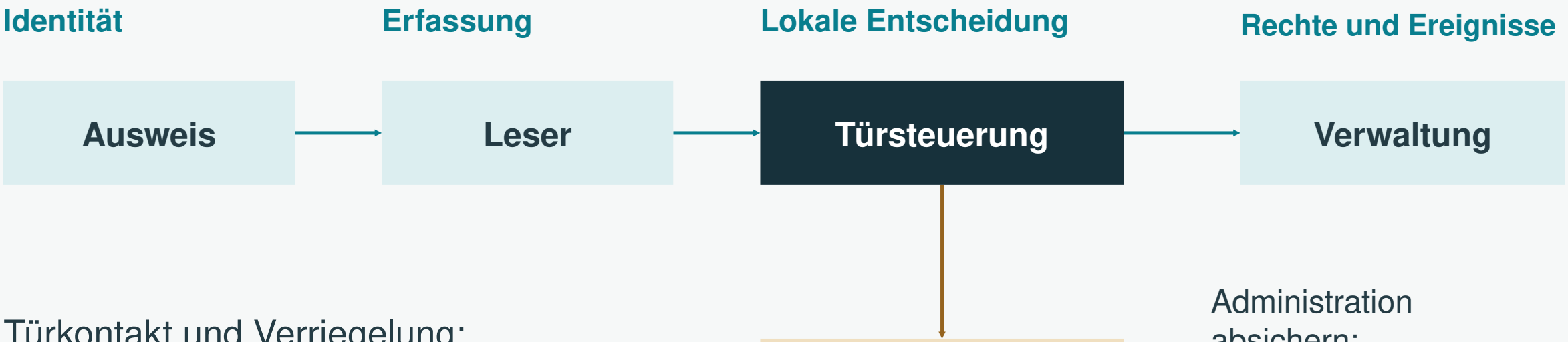
Angriffe erkennen. Gezielt reagieren.

MFA risikogerecht: Karte und PIN möglich. Notbetrieb testen.

Stand der Technik ergibt sich aus dem Schutzbedarf und der nachgewiesenen Funktion.

Entwicklungsmodell, keine gesetzliche Rangfolge. Biometrie ist keine allgemeine Voraussetzung.

Auch das Zutrittssystem braucht Schutz



Türkontakt und Verriegelung: Manipulation erkennen, Fluchtanforderungen beachten.

Administration absichern: Mehrfaktorprüfung, getrennte Netze und begrenzte Dienste.

Zutrittsnetz und Prozesssteuerung erhalten definierte, begrenzte Schnittstellen.

Physischer Türschutz und digitale Systemhärtung werden gemeinsam geplant.

CRA ergänzt die Sicherheit der Produkte

CER & NIS-2 führen das Schutzkonzept.

Leser und Controller

Sichere Voreinstellungen, Zugriffsschutz und Integrität

Verwaltungssoftware

Schwachstellen bearbeiten, sichere Updates liefern

Produktlebenszyklus

Konformität dokumentieren, Supportende offenlegen

Support grundsätzlich mindestens fünf Jahre; erwartete Nutzung berücksichtigen.

CRA ist eine EU-Verordnung: Hauptpflichten ab 11.12.2027, Herstellermeldungen seit 11.09.2026.

Kryptografie schützt die gesamte Verbindung

Ausweis ↔ Leser	Leser ↔ Controller	Controller ↔ Server
Echtheit prüfen; Kopieren und Wiederholen von Signalen erschweren.	Nachrichten authentisieren; Integrität und erforderliche Vertraulichkeit schützen.	Gegenstellen prüfen; Übertragung und Administration absichern.

Schlüssel Erzeugen → schützen → verteilen → erneuern → widerrufen / löschen

Updates Herkunft und Unverändertheit prüfen; nur autorisierte Firmware zulassen.

Verfahren und Parameter risikogerecht festlegen; keine pauschale AES-256- oder TLS-1.3-Pflicht.

Beschaffung verbindet Hersteller und Betreiber

Hersteller liefert

Sicherheits- und Konformitätsangaben
Updateweg und Schwachstellenkontakt
Supportzeitraum und Integrationshinweise

Betreiber übernimmt

Sichere Konfiguration und Rechte
Wartung, Monitoring und Notbetrieb
Abnahme und spätere Austauschplanung



Abnahme am Wasserwerk: Sperre, Ausfall, Wiederanlauf und Update testen

Ein sicheres Produkt braucht einen sicheren Betrieb – und überprüfbare Herstellerzusagen.

Verlorener Ausweis: Wann wirkt die Sperre?

Verlust gemeldet

Identität prüfen.
Ausweis sperren.
Risiko bis zur Sperre
aktiv begrenzen.

Online-Tür · Leitwarte

Sperre verteilt? Controller bestätigt?
Zutrittsversuch tatsächlich abgewiesen?

Offline-Tür · Pumpstation

Lokales Update oder Ablauf der Berechtigung.
Bis dahin: vorab festgelegte Ersatzmaßnahme.

Sperrzeit am realen Schloss messen – einschließlich unterbrochener Verbindung.

Strom- oder Netzausfall: Der Betrieb muss handeln

1 **Verbindung unterbrochen**

Lokale Rechte und definierte Sperrregeln wirken weiter.

2 **Stromversorgung gestört**

Tür, Controller und Versorgung nach Schutzbedarf auslegen.

3 **Notzugang erforderlich**

Berechtigtes Betriebspersonal erreicht die kritische Anlage.

4 **System wieder verfügbar**

Rechte, Zeit und Ereignisse kontrolliert abgleichen.



Je Tür gemeinsam festlegen: Flucht, Schutz gegen Zutritt und sichere Wiederherstellung.

Gemeinsame Übung: den Ablauf beherrschen

08:10

Netz fällt aus

Ein Techniker muss die Leitwarte erreichen.

CER: Notzugang gelingt, Flucht bleibt gewährleistet.

08:20

Ausweis verloren

An der Pumpstation ist das Recht noch gespeichert.

NIS-2: Restrisiko begrenzen, Sperrwirkung nachweisen.

08:35

System kehrt zurück

Rechte, Zeit und Ereignisse werden abgeglichen.

Gemeinsam: Funktion prüfen, Vorfälle bewerten.

CRA ergänzt bei Produktfehlern: Hersteller einbinden und sichere Abhilfe prüfen.

Ein Vorfall kann zwei Meldewege auslösen

Beispiel: Manipulation an der Zutrittssteuerung stört den Wasserwerksbetrieb.

NIS-2	**24 h**	**72 h**	**1 Monat***
	Frühwarnung	Vorfallmeldung	Abschlussbericht
CER	**24 h**	**1 Monat**	**HCPN**
	Erste Meldung	Detailbericht, soweit relevant	Zuständiger Kanal

* NIS-2: ein Monat nach der Vorfallmeldung. Erste Fristen jeweils ab Kenntnis.

Meldepflicht anhand der jeweiligen Erheblichkeit prüfen; CRA-Herstellermeldung separat.

Stand der Technik im Audit belegen

Leitwarte

Ein verlorener Ausweis muss zuverlässig unwirksam werden.

Die zulässige Sperrzeit folgt aus der Risikoanalyse.

Anforderung

Ziel, zulässige Sperrzeit und Verantwortliche sind schriftlich festgelegt.

Lösung

Architektur, sichere Einstellungen und Herstellersupport passen zum Schutzziel.

Betriebstest

Der Ausweis wird an der echten Tür abgewiesen. Netzausfall und Wiederanlauf werden mitgeprüft.

Dokumentation

Testprotokoll, Abweichungen und Maßnahmen zeigen Ergebnis und weitere Verantwortung.

Der Nachweis verbindet Risikoanalyse, Produktauswahl und wirksamen Betrieb.

Nachweise im ISMS dauerhaft verankern

ISMS = Informationssicherheitsmanagementsystem



Risiko	Maßnahme	Nachweis	Verbesserung
Verlorener Ausweis an der Pumpstation	Begrenzte Gültigkeit und Sperrprozess	Sperrtest und Ereignisprotokoll	Abweichung beheben und erneut prüfen

Ein gemeinsamer Nachweisbestand

Zonenplan · Rechteprüfung · Konfiguration · Wartung · Vorfälle · Übungsprotokolle

Ein dokumentierter Reifegrad unterstützt die Aufsicht; eine automatische Auditbefreiung gibt es nicht.

Umsetzungsplan für das Wasserwerk

01–30

Einordnen und erfassen

Betroffenheit und Registrierung
Zonen, Anlagen und Dienstleister
Schlüssel und Berechtigungen

31–60

Lücken schließen

Risikoanalyse und Prioritäten
Technikauswahl und Sperrprozess
Notzugang und Produktzusagen

61–90

Prüfen und verankern

Ausfall- und Wiederanlauftest
Schulung und Nachweisbestand
ISMS und laufende Rechteprüfung

Arbeitsplan als Beispiel. Gesetzliche und benennungsbezogene Fristen gehen vor.

Vier Entscheidungen für einen wirksamen Schutz

1 **Schutzbedarf bestätigen**

Trinkwasserversorgung, Zonen und maximal tragbare Ausfälle festlegen.

2 **Verantwortung verbinden**

Leitung, Betrieb, IT, HR und Lieferanten verbindlich zusammenführen.

3 **Zutrittskonzept freigeben**

Rechteentzug, Notbetrieb, Kryptografie und Support finanzieren.

4 **Wirksamkeit demonstrieren**

Gemeinsamen Ausfalltest terminieren und Nachweise bewerten.

CER und NIS-2 führen das Programm. CRA stärkt die dafür eingesetzten Produkte.

CER: Sektoren und typische Betreiber

01 Energie
Stromnetz, Gasversorgung, Energiespeicher

02 Verkehr
Flughafen, Bahn-Infrastruktur, öffentlicher Verkehr

03 Bankwesen
Kreditinstitute

04 Finanzmarktinfrastrukturen
Handelsplätze und zentrale Gegenparteien

05 Gesundheit
Krankenhäuser und weitere erfasste Leistungserbringer

06 Trinkwasser
Versorgung und Verteilung von Trinkwasser

07 Abwasser
Sammlung, Behandlung und Beseitigung

08 Digitale Infrastruktur
Rechenzentren, Cloud, DNS und Telekommunikation

09 Öffentliche Verwaltung
Erfasste zentrale öffentliche Einrichtungen

10 Weltraum
Betreiber erfasster Bodeninfrastruktur

11 Lebensmittel
Erfasste Großproduktion, Verarbeitung und Großhandel

12 Abfallbewirtschaftung
Erfasste Abfallsammlung, Behandlung und Entsorgung

Kritisch wird die Einrichtung durch förmliche Benennung nach Art. 7 des CER-Gesetzes.

NIS-2: zehn Maßnahmengruppen im Zutrittsbetrieb

01 Risikoanalyse und Sicherheitskonzepte
Zonen, Rollen und Ausfallfolgen bewerten

02 Bewältigung von Vorfällen
Sperren, eingrenzen, dokumentieren und melden

03 Betriebskontinuität und Krisenmanagement
Notzugang, Sicherung und Wiederanlauf testen

04 Sicherheit der Lieferkette
Wartungsfirma, Hersteller und Support prüfen

05 Beschaffung, Entwicklung und Wartung
Härtung, Updates und Schwachstellen steuern

06 Wirksamkeit der Maßnahmen bewerten
Sperr-, Ausfall- und Wiederherstellungstests

07 Cyberhygiene und Schulung
Administration, Betrieb und Externe schulen

08 Kryptografie und Verschlüsselung
Kommunikation, Schlüssel und Firmware schützen

09 Personal, Zugriff und Anlagenverwaltung
Eintritt, Wechsel, Austritt und Inventar verbinden

10 MFA und gesicherte Kommunikation
Adminzugänge und Krisenkommunikation absichern

Nationaler Art. 12 / EU-Art. 21: Maßnahmen angemessen und verhältnismäßig umsetzen.

CER: Fristen und sensible Funktionen

Benennung

Mitteilung an die Einrichtung

9 Monate

Risikoanalyse erstellen

10 Monate

Kapitel 4 grundsätzlich anwendbar

Risikoanalyse aktualisieren

Bei Bedarf, mindestens alle vier Jahre.

Hintergrundüberprüfungen

Gesetzlich definierte sensible Funktionen. Einwilligung und geregeltes Verfahren beachten.

Bescheid: fünf Jahre gültig. Erneuerung sechs bis vier Monate vor Ablauf beantragen.

Aufsicht und Sanktionen unterscheiden sich

Thema	NIS-2	CER
Zuständige Stelle	ILR; CSSF für gesetzlich zugewiesene Finanzbereiche	HCPN im CER-Rahmen, Sonderbereiche beachten
Geldbußen	Wesentlich: bis 10 Mio. € / 2 %* Wichtig: bis 7 Mio. € / 1,4 %*	Bis 250.000 € nach nationalem Art. 19
Leitung	Billigung, Aufsicht und Schulung nach nationalem Art. 13	Verantwortliche Umsetzung der Resilienzmaßnahmen

* Jeweils der höhere Betrag aus Festbetrag und weltweitem Jahresumsatz.

DORA: digitale operationale Resilienz im Finanzsektor. Überschneidungen je Pflicht prüfen.

Zutrittssysteme nach ihrer Funktion vergleichen

Kriterium	Mechanisch	Elektronisch offline	Elektronisch online
Rechte verändern	Schlüsselvergabe / gegebenenfalls Zylindertausch	Lokal, über Datenträger oder definierte Rückkanäle	Zentrale Verteilung mit Wirksamkeitskontrolle
Verlust und Entzug	Rückgabe oder Austausch; Kopierbarkeit bewerten	Sperrverteilung und Gültigkeitsdauer entscheiden	Bestätigung am Controller; Netzausfall berücksichtigen
Ereignisse nachweisen	Organisatorische Ausgabe- und Nutzungsbelege	Speicher, Auslesung und Zeitstempel prüfen	Erfassung, Übertragung und Auswertung absichern
Ausfall beherrschen	Mechanischer Notzugang und Schlüsselverfügbarkeit	Energiequelle, lokale Rechte und Ersatzverfahren	Stromreserve, lokale Autonomie und Wiederanlauf

Elektromechanisch oder batterielos beschreibt noch nicht, wie Rechte aktualisiert werden.

Die geeignete Kombination ergibt sich aus Schutzbedarf, Nutzung und nachgewiesener Funktion.

CRA: Einstufung folgt der Kernfunktion

01

Grundkategorie

Anforderungen gelten ebenfalls. Das Konformitätsverfahren folgt den gesetzlichen Voraussetzungen.

02

Wichtige Produkte

Anhang III, Klassen I und II. Beispiele für Klasse I: IAM/PAM und bestimmte Smart-Home-Schlösser.

03

Kritische Produkte

Anhang IV. Eigene Kategorien und gegebenenfalls zusätzliche Zertifizierungsanforderungen.

Ein Produkt wird durch seinen Einsatz in KRITIS allein noch nicht zum kritischen CRA-Produkt.

Technische Abnahme braucht prüfbare Belege

Schutzziel	Prüffrage	Geeigneter Beleg
Identität und Berechtigung	Sind Geräte eindeutig identifizierbar und Rechte wirksam entziehbar?	Identitätskonzept, Sperr- und Rollentest
Geschützte Kommunikation	Sind Echtheit, Integrität und erforderliche Vertraulichkeit durchgängig geschützt?	Protokoll-/Kryptokonzept, Konfigurationsprüfung
Firmware und Updates	Akzeptiert das Produkt nur autorisierte und unveränderte Updates?	Update- und Negativtest, Signaturprüfung
Schlüssel und Zertifikate	Funktionieren Erneuerung, Widerruf und Ersatz bei Kompromittierung?	Lebenszyklusverfahren, Ablauf-/Widerrufstest
Verfügbarkeit und Support	Funktioniert der definierte Notbetrieb bis zum geplanten Produktende?	Ausfalltest, Supportzusage, Ersatz- und Migrationsplan

Keine universelle Vorgabe für AES-256, TLS 1.3, HSM oder Post-Quanten-Verfahren.

Meldepflichten: Auslöser und Folgeberichte

Regime / Auslöser	Erste Meldung	Folgemeldung	Abschluss
NIS-2 Erheblicher Vorfall	24 h ab Kenntnis	72 h ab Kenntnis*	1 Monat nach der Vorfallmeldung
CER Erhebliche Störung	24 h ab Kenntnis	Kein allgemeiner 72-h-Schritt	Detailbericht binnen 1 Monat, soweit relevant
CRA Hersteller Aktiv ausgenutzte Schwachstelle	24 h ab Kenntnis	72 h ab Kenntnis	14 Tage nach Verfügbarkeit einer Abhilfemaßnahme
CRA Hersteller Schwerwiegender Sicherheitsvorfall	24 h ab Kenntnis	72 h ab Kenntnis	1 Monat nach der Vorfallmeldung

* Sonderregeln für Vertrauensdienste und fortdauernde Vorfälle beachten.

Meldepflichten separat bewerten, Fakten und Kommunikation gemeinsam koordinieren.

Nationale Resilienz braucht vernetzte Verantwortung

Öffentliche Stellen

SNR sieht Resilienzbeauftragte und Kontinuitätspläne in allen öffentlichen Institutionen vor.

Zivile und militärische Vorsorge

Wesentliche Dienste, Transport und Logistik unterstützen auch die Handlungsfähigkeit im Bündnis.

Bezug zum Wasserwerk

Krisenkontakte, Ersatzressourcen und Wiederanlauf mit den zuständigen Stellen abstimmen.

SNR liefert den strategischen Rahmen; konkrete Unternehmenspflichten ergeben sich aus dem Recht.

Sensible Funktionen brauchen besondere Prüfung

Wer darf die Leitwarte warten?

Funktion und Zugang zum kritischen Dienst bestimmen den Prüfbedarf.

1. Sensible Funktion festlegen
2. Gesetzliches Verfahren durchführen
3. Zutrittsrechte getrennt freigeben

5 Jahre

Gültigkeit des Bescheids

Erneuerung beantragen:

6 bis 4 Monate vor Ablauf

Keine pauschale Überprüfung aller Beschäftigten; gesetzliche Voraussetzungen beachten.

NIS-2: Einordnung an konkreten Beispielen

Fiktive Einrichtung	Regelfall der Einstufung	Warum?
CER-benannter Wasserversorger	Wesentlich, auch bei kleiner Größe	Kritische CER-Einrichtung
Großes Krankenhaus	Wesentlich	Erfasste Einrichtungsart in Anhang I
Mittleres Krankenhaus, ohne Sonderstatus	Wichtig	Anhang I, mittlere Größe
Mittlerer oder großer Maschinenbauer	Wichtig, sofern erfasste Herstellungsart	Anhang II, ohne wesentlichen Sonderstatus
DNS-Anbieter mit kleinem Team	Wesentlich	Größenunabhängiger Sondertatbestand

„Mittel“ und „groß“ folgen der EU-KMU-Definition. Partner und verbundene Unternehmen zählen mit.

Sektor und Einrichtungsart prüfen, Größe berechnen, Sondertatbestände berücksichtigen.

Rechtsgrundlagen und Quellen

NIS-2 in Luxemburg	Gesetz vom 5. Mai 2026, Mémorial A 225 https://legilux.public.lu/eli/etat/leg/loi/2026/05/05/a225/jo
CER in Luxemburg	Gesetz vom 5. Mai 2026, Mémorial A 226 https://legilux.public.lu/eli/etat/leg/loi/2026/05/05/a226/jo
Cyber Resilience Act	Verordnung (EU) 2024/2847 https://eur-lex.europa.eu/eli/reg/2024/2847/oj

Nationale Resilienzstrategie und Behördenhinweise

letzprepare.public.lu hcpn.gouvernement.lu ilr.lu digital-strategy.ec.europa.eu