EIWTC · CER / NIS-2 / CRA

Podcast-Transkript

Cyber- und Sabotageschutz im Wasserwerk

Deutsch – redaktionell bearbeitete Lesefassung

Redaktionell bearbeitete Fassung nach der eingereichten PDF, kein unabhängig verifizierter Wort-für-Wort-Audioabgleich. Fachinformationen, keine Rechtsberatung.

Inhaltsübersicht

01 · Begrüßung, Aufhänger & Vorstellung des Rahmens

02 · Modellannahmen & Der All-Hazards-Ansatz

03 · Nationale Strategie & Das Dreigespann CER, NIS-2 und CRA

04 · Die Gesetze vom 5. Mai 2026, Artikelbezüge & Haftung

05 · Das Zwiebelschalenprinzip & Der Zutrittslebenszyklus

06 · Grenzen der Mechanik, Stand der Technik & Reifegradmodell

07 · Systemaufbau, Kryptografie & Die Rolle des Cyber Resilience Acts (CRA)

08 · Detaillierte Analyse der 3 Audit-Praxisfälle

09 · Gemischte Meldepflichten (24h / 72h / 1M) & Behördenwege

10 · Der 90-Tage-Umsetzungsplan & Die 4 Management-Entscheidungen

11 · Reserve-Exkurse, DORA-Sonderregeln & Technische Vertiefung

Kapitel 1: Begrüßung, Aufhänger & Vorstellung des Rahmens

Moderator (Chris)
Herzlich willkommen zu unserer heutigen Spezialausgabe im Podcast für kritische Infrastrukturen und Resilienz! Wir sprechen heute über ein Thema, das auf den ersten Blick sehr physisch und alltäglich wirkt, aber bei genauerem Hinsehen das direkte Bindeglied zwischen digitaler Cybersicherheit, physischem Sabotageschutz und staatlicher Regulierung darstellt: die Zutrittskontrolle in kritischen Infrastrukturen am konkreten Beispiel eines Wasserwerks.

Klaus Wollscheid
Hallo Chris, vielen Dank für die Einladung! Ich freue mich sehr, heute hier zu sein. Als CEO der EIWTC SARL und CSO der BEWENG S.A. beschäftige ich mich täglich genau mit dieser Schnittstelle. Denn ob im Wasserwerk, im Krankenhaus oder im Rechenzentrum – eine unbefugt geöffnete Tür kann im schlimmsten Fall die gesamte Versorgung lahmlegen.

Moderator (Chris)
Klaus, wir haben heute ein enorm dichtes Programm vor uns. Seit den neuen Luxemburger Gesetzen vom 5. Mai 2026, die die europäischen Richtlinien CER und NIS-2 in nationales Recht umgesetzt haben, sowie dem EU Cyber Resilience Act (CRA) stehen Betreiber vor ganz konkreten rechtlichen und technischen Pflichten. Wir wollen heute wirklich jedes Detail ausleuchten: vom Zwiebelschalenprinzip über den Zutrittslebenszyklus bis hin zu konkreten Audit-Praxisfällen und den Reserve-Sonderregeln.

Klaus Wollscheid
Absolut! Und das Wichtigste dabei ist: Wir betrachten das nicht theoretisch im luftleeren Raum, sondern an einem ganz anschaulichen Modell – unserem fiktiven, aber hochrealistischen kritischen Wasserwerk. Denn beim Wasserwerk geht es um nichts Geringeres als um die lückenlose Aufrechterhaltung der Trinkwasserversorgung der Bevölkerung.

Kapitel 2: Modellannahmen & Der All-Hazards-Ansatz

Moderator (Chris)
Lass uns direkt beim Wasserwerk ansetzen. Welche Standorte und Bereiche umfasst unser Modellbeispiel genau?

Klaus Wollscheid
Wir nehmen für unser Modell an, dass das Wasserwerk förmlich als kritische Einrichtung benannt wurde. Die Anlage gliedert sich typischerweise in vier Kernbereiche: Erstens das äußere Werkstor, an dem Besucher empfangen und begleitet werden. Zweitens das Betriebsgebäude, in dem Techniker auftragsbezogene Rechte erhalten. Drittens die zentrale Leitwarte, wo das Betriebspersonal rund um die Uhr die Versorgung aufrechterhält und die Wartung nur nach förmlicher Freigabe erfolgt. Und viertens das Herzstück: die eigentliche Steuerung und Sensorik. Zusätzlich nehmen wir noch eine abgelegene, dezentrale Pumpstation an, die zeitweise nur eine unterbrochene Netzverbindung hat.

Moderator (Chris)
Das klingt extrem praxisnah! Warum ist die Zutrittskontrolle bei diesem Aufbau so eine Schlüsselstelle? Was kann schiefgehen?

Klaus Wollscheid
Wir sprechen im modernen Sicherheitsmanagement vom 'All-Hazards-Ansatz' – also der gemeinsamen Betrachtung physischer und digitaler Risiken. Sehen wir uns die Kette an: Ein verlorener oder entwendeter Mitarbeiterausweis bleibt im System gültig. Ein Unbefugter verschafft sich damit Zutritt durch eine Tür. Er gelangt zum Steuerschrank oder an eine offene Netzwerkbuchse im Betriebsgebäude. Dort nimmt er eine Manipulation vor oder speist Schadsoftware ein – und das Resultat ist der plötzliche Ausfall der Steuerung und eine Beeinträchtigung der Trinkwasserleistung! Eine einfache physisch offene Tür führt also direkt zum IT-Ausfall und zum Versorgungsstopp.

Moderator (Chris)
Und der All-Hazards-Ansatz geht ja noch weiter als nur klassische Sabotage, richtig?

Klaus Wollscheid
Exakt. Neben Cyberangriffen und gezielter Sabotage bewerten wir immer auch Naturgefahren wie Hochwasser, Stromausfälle, Personalausfälle durch Pandemien sowie Lieferengpässe. Alles muss gemeinsam bewertet werden: Eintrittswege, Abhängigkeiten, Folgen und die konkreten Pläne zum Wiederanlauf.

Kapitel 3: Nationale Strategie & Das Dreigespann CER, NIS-2 und CRA

Moderator (Chris)
Das bringt uns direkt zur rechtlichen und strategischen Einbettung. Luxemburg hat eine übergeordnete nationale Resilienzstrategie mit acht Säulen verabschiedet. Wie ordnen sich unsere Gesetze dort ein?

Klaus Wollscheid
Luxemburg gliedert seine Resilienz in acht Säulen: Säule 1 (Demokratie, Rechtsstaat und Regierung), Säule 2 (Resiliente Gesellschaft), Säule 3 ist die CER-Säule für wesentliche Dienste und kritische Infrastrukturen, Säule 4 (Resiliente Wirtschaft), Säule 5 (Strategische und logistische Ressourcen), Säule 6 ist die NIS-2-Säule für Cyberresilienz, Säule 7 (Zivile Verteidigung) und Säule 8 (Schutz und Verteidigung des eigenen Territoriums). Man sieht sofort: CER sichert die physikalische und operative Versorgung, NIS-2 schützt die digitalen Netze und Systeme, und der Cyber Resilience Act (CRA) sichert die eingesetzten digitalen Produkte ab.

Moderator (Chris)
Welche Sektoren fallen in Luxemburg unter diesen Regulierungsrahmen?

Klaus Wollscheid
Unter CER fallen 12 Sektoren: Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheit, Trinkwasser, Abwasser, Digitale Infrastruktur, Öffentliche Verwaltung, Weltraum, Lebensmittel und Abfallbewirtschaftung. NIS-2 erfasst viele dieser Bereiche und ergänzt weitere Sektoren, darunter: IKT-Dienste (B2B), Post- und Kurierdienste, Chemikalien, bestimmte Herstellungsbereiche, digitale Anbieter sowie Forschung. Das ist eine vereinfachte Sektorübersicht. Die konkrete Betroffenheit hängt von der Einrichtungsart, Größenkriterien und gesetzlichen Sonderregeln ab.

Moderator (Chris)
Wie werden die Einrichtungen darin kategorisiert? Es gibt ja die Begriffe 'Kritisch', 'Wesentlich' und 'Wichtig'.

Klaus Wollscheid
Das ist ein ganz entscheidender Punkt für die Audits! Unter CER heißt die Einstufung 'Kritische Einrichtung' – das erfolgt durch förmliche Benennung durch den Staat aufgrund der gesellschaftlichen Bedeutung. Unter NIS-2 unterscheidet man zwischen 'Wesentlichen Einrichtungen' (in der Regel große Unternehmen aus Anhang I oder Sondertatbestände) und 'Wichtigen Einrichtungen' (mittlere Unternehmen aus Anhang I sowie mittlere und große aus Anhang II). Für unser Wasserwerk gilt der wichtige Grundsatz: Sobald ein Wasserwerk unter CER förmlich als kritisch benannt ist, gilt es unter NIS-2 automatisch als 'Wesentliche Einrichtung' – völlig unabhängig von seiner Mitarbeiterzahl oder seinem Umsatz!

Kapitel 4: Die Gesetze vom 5. Mai 2026, Artikelbezüge & Haftung

Moderator (Chris)
Kommen wir zu den konkreten Rechtsgrundlagen in Luxemburg. Welches Datum müssen sich Sicherheitsverantwortliche rot im Kalender anstreichen?

Klaus Wollscheid
Den 5. Mai 2026! An diesem Tag wurden im Mémorial A die beiden nationalen Gesetze veröffentlicht: Mémorial A 225 regelt NIS-2 in Luxemburg, und Mémorial A 226 regelt das CER-Gesetz. Beide Gesetze traten am 10. Mai 2026 in Kraft. Und das Schöne ist: Beide Gesetze nennen in ihrer Paragraphenstruktur genau denselben Artikel für die Sicherheitsmaßnahmen, nämlich Artikel 12!

Moderator (Chris)
Wo verknüpfen Artikel 12 im CER-Gesetz und Artikel 12 im NIS-2-Gesetz die Zutrittskontrolle?

Klaus Wollscheid
Im luxemburgischen CER-Gesetz verlangen Art. 12 Abs. 1 Nr. 2 und 5 (entspricht EU CER Art. 13 Abs. 1 b & e) den physischen Schutz der Anlagen sowie angemessene Personal- und Zutrittsberechtigungen. Im luxemburgischen NIS-2-Gesetz fordern Art. 12 Abs. 2 Nr. 8–10 (entspricht EU NIS-2 Art. 21 Abs. 2 h, i & j) Kryptografie, strikte Zugriffskontrollen, Zutrittssicherungen und eine angemessene Authentifizierung. Im Wasserwerk bedeutet das ganz konkret: Nur freigegebene Personen gelangen in die Leitwarte, der Zutrittsserver ist digital gehärtet, entzogene Rechte werden innerhalb einer risikogerecht festgelegten Frist tatsächlich unwirksam und der Notbetrieb ist funktional nachgewiesen.

Moderator (Chris)
Wie sieht es mit der Verantwortung der Geschäftsführung und den Sanktionen aus?

Klaus Wollscheid
Die Geschäftsleitung trägt verbindliche Verantwortung für die Sicherheitsmaßnahmen! Unter NIS-2 lautet die Formel: Billigen, Ermöglichen, Überwachen und Lernen. Die Leitung muss das Zutrittskonzept billigen, Budget und Ressourcen ermöglichen, Ausfalltests überwachen und aus Abweichungen lernen. Bei entsprechenden Gesetzesverstößen sieht NIS-2 für wesentliche Einrichtungen Geldbußen von bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes vor; für wichtige Einrichtungen bis zu 7 Millionen Euro oder 1,4 %, jeweils nach den gesetzlichen Bemessungsregeln. Unter CER sieht der nationale Art. 19 Geldbußen von bis zu 250.000 Euro vor. Diese Unternehmenssanktionen bedeuten nicht automatisch eine persönliche Haftung einzelner Geschäftsleitungsmitglieder; dafür gelten gesonderte gesetzliche Voraussetzungen.

Moderator (Chris)
Welche Fristen müssen Betreiber und Hersteller beachten?

Klaus Wollscheid
Gehen wir die Zeitleiste durch: Am 10. Mai 2026 traten CER und NIS-2 in Luxemburg in Kraft. Am 10. Juli 2026 lief die Frist zur erstmaligen Selbstregistrierung unter NIS-2 ab. Seit dem 11. September 2026 gelten die ersten CRA-Meldepflichten für Hersteller bei aktiv ausgenutzten Schwachstellen. Am 11. Dezember 2027 treten die vollen Hauptpflichten des EU Cyber Resilience Acts (CRA 2024/2847) für digitale Produkte in Kraft. Für CER-benannte Einrichtungen gilt zudem: Binnen 9 Monaten nach Benennung muss die umfassende Risikoanalyse vorliegen, und nach zehn Monaten werden die einschlägigen Vorschriften des Kapitels 4 grundsätzlich anwendbar – vorbehaltlich gesetzlicher Ausnahmen!

Kapitel 5: Das Zwiebelschalenprinzip & Der Zutrittslebenszyklus

Moderator (Chris)
Kommen wir zum Kern der physischen Schutzarchitektur: dem Zwiebelschalenprinzip. Wie ist dieses Modell im Wasserwerk aufgebaut?

Klaus Wollscheid
Das Zwiebelschalenprinzip gliedert das Objekt in vier von außen nach innen geschachtelte Schutzgrenzen. Schale 1 ist das Gelände bzw. der äußere Perimeter: Zaun, Werkstor, Schranke und Besucherführung. Schale 2 ist das Gebäude bzw. der innere Perimeter: Kontrollierte Außentüren, die nur berechtigte Personen hineinlassen. Schale 3 umfasst die sensiblen Räume: Die Leitwarte, das Labor oder der Serverraum mit eigenen rollenbezogenen Zutrittsrechten. Schale 4 schützt die kritischen Komponenten direkt: Der verschlossene Steuerschrank, die SPS-Steuerung oder das Server-Rack, das nur mit gesonderter Freigabe für eine konkrete Aufgabe geöffnet werden darf. Jede entsprechend ausgelegte Schale soll unberechtigten Zugang erschweren und Zeit für eine Reaktion schaffen. EN 50600-2-5 behandelt Sicherungssysteme für Rechenzentren; unsere vier Schalen sind ein Planungsmodell für das Wasserwerk, keine allgemeine Normvorgabe.

Moderator (Chris)
Wie funktioniert dieser Durchlauf an einem konkreten Beispiel, etwa bei einem externen Wartungstechniker?

Klaus Wollscheid
Nehmen wir an, ein externer Techniker soll heute die Pumpe 3 in der Leitwarte warten. An Schale 1 (Werkstor) wird seine Identität und sein Wartungstermin geprüft. Er erhält beim Empfang seinen Ausweis. An Schale 2 (Gebäudeeingang) schaltet der Ausweis nur das zeitlich befristete Fenster für das Gebäude frei. An Schale 3 (Leitwarte) gibt der Betriebsleiter den Zutritt frei, gegebenenfalls erfolgt der Zutritt nur in Begleitung. An Schale 4 (Steuerschrank) wird die Schlüssel-oder Freigabebox für den konkreten Schrank freigeschaltet. Nach Abschluss der Wartung werden die befristeten Rechte nach dem vereinbarten Verfahren entzogen, die Schränke wieder verschlossen und die wesentlichen Schritte für eine Prüfung nachvollziehbar dokumentiert!

Moderator (Chris)
Wie steuert man diese Berechtigungen über den gesamten Lebenszyklus von Mitarbeitern und Fremdfirmen?

Klaus Wollscheid
Wir sprechen vom Zutrittslebenszyklus, der drei Phasen umfasst: 1. Eintritt: Identität prüfen, Rolle im HR-System festlegen, Karte ausgeben. 2. Änderung: Ändert sich die Aufgabe oder Abteilung, werden bisherige Rechte entsprechend dem festgelegten Prozess wirksam entzogen und nur die benötigten neuen Rechte vergeben. 3. Austritt: Beim Ausscheiden muss der Ausweis innerhalb der festgelegten Frist wirksam gesperrt werden; die tatsächliche Sperrwirkung ist zu überprüfen und zu dokumentieren. Für gesetzlich definierte sensible Funktionen kann im CER-Rahmen eine förmliche Personalüberprüfung erforderlich sein. Ein entsprechender Bescheid gilt grundsätzlich fünf Jahre; die Erneuerung ist im gesetzlichen Zeitfenster sechs bis vier Monate vor Ablauf zu beantragen!

Moderator (Chris)
Was passiert, wenn eine der Schalen ausfällt oder umgangen wird?

Klaus Wollscheid
Das ist der Härtetest! Wenn Schale 1 – zum Beispiel das Werkstor – wegen einer Störung offen steht, sollen die inneren Schalen 2, 3 und 4 unberechtigten Zutritt weiterhin wirksam begrenzen. Gleichzeitig soll eine geeignete Überwachung etwa zu lange offenstehende Leitwartentüren erkennen und eine vorher festgelegte Reaktion ermöglichen. Auch Lieferanten und Seiteneingänge sind nach passenden, klar festgelegten Zutrittsregeln einzubeziehen.

Kapitel 6: Grenzen der Mechanik, Stand der Technik & Reifegradmodell

Moderator (Chris)
Viele kleinere oder ältere Wasserwerke verlassen sich bis heute auf rein mechanische Schließanlagen. Warum reicht das unter NIS-2 und CER oft nicht mehr aus?

Klaus Wollscheid
Rein mechanische Schlüssel haben drei große Schwachstellen im Audit: Erstens: Die Nachvollziehbarkeit. Ein mechanisches Schloss erzeugt kein digitales Ereignisprotokoll. Das Schloss allein weist also nicht nach, wer die Tür wann geöffnet hat. Zweitens: Verlust und Kopien. Geht ein Generalhauptschlüssel verloren, kann er nicht per Mausklick gesperrt werden. Je nach Schließhierarchie müssen betroffene Zylinder und geeignete Ersatzmaßnahmen geprüft werden. Drittens: Zeit- und Rollensteuerung. Ein mechanischer Schlüssel gilt rund um die Uhr und kennt keine Schichtpläne oder befristete Wartungsfenster.

Moderator (Chris)
NIS-2 fordert ja Maßnahmen nach dem 'Stand der Technik'. Wie wird dieser juristische Begriff im Zutrittskontext definiert?

Klaus Wollscheid
Stand der Technik bedeutet: Schutzmaßnahmen auf dem aktuellen technischen Entwicklungsstand, die für das konkrete Risiko geeignet und praktisch wirksam sind. Der Prozess umfasst vier Schritte: 1. Risiko und Schutzbedarf ermitteln, 2. Geeignete Maßnahmen nach Normen auswählen, 3. Wirksamkeit im Betrieb testen und nachweisen, 4. Regelmäßig neu bewerten. Aufwand und Kosten fließen im Rahmen der Verhältnismäßigkeit ein, aber das erforderliche Schutzniveau der kritischen Anlage bleibt maßgeblich!

Moderator (Chris)
Ihr habt dazu ein sehr eingängiges Entwicklungsmodell mit vier Stufen erarbeitet. Kannst du uns diese vier Reifegrade erklären?

Klaus Wollscheid
Sehr gerne. Stufe 01 (Reaktiv / Mechanik): Rein mechanische Schlüssel. Vergabe wird manuell protokolliert. Bei Verlust werden die betroffenen Schlösser und Ersatzmaßnahmen anhand des Schließplans bewertet. Stufe 02 (Identifiziert / Elektronik): Einsatz von Elektronik und RFID-Medien. Individuelle Ausweise ermöglichen ereignisbezogene Protokolle und gezielte Kartensperrungen. Die Sperrzeit hängt jedoch stark von der Systemarchitektur ab. Stufe 03 (Dynamisch / Rechteverwaltung): Je nach System automatisierte Rollen- und Rechteverwaltung. Befristete Wartungsfenster, automatische Kopplung an das HR-System beim Offboarding. Stufe 04 (Proaktiv / Überwachung): Risikogerechte Überwachung ausgewählter Zutrittspunkte, gegebenenfalls automatisierte Angriffserkennung, risikogerechte Mehrfaktor-Authentifizierung (z.B. Karte + PIN an der Leitwarte) und regelmäßig getesteter Notbetrieb.

Kapitel 7: Systemaufbau, Kryptografie & Die Rolle des Cyber Resilience Acts (CRA)

Moderator (Chris)
Wenn wir ein elektronisches Zutrittssystem installieren, wird dieses System selbst zu einem attraktiven Ziel für Cyberangriffe. Wie schützt man die Zutrittsinfrastruktur?

Klaus Wollscheid
Genau deshalb gilt: Auch das Zutrittssystem braucht gehärteten Schutz! Die Kette besteht aus Ausweis, Leser, Türsteuerung (Controller) und Verwaltungssoftware. Je nach Schutzbedarf können an der Tür Manipulationskontakte und geeignete Verriegelungen erforderlich sein. Der Zutrittsserver sollte entsprechend der Risikoanalyse abgesichert werden, etwa durch Netzwerksegmentierung und angemessene Mehrfaktor-Authentifizierung für die Administration. Auch die Verbindungen zwischen den Komponenten brauchen passende Authentisierungs- und kryptografische Schutzmaßnahmen!

Moderator (Chris)
Wie sieht diese Kryptografie auf den drei Übertragungsstrecken genau aus?

Klaus Wollscheid
Wir sichern drei Abschnitte ab: Strecke 1 (Ausweis <-> Leser): Prüfung der Echtheit des Ausweises mittels verschlüsselter Challenge-Response-Verfahren (z.B. MIFARE DESFire), um das Kopieren und Replay-Angriffe wirksam zu erschweren. Strecke 2 (Leser <-> Controller): Authentifizierung der Nachrichten und Schutz vor Manipulation am Buskabel (z.B. mittels OSDP v2 mit Secure Channel). Strecke 3 (Controller <-> Server): Gegenseitige Zertifikatsprüfung und verschlüsselte Netzwerkübertragung. Ganz wichtig für Audits: Es gibt keine starre Pflicht zu AES-256 oder TLS 1.3 für jede Tür – das Verfahren muss risikogerecht gewählt und im Schlüsselmanagement-Lebenszyklus verankert sein!

Moderator (Chris)
Welche Rolle spielt hierbei der neue EU Cyber Resilience Act (CRA)?

Klaus Wollscheid
Der CRA (Verordnung EU 2024/2847) nimmt die Produkthersteller in die Pflicht. Hersteller von Lesern, Controllern und Zutrittssoftware, soweit ihre Produkte unter den CRA fallen, müssen geeignete sichere Voreinstellungen (Security by Default) vorsehen, Schwachstellen im vorgesehenen Supportzeitraum bearbeiten und Sicherheitsupdates bereitstellen. Der CRA sieht grundsätzlich mindestens fünf Jahre Sicherheitsunterstützung vor, sofern die erwartete Nutzungsdauer nicht kürzer ist; bei längerer Nutzung kann ein längerer Zeitraum erforderlich sein. Bei der Produktübergabe verbindet die Beschaffung den Hersteller und den Betreiber: Der Betreiber übernimmt die sichere Konfiguration und der Hersteller stellt die gesetzlich erforderlichen und vertraglich vereinbarten Support- und Updatewege bereit.

Kapitel 8: Detaillierte Analyse der 3 Audit-Praxisfälle

Moderator (Chris)
Jetzt kommen wir zum absolut spannendsten Teil für alle Auditoren und Praxis-Sicherheitsverantwortlichen: Den drei konkreten Praxisfällen im Wasserwerk! Lass uns Praxisfall 1 durchgehen: Ein Mitarbeiter verliert seinen Ausweis. Was passiert?

Klaus Wollscheid
Praxisfall 1 zeigt den Unterschied zwischen Online- und Offline-Türen! Der Mitarbeiter meldet den Verlust. Im zentralen System wird die Karte gesperrt. An der Online-Tür zur Leitwarte kann die Sperre bei funktionierender Verbindung zeitnah wirksam werden. Entscheidend ist, dass der Controller die Änderung übernimmt und die Tür einen gesperrten Ausweis tatsächlich abweist. Aber an der abgelegenen Offline-Tür zur Pumpstation ist die Türsteuerung nicht dauerhaft online. Hier hängt die Sperrwirkung beispielsweise davon ab, wann ein lokales Sperrdaten-Update ankommt oder eine zeitlich begrenzte Berechtigung abläuft. Für das Audit heißt das: Die maximale Sperrzeit muss im Vorfeld in der Risikoanalyse definiert sein und am realen Schloss – inklusive simuliertem Netzausfall – nachgewiesen werden!

Moderator (Chris)
Wie sieht Praxisfall 2 aus: Totaler Strom- oder Netzausfall im Wasserwerk?

Klaus Wollscheid
Praxisfall 2 betrifft den Notbetrieb! Fällt die Netzwerkverbindung aus, dürfen die Türcontroller nicht in Panik verfallen oder alle Türen unberechtigt freigeben. Sie sollen entsprechend der vereinbarten Auslegung mit lokalen Rechten und Sperrregeln sicher weiterarbeiten. Bei einem Stromausfall ist die erforderliche Energieautonomie oder ein geeignetes Ersatzverfahren einzuplanen. Besonders wichtig: Sichere Flucht, Schutz gegen unberechtigten Zutritt und Notöffnung müssen für jede Tür nach den einschlägigen Bau- und Brandschutzanforderungen abgestimmt und getestet werden. Berechtigtes Betriebspersonal muss jedoch über definierte Notzugänge an die Anlage gelangen können. Kehrt der Strom zurück, müssen sich Ereignisse und Zeitstempel kontrolliert abgleichen.

Moderator (Chris)
Und Praxisfall 3 kombiniert diese Szenarien zu einer gemeinsamen Ausfallübung. Wie läuft dieser Stresstest zeitlich ab?

Klaus Wollscheid
Wir simulieren in der Audit-Übung eine dreistufige Abfolge: Um 08:10 Uhr fällt das Netz aus. Ein Techniker muss die Leitwarte erreichen. Ergebnis: der Notzugang wird geprüft und die vorgesehenen Fluchtfunktionen werden nachgewiesen. Um 08:20 Uhr meldet ein Mitarbeiter einen Ausweisverlust. An der offline betriebenen Pumpstation ist das Recht noch auf der Karte gespeichert. Ergebnis: Das Restrisiko wird durch vordefinierte organisatorische Ersatzmaßnahmen wirksam begrenzt. Um 08:35 Uhr kehrt das System zurück. Ergebnis: Die lokal gespeicherten Ereignisse werden im Rahmen der Systemmöglichkeiten kontrolliert abgeglichen. Bei Hinweisen auf Produktfehler wird der Hersteller eingebunden; ob eine gesetzliche CRA-Meldung erforderlich ist, prüft der jeweils verpflichtete Akteur. Die Übung liefert damit wichtige Wirksamkeitsnachweise für die operative Resilienz!

Kapitel 9: Gemischte Meldepflichten (24h / 72h / 1M) & Behördenwege

Moderator (Chris)
Wenn ein schwerwiegender Vorfall auftritt – zum Beispiel eine Sabotage an der Zutrittskontrolle, die den Wasserwerksbetrieb stört –, greifen strikte gesetzliche Meldepflichten. Wie unterscheiden sich die Meldewege unter NIS-2, CER und CRA?

Klaus Wollscheid
Das ist eine der komplexesten Fragen in der Praxis, weil ein einziger Vorfall zwei verschiedene gesetzliche Meldekanäle gleichzeitig auslösen kann! Sehen wir uns die Fristen genau an: Unter NIS-2 (bei erheblichen Sicherheitsvorfällen): 1. Binnen 24 Stunden ab Kenntnisnahme: Abgabe einer Frühwarnung. 2. Binnen 72 Stunden ab Kenntnisnahme: Abgabe der eigentlichen Vorfallmeldung. 3. Binnen 1 Monats (nach der Vorfallmeldung): Abgabe des verbindlichen Abschlussberichts. Unter CER (bei erheblichen Störungen der Resilienz): 1. Binnen 24 Stunden ab Kenntnisnahme: Erste Meldung der Störung. 2. Binnen 1 Monats: Abgabe eines detaillierten Abschlussberichts. Es gibt bei CER keinen allgemeinen 72-Stunden-Zwischenschritt! Zuständig ist bei CER das Haut-Commissariat à la Protection Nationale (HCPN) und bei NIS-2 die ILR bzw. für den Finanzsektor die CSSF. CRA-Herstellermeldungen bei Schwachstellen laufen separat über die ENISA bzw. nationale CSIRTs.

Kapitel 10: Der 90-Tage-Umsetzungsplan & Die 4 Management-Entscheidungen

Moderator (Chris)
Wie verankert man diese vielen Anforderungen im laufenden Informationssicherheitsmanagementsystem (ISMS)?

Klaus Wollscheid
Wir empfehlen einen geschlossenen ISMS-Kreislauf aus vier Schritten: Risiko identifizieren -> Maßnahme festlegen -> Nachweis im Betrieb erbringen -> Kontinuierlich verbessern. Im Audit zählt der Nachweisbestand: Zonenplan, Rechteprüfung, Konfigurationsnachweise, Wartungsprotokolle, Vorfallprotokolle und Übungsprotokolle der Notfalltests. Ein hoher dokumentierter Reifegrad unterstützt die Aufsicht enorm – allerdings gibt es keine automatische Auditbefreiung!

Moderator (Chris)
Für Betreiber, die jetzt starten müssen: Wie sieht ein pragmatischer 90-Tage-Umsetzungsplan aus?

Klaus Wollscheid
Wir gliedern die ersten 90 Tage in drei klare Phasen von jeweils 30 Tagen: Tag 01 bis 30 (Einordnen und erfassen): Betroffenheit und Registrierung klären, Zonen, Anlagen und Dienstleister erfassen, Schlüssel- und Berechtigungsverzeichnisse konsolidieren. Tag 31 bis 60 (Lücken schließen): Risikoanalyse durchführen, Prioritäten setzen, geeignete Zutrittstechnik und Sperrprozesse auswählen, Notzugänge und CRA-Herstellerzusagen einholen. Tag 61 bis 90 (Prüfen und verankern): Ausfall- und Wiederanlauftests an den echten Türen durchführen, Personal schulen, Nachweisbestand aufbauen und das System im ISMS verankern.

Moderator (Chris)
Zum Abschluss unseres Hauptteils: Welches sind die vier zentralen Management-Entscheidungen, die die Geschäftsführung jetzt treffen muss?

Klaus Wollscheid
Es sind exakt vier Entscheidungen: 1. Schutzbedarf bestätigen: Trinkwasserversorgung, Zonen und maximal tragbare Ausfallzeiten verbindlich festlegen. 2. Verantwortung verbinden: Geschäftsleitung, Betrieb, IT, HR und externe Lieferanten an einen Tisch bringen. 3. Zutrittskonzept freigeben: Notwendige Budgets für Rechteentzug, Notbetrieb, Kryptografie und Herstellersupport bereitstellen. 4. Wirksamkeit demonstrieren: Einen gemeinsamen praktischen Ausfalltest terminieren und die Nachweise im Audit bewerten. CER und NIS-2 führen das Programm – und der CRA stärkt die dafür eingesetzten Produkte!

Kapitel 11: Reserve-Exkurse, DORA-Sonderregeln & Technische Vertiefung

Moderator (Chris)
Klaus, wir haben in der Präsentation noch 12 Reserve-Folien mit extrem wertvollem Spezialwissen. Lass uns die wichtigsten Punkte für Experten durchgehen. Wie verhält sich NIS-2 zum Finanzsektor und DORA?

Klaus Wollscheid
In der Reserve-Folie R4 ist das klar geregelt: Für erfasste Finanzunternehmen können DORA-Regeln (Digital Operational Resilience Act) als speziellere Vorgaben einschlägig sein; welche NIS-2-Pflichten dadurch überlagert werden, ist je Einrichtung und Verpflichtung zu prüfen. Die CSSF ist für ihr gesetzlich zugewiesene Finanzbereiche zuständig; bei CER und NIS-2 gelten jeweils die einschlägigen nationalen Zuständigkeiten, unter anderem HCPN und ILR.

Moderator (Chris)
Wie unterscheidet der Cyber Resilience Act (CRA) die Produktklassen bei Zutrittssystemen?

Klaus Wollscheid
Reserve R6 zeigt die Einstufung: Klasse 01 (Grundkategorie): Allgemeine digitale Produkte. Klasse 02 (Wichtige Produkte nach Anhang III, Klasse I & II): Hierunter fallen Identity & Privileged Access Management (IAM/PAM) sowie bestimmte Smart-Home- und Sicherheitsschlösser. Klasse 03 (Kritische Produkte nach Anhang IV): Spezifische hochkritische Komponenten. Wichtig: Ein Produkt wird nicht allein dadurch zum kritischen CRA-Produkt, weil es in einer kritischen Infrastruktur eingesetzt wird – maßgeblich ist die Kernfunktion des Produkts!

Moderator (Chris)
Welche Abnahmekriterien empfiehlt EIWTC für die technische Abnahme von Zutrittssystemen?

Klaus Wollscheid
Reserve R7 gibt dafür eine Fünf-Punkte-Checkliste an die Hand: 1. Identität & Berechtigung: Eindeutige Geräteidentifikation und wirksamer Sperrtest. 2. Geschützte Kommunikation: Authentifizierte und verschlüsselte Bus- und Netzverbindungen. 3. Firmware & Updates: Signierte Firmware und erfolgreicher Negativtest mit unautorisierten Updates. 4. Schlüssel & Zertifikate: Geregelter Lebenszyklus für Erneuerung, Widerruf und Notfallersatz. 5. Verfügbarkeit & Support: Nachgewiesener Notbetrieb und schriftliche Herstellersupportzusage für den nach CRA und erwarteter Nutzung einschlägigen Zeitraum.

Moderator (Chris)
Welche Rolle spielt die zivile und militärische Gesamtverteidigung im Rahmen des Strategischen Resilienzrahmens (SNR)?

Klaus Wollscheid
Reserve R9 betont: Nationale Resilienz braucht vernetzte Verantwortung! Der Strategische Resilienzrahmen (SNR) sieht Resilienzbeauftragte und Kontinuitätspläne in allen öffentlichen Institutionen vor. Ein Wasserwerk kann als wesentlicher Versorgungsdienst für die nationale Krisenvorsorge und gegebenenfalls für weitere staatliche Aufgaben bedeutsam sein. Krisenkontakte und Wiederanlaufpläne sind daher mit den jeweils zuständigen Stellen und nach den tatsächlichen Aufgaben abzustimmen.

Moderator (Chris)
Klaus, das war eine fantastische, absolut umfassende und detaillierte Reise durch alle Facetten des Cyber- und Sabotageschutzes für kritische Infrastrukturen! Vielen herzlichen Dank für dieses fundierte Expertenwissen und die klaren Praxistipps.

Klaus Wollscheid
Sehr gerne, Chris! Vielen Dank und allen Betreibern viel Erfolg bei der Umsetzung!