EIWTC · CER / NIS-2 / CRA

Podcast transcript

Cyber- und Sabotageschutz im Wasserwerk

English – translation of the edited German text

Translated from the edited German PDF-based text; not independently checked word for word against the audio. Professional information, not legal advice.

Contents

01 · Welcome, key issues and the framework
02 · Model assumptions and the all-hazards approach
03 · National strategy: CER, NIS 2 and CRA working together
04 · Laws of 5 May 2026, legal provisions and responsibility
05 · The onion-layer principle and the access-rights lifecycle
06 · Limits of mechanical locks, state of the art and maturity levels
07 · System architecture, cryptography and the role of the CRA
08 · In-depth analysis of three practical audit cases
09 · Incident reporting and authorities: 24 hours, 72 hours, one month
10 · The 90-day implementation plan and four management decisions
11 · Further detail: DORA, special rules and technical topics

Chapter 1: Welcome, key issues and the framework

Host (Chris)
A very warm welcome to today's special episode of our podcast on critical infrastructure and resilience! Today we are discussing a topic that may seem very physical and ordinary at first glance, but on closer inspection forms the direct link between digital cybersecurity, physical protection against sabotage and government regulation: access control in critical infrastructure, using a water treatment plant as a practical example.

Klaus Wollscheid
Hello Chris, thank you very much for inviting me! I'm delighted to be here. As CEO of EIWTC SARL and CSO of BEWENG S.A., I deal with precisely this interface every day. Whether at a waterworks, a hospital or a data centre, a door opened without authorisation can, in the worst case, bring an entire essential service to a standstill.

Host (Chris)
Klaus, we have an exceptionally comprehensive programme ahead of us today. Following the new Luxembourg laws of 5 May 2026 transposing the European CER and NIS 2 directives into national law, and the EU Cyber Resilience Act (CRA), operators face very specific legal and technical obligations. We want to look at every detail: from the onion-layer principle and the access-rights lifecycle to practical audit cases and the special provisions covered in the reserve slides.

Klaus Wollscheid
Absolutely! Most importantly, we will not treat this as an abstract theoretical exercise. Instead, we will use a very tangible model: our fictional, yet highly realistic, critical waterworks. After all, at a waterworks nothing less than the uninterrupted supply of drinking water to the population is at stake.

Chapter 2: Model assumptions and the all-hazards approach

Host (Chris)
Let's start with the waterworks itself. Which sites and areas does our example cover exactly?

Klaus Wollscheid
For our model, we assume that the waterworks has been formally designated as a critical entity. The facility typically comprises four core areas. First, the outer works gate, where visitors are received and escorted. Second, the operations building, where technicians receive access rights tied to their assignments. Third, the central control room, where operating personnel maintain the supply around the clock and maintenance takes place only after formal approval. And fourth, the heart of the operation: the actual control equipment and sensors. We also assume a remote, decentralised pumping station with an intermittently disrupted network connection.

Host (Chris)
That sounds extremely practical! Why is access control such a crucial element of this arrangement? What can go wrong?

Klaus Wollscheid
In modern security management we speak of the all-hazards approach: assessing physical and digital risks together. Consider the chain of events. A lost or stolen employee badge remains valid in the system. An unauthorised person uses it to pass through a door. They reach a control cabinet or an exposed network socket in the operations building. There, they tamper with equipment or introduce malware, resulting in a sudden control-system outage and disruption to the drinking-water supply! An inadequately protected physical door can therefore lead directly to an IT failure and interruption of the service.

Host (Chris)
And the all-hazards approach goes beyond classic sabotage, doesn't it?

Klaus Wollscheid
Exactly. Alongside cyberattacks and deliberate sabotage, we always assess natural hazards such as flooding, power outages, staff absences caused by pandemics and supply shortages. Everything has to be assessed together: points of entry, dependencies, consequences and concrete recovery plans.

Chapter 3: National strategy: CER, NIS 2 and CRA working together

Host (Chris)
This leads us straight to the legal and strategic context. Luxembourg has adopted an overarching national resilience strategy with eight pillars. How do these laws fit into it?

Klaus Wollscheid
Luxembourg structures its resilience around eight pillars. Pillar 1: democracy, the rule of law and government. Pillar 2: a resilient society. Pillar 3 is the CER pillar, covering essential services and critical infrastructure. Pillar 4: a resilient economy. Pillar 5: strategic and logistical resources. Pillar 6 is the NIS 2 pillar, covering cyber resilience. Pillar 7: civil defence. And pillar 8: protection and defence of national territory. You can immediately see the distinction: CER safeguards physical and operational service continuity, NIS 2 protects digital networks and systems, and the Cyber Resilience Act (CRA) strengthens the security of the digital products used.

Host (Chris)
Which sectors fall within these regulatory frameworks in Luxembourg?

Klaus Wollscheid
CER covers twelve sectors: energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, space, food and waste management. NIS 2 covers many of these areas and includes further sectors, such as: ICT services (B2B), postal and courier services, chemicals, certain manufacturing industries, digital providers and research. This is a simplified sector overview; whether an organisation is covered depends on the entity type, size criteria and applicable legal exceptions.

Host (Chris)
How are entities in those sectors categorised? We hear the terms 'critical', 'essential' and 'important'.

Klaus Wollscheid
That distinction is absolutely crucial for audits! Under CER, the classification is 'critical entity', resulting from a formal state designation based on societal importance. NIS 2 distinguishes 'essential entities' — generally large organisations under Annex I or covered by special provisions — and 'important entities', such as medium-sized Annex I organisations and medium-sized or large Annex II organisations. For our waterworks, an important rule applies: once it has been formally designated as critical under CER, it also qualifies as an 'essential entity' under NIS 2, regardless of its workforce or turnover!

Chapter 4: Laws of 5 May 2026, legal provisions and responsibility

Host (Chris)
Let's turn to the specific legal provisions in Luxembourg. Which date should security managers circle in red on their calendars?

Klaus Wollscheid
5 May 2026! That was the date of publication of the two national laws in Mémorial A: issue 225 covers NIS 2 in Luxembourg, and issue 226 covers CER. Both laws came into force on 10 May 2026. And interestingly, both place the security measures under the same article number: Article 12!

Host (Chris)
Where do Article 12 of the CER law and Article 12 of the NIS 2 law connect with access control?

Klaus Wollscheid
In the Luxembourg CER law, Article 12(1), points 2 and 5 — corresponding to Article 13(1)(b) and (e) of the EU CER directive — requires physical protection of installations and appropriate personnel security and access rights. In the Luxembourg NIS 2 law, Article 12(2), points 8 to 10 — corresponding to Article 21(2)(h), (i) and (j) of the EU NIS 2 directive — addresses cryptography, strict access control, physical access safeguards and appropriate authentication. At our waterworks this means, in practical terms, that only authorised people enter the control room, the access-control server is digitally hardened, revoked rights become ineffective within a risk-based, specified revocation period and emergency operation has been functionally demonstrated.

Host (Chris)
What about management's responsibilities and the possible sanctions?

Klaus Wollscheid
Senior management has clearly defined duties in relation to security! Under NIS 2, the formula is: approve, enable, oversee and learn. Management must approve the access-control concept, make budgets and resources available, oversee outage tests and learn from discrepancies. Where the statutory conditions for a breach are met, NIS 2 provides for fines on entities of up to EUR 10 million or 2% of worldwide annual turnover for essential entities; for important entities, up to EUR 7 million or 1.4%. Under CER, national Article 19 provides for fines of up to EUR 250,000. These fines on organisations do not automatically establish personal liability for an individual director; separate legal conditions apply.

Host (Chris)
Which deadlines must operators and manufacturers observe?

Klaus Wollscheid
Let's walk through the timeline. CER and NIS 2 came into force in Luxembourg on 10 May 2026. The deadline for initial NIS 2 self-registration expired on 10 July 2026. Since 11 September 2026, the first CRA reporting obligations have applied to manufacturers in relation to actively exploited vulnerabilities. On 11 December 2027, the main requirements of the EU Cyber Resilience Act (Regulation 2024/2847) take effect for digital products. And for entities designated under CER, a comprehensive risk assessment must be available within nine months of designation, with the relevant Chapter 4 provisions generally becoming applicable after ten months, subject to statutory exceptions!

Chapter 5: The onion-layer principle and the access-rights lifecycle

Host (Chris)
Let's turn to the core of physical security architecture: the onion-layer principle. How does this model work at the waterworks?

Klaus Wollscheid
The onion-layer principle divides the site into four nested protective boundaries, from outside to inside. Layer 1 is the site or outer perimeter: fence, works gate, barrier and visitor management. Layer 2 is the building or inner perimeter: controlled external doors that allow only authorised people inside. Layer 3 covers sensitive rooms: the control room, laboratory or server room, each with its own role-based access rights. Layer 4 protects the critical components directly: a locked control cabinet, programmable logic controller or server rack that may only be opened with separate approval for a specific task. Each appropriately designed layer aims to make unauthorised access harder and allow time for a response. EN 50600-2-5 addresses security systems for data centres; our four layers are a planning model for the waterworks, not a universally mandated standard.

Host (Chris)
How does this work for a specific person, such as an external maintenance technician?

Klaus Wollscheid
Suppose an external technician is scheduled to service pump 3 in the control room today. At layer 1, the works gate, their identity and appointment are checked, and they receive a badge at reception. At layer 2, the building entrance, the badge grants access only during a limited time window. At layer 3, the control room, the operations manager authorises entry, perhaps only with an escort. At layer 4, the control cabinet, the key or release box for that specific cabinet is unlocked. Once maintenance is finished, temporary rights are revoked under the agreed procedure, the cabinets are locked again and the key steps are documented so they can be checked in an audit!

Host (Chris)
How can these rights be managed throughout the lifecycle of employees and contractors?

Klaus Wollscheid
We call this the access-rights lifecycle, with three stages. First, joining: verify identity, assign a role in the HR system and issue a card. Second, moving: when duties or departments change, previous rights must be effectively removed under the defined procedure, with only the required new rights granted. Third, leaving: when someone departs, the badge must become unusable within the defined period, with the actual effect verified and documented. For certain legally defined sensitive functions, a formal personnel background check may be required under CER. A corresponding decision is generally valid for five years, and renewal must be requested within the statutory period of six to four months before expiry!

Host (Chris)
What happens if one of the layers fails or is bypassed?

Klaus Wollscheid
That is the real stress test! If layer 1 — say, the works gate — is left open because of a fault, inner layers 2, 3 and 4 should continue to limit unauthorised access effectively. At the same time, exceptional situations, such as a control-room door standing open too long, should be identified by suitable monitoring and trigger a predefined response. Suppliers and side entrances must also be included in appropriate, clearly documented access rules.

Chapter 6: Limits of mechanical locks, state of the art and maturity levels

Host (Chris)
Many smaller or older waterworks still rely on purely mechanical locking systems. Why are these often no longer sufficient under NIS 2 and CER?

Klaus Wollscheid
Purely mechanical keys have three major weaknesses in an audit. First, traceability: a mechanical lock does not generate a digital event log, so the lock itself cannot establish who opened the door and when. Second, loss and copying: if a master key is lost, it cannot be blocked with a mouse click, and the affected cylinders and appropriate alternatives must be assessed against the key hierarchy. Third, time and role control: a mechanical key works around the clock and does not recognise shift schedules or temporary maintenance windows.

Host (Chris)
NIS 2 calls for measures reflecting the 'state of the art'. How is that legal term understood in the context of access control?

Klaus Wollscheid
State of the art means protective measures that reflect current technological development, are suitable for the specific risk and are effective in practice. The process has four steps: first, establish the risk and protection needs; second, choose suitable measures based on standards; third, test and demonstrate effectiveness in operation; and fourth, reassess them regularly. Effort and costs are part of the proportionality assessment, but the required protection level of the critical facility remains decisive!

Host (Chris)
You have developed a very memorable model with four stages. Can you explain these levels of maturity?

Klaus Wollscheid
Of course. Stage 01, reactive/mechanical: purely mechanical keys; issuance is recorded manually, and a lost key may require the lock to be changed. Stage 02, identified/electronic: electronics and RFID credentials; individual badges allow event-based logs and targeted card blocking, although blocking time depends heavily on the system architecture. Stage 03, dynamic/rights management: role and rights management automated where supported by the system, temporary maintenance windows and automatic links to the HR system during offboarding. Stage 04, proactive/monitoring: risk-based monitoring of selected access points, with automated attack detection where appropriate, risk-appropriate multi-factor authentication — for example, card plus PIN at the control room — and regularly tested emergency operation.

Chapter 7: System architecture, cryptography and the role of the CRA

Host (Chris)
When we install an electronic access-control system, the system itself becomes an attractive target for cyberattacks. How can we protect the access-control infrastructure?

Klaus Wollscheid
Exactly — the access-control system itself must also be hardened! The chain comprises the badge, reader, door controller and management software. Depending on the protection requirements, the door may need tamper contacts and suitable locking hardware. The access-control server should be secured based on risk assessment, for example through network segmentation and appropriate multi-factor authentication for administrators. Connections between components also need appropriate authentication and cryptographic protection!

Host (Chris)
What does that cryptography look like across the three transmission links?

Klaus Wollscheid
We secure three sections. Link 1, badge to reader: verify the badge's authenticity with encrypted challenge-response methods — for example, MIFARE DESFire — to make copying and replay attacks substantially harder. Link 2, reader to controller: authenticate messages and protect against tampering on the bus cable, for example with OSDP v2 Secure Channel. Link 3, controller to server: mutual certificate checking and encrypted network transmission. And something particularly important for audits: there is no rigid requirement to use AES-256 or TLS 1.3 at every door. The method must be selected according to risk and embedded in the cryptographic key-management lifecycle!

Host (Chris)
What role does the new EU Cyber Resilience Act (CRA) play here?

Klaus Wollscheid
The CRA, Regulation (EU) 2024/2847, places obligations on product manufacturers. For products within the CRA’s scope, manufacturers of readers, controllers and access-management software must provide suitable secure defaults, address vulnerabilities during the applicable support period and provide security updates. The CRA generally requires at least five years of support unless the expected product lifetime is shorter; longer expected use may require a longer support period. At product handover, procurement links the manufacturer and the operator: the operator takes responsibility for secure configuration, while the manufacturer provides the legally required and contractually agreed support and update channels.

Chapter 8: In-depth analysis of three practical audit cases

Host (Chris)
Now we come to the most exciting part for auditors and security practitioners: the three practical audit cases at the waterworks! Let's start with case 1: an employee loses their badge. What happens?

Klaus Wollscheid
Case 1 illustrates the difference between online and offline doors! The employee reports the loss and the badge is blocked in the central system. At the online door leading to the control room, revocation can take effect promptly if connectivity is working. What matters is that the controller receives the change and the door actually rejects the blocked badge. But the remote offline door at the pumping station is not permanently connected. There, the effective time can depend, for example, on delivery of local revocation data or expiry of a time-limited credential. For the audit, that means the maximum revocation time must be specified in the risk assessment beforehand and demonstrated at the actual lock, including during a simulated network outage!

Host (Chris)
What about case 2: a complete power or network outage at the waterworks?

Klaus Wollscheid
Case 2 concerns emergency operation! If the network connection fails, door controllers must not panic or unlock all doors for unauthorised access. They should continue operating safely under the design requirements, using locally stored rights and revocation rules. If power fails, the required autonomy or a suitable fallback procedure must be planned. Crucially, safe escape, protection against unauthorised access and emergency opening must be coordinated and tested for each door against applicable building and fire-safety requirements. Authorised operating staff must still be able to reach the plant through defined emergency entrances. When power returns, events and timestamps must be reconciled in a controlled manner.

Host (Chris)
And case 3 combines these scenarios in a joint outage exercise. What is the timeline of that stress test?

Klaus Wollscheid
In the audit exercise we simulate three stages. At 08:10 the network goes down and a technician needs to reach the control room: emergency access is tested and the required escape functions are demonstrated. At 08:20 an employee reports a lost badge; the access right remains stored on the credential at the offline pumping station: predefined organisational fallback measures effectively limit the residual risk. At 08:35 the system comes back online: locally stored events are reconciled in a controlled manner within the system’s capabilities. If a possible product defect is identified, the manufacturer is involved; whether CRA reporting is legally required is assessed separately by the responsible party. This exercise provides useful evidence of operational resilience!

Chapter 9: Incident reporting and authorities: 24 hours, 72 hours, one month

Host (Chris)
When a serious incident occurs — for example sabotage of access control that disrupts the waterworks — strict statutory reporting duties may arise. How do the reporting routes under NIS 2, CER and CRA differ?

Klaus Wollscheid

This is one of the most complex practical questions, because a single incident can trigger two separate statutory reporting channels at the same time! Let's look at the deadlines. Under NIS 2, for significant security incidents: first, an early warning within 24 hours of becoming aware; second, the incident notification within 72 hours; third, a mandatory final report one month after that notification. Under CER, for serious resilience disruptions: first, an initial report within 24 hours of becoming aware; second, a detailed final report within one month. CER has no general 72-hour intermediate step! For CER, the responsible authority is the Haut-Commissariat à la Protection Nationale (HCPN); for NIS 2 it is the ILR, or the CSSF in the financial sector. Manufacturers' CRA vulnerability reports follow separate channels involving ENISA and national CSIRTs.

Chapter 10: The 90-day implementation plan and four management decisions

Host (Chris)

How can all these requirements be embedded in the ongoing information security management system, or ISMS?

Klaus Wollscheid

We recommend a closed ISMS cycle in four steps: identify the risk, define a measure, demonstrate evidence in operation and continuously improve. In an audit, the evidence base matters: zoning plans, access-rights reviews, configuration records, maintenance logs, incident reports and emergency-exercise records. A high documented maturity level greatly supports supervisory review, but it does not grant an automatic exemption from audits!

Host (Chris)

For operators who need to start now, what would a pragmatic 90-day implementation plan look like?

Klaus Wollscheid

We divide the first 90 days into three clear 30-day phases. Days 01 to 30, classify and inventory: establish applicability and registration, record zones, equipment and service providers, and consolidate key and access-rights inventories. Days 31 to 60, close gaps: conduct the risk assessment, set priorities, choose suitable access-control technology and revocation processes, establish emergency access, and obtain CRA-related manufacturer assurances. Days 61 to 90, test and embed: carry out outage and recovery tests at real doors, train staff, build the evidence base and embed the system in the ISMS.

Host (Chris)

To conclude our main section, what four key management decisions should senior management take now?

Klaus Wollscheid

There are exactly four decisions. First, confirm protection needs: establish binding requirements for the drinking-water supply, zones and maximum tolerable outage durations. Second, connect responsibilities: bring senior management, operations, IT, HR and external suppliers together. Third, approve the access-control concept: allocate the necessary budgets for revocation, emergency operation, cryptography and manufacturer support. Fourth, demonstrate effectiveness: schedule a joint practical outage test and assess the evidence in an audit. CER and NIS 2 drive the programme, while the CRA strengthens the products used to implement it!

Chapter 11: Further detail: DORA, special rules and technical topics

Host (Chris)

Klaus, our presentation also has twelve reserve slides full of valuable specialist knowledge. Let's explore the main points for experts. How does NIS 2 relate to the financial sector and DORA?

Klaus Wollscheid
Reserve slide R4 explains this clearly. For financial entities within its scope, DORA may apply as a more specific regime; any overlap with NIS 2 must be assessed obligation by obligation. The CSSF supervises the financial areas assigned to it by law. CER and NIS 2 responsibilities depend on the relevant entity and regime, including the roles of the HCPN and ILR.

Host (Chris)
How does the Cyber Resilience Act classify product categories for access-control systems?

Klaus Wollscheid
Reserve slide R6 shows three groupings. Category 01, the basic category: general digital products. Category 02, important products under Annex III, Classes I and II: this includes identity and privileged access management (IAM/PAM) and certain smart-home and security locks. Category 03, critical products under Annex IV: specific highly critical components. Importantly, a product does not become a critical CRA product simply because it is installed in critical infrastructure — its core function determines its classification!

Host (Chris)
What acceptance criteria does EIWTC recommend when commissioning access-control systems?

Klaus Wollscheid
Reserve slide R7 provides a five-point checklist. First, identity and authorisation: unambiguous device identification and a successful revocation test. Second, protected communication: authenticated and encrypted bus and network connections. Third, firmware and updates: signed firmware and a successful negative test with unauthorised updates. Fourth, keys and certificates: managed processes for renewal, revocation and emergency replacement. Fifth, availability and support: demonstrated emergency operation and a written manufacturer support commitment for the period applicable under the CRA and expected product use.

Host (Chris)
What role do civil and military national defence play within the strategic national resilience framework, the SNR?

Klaus Wollscheid
Reserve slide R9 highlights that national resilience requires connected responsibilities! The strategic national resilience framework calls for resilience officers and continuity plans in all public institutions. A waterworks may be important for national crisis preparedness and, depending on its actual functions, for certain public continuity responsibilities. Crisis contacts and recovery plans should therefore be coordinated with the competent authorities in line with the duties actually assigned.

Host (Chris)
Klaus, that was a fantastic, truly comprehensive and detailed journey through every aspect of cyber and sabotage protection for critical infrastructure! Thank you so much for your expert insights and practical advice.

Klaus Wollscheid
My pleasure, Chris! Thank you, and I wish every operator the very best with implementation!