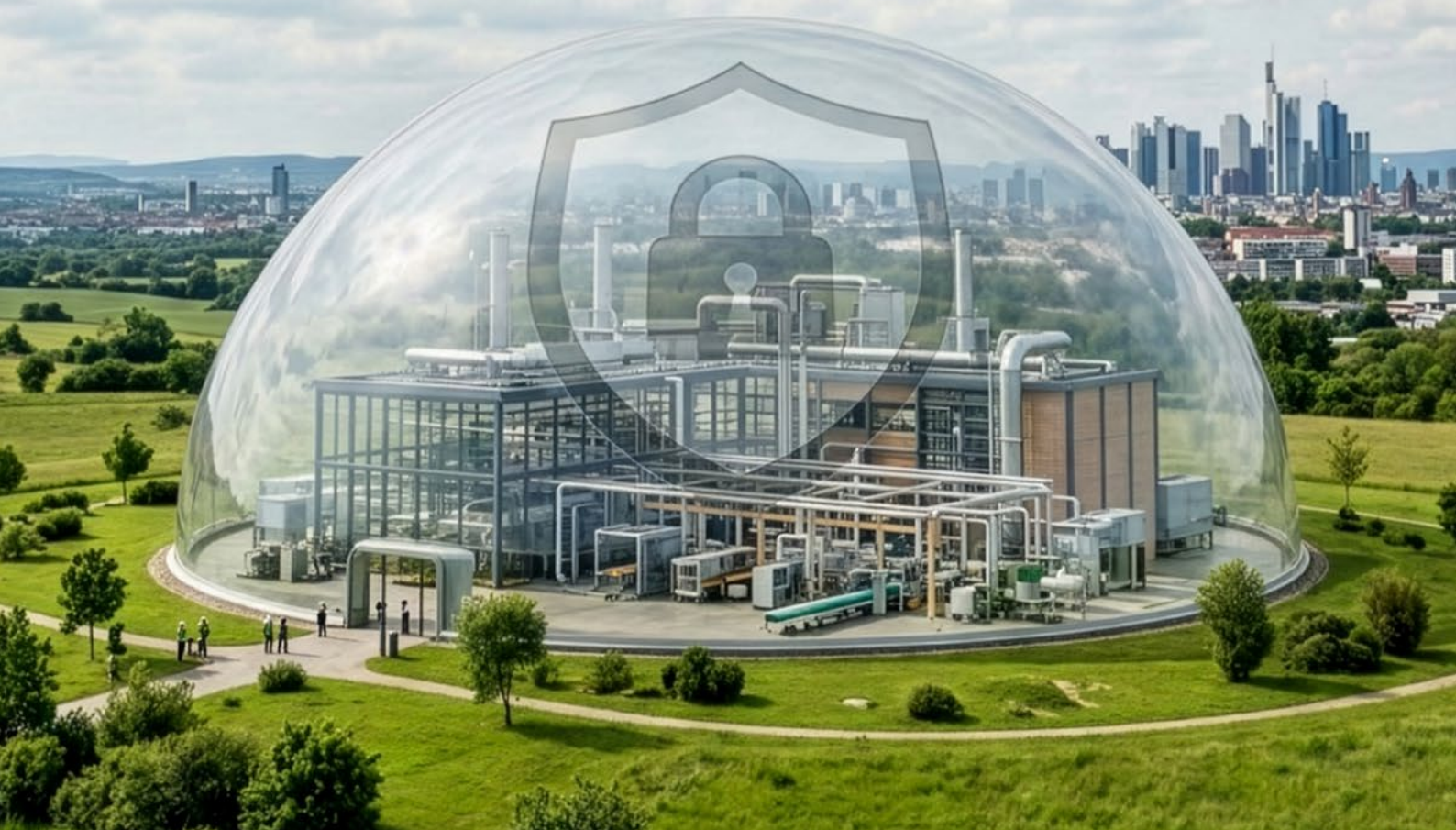
EVVA
access to security

Bílá kniha

První ochranná bariéra
Kontrola přístupu ke kritickým infrastrukturám

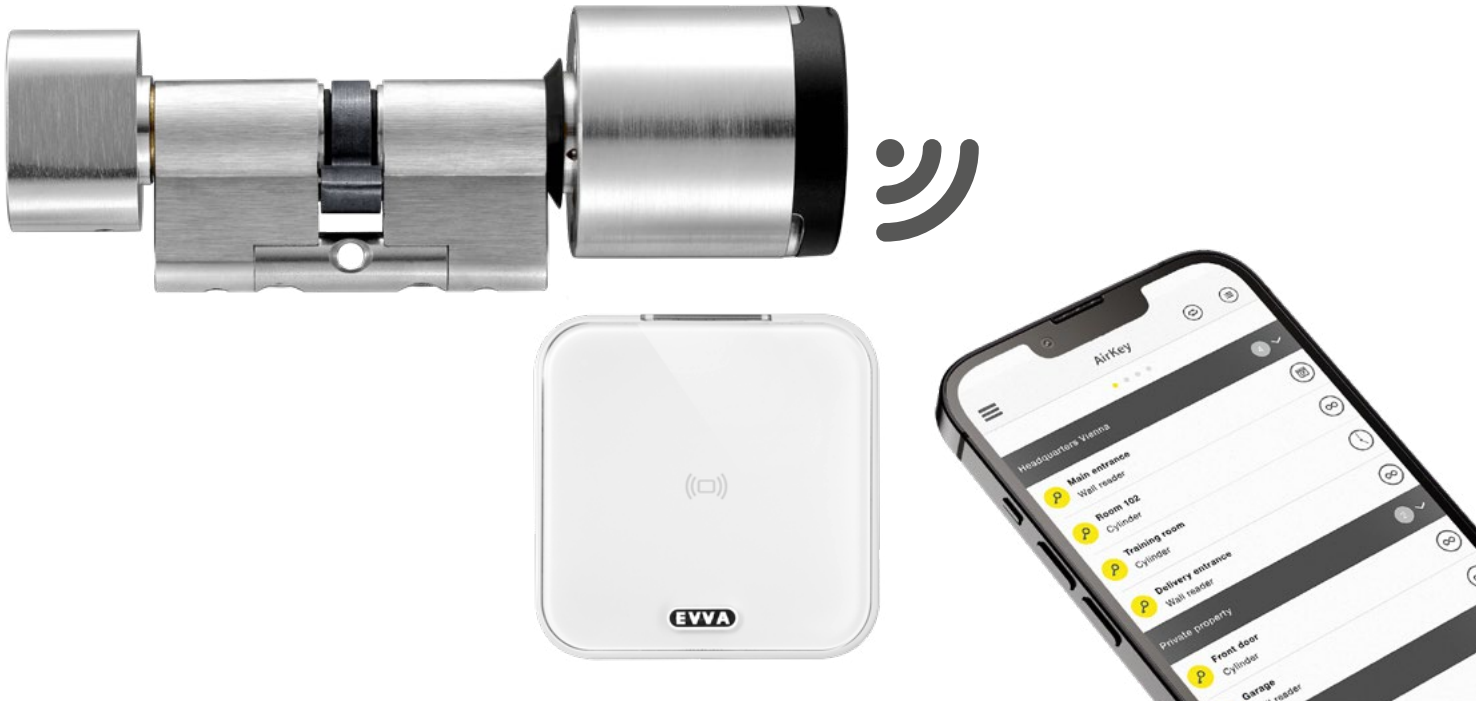


První ochranná bariéra Kontrola přístupu ke kritickým infrastrukturám

Jak moderní systémy kontroly přístupu přispívají ke splnění požadavků směrnic NIS2 a CER – a jak trvale zvyšují fyzickou bezpečnost.

Kontrola přístupu jako klíčová součást pro dodržování požadavků směrnic NIS2 a CER

Svět i my jsme se – zejména v posledních několika letech – změnili. Geopolitické změny, jako jsou války, politická nestabilita, klimatické změny a nové technologie, ovlivňují náš každodenní život a vyžadují vyšší odolnost zařízení nezbytných pro život, zejména posílení fyzické ochrany.
Evropská unie prostřednictvím evropské směrnice NIS2 (2022/2555) a doplňující směrnice CER (2022/2557) výrazně zvyšuje bezpečnostní požadavky kladené na provozovatele kritických a důležitých zařízení. Cílem obou předpisů je především posílit odolnost vůči digitálním a fyzickým hrozbám – do popředí moderních bezpečnostních architektur se tak dostává i kontrola přístupu. V této bílé knize se chceme věnovat především tématu „Fyzická ochranná opatření pro kritická zařízení".



Regulační rámec: NIS2 a CER

Vysvětlení pojmů

NIS2 a CER jsou směrnice EU, které je třeba transponovat do vnitrostátních právních předpisů; přehled příslušných právních označení na evropských trzích najdete na straně 15 této bílé knihy.

NIS2

Kyberbezpečnost pro kritická a důležitá odvětví

- EU (2022/2555)
  Cíl: Zvýšení úrovně kybernetické bezpečnosti prostřednictvím minimálních standardů platných v celé EU. Ukládá podnikům a organizacím povinnost systematicky zlepšovat svou IT a kybernetickou bezpečnost a hlásit incidenty.
- **Vztahuje se na:**
  - „Zásadní" subjekty: mezi ně patří podniky s vysokou kritičností, jejichž výpadek by měl značné dopady na společnost, ekonomiku nebo veřejnou bezpečnost; patří sem energetika, doprava, bankovnictví, zdravotnictví, vodárenství, telekomunikace/IT
  - „Důležité" sektory: mezi ně patří podniky s jinými kritickými dopady, jako jsou pošta, odpadové hospodářství, chemický průmysl, potravinářství, výroba zboží (od 50 zaměstnanců a obratu 10 mil. EUR)
- Mezi **požadavky** kladené na podniky, na které se vztahuje směrnice NIS-2, patří mimo jiné:
  - Řízení kybernetické bezpečnosti (analýzy rizik, bezpečnostní koncepce, reakce na incidenty, zajištění kontinuity činnosti)
  - Povinnost hlásit bezpečnostní incidenty
  - Odpovědnost vedení podniku
  - Přísný dohled a sankce

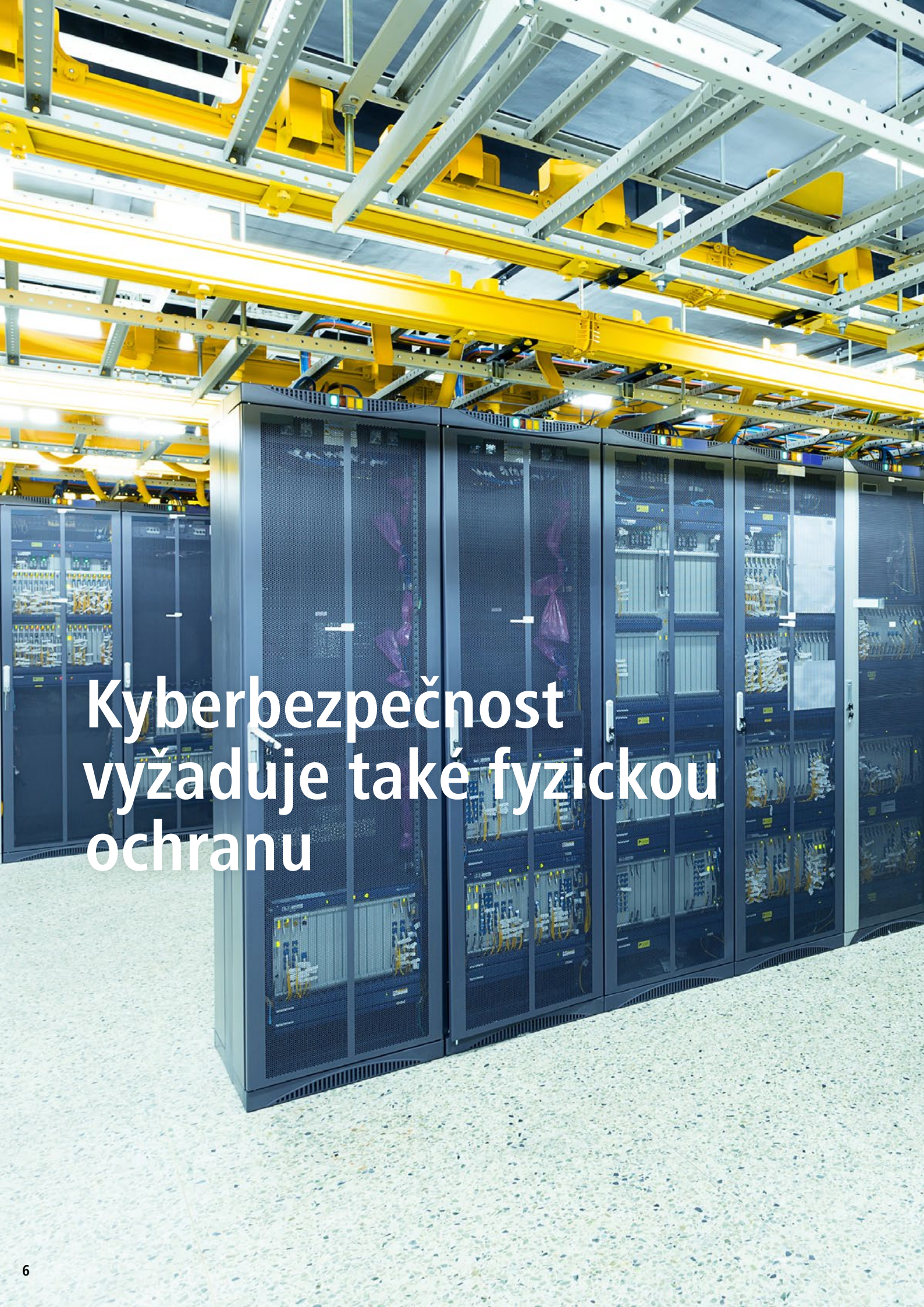
CER

Fyzická odolnost kritických infrastruktur

- Směrnice EU (2022/2557)
- **Cíl:** Zvýšení fyzické odolnosti vůči nedigitálním hrozbám a rizikům (přístup „all hazardous")
- **Vztahuje se na:** Provozovatele kritické infrastruktury, jako jsou:
  - Energetika
  - Doprava
  - Bankovnictví
  - Zdravotnictví
  - Vodárenství
  - Telekomunikace/IT
  - Potravinářství
  - Chemický průmysl
- **Požadavky:**
  - Analýzy rizik
  - Plány pro mimořádné situace a obnovení provozu
  - Bezpečnostní opatření
  - Řízení dodavatelských řetězců a závislostí
  - Povinnost hlásit závažné incidenty
  - Zajištění kontinuity životně důležitých služeb

Ve zkratce

Stručně řečeno to znamená, že subjekty, na které se vztahují směrnice NIS2 a CER, musí po provedení systematické analýzy hrozeb a rizik a jejich vyhodnocení zavést také opatření pro účinnou fyzickou ochranu. Patří sem zejména kontrola přístupu, monitorování a postupy pro detekci incidentů.CER toto dále upřesňuje: Provozovatelé kritických zařízení musí každé čtyři roky provádět analýzy rizik, zavádět vhodná opatření fyzické ochrany a účinně zabraňovat neoprávněnému vstupu.



Kyberbezpečnost vyžaduje také fyzickou ochranu

Relevantní bezpečnostní prvky pro použití v prostředí NIS2 a CER

Fyzická bezpečnost přístupu

- Přísná kontrola přístupu do kritických oblastí
- Přístupové prostředky odolné proti padělání
- Nejmodernější technologie

IT bezpečnost a šifrování

- Zabezpečená komunikace s využitím nejnovějších kryptografických standardů (TLS, AES, ECDSA)
- Žádná nezabezpečená hesla

Zaznamenávání a audity

- Úplná dokumentace všech přístupů a systémových akcí
- Protokoly splňující požadavky na audit s funkcí exportu jako auditní dokument

Reakce na incidenty & ochrana přístupu

- Rychlé zablokování napadených přístupů
- Nouzové plány pro případ výpadku nebo útoku (offline provoz dveří)

Kontinuita podnikání a zálohování dat

- Koncepce automatizovaného zálohování dat
- Strategie obnovy po výpadku, redundance

Řízení zranitelností a aktualizace

- Průběžné sledování bezpečnostních zranitelností softwaru (CVE) ze strany výrobců
- Včasné, podepsané a ověřené aktualizace

Ochrana osobních údajů a bezpečnost dat

- Ochrana soukromí již od návrhu, soulad s GDPR
- Funkce pro mazání osobních údajů
- Konfigurovatelné protokolování
- Zásada dvou očí při nahlížení do protokolů

Produkty EVVA a jejich řešení regulačních požadavků

Xesar

Přístupový systém splňující nejvyšší bezpečnostní požadavky

Fyzická a IT bezpečnost

- Přístupová práva založená na rolích pro jednotlivce/skupiny
- MIFARE DESFire EV1/EV2/EV3 (EAL5+), individuální klíče AES pro jednotlivá zařízení
- Šifrovaná komunikace typu „challenge-response“ (žádné protokoly v otevřeném textu)
- TLS ≥ 1.2 pro systémovou komunikaci
- Interní šifrování AES 256 bitů
- Hashovaná hesla (Bcrypt)

Protokoly přístupu a systémové protokoly

- Úplné a proti manipulaci zabezpečené protokoly událostí a systému
- Exporty splňující požadavky na auditovatelnost
- Možnost předložení důkazů o auditu a incidentech kdykoli

Reakce na incidenty a odolnost

- Blokování v reálném čase (online), seznamy blokovaných položek pro offline komponenty
- Varovné mechanismy v případě nejistého stavu blokování
- Samostatný offline provoz v případě výpadku IT nebo sítě

Aktualizace a správa zranitelností

- Nepřetržité sledování CVE
- Kryptograficky podepsané aktualizace (RSA/SHA256, AES256CCM)
- Ověřené aktualizace firmwaru a softwaru

Kontinuita podnikání

- Šifrované zálohy
- Obnova v případě nouze pomocí bezpečnostního listu zařízení
- Možnost víceuživatelského provozu a nepřetržitého provozu serveru 24/7

Ochrana osobních údajů

- Ochrana soukromí již od návrhu
- Aplikace neobsahuje žádné osobní údaje
- Možnost konfigurace automatického odstranění osobních údajů

AirKey

Mobilní řešení pro řízení přístupu splňující nejvyšší standardy

Fyzická a IT bezpečnost

- Přístupová média založená na smartphonech a RFID (JCOP SmartMX3, EAL6+)
- Ověřování pomocí ECDSA256 + AESSessionKeys
- Online správa zabezpečená protokolem TLS

Protokoly přístupu a systémové protokoly

- Protokolování v souladu s požadavky na auditovatelnost
- Exporty v souladu s požadavky na auditovatelnost
- Automatická aktualizace blokovacích seznamů a protokolů
- Flexibilní konfigurace v souladu s předpisy o ochraně osobních údajů

Reakce na incidenty a odolnost

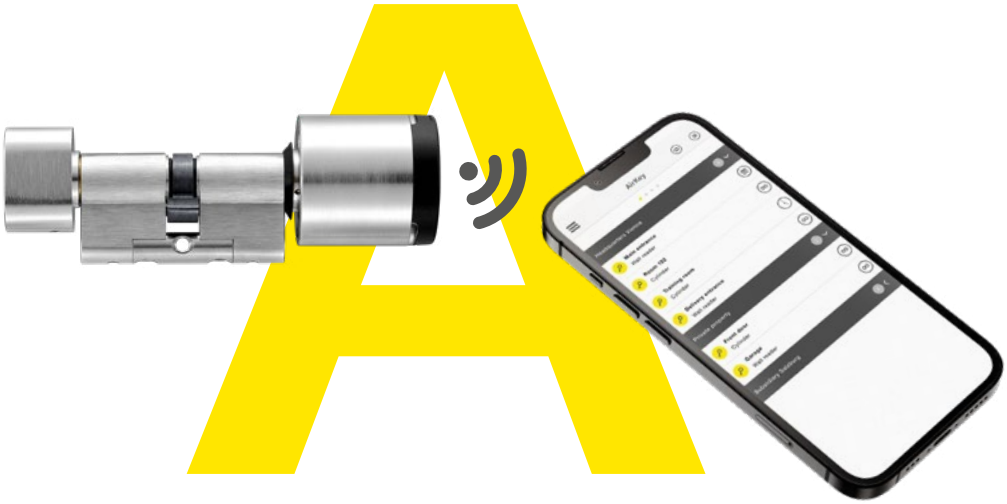
- Blokování v reálném čase přes internet
- Funkce dveří v režimu offline i při výpadku serveru
- Výstražné hlášení v případě stavů ohrožujících bezpečnost

Aktualizace a provoz

- Centrální správa aktualizací s podpisem
- Datová centra v Rakousku s certifikací ISO 27001
- Redundantní servery EVVA, klíče zabezpečené pomocí HSM

Ochrana osobních údajů

- Koncepce mazání v souladu s GDPR
- Privacy by Design
- Zásada dvojího dohledu při nahlížení do protokolů lze aktivovat

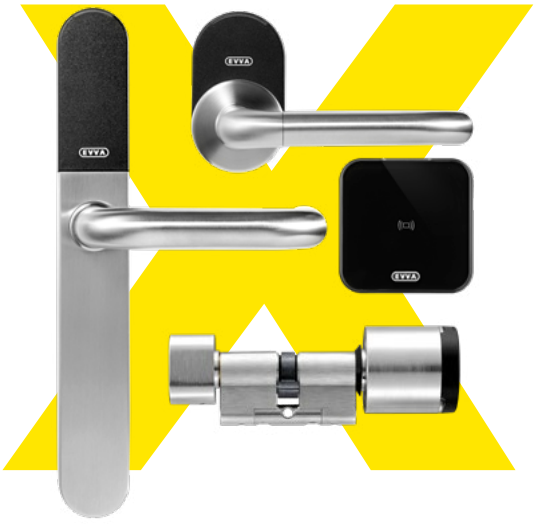


NORMY A STAV CERTIFIKACE

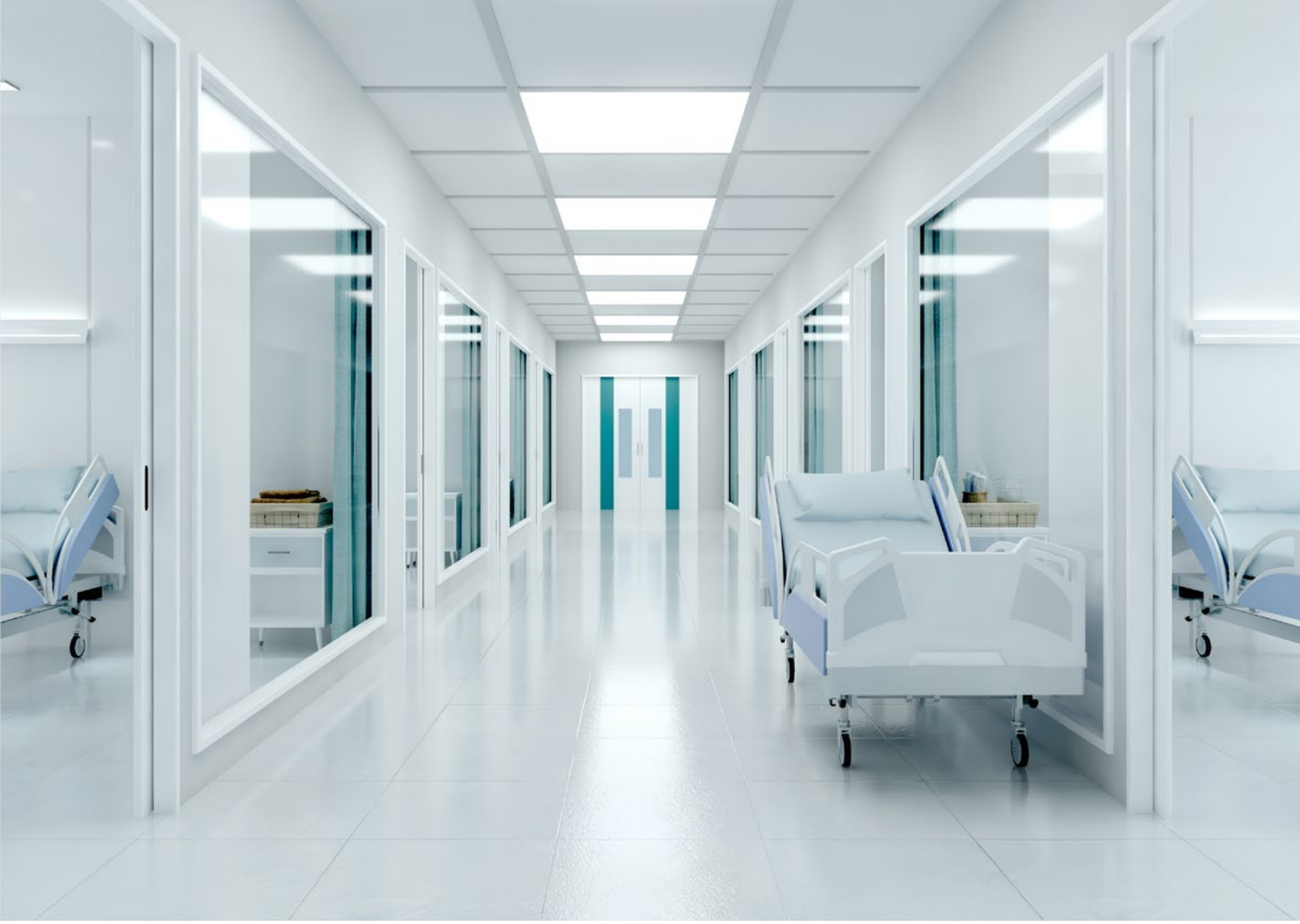
Úspěšně
prošlo kontrolou
(TÜV)

EN 18031-1

SPLNĚNY POŽADAVKY RED*



*RED: Směrnice o rádiových zařízeních



Praktický příklad 1:

Kontrola přístupu v nemocnici

NIS2/CER-relevantní

Výchozí situace

Nemocnice patří mezi „klíčová zařízení“ podle směrnice NIS2 a podléhá přísným požadavkům na informační a fyzickou bezpečnost. Obzvláště citlivé prostory, jako jsou serverovny, sklady léků nebo jednotky intenzivní péče, musí být chráněny před neoprávněným vstupem.

Řešení s Xesarem

- Přístupová práva založená na rolích pro různé skupiny zaměstnanců (např. IT, ošetřovatelský personál, administrativa)
- Přístupová média s individuálními, vysoce bezpečnými technologiemi (MIFARE DESFire EV3)
- Kompletní protokolování všech přístupů, auditovatelné záznamy pro účely auditu
- Rychlé zablokování ztracených médií pomocí blokovacích seznamů v reálném čase
- Offline provoz dveří v případě výpadku serveru (zajištění kontinuity provozu)
- Pravidelné, podepsané aktualizace softwaru a správa zranitelností

Přidaná hodnota

Nemocnice zavádí opatření založená na rizicích, je schopna bezchybně dokumentovat všechny incidenty a tím zvyšuje fyzickou odolnost tohoto zařízení.

Praktický příklad 2:

Výrobní podnik jako dodavatel pro kritickou infrastrukturu

Dodavatelský řetězec / relevantní pro CER

Výchozí situace

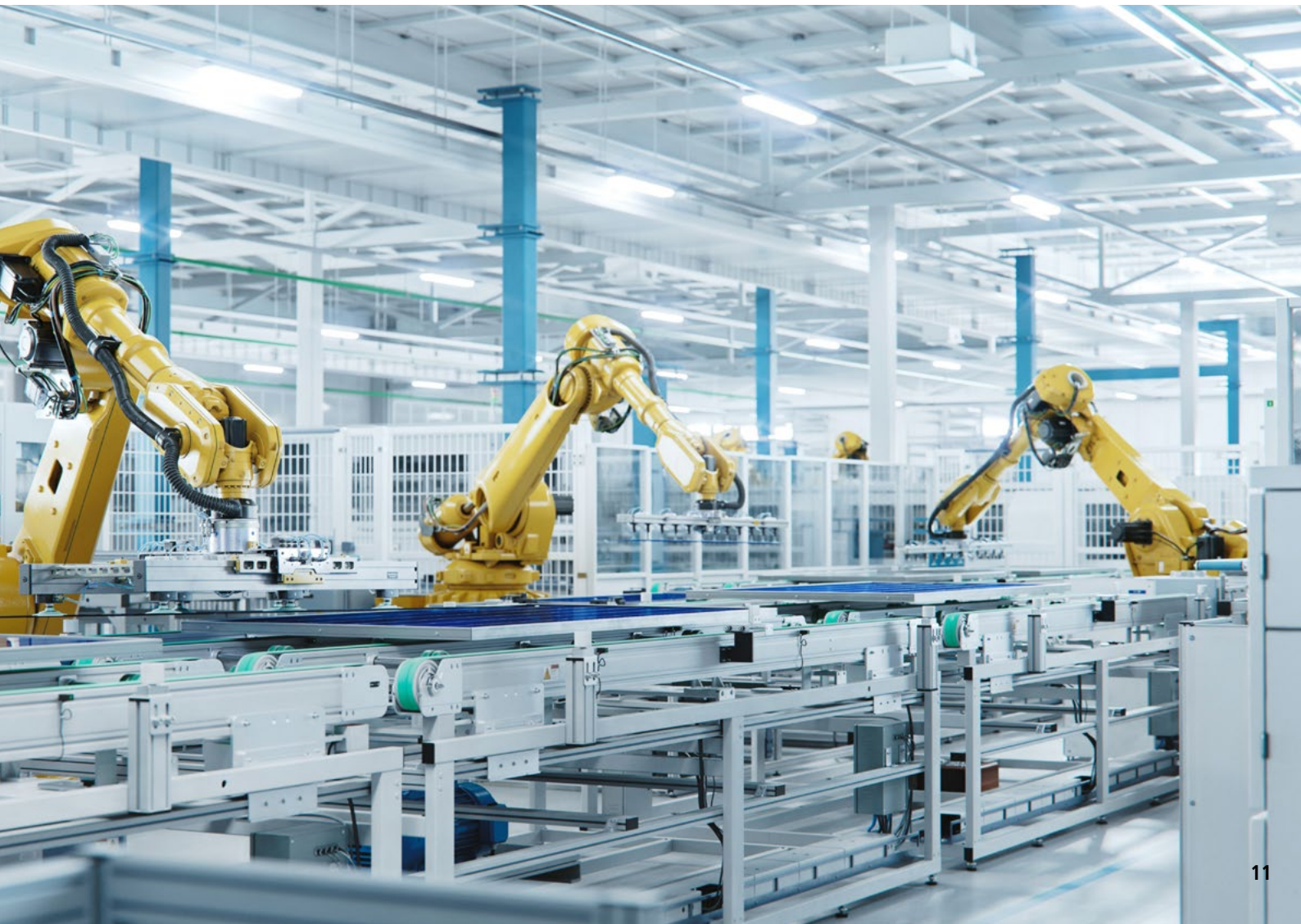
Středně velká strojírenská firma dodává své produkty energetickým společnostem, a proto se na ni nepřímo vztahuje směrnice o CER. Podnik musí prokázat, že jeho přístupové systémy a IT infrastruktura jsou odolné a bezpečné.

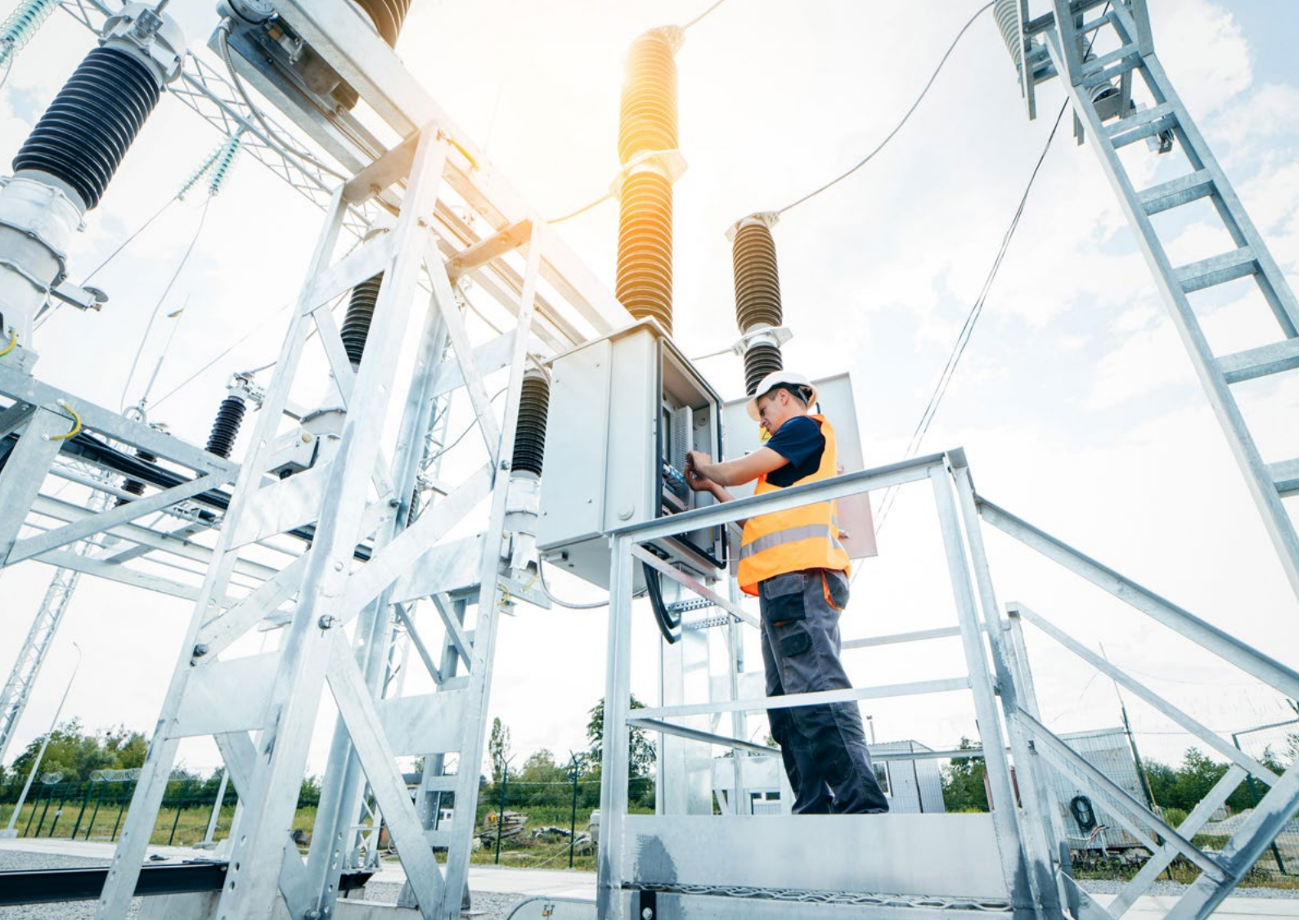
Řešení s AirKey

- Přístupová práva jsou spravována centrálně, a to i pro externí poskytovatele služeb (např. údržbářský personál)
- Bezpečná cloudová aplikace
- Přístupová média (smartphony, RFID) s velmi vysokým šifrováním (ECDSA-256, AES-128)
- Protokolování všech vstupů, export pro účely auditů
- Funkce mazání v souladu s GDPR a zásada „Privacy by Design“
- Aktualizace a správa zranitelností centrálně prostřednictvím společnosti EVVA

Přidaná hodnota

Společnost může svým zákazníkům prokázat, že zavedla přiměřená opatření k zajištění bezpečnosti v dodavatelském řetězci, pokud jde o přístup, a že je optimálně připravena na audity a certifikace.





Praktický příklad 3:

Řízení mimořádných situací a odolnost v městské správě

CER-relevantní

Výchozí situace

Městská správa provozuje kritickou infrastrukturu (např. vodovody a čistírny odpadních vod) a musí zajistit, aby v případě nouze (např. kybernetický útok, výpadek elektřiny) byl i nadále možný přístup do důležitých oblastí.

Řešení s Xesarem

- Funkční provoz v režimu offline při výpadku proudu nebo kybernetickém útoku
- Rychlé zablokování kompromitovaných přístupových médií, varovné hlášky v případě nevyřízených bezpečnostních úkolů
- Funkce zálohování a obnovy konfiguračních dat

Přidaná hodnota

Městská správa zůstává schopná fungovat i v případě krize – obyvatelé a místní podniky nejsou výpadky a poruchami nijak dotčeni.

Praktický příklad 4:

Ochrana osobních údajů a vedení záznamů ve výzkumném ústavu

NIS2/CER-relevantní

Výchozí situace

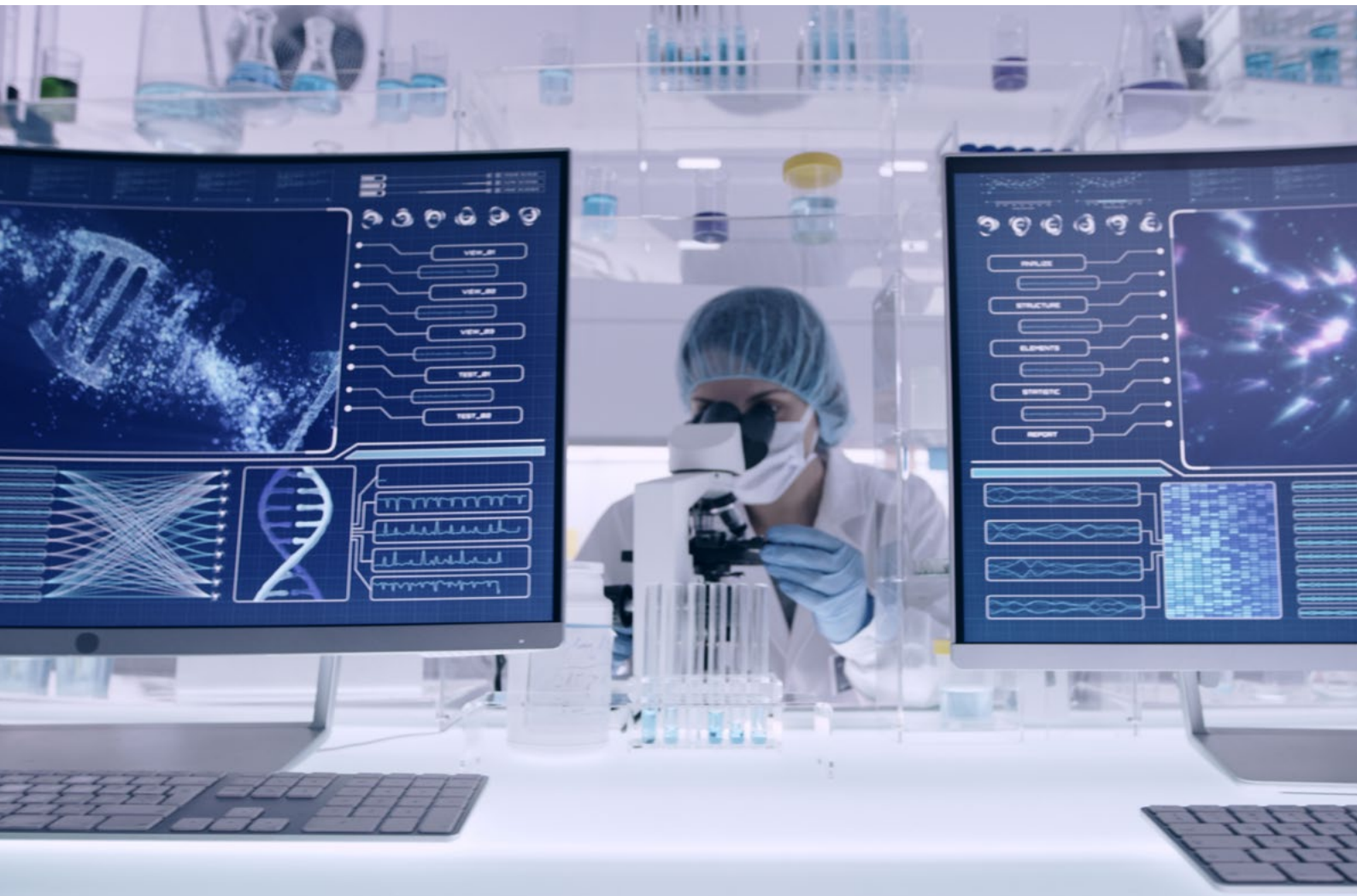
Výzkumný ústav zpracovává citlivé osobní údaje a musí splňovat požadavky nařízení GDPR i směrnice NIS2.

Řešení s AirKey

- Privacy by Design: Žádné ukládání osobních údajů v backendu
- Konfigurovatelné protokolování, funkce pro mazání osobních údajů
- Implementace v souladu s GDPR

Přidaná hodnota

Institut je kdykoli schopen prokázat dodržování ochrany osobních údajů a transparentnosti vůči dozorovým orgánům a partnerům.



Bezpečnostní kontrola pro provozovatele kritických infrastruktur

1. Organizační bezpečnostní rámec

- Máme zavedený závazný bezpečnostní plán, který zajišťuje fyzickou bezpečnost?
- Existují jasně definované struktury rolí, oprávnění a odpovědností v oblastech bezpečnosti, IT, správy budov a oblastech souvisejících s KRITIS?
- Jsou bezpečnostní směrnice a procesy pravidelně kontrolovány a aktualizovány?
- Je dodržování předepsané povinnosti hlášení bezpečnostních incidentů procesně zajištěno?

2. Analýza rizik a dodržování předpisů

- Provedli jsme v posledních 4 letech analýzu rizik v souladu se zákonem KRITIS/CER?
- Identifikovali jsme všechny fyzické a digitální slabiny v rámci celého procesního řetězce?
- Jsme s našimi řešeními pro řízení přístupu dobře připraveni z hlediska směrnice NIS2, zejména pokud jde o bezpečné protokoly a ochranu proti neoprávněné manipulaci?
- Používáme výhradně technicky moderní systémy (žádné nešifrované protokoly, jako např. Wiegand)?

3. Přístupová oprávnění a identity

- Jsou všechna přístupová oprávnění přiřazena na základě rolí a je možné jejich přiřazení dohledat?
- Jsou přístupová oprávnění pravidelně obnovována nebo automaticky odebrána, pokud již nejsou potřebná?
- Máme jasné postupy pro nástup, změnu role a odchod zaměstnanců a dodavatelů?

4. Technická bezpečnost systému kontroly přístupu

- Jsou všechny čtečky přístupu, karty a identifikační prostředky šifrovány?
- Jsou všechny dveře, serverovny a dispečinky kritické z hlediska bezpečnosti zabezpečeny elektronickými přístupovými systémy?
- Jsou údaje relevantní pro bezpečnost (např. protokoly) ukládány tak, aby vyhovovaly požadavkům auditu, a jsou chráněny před manipulací?

5. Monitorování, protokolování a transparentnost

- Jsou všechny přístupy a pokusy o přístup automaticky zaznamenávány?
- Jsou naše záznamy o přístupech vhodné pro audit, chráněné proti manipulaci a uchovávány po dostatečně dlouhou dobu?
- Používáme monitorovací nástroje, které propojují fyzické a digitální bezpečnostní události?

6. Ochrana kritických oblastí

- Jsou prostory jako serverovny, dispečinky, energetická a zásobovací zařízení nebo rozvaděče zvláště chráněny?
- Existují víceúrovňové přístupové zóny s postupně se zvyšující úrovní zabezpečení?
- Jsou citlivé prostory dodatečně zabezpečeny kamerovým systémem, monitorováním stavu dveří nebo poplašnou technikou?
- Máme plán pro nouzový přístup (např. v případě výpadku proudu nebo poruchy systému)?

7. Dodavatelé a poskytovatelé služeb

- Mají externí firmy a poskytovatelé služeb pouze časově omezená a jasně definovaná přístupová oprávnění?
- Jsou přístupy pro dočasné zaměstnance technicky omezeny a přísně monitorovány?
- Je využívání externích přístupů pravidelně kontrolováno?

8. Schopnost reagovat na mimořádné situace a obnovit provoz

- Existuje plán pro řízení mimořádných situací a krizí, který zahrnuje aspekty fyzické bezpečnosti?
- Jsou definovány postupy pro:
  - okamžité zablokování přístupu jednotlivých uživatelů nebo skupin
  - rychlé obnovení přístupové infrastruktury po útoku
  - scénáře evakuace nebo reakce na incidenty
- Jsou tyto plány pravidelně nacvičovány?

9. Školení a osvěta

- Jsou všichni zaměstnanci proškoleni v zacházení s přístupovými prostředky?
- Existuje průběžný program zvyšování povědomí o bezpečnostních směrnicích a správném chování?
- Vědí zaměstnanci, jak nahlásit podezřelé aktivity?

10. Udržitelnost a další rozvoj

- Je naše řešení přístupového systému škálovatelné pro nové pobočky nebo další požadavky?
- Můžeme bez problémů integrovat nové bezpečnostní standardy (aktualizace NIS2, směrnice BSI, rozšíření rámcového zákona KRITIS)?
- Máme jasný plán modernizace pro případ, že technologie zastarají nebo se objeví bezpečnostní mezery?

Směrnice NIS2 a nařízení CER jsou v jednotlivých členských státech EU prováděny pod následujícími názvy v národních právních předpisech

	NIS2	CER
Rakousko	NISG2026 (Zákon o bezpečnosti sítí a informací z roku 2026)	RKEG (Zákon o odolnosti kritických zařízení)
Německo	NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)	KRITIS-Dachgesetz (Zákon o posílení fyzické odolnosti kritických zařízení)
Belgie	Loi NIS2 (Zákon ze dne 26. dubna 2024 o kybernetické bezpečnosti síťových a informačních systémů)	Loi relative à la résilience des entités critiques (národní zákon o provádění CER, 2025/26)
Nizozemsko	Cyberbeveiligingswet (v rámci parlamentního procesu, stav z dubna 2026)	Wet weerbaarheid kritieke entiteiten (navrhovaný zákon o CER, stav z dubna 2026)
Švédsko	Cybersäkerhetslagen (Cybersecurity Act, SFS 2025:1506)	Lag om motståndskraft hos kritiska verksamheter (Zavedení CER se připravuje, stav k dubnu 2026)
Italien	Decreto Legislativo n. 138/2024	Decreto Legislativo n. 134/2024
Česká republika	Zákon o kybernetické bezpečnosti (novela/ nové znění týkající se provádění směrnice NIS2)	Zákon o odolnosti kritických subjektů (Zákon o provedení směrnice CER)
Polsko	Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) – Novela směrnice NIS2	Ustawa o odporności podmiotów krytycznych (ve fázi realizace)
Slovensko	Zákon o kybernetickej bezpečnosti (novela zákona NIS2)	Zákon o odolnosti kritických subjektov

www.evva.com