EVVA
access to security

Whitepaper

Prvá ochranná bariéra

Kontrola prístupu pre kritickú infraštruktúru

Prvá ochranná bariéra
Kontrola prístupu pre kritickú infraštruktúru

Ako moderná kontrola prístupu prispieva k splneniu požiadaviek smerníc NIS2 a CER – a trvalo zvyšuje fyzickú bezpečnosť.

Kontrola prístupu ako kľúčová zložka pre súlad s nariadeniami NIS2 a CER

Svet, a aj my sami, sme sa – najmä v posledných rokoch – zmenili. Geopolitické zmeny, ako sú vojny, politická nestabilita, klimatické zmeny a nové technológie, ovplyvňujú náš každodenný život a vyžadujú si vyššiu odolnosť zariadení nevyhnutných pre život, najmä posilnenie fyzickej ochrany.

Prostredníctvom európskej smernice NIS2 (2022/2555) a doplnkovej smernice CER (2022/2557) Európska únia výrazne sprísňuje bezpečnostné požiadavky na prevádzkovateľov kritických a dôležitých zariadení. Cieľom oboch právnych predpisov je predovšetkým posilniť odolnosť voči digitálnym a fyzickým hrozbám – v dôsledku toho sa do popredia moderných bezpečnostných architektúr dostáva aj kontrola prístupu. V tejto bielej knihe sa chceme venovať predovšetkým téme „Fyzické bezpečnostné opatrenia pre kritické zariadenia“.

Regulačný rámec: NIS2 a CER

Vysvetlenie pojmov

NIS2 a CER sú smernice EÚ, ktoré je potrebné transponovať do vnútroštátnych právnych predpisov; prehľad príslušných právnych označení na európskych trhoch nájdete na strane 15 tejto bielej knihy.

NIS2

Kyberbezpečnosť pre kritické a dôležité odvetvia

- Smernica EÚ (2022/2555)
- **Cieľ:** Zvýšenie úrovne kybernetickej bezpečnosti prostredníctvom minimálnych noriem platných v celej EÚ. Ukladá podnikom a organizáciám povinnosť systematicky zlepšovať svoju IT a kybernetickú bezpečnosť a hlásiť incidenty.
- **Vzťahuje sa na:**
  - „Kľúčové" zariadenia: patria sem podniky s vysokou kritickosťou, ktorých výpadok by mal závažný vplyv na spoločnosť, hospodárstvo alebo verejnú bezpečnosť; medzi ne patria energetika, doprava, bankovníctvo, zdravotníctvo, vodné hospodárstvo, telekomunikácie/IT
  - „Dôležité" sektory: patria sem podniky s iným kritickým vplyvom, ako sú pošta, odpadové hospodárstvo, chemický priemysel, potravinárstvo, výroba tovaru (od 50 zamestnancov a obratu 10 miliónov EUR)
- Požiadavky na podniky, na ktoré sa vzťahuje smernica NIS-2, zahŕňajú okrem iného:
  - Riadenie kybernetickej bezpečnosti (analýzy rizík, bezpečnostné koncepcie, reakcia na incidenty, zabezpečenie kontinuity činnosti)
  - Povinnosť hlásiť bezpečnostné incidenty
  - Zodpovednosť vedenia
  - Prísny dohľad a sankcie

CER

Fyzická odolnosť kritických infraštruktúr

- Smernica EÚ (2022/2557)
- **Cieľ:** Zvýšenie fyzickej odolnosti voči nedigitálnym hrozbám a nebezpečenstvám (prístup zohľadňujúci všetky druhy nebezpečenstiev)
- **Vzťahuje sa na:** prevádzkovateľov kritickej infraštruktúry, ako sú:
  - energetika
  - doprava
  - bankovníctvo
  - zdravotníctvo
  - vodné hospodárstvo
  - telekomunikácie/IT
  - potravinárstvo
  - chemický priemysel
- **Požiadavky:**
  - analýzy rizík
  - plány pre núdzové situácie a obnovenie
  - prevádzky
  - bezpečnostné opatrenia
  - riadenie dodávateľských reťazcov a súvislostí
  - povinnosť hlásiť závažné incidenty
  - zabezpečenie kontinuity životne dôležitých služieb

V skratke

Zhrnuté, to znamená, že zariadenia, na ktoré sa vzťahujú smernice NIS2 a CER, musia po vykonaní systematickej analýzy hrozieb a rizík, ako aj jej vyhodnotení, zaviesť aj opatrenia na účinnú fyzickú ochranu. Patria sem najmä kontrola prístupu, monitorovanie a postupy na detekciu incidentov.

CER to ďalej konkretizuje: Prevádzkovatelia kritických zariadení musia každé štyri roky vykonávať analýzy rizík, zavádzať vhodné opatrenia fyzickej ochrany a účinne zabraňovať neoprávnenému vstupu.

Kyberbezpečnosť si vyžaduje aj fyzickú ochranu

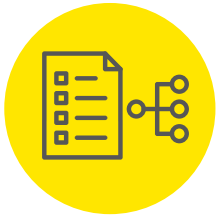
Relevantné bezpečnostné prvky pre použitie v prostredí NIS2 a CER

Fyzická bezpečnosť prístupu

- Prísna kontrola prístupu do kritických oblastí
- Prístupové médiá odolné proti falšovaniu
- Najmodernejšie technológie

IT bezpečnosť a šifrovanie

- Zabezpečená komunikácia s využitím najnovších kryptografických štandardov (TLS, AES, ECDSA)
- Žiadne nezabezpečené heslá



Vedenie záznamov a audity

- Úplná dokumentácia všetkých prístupov a systémových akcií
- Protokoly spĺňajúce požiadavky na audit s funkciou exportu ako audítorský dokument

Reakcia na incidenty a ochrana prístupu

- Rýchle zablokovanie kompromitovaných prístupov
- Núdzové plány pre prípad výpadku alebo útoku (prevádzka dverí v režime offline)

Kontinuita podnikania a zálohovanie dát

- Koncepcia automatizovaného zálohovania dát
- Stratégia obnovenia prevádzky po výpadku, redundancia

Správa zraniteľností a aktualizácie

- Neustále sledovanie bezpečnostných chýb v softvéri (CVE) zo strany výrobcov
- Včasné, podpísané a overené aktualizácie

Ochrana osobných údajov a bezpečnosť údajov

- Ochrana súkromia už pri návrhu, súlad s nariadením GDPR
- Funkcie na vymazanie osobných údajov
- Konfigurovateľné protokolovanie
- Princíp štyroch očí pri nahliadaní do protokolov

Produkty EVVA a ich riešenia v súlade s regulačnými požiadavkami

Xesar

Prístupový systém spĺňajúci najvyššie bezpečnostné požiadavky

Fyzická a IT bezpečnosť

- Práva prístupu založené na rolách pre jednotlivcov/skupiny
- MIFARE DESFire EV1/EV2/EV3 (EAL5+), individuálne AES kľúče pre každé zariadenie
- Šifrovaná komunikácia typu „challenge-response“ (bez protokolov v čitateľnej podobe)
- TLS ≥ 1.2 pre systémovú komunikáciu
- Interné šifrovanie AES 256-bit
- Hashované heslá (Bcrypt)

Protokoly prístupu a systémové protokoly

- Úplné protokoly udalostí a systémové protokoly chránené proti manipulácii
- Exporty spĺňajúce požiadavky na audit
- Možnosť kedykoľvek predložiť dôkazy o audite a incidentoch

Reakcia na incidenty a odolnosť

- Blokovanie v reálnom čase (online), zoznamy blokovaných položiek pre offline komponenty
- Varovné mechanizmy v prípade neistého stavu blokovania
- Samostatná prevádzka v režime offline v prípade výpadku IT alebo siete

Aktualizácie a riadenie zraniteľností

- Neustále monitorovanie CVE
- Kryptograficky podpísané aktualizácie (RSA/SHA256, AES256CCM)
- Overené aktualizácie firmvéru a softvéru

Nepretržité fungovanie podniku

- Šifrované zálohy
- Obnova v núdzových situáciách pomocou bezpečnostného listu zariadenia
- Možnosť prevádzky na viacerých pracoviskách a nepretržitej prevádzky servera

Ochrana osobných údajov

- Privacy by Design
- V aplikácii sa nenachádzajú žiadne osobné údaje
- Možnosť nastavenia automatického odstránenia osobných údajov

AirKey

Mobilné riešenie prístupu spĺňajúce najvyššie štandardy

Fyzická a IT bezpečnosť

- Samrtfóny a prístupové médiá založené na technológii RFID (JCOP SmartMX3, EAL6+)
- Autentifikácia ECDSA256 + AESSessionKeys
- Online správa zabezpečená protokolom TLS

Protokoly prístupu a systémové protokoly

- Protokolovanie v súlade s požiadavkami na audit
- Exporty v súlade s požiadavkami na audit
- Automatická aktualizácia zoznamov blokovaných adries a protokolov
- Flexibilná konfigurácia v súlade s predpismi o ochrane osobných údajov

Reakcia na incidenty a odolnosť

- Blokovanie v reálnom čase cez internet
- Fungovanie dverí v režime offline aj v prípade výpadku servera
- Varovné upozornenia v prípade stavov kritických z hľadiska bezpečnosti

Aktualizácie a prevádzka

- Centralizovaná správa aktualizácií s podpisom
- Dátové centrá s certifikáciou ISO 27001 v Rakúsku
- Redundantné servery EVVA, kľúče zabezpečené pomocou HSM

Ochrana osobných údajov

- Centralizovaná správa aktualizácií s podpisom
- Dátové centrá s certifikáciou ISO 27001 v Rakúsku
- Redundantné servery EVVA, kľúče zabezpečené pomocou HSM

NORMY A STAV CERTIFIKÁCIE

Úspešne
skúšané (TÜV)
EN 18031-1

RED* – POŽIADAVKY SPLNENÉ

*RED: Radio Equipment Directive

Praktický príklad 1

Kontrola prístupu v nemocnici

NIS2/CER-relevantné

Východisková situácia

Nemocnica patrí medzi „kľúčové zariadenia“ podľa smernice NIS2 a podlieha prísnym požiadavkám na IT a fyzickú bezpečnosť. Obzvlášť citlivé priestory, ako sú serverovne, sklady liekov alebo jednotky intenzívnej starostlivosti, musia byť chránené pred neoprávneným vstupom.

Riešenie s Xesarom

- Prístupové práva založené na rolách pre rôzne skupiny zamestnancov (napr. IT, ošetrovateľský personál, administratíva)
- Prístupové médiá s individuálnymi, vysoko bezpečnými technológiami (MIFARE DESFire EV3)
- Kompletné zaznamenávanie všetkých prístupov, revíziou overené protokoly pre audity
- Rýchle zablokovanie stratených médií prostredníctvom zoznamov blokovaných médií v reálnom čase
- Offline prevádzka dverí v prípade výpadku servera (zabezpečenie kontinuity prevádzky)
- Pravidelné, podpísané aktualizácie softvéru a riadenie zraniteľností

Pridaná hodnota

Nemocnica zavádza opatrenia založené na riziku, dokáže bezchybne zdokumentovať všetky udalosti a tým zvyšuje fyzickú odolnosť tohto zariadenia.

Praktický príklad 2

Výrobný závod ako dodávateľ pre kritickú infraštruktúru

Dodávateľský reťazec/ relevantné pre CER

Východisková situácia

Stredne veľká strojárska spoločnosť dodáva svoje výrobky dodávateľom energie, a preto sa na ňu nepriamo vzťahuje smernica o CER. Spoločnosť musí preukázať, že jej systémy prístupu a IT infraštruktúra sú odolné a bezpečné.

Riešenie s AirKey

- Prístupové práva sa spravujú centrálne, a to aj v prípade externých poskytovateľov služieb (napr. údržbársky personál)
- Bezpečná aplikácia založená na cloude
- Prístupové médiá (smartfóny, RFID) s veľmi vysokým stupňom šifrovania (ECDSA-256, AES-128)
- Protokolovanie všetkých prístupov, export pre audity
- Funkcie mazania v súlade s nariadením GDPR a zásada „Privacy by Design“
- Aktualizácie a riadenie zraniteľností centrálne prostredníctvom spoločnosti EVVA

Pridaná hodnota

Spoločnosť môže svojim zákazníkom preukázať, že v dodávateľskom reťazci zaviedla primerané opatrenia na zabezpečenie prístupu a že je optimálne pripravená na audity a certifikácie.

Praktický príklad 3

Riadenie mimoriadnych situácií a odolnosť v mestskej správe

CER-relevantné

Východisková situácia

Mestská samospráva prevádzkuje kritickú infraštruktúru (napr. vodovody a čistiarne odpadových vôd) a musí zabezpečiť, aby v prípade núdze (napr. kybernetický útok, výpadok elektrickej energie) bol naďalej možný prístup do dôležitých oblastí.

Riešenie s Xesarom

- Fungovanie prevádzky v režime offline v prípade výpadku prúdu alebo kybernetického útoku
- Rýchle zablokovanie kompromitovaných prístupových médií, varovné upozornenia v prípade nevyriešených bezpečnostných úloh
- Funkcie zálohovania a obnovy konfiguračných údajov

Pridaná hodnota

Mestská samospráva zostáva schopná fungovať aj v prípade krízovej situácie – obyvatelia a miestne podniky nie sú ovplyvnení výpadkami a poruchami.

Praktický príklad 4

Ochrana osobných údajov a vedenie záznamov vo výskumnom ústave

NIS2/CER-relevantné

Východisková situácia

Výskumný ústav spracúva citlivé osobné údaje a musí spĺňať požiadavky nariadenia GDPR a smernice NIS2.

Riešenie s AirKey

- Privacy by Design: Žiadne ukladanie osobných údajov v backende
- Konfigurovateľné protokolovanie, funkcie na vymazanie osobných údajov
- Implementácia v súlade s nariadením GDPR

Pridaná hodnota

Inštitút môže kedykoľvek preukázať dodržiavanie ochrany osobných údajov a transparentnosti voči dozorným orgánom a partnerom.

Bezpečnostná kontrola pre prevádzkovateľov kritických infraštruktúr

1. Organizačný bezpečnostný rámec

- Máme záväzný bezpečnostný plán na zabezpečenie fyzickej bezpečnosti?
- Existujú jasne definované štruktúry rolí, právomocí a zodpovedností v oblasti bezpečnosti, IT, správy budov a oblastí relevantných pre KRITIS?
- Sú bezpečnostné smernice a procesy pravidelne kontrolované a aktualizované?
- Je dodržiavanie predpísanej povinnosti hlásiť bezpečnostné incidenty procesne zabezpečené?

2. Analýza rizík a dodržiavanie predpisov

- Vykonali sme v priebehu posledných 4 rokov analýzu rizík v súlade so zákonom KRITIS/CER?
- Identifikovali sme všetky fyzické a digitálne slabé miesta v rámci celého procesného reťazca?
- Sme s našimi riešeniami prístupového systému dobre pripravení z hľadiska smernice NIS2, najmä pokiaľ ide o bezpečné protokoly a ochranu proti manipulácii?
- Používame výlučne technicky moderné systémy (žiadne nešifrované protokoly, ako napr. Wiegand)?

3. Prístupové oprávnenia a identity

- Sú všetky prístupové oprávnenia priradené na základe rolí a je možné ich vysledovať?
- Sú prístupové oprávnenia pravidelne recertifikované alebo automaticky odobraté, ak už nie sú potrebné?
- Máme jasné postupy pre nástup, zmenu rolí a odchod zamestnancov a dodávateľov?

4. Technická bezpečnosť systému kontroly prístupu

- Sú všetky čítačky prístupových kariet, karty a identifikačné médiá šifrované?
- Sú všetky dvere kritické z hľadiska bezpečnosti, serverové miestnosti a dispečingy zabezpečené elektronickými systémami kontroly prístupu?
- Sú údaje relevantné z hľadiska bezpečnosti (napr. protokoly) ukladané spôsobom, ktorý spĺňa požiadavky auditu, a chránené pred manipuláciou?

5. Monitorovanie, zaznamenávanie a transparentnosť

- Sú všetky prístupy a pokusy o prístup automaticky zaznamenávané?
- Sú naše protokoly o prístupoch vhodné na audítorské účely, chránené proti manipulácii a uchovávané dostatočne dlho?
- Používame monitorovacie nástroje, ktoré prepojujú fyzické a digitálne bezpečnostné udalosti?

6. Ochrana kritických oblastí

- Sú priestory ako serverovne, riadiace strediská, energetické a zásobovacie zariadenia alebo rozvádzače osobitne chránené?
- Existujú viacstupňové zóny prístupu s postupne sa zvyšujúcou úrovňou bezpečnosti?
- Sú citlivé priestory dodatočne zabezpečené kamerovým systémom, monitorovaním stavu dverí alebo poplašnou technikou?
- Máme plán pre núdzový prístup (napr. v prípade výpadku prúdu alebo poruchy systému)?

7. Dodávatelia a poskytovatelia služieb

- Haben externe Firmen und Dienstleister nur zeitlich begrenzte und klar definierte Zutrittsrechte?
- Sind Zugänge für temporäres Personal technisch eingeschränkt und streng überwacht?
- Wird die Nutzung externer Zugänge regelmäßig auditiert?

8. Schopnosť reagovať na núdzové situácie a obnoviť prevádzku

- Existuje plán riadenia mimoriadnych situácií a kríz, ktorý zahŕňa aspekty fyzickej bezpečnosti?
- Sú definované postupy pre:
  - Okamžité zablokovanie prístupu jednotlivých používateľov alebo skupín
  - Rýchlu obnovu infraštruktúry prístupu po útoku
  - Scenáre evakuácie alebo reakcie na incidenty
- Prebiehajú pravidelné nácviky týchto plánov?

9. Školenie a osvetová činnosť

- Sú všetci zamestnanci zaškolení v oblasti zaobchádzania s prístupovými prostriedkami?
- Existuje priebežný program zvyšovania povedomia o bezpečnostných smerniciach a správnom správaní?
- Vedia zamestnanci, ako nahlásiť podozrivé aktivity?

10. Udržateľnosť a ďalší rozvoj

- Je naše riešenie prístupového systému škálovateľné pre nové pobočky alebo dodatočné požiadavky?
- Môžeme bez problémov integrovať nové bezpečnostné štandardy (aktualizácie NIS2, smernice BSI, rozšírenia v rámcovom zákone KRITIS)?
- Máme jasný plán modernizácie pre prípad, že sa technológie stanú zastaralými alebo sa zistia bezpečnostné chyby?

Smernice NIS2 a CER sa v jednotlivých členských štátoch EÚ implementujú pod nasledujúcimi názvami vnútroštátnych právnych predpisov

	NIS2	CER
Rakúsko	NISG2026 (Zákon o bezpečnosti sietí a informácií z roku 2026)	RKEG (Zákon o odolnosti kritických zariadení)
Nemecko	NIS-2-Umsetzungs- und Cybersicher-heitsstärkungsgesetz (NIS2UmsuCG)	KRITIS-Dachgesetz (Zákon o posilnení fyzickej odolnosti kritických zariadení)
Belgicko	Loi NIS2 (Zákon z 26. apríla 2024 o kybernetickej bezpečnosti sieťových a informačných systémov)	Loi relative à la résilience des entités critiques (národný zákon o imple-mentácii CER, 2025/26)
Holandsko	Cyberbeveiligingswet (v procese parlament-ného schvaľovania, stav z apríla 2026)	Wet weerbaarheid kritie-ke entiteiten (navrhovaný zákon o CER, stav z apríla 2026)
Švédsko	Cybersäkerhetslagen (Cybersecurity Act, SFS 2025:1506)	Lag om motståndskraft hos kritiska verksamheter (Implementácia CER sa pripravuje, stav: apríl 2026)
Taliansko	Decreto Legislativo n. 138/2024	Decreto Legislativo n. 134/2024
Česko	Zákon o kybernetické bezpečnosti (novela/ nové znenie týkajúce sa transpozície smer-nice NIS2)	Zákon o odolnosti kri-tických subjektů (Zákon o vykonávaní CER)
Polen	Ustawa o Kra-jowym Systemie Cyberbezpieczeństwa (KSC) – Novela smer-nice NIS2	Ustawa o odporności podmiotów krytycznych (v procese realizácie)
Slovensko	Zákon o kybernetickej bezpečnosti (novela zákona NIS2)	Zákon o odolnosti kritických subjektov

www.evva.com