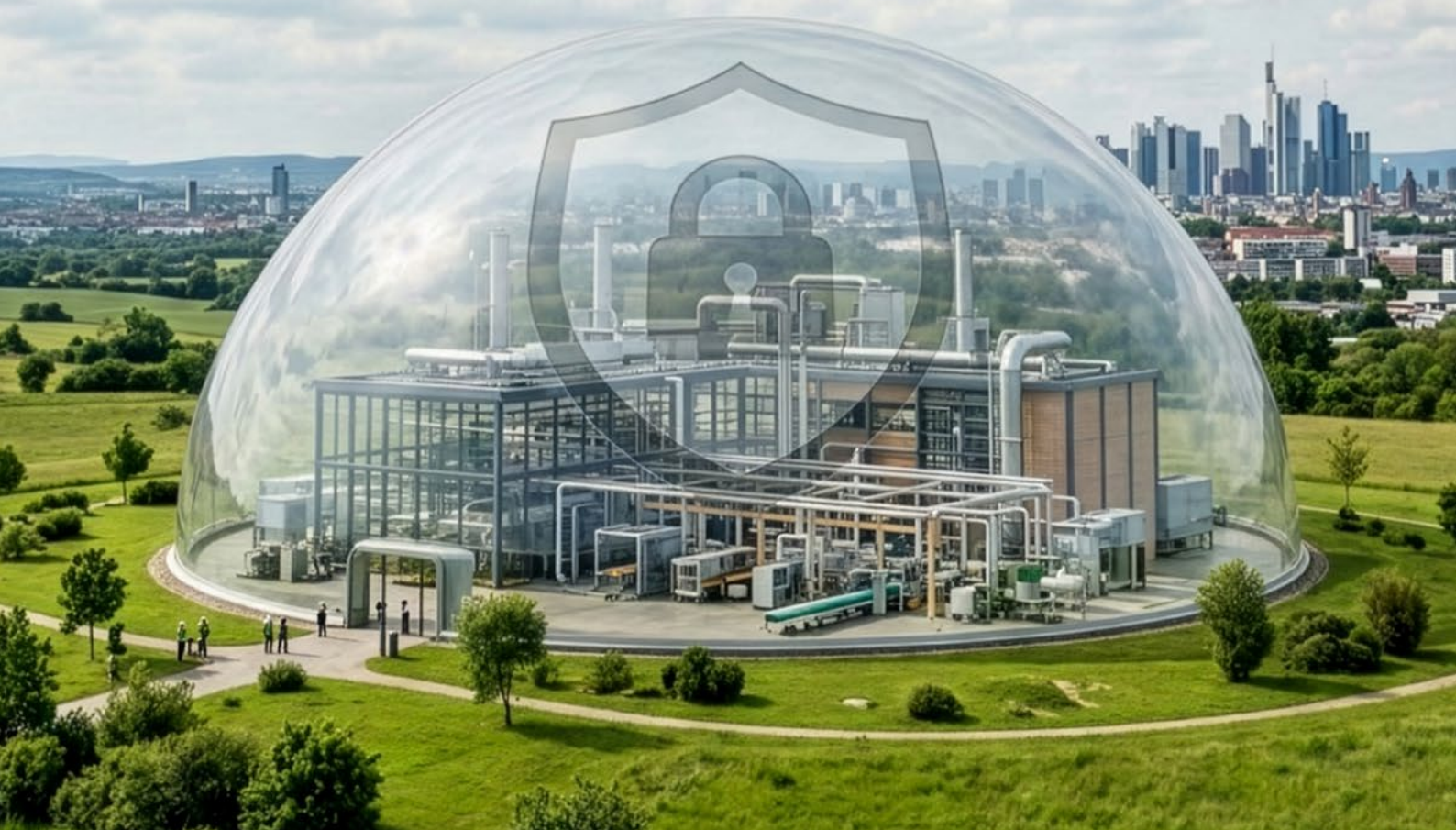
EVVA
access to security

Whitepaper

Pierwsza linia ochrony
Kontrola dostępu w infrastrukturze krytycznej



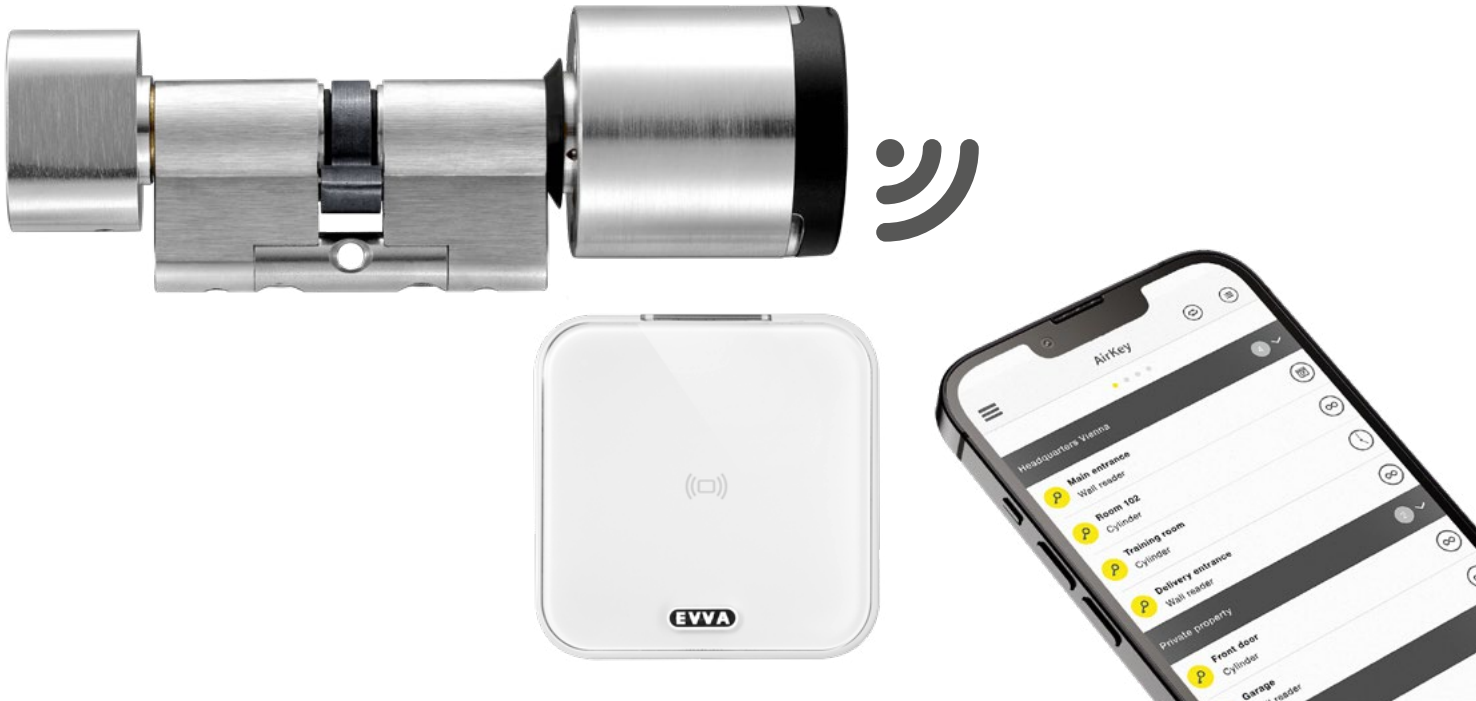
Pierwsza linia ochrony
Kontrola dostępu w infrastrukturze krytycznej

W jaki sposób nowoczesna kontrola dostępu przyczynia się do spełnienia wymogów NIS2 i CER – oraz trwale zwiększa bezpieczeństwo fizyczne.

Kontrola dostępu jako kluczowy element zapewnienia zgodności z dyrektywą NIS2 i rozporządzeniem CER

Świat i my sami zmieniliśmy się – szczególnie w ciągu ostatnich kilku lat. Zmiany geopolityczne, takie jak wojny i niestabilność polityczna, zmiany klimatyczne oraz rozwój nowych technologii wpływają na naszą codzienność i zwiększają potrzebę zapewnienia odporności obiektów o kluczowym znaczeniu. Szczególnie istotne staje się wzmocnienie ich ochrony.
Wraz z europejską dyrektywą NIS2 (2022/2555) oraz uzupełniającą ją dyrektywą CER (2022/2557) Unia Europejska znacząco podnosi wymagania dotyczące bezpieczeństwa dla operatorów kluczowych obiektów infrastruktury krytycznej. Oba akty prawne mają na celu kompleksowe zwiększenie odporności na zagrożenia cyfrowe i fizyczne – tym samym czyniąc kontrolę dostępu jednym z najważniejszych elementów nowoczesnej architektury bezpieczeństwa.

W niniejszym opcacowaniu chcemy skupić się przede wszystkim na zagadnieniu: „Środki ochrony dla obiektów infrastruktury krytycznej".



Regulacje prawne NIS2 i CER

Objaśnienia pojęć

NIS2 i CER to dyrektywy Unii Europejskiej, które wymagają wdrożenia do prawa krajowego poszczególnych państw członkowskich. Przegląd odpowiednich regulacji prawnych oraz stosowanych oznaczeń na rynkach europejskich znajduje się na stronie 15 niniejszego opracowania.

NIS2

Cyberbezpieczeństwo w kluczowych i ważnych sektorach

- Dyrektywa UE (2022/2555)
- **Cel:** podniesienie poziomu cyberbezpieczeństwa przez wprowadzenie minimalnych standardów obowiązujących w całej UE. Obowiązki: organizacje muszą stale doskonalić swoje zabezpieczenia IT i cyberbezpieczeństwo, a także raportować występujące incydenty.
- **Dotyczy:**
  - „Kluczowe" podmioty: to organizacje o strategicznym znaczeniu, których zakłócenie działania miałoby istotny wpływ na społeczeństwo, gospodarkę lub bezpieczeństwo publiczne, w tym sektory: energetyki, transportu, bankowości, ochrony zdrowia, gospodarki wodnej, telekomunikacji/IT.
  - „Ważne" podmioty: to organizacje działające w innych sektorach, takich jak: usługi pocztowe, gospodarka odpadami, przemysł chemiczny, produkcja żywności i towarów (od 50 pracowników i 10 mln EUR obrotu).
- Wymagania wobec organizacji objętych dyrektywą NIS2 obejmują m.in.:
  - zarządzanie cyberbezpieczeństwem (analiza ryzyka, środki bezpieczeństwa, reagowanie na incydenty, ciągłość działania)
  - obowiązek zgłaszania
  - incydentow
  - odpowiedzialność kierownictwa
  - ścisły nadzór i sankcje za nieprzestrzeganie wymagań.

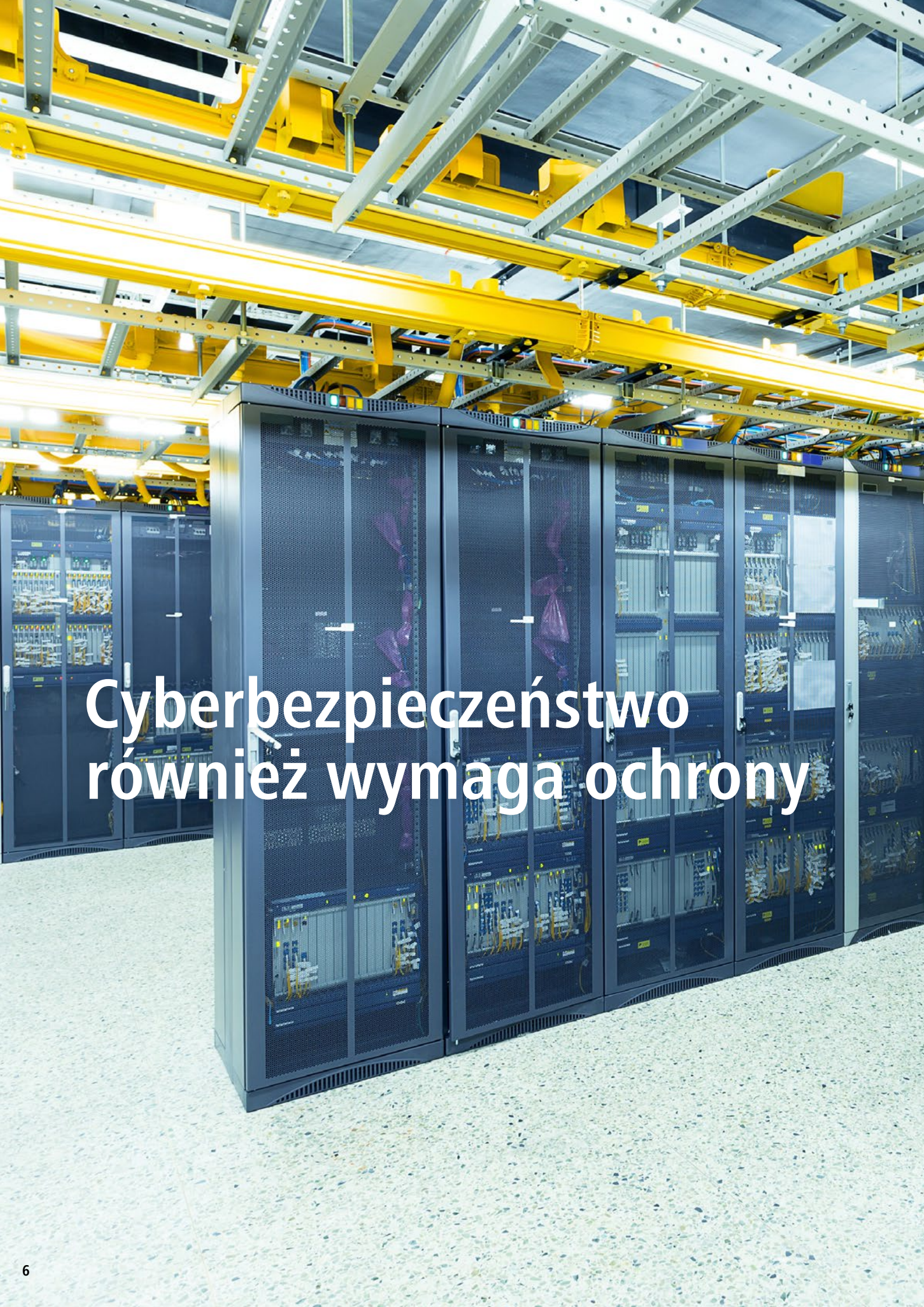
CER

Bezpieczeństwo infrastruktury krytycznej

- Dyrektywa UE (2022/2557)
- **Cel:** zwiększenie odporności fizycznej na zagrożenia niedotyczące cyberprzestrzeni oraz wszelkiego rodzaju zagrożenia (podejście obejmujące wszystkie rodzaje zagrożeń: „all-hazards approach").
- **Dotyczy: operatorów infrastruktury krytycznej w sektorach:**
  - energetyka
  - transport
  - bankowość
  - ochrona zdrowia
  - gospodarka wodna
  - telekomunikacja/IT
  - produkcja i dystrybucja żywności
  - przemysł chemiczny
- Wymagania:
  - analizy ryzyka
  - opracowanie planów reagowania kryzysowego i przywrócenia działalności
  - wdrożenie środków bezpieczeństwa
  - zarządzanie łańcuchem dostaw
  - obowiązek zgłaszania poważnych incydentow
  - zapewnienie ciągłości świadczenia kluczowych usług.

W skrócie

Podsumowując, organizacje objęte dyrektywami NIS2 i CER są zobowiązane do przeprowadzenia systematycznej analizy oraz oceny zagrożeń i ryzyka, a następnie wdrożenia środków zapewniających skuteczną ochronę. Obejmują one w szczególności kontrolę dostępu, monitoring oraz procedury wykrywania incydentów. Dyrektywa CER precyzuje te wymagania, nakładając na operatorów infrastruktury krytycznej obowiązek przeprowadzania analiz ryzyka co cztery lata, wdrażania odpowiednich środków ochrony oraz skutecznego zapobiegania nieuprawnionemu dostępowi.



Cyberbezpieczeństwo również wymaga ochrony

Funkcje bezpieczeństwa wspierające wymagania dyrektyw NIS2 i CER

Kontrola dostępu do obiektów

- Ścisła kontrola dostępu do stref krytycznych
- Odporne na manipulację nośniki dostępu
- Nowoczesne rozwiązania technologiczne

Bezpieczeństwo IT i ochrona kryptograficzna

- Szyfrowana komunikacja wykorzystująca aktualne standardy kryptograficzne (TLS, AES, ECDSA)
- Wyeliminowanie stosowania słabych lub niezabezpieczonych haseł.haseł

Logowanie i audyt

- Pełna rejestracja wszystkich zdarzeń dostępu oraz działań wykonywanych w systemie.
- Niezmienialne logi audytowe z możliwością eksportu, wspierające procesy audytowe.

Reagowanie na incydenty i zabezpieczenie dostępu

- Szczegółowa dokumentacja wszystkich zdarzeń dostępu oraz aktywności systemu
- Zabezpieczone przed modyfikacją logi audytowe z funkcją eksportu wspierającą audyty i procesy zgodności

Zapewnienie ciągłości działania i kopie zapasowe danych

- Zautomatyzowany proces tworzenia kopii zapasowych danych
- Plan odtworzenia systemu po awarii oraz mechanizmy zapewniające redundancję.

Zarządzanie lukami oraz proces aktualizacji

- Stały monitoring przez producenta znanych luk bezpieczeństwa w oprogramowaniu (CVE)
- Regularne,podpisane cyfrowo i zweryfikowane aktualizacje.

Ochrona danych i bezpieczeństwo informacji

- Podejście Privacy by Design oraz zgodności z RODO
- Możliwość usuwania danych osobowych
- Elastyczna konfiguracja mechanizmów logowania
- Zasada podwójnej kontroli przy dostępie do logów.

Produkty EVVA jako odpowiedź na wymagania regulacyjne

Xesar

System kontroli dostępu spełniający najwyższe wymagania w zakresie bezpieczeństwa

Kontrola dostępu i IT

- Uprawnienia dostępu przypisane do ról dla osób lub grup
- MIFARE DESFire EV1/EV2/EV3 (EAL5+) oraz indywidualne dla systemu klucze AES
- Szyfrowana komunikacja typu „challenge-response" (brak protokołów w postaci jawnego tekstu)
- Protokół TLS ≥ 1.2 do komunikacji systemowej
- Wewnętrzne szyfrowanie AES 256-bit
- Hasła zabezpieczone poprzez haszowanie (Bcrypt).

Logi dostępu i zdarzeń systemowych

- Pełne i zabezpieczone przed modyfikacją logi dostępu i systemowe
- Eksport danych zgodny z wymogami audytowymi
- Stała możliwość przeprowadzania audytu, kontroli zgodności oraz obsługi incydentów.

Reagowanie na incydenty i odporność

- Blokowanie w czasie rzeczywistym (online), listy blokad dla elementów pracujących w trybie offline
- Mechanizmy ostrzegania w przypadku niebezpiecznego statusu blokady
- Niezależna praca w trybie offline w przypadku awarii systemu IT lub sieci.

Aktualizacje i zarządzanie lukami w zabezpieczeniach

- Ciągłe monitorowanie podatności CVE
- Aktualizacje podpisane kryptograficznie (RSA/SHA-256, AES-256 CCM)
- Zweryfikowane aktualizacje oprogramowania i firmware.

Zapewnienie ciągłości działania

- Szyfrowane kopie zapasowe
- Odtwarzanie systemu po awarii na podstawie dokumentacji bezpieczeństwa systemu
- Możliwość pracy wielożytkownikowej oraz całodobowej pracy serwera (24/7)

Ochrona prywatności i danych

- Zastosowanie zasady Privacy by Design
- Aplikacja nie przechowuje danych osobowych
- Możliwość skonfigurowania automatycznego usuwania danych umożliwiających identyfikację osób

AirKey

Mobilne rozwiązanie w zakresie kontroli dostępu spełniające najwyższe standardy

Bezpieczeństwo fizyczne i informatyczne

- Bezpieczeństwo fizyczne i informatyczne
- Nośniki dostępu oparte na smartfonach i technologii RFID (JCOP SmartMX3, EAL6+)
- Uwierzytelnianie z ECDSA-256 oraz kluczami AES
- Zarządzanie online zabezpieczone protokołem TLS

Logi dostępu i zdarzeń systemowych

- Rejestrowanie zdarzeń na potrzeby audytów
- Eksport logów zgodny z wymaganiami audytowymi
- Automatyczna aktualizacja list blokad i dzienników zdarzeń
- Elastyczna konfiguracja zgodna z przepisami o ochronie danych

Reagowanie na incydenty i odporność

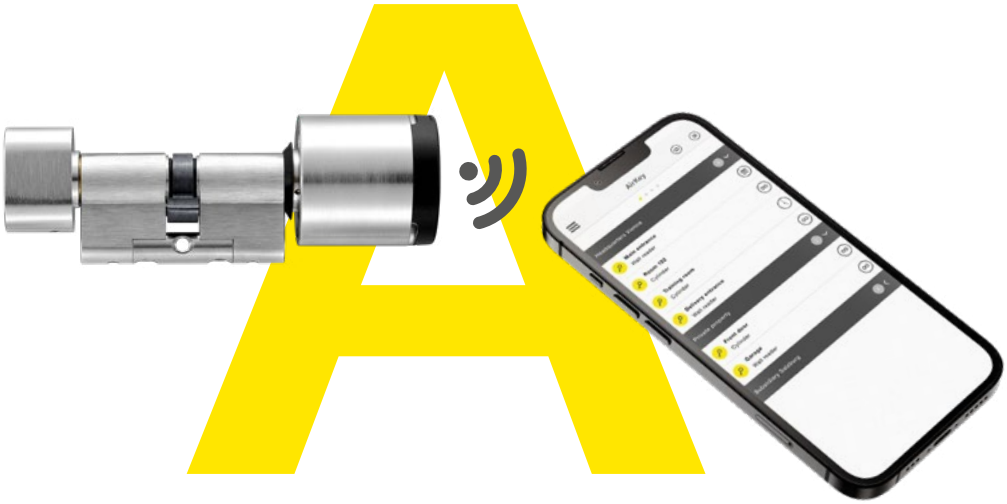
- Blokowanie dostępu w czasie rzeczywistym przez Internet
- Zachowanie funkcjonalności drzwi w trybie offline nawet podczas awarii serwera
- Automatyczne alerty w przypadku wykrycia stanów zagrażających bezpieczeństwu

Aktualizacje i utrzymanie systemu

- Centralne zarządzanie podpisanymi cyfrowo aktualizacjami
- Dane przetwarzane w centrach danych w Austrii posiadających certyfikat ISO 27001
- Redundantne serwery EVVA oraz klucze kryptograficzne chronione przez sprzętowe moduły bezpieczeństwa (HSM)

Ochrona prywatności i danych

- Mechanizmy usuwania danych zgodne z RODO
- Zastosowanie zasady Privacy by Design
- Możliwość włączenia zasady czterech oczu przy dostępie do logów

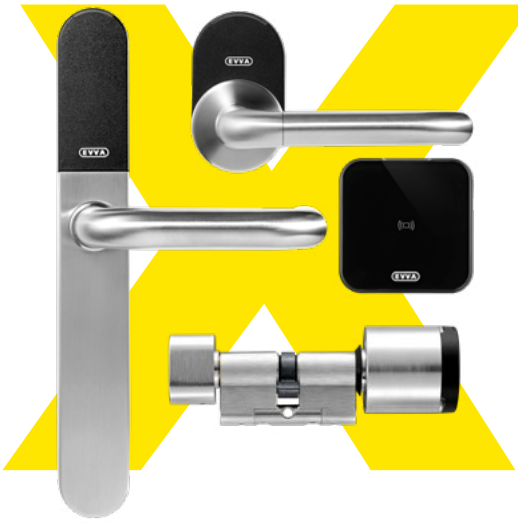


ZGODNOŚĆ ZE STANDARDAMI I STATUS CERTYFIKACJI

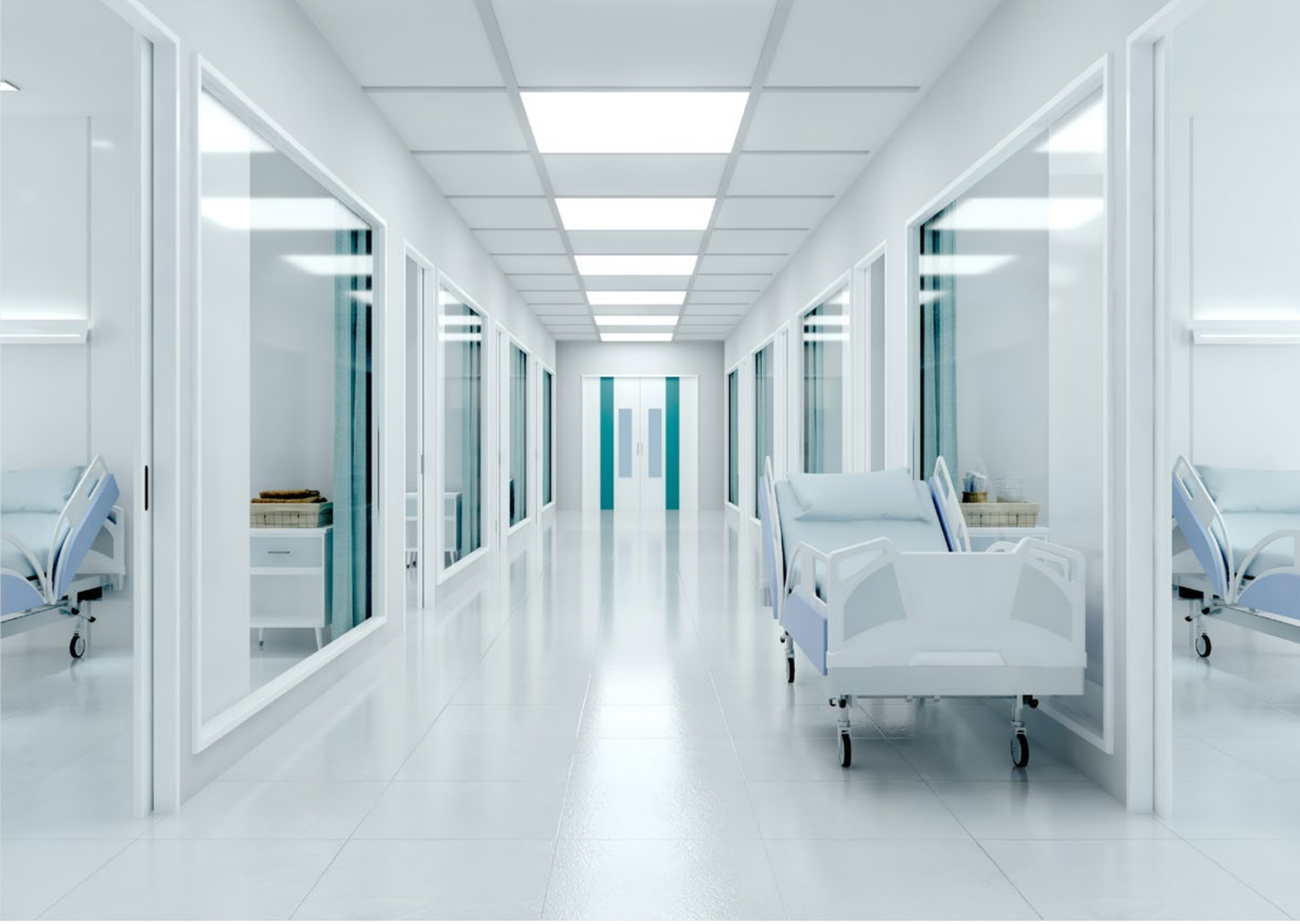
Pomyślna
ocena
zgodności(TÜV)

EN 18031-1

SPEŁNIA WYMAGANIA RED*



*RED: Dyrektywa w sprawie urządzeń radiowych



Praktyczny przykład 1:

System kontroli dostępu w szpitalu

Znaczenie dla NIS2/CER

Sytuacja wyjściowa

Szpital jest jednym z „podmiotów kluczowych" objętych dyrektywą NIS2 i musi spełniać wysokie wymagania dotyczące bezpieczeństwa cybernetycznego oraz ochrony. Obszary o szczególnym znaczeniu, takie jak pomieszczenia serwerowe, magazyny leków czy oddziały intensywnej terapii, wymagają skutecznej ochrony przed dostępem osób nieuprawnionych.

Rozwiązanie z wykorzystaniem Xesar

- Zarządzanie uprawnieniami dostępu w oparciu o role dla różnych grup użytkowników (np. IT, utrzymanie techniczne, administracja)
- Bezpieczne nośniki dostępu oparte na technologiach kryptograficznych (MIFARE DESFire EV3)
- Kompleksowa rejestracja zdarzeń dostępu oraz zabezpieczone przed modyfikacją logi audytowe wspierające procesy kontroli i zgodności
- Natychmiastowe blokowanie utraconych nośników dzięki listom blokad aktualizowanym w czasie rzeczywistym
- Zachowanie funkcjonalności drzwi w trybie offline w przypadku awarii serwera, zapewniające ciągłość działania
- Regularne aktualizacje oprogramowania z podpisem cyfrowym oraz proces zarządzania podatnościami

Wartość dodana

Szpital wdraża środki ochrony oparte na ocenie ryzyka, zapewnia pełną identyfikowalność i dokumentację incydentów na potrzeby audytów, wzmacniając tym samym odporność obiektu na różne zagrożenia.

Praktyczny przykład 2:

Produkcja dla sektora infrastruktury krytycznej

Łańcuch dostaw ma znaczenie dla CER

Sytuacja wyjściowa

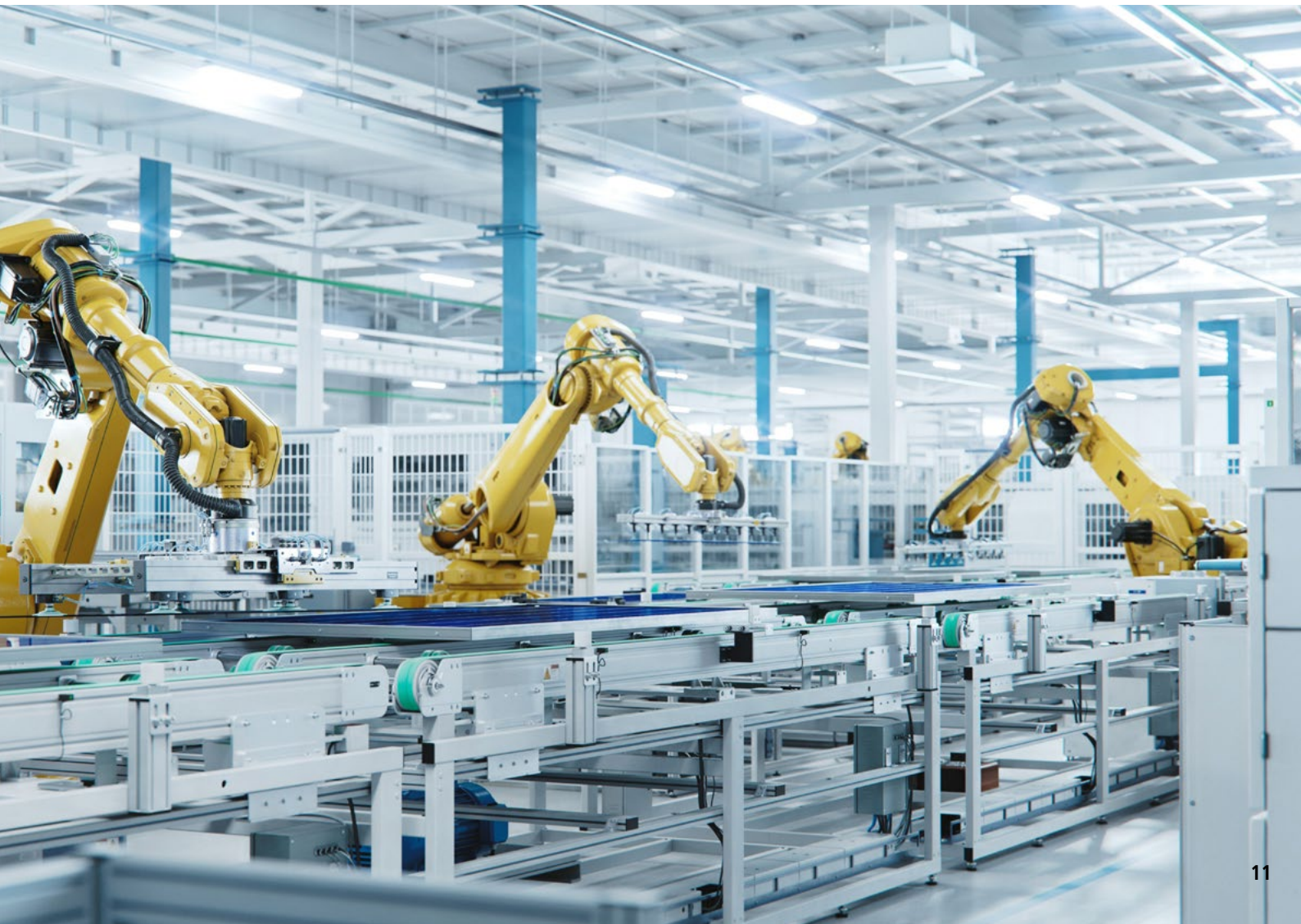
Średniej wielkości producent maszyn, będący dostawcą dla sektora energetycznego, podlega pośrednio wymaganiom wynikającym z dyrektywy CER. Przedsiębiorstwo musi zapewnić, że stosowane systemy kontroli dostępu oraz infrastruktura informatyczna charakteryzują się odpowiednią odpornością i poziomem bezpieczeństwa.

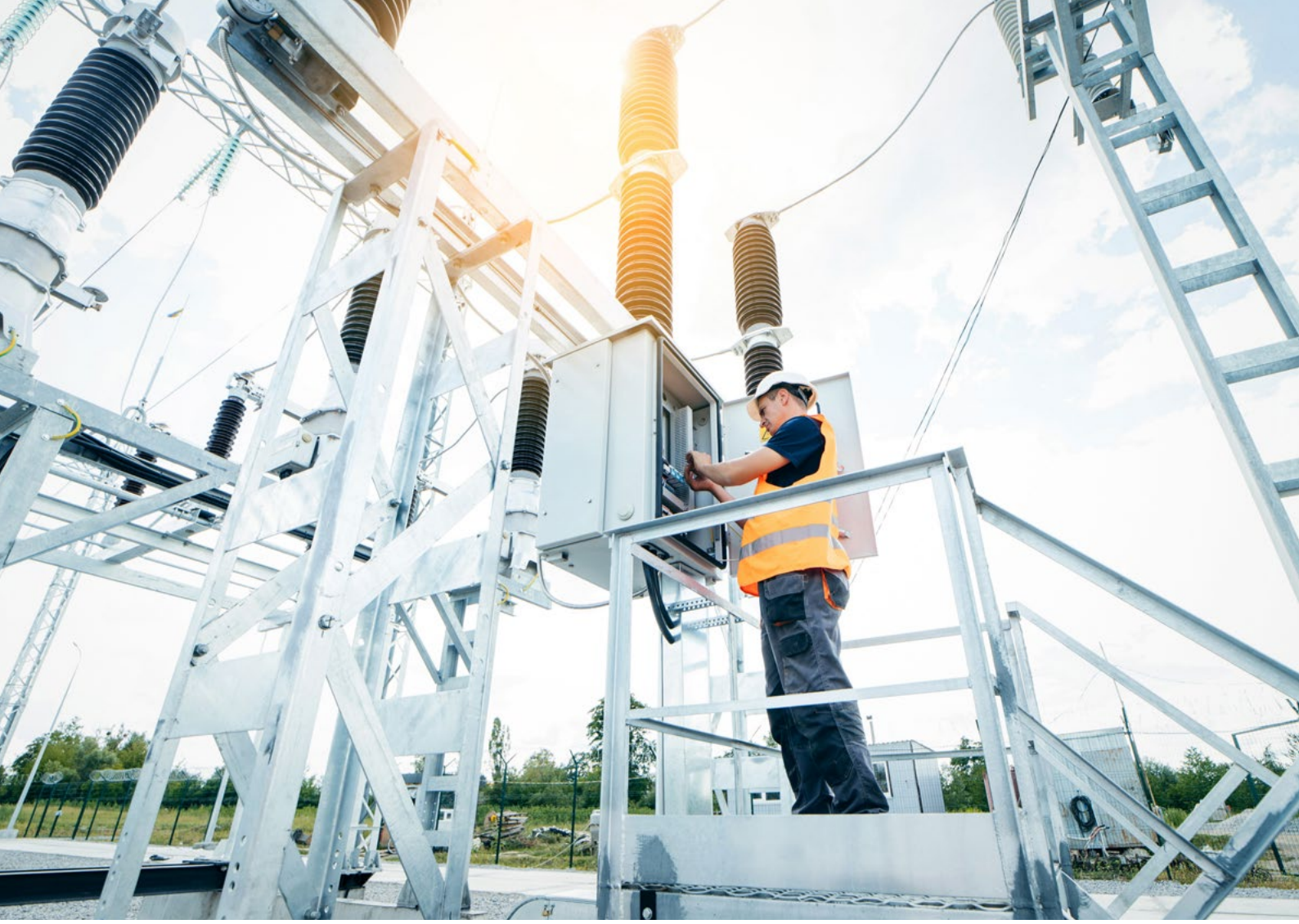
Rozwiązanie z wykorzystaniem AirKey

- Centralne zarządzanie uprawnieniami dostępu, obejmujące również dla zewnętrznych dostawców usług (np. personel techniczny)
- Bezpieczna aplikacja parta na chmurze
- Nośniki dostępu (smartfony, RFID) wykorzystujące zaawansowane mechanizmy szyfrowania (ECDSA-256, AES-128)
- Rejestrowanie wszystkich wejść, eksport danych na potrzeby audytów
- Mechanizmy usuwania danych zgodne z RODO oraz podejście Privacy by Design
- Centralne zarządzanie aktualizacjami i procesem obsługi podatności przez EVVA.

Wartość dodana

Przedsiębiorstwo może potwierdzić swoim klientom wdrożenie odpowiednich środków ochrony dostępu, które wspierają bezpieczeństwo całego łańcucha dostaw, a także zapewniają gotowość do przeprowadzania audytów i uzyskiwania wymaganych certyfikacji.





Praktyczny przykład 3:

Zarządzanie kryzysowe i odporność samorządu lokalnego

CER-istotne

Sytuacja wyjściowa

Jednostka samorządu lokalnego odpowiada za funkcjonowanie infrastruktury krytycznej (np. obiektów wodociągowych i oczyszczalni ścieków) oraz musi zagwarantować utrzymanie dostępu do kluczowych stref również w sytuacjach kryzysowych, takich jak cyberatak lub awaria zasilania.

Rozwiązanie z wykorzystaniem Xesar

- Utrzymanie pełnej funkcjonalności w trybie offline w przypadku awarii zasilania lub cyberataku
- Natychmiastowe blokowanie przejętych lub zagrożonych nośników dostępu oraz alerty dotyczące niezrealizowanych zadań bezpieczeństwa
- Mechanizmy tworzenia kopii zapasowych i odtwarzania konfiguracji systemu.

Wartość dodana

Władze miejskie zachowują zdolność do działania nawet w sytuacji kryzysowej – mieszkańcy i lokalne przedsiębiorstwa nie odczuwają skutków awarii i zakłóceń.

Praktyczny przykład 4:

Ochrona danych i rejestrowanie zdarzeń w instytucie badawczym

Znaczenie dla NIS2/CER

Sytuacja wyjściowa

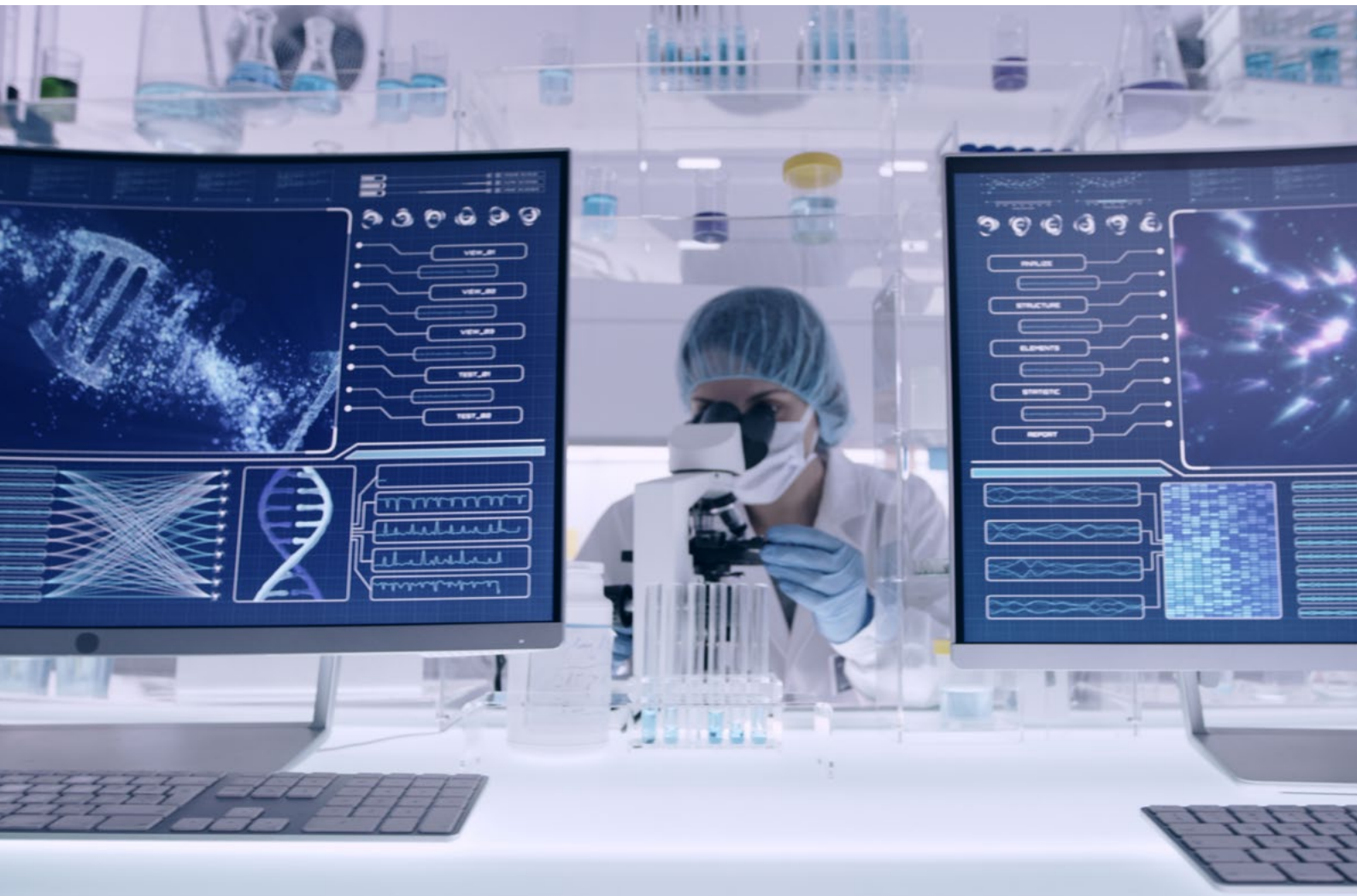
Instytut badawczy przetwarza dane osobowe o szczególnym znaczeniu i jest zobowiązany do zapewnienia zgodności z wymaganiami RODO oraz NIS2.

Rozwiązanie z wykorzystaniem AirKey

- Ochrona danych zgodnie z zasadą Privacy by Design: brak przechowywania danych osobowych w warstwie backendowej systemu
- Elastycznie konfigurowane logowanie oraz funkcje usuwania danych identyfikujących użytkowników
- Rozwiązanie wdrożone zgodnie z wymaganiami RODO

Wartość dodana

Instytut może w dowolnym momencie udokumentować zgodność z wymaganiami dotyczącymi ochrony danych oraz zapewnić przejrzystość działań wobec organów nadzorczych i partnerów.



Lista kontrolna dla operatorów infrastruktury krytycznej

1. Organizacyjne ramy bezpieczeństwa

- Czy jest stworzona aktualna koncepcja bezpieczeństwa, obejmująca ochronę danej organizacji?
- Czy role, uprawnienia oraz struktury odpowiedzialności w obszarach bezpieczeństwa, IT i zarządzania obiektami są jasno zdefiniowane dla obszarów istotnych z punktu widzenia infrastruktury krytycznej?
- Czy wytyczne i procesy dotyczące bezpieczeństwa są regularnie weryfikowane i aktualizowane?
- Czy istnieje proces zapewniający realizację obowiązków raportowania incydentów bezpieczeństwa?

2. Analiza ryzyka i zgodność z przepisami

- Czy w ciągu ostatnich 4 lat przeprowadzono ocenę ryzyka zgodnie z wymaganiami ustawy o ochronie infrastruktury krytycznej / dyrektywy CER?
- Czy zidentyfikowano wszystkie podatności fizyczne i cyfrowe w całym łańcuchu procesów?
- Czy rozwiązania kontroli dostępu są odpowiednio dostosowane do wymagań NIS2, w szczególności w zakresie bezpiecznych protokołów komunikacyjnych oraz ochrony przed manipulacją?
- Czy stosowane są wyłącznie systemy i technologie zgodne z aktualnym stanem techniki (bez niezabezpieczonych protokołów, takich jak Wiegand)?

3. Zarządzanie uprawnieniami dostępu

- Czy wszystkie uprawnienia dostępu są zarządzane zgodnie z zasadą dostępu opartego na rolach i przypisane do konkretnych użytkowników?
- Czy uprawnienia dostępu są regularnie weryfikowane i potwierdzane lub automatycznie odbierane, gdy nie są już wymagane?
- Czy wdrożono jasno zdefiniowane procesy nadawania dostępu, zmiany zakresu uprawnień oraz jego odbierania pracownikom i zewnętrznym usługodawcom?

4. Techniczne bezpieczeństwo systemu kontroli dostępu

- Czy wszystkie czytniki, karty i nośniki wykorzystywane w systemie kontroli dostępu są zabezpieczone szyfrowaniem?
- Czy wszystkie drzwi do stref o znaczeniu krytycznym, pomieszczenia serwerowe oraz centra sterowania są zabezpieczone elektronicznymi systemami kontroli dostępu?
- Czy dane istotne z punktu widzenia bezpieczeństwa (np. logi) są przechowywane w sposób zapewniający ich odporność na manipulację oraz możliwość wykorzystania podczas audytów?

5. Monitorowanie, rejestrowanie i przejrzystość

- Czy wszystkie zdarzenia oraz próby uzyskania dostępu są automatycznie rejestrowane?
- Czy logi systemu są zabezpieczone przed manipulacją, spełniają wymagania audytowe oraz są przechowywane przez wymagany okres?
- Czy korzystamy z narzędzi monitorujących, które umożliwiają powiązanie zdarzeń z zakresu kontroli dostępu i cyberbezpieczeństwa?

6. Ochrona obszarów o znaczeniu krytycznym

- Czy obszary takie jak serwerownie, centra sterowania, obiekty energetyczne i infrastruktury technicznej oraz rozdzielnie elektryczne są objęte szczególnymi środkami ochrony?
- Czy wdrożono wielopoziomowe strefy dostępu o zróżnicowanym poziomie zabezpieczeń?
- Czy pomieszczenia o podwyższonym znaczeniu są dodatkowo chronione za pomocą monitoringu wizyjnego, monitorowania stanu drzwi lub systemów alarmowych?
- Czy stworzono plan zapewnienia dostępu awaryjnego (np. w przypadku przerwy w dostawie zasilania lub awarii systemu)?przypadku awarii zasilania lub usterki systemu)?

7. Dostawcy i usługodawcy

- Czy firmy zewnętrzne i usługodawcy posiadają wyłącznie czasowe i jasno określone uprawnienia dostępu?
- Czy dostęp pracowników tymczasowych i zewnętrznych jest odpowiednio ograniczony technicznie oraz ściśle nadzorowany?
- Czy korzystanie z zewnętrznych punktów dostępu jest regularnie poddawane audytom?

8. Reagowanie w sytuacjach awaryjnych

- Czy organizacja posiada plan reagowania na sytuacje awaryjne i kryzysowe uwzględniający system kontroli dostępu?
- Czy zostały opracowane procedury dotyczące:
  - natychmiastowego odbierania uprawnień dostępu wybranym pracownikom lub grupom
  - szybkiego odtworzenia funkcjonowania systemu kontroli dostępu po ataku lub awarii
  - postępowania na wypadek ewakuacji i innych incydentów?
- Czy procedury te są regularnie testowane podczas ćwiczeń?

9. Szkolenia i świadomość bezpieczeństwa

- Czy wszyscy pracownicy przeszli szkolenie z zakresu korzystania z nośników dostępu?
- Czy istnieje stały program budowania świadomości w zakresie wytycznych bezpieczeństwa i właściwych zachowań?
- Czy pracownicy znają procedury zgłaszania podejrzanych incydentów?

10. Rozwój i gotowość na przyszłe wymagania

- Czy rozwiązanie do kontroli dostępu jest skalowalne i umożliwia objęcie nowych lokalizacji oraz spełnienie przyszłych wymagań?
- Czy można bez problemu wdrażać nowe standardy bezpieczeństwa (aktualizacje NIS2, wytyczne BSI czy zmiany w przepisach)?
- Czy stworzono plan modernizacji systemu na wypadek, gdyby technologie stały się przestarzałe lub wykryto luki w zabezpieczeniach?

NIS2 i CER są wdrażane w poszczególnych państwach członkowskich UE na podstawie następujących krajowych aktów prawnych.

	NIS2	CER
Austria	NISG2026 (Ustawa o bezpieczeństwie sieci i informacji z 2026 r.)	RKEG (Ustawa o odporności infrastruktury krytycznej)
Niemcy	NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)	KRITIS-Dachgesetz (Ustawa o wzmocnieniu odporności fizycznej obiektów o znaczeniu krytycznym)
Belgia	Loi NIS2 (Ustawa z dnia 26 kwietnia 2024 r. o cyberbezpieczeństwie sieci i systemów informatycznych)	Loi relative à la résilience des entités critiques (krajowa ustawa o wdrożeniu systemu CER, 2025/26)
Holandia	Cyberbeveiligingswet (w trakcie wdrażania na szczeblu parlamentarnym, stan na kwiecień 2026 r.)	Wet weerbaarheid kritieke entiteiten (projekt ustawy o CER, stan na kwiecień 2026 r.)
Szwecja	Cybersäkerhetslagen (Cybersecurity Act, SFS 2025:1506)	Lag om motståndskraft hos kritiska verksamheter (Wdrażanie CER w przygotowaniu, stan na kwiecień 2026 r.)
Włochy	Decreto Legislativo n. 138/2024	Decreto Legislativo n. 134/2024
Czechy	Zákon o kybernetické bezpečnosti (nowelizacja/nowa wersja dotycząca wdrożenia dyrektywy NIS2)	Zákon o odolnosti kritických subjektů (Ustawa o wdrożeniu CER)
Polska	Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC)	Dyrektywa w sprawie odporności podmiotów krytycznych
Słowacja	Zákon o kybernetickej bezpečnosti (NIS2-Novelle)	Zákon o odolnosti kritických subjektov

www.evva.com

I.ALLG.NIS2-CER.ID.WHPAP.SPL.LN | 26R1