Chmura czy rozwiązania on-premise w systemach kontroli dostępu

Jak dyrektywa NIS2 zmienia reguły gry w zabezpieczeniach fizycznych

Europejski krajobraz bezpieczeństwa fizycznego przechodzi fundamentalną transformację. Dyrektywa NIS2, najbardziej kompleksowe prawodawstwo dotyczące cyberbezpieczeństwa w historii UE, wymusza na organizacjach rewizję dotychczasowych podejść do kontroli dostępu fizycznego. W obliczu kar sięgających 10 mln euro lub 2% globalnego rocznego obrotu wybór między rozwiązaniami chmurowymi a lokalnymi przestaje być jedynie decyzją technologiczną – staje się kwestią strategicznego zarządzania ryzykiem regulacyjnym.

Jan T. Grusznic

NIS2: Nowa era wymagań dla systemów bezpieczeństwa

Dyrektywa NIS2, która weszła w życie w styczniu 2023 roku, objęła swoim zakresem 18 sektorów krytycznych w całej Unii Europejskiej. W przeciwieństwie do swojego poprzednika NIS2 nie ogranicza się wyłącznie do cyberbezpieczeństwa w wymiarze cyfrowym. Wyraźnie wymaga podejścia uwzględniającego wszystkie zagrożenia, chroniącego zarówno systemy sieciowe, jak i ich środowisko fizyczne.

Artykuł 21 ust. 2 dyrektywy nie pozostawia miejsca na interpretację. Organizacje muszą:

- zapobiegać nieautoryzowanemu dostępowi fizycznemu do obiektów,
- wdrażać uwierzytelnianie wieloskładnikowe (MFA), tam gdzie jest to możliwe,
- prowadzić kompleksowe dzienniki audytu,
- chronić fizyczne lokalizacje przechowujące krytyczną infrastrukturę IT.

W kontekście systemów kontroli dostępu (SKD) oznacza to konieczność sformalizowania polityk, stosowania silnego uwierzytelniania dla kont administratorów oraz zabezpieczenia łańcucha dostaw poprzez weryfikację standardów bezpieczeństwa u dostawców systemów. Na ten ostatni aspekt zwraca uwagę Przemysław Kaźmierczak, kierownik ds. produktu / Dział Wsparcia Technicznego w C&C Partners, podkreślając zmianę roli producentów i dostawców:

– Nie są oni już tylko dostarczycielami sprzętu, ale partnerami dbającymi o realną odporność organizacji. W praktyce oznacza to oferowanie i dostarczanie rozwiązań niepochodzących od podmiotów wysokiego ryzyka (tzw. high-risk vendors). Istotne jest, aby unikać wyboru rozwiązań, co do których istnieją wątpliwości w kontekście bezpieczeństwa łańcucha dostaw.

Rynek stawia na chmurę

Dane branżowe pokazują, że 70% organizacji planuje przyjąć usługi chmurowe w obszarze kontroli dostępu. To nie tylko trend technologiczny – to strategiczna odpowiedź na złożoność regulacyjną i rosnące wymagania operacyjne.

Bartłomiej Zadumiński, kierownik Działu Wsparcia i Rozwoju Oprogramowania w Unicard Systems, zauważa, że *za takim krokiem stoi zazwyczaj kombinacja kilku równie ważnych czynników: automatyzacja procesów, bezpieczeństwo, elastyczność, redukcja kosztów operacyjnych oraz usprawnienie integracji. To aspekty, które razem tworzą silną motywację do zmiany.*

Przyznaje też, że coraz częściej decydującym impulsem są zmiany legislacyjne, takie jak ustawa o Krajowym Systemie Cyberbezpieczeństwa czy obowiązki wynikające z dyrektywy NIS2, wymuszające wdrożenie rozwiązań zapewniających kontrolę nad dostępem, lepszą audytowalność i natychmiastową reakcję na incydenty.

– Właśnie w odpowiedzi na te wyzwania przygotowaliśmy dedykowane narzędzia migracyjne, które pozwalają na płynne i bezpieczne przejście z tradycyjnych rozwiązań lokalnych do modelu chmurowego bez przestojów i z pełnym wsparciem technicznym – dodaje.

Przejście do środowiska chmurowego nie jest już jedynie kwestią optymalizacji kosztów IT, ale strategicznym wyborem warunkującym zdolność organizacji do spełnienia rygorystycznych wymogów prawnych oraz integracji nowoczesnych, wirtualnych poświadczeń mobilnych.

Automatyzacja zgodności z przepisami

Wymogi sprawozdawcze NIS2 dotyczące incydentów są niezwykle rygorystyczne:

- wczesne ostrzeżenie w ciągu 24 godzin od wykrycia incydentu,
- szczegółowy raport w ciągu 72 godzin,
- końcowy, kompleksowy raport w ciągu miesiąca.

Dotrzymanie tych terminów przy dziennikach dostępu rozproszonych na wielu lokalnych serwerach, wymagających ręcznej kompilacji, jest praktycznie niemożliwe.

Chmurowe systemy SKD automatycznie generują dokumentację zgodności, centralizują dzienniki dostępu ze wszystkich obiektów i zapewniają możliwość raportowania w czasie rzeczywistym. Jedno kliknięcie pozwala wyeksportować wszystko, czego wymagają regulatorzy: dzienniki wejść i wyjść z oznaczeniem czasu, nieudane próby dostępu, zdarzenia wymuszonych drzwi oraz pełną dokumentację cyklu życia kart – od wydania po dezaktywację.

Ilustracja: A&S AI Studio

TAB. 1. Harmonogram raportowania zgodnie z NIS2

Termin	Rodzaj dokumentu	Wymagana zawartość
Do 24 godzin	Wczesne ostrzeżenie	Informacja o poważnym charakterze incydentu i skutkach transgranicznych
Do 72 godzin	Pełny raport	Opis incydentu, jego dotkliwość, skutki i podjęte środki zaradcze
Po 1 miesiącu	Raport końcowy	Szczegółowa analiza przyczyn, kroki naprawcze i długofalowe wnioski

– Potrzeby w zakresie raportowania są zwykle definiowane już na etapie wdrożenia systemu i dostosowywane do profilu działalności oraz polityki bezpieczeństwa organizacji – podkreśla Bartłomiej Zadumiński z Unicard Systems i dodaje, że *częstą praktyką jest wykorzystywanie raportów w sposób cykliczny, zwłaszcza na potrzeby audytów oraz zgodności z regulacjami wewnętrznymi i zewnętrznymi. Z tego względu funkcja automatycznej dystrybucji raportów w określonych interwałach czasowych cieszy się dużym zainteresowaniem klientów.*

Najwyższe standardy bezpieczeństwa

Niewiele organizacji może dorównać poziomowi zabezpieczeń oferowanemu przez profesjonalnych dostawców chmury. Szyfrowanie klasy korporacyjnej, całodobowe monitorowanie bezpieczeństwa, regularne aktualizacje i zaawansowane wykrywanie zagrożeń wymagają zasobów, których większość firm nie jest w stanie uzasadnić ekonomicznie.

Dostawcy chmury oferują:

- geograficznie redundantne przechowywanie danych w wielu centrach danych,
- automatyczne systemy tworzenia kopii zapasowych,
- gwarancje czasu pracy na poziomie 99,9%+,
- pełną funkcjonalność podczas utraty łączności internetowej.

Przemysław Kaźmierczak z firmy C&C Partners podkreśla, że nowoczesne systemy kontroli dostępu oparte na chmurze utrzymują pełną funkcjonalność podczas awarii Internetu, o ile kontrolery lokalne są zdolne do realizacji 100% funkcjonalności w trybie offline. Dodaje przy tym, że lokalna inteligencja kontrolerów nie może w żaden sposób ograniczać funkcjonowania obiektu w przypadku braku dostępu do Internetu. Każde zdarzenie musi zostać zbuforowane, aby później możliwa była jego pełna synchronizacja z bazą danych w chmurze.

TAB. 2. Porównanie rozwiązań on-premise i chmurowych

Kategoria	On-Premise	Cloud (SaaS)	Korzyść biznesowa
Model finansowy	Wysoki CAPEX (sprzęt, licencje)	Elastyczny OPEX (subskrypcja)	Lepsza przewidywalność budżetu
Utrzymanie	Ręczne aktualizacje, konserwacja	Automatyczne aktualizacje w czasie rzeczywistym	Redukcja obciążenia działów IT
Dostępność	Ograniczona do sieci lokalnej/VPN	Globalny dostęp przez przeglądarkę/aplikację	Możliwość pracy zdalnej administratorów
Integracja	Często ograniczone API, silosy	Natywne integracje REST API	Spójny ekosystem HR i IT
Bezpieczeństwo	Zależne od lokalnych standardów	Najwyższe standardy centrów danych	Większa odporność na awarie i ataki

Integracja i zaawansowane funkcje

Kontrola dostępu fizycznego nie funkcjonuje w próżni. Nowoczesne ekosystemy bezpieczeństwa wymagają bezproblemowej integracji z systemami zarządzania wideo, platformami do zarządzania gośćmi, systemami zarządzania tożsamością i dostępem (IAM), bazami danych HR, systemami alarmowymi oraz platformami zarządzania budynkami (BMS).

Platformy chmurowe zazwyczaj oferują szersze możliwości integracyjne dzięki standardowym interfejsom API RESTful. Są projektowane z myślą o łączności i interoperacyjności. Systemy on-premise często wymagają pracy z zastrzeżonymi protokołami, ograniczoną dokumentacją oraz realizacji projektów integracyjnych rozciągających się na wiele miesięcy.

Zaawansowane platformy chmurowe oferują obecnie:

- analizę behawioralną opartą na AI do wykrywania anomalii,
- predykcyjne analizy zagrożeń w obszarze bezpieczeństwa,
- analizę wzorców dostępu,
- powiadomienia w czasie rzeczywistym o nieautoryzowanych próbach.

– Zdajemy sobie sprawę, że to dyrektywa CER w dużym stopniu kształtuje wymagania dotyczące ochrony fizycznej infrastruktury krytycznej. Jednocześnie, zgodnie z unijnymi zaleceniami, przepisy CER i NIS2 należy wdrażać w sposób skoordynowany, ponieważ tworzą spójne ramy organizacyjne dla systemów bezpieczeństwa w wymiarze fizycznym oraz cyfrowym – mówi Bartłomiej Zadumiński.

– W praktyce oznacza to wsparcie zarówno technologiczne, jak i merytoryczne. Od strony systemowej oferujemy m.in. mechanizmy kontroli uprawnień, kompletną rejestrację zdarzeń i aktywności użytkowników, integrację z rozwiązaniami klasy SIEM, a także dostęp do szczegółowych logów umożliwiających sprawną analizę incydentów i przygotowanie się do audytu – dodaje.

Rewolucja mobilna: wirtualne identyfikatory

Wypieranie fizycznych kart plastikowych przez wirtualne identyfikatory w smartfonach i urządzeniach ubieralnych to jeden z najsilniejszych trendów rynkowych. W 2024 roku blisko 80% organizacji w USA wdrażało lub planowało wdrożenie mobilnych poświadczeń. Trend ten jest równie widoczny w Europie.

Popularność tego rozwiązania wynika z faktu, że użytkownicy rzadziej zapominają lub pożyczają telefon niż kartę plastikową, co samo w sobie podnosi poziom bezpieczeństwa. Technologie mobilne w systemach SKD opierają się na dwóch standardach:

- NFC *(Near Field Communication)* – zapewnia interakcję zbliżeniową (do kilku centymetrów), idealną w przypadku drzwi o dużym natężeniu ruchu,
- BLE *(Bluetooth Low Energy)* – umożliwia dostęp z odległości kilku metrów, pozwalając na realizację funkcji *hands-free*.

Centralne zarządzanie infrastrukturą rozproszoną

Dla organizacji posiadających infrastrukturę rozproszoną – takich jak sieci placówek bankowych, punkty logistyczne czy biura międzynarodowe – centralizacja zarządzania uprawnieniami w chmurze jest warunkiem koniecznym do utrzymania spójnej polityki bezpieczeństwa.

W tradycyjnych modelach każda lokalizacja funkcjonowała jako izolowana „wyspa", co utrudniało szybkie wycofywanie poświadczeń w skali całej firmy. Chmurowy system SKD tworzy jeden, spójny ekosystem danych, w którym każda zmiana uprawnień wprowadzona w centrali jest natychmiast propagowana do wszystkich kontrolerów w sieci.

Centralny monitoring umożliwia wykrywanie anomalii wykraczających poza pojedynczą lokalizację, takich jak próba użycia tego samego poświadczenia w dwóch odległych miejscach w krótkim czasie – klasyczny sygnał naruszenia bezpieczeństwa.

Wymagania techniczne: standard OSDP

Wytyczne ENISA wskazują, że fizyczna kontrola dostępu musi być zintegrowana z polityką bezpieczeństwa sieci i systemów informatycznych. Konieczne jest monitorowanie nie tylko samych przejść, ale również stanu urządzeń brzegowych – czytników i kontrolerów.

– Dostawcy odgrywają krytyczną rolę w edukowaniu klientów i uświadamianiu im konieczności stosowania bezpiecznych i odpornych na ataki rozwiązań – zauważa Przemysław Kaźmierczak z C&C Partners i podaje przykład:

– W systemach kontroli dostępu kluczowy jest wybór standardu kart dostępowych. Powinien to być w pełni bezpieczny i – najlepiej – otwarty standard (np. MIFARE DESFire EV3 czy najnowszy MIFARE DUOX). Dostawca powinien nie tylko pomóc w doborze technologii kart, ale także wspierać klienta w ich prawidłowym zabezpieczeniu przy użyciu własnych, unikatowych kluczy kryptograficznych.

TAB. 3. Identyfikatory wirtualne vs. tradycyjne karty

Funkcjonalność	ID wirtualny (NFC/BLE)	Karta plastikowa	Korzyść operacyjna
Uwierzytelnianie	Biometria telefonu (Face ID/PIN)	Brak zabezpieczenia nośnika	Skuteczne MFA w jednym urządzeniu
Logistyka	Wydawanie zdalne (e-mail/cloud)	Druk, personalizacja, wysyłka	Oszczędność czasu i kosztów
Ekologia	Zerowy ślad węglowy plastiku	Produkcja i utylizacja PVC	Realizacja celów zrównoważonego rozwoju
Elastyczność	Wiele kluczy w jednej aplikacji	Konieczność noszenia pęku kart	Wyższy komfort użytkownika
Bezpieczeństwo	Szyfrowanie AES-128/256	Podatność na klonowanie (starsze karty)	Ochrona przed nieuprawnionym kopiowaniem

Według Przemysława Kaźmierczaka samo zabezpieczenie karty to tylko połowa sukcesu. *– NIS2 wymaga ochrony danych na każdym etapie ich przesyłu. Dlatego wdrożenie standardu OSDP (Open Supervised Device Protocol) w wersji 2.2 jest w tym kontekście kluczowe. Zapewnia on szyfrowanie komunikacji AES-128 oraz ciągły nadzór nad stanem okablowania i urządzeń, eliminując podatności klasycznego protokołu Wiegand na ataki typu sniffer.*

Technologia Energy Harvesting: bezpieczeństwo bez kabli i baterii

Poważnym wyzwaniem dla systemów SKD w infrastrukturze rozproszonej są punkty, do których doprowadzenie zasilania jest niemożliwe lub zbyt kosztowne – szafy teletechniczne, bramy w terenie otwartym, kłódki na kontenerach czy zamki w zabytkowych drzwiach.

Rozwiązaniem są systemy elektroniczne offline wykorzystujące technologię Energy Harvesting, czyli pozyskiwanie energii z otoczenia lub bezpośrednio od użytkownika:

- **Indukcja z telefonu** ***(NFC Power Harvesting)*** – zamek nie posiada wewnętrznej baterii. Energia potrzebna do odblokowania mechanizmu jest przesyłana bezprzewodowo ze smartfona użytkownika za pośrednictwem pola NFC w momencie zbliżenia urządzenia. Pobór energii wynosi mniej niż 1% pojemności baterii telefonu.
- **Energia kinetyczna** ***(Kinetic Energy Harvesting)*** – w systemach opartych na inteligentnych kluczach energia elektryczna jest generowana przez mikroprądnicę podczas fizycznego wsuwania klucza do cylindra zamka. Krótki ruch wystarcza do przeprowadzenia uwierzytelnienia cyfrowego i otwarcia zamka.

Rozwiązania offline mogą być w pełni zintegrowane z chmurowym systemem zarządzania dzięki koncepcji „Smartphone-as-a-Gateway". W momencie otwarcia zamka za pomocą aplikacji telefon synchronizuje dane między zamkiem a chmurą, przekazując listy zablokowanych kluczy oraz pobierając ścieżki audytu.

Cyberbezpieczeństwo: ochrona przed atakami Man-in-the-Middle

Przejście do chmury oraz otwarcie systemów SKD na komunikację mobilną i sieci publiczne zwiększa ekspozycję na specyficzne cyberzagrożenia, w szczególności ataki typu Man-in-the-Middle (MitM).

Skuteczna ochrona przed MitM w nowoczesnych systemach SKD opiera się na kilku filarach:

- szyfrowanie *end-to-end* (np. AES-256) na każdym etapie transmisji – od aplikacji mobilnej, przez czytnik, aż po bazę danych w chmurze,
- tokenizacja i jednorazowe tokeny (OTP),
- wzajemne uwierzytelnianie z wykorzystaniem certyfikatów X.509,
- zabezpieczenie warstwy transportowej (TLS 1.3) w komunikacji kontroler–chmura.

Wdrożenie modelu Zero Trust w kontroli dostępu oznacza, że system nie ufa domyślnie żadnemu urządzeniu ani użytkownikowi – nawet jeśli znajduje się on w sieci firmowej. Każde żądanie otwarcia drzwi jest weryfikowane pod kątem tożsamości, stanu urządzenia mobilnego (np. brak root/jailbreak) oraz kontekstu (czas i lokalizacja).

Polski rynek a wdrożenie NIS2

Polski rynek elektronicznych systemów bezpieczeństwa znajduje się w fazie intensywnego wzrostu, szacowanego na 10–15% rocznie. Inwestycje w cyberbezpieczeństwo i ciągłość działania są priorytetem dla 81% polskich firm w 2026 roku, co jest bezpośrednio skorelowane z koniecznością dostosowania się do dyrektywy NIS2.

Mimo opóźnień w krajowej legislacji eksperci zalecają niezwłoczne rozpoczęcie procesów modernizacji systemów SKD, ponieważ czas na pełne wdrożenie po wejściu w życie ustawy będzie bardzo ograniczony.

Wiele polskich przedsiębiorstw z sektorów energetyki, transportu i ochrony zdrowia stoi przed wyzwaniem modernizacji systemów on-premise, które często nie posiadają możliwości bezpiecznej integracji z chmurą ani obsługi mobilnych poświadczeń. Przejście na model chmurowy pozwala tym firmom szybko nadrobić lukę technologiczną bez konieczności budowy własnych, kosztownych centrów danych.

Wiele takich migracji zakończonych sukcesem już się odbyło. Bartłomiej Zadumiński z Unicard Systems wskazuje przykład:

– W ramach migracji do impero 360® objęliśmy m.in. sześć oddziałów ArcelorMittal Poland, jednej z największych firm przemysłowych w Polsce. System obsługuje dziś ponad 60 tys. zdarzeń dziennie w przeszło 130 punktach kontroli w lokalizacjach o wysokim natężeniu ruchu.

Kiedy rozwiązania on-premise są uzasadnione

Systemy on-premise nie są przestarzałe – w niektórych scenariuszach tradycyjna infrastruktura pozostaje uzasadniona:

- bezwzględne wymogi suwerenności danych – organizacje wojskowe, niektóre instytucje rządowe lub wysoce regulowane podmioty finansowe mogą nie mieć prawnego wyboru,
- zawodne łącze internetowe – lokalizacje wymagające całkowitej niezależności sieciowej,
- duże inwestycje w systemy legacy – w niektórych organizacjach koszty migracji i przebudowy niestandardowych integracji mogą przewyższać potencjalne korzyści.

Podsumowanie: strategiczne rekomendacje na lata 2025–2026

Transformacja systemów fizycznej kontroli dostępu w kierunku rozwiązań chmurowych, mobilnych i energooszczędnych nie jest jedynie trendem technologicznym, lecz operacyjną koniecznością w erze cyfrowej odporności.

Migracja do chmury oferuje bezprecedensowe możliwości centralnego zarządzania w strukturach rozproszonych, zapewniając spójność danych, automatyzację procesów HR oraz najwyższy poziom bezpieczeństwa oferowany przez wyspecjalizowanych dostawców.

Jednocześnie dyrektywa NIS2 nakłada na kadrę zarządzającą obowiązek traktowania bezpieczeństwa fizycznego jako integralnego elementu cyberbezpieczeństwa. W praktyce oznacza to odejście od przestarzałych standardów na rzecz szyfrowanej komunikacji (OSDP, TLS) oraz silnego uwierzytelniania (MFA). •

Jan T. Grusznic
redaktor „a&s Polska"

Artykuł powstał we współpracy z firmami: