NIS2 I CER – JAK SYSTEM KONTROLI DOSTĘPU IMPERO 360® WSPIERA INFRASTRUKTURĘ KRYTYCZNĄ?

Bartłomiej Zadumiński

Rosnące wymagania dotyczące ochrony infrastruktury krytycznej sprawiają, że organizacje muszą wykazać pełną kontrolę nad dostępem – nie tylko logicznym, ale i fizycznym. W artykule pokazuję, jak impero 360® wspiera zgodność z regulacjami NIS2 i CER, łącząc bezpieczeństwo techniczne z operacyjnym.

Formalne obowiązki kontra realne możliwości organizacji

W ostatnich miesiącach temat cyberbezpieczeństwa i ochrony infrastruktury krytycznej zyskał na znaczeniu nie tylko z powodu rosnącej liczby incydentów w Europie, ale przede wszystkim w związku z nowymi wymogami prawnymi. Dyrektywa **NIS2** koncentruje się na odporności systemów informacyjnych i sieciowych, natomiast **CER** rozszerza to podejście o fizyczne bezpieczeństwo – ludzi, obiektów i procesów.

Zgodnie z regulacjami, objęte nimi podmioty muszą **zarządzać ryzykiem w sposób ciągły i udokumentowany.** Nie wystarczy zabezpieczyć system IT – trzeba wykazać, że organizacja wie:

- kto ma dostęp do stref i zasobów krytycznych,
- jakie są procedury reagowania na incydent,
- czy możliwa jest szybka ewakuacja lub odcięcie dostępu w sytuacjach zagrożenia.

Branże objęte przepisami to m.in. energetyka, zdrowie, przemysł spożywczy, transport, wodociągi, finanse, administracja publiczna, logistyka oraz dostawcy usług cyfrowych. Przepisy dotyczą nie tylko operatorów, ale też firm współpracujących z nimi – serwisantów, podwykonawców i dystrybutorów. Każdy z nich **musi być w stanie udowodnić, że ma kontrolę nad dostępem do swojej infrastruktury – cyfrowej, jak i fizycznej**.

W praktyce oznacza to m.in.:

- prowadzenie rejestru dostępu do obiektów i stref o znaczeniu krytycznym,
- weryfikację tożsamości osób przebywających na terenie infrastruktury,
- możliwość śledzenia historii zdarzeń i przygotowania raportu audytowego na żądanie,
- wdrożenie procedur reagowania – nie tylko na ataki hakerskie, ale też na incydenty fizyczne (np. wtargnięcia, sabotaż, awarie).

Dlaczego na NIS2 oraz CER trzeba patrzeć razem?

Dyrektywy NIS2 i CER regulują dwa różne obszary bezpieczeństwa, ale w praktyce obejmują te same organizacje i ten sam cel: zapewnienie ciągłości działania infrastruktury krytycznej w sytuacji zagrożenia.

- **NIS2** skupia się na ochronie systemów informacyjnych i sieci – zarządzaniu ryzykiem cyfrowym, zgłaszaniu incydentów, zabezpieczaniu danych i zapewnieniu ciągłości działania usług online.
- **CER** koncentruje się na odporności fizycznej i operacyjnej – ochronie obiektów, ludzi, procesów i zasobów.

W teorii to dwa osobne obszary, **w praktyce – nie da się ich rozdzielić**. Dane są przechowywane w serwerowniach, do których ktoś musi mieć dostęp. Pracownicy tymczasowi czy firmy zewnętrzne często mają dostęp do tej samej infrastruktury, którą próbujemy chronić przed cyberzagrożeniami. A incydenty fizyczne – kradzież, sabotaż – mogą mieć ten sam efekt, co udany atak hakerski.

Zgodnie z obecnymi projektami ustaw, **wszystkie podmioty uznane za „krytyczne" w rozumieniu CER zostaną automatycznie zakwalifikowane jako „kluczowe" w NIS2**. To oznacza, że traktowanie tych przepisów osobno prowadzi do chaosu organizacyjnego – odrębne procedury i zespoły, niespójne systemy.

Stawką nie są wyłącznie formalna zgodność z przepisami czy spełnienie wymogów audytowych. To również:

- odpowiedzialność zarządu za nadzór nad bezpieczeństwem,
- ryzyko przerw w działalności operacyjnej,
- utrata zaufania interesariuszy.

W przypadku zakładów przemysłowych czy obiektów infrastruktury technicznej **ryzyko wzrasta szczególnie tam, gdzie występuje duża rotacja pracowników tymczasowych lub firm**

zewnętrznych – osób, których często nikt nie zna z imienia i nazwiska, a które mają fizyczny dostęp do newralgicznych stref. Z kolei po stronie systemów IT incydenty takie jak zaszyfrowanie lub wyciek danych mogą w bezpośredni sposób przełożyć się na wstrzymanie produkcji lub uniemożliwienie świadczenia usług. Dlatego odpowiednio zaprojektowany system bezpieczeństwa jest warunkiem utrzymania ciągłości działania.

Jak system kontroli dostępu impero 360® przyczynia się do zgodności z NIS2 i CER?

Jednymi z obszarów wskazywanych w NIS2 i CER są analiza ryzyka i kontrola dostępu do infrastruktury krytycznej – zarówno w kontekście ochrony obiektów, jak i identyfikowalności osób przebywających w strefach o podwyższonym ryzyku.

W tym kontekście warto przyjrzeć się **impero 360® od Unicard Systems** – chmurowemu systemowi kontroli dostępu. Rozwiązanie:

- jest zbudowane na platformie **Microsoft Azure**,
- integruje się z istniejącą infrastrukturą IT,
- umożliwia zarządzanie dostępem w czasie rzeczywistym,
- rejestruje wszystkie zdarzenia i **wspiera organizację w reagowaniu na incydenty – również w trybie offline.**

Separacja stref i zarządzanie uprawnieniami

impero 360® umożliwia precyzyjne tworzenie i zarządzanie strefami dostępu – w wymiarze fizycznym, jak i logicznym. Uprawnienia przypisywane są na podstawie:

- roli użytkownika,
- jego obowiązków,
- lokalizacji,
- harmonogramu pracy,
- rodzaju wykonywanych zadań.

Takie podejście pozwala skutecznie ograniczyć dostęp do wyłącznie niezbędnych obszarów, realizując zasadę najmniejszych uprawnień (least privilege) oraz separację obowiązków (segregation of duties).

Rejestrowanie i identyfikacja zdarzeń

Każda próba wejścia, opuszczenia strefy, czy nieautoryzowanego dostępu jest **rejestrowana i przypisywana do konkretnej tożsamości – pracownika, dostawcy czy gościa**.

Zdarzenia zapisywane są w formie czytelnych logów, z możliwością filtrowania, eksportu i generowania raportów. Dane mogą być także zintegrowane z innymi systemami (np. HR, CCTV, SIEM), co pozwala na kompleksową analizę zdarzeń.

Rysunek 1. Czytniki Unicard Systems

Reakcja na incydenty i tryb awaryjny

W sytuacjach zagrożenia impero 360® pozwala natychmiastowo:

- cofnąć uprawnienia,
- zablokować przejścia,
- uruchomić scenariusze ewakuacyjne lub inne procedury kryzysowe.

Brak połączenia z siecią nie blokuje działania systemu – użytkownicy nadal mogą korzystać z przyznanych uprawnień, a dostęp i zdarzenia są zapisywane i synchronizowane po przywróceniu łączności.

Dane dla audytów i regulatorów

System oferuje zestaw gotowych narzędzi raportowych – m.in. **historię dostępu, przeglądy uprawnień, logi systemowe, rejestry zmian** – które można wykorzystać podczas audytów wewnętrznych i zewnętrznych (CSIRT, RCB, KNF).

W przypadku audytu lub incydentu organizacja może:

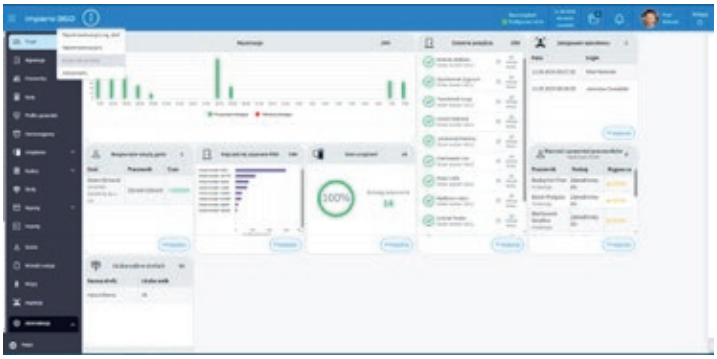
- w krótkim czasie wygenerować raporty dostępu, historię uprawnień oraz logi zdarzeń;
- zapewnić pełną identyfikowalność i nadzór nad ruchem osób – pracowników oraz podmiotów zewnętrznych – z możliwością szybkiej analizy przebiegu zdarzeń.

To nie tylko obowiązek formalny, ale realna podstawa do szybkiego reagowania na incydenty – zanim urosną one do rangi kryzysu.

Integracja z systemami bezpieczeństwa i IT

impero 360® współpracuje z systemami CCTV, SSWiN, BMS, ERP, Entra ID (Azure Directory) i systemami HR. Pozwala więc zbudować **jednolitą architekturę bezpieczeństwa, obejmującą aspekt fizyczny i cyfrowy**.

Otwarte API umożliwia pełną integrację ze środowiskiem klienta oraz automatyzację procesów zgodną z politykami organizacji.



Rysunek 2. Widok pulpitu platformy impero 360

Odporność na manipulacje i sabotaż

impero 360® wykorzystuje **protokół komunikacyjny OSDP** (Open Supervised Device Protocol) z szyfrowaniem AES-128 oraz stałym monitorowaniem integralności sygnału. System **spełnia wymagania klasy bezpieczeństwa niezbędne dla infrastruktury krytycznej**, co oznacza najwyższy poziom zabezpieczeń przed próbami:

- sabotażu,
- podmiany urządzeń,
- ingerencji fizycznej.

Bezpieczna architektura chmurowa

impero 360® działa w środowisku Microsoft Azure, zapewniając przetwarzanie danych w centrach zgodnych z międzynarodowymi normami bezpieczeństwa – **ISO/IEC 27001**, **SOC 1/2/3** – oraz w pełni zgodnych z **RODO**. Dane są szyfrowane zarówno w tranzycie, jak i w spoczynku, a dostęp do nich jest stale monitorowany i szczegółowo rejestrowany.

System wykorzystuje nowoczesną architekturę opartą na **Kubernetes**, co gwarantuje wysoką dostępność, elastyczne skalowanie zasobów oraz odporność na awarie – nawet w środowiskach rozproszonych i o krytycznym znaczeniu operacyjnym.

Dzięki modelowi chmurowemu użytkownicy zawsze korzystają z najnowszej wersji oprogramowania – regularnie aktualizowanej pod kątem bezpieczeństwa oraz zgodności z wymaganiami regulatorów. System i jego **komponenty są stale rozwijane i monitorowane, także dzięki narzędziom bezpieczeństwa dostarczanym przez Microsoft w ramach platformy Azure.** Nad bezpieczeństwem tej infrastruktury czuwa ponad 10 000 ekspertów ds. zabezpieczeń i analizy zagrożeń, co pozwala utrzymać standardy ochrony na poziomie trudnym do osiągnięcia w przypadku lokalnych serwerowni.

Zarządzanie gośćmi, podwykonawcami i personelem zewnętrznym

impero 360® umożliwia kontrolę nad ruchem osób trzecich – serwisantów, kontrahentów, czy pracowników tymczasowych. System wspiera **kontrolowaną awizację**, weryfikację tożsamości przy wejściu, nadawanie tymczasowych uprawnień oraz automatyczne ograniczanie dostępu do wybranych stref i przedziałów czasowych.

Każda wizyta jest ewidencjonowana, a gospodarze lub wyznaczone osoby mogą zdalnie zatwierdzać wejścia. To pozwala utrzymać **przejrzystość i rozliczalność** także w przypadku osób, które nie należą do stałego personelu.

Zgodność to proces – potrzebujesz narzędzia, które go wspiera

Regulacje NIS2 i CER nie sprowadzają się do wdrożenia jednego rozwiązania czy podpisania deklaracji zgodności. To wymagania, które trzeba **wdrożyć, utrzymać i udowodnić w praktyce** – w procedurach, logach systemowych, działaniach operacyjnych.

Przepisy to jedno – ale **rzeczywistość geopolityczna i zagrożenia hybrydowe pokazują, że bezpieczeństwo infrastruktury krytycznej musi być priorytetem niezależnie od litery prawa**. Wiele incydentów – również w Polsce – można byłoby ograniczyć lub im zapobiec, gdyby organizacje dysponowały odpowiednimi narzędziami i procedurami.

impero 360® zapewnia narzędzia, które wspierają ten proces: zarządzanie uprawnieniami, ewidencję dostępu, obsługę zdarzeń, integrację z systemami bezpieczeństwa i gotowość na audyt. **To solidna baza, na której można oprzeć politykę bezpieczeństwa.**

Równolegle z systemem, Unicard Systems dostarcza wiedzę i wsparcie wdrożeniowe – w oparciu o bieżące projekty legislacyjne, praktyki audytorów i wymagania branżowe. Dzięki temu organizacja może nie tylko przygotować się do nowych obowiązków, ale też faktycznie nimi zarządzać – zgodnie z logiką ciągłego doskonalenia.

Osoby zainteresowane tematyką NIS2 i CER mogą wziąć udział w cyklu bezpłatnych webinarów organizowanych przez Unicard Systems. Podczas spotkań eksperci Unicard oraz zaproszeni goście omówią praktyczne aspekty wdrażania nowych regulacji, wytłumaczą, jak interpretować wymagania dotyczące bezpieczeństwa fizycznego i cyberbezpieczeństwa, a także pokażą, jak system impero 360® wspiera organizacje w utrzymaniu zgodności. To również doskonała okazja do zadawania pytań i dzielenia się doświadczeniami.

Zapraszamy do rejestracji:
www.unicard.pl/webinary-nis2

Bartłomiej Zadumiński
Odpowiada za rozwój kluczowych rozwiązań programistycznych firmy – w tym chmurowego systemu kontroli dostępu impero 360®. Zarządza zespołem odpowiedzialnym za rozwój funkcjonalny, wsparcie techniczne i dopasowanie oprogramowania do potrzeb użytkowników – zarówno pod względem technologicznym, jak i regulacyjnym.