Od dyrektywy do codziennych decyzji

– jak NIS2 i CER wpływają na zarządzanie dostępem w farmacji?

Bartłomiej Zaduminski
Kierownik Działu Wsparcia i Rozwoju Oprogramowania w Unicard Systems

O bezpieczeństwie organizacji coraz częściej decydują procedury i uprawnienia – kto może wejść do strefy krytycznej, na jakich zasadach, jak to jest rejestrowane i jak szybko organizacja potrafi przywrócić kontrolę po incydencie.

W Polsce od 2026 r. kierunek tych działań wyznaczają dwie regulacje unijne. Dyrektywa NIS2 skupia się na ochronie sieci i systemów informacyjnych, zarządzaniu ryzykiem oraz obowiązkach związanych z wykrywaniem i raportowaniem incydentów. CER uzupełnia to podejście, koncentrując się na tym, aby podmioty uznane za krytyczne były lepiej przygotowane na zakłócenia, zwłaszcza te dotyczące zagrożeń fizycznych.

W dalszej części pokazuję, jak oba akty wpływają na zasady zarządzania dostępem w organizacjach farmaceutycznych. Wyjaśniam też, jak powiązać fizyczną kontrolę dostępu z procedurami bezpieczeństwa, audytowalnością i reagowaniem na incydenty, aby spełnić wymogi przepisów.

Dyrektywa NIS2 – co to jest i kogo dotyczy?

NIS2 (2022/2555) zastępuje wcześniejszą dyrektywę NIS (Network and Information Security) i rozszerza zakres obowiązków organizacji w obszarze bezpieczeństwa systemów informacyjnych. Jej celem jest ujednolicenie standardów ochrony w Unii Europejskiej oraz wzmocnienie nadzoru nad sposobem zarządzania bezpieczeństwem w podmiotach o istotnym znaczeniu dla gospodarki i usług publicznych.
Dyrektywa obejmuje m.in:

- infrastrukturę sieciową i systemy IT,
- systemy wspierające procesy operacyjne, w tym systemy przemysłowe,
- środowiska przetwarzania i przechowywania danych.

NIS2 wprowadza podział podmiotów objętych regulacją na kluczowe i ważne. Obszar „zdrowie" został ujęty w grupie sektorów o wysokiej krytyczności, a w jego zakresie wskazano m.in.:

- wytwarzanie podstawowych produktów farmaceutycznych i preparatów farmaceutycznych,
- działalność badawczo-rozwojową związaną z produktami leczniczymi.

W praktyce oznacza to, że firmy z branży farmaceutycznej – w szczególności wytwórcy substancji czynnych (API) i produktów

leczniczych, podmioty prowadzące działalność badawczo-rozwojową nad lekami, a także uczestnicy łańcucha dystrybucji (np. hurtownie, importerzy czy podmioty posiadające pozwolenia na dopuszczenie do obrotu) – mogą zostać zakwalifikowane jako podmioty kluczowe lub ważne, w zależności od wielkości przedsiębiorstwa.
Obowiązki wynikające z NIS2 to m.in.:

- wprowadzenie spójnego modelu zarządzania ryzykiem dla środowisk IT oraz OT,
- wdrożenie rozwiązań, które wspierają ciągłość działania (w tym kopie zapasowe i odtwarzanie po incydentach),
- uwzględnienie ryzyk po stronie dostawców i usługodawców oraz wzmocnienie bezpieczeństwa łańcucha dostaw.

Istotnym elementem dyrektywy NIS2 są obowiązki raportowania incydentów. Organizacje muszą przekazywać zgłoszenia w określonych terminach – wstępną notyfikację po wykryciu incydentu (do 24 godzin), raport uzupełniający (do 72 godzin), a następnie szczegółową analizę przyczyn, działań naprawczych i wniosków długoterminowych (do 1 miesiąca).

Oznacza to konieczność stworzenia jasno określonych procedur identyfikacji incydentów, przeszkolenia zespołów oraz dostosowania procedur do standardów wymaganych przez NIS2. Co istotne, obowiązki nie dotyczą wyłącznie działów IT. Dyrektywa jednoznacznie wskazuje na rolę wyższego kierownictwa – to zarząd ma zapewnić nadzór oraz środki niezbędne do spełnienia wymagań regulacyjnych.

Dyrektywa CER – odporność krytycznych podmiotów

Dyrektywa 2022/2557 (CER – Critical Entities Resilience) dotyczy odporności operacyjnej podmiotów uznanych za krytyczne. Wymaga, aby organizacje były przygotowane na zdarzenia, które mogą zakłócić świadczenie usług lub prowadzenie działalności oraz posiadały mechanizmy ograniczania skutków incydentów. CER przesuwa nacisk z „reakcji po fakcie" na systematyczne planowanie, utrzymanie i regularną weryfikację rozwiązań zapewniających ciągłość działania. CER wskazuje m.in. następujące zagrożenia:

- zdarzenia naturalne i awarie (np. pożar, zalanie, uszkodzenia infrastruktury),
- przerwy w dostępności mediów i usług technicznych (np. zasilanie, HVAC, łączność),
- działania celowe (np. sabotaż, wtargnięcia, zakłócenia pracy obiektu).

Po uznaniu organizacji za podmiot krytyczny należy ocenić rodzaje zagrożeń, opracować i wdrożyć plan odporności oraz zastosować środki ochrony fizycznej, takie jak kontrola dostępu, monitoring czy procedury ewakuacyjne. Przepisy wymagają także zgłaszania i analizowania incydentów, tak aby organizacja mogła wyciągać wnioski i na bieżąco wzmacniać swoje zabezpieczenia.

I chociaż NIS2 i CER to dwie różne perspektywy – NIS2 koncentruje się na bezpieczeństwie systemów informacyjnych, a CER na odporności operacyjnej podmiotów krytycznych – to ich wdrożenie powinno być prowadzone wspólnie. Często dotyczą tych samych organizacji, a zdarzenia cyfrowe i fizyczne wpływają na te same procesy oraz zasoby.

Fizyczna kontrola dostępu dla firm farmaceutycznych a CER i NIS2

NIS2 i CER poszerzają podejście do bezpieczeństwa – obok ochrony przed cyberatakami istotna jest także zdolność organizacji do utrzymania ciągłości działania w razie zakłóceń. W branży farmaceutycznej oznacza to, że fizyczna kontrola dostępu powinna być elementem zarządzania ryzykiem, a nie jedynie „ochroną budynku". Musi umożliwiać identyfikację, ograniczanie i dokumentowanie wejść do wszystkich obszarów, które mają znaczenie dla świadczenia usług krytycznych.

> **W branży farmaceutycznej fizyczna kontrola dostępu przestaje być jedynie ochroną budynku** – staje się elementem zarządzania ryzykiem, który musi umożliwiać identyfikację, ograniczanie i dokumentowanie dostępu do wszystkich obszarów kluczowych dla ciągłości działania

Kontrola dostępu jako system bezpieczeństwa operacyjnego

W środowisku farmaceutycznym ważne jest zabezpieczenie obszarów istotnych z punktu widzenia działalności i wymagań prawnych, takich jak:

- magazyny substancji kontrolowanych i gotowych produktów leczniczych,
- laboratoria badawczo-rozwojowe (R&D), w których przechowywana jest własność intelektualna i prowadzone są badania kliniczne,
- pomieszczenia serwerowe oraz infrastruktura OT, w tym systemy sterowania produkcją i automatyki przemysłowej (np. SCADA),
- strefy czyste, gdzie nieuprawniona obecność może skutkować skażeniem mikrobiologicznym i koniecznością wstrzymania produkcji.

Z perspektywy NIS2 i CER system KD powinien rejestrować każde wejście, wyjście oraz próbę nieautoryzowanego dostępu, przypisując zdarzenie do konkretnej osoby, identyfikatora lub uprawnienia czasowego. Takie dane są ważną częścią dokumentacji i mogą być wykorzystywane podczas audytów, kontroli

NIS2 w praktyce: terminy wdrożenia

3 kwietnia 2026	Wejście ustawy w życie
3 października 2026	Samoidentyfikacja (ocena statusu, czy organizacja jest podmiotem ważnym/kluczowym) oraz rejestracja w wykazie podmiotów ważnych i kluczowych
3 kwietnia 2027	Termin na wdrożenie wymogów (m.in. systemy kontroli dostępu, analiza ryzyka, zarządzanie incydentami, bezpieczeństwo łańcucha dostaw)
3 kwietnia 2028	Najwcześniejszy moment potencjalnego nałożenia sankcji za brak zgodności oraz termin na pierwszy obowiązkowy audyt cyberbezpieczeństwa

organów nadzorczych, analiz CSIRT oraz dochodzeń po wypadku lub incydencie.

Istotnym wymogiem jest również kontrola dostępu osób zewnętrznych – serwisantów, integratorów, pracowników kontraktowych. Ich dostęp powinien być ograniczony do konkretnych stref i przedziałów czasowych, zgodnie z zasadą minimalnych uprawnień. W praktyce oznacza to korzystanie z identyfikatorów tymczasowych, dostępu pod nadzorem lub automatycznego odbierania uprawnień po zakończeniu prac.

Nowoczesne systemy KD, jak rozwiązania oferowane przez Unicard Systems, wykorzystują także inne funkcje zwiększające bezpieczeństwo fizyczne i zgodność regulacyjną, jak:

- **śluzy higieniczne**, które wymuszają wykonanie określonych procedur sanitarnych (np. dezynfekcja rąk lub butów) przed uzyskaniem dostępu do strefy czystej,
- **ograniczenia liczby osób** w pomieszczeniu lub strefie,
- **alarmowanie** o zdarzeniach takich jak zbyt długie przetrzymanie otwartych drzwi.

Automatyzacja tych procesów zmniejsza ryzyko błędu ludzkiego i pomaga konsekwentnie stosować polityki bezpieczeństwa.

W świetle dyrektyw NIS2 i CER decyzje o nadawaniu uprawnień muszą być udokumentowane i uzasadnione, ponieważ nieautoryzowany dostęp w zakładzie farmaceutycznym może prowadzić do wstrzymania produkcji, naruszenia wymagań GMP lub utraty integralności produktu leczniczego

Kontrola dostępu jako źródło danych o ryzyku i incydentach

Dyrektywy NIS2 i CER wymagają wdrożenia rozwiązań, które pozwalają wykrywać incydenty i skutecznie na nie reagować. W tym kontekście logi z systemów kontroli dostępu są cennym źródłem danych. Rejestrowanie zdarzeń wejścia i wyjścia pozwala wykrywać anomalie, takie jak próby dostępu poza godzinami pracy, wejścia do nieautoryzowanych stref czy użycia nieaktywnych identyfikatorów. System może automatycznie generować alarmy, blokować dostęp lub przekazywać informacje do zespołów bezpieczeństwa.

Szczególnie istotna jest integracja systemów KD z innymi platformami zarządzania bezpieczeństwem, takimi jak:

- systemy BMS (Building Management System),
- systemy zarządzania bezpieczeństwem fizycznym (PSIM),
- platformy SIEM wykorzystywane przez zespoły cyberbezpieczeństwa.

Dzięki takiej integracji możliwa jest korelacja zdarzeń fizycznych i cyfrowych. Przykładowo próba logowania do systemu produkcyjnego może zostać powiązana z obecnością użytkownika w pomieszczeniu serwerowym.

Wybrane rozwiązania technologiczne, które wspierają zgodność z regulacjami

W kontekście odporności operacyjnej wymaganej przez CER ważne jest, aby systemy kontroli dostępu działały także w sytuacjach awaryjnych. W praktyce oznacza to m.in. możliwość pracy kontrolerów w trybie offline – w przypadku utraty łączności z systemem centralnym dostęp dla uprawnionych osób pozostaje możliwy, a zdarzenia są synchronizowane po przywróceniu komunikacji.
System KD powinien również wspierać najważniejsze zasady bezpieczeństwa, takie jak:

- **least privilege** – użytkownik posiada dostęp wyłącznie do stref niezbędnych do wykonywania obowiązków,
- **segregation of duties** – rozdzielenie uprawnień w sposób zapobiegający nadużyciom lub sabotażowi,
- **kompletną rejestrację zdarzeń** administracyjnych i operacyjnych.

Zaawansowane rozwiązania umożliwiają także wykrywanie prób manipulacji przy urządzeniach, takich jak otwarcie obudowy kontrolera, odłączenie czytnika czy przerwanie zasilania. Te zdarzenia mogą wskazywać na próbę sabotażu i wymagają natychmiastowej reakcji.

Nowe regulacje a zmiana podejścia w codziennych decyzjach operacyjnych

W świetle dyrektyw NIS2 i CER decyzje o nadawaniu uprawnień muszą być udokumentowane, uzasadnione oraz przypisane do konkretnych właścicieli obszarów. W sektorze farmaceutycznym ma to duże znaczenie, ponieważ nieautoryzowany dostęp może prowadzić do wstrzymania produkcji, naruszenia wymagań GMP lub utraty integralności produktu leczniczego.

Co muszą zmienić dyrektorzy zakładów i działy techniczne?

Pierwszym krokiem jest formalizacja polityk fizycznego dostępu zgodnie z NIS2 i CER. Wymaga to opracowania i wdrożenia procedur określających, kto może uzyskać dostęp do określonych stref, na jakiej podstawie oraz w jaki sposób uprawnienia są nadawane,

weryfikowane i odbierane. Zasady te powinny być spójne z przyjętymi w organizacji politykami bezpieczeństwa.

Konieczne jest również wprowadzenie nowych kryteriów nadawania uprawnień, uwzględniających nie tylko stanowisko pracownika, ale także:

- rzeczywiste potrzeby operacyjne,
- poziom ryzyka,
- wrażliwość danej strefy.

Dyrektywy podkreślają także znaczenie regularnego testowania skuteczności wdrożonych środków bezpieczeństwa. Oznacza to m.in. okresowe audyty uprawnień, przeglądy logów dostępu, testy procedur reagowania na incydenty oraz – w uzasadnionych przypadkach – przeprowadzenie symulowanych prób nieautoryzowanego dostępu. Ich celem jest potwierdzenie, że zabezpieczenia działają zgodnie z założeniami i są adekwatne do aktualnego poziomu zagrożeń.
Współpraca działów: IT, produkcja, HR

System kontroli dostępu odzwierciedla strukturę organizacyjną i podział odpowiedzialności w zakładzie. Przykładowo:

- **osoby odpowiedzialne za konkretne strefy** (np. kierownicy produkcji lub infrastruktury technicznej) wskazują obszary kontrolowane – magazyny substancji czynnych, laboratoria, OT oraz strefy czyste – i ustalają zasady wejścia, w tym okna czasowe oraz wymogi higieniczne,
- **dział IT** odpowiada za konfigurację systemu kontroli dostępu zgodnie z tymi wymaganiami, przypisanie uprawnień do konkretnych identyfikatorów oraz poprawne zapisywanie i przechowywanie zdarzeń,
- **HR** dostarcza informacje o zatrudnieniu, zmianach stanowisk i zakończeniu współpracy, co umożliwia nadawanie, modyfikowanie lub usuwanie uprawnień we właściwym czasie.

Taki model pozwala wykazać podczas audytu, że dostęp do infrastruktury krytycznej był nadawany świadomie i zgodnie z zakresem obowiązków.

Ważne jest również przygotowanie pracowników do użytkowania systemu kontroli dostępu zgodnie z obowiązującymi procedurami. Dotyczy to m.in.:

- korzystania z indywidualnych identyfikatorów,
- zakazu udostępniania kart innym osobom,
- natychmiastowego zgłaszania utraty identyfikatora.

Wnioski i rekomendacje dla branży farmaceutycznej

Wdrożenie wymagań NIS2 i CER nie powinno być postrzegane wyłącznie jako spełnienie obowiązków prawnych. To inwestycja w odporność operacyjną organizacji, która w sektorze farmaceutycznym przekłada się na ciągłość wytwarzania, bezpieczeństwo produktu oraz zaufanie pacjentów i partnerów.

Pierwszym krokiem powinna być ocena, czy obecny system kontroli dostępu pozwala jasno ustalić, kto, kiedy i do jakiej strefy wszedł. Ważne jest także, czy system rejestruje zdarzenia w sposób umożliwiający ich późniejszą analizę podczas incydentu lub audytu. Rozwiązania oparte na przestarzałych i słabo zabezpieczonych nośnikach mogą stanowić istotną lukę bezpieczeństwa i zostać uznane za niewystarczające z punktu widzenia zarządzania ryzykiem.

Kolejnym krokiem jest uporządkowanie zasad nadawania uprawnień w całej organizacji, także wtedy, gdy obejmuje ona więcej niż jeden zakład. Duże znaczenie ma również możliwość rozbudowy systemu bez konieczności kosztownej wymiany całej infrastruktury.

Równolegle należy zadbać o kwestie organizacyjne. Nawet dobrze zaprojektowany system nie będzie skuteczny, jeśli użytkownicy nie będą przestrzegać przyjętych polityk. Dlatego reguły fizycznej kontroli dostępu powinny być stałym elementem szkoleń z bezpieczeństwa. Pracownicy muszą wiedzieć, że identyfikator wymaga takiej samej ochrony jak dane logowania do systemów. To samo dotyczy firm zewnętrznych i pracowników tymczasowych – ich dostęp powinien być nadawany, ograniczany i odbierany według jasno określonych zasad.

Warto również pamiętać, że budowanie odporności operacyjnej nie jest działaniem jednorazowym. NIS2 i CER wymagają stałego podejścia: regularnych przeglądów uprawnień, sprawdzania skuteczności zabezpieczeń, analizy logów i gotowości do reagowania na incydenty. ■

Bibliografia:

1. https://dziennikustaw.gov.pl/D2026000025201.pdf
2. https://www.gov.pl/web/baza-wiedzy/sejm-uchwalil-nowelizacje-ustawy-o-krajowym-systemie-cyberbezpieczenstwa
3. https://grantthornton.pl/publikacja/apteki-producenci-lekow-i-wyrobow-medycznych-a-nis2/#