NIS2 i CER a kontrola dostępu w branży spożywczej – od czego zacząć? Cz. I

Przewodnik dla zarządów i dyrektorów operacyjnych

Bartłomiej Zadumiński
Kierownik Działu Wsparcia i Rozwoju Oprogramowania w Unicard Systems

Jak przygotować zakład spożywczy na wymagania NIS2 i CER? Nowe przepisy unijne wprowadzają obowiązki nie tylko w obszarze IT, ale również w zakresie ochrony fizycznej i kontroli dostępu. W tym przewodniku pokazujemy, jak podejść do tematu strategicznie – krok po krok i na podstawie doświadczeń z wdrożeń w dużych organizacjach.

NIS2 i CER – co trzeba wiedzieć na start?

Nowe unijne przepisy dotyczące odporności i bezpieczeństwa podmiotów kluczowych, ważnych oraz krytycznych wprowadzają konkretne wymagania wobec wielu branż – w tym sektora spożywczego. Dyrektywy NIS2 i CER obejmują zarówno obszar cyberbezpieczeństwa, jak i ochrony fizycznej, a ich wdrożenie będzie miało bezpośredni wpływ na sposób funkcjonowania zakładów produkcyjnych, centrów dystrybucyjnych oraz firm obsługujących łańcuch dostaw.

NIS2 – cyberbezpieczeństwo dla podmiotów kluczowych i ważnych

Dyrektywa 2022/2555, znana szerzej jako NIS2, obowiązuje w Unii Europejskiej od stycznia 2023 r. **Jej głównym celem jest podniesienie poziomu odporności cyfrowej organizacji świadczących usługi istotne dla funkcjonowania społeczeństwa i gospodarki.** W Polsce trwają prace nad nowelizacją ustawy o KSC wdrażającą NIS2 (projekt procedowany w Sejmie – druk 1955). Na poziomie UE termin transpozycji minął 17 października 2024 r., co zwiększa presję na szybkie przyjęcie przepisów krajowych.

Branża spożywcza została bezpośrednio ujęta w Załączniku II dyrektywy jako „inny sektor krytyczny". To oznacza, że wiele podmiotów zostanie zaklasyfikowanych jako tzw. Important Entities – organizacje istotne z punktu widzenia bezpieczeństwa państwa.Zakres obowiązków wynikających z NIS2 obejmuje między innymi:

- wdrożenie systemowego podejścia do zarządzania ryzykiem w systemach IT i OT,
- zapewnienie mechanizmów wykrywania, reagowania i zgłaszania incydentów,
- gwarancję ciągłości działania usług,
- ochronę łańcucha dostaw,
- wyznaczenie osób odpowiedzialnych na poziomie zarządu.

W praktyce oznacza to **konieczność zbudowania przejrzystej struktury odpowiedzialności, przeszkolenia zespołów i dostosowania procedur do rygorystycznych standardów cyberbezpieczeństwa.** Co istotne, odpowiedzialność nie spoczywa wyłącznie na działach IT. Zgodnie z zapisami dyrektywy, to zarząd organizacji musi zapewnić nadzór i środki pozwalające na spełnienie wymagań regulacyjnych.

CER – fizyczna i operacyjna odporność

Dyrektywa 2022/2557 (CER – Critical Entities Resilience) wprowadza regulacje uzupełniające wobec NIS2. **Jej przedmiotem jest odporność fizyczna i operacyjna infrastruktury, obejmująca zagrożenia takie jak awarie techniczne, katastrofy naturalne, akty sabotażu czy ataki terrorystyczne.**

Branża spożywcza została objęta zakresem CER jako infrastruktura krytyczna, co oznacza, że państwa członkowskie mają obowiązek zidentyfikować firmy pełniące funkcje newralgiczne w łańcuchach dostaw żywności. Termin na przeprowadzenie tej identyfikacji mija w lipcu 2026 r.

Po zaklasyfikowaniu jako podmiot krytyczny, firma będzie musiała m.in.:

- przeprowadzić ocenę ryzyka typu all-hazards,
- przygotować i wdrożyć plan odporności organizacyjnej,
- zapewnić odpowiednie środki ochrony fizycznej (np. kontrola dostępu, systemy monitoringu, procedury ewakuacyjne),
- opracować i wdrożyć systemy zgłaszania oraz analizowania incydentów.

Z perspektywy operacyjnej, **CER wymusza spojrzenie na zakład lub centrum logistyczne jako całość – nie tylko pod kątem produkcji, ale też bezpieczeństwa osób, zasobów, informacji oraz współpracujących firm zewnętrznych.**

Podejście zintegrowane: NIS2 + CER

Choć NIS2 i CER dotyczą formalnie różnych obszarów – odpowiednio: cyberbezpieczeństwa i odporności fizycznej – w rzeczywistości powinny być wdrażane razem. Powód jest prosty: **obie regulacje mają zastosowanie do tych samych organizacji, a zagrożenia cyfrowe i fizyczne coraz częściej się przenikają.**

Przykład? Awaria zasilania, sabotaż fizyczny czy nieautoryzowany dostęp do stref technicznych mogą wywołać skutki porównywalne z atakiem hakerskim. Z drugiej strony, nieuprawniony dostęp do systemu sterującego produkcją żywności może skutkować zagrożeniem zdrowia publicznego. Dlatego podejście silosowe – osobno IT, osobno ochrona fizyczna – nie sprawdzi się w środowisku objętym wymogami NIS2 i CER.

Zintegrowane wdrożenie przepisów oznacza:

- spójne zarządzanie ryzykiem – cyfrowym i fizycznym,
- jednolite standardy kontroli dostępu (zarówno do danych, jak i do obiektów),
- wspólne procedury reagowania na incydenty,
- centralne zarządzanie odpowiedzialnością – na poziomie zarządu, a nie tylko działu bezpieczeństwa.

Zgodnie z projektami krajowych przepisów, **każdy podmiot uznany za „krytyczny" w rozumieniu CER automatycznie stanie się podmiotem „kluczowym" w NIS2.** To oznacza, że próba rozdzielnego wdrażania tych wymagań skończy się niepotrzebnym dublowaniem procedur, wzrostem kosztów i trudnościami we wdrożeniu skutecznego nadzoru.

Rola kontroli dostępu w kontekście NIS2 i CER

Zarówno NIS2, jak i CER wyraźnie wskazują, że bezpieczeństwo organizacji nie kończy się na zaporach sieciowych i kopiach zapasowych. **Ochrona fizyczna infrastruktury oraz kontrola dostępu do stref newralgicznych są traktowane jako nieodzowny element systemu odporności.**

NIS2 wymaga wdrożenia środków zarządzania ryzykiem cyber (w tym polityk kontroli dostępu i ochrony zasobów). Dyrektywa CER z kolei wprowadza konkretne wymagania związane z bezpieczeństwem fizycznym – ocenę ryzyka dla dostępu do obiektów, konieczność wdrożenia środków technicznych i organizacyjnych, czy systemy nadzoru i kontroli obecności.

W tym kontekście kontrola dostępu nabiera strategicznego znaczenia. Dobrze zaprojektowany system:

- **chroni strefy krytyczne**, takie jak serwerownie, chłodnie, stacje dozujące, hale produkcyjne czy systemy SCADA,
- **umożliwia przypisanie konkretnych uprawnień do ról i funkcji** – także w odniesieniu do pracowników tymczasowych czy firm zewnętrznych,
- **wspiera zarządzanie incydentami** – pozwala odtworzyć historię zdarzeń i wskazać osoby obecne w danym miejscu w określonym czasie,
- **integruje się z systemami BMS, CCTV, przeciwpożarowymi** – tworząc spójne środowisko bezpieczeństwa, zdolne do reakcji w czasie rzeczywistym,
- **działa również w trybie offline** – co ma istotne znaczenie w przypadku awarii zasilania lub sieci.

W środowisku przemysłowym, gdzie systemy OT coraz częściej są połączone z infrastrukturą IT, kontrola dostępu jest warstwą łączącą dwa światy: fizyczny i cyfrowy. To właśnie w tym miejscu przecinają się wymagania NIS2 i CER, a ich wspólna realizacja zaczyna się od odpowiedzi na proste pytanie: kto ma dostęp, gdzie, kiedy i na jakich zasadach?

W branży spożywczej system kontroli dostępu może również wspierać realizację zasad HACCP, a w praktyce stanowić jeden z elementów systemu zarządzania bezpieczeństwem żywności. Odpowiednio zaprojektowane KD ogranicza dostęp do krytycznych punktów kontroli (CCP) wyłącznie do uprawnionych osób, pozwala egzekwować procedury wejścia do stref czystych oraz dokumentować obecność personelu na poszczególnych etapach procesu produkcyjnego.

Co musi zapewniać nowoczesny system kontroli dostępu dla branży spożywczej?

Podstawą jest możliwość tworzenia stref bezpieczeństwa – logicznych i fizycznych – z przypisaniem uprawnień do konkretnych ról, funkcji i osób. Operator linii produkcyjnej nie musi mieć dostępu do serwerowni, a technik serwisowy do magazynu substancji pomocniczych. Rozdział uprawnień powinien być nie tylko możliwy, ale łatwo konfigurowalny i możliwy do zablokowania w razie potrzeby. System kontroli dostępu w środowisku zakładu produkcyjnego musi również:

- **rejestrować wszystkie wejścia i wyjścia** – nie tylko pracowników etatowych, ale także gości, serwisantów, firm zewnętrznych,
- **umożliwiać natychmiastowe odebranie uprawnień lub zdalne zamknięcie wybranej strefy**,
- **wykorzystywać śluzy dezynfekcyjne**, które zapewniają odpowiednią higienę przy wejściu do stref czystych i jednocześnie pomagają kontrolować, kto i kiedy wchodzi do chronionych obszarów,
- **monitorować maksymalną pojemność stref** (np. hal z ograniczoną liczbą stanowisk),
- **umożliwiać weryfikację**, kto przebywał na danej linii produkcyjnej w określonym czasie – co może mieć znaczenie w przypadku incydentu lub inspekcji sanitarnych,
- **wykorzystywać alerty**, np. o zdarzeniach takich jak zbyt długie przetrzymanie otwartych drzwi.

Istotnym wymogiem jest także **możliwość raportowania, zarówno na potrzeby audytów wewnętrznych, jak i zewnętrznych kontroli,** np. ze strony organów nadzorczych czy partnerów biznesowych. Niezbędna jest też zdolność do pracy w trybie offline – tak, aby w przypadku utraty łączności system wciąż rejestrował zdarzenia.

Od czego zacząć? Plan działań dla firm z sektora spożywczego

Wdrożenie wymagań wynikających z dyrektyw NIS2 i CER nie sprowadza się do jednorazowej inwestycji. To proces, który wymaga zaangażowania zarządu, identyfikacji ryzyk i dostosowania istniejących procedur do wymogów regulacyjnych. Szczególnie w branży spożywczej – złożonej, rozproszonej i narażonej zarówno na zagrożenia cyfrowe, jak i fizyczne – działania trzeba uporządkować i zaplanować krok po kroku.

Zapraszamy do części drugiej artykułu w następnym wydaniu „Rzeźnika polskiego"

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.