SETCONTROL

BROSZURA INFORMACYJNA · KSC / NIS2

DLA BRANŻY SPOŻYWCZEJ · PRODUKCJA · PIEKARNIE · HURT · SIECI SKLEPÓW

TWOJA PRODUKCJA NIE MOŻE STANĄĆ



Cyberbezpieczeństwo w branży spożywczej według ustawy o Krajowym Systemie Cyberbezpieczeństwa po nowelizacji wdrażającej dyrektywę NIS2 – od sterowników linii produkcyjnej po kasy w sklepach. Sprawdzamy, czy firma podlega ustawie, i przygotowujemy ją do audytu.

WEJŚCIE W ŻYCIE

03.04.2026

Samoidentyfikacja – czy firma podlega obowiązkom KSC.

WPIS DO S46 · MINĄŁ

03.10.2026

Wniosek o wpis do wykazu. Brak wpisu? Złóż niezwłocznie.

SZBI

03.04.2027

Pełne wdrożenie SZBI i podłączenie do systemu S46.

KARY

03.04.2028

Możliwość nakładania kar administracyjnych.

SETCONTROL Sp. z o.o. · automatyka przemysłowa i cyberbezpieczeństwo OT/IT
Warszewka 14, 09-210 Drobin · info@setcontrol.pl · **+48 500 440 810**

PRODUKCJA, PRZETWARZANIE
I DYSTRYBUCJA ŻYWNOŚCI
ZAŁĄCZNIK NR 2 DO USTAWY O KSC

CZEGO DOWIESZ SIĘ Z TEJ BROSZURY

- Czy Twoja firma spożywcza podlega ustawie o KSC – i dlaczego sklepy, piekarnia i hurtownia to trzy różne sytuacje
- Jakie obowiązki spoczywają na firmie i jej zarządzie
- Kalendarz wdrożenia – najważniejsze daty i terminy
- Specyfika branży: biuro, automatyka linii produkcyjnych i łańcuch chłodniczy
- Jak zgłaszać incydenty i przygotować się do audytu
- Jakie kary grożą za niedopełnienie obowiązków

W CZYM POMAGAMY

01 AUTOMATYKA PRZEMYSŁOWA I AKPIA
Sterowniki PLC, SCADA i linie produkcyjne – projekt, utrzymanie i bezpieczna integracja z IT.

02 CYBERBEZPIECZEŃSTWO OT/IT
Inwentaryzacja systemów, analiza ryzyka, podział sieci i monitoring zakładu oraz sklepów.

03 ZGODNOŚĆ Z KSC / NIS2
Samoidentyfikacja, wpis do S46, wdrożenie SZBI i audyt gotowości przed 3 kwietnia 2027 r.

KONTEKST

01 DLACZEGO USTAWA O KSC DOTYCZY BRANŻY SPOŻYWCZEJ

Ustawa o KSC po nowelizacji wdrażającej dyrektywę NIS2 objęła nowy sektor **„Produkcja, przetwarzanie i dystrybucja żywności”**. Znalazł się on w załączniku nr 2 do ustawy, obok m.in. chemikaliów, usług pocztowych, gospodarki odpadami i produkcji wyrobów medycznych. Zatrzymanie produkcji lub dostaw żywności bardzo szybko przekłada się na puste półki, straty i ryzyko dla konsumentów.

W 2025 roku zespoły CSIRT odebrały **272 941 zgłoszeń** o incydentach. Produkcja i dystrybucja żywności są coraz bardziej zależne od IT i automatyki – atak, zwłaszcza ransomware, może zatrzymać zakład lub magazyn w ciągu godzin.

JAK WYGLĄDA CYBERATAK W FIRMIE SPOŻYWCZEJ

SCENARIUSZ	SKUTEK DLA FIRMY
Ransomware w ERP lub systemie magazynowym (WMS)	Brak przyjmowania zamówień, kompletowania i wydawania towaru; zatrzymanie dostaw do sklepów i odbiorców
Awaria lub przejęcie sterowników linii produkcyjnej	Zatrzymanie pieców, mieszalników, linii pakujących; psucie się półproduktów; błędy w recepturach i parametrach
Zakłócenie monitoringu łańcucha chłodniczego	Utrata dowodów zgodności z HACCP, utylizacja towaru, ryzyko dla bezpieczeństwa żywności
Atak na kasy, POS i systemy płatnicze	Przestój sprzedaży, utrata przychodów, wyciek danych płatniczych i danych klientów
Phishing i wyłudzenia (fałszywe faktury, zmiana numeru konta)	Straty finansowe, przejęcie poczty i kont uprzywilejowanych
Atak przez dostawcę oprogramowania lub serwisanta maszyn	Dostęp do sieci zakładu „tylnymi drzwiami” przez zdalny dostęp serwisowy

ORGAN WŁAŚCIWY DLA SEKTORA ŻYWNOŚCI

Każdemu sektorowi przypisano organ właściwy zgodnie z działami administracji rządowej. Dla sektora żywności jest to co do zasady **minister właściwy do spraw rolnictwa** – prowadzi nadzór i nakłada kary. Przed złożeniem wniosku o wpis do wykazu warto potwierdzić aktualne wskazanie w załączniku do ustawy.

SAMOIDENTYFIKACJA

02 CZY MOJA FIRMA PODLEGA USTAWIE?

Ustawa działa na zasadzie **samoidentyfikacji** – firma sama ocenia, czy podlega obowiązkom, a ryzyko błędnej oceny ponosi jej zarząd. Firma spożywcza podlega ustawie, jeżeli spełnia **jednocześnie dwa warunki**:

WARUNEK 1

CO NAJMNIEJ ŚREDNIA FIRMA

Według progów zatrudnienia i finansów z tabeli poniżej.

WARUNEK 2

HURT LUB PRODUKCJA PRZEMYSŁOWA

Przedsiębiorstwo spożywcze (art. 3 pkt 2 rozp. (WE) nr 178/2002) zajmujące się dystrybucją hurtową albo przemysłową produkcją i przetwarzaniem żywności.

Przedsiębiorstwem spożywczym jest każdy podmiot publiczny lub prywatny, także niedziałający dla zysku – dotyczy to więc również spółdzielni.

2.1. JAK OKREŚLIĆ WIELKOŚĆ FIRMY

Uwzględnia się również przedsiębiorstwa powiązane i partnerskie (chyba że ich systemy informacyjne są w pełni niezależne).

WIELKOŚĆ	ZATRUDNIENIE	ROCZNY OBRÓT / SUMA BILANSOWA	STATUS W KSC
Mikro	< 10 osób	≤ 2 mln EUR	CO DO ZASADY NIE PODLEGA*
Mała	< 50 osób	≤ 10 mln EUR	CO DO ZASADY NIE PODLEGA*
Średnia	< 250 osób	≤ 50 mln EUR obrotu lub ≤ 43 mln EUR bilansu	PODMIOT WAŻNY
Duża	≥ 250 osób	> 50 mln EUR obrotu i > 43 mln EUR bilansu	PODMIOT WAŻNY

* Mała lub mikro firma może zostać objęta ustawą w przypadkach wyjątkowych – patrz ramka na następnej stronie. Firma jest duża, gdy zatrudnia co najmniej 250 osób albo przekracza oba progi finansowe.

2.2. JAKA DZIAŁALNOŚĆ JEST OBJĘTA USTAWĄ

Sam rozmiar nie wystarcza. Zakres sektora jest węższy niż „cała branża spożywcza” – ustawa obejmuje wyłącznie **dystrybucję hurtową** oraz **przemysłową produkcję i przetwarzanie** żywności.

RODZAJ DZIAŁALNOŚCI	OCENA	UWAGI
Przemysłowa produkcja i przetwarzanie żywności (zakłady, wytwórnie, przetwórnie, piekarnie o skali przemysłowej)	OBJĘTA	Jeśli firma jest co najmniej średnia
Hurtowa dystrybucja żywności (hurtownie, centra dystrybucyjne zaopatrujące zewnętrznych odbiorców)	OBJĘTA	Jeśli firma jest co najmniej średnia
Sprzedaż detaliczna (sklepy, supermarkety)	CO DO ZASADY NIE	Sama sprzedaż detaliczna nie została wymieniona w sektorze
Lokalna, rzemieślnicza produkcja (np. piekarnia zaopatrująca kilka punktów)	WYMAGA ANALIZY	Ustawa mówi o produkcji „przemysłowej” – liczy się skala i sposób działania

SIEĆ SKLEPÓW Z WŁASNĄ PIEKARNIĄ – NA CO ZWRÓCIĆ UWAGĘ

Sklepy same w sobie nie czynią firmy podmiotem KSC. Decydujące jest to, co firma robi poza detalem.

- **Charakter piekarni:** zakład przemysłowy (skala wypieku, zautomatyzowane linie, liczba zatrudnionych) czy mała wytwórnia rzemieślnicza.
- **Komu piekarnia sprzedaje:** zaopatrywanie wyłącznie własnych sklepów to co innego niż dostawy do zewnętrznych odbiorców (inne sklepy, instytucje, hurt) – ta druga działalność może być uznana za dystrybucję hurtową.
- **Wielkość liczy się łącznie** z podmiotami powiązanymi i partnerskimi – w spółdzielniach i grupach zakupowych ustala się ją osobno dla każdego podmiotu i jego powiązań.
- **Inna działalność:** np. apteki ogólnodostępne to sektor ochrony zdrowia (załącznik nr 1) – odrębna przesłanka i inny status.

W przypadkach granicznych zalecamy formalną analizę zakwalifikowania, a nie „bezpieczne założenie".

KIEDY MNIEJSZA FIRMA TEŻ PODLEGA USTAWIE

Organ właściwy może decyzją administracyjną uznać mniejszą firmę za podmiot ważny lub kluczowy, jeżeli:

- jest jedynym świadczącym daną usługę o znaczeniu krytycznym społecznie lub gospodarczo,
- zakłócenie usług spowoduje poważne zagrożenie dla bezpieczeństwa, porządku publicznego lub życia i zdrowia ludzi,
- zakłócenie spowoduje ryzyko systemowe dla innych podmiotów kluczowych lub ważnych,
- świadczenie usług ma istotne znaczenie na poziomie krajowym lub województwa.

NAWET JEŚLI FIRMA NIE PODLEGA USTAWIE

- **RODO** obowiązuje każdą firmę – dane klientów (np. programy lojalnościowe), pracowników i monitoringu.
- **PCI DSS** – standard bezpieczeństwa dla firm przyjmujących płatności kartami.
- **Wymagania odbiorców:** kontrahenci objęci KSC muszą dbać o łańcuch dostaw i coraz częściej poproszą o potwierdzenie cyberbezpieczeństwa.

2.3. KOGO WLICZAĆ DO ZATRUDNIENIA

- pracowników na umowę o pracę – w sklepach, piekarni, magazynie i biurze
- osoby na umowie zlecenia, agencyjnej lub o świadczenie usług (w tym sezonowe)
- osoby na umowie o dzieło
- właścicieli-kierowników
- partnerów prowadzących regularną działalność i czerpiących z niej korzyści

NARZĘDZIE POMOCNICZE

PARP udostępnia bezpłatny **Kwalifikator MŚP**: kwalifikator.parp.gov.pl – pozwala ustalić wielkość przedsiębiorstwa z uwzględnieniem podmiotów partnerskich i powiązanych.

STATUS

03 PODMIOT WAŻNY – CO TO OZNACZA?

Sektor żywności jest w załączniku nr 2, dlatego firmy spożywcze są **podmiotami ważnymi** – niezależnie od tego, czy są średnie, czy duże. Merytoryczne obowiązki w zakresie SZBI są takie same jak podmiotu kluczowego. Różnice dotyczą nadzoru, audytów i wysokości kar.

CECHA	PODMIOT WAŻNY (SEKTOR ŻYWNOŚCI)	PODMIOT KLUCZOWY (DLA PORÓWNANIA)
Charakter nadzoru	ex post – reaktywny, po zdarzeniu	ex ante – proaktywny, bieżący
Audyt cykliczny	tylko na żądanie organu	co 3 lata + na żądanie organu
Obowiązek wdrożenia SZBI	**TAK – takie same wymagania**	TAK
Maks. kara administracyjna	7 mln EUR lub 1,4% przychodu	10 mln EUR lub 2% przychodu
Minimalna kara	15 000 zł	20 000 zł
Wczesne ostrzeżenie o incydencie (24 h)	TAK	TAK

PAMIĘTAJ

Jeśli firma spełnia jednocześnie kryteria podmiotu kluczowego i ważnego (np. oprócz sklepów prowadzi apteki ogólnodostępne), zawsze kwalifikuje się ją jako **podmiot kluczowy**.

MNIEJ NADZORU TO NIE MNIEJ OBOWIĄZKÓW

Terminy wdrożenia SZBI, zgłaszanie incydentów i odpowiedzialność zarządu są takie same jak dla podmiotów kluczowych. Organ może zażądać audytu w każdej chwili.

KALENDARZ WDROŻENIA

04 NAJWAŻNIEJSZE DATY

3 KWIETNIA 2026 MINĄŁ

Wejście ustawy w życie. Samoidentyfikacja – czy firma podlega obowiązkom KSC. Wszystkie firmy spożywcze

3 PAŹDZIERNIKA 2026 MINĄŁ

Termin wniosku o wpis do wykazu podmiotów kluczowych i ważnych (system S46). Podmioty ważne

3 KWIETNIA 2027

Pełne wdrożenie SZBI po raz pierwszy oraz podłączenie do systemu S46. Podmioty ważne

3 KWIETNIA 2028

Możliwość nakładania kar administracyjnych (poza ekstraordynaryjną). Podmioty ważne

NA ŻĄDANIE ORGANU

Audyt bezpieczeństwa systemu informacyjnego – brak obowiązku cyklicznego.

TERMIN WPISU DO WYKAZU MINĄŁ – NIE ZWLEKAJ

Wniosek o wpis składa się w ciągu 6 miesięcy od spełnienia przesłanek – dla firm istniejących w dniu wejścia ustawy w życie do 3 października 2026 r. Jeżeli firma spełnia przesłanki, a nie złożyła wniosku w systemie S46, powinna zrobić to **niezwłocznie**. Późniejsze zmiany danych zgłasza się w ciągu 14 dni.

UWAGA NA „KARĘ EKSTRAORDYNARYJNĄ"

Specjalna kara **do 100 mln zł** może być nałożona już od dnia wejścia ustawy w życie, jeżeli zaniedbanie spowoduje bezpośrednie i poważne zagrożenie dla obronności, bezpieczeństwa państwa, porządku publicznego lub życia i zdrowia ludzi. W branży spożywczej może to być incydent prowadzący do skażenia lub zafałszowania żywności albo poważnego zakłócenia jej dostaw.

OBOWIĄZKI

05 OBOWIĄZKI FIRMY KROK PO KROKU

01 SAMOOCENA
Czy firma spełnia warunki wielkości i rodzaju działalności (rozdział 2).

02 WNIOSEK O WPIS DO WYKAZU
Przez system S46 – w terminie 6 miesięcy od spełnienia przesłanek.

03 PODŁĄCZENIE DO S46
Dostęp, administratorzy konta, dyżury do zgłaszania incydentów.

04 OSOBY KONTAKTOWE
Minimum dwie (jedna w mikro- lub małej firmie).

05 STRUKTURA CYBERBEZPIECZEŃSTWA
Wewnętrzna komórka albo umowa z dostawcą usług zarządzanych.

06 WDROŻENIE SZBI
Obejmujące IT i automatykę produkcji – szczegóły w rozdziale 6.

07 WERYFIKACJA NIEKARALNOŚCI
Personelu realizującego zadania cyberbezpieczeństwa i obsługi incydentów.

08 SZKOLENIA
Kierownik raz w roku oraz cały personel – produkcja, magazyn, sklepy, biuro.

09 INFORMACJA DLA ODBIORCÓW
Dostęp do informacji o cyberzagrożeniach i kanał zgłaszania incydentów.

10 AUDYT
Obowiązkowy tylko na żądanie organu, ale zalecany przed 3.04.2027 r.

5.2. OSOBY KONTAKTOWE – KTO TO MOŻE BYĆ

Każda osoba związana z firmą umową o pracę lub innym stosunkiem zatrudnienia. Nie jest wymagane wykształcenie z cyberbezpieczeństwa, ale niezbędna jest dobra znajomość organizacji.

5.3. WEWNĘTRZNIE CZY OUTSOURCING?

Własna komórka (np. dział IT), umowa z dostawcą usług zarządzanych albo model mieszany. Zadań nie powinno się powierzać przeciążonemu help-deskowi. Przy własnej produkcji w zespole lub u dostawcy potrzebna jest też **wiedza o automatyce przemysłowej**.

SERCE WYMAGAŃ USTAWY

06 SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

SZBI wdraża się w systemie informacyjnym wykorzystywanym w procesach mających wpływ na świadczenie usługi – w firmie spożywczej obejmuje to m.in. ERP i księgowość, systemy magazynowe (WMS), zamówienia i EDI, kasy i POS, sterowanie produkcją (PLC, SCADA), monitoring temperatur i HACCP, śledzenie partii oraz sieć łączącą zakład, magazyn i sklepy.

6.1. SPECYFIKA BRANŻY SPOŻYWCZEJ – IT I OT

OBSZAR	TYPOWE SYSTEMY	TYPOWE RYZYKA
Produkcja (OT)	Sterowniki PLC, SCADA, piece, mieszarki, dozowniki, linie pakujące, wagi	Stare systemy bez aktualizacji, brak podziału sieci, zdalny dostęp serwisantów, brak kopii konfiguracji sterowników
Łańcuch chłodniczy	Czujniki i rejestratory temperatury, systemy HACCP	Zakłócenie lub fałszowanie odczytów, brak alarmów przy awarii, utrata dowodów zgodności
Magazyn i logistyka	WMS, terminale, skanery, EDI z odbiorcami	Ransomware zatrzymujący wydania, brak planu pracy „na papierze”
Sprzedaż	Kasy, POS, terminale płatnicze, programy lojalnościowe, e-commerce	Wyciek danych klientów i kart, przestój sprzedaży w wielu sklepach naraz
Administracja	ERP, księgowość, poczta, HR	Phishing, wyłudzenia faktur, przejęcie kont uprzywilejowanych

6.2. CO MUSI OBEJMOWAĆ SZBI

POLITYKI I PROCEDURY

- polityka szacowania ryzyka i polityka bezpieczeństwa systemu informacyjnego
- polityki tematyczne, np. urządzenia mobilne, zdalny dostęp serwisantów
- kontrola dostępu – kto i do czego (ERP, dane klientów, sterowniki linii)
- kryptografia i szyfrowanie
- ocena skuteczności wdrożonych środków

RYZYKO I INCYDENTY

- systematyczne szacowanie ryzyka i zarządzanie nim
- informacje o cyberzagrożeniach i podatnościach
- procedury zarządzania i obsługi incydentów
- BCP, plany awaryjne (ISCP) i odtworzenia (DRP) – np. jak piec chleb i wydawać towar, gdy padnie system

BEZPIECZEŃSTWO TECHNICZNE

- bezpieczeństwo nabywania, rozwoju i eksploatacji systemów – także maszyn i linii z oprogramowaniem
- bezpieczeństwo fizyczne – serwerownie, szafy sterownicze, magazyny
- łańcuch dostaw – dostawcy ERP, WMS, POS, integratorzy i serwisanci maszyn
- ciągły monitoring – logi, alerty, korelacja zdarzeń
- kopie zapasowe, także odizolowane (offline), z testami odtwarzania
- regularne aktualizacje zgodnie z zaleceniami producenta
- MFA – zdalny dostęp, ERP, konta uprzywilejowane
- inwentaryzacja IT i OT (sterowniki, czujniki, kasy, terminale), kontrola nośników
- dobra praktyka: oddzielne sieci – biurowa, produkcyjna, płatnicza i gościnna

ZASOBY LUDZKIE

- weryfikacja personelu, postanowienia o poufności
- szkolenia dla całego personelu: produkcja, magazyn, sprzedawcy, biuro, zarząd
- podstawowe zasady cyberhigieny
- bezpieczne kanały komunikacji wewnątrz firmy i z innymi podmiotami KSC

WERYFIKACJA NIEKARALNOŚCI

Osoby realizujące zadania SZBI i zgłaszania incydentów przedstawiają zaświadczenie o niekaralności za przestępstwa przeciwko ochronie informacji (rozdz. XXXIII Kodeksu karnego, art. 265–269b). Wyjątek: osoba z ważnym poświadczeniem bezpieczeństwa „poufne” lub wyższym.

6.3. DOKUMENTACJA SZBI

DOKUMENTACJA NORMATYWNA

opisuje usługę, systemy, infrastrukturę i bezpieczeństwo:

- dokumentacja SZBI
- ochrona infrastruktury (serwerownie, sieci, sieć produkcyjna)
- zarządzanie ciągłością działania (BCP/DRP)
- dokumentacja techniczna systemu informacyjnego
- specyfika sektora – powiązanie z HACCP, wycofaniem produktu i ochroną żywności przed celowym zanieczyszczeniem

DOKUMENTACJA OPERACYJNA

potwierdza wykonywanie czynności:

- rejestry i protokoły
- automatycznie generowane logi systemowe
- raporty z monitoringu i ze szkoleń

Firmy z HACCP, ISO 22000, BRC lub IFS mają nawyk dokumentowania i audytów – SZBI można oprzeć na istniejących procedurach.

UWAGA NA „PAPIEROWY SZBI”

Dokumentacja kupiona „w pakiecie NIS2”, podpisana przez zarząd i schowana w szafie, nie zapewni zgodności z ustawą. Wymagane jest realne wdrożenie – przetestowane procedury, świadomy personel, działające zabezpieczenia techniczne.

INCYDENTY

07 ZGŁASZANIE INCYDENTÓW

Każdym incydentem trzeba zarządzać, ale obowiązkowemu zgłoszeniu do CSIRT podlegają **incydenty poważne** – powodujące lub mogące spowodować poważne obniżenie jakości lub przerwanie usługi (np. zatrzymanie produkcji lub dostaw żywności), straty finansowe albo poważną szkodę u innych osób.

24 h	72 h	30 dni	na żądanie
WCZESNE OSTRZEŻENIE	PEŁNE ZGŁOSZENIE	SPRAWOZDANIE KOŃCOWE	SPRAWOZDANIE OKRESOWE
Identyfikacja podmiotu, zgłaszający, moment wykrycia, czy działanie bezprawne, wpływ transgraniczny.	Wpływ (zakłady, magazyny, sklepy, odbiorcy), zasięg, przyczyny, działania naprawcze.	Szczegółowy opis, źródło, środki ograniczające ryzyko, skutki transgraniczne.	Działania w trakcie obsługi incydentu.

KOMU ZGŁASZAĆ

Przez system S46 do właściwego CSIRT – sektorowego, jeśli powołano go dla sektora, w pozostałych przypadkach do CSIRT poziomu krajowego (dla firm komercyjnych co do zasady **CSIRT NASK – info@cert.pl**). Gdy incydent dotyka kilku sektorów, wystarczy jedno zgłoszenie. CSIRT GOV i CSIRT MON obsługują administrację publiczną i sektor obronny.

OBOWIĄZEK INFORMOWANIA ODBIORCÓW

Firma informuje odbiorców (klientów, kontrahentów, sieci handlowe) o incydencie poważnym, jeśli ma on niekorzystny wpływ na świadczenie usług – wraz z informacją o możliwych środkach zapobiegawczych.

INCYDENT TO CZĘSTO WIĘCEJ NIŻ JEDEN OBOWIĄZEK

- **Dane osobowe** klientów lub pracowników – osobne zgłoszenie do UODO w ciągu 72 godzin (RODO).
- **Bezpieczeństwo żywności** – jeśli incydent dotknął receptur, parametrów produkcji lub chłodzenia, równolegle uruchom procedury HACCP i wycofania produktu (art. 19 rozp. 178/2002).
- **Dane płatnicze** – przy incydencie z kartami skontaktuj się z bankiem rozliczającym.

AUDYTY

08 AUDYTY BEZPIECZEŃSTWA

Audyt to formalne sprawdzenie zgodności z ustawą i skuteczności SZBI – dotyczy całego systemu informacyjnego firmy, a nie tylko jego części.

STATUS	CYKLICZNOŚĆ	PIERWSZY AUDYT
Podmiot ważny (sektor żywności)	tylko na żądanie organu właściwego	brak obowiązku cyklicznego
Podmiot kluczowy (dla porównania)	co najmniej raz na 3 lata + na żądanie organu	do 3 kwietnia 2028 r.

8.2. KTO MOŻE BYĆ AUDYTOREM

- akredytowana jednostka oceniająca zgodność w zakresie bezpieczeństwa systemów informacyjnych
- co najmniej dwóch audytorów z certyfikatami (np. CISA, CISM, CISSP, ISO 27001 LA, ISO 22301 LA, CRISC, SSCP, ISA/IEC 62443 Cybersecurity Expert) lub odpowiednim doświadczeniem (3 lata praktyki albo 2 lata + studia podyplomowe)
- CSIRT sektorowy

OGRANICZENIE NIEZALEŻNOŚCI

Audytu nie przeprowadzi osoba, która w tej firmie realizuje – lub w ciągu roku przed audytem realizowała – zadania SZBI lub zgłaszania incydentów. To ważne, jeśli rozważasz audyt siłami własnego działu IT.

8.3. DLACZEGO WARTO, CHOĆ NIEOBOWIĄZKOWO

WIESZ, OD CZEGO ZACZĄĆ
Analiza luk przed 3.04.2027 r. pozwala zaplanować budżet i kolejność działań.

DOWÓD NALEŻYTEJ STARANNOŚCI
Zarząd ma udokumentowane świadome zarządzanie ryzykiem – ważne wobec odpowiedzialności osobistej.

ARGUMENT WOBEC KONTRAHENTÓW
Odbiorcy objęci KSC zapytają o bezpieczeństwo łańcucha dostaw.

GOTOWOŚĆ NA ŻĄDANIE ORGANU
Gdy organ zażąda audytu, firma nie zaczyna od zera.

Audyt na żądanie organu musi przeprowadzić audytor spełniający warunki z punktu 8.2.

8.4. JAK PRZEBIEGA AUDYT W FIRMIE SPOŻYWCZEJ

01 ZAKRES
Systemy, lokalizacje (zakład, magazyn, sklepy) i procesy – w tym granica między IT a automatyką produkcji.

02 INWENTARYZACJA
Serwery, stacje, sterowniki, czujniki, kasy, urządzenia sieciowe, usługi w chmurze.

03 ANALIZA RYZYKA
Zagrożenia dla ciągłości produkcji, dostaw i sprzedaży oraz bezpieczeństwa żywności.

04 DOKUMENTY I WYWIADY
Polityki, procedury, plany ciągłości, rozmowy z kierownictwem, IT i produkcją.

05 WERYFIKACJA TECHNICZNA
Konfiguracja, podział sieci, kopie i test odtwarzania, dostęp zdalny, uprawnienia.

06 RAPORT I PLAN NAPRAWCZY
Wyniki z oceną ryzyka, priorytety, rekomendowany harmonogram i budżet.

ZARZĄD

09 ODPOWIEDZIALNOŚĆ KIEROWNIKA FIRMY

Kierownikiem podmiotu jest członek zarządu lub innego organu zarządzającego – zwykle prezes lub członek zarządu spółki, zarząd spółdzielni albo właściciel prowadzący działalność.

- decyzje o przygotowaniu, wdrożeniu, przeglądzie i nadzorze SZBI
- adekwatne środki finansowe na cyberbezpieczeństwo w budżecie
- przydzielanie zadań i nadzór nad ich wykonaniem
- świadomość obowiązków wśród personelu
- zgodność z ustawą i regulacjami wewnętrznymi
- weryfikacja niekaralności osób realizujących zadania
- coroczne obowiązkowe szkolenie z cyberbezpieczeństwa

ODPOWIEDZIALNOŚĆ OSOBISTA

Kierownik odpowiada osobiście za wykonanie obowiązków – także gdy delegował je na inną osobę za jej zgodą. Maksymalna kara dla kierownika podmiotu prywatnego: **do 300% wynagrodzenia**.

SANKCJE

10 KARY PIENIĘŻNE

Kary nakłada organ właściwy – dla sektora żywności co do zasady minister właściwy do spraw rolnictwa – od 3 kwietnia 2028 r. (z wyjątkiem kary ekstraordynaryjnej, obowiązującej od dnia wejścia ustawy w życie).

FIRMA · PODMIOT WAŻNY

7 mln EUR lub 1,4% przychodu

decyduje kwota wyższa · minimum 15 000 zł

KIEROWNIK FIRMY

do 300% wynagrodzenia

podmiot prywatny (w tym spółka i spółdzielnia); w podmiocie publicznym do 100%

KARA OKRESOWA

500 – 100 000 zł / dzień

za każdy dzień opóźnienia w wykonaniu decyzji

KARA EKSTRAORDYNARYJNA · OD 3.04.2026

do 100 mln zł

bezpośrednie i poważne cyberzagrożenie dla państwa, porządku publicznego lub życia i zdrowia oraz ryzyko poważnej szkody lub utrudnień w usługach

10.5. NAJCZĘSTSZE PRZYCZYNY NAKŁADANIA KAR

- brak wpisu do wykazu w terminie lub niezgodne dane
- brak systematycznego szacowania ryzyka
- niewdrożenie SZBI lub jego niezgodność z wymogami
- niezgłoszenie lub nieobsłużenie incydentu poważnego
- nieinformowanie odbiorców o incydencie poważnym
- utrudnianie kontroli lub pracy urzędnika monitorującego
- nieprzekazywanie informacji i dokumentów na żądanie
- niewykonanie zaleceń pokontrolnych w terminie
- niewdrożenie polecenia zabezpieczającego w terminie
- brak współpracy z CSIRT podczas obsługi incydentu
- brak struktury cyberbezpieczeństwa lub umowy z dostawcą
- nieprzeprowadzenie audytu, którego zażądał organ

10.6. GWARANCJE PROCEDURALNE

01
Ostrzeżenie wskazujące czynności zapobiegające naruszeniu, wraz z terminem.

02
Informacja o wstępnych ustaleniach mogących prowadzić do kary, z uzasadnieniem.

03
7 dni na stanowisko firmy – organ musi się do niego ustosunkować.

Organ może odstąpić od ostrzeżenia, jeśli utrudniłoby to natychmiastowe działanie wobec incydentu lub zagroziło bezpieczeństwu państwa.

WSPARCIE

11 OD CZEGO ZACZĄĆ

01 USTAL STATUS FIRMY
Kwalifikator MŚP (PARP) i ocena, czy działalność to produkcja przemysłowa lub hurt.

02 ZŁÓŻ WNIOSEK W S46
Jeśli firma podlega ustawie, a nie ma jeszcze wpisu do wykazu.

03 WYZNACZ LIDERA PROJEKTU
Osobę odpowiedzialną za wdrożenie KSC – z poparciem zarządu.

04 SZKOLENIE ZARZĄDU
Bezpłatne szkolenia Ministerstwa Cyfryzacji budują świadomość kierownictwa.

05 WSTĘPNA INWENTARYZACJA
ERP, WMS, POS i kasy, sterowniki i SCADA linii, monitoring temperatur, urządzenia osobiste, zdalny dostęp serwisantów.

06 WSTĘPNE SZACOWANIE RYZYKA
Największe luki – zacznij od kopii zapasowych i dostępu zdalnego.

07 PLAN WDROŻENIA Z BUDŻETEM
Kamienie milowe dopasowane do kalendarza ustawy, w tym do 3 kwietnia 2027 r.

08 AUDYT GOTOWOŚCI I PARTNER
Współpraca z dostawcą usług zarządzanych, jeśli firma nie ma własnych zasobów. Zarezerwuj środki – to inwestycja, nie koszt.

PRAKTYCZNA WSKAZÓWKA – UWIERZYTELNIANIE WIELOSKŁADNIKOWE

Ministerstwo Cyfryzacji szczególnie rekomenduje MFA wszędzie, gdzie to możliwe. W firmie spożywczej przede wszystkim: zdalny dostęp do sieci i systemów (także dla serwisantów maszyn), konta uprzywilejowane oraz dostęp do ERP i danych klientów. To jeden z najprostszych środków, który drastycznie obniża ryzyko skutecznego ataku.

OFICJALNE ŹRÓDŁA WIEDZY

- cyber.gov.pl – rekomendacje i ostrzeżenia
- moje.cert.pl – materiały edukacyjne i alerty CERT Polska
- gov.pl/web/baza-wiedzy/harmonogramszkolen – bezpłatne szkolenia MC
- gov.pl/web/system-s46/uzyskaj-dostep – dostęp do systemu S46
- kwalifikator.parp.gov.pl – Kwalifikator MŚP

AKTY PRAWNE

- Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (po nowelizacji), załącznik nr 2
- Dyrektywa NIS2 (UE) 2022/2555
- Rozporządzenie (WE) nr 178/2002 – prawo żywnościowe
- Rozporządzenie wykonawcze Komisji (UE) 2024/2690

Zastrzeżenie. Broszura ma charakter informacyjny i nie stanowi opinii ani porady prawnej. Opracowana na podstawie publikacji Ministerstwa Cyfryzacji „Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa po nowelizacji – Pytania i odpowiedzi" oraz przepisów załącznika nr 2 do ustawy i dyrektywy NIS2; stan na październik 2026 r. Zakwalifikowanie konkretnej firmy (zwłaszcza piekarni i produkcji o niejasnym charakterze) wymaga indywidualnej analizy; w razie wątpliwości warto skonsultować się z radcą prawnym i sprawdzić aktualny stan prawny na cyber.gov.pl.

PARTNER WDROŻENIA

SPRAWDŹ, CZY TWOJA FIRMA PODLEGA USTAWIE.



Skontaktuj się z nami – wspólnie ocenimy status firmy i zaplanujemy wdrożenie. Łączymy automatykę linii produkcyjnych z cyberbezpieczeństwem IT, więc zabezpieczamy całość: od pieca i pakowaczki po kasy w sklepach.

01
AUTOMATYKA I AKPIA
Sterowniki PLC, SCADA i linie produkcyjne – projekt, utrzymanie i bezpieczna integracja z IT.

02
CYBERBEZPIECZEŃSTWO OT/IT
Inwentaryzacja, analiza ryzyka, podział sieci i monitoring zakładu, magazynu oraz sklepów.

03
ZGODNOŚĆ Z KSC / NIS2
Samoidentyfikacja, wpis do S46, wdrożenie SZBI i audyt gotowości przed 3.04.2027.

OD 2011
na rynku automatyki przemysłowej

OT + IT
automatycy i specjaliści cyber w jednym zespole

24H
serwis wsparcia dla zakładów i linii

BEZ PRZESTOJU
zabezpieczamy instalację bez zatrzymywania produkcji

KOMÓRKA CYBERBEZPIECZEŃSTWA
+48 512 696 638

CENTRALA · SERWIS WSPARCIA 24H
+48 500 440 810

E-MAIL
info@setcontrol.pl

ADRES
SETCONTROL Sp. z o.o.
Warszewka 14, 09-210 Drobin

WWW
setcontrol.pl