SETCONTROL

BROSZURA INFORMACYJNA · NIS2 / KSC

SEKTOR: PRODUKCJA PRZEMYSŁOWA

NIS2 & KSC W ZAKŁADZIE PRODUKCYJNYM



Obowiązki wynikające z nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa dla przedsiębiorstw produkcyjnych – od sterowników PLC i systemów SCADA po ERP i MES. Kto podlega ustawie, co trzeba wdrożyć, jakie są terminy i kary.

WEJŚCIE W ŻYCIE

03.04.2026

Samoidentyfikacja – firma sama ocenia, czy podlega ustawie.

WPIS DO S46 · MINĄŁ

03.10.2026

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

SZBI

03.04.2027

Pełne wdrożenie SZBI i podłączenie do systemu S46.

KARY

03.04.2028

Start nakładania standardowych kar pieniężnych.

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

KLASYFIKACJA PODMIOTÓW

01 KTO PODLEGA USTAWIE?

Produkcja przemysłowa znalazła się w **załączniku nr 2** do ustawy o KSC – wśród sektorów „innych krytycznych". Oznacza to, że co najmniej średnie przedsiębiorstwo produkcyjne z objętej branży jest **podmiotem ważnym** – niezależnie od tego, czy jest średnie, czy duże.

Ustawa działa na zasadzie **samoidentyfikacji**: to firma sama ocenia, czy podlega obowiązkom, a ryzyko błędnej oceny ponosi jej zarząd.

BRANŻE PRODUKCJI OBJĘTE USTAWĄ

- wyroby medyczne i wyroby do diagnostyki in vitro
- komputery, wyroby elektroniczne i optyczne
- urządzenia elektryczne
- maszyny i urządzenia
- pojazdy samochodowe, przyczepy i naczepy
- pozostały sprzęt transportowy

Osobnymi sektorami załącznika nr 2 są m.in. **chemikalia** (produkcja i dystrybucja) oraz **żywność** (produkcja, przetwarzanie i dystrybucja) – dla branży spożywczej przygotowaliśmy osobną broszurę.

PROGI WIELKOŚCI PRZEDSIĘBIORSTWA

WIELKOŚĆ	ZATRUDNIENIE	ROCZNY OBRÓT / SUMA BILANSOWA	STATUS W KSC
Mikro	< 10 osób	≤ 2 mln EUR	CO DO ZASADY POZA USTAWĄ
Mała	< 50 osób	≤ 10 mln EUR	CO DO ZASADY POZA USTAWĄ
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

Wielkość liczy się łącznie z przedsiębiorstwami powiązanymi i partnerskimi. Pomoże bezpłatny Kwalifikator MŚP: kwalifikator.parp.gov.pl.

KIEDY ZAKŁAD PRODUKCYJNY MOŻE STAĆ SIĘ PODMIOTEM KLUCZOWYM

- **Podmiot krytyczny (dyrektywa CER)** – przedsiębiorstwo uznane za podmiot krytyczny, np. kluczowy dostawca dla energetyki, transportu czy obronności, jest podmiotem kluczowym niezależnie od wielkości.
- **Decyzja organu** – organ właściwy może uznać także mniejszą firmę za podmiot ważny lub kluczowy, jeśli jest jedynym dostawcą usługi o krytycznym znaczeniu albo zakłócenie jej działania stworzyłoby poważne lub systemowe zagrożenie.
- **Kilka rodzajów działalności** – jeśli firma spełnia jednocześnie kryteria podmiotu kluczowego i ważnego, kwalifikuje się ją jako kluczowy.

PODMIOT WAŻNY – MNIEJ NADZORU, TE SAME OBOWIĄZKI

Nadzór ex post (po zdarzeniu), audyt tylko na żądanie organu. Wymagania SZBI, zgłaszanie incydentów i odpowiedzialność zarządu są **takie same** jak dla podmiotów kluczowych.

ORGAN WŁAŚCIWY

Dla produkcji przemysłowej co do zasady minister właściwy do spraw gospodarki. Incydenty zgłasza się przez system S46 – dla firm prywatnych co do zasady do CSIRT NASK.

KALENDARZ WDROŻENIA

02 KLUCZOWE TERMINY

3 KWIETNIA 2026 MINĄŁ

Wejście ustawy w życie. Samoidentyfikacja – ustalenie, czy firma podlega obowiązkom KSC.

3 PAŹDZIERNIKA 2026 MINĄŁ

Wniosek o wpis do wykazu podmiotów kluczowych i ważnych w systemie S46 (6 miesięcy od spełnienia przesłanek). Jeśli wniosku nie złożono – zrób to niezwłocznie. Zmiany danych zgłasza się w ciągu 14 dni.

3 KWIETNIA 2027

Pełne wdrożenie SZBI i podłączenie do systemu S46: polityki, procedury, szacowanie ryzyka IT/OT, monitoring, łańcuch dostaw, dyżury do zgłaszania incydentów.

3 KWIETNIA 2028

Start nakładania **standardowych kar pieniężnych**. Pierwszy obowiązkowy audyt dla podmiotów kluczowych. Podmioty ważne – audyt na żądanie organu.

KARA EKSTRAORDYNARYJNA OBOWIĄZUJE OD PIERWSZEGO DNIA

Do 100 mln zł – gdy zaniedbanie powoduje bezpośrednie i poważne zagrożenie dla bezpieczeństwa państwa, porządku publicznego lub życia i zdrowia ludzi. Bez okresu przejściowego.

ZGŁASZANIE INCYDENTÓW POWAŻNYCH

03 ZEGAR INCYDENTU

0 h	24 h	72 h	1 mies.
WYKRYCIE	WCZESNE OSTRZEŻENIE	PEŁNE ZGŁOSZENIE	RAPORT KOŃCOWY
Start wszystkich terminów. Brak monitoringu = brak wykrycia = spóźnione zgłoszenie.	Zgłoszenie wstępne do CSIRT przez system S46.	Opis zdarzenia, zasięg, skutki, działania naprawcze.	Przyczyny, wdrożone środki, skutki transgraniczne.

PRZYKŁADY INCYDENTÓW DO ZGŁOSZENIA W PRODUKCJI

- ransomware szyfrujący ERP / MES i wstrzymujący produkcję
- nieautoryzowany dostęp do sterowników PLC lub systemów SCADA, zmiana parametrów procesu
- atak na sterowanie robotami i maszynami, sabotaż oprogramowania sterującego
- wyciek dokumentacji technicznej lub danych klientów, DDoS na systemy zamówień i logistyki

Naruszenie danych osobowych wymaga dodatkowo osobnego zgłoszenia do UODO w ciągu 72 godzin (RODO).

WYMAGANIA SZBI

04 CO MUSI WDROŻYĆ ZAKŁAD PRODUKCYJNY?

Sektor produkcji wymaga szczególnej uwagi na środowiska OT – sterowniki PLC, systemy SCADA i sieci przemysłowe, które historycznie projektowano bez myśli o cyberbezpieczeństwie.

01 SZACOWANIE RYZYKA IT I OT
Linie produkcyjne, PLC, sieci przemysłowe, SCADA oraz ERP i MES. Rejestr ryzyk aktualizowany co najmniej raz w roku i po każdym istotnym incydencie.

02 POLITYKI BEZPIECZEŃSTWA
Ogólne i tematyczne: dostęp, hasła, urządzenia mobilne, praca zdalna, nośniki wymienne. Zatwierdza i przegląda kierownictwo.

03 BEZPIECZEŃSTWO SYSTEMÓW IT/OT
Nabywanie, wdrażanie, utrzymanie i aktualizacja: PLC, SCADA/HMI, robotyka, MES, ERP, CMMS.

04 BEZPIECZEŃSTWO FIZYCZNE
Kontrola dostępu do hal, serwerowni, szaf sterowniczych i rozdzielni. Ochrona przed zalaniem, pożarem i temperaturą.

05 KADRY I WERYFIKACJA PERSONELU
Zaświadczenia o niekaralności dla osób realizujących zadania SZBI. Natychmiastowe odbieranie dostępów, zasada minimalnych uprawnień.

06 ŁAŃCUCH DOSTAW ICT
Dostawcy ERP/MES, chmury, serwisanci maszyn ze zdalnym dostępem, integratorzy automatyki – wymagania bezpieczeństwa w umowach.

07 CIĄGŁOŚĆ DZIAŁANIA (BCP / DRP)
Scenariusze: ransomware na ERP/MES, atak na sterowanie linią, sabotaż PLC, utrata zasilania. Testy co najmniej raz w roku.

08 MONITORING CIĄGŁY I LOGI
Zbieranie i analiza logów IT i OT, SIEM z obsługą protokołów przemysłowych, alerty na zmiany konfiguracji sterowników.

09 SZKOLENIA I CYBERHIGIENA
Dla wszystkich – także operatorów maszyn i służb utrzymania ruchu. Testy phishingowe, procedury zgłaszania.

10 UWIERZYTELNIANIE WIELOSKŁADNIKOWE
Zdalny dostęp do IT/OT, konta uprzywilejowane, dostęp serwisantów do PLC/SCADA.

11 AKTYWA I AKTUALIZACJE
Inwentaryzacja i aktualizacje: serwery, ERP/MES, firmware PLC, SCADA/HMI, systemy wbudowane. Plan dla urządzeń bez wsparcia (EOL).

12 KRYPTOGRAFIA I SZYFROWANIE
Dane w spoczynku (receptury, projekty, dane klientów) i w transmisji – VPN dla serwisu, szyfrowanie komunikacji tam, gdzie to możliwe.

UWAGA NA „PAPIEROWY SZBI"
Dokumentacja kupiona „w pakiecie NIS2", podpisana i schowana w szafie, nie zapewni zgodności. Wymagane jest realne wdrożenie – przetestowane procedury, świadomy personel i działające zabezpieczenia techniczne.

KARY PIENIĘŻNE

05 ILE KOSZTUJE ZANIECHANIE

PODMIOT WAŻNY · KARA MAKSYMALNA

7 mln EUR lub 1,4% przychodu

decyduje kwota wyższa · minimum 15 000 zł

PODMIOT KLUCZOWY · KARA MAKSYMALNA

10 mln EUR lub 2% przychodu

decyduje kwota wyższa · minimum 20 000 zł

KARA OKRESOWA

500 – 100 000 zł / dzień

za każdy dzień opóźnienia w wykonaniu decyzji

KIEROWNIK PODMIOTU PRYWATNEGO

do 300% wynagrodzenia

odpowiedzialność osobista – także przy delegowaniu zadań

KARA EKSTRAORDYNARYJNA · OD DNIA WEJŚCIA USTAWY W ŻYCIE

do 100 mln zł

przy bezpośrednim i poważnym zagrożeniu dla bezpieczeństwa państwa, porządku publicznego lub życia i zdrowia ludzi

Przed nałożeniem kary organ kieruje ostrzeżenie, informuje o wstępnych ustaleniach i daje 7 dni na stanowisko. Standardowe kary – od 3.04.2028 r.

TYPOWE SCENARIUSZE ATAKÓW

06 JAK WYGLĄDA ATAK NA ZAKŁAD PRODUKCYJNY

WEKTOR WEJŚCIA	CO SIĘ DZIEJE	CZEGO TO UCZY
Niezałatana bramka VPN / firewall	Ransomware przez tygodnie porusza się po sieci, a potem szyfruje ERP, serwery z dokumentacją CAD/CAM i plany produkcji. Linia staje.	Aktualizacje urządzeń brzegowych z tym samym priorytetem co serwerów; segmentacja IT/OT ogranicza zasięg ataku.
Nieaktywne konto serwisowe integratora	Ktoś loguje się do SCADA i zmienia parametry procesu. Bez alertów zmiana zostaje niezauważona, a wadliwa partia trafia do klientów.	Konta serwisowe z terminem ważności, MFA i rejestracją sesji; alarm na każdą zmianę konfiguracji PLC/SCADA.
Phishing / infostealer u pracownika	Przejęte konto daje dostęp do sieci; atak „living-off-the-land” bez klasycznego malware, kradzież danych i podwójny szantaż.	EDR i centralny SIEM z korelacją logów; szkolenia i MFA na kontach użytkowników.
Kopie zapasowe w tej samej sieci	Ransomware szyfruje również backupy – odtworzenie trwa tygodnie zamiast godzin.	Reguła 3-2-1-1: jedna kopia odizolowana (offline), testy odtwarzania.

PLAN DZIAŁANIA

07 DZIAŁANIA PRIORYTETOWE DLA PRODUKCJI

01 SAMOIDENTYFIKACJA STATUSU
Sprawdź PKD, zatrudnienie i obroty (z podmiotami powiązanymi). Oceń, czy branża jest w załączniku nr 2 i czy firma nie jest podmiotem krytycznym (CER).

02 WPIS DO WYKAZU W S46
Termin minął 3.10.2026 r. Jeżeli firma spełnia przesłanki, a wniosku nie ma w systemie – złóż go niezwłocznie (Profil Zaufany lub e-dowód).

03 INWENTARYZACJA AKTYWÓW IT/OT
Serwery, stacje, ERP/MES, sterowniki PLC, SCADA/HMI, roboty, switche i firewalle OT. Nie da się chronić tego, czego się nie zna.

04 SEGMENTACJA SIECI IT/OT
Oddzielenie sieci biurowej od produkcyjnej (strefa DMZ, firewall OT), kontrola ruchu między strefami, brak bezpośredniego dostępu z internetu do OT.

05 AKTUALIZACJE: VPN, FIREWALLE, PLC, SCADA
Regularne łatanie urządzeń brzegowych, zarządzanie firmware sterowników i oprogramowaniem SCADA, plan dla urządzeń EOL.

06 KONTROLA DOSTĘPU SERWISANTÓW I DOSTAWCÓW
MFA dla połączeń zdalnych, konta z terminem ważności, zasada minimalnych uprawnień, rejestrowanie sesji do OT.

07 MONITORING CIĄGŁY I ALERTY OT
EDR na stacjach i serwerach, SIEM z korelacją logów IT i OT, alerty na zmiany konfiguracji PLC, nowe połączenia i ruch lateralny.

08 KOPIE ZAPASOWE OFFLINE (3-2-1-1)
Trzy kopie, dwa nośniki, jedna poza zakładem, jedna odizolowana. Zakres: ERP, CAD/CAM, konfiguracje PLC/SCADA, MES. Testy odtwarzania co kwartał.

09 BCP / DRP Z TESTAMI
Praca „na papierze” przy awarii ERP, przejście na sterowanie ręczne przy ataku na PLC, utrata zasilania. Testy co najmniej raz w roku, dokumentacja dostępna offline.

10 GOTOWOŚĆ AUDYTOWA
Kompletna dokumentacja SZBI: polityki, rejestr ryzyk, procedury, rejestr incydentów, raporty z testów, inwentaryzacja. Audyt dobrowolny przed 3.04.2027 pokaże luki.

SPECYFIKA OT

08 CYBERBEZPIECZEŃSTWO OT W PRODUKCJI

Automatyka to nasza codzienność – sami projektujemy szafy sterownicze i programujemy PLC. Dlatego wiemy, gdzie w zakładzie są słabe punkty i jak je zabezpieczyć bez zatrzymywania linii.

TYPOWE SYSTEMY OT W ZAKŁADZIE

- sterowniki PLC (Siemens, Beckhoff, ABB, Rockwell, Schneider)
- systemy SCADA / HMI sterowania procesem
- roboty przemysłowe i maszyny CNC
- systemy zarządzania produkcją (MES)
- systemy wizyjne i kontroli jakości
- sieci przemysłowe: Profinet, EtherNet/IP, Modbus
- CMMS – utrzymanie ruchu
- klimatyzacja i warunki środowiskowe

NAJCZĘSTSZE SŁABOŚCI

- płaska sieć – brak segmentacji IT/OT
- przestarzałe systemy bez wsparcia producenta (EOL)
- zdalny dostęp serwisantów bez MFA
- aktywne konta po zakończeniu umów serwisowych
- brak monitoringu i alertów w sieci OT
- kopie zapasowe w tej samej sieci
- brak procedury reagowania na incydent OT
- domyślne hasła w urządzeniach przemysłowych

ZALECANE ŚRODKI TECHNICZNE

- firewall IT/OT i przemysłowa strefa DMZ
- MFA dla wszystkich połączeń zdalnych do OT
- SIEM z obsługą protokołów przemysłowych
- EDR na stacjach inżynierskich i HMI
- zarządzanie aktualizacjami firmware PLC/SCADA
- kopie konfiguracji sterowników offline
- NAC – kontrola dostępu do sieci OT
- pasywny monitoring ruchu OT (IDS przemysłowy)

KLUCZOWE DOKUMENTY SZBI

- polityka bezpieczeństwa systemów OT
- procedura dostępu serwisantów zewnętrznych
- plan ciągłości działania linii (BCP)
- procedura reagowania na incydent (IRP)
- rejestr aktywów IT/OT
- polityka aktualizacji OT
- weryfikacja i klasyfikacja dostawców ICT
- rejestr ryzyk IT/OT z planem postępowania

Źródła: ustawa z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa (po nowelizacji) wraz z załącznikiem nr 2; dyrektywa (UE) 2022/2555 (NIS2); publikacja Ministerstwa Cyfryzacji „Ustawa o KSC po nowelizacji – pytania i odpowiedzi"; cyber.gov.pl. Stan prawny: październik 2026 r. Materiał informacyjny – nie stanowi porady prawnej. Zakwalifikowanie konkretnej firmy wymaga indywidualnej analizy.

PARTNER WDROŻENIA

NIE MUSICIE WDRAŻAĆ TEGO SAMI.



Kompleksowo wspieramy zakłady produkcyjne w obowiązkach z ustawy o KSC i dyrektywy NIS2 – od inwentaryzacji aktywów, przez audyt, po wdrożenie SZBI i modernizację infrastruktury OT/IT. Pierwsza konsultacja KSC jest bezpłatna.

01
INWENTARYZACJA I AUDYT
Inwentaryzacja sieci IT/OT, audyt cyberbezpieczeństwa i zgodności z KSC, analiza luk względem ISO 27001.

02
SZBI I DOKUMENTACJA
Polityki, procedury, rejestr ryzyk, BCP/DRP, procedury zgłaszania incydentów i szkolenia zarządu.

03
MODERNIZACJA OT
Segmentacja sieci, bezpieczny zdalny dostęp, modernizacja sterowni, PLC i SCADA, monitoring.

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 procesu

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