

Cyberbezpieczeństwo i NIS2 • Moduł II: Jak przygotować organizację do wymagań NIS2 i KSC

Szkolenie otwarte • 18.09.2026 • Organizator: Platforma Wiedzy

Prowadzący: **Paweł Maliszewski**, Perfectinfo Sp. z o.o.

W tym Module:

1. SZBI jako fundament organizacji
2. MODEL PRZYGOTOWANIA DO NIS2 – KROK PO KROKU
3. Bezpieczeństwo łańcucha dostaw
4. Nadzór, audyty i pomiar skuteczności

Plan dnia:

9:00–10:30 • Moduł I: NIS2 i nowelizacja KSC – wymagania, zakres obowiązków i odpowiedzialność

10:30–10:45 • Przerwa

 **10:45–12:15** • **Moduł II: Jak przygotować organizację do wymagań NIS2 i KSC – jesteśmy tutaj**

12:15–12:45 • Przerwa obiadowa

12:45–15:00 • Moduł III: Incydenty, pracownicy i współczesne zagrożenia (krótka przerwa ok. 13:45)



SZBI: czym jest i jak łączy się z NIS2 i KSC

System Zarządzania Bezpieczeństwem Informacji (SZBI) to sposób zarządzania, a nie program ani segregator: organizacja ustala, co chroni i przed czym, wdraża zabezpieczenia, sprawdza, czy działają, i je poprawia. Obejmuje system informacyjny wykorzystywany w procesach wpływających na świadczenie usługi (art. 8 ust. 1 KSC).

Wymóg	Dyrektywa NIS2	Ustawa o KSC
Szacowanie ryzyka i środki proporcjonalne do ryzyka (SZBI)	art. 21 ust. 1–2	art. 8 ust. 1
Rola kierownictwa i szkolenia	art. 20	art. 8c–8e
Ciągłość działania i kopie zapasowe	art. 21 ust. 2 lit. c	art. 8 ust. 1 pkt 2 lit. f
Łańcuch dostaw	art. 21 ust. 2 lit. d i ust. 3	art. 8 ust. 1 pkt 2 lit. e i ust. 2
Zgłaszanie incydentów	art. 23	art. 11–12c

- **Polska ustawa jest bardziej szczegółowa:** dokumentacja normatywna i operacyjna, w tym logi (art. 10), oraz audyt podmiotu kluczowego co najmniej raz na 3 lata (art. 15). Podmiot ważny publiczny stosuje uproszczony SZBI z zał. nr 4 (art. 8 ust. 3).
- **Dostawcy usług cyfrowych** – m.in. DNS, chmury, centrów danych, usług zarządzanych i MSSP – stosują szczegółowe wymagania rozporządzenia wykonawczego 2024/2690 (art. 8b KSC).
- **Termin:** SZBI ma działać najpóźniej 3.04.2027 (art. 33 ust. 1 nowelizacji). Certyfikat ISO/IEC 27001 ułatwia zbudowanie SZBI, ale nie daje domniemania zgodności z ustawą o KSC.

Analogia: SZBI działa jak bezpieczeństwo w lotnictwie – procedury, przeglądy, szkolenia załóg i analiza każdego zdarzenia, a nie jednorazowy zakup zamka do kokpitu.

Źródła: dyrektywa NIS2 (2022/2555); ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); ustawa z 23.01.2026 o zmianie ustawy o KSC (Dz.U. 2026 poz. 252); rozporządzenie wykonawcze Komisji (UE) 2024/2690

Cyberbezpieczeństwo jako zarządzanie organizacją

Ustawa traktuje cyberbezpieczeństwo jak decyzję zarządczą: środki mają uwzględniać najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo incydentów, narażenie na ryzyka oraz skutki społeczne i gospodarcze (art. 8 ust. 1 pkt 2 KSC). Takiego bilansu nie robi sam dział IT.

Kto	Rola w SZBI	Podstawa
Kierownik (zarząd)	decyzje o SZBI, środki finansowe, przydział zadań i nadzór	art. 8c, 8d KSC
Właściciele procesów	które procesy są krytyczne i jak długo mogą stać	art. 8 ust. 1 pkt 1 i pkt 2 lit. f
Kadry	bezpieczeństwo zasobów ludzkich, informacja z KRK, nadawanie i odbieranie dostępów	art. 8 ust. 1 pkt 2 lit. d i n, art. 8f
Zakupy i dział prawny	łańcuch dostaw, wymagania w umowach	art. 8 ust. 1 pkt 2 lit. e, art. 8 ust. 2
Administracja budynków	bezpieczeństwo fizyczne i środowiskowe	art. 8 ust. 1 pkt 2 lit. c
IT i bezpieczeństwo	środki techniczne, monitorowanie, obsługa incydentów	art. 8 ust. 1 pkt 2 lit. g, pkt 4
Każdy pracownik	cyberhigiena i zgłaszanie zdarzeń	art. 8 ust. 1 pkt 2 lit. i–j

☐ **Test dla zarządu:** jeżeli o tym, jak długo firma może działać bez kluczowego systemu, decyduje wyłącznie informatyk – SZBI nie jest jeszcze częścią zarządzania organizacją.

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252)

Ciągłość działania i odporność

Art. 8 ust. 1 pkt 2 lit. f KSC — wdrażanie, dokumentowanie, **testowanie** i utrzymywanie trzech rodzajów planów:

Plan ciągłości działania

Jak dalej świadczyć usługę mimo zakłócenia

Plan awaryjny

Jak pracować w trybie zastępczym, np. ręcznie lub na papierze

Plan odtworzenia działalności

Jak odbudować system po zdarzeniu przekraczającym własne zdolności

Dokumentacja systemu zarządzania ciągłością działania należy do dokumentacji normatywnej (art. 10 ust. 3 pkt 3).

Trzy pojęcia do każdego planu

BIA

Analiza wpływu na działalność — które procesy są krytyczne i co oznacza ich przestój

RTO

W jakim czasie proces musi wrócić

RPO

Ile danych można stracić, czyli jak stara może być ostatnia kopia

 **Scenariusz, o którym plany często zapominają:** utrata wszystkich systemów naraz, łącznie z pocztą, telefonami VoIP i dostępem do samego planu. Plan reagowania warto mieć także na papierze i offline (CISA).

Odporność to zdolność do działania w trakcie ataku i szybkiego powrotu — sprawdza się ją ćwiczeniem, a nie deklaracją. Norma: ISO 22301.

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); CISA #StopRansomware Guide; ISO 22301:2019

Kopie zapasowe, które przetrwają ransomware

Przestępcy najpierw szukają kopii

- **CERT Polska (2025 r.):** w atakach ransomware w Polsce priorytetem było zlokalizowanie serwerów kopii zapasowych i wirtualizatorów. Kopie na serwerach NAS atakujący zwykle kasowali, a na wirtualizatorach usuwali migawki.
- **Veeam (2025 r., ankieta 1 300 organizacji):** repozytoria kopii były celem ataku u 89% organizacji, średnio 34% repozytoriów zmieniono lub usunięto.

☐ **Reguła 3-2-1:** trzy kopie, dwa rodzaje nośników, jedna poza siedzibą (ENISA). Wariant 3-2-1-1-0 dodaje kopię niezmienną i zero błędów w teście odtworzenia – to praktyka rynkowa (Veeam).

Kopia, która przetrwa atak	Źródło wytycznej
Kopia offline lub niezmiennalna, odpięta od domeny Active Directory firmy	CISA; Mandiant
Serwer kopii i jego administratorzy w najwyższej warstwie uprawnień (Tier 0)	ASD, CISA, NSA i in.
Zwykłe konta nie mogą zmieniać ani usuwać kopii	ASD Essential Eight
Test odtworzenia co najmniej raz w roku, z zapisem wyniku; przed odtworzeniem sprawdzenie, czy kopia nie jest zainfekowana	CISA CPG 2.0
Synchronizacja z chmurą to nie kopia – zaszyfrowane pliki nadpiszą wersje w chmurze	CISA

Wymogi: kopie odseparowane i testowane – zał. nr 4 do ustawy o KSC dla podmiotów ważnych publicznych; kopie poza siecią systemu i udokumentowane testy odtworzenia – rozporządzenie 2024/2690 (pkt 4.2) dla dostawców usług cyfrowych.

Źródła: CERT Polska, Raport roczny 2025 (8.04.2026); Veeam: 2025 Ransomware Trends Report (23.04.2025); CISA #StopRansomware Guide; Mandiant M-Trends 2026 (23.03.2026); ASD, CISA, NSA i in.: Detecting and Mitigating Active Directory Compromises (IX 2024); ASD Essential Eight Maturity Model (27.11.2023); CISA Cybersecurity Performance Goals 2.0 (11.12.2025); ENISA: Technical Implementation Guidance on cybersecurity risk management measures (26.06.2025); Veeam: 3-2-1 Backup Rule Explained; ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); rozporządzenie wykonawcze Komisji (UE) 2024/2690

Historia: Norsk Hydro

Co się stało

Tuż po północy 19.03.2019 r. Norsk Hydro – norweski koncern aluminiowy zatrudniający 35 tys. osób w 40 krajach – wykrył nietypową aktywność serwerów. Ransomware zaszyfrował komputery i serwery firmy.

Jak do tego doszło

Według Hydro przestępcy dostali się do sieci IT i niezauważeni zdobywali w niej coraz wyższe uprawnienia. Według Microsoft początkiem był zainfekowany e-mail od zaufanego klienta, otwarty przez pracownika w grudniu 2018 r.

Skutki

Hydro odłączyło wszystkie serwery i komputery, uruchomiło procedury ręczne i zastępcze kanały komunikacji. Firma nie zapłaciła okupu: odbudowywała systemy z kopii zapasowych z pomocą zespołu reagowania Microsoft. Codzienne webcasty i konferencje prasowe, informacje na Facebooku, zgłoszenie na policję. W kwietniu 2019 r. w czterech z pięciu obszarów działalności produkcja szła w normalnym tempie, ale z obejściami ręcznymi. Koszt pierwszego pełnego tygodnia: ok. NOK 300–350 mln; I półrocza 2019 r.: NOK 550–650 mln (szacunki Hydro).

Lekcja dla Państwa

- Ciągłość działania to ludzie i procedury ręczne, a nie tylko zapasowe serwery.
- Kopie zapasowe, z których da się odtworzyć systemy, dają realny wybór: nie płacić okupu.
- Jawna komunikacja od pierwszego dnia chroni zaufanie klientów, pracowników i rynku.

Źródła: Hydro: „The cyber attack on Hydro in brief” (12.04.2019); Hydro: komunikaty z 26.03.2019 i 23.07.2019; Hydro: raport Q1 2019; Microsoft (16.12.2019)

Anatomia ataku: LockerGoga w Norsk Hydro

1 Wektor ataku

Załącznik w prawdziwym wątku e-mail od pracownika zaufanego klienta – „part of a legitimate conversation” (CISO Hydro) – otwarty w grudniu 2018 r., trzy miesiące przed szyfrowaniem. Trojan „captured administrative credentials, allowing the hackers to command the entire IT infrastructure”, a ransomware LockerGoga uruchomiono „via a manual push from (Norsk Hydro's) own domain controllers” (Microsoft DART).

2 Dlaczego się udało

Technicznie: poświadczenia administratora domeny dały kontrolę nad całą infrastrukturą – brak izolacji kont uprzywilejowanych (model warstwowy z Modułu II), jedna platforma IT dla 40 krajów, brak segmentacji między IT a fabrykami; przez trzy miesiące nikt nie wykrył rekonesansu.

Organizacyjnie: e-mail od znanej osoby, „had been expected to hear from” – przejęta skrzynka kontrahenta omija czujność; strata udokumentowana na ponad 800 mln NOK, z polisy cyber do końca III kw. 2019 r. rozpoznano tylko 33 mln NOK.

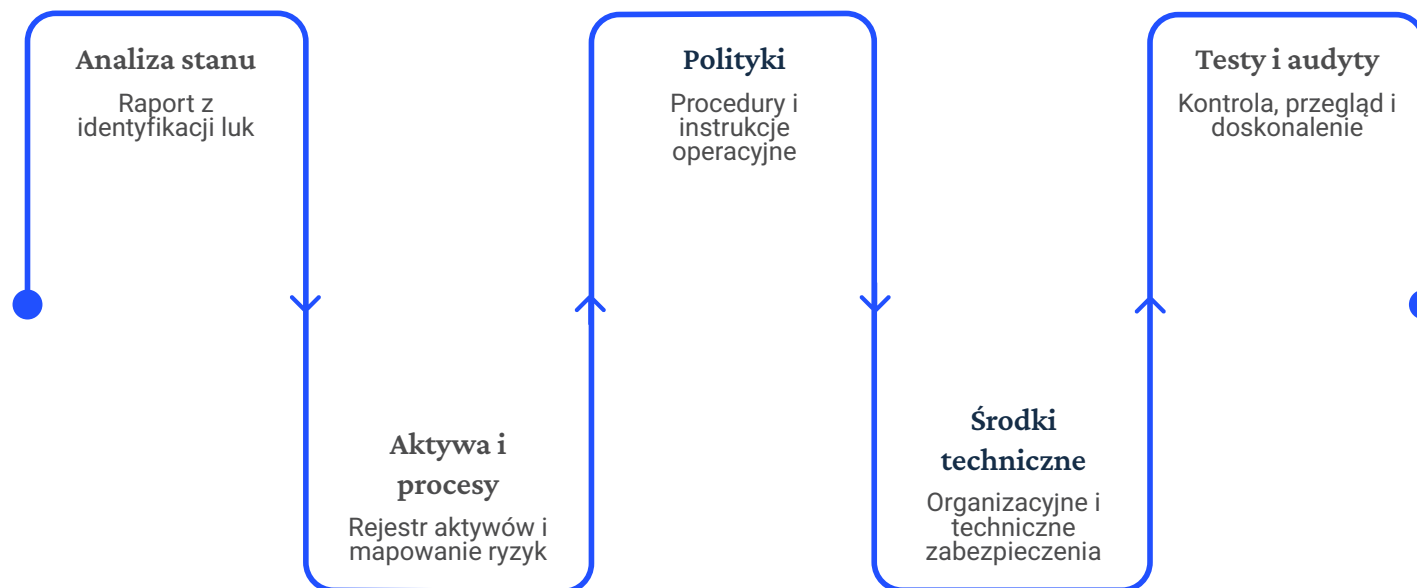
3 Jak temu zaradzić

Zabezpieczenia (CISO w wywiadzie dla norweskiego nadzoru Havtil, 2023): kopie zapasowe „should not be connected to the regular IT platform”; separacja „IT platform and the factories”; przywrócenie części ręcznych układów sterowania maszyn; reorganizacja zespołu bezpieczeństwa „to better detect and respond”. Do tego: konta administratorów wyłącznie ze stacji administracyjnych, EDR wykrywający zrzut poświadczeń, filtr załączników z detonacją w piaskownicy.

Procedury: „a lot of drills, thinking through different scenarios”; szkolenia z rozpoznawania złośliwych e-maili; decyzja o niepłaceniu podjęta z góry – „Even if we'd paid, the attackers would still have had access to our system”; jawna komunikacja od pierwszego dnia; weryfikacja nietypowych załączników od kontrahentów innym kanałem.

Źródła: Microsoft (16.12.2019); Hydro: Cyber-attack on Hydro (aktualizacja 15.05.2024); Havtil: wywiad z CISO Hydro (8.05.2023)

Model przygotowania w 5 krokach



Krok	Pytanie	Główny produkt
Krok 1: analiza stanu obecnego i identyfikacja luk	Gdzie jesteśmy wobec ustawy?	raport z analizy luk i plan wdrożenia
Krok 2: aktywa, procesy i ryzyka	Co chronimy i przed czym?	rejestr aktywów, analiza wpływu, szacowanie ryzyka
Krok 3: polityki, procedury i instrukcje	Jakie zasady obowiązują?	dokumentacja normatywna SZBI
Krok 4: środki techniczne i organizacyjne	Jak ograniczamy ryzyko?	wdrożone zabezpieczenia, szkolenia, osoby do kontaktu
Krok 5: testowanie, audytowanie i doskonalenie	Czy to działa?	wyniki testów, audyt, działania korygujące

Zasada: krok 2 wyznacza priorytety kroków 3 i 4, bo środki mają być proporcjonalne do oszacowanego ryzyka (art. 8 ust. 1 pkt 2 KSC). Krok 5 zamyka cykl i wraca do kroku 2.

Horyzont: obowiązek z rozdziału 3 ustawy o KSC – do 3.04.2027 (art. 33 ust. 1 nowelizacji).

Analogia: remont budynku – inspekcja (1), inwentaryzacja i ocena, co grozi zawaleniem (2), projekt (3), prace (4), odbiór i przeglądy okresowe (5).

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); ustawa z 23.01.2026 o zmianie ustawy o KSC (Dz.U. 2026 poz. 252)

Krok 1: analiza stanu obecnego i identyfikacja luk

Cel

Wiedzieć, gdzie organizacja jest dziś wobec wymagań ustawy o KSC, i zaplanować drogę do 3.04.2027.

Co robimy

- potwierdzamy status podmiotu i usługi objęte ustawą (art. 5 KSC);
- ustalamy zakres SZBI: system informacyjny wykorzystywany w procesach wpływających na świadczenie usługi (art. 8 ust. 1);
- porównujemy stan faktyczny z wymogami art. 8–15: wywiady, przegląd dokumentów, sprawdzenie konfiguracji na próbce systemów.

Produkty kroku

- analiza podlegania ustawie i wniosek o wpis do wykazu do 3.10.2026, jeśli podmiot nie został wpisany z urzędu;
- opisany zakres SZBI: usługi, lokalizacje, systemy i dostawcy;
- raport z analizy luk: wymóg → stan obecny → luka → priorytet;
- plan wdrożenia z harmonogramem, właścicielami zadań i budżetem do decyzji kierownika (art. 8d pkt 2–3).



Uwaga: analiza luk nie zastępuje audytu z art. 15. Audyt podmiotu kluczowego prowadzi m.in. akredytowana jednostka oceniająca zgodność albo co najmniej dwóch uprawnionych audytorów; audytorem nie może być osoba, która realizuje w podmiocie zadania z art. 8 i 9–13 lub realizowała je w roku przed audytem (art. 15 ust. 2–2a).

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); komunikat MC z 8.04.2026 (Dz. Urz. Min. Cyfr. 2026 poz. 7)

Krok 2: identyfikacja aktywów, procesów i ryzyk

Cel

Wiedzieć, co chronimy, co jest krytyczne i które ryzyka są największe.

Co robimy

- inwentaryzujemy aktywa: systemy, dane, urządzenia, sieci, systemy sterowania (OT) i usługi chmurowe (zarządzanie aktywami — art. 8 ust. 1 pkt 2 lit. m KSC);
- mapujemy procesy i ich zależności od systemów i dostawców;
- szacujemy ryzyko według jednej, opisanej metodyki (art. 8 ust. 1 pkt 1).

⊗ **Z praktyki:** w rejestrach najczęściej brakuje systemów sterowania, kont serwisowych dostawców i usług SaaS kupionych przez działy bez udziału IT.

Produkty kroku

- rejestr aktywów z klasyfikacją i osobą odpowiedzialną za każde aktywo;
- analiza wpływu na działalność (BIA) z RTO i RPO dla procesów krytycznych;
- rejestr dostawców ICT z oceną krytyczności (dobra praktyka; rozporządzenie 2024/2690, pkt 5.2);
- metodyka i raport z szacowania ryzyka;
- plan postępowania z ryzykiem z decyzjami kierownika o ryzykach akceptowanych.

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); rozporządzenie wykonawcze Komisji (UE) 2024/2690

Krok 3: polityki, procedury i instrukcje

Cel: spisać zasady tak, żeby były stosowane, a nie tylko przyjęte.

Polityka

Co i dlaczego; przyjmuje kierownik

Procedura

Kto, co i kiedy; odpowiada właściciel procesu

Instrukcja

Jak krok po kroku; dla pracownika lub administratora

Produkty kroku

- polityka szacowania ryzyka, polityka bezpieczeństwa systemu informacyjnego i polityki tematyczne: kontrola dostępu, kryptografia, kopie zapasowe, dostawcy, praca na odległość (art. 8 ust. 1 pkt 2 lit. a, k, n KSC);
- procedura zarządzania incydentami ze ścieżką zgłoszeń: 24 h / 72 h / miesiąc do CSIRT i 72 h do UODO;
- plany ciągłości działania, awaryjne i odtworzenia (lit. f);
- dokumentacja ochrony infrastruktury i dokumentacja techniczna systemu (art. 10 ust. 3);
- zasady nadzoru nad dokumentacją: dostęp, wersje, przechowywanie co najmniej 2 lata od wycofania (art. 10 ust. 6–7).

 **Pułapka:** wzór z internetu z cudzą nazwą firmy. Organ nadzoru może żądać dowodów realizacji wymogów SZBI (art. 53 ust. 2 pkt 6), a dokument, którego nikt nie stosuje, takim dowodem nie jest.

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); RODO (rozporządzenie 2016/679)

Krok 4: środki techniczne i organizacyjne — od czego zacząć

Cel: najpierw wdrożyć zabezpieczenia, które zatrzymują najczęstsze ataki — w kolejności wynikającej z ryzyka, a nie z katalogu producenta.

Od czego zacząć — wspólny rdzeń uznanych zestawów

(CIS IG1: 56 zabezpieczeń · ASD Essential Eight · Cyber Essentials: 5 kontroli · CISA CPG 2.0)

1. inwentaryzacja urządzeń, oprogramowania i usług dostępnych z internetu;
2. łatki według ryzyka — najpierw systemy dostępne z internetu;
3. osobne konta administratorów i minimalne uprawnienia — według CISA niski koszt, wysoki wpływ;
4. MFA na pocztę, dostępie zdalnym i kontach uprzywilejowanych (Moduł III);
5. kopie offline lub niezmiennialne z testem odtworzenia;
6. centralne logi i obsługa alertów przez całą dobę;
7. poczta: SPF, DKIM i DMARC; dla domen, z których nie wysyła się poczty, CERT Polska zaleca rekordy „v=spf1 -all” i „p=reject”.

Produkty kroku

- plan łatania z terminami i rejestr zasobów dostępnych z internetu (art. 8 ust. 1 pkt 3 i pkt 5 lit. b KSC);
- polityka kontroli dostępu z osobnymi kontami administratorów (art. 8 ust. 1 pkt 2 lit. n);
- uwierzytelnianie wieloskładnikowe w stosownych przypadkach (lit. l) i kopie odseparowane od sieci (zał. nr 4 pkt I.10);
- monitorowanie w trybie ciągłym — własne struktury albo dostawca usług zarządzanych w zakresie cyberbezpieczeństwa (lit. g, art. 14);
- osoby do kontaktu i dostęp do systemu S46 do zgłaszania incydentów (art. 9, art. 11 ust. 2).

i Dowody dla audytora: wytyczne ENISA do rozporządzenia 2024/2690 (06.2025) podają przy każdym wymogu przykładowe dowody, np. zapisy testów odtworzenia kopii i uzasadnione decyzje o niezainstalowaniu łatki.

Źródła: CIS Controls v8.1 (25.06.2024); ASD Essential Eight Maturity Model (27.11.2023); NCSC UK: Cyber Essentials; CISA Cybersecurity Performance Goals 2.0 (11.12.2025); CERT Polska: Mechanizmy weryfikacji nadawcy wiadomości (28.10.2021); ENISA: Technical Implementation Guidance on cybersecurity risk management measures (26.06.2025); ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); rozporządzenie wykonawcze Komisji (UE) 2024/2690

Historia: atak na polską energetykę 29.12.2025

Co się stało

29.12.2025 r. przeprowadzono skoordynowane ataki na co najmniej 30 farm wiatrowych i fotowoltaicznych, dużą elektrociepłownię dostarczającą ciepło dla prawie pół miliona odbiorców i firmę produkcyjną. Według CERT Polska wszystkie ataki miały cel wyłącznie destrukcyjny.

Jak do tego doszło

Farmy: na każdym obiekcie interfejs VPN urządzenia FortiGate był dostępny z internetu i pozwalał logować się bez uwierzytelniania wieloskładnikowego; część urządzeń była wcześniej przez dłuższy czas podatna. W branży powszechnie używa się tych samych kont i haseł na wielu obiektach.

Sterowniki i panele: domyślne poświadczenia, np. konto „Default” w sterownikach RTU; weryfikacji podpisu wgrywanego firmware nie włączono na żadnym urządzeniu, które ją obsługiwało.

Elektrociepłownia: pierwsze działania napastnika w marcu–maju 2025 r., w drugiej połowie lipca zrzut całej bazy Active Directory; logowania przez SSL-VPN na konta bez dwuskładnikowego uwierzytelniania.

Skutki

Farmy straciły komunikację z operatorami sieci dystrybucyjnej, a sterowniki dostały uszkodzony firmware — bieżąca produkcja energii trwała. W elektrociepłowni oprogramowanie EDR rozpoznało i zablokowało wiper rozsyłany politykami GPO; dostaw ciepła nie przerwano. Napastnik przywrócił urządzenia brzegowe do ustawień fabrycznych — z żadnego nie udało się odzyskać pełnych logów.

Lekcja dla Państwa

- Urządzenie brzegowe wymaga łątek, unikalnych haseł na każdym obiekcie i logów przechowywanych poza nim.
- Odbiór prac od integratora obejmuje zmianę wszystkich haseł domyślnych i włączenie zabezpieczeń producenta.
- Napastnik był w sieci miesiącami: wykrywa go monitorowanie kont uprzywilejowanych, a nie tylko antywirus.

Źródła: CERT Polska: Raport z incydentu w sektorze energii z 29.12.2025 (30.01.2026)

Anatomia ataku: VPN bez MFA i domyślne hasła w energetyce

1 Wektor ataku

Portal SSL-VPN urządzeń FortiGate dostępny z internetu z kontami „bez wieloskładnikowego uwierzytelniania” (CERT Polska). Na farmach OZE „powszechną praktyką w branży jest wykorzystywanie tych samych kont i haseł w wielu obiektach” — przejęcie jednego konta otwierało kolejne obiekty. W elektrociepłowni ten sam VPN, potem pulpit zdalny na maszyny przesiadkowe, konta administratorów domeny i wiper rozsyłany z kontrolera domeny. W firmie produkcyjnej konfiguracja podatnego urządzenia brzegowego wyciekła wcześniej na forum przestępcze.

2 Dlaczego się udało

Technicznie: urządzenia „przez dłuższy czas były podatne, w tym na zdalne wykonanie kodu”; sterowniki RTU z domyślnym kontem „Default” uprawnionym do zmiany firmware; weryfikacja podpisu firmware (secure update) dostępna, ale niewłączona na żadnym urządzeniu; panele HMI z domyślnym hasłem administratora; VLAN-y istniały, lecz napastnik był administratorem firewalla; po przywróceniu urządzeń do ustawień fabrycznych nie zostały żadne logi.

Organizacyjny: wdrożenia niezgodne z zaleceniami producenta — „gdyby urządzenie zostało wdrożone zgodnie z zaleceniami producenta, to domyślne konto FTP zostałoby automatycznie zablokowane”; skanowanie sieci 25.12 (cztery dni przed atakiem) nie wywołało reakcji; w elektrociepłowni ślady „kilka miesięcy przed uruchomieniem” wipera.

3 Jak temu zaradzić

Zabezpieczenia (zalecenia Pełnomocnika Rządu ds. Cyberbezpieczeństwa dla OZE, 19.01.2026): dostęp zdalny „wyłącznie z wykorzystaniem tunelu VPN site-to-site”; „żadne urządzenia OT (...) nie powinny być osiągalne bezpośrednio z internetu”; interfejsy administracyjne poza internetem; zmiana „wszystkich domyślnych haseł (...)” włącznie z urządzeniami OT”; segmentacja co najmniej VLAN; kopia konfiguracji „w odizolowanym środowisku offline”. Wnioski z raportu: MFA na każdym dostępie zdalnym, unikalne hasła na każdym obiekcie, włączony secure update, logi do zewnętrznego kolektora, EDR — w elektrociepłowni to on zatrzymał wiper.

Procedury: osoba odpowiedzialna za cyberbezpieczeństwo instalacji i kontakt z CSIRT; rejestracja adresacji i domen w moje.cert.pl; inwentarz sprzętu z interfejsami i uprawnieniami; odbiór prac od integratora z listą zabezpieczeń producenta; zgłaszanie nietypowego zachowania urządzeń do CSIRT „niezwłocznie”.

Źródła: CERT Polska: Raport z incydentu w sektorze energii z 29.12.2025 (30.01.2026); Pełnomocnik Rządu ds. Cyberbezpieczeństwa: komunikat dotyczący cyberbezpieczeństwa OZE (19.01.2026)

Podatności, łatki i urządzenia brzegowe

Okno na łatanie prawie się zamknęło

- **Mandiant (M-Trends 2026):** średni czas od ujawnienia podatności do jej wykorzystania szacowany na -7 dni – ataki zwykle zaczynają się, zanim wyjdzie łatka.
- **VulnCheck (I półrocze 2026):** 23,43% wykorzystywanych podatności z katalogu VulnCheck miało ślady ataku w dniu publikacji albo wcześniej.
- **Verizon:** w pełni załatano tylko 26% krytycznych podatności z katalogu CISA KEV; mediana – 43 dni.

Urządzenia brzegowe (VPN, firewall)

Wytyczne ASD, CISA, NCSC i partnerów (4.02.2025, 5.02.2026): inwentarz z datami końca wsparcia i wymiana urządzeń bez wsparcia · interfejsy administracyjne niedostępne z internetu · zmiana haseł domyślnych · logi przesyłane do centralnego systemu.

Wymogi: aktualizacje zgodnie z zaleceniami producenta (art. 8 ust. 1 pkt 5 lit. b KSC); dostawcy usług cyfrowych – łatki w rozsądnym czasie, a rezygnację z łatki trzeba udokumentować i uzasadnić (rozporządzenie 2024/2690, pkt 6.6).

Źródła: Mandiant M-Trends 2026 (23.03.2026); VulnCheck: State of Exploitation 1H 2026 (28.07.2026); Verizon DBIR 2026 (19.05.2026); CISA BOD 26-04 (10.06.2026); ASD i partnerzy: Mitigation Strategies for Edge Devices (4.02.2025); CISA, FBI i NCSC UK: Reducing the Attack Surface for End-of-Support Edge Devices (5.02.2026); ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); rozporządzenie wykonawcze Komisji (UE) 2024/2690

Priorytet według ryzyka — dyrektywa CISA BOD 26-04 z 10.06.2026

Sytuacja	Termin
System dostępny z internetu, podatność z katalogu KEV dająca pełną kontrolę	3 dni i sprawdzenie, czy system nie został już przejęty
System dostępny z internetu, pozostałe podatności z KEV	3 albo 14 dni – zależnie od tego, czy exploit da się zautomatyzować
System wewnętrzny, podatność z KEV	3 dni i sprawdzenie przy exploicie zautomatyzowanym dającym pełną kontrolę, w pozostałych przypadkach 14 dni
Podatności spoza KEV	od 3 do 60 dni albo przy najbliższej modernizacji systemu

Odłączenie systemu od internetu to dopuszczalna mitygacja.

Konta administratorów i Active Directory

Dlaczego Active Directory: wytyczne sześciu agencji (ASD, CISA, NSA, CCCS, NCSC-NZ, NCSC-UK) opisują 17 technik ataku na AD i zauważają, że każdy użytkownik domeny ma uprawnienia wystarczające do znalezienia jej słabości. Zabezpieczenie dostępu uprzywilejowanego ma być najwyższym priorytetem. W elektrociepłowni z Historii napastnik zgrał całą bazę AD kilka miesięcy przed atakiem.

Model warstwowy (Microsoft Enterprise Access Model)

Warstwa	Co obejmuje	Zasada
Tier 0	kontrolery domeny, urząd certyfikacji AD CS, Entra Connect, serwery kopii zapasowych i ich administratorzy	administracja tylko z dedykowanych stacji (PAW), MFA odporne na phishing
Tier 1	serwery i aplikacje	osobne konta administratorów serwerów
Tier 2	stacje robocze	unikalne hasło lokalnego administratora na każdym komputerze

Od czego zacząć

- osobne konta administratorów, bez poczty i przeglądania internetu — według CISA niski koszt, wysoki wpływ;
- **Windows LAPS** — bezpłatny, wbudowany w Windows: unikalne, automatycznie zmieniane hasło lokalnego administratora;
- konta usług jako gMSA (hasło 120 znaków, zmieniane automatycznie) albo z hasłem co najmniej 30 znaków;
- w Microsoft 365 bez stałych przypisać ról o najwyższych uprawnieniach (CISA SCuBA);
- przegląd uprawnień i szybkie odbieranieostępów — NIK w 2026 r. wskazała w urzędach nieodebrane uprawnienia byłych pracowników;
- samoocena AD bezpłatnymi narzędziami, np. PingCastle, BloodHound, Purple Knight.

Wymogi: polityka kontroli dostępu (art. 8 ust. 1 pkt 2 lit. n KSC); dostawcy usług cyfrowych — osobne konta wyłącznie do administracji (rozporządzenie 2024/2690, pkt 11.3).

Źródła: ASD, CISA, NSA i in.: Detecting and Mitigating Active Directory Compromises (IX 2024); Microsoft Learn: Enterprise access model; CISA Cybersecurity Performance Goals 2.0 (11.12.2025); Microsoft Learn: Windows LAPS overview; CISA SCuBA: Microsoft Entra ID baseline; NIK, komunikat z 21.07.2026: Cyberbezpieczny Samorząd; ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); rozporządzenie wykonawcze Komisji (UE) 2024/2690

Logi i monitorowanie: co zbierać i jak długo

Bez logów nie ma śledztwa

- **CERT Polska (2025 r.):** przy atakach ransomware najczęściej brakuje logów z urządzeń brzegowych i kontrolera domeny; bez centralnego kolektora logi sięgają zaledwie kilku dni wstecz.
- **Mandiant:** w 34% włamań z 2024 r. nie ustalono wektora wejścia (M-Trends 2025); przy włamaniach trwających ok. 400 dni standardowa retencja 90 dni nie pozwala ustalić wektora wejścia (M-Trends 2026).

Zasady

- logi w centralnym systemie, poza monitorowanym urządzeniem, chronione przed zmianą;
- zsynchronizowany czas we wszystkich systemach;
- alarm, gdy ktoś wyłączy logowanie (CISA CPG 2.0);
- ktoś odbiera alerty także w nocy i w weekend – własny zespół albo dostawca usług zarządzanych (art. 14 KSC).

Jak długo? Rozporządzenie 2024/2690 (pkt 3.2) wymienia m.in. zdarzenia uwierzytelniania, działania kont administracyjnych, zmiany uprawnień i konfiguracji oraz włączanie i wyłączanie logowania – i każe przechowywać logi przez z góry określony okres, bez podania liczby dni. Okres ustala się według ryzyka; domyślne okresy retencji zwykle nie wystarczają (ASD i CISA).

Wymogi: monitorowanie systemu w trybie ciągłym (art. 8 ust. 1 pkt 2 lit. g KSC); logi to część dokumentacji operacyjnej (art. 10 KSC).

Co logować najpierw

(wytyczne ASD, CISA, FBI, NSA i partnerów, 08.2024)

- Systemy krytyczne
- Usługi internetowe z dostępem zdalnym
- Serwery tożsamości i domeny
- Urządzenia brzegowe
- Stacje administratorów
- Oprogramowanie bezpieczeństwa
- Proxy, DNS i poczta
- W chmurze: działania administratorów i zmiany uprawnień

Źródła: CERT Polska, Raport roczny 2025 (8.04.2026); Mandiant M-Trends 2025; Mandiant M-Trends 2026 (23.03.2026); ASD, CISA, FBI, NSA i in.: Best practices for event logging and threat detection (VIII 2024); CISA Cybersecurity Performance Goals 2.0 (11.12.2025); rozporządzenie wykonawcze Komisji (UE) 2024/2690; ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252)

Krok 5: testowanie, audytowanie i doskonalenie

Cel: wykazać sobie, zarządowi i organowi nadzoru, że SZBI działa – i stale go poprawiać.

Produkty kroku

- harmonogram i raporty testów: odtworzenie kopii, ćwiczenie sztabowe, test penetracyjny, symulacja phishingu (art. 8 ust. 1 pkt 2 lit. b i f KSC);
- wskaźniki KPI i KRI z procedurą oceny skuteczności środków (lit. h);
- audyt wewnętrzny (dobra praktyka; ISO/IEC 27001:2022, rozdz. 9.2), a w podmiocie kluczowym audyt z art. 15 co najmniej raz na 3 lata – pierwszy do 3.04.2028;
- przegląd SZBI przez kierownika z decyzjami i budżetem (art. 8d pkt 1–2);
- rejestr działań korygujących z właścicielami i terminami (dobra praktyka; ISO/IEC 27001:2022, rozdz. 10.2).

Rytm przeglądów

Rozporządzenie 2024/2690 wymaga przeglądu polityki bezpieczeństwa oraz wyników oceny ryzyka co najmniej raz w roku i po poważnych incydentach (pkt 1.1.2 i 2.1.4) – dobry wzorzec także dla podmiotów spoza jego zakresu.



Szczegóły w temacie 4 tego Modułu: KPI i KRI, audyty, testy, ćwiczenia i doskonalenie.

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); ustawa z 23.01.2026 o zmianie ustawy o KSC (Dz.U. 2026 poz. 252); rozporządzenie wykonawcze Komisji (UE) 2024/2690; ISO/IEC 27001:2022

Ciekawostka 3: pociągi Newag Impuls

2021–2023: po przetargu Kolei Dolnośląskich pociągi Newag Impuls serwisowała firma SPS. W 2022 r. SPS zwróciła się do ekspertów Dragon Sector o analizę oprogramowania pociągów.

Ustalenia Dragon Sector

- Dragon Sector zbadał 30 pociągów i w 24 znalazł mechanizmy blokujące pociąg po spełnieniu określonych warunków.
- Najczęstszy warunek: długi postój — początkowo 10 dni bez jazdy z prędkością 60 km/h przez 3 minuty, później 20–21 dni.
- W 2 pociągach blokada zależała też od położenia GPS w strefach obejmujących warsztaty.
- W oprogramowaniu była kombinacja odblokowania z panelu w kabinie.

Status sprawy

CSIRT NASK ocenił raporty Dragon Sector jako wiarygodne. Newag zaprzecza ich ustaleniom i pozwał badaczy. Prokuratura Regionalna w Krakowie prowadziła śledztwo w sprawie, bez przedstawienia zarzutów (stan z komunikatu z 17.06.2024).

-  **Lekcja dla Państwa:** kupując maszynę, kupują Państwo także oprogramowanie dostawcy, którego nie widać. Rejestr aktywów (krok 2) obejmuje systemy sterowania i ich oprogramowanie, a ocena dostawcy — to, kto i na jakich zasadach może je serwisować. Ustawa o KSC pozwala CSIRT MON, NASK i GOV badać produkt ICT niezależnie od postanowień umów licencyjnych (art. 33 ust. 1d–1f).

Źródła: Dragon Sector, wystąpienie „Train DRM” na 37C3 (XII 2023); CyberDefence24 (2.01.2025); OKO.press (31.08.2024); Prokuratura Regionalna w Krakowie (17.06.2024); ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252)

Wymagania wobec dostawców

Ustawa o KSC

- SZBI obejmuje „bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi” (art. 8 ust. 1 pkt 2 lit. e).
- Podmiot uwzględnia podatności związane z dostawcą, ogólną jakość jego produktów i usług ICT, wyniki skoordynowanej unijnej oceny ryzyka i wyniki postępowania w sprawie dostawcy wysokiego ryzyka (art. 8 ust. 2).
- Powierzenie obowiązków innej osobie nie zwalnia kierownika (art. 8c ust. 3). Umowę z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa podaje się we wniosku o wpis do wykazu (art. 7 ust. 2 pkt 16).
- Postanowienia umów blokujące badanie produktu ICT przez CSIRT MON, CSIRT NASK lub CSIRT GOV są nieważne (art. 33 ust. 1d–1f).
- Przepisy o dostawcy wysokiego ryzyka (art. 67b–67c) są objęte wnioskiem Prezydenta w sprawie K 19/26 – stan na 17.09.2026: bez rozstrzygnięcia.

Dyrektywa NIS2

- bezpieczeństwo łańcucha dostaw, w tym relacje z bezpośrednimi dostawcami i usługodawcami (art. 21 ust. 2 lit. d);
- podatności każdego bezpośredniego dostawcy, jakość produktów i praktyk cyberbezpieczeństwa, w tym procedur bezpiecznego opracowywania (art. 21 ust. 3);
- zachęta do wpisywania środków bezpieczeństwa do umów z dostawcami (motyw 85).

RODO

Dostawca przetwarzający dane osobowe – umowa powierzenia i wystarczające gwarancje (art. 28 RODO).

i Czego ustawa nie mówi: nie podaje listy klauzul umownych ani częstotliwości audytów dostawców – ustala je SZBI według ryzyka.

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); dyrektywa NIS2 (2022/2555); RODO (rozporządzenie 2016/679); Trybunał Konstytucyjny, sprawa K 19/26 (stan 17.09.2026)

Ryzyko dostawców IT i chmury

Dostawcy to częsta droga ataku: udział stron trzecich w naruszeniach sięga 48%, o 60% więcej niż rok wcześniej; tylko 23% dostawców w pełni usunęło braki lub błędy konfiguracji MFA na kontach chmurowych (Verizon).

Kryterium	Pytanie
Wpływ na usługę	Czy bez dostawcy zatrzymuje się proces krytyczny – i na jak długo?
Dostęp	Czy ma zdalny lub uprzywilejowany dostęp do systemów albo dostęp do danych?
Zastępowalność	Jak szybko zmienimy dostawcę i czy odzyskamy dane?
Koncentracja	Ile procesów zależy od jednego dostawcy lub jednej chmury?
Jakość i podatności	Jak dostawca usuwa podatności i informuje o incydentach? (art. 8 ust. 2 pkt 1–2 KSC)

Wynik oceny: dostawcy krytyczni, istotni i pozostali – od kategorii zależy zakres umowy, monitorowania i audytu.

Źródła: Verizon DBIR 2026 (19.05.2026); ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); Mandiant: UNC5537 Targets Snowflake Customer Instances (10.06.2024)

Chmura — odpowiedzialność współdzielona

Dostawca odpowiada za infrastrukturę, a klient zwykle za konfigurację, konta, MFA, uprawnienia i kopie danych. Certyfikat ISO/IEC 27001 dostawcy to dowód do oceny, a nie jej zastępstwo – trzeba sprawdzić zakres certyfikatu.

Snowflake (2024)

Platforma nie została przełamana, zawiodła konfiguracja klientów. Mandiant i Snowflake powiadomiły ok. 165 organizacji. Przestępcy logowali się hasłami skradzionymi przez złośliwe oprogramowanie typu infostealer: przejęte konta nie miały MFA ani list dozwolonych adresów, część haseł nie była zmieniana nawet 4 lata, a infekcje zaczynały się m.in. na laptopach podwykonawców używanych też prywatnie.

Historia: McDonald's Polska i Collins Aerospace

Co się stało

21.07.2025 r. Prezes UODO ogłosił kary łącznie 16 932 657 zł dla McDonald's Polska i 183 858 zł dla jej dostawcy – agencji PR 24/7 Communication, podmiotu przetwarzającego dane pracowników w module grafików pracowniczych.

Jak do tego doszło

- Przez nieprawidłową konfigurację serwera dostawcy dostępna była kopia bazy grafików z imionami i nazwiskami, numerami PESEL lub paszportów i godzinami pracy.
- Spółka nie zweryfikowała dostawcy pod kątem zdolności do zabezpieczenia danych – oparła się na wcześniejszej współpracy PR.
- Zapisy umowy powierzenia o audytach i inspekcjach nie były realizowane, a analizy ryzyka nie przeprowadził ani administrator, ani dostawca.

Skutki

UODO wskazał naruszenie art. 28 ust. 1 RODO (weryfikacja podmiotu przetwarzającego) i obowiązków z art. 24, 25 i 32 RODO. Powierzenie przetwarzania danych dostawcy nie zwalnia administratora z obowiązku zapewnienia ich bezpieczeństwa.

Lekcja dla Państwa

- Odpowiedzialność za dostawcę zostaje u Państwa: w RODO (art. 28) i w KSC (art. 8 ust. 1 pkt 2 lit. e, art. 8c ust. 3).
- Prawo audytu w umowie chroni tylko wtedy, gdy się z niego korzysta.
- **Collins Aerospace, wrzesień 2025 r.:** ransomware w systemie odprawy MUSE, wspólnym dla wielu linii, zmusił Heathrow, Brukselę, Berlin i Dublin do odprawy ręcznej; Bruksela poprosiła linie o odwołanie połowy z 276 odlotów 22.09.2025. Dostawca wspólny dla wielu organizacji to pojedynczy punkt awarii – plan ciągłości przewiduje pracę bez jego systemu.

Źródła: UODO, komunikat z 21.07.2025; RTX, formularz 8-K (SEC, 24.09.2025); NBC News (21.09.2025)

Anatomia ataku: dostawca jako słabe ogniwo

1 Wektor ataku

McDonald's Polska: nie było włamania. Plik z bazą grafików pracowniczych leżał od 14–15.01.2019 do 22.07.2020 – ok. 18 miesięcy – w publicznym katalogu serwera dostawcy z włączonym podglądem zawartości: „dowolna osoba po przejściu na stronę główną aplikacji (...) widziała katalogi oraz pliki dostępne na serwerze” (decyzja UODO). O wycieku administratora poinformowała osoba trzecia e-mailem na adres ogólny.

Collins Aerospace: RTX i ENISA nie podały, jak doszło do infekcji ransomware systemu MUSE; RTX: system działa „outside of the RTX enterprise network, residing on customer-specific networks”.

2 Dlaczego się udało

Technicznie: błąd konfiguracji serwera (katalog public_html z listingiem) wykrywalny każdym skanerem; PESEL i numer paszportu użyte jako identyfikator pracownika – dane nadmiarowe (art. 5 ust. 1 lit. c RODO); podmiot przetwarzający nie prowadził „regularnego testowania, mierzenia oraz oceniania skuteczności” zabezpieczeń.

Organizacyjnie: administrator „nie przeprowadził analizy ryzyka”, „nie weryfikował bezpośrednio” zabezpieczeń dostawcy i „nie korzystała ze swoich uprawnień w zakresie prawa do przeprowadzania audytów”; podwykonawca dostawcy pracował bez umowy podpowierzenia – zawarto ją po naruszeniu; IOD nie został włączony. Lotniska: jeden dostawca dla wielu hubów, więc jeden incydent zatrzymał odprawę w kilku krajach naraz.

3 Jak temu zaradzić

Zabezpieczenia: skanowanie powierzchni zewnętrznej własnej i dostawców (bezpłatnie: moje.cert.pl), dane pracownicze bez PESEL tam, gdzie wystarczy numer, szyfrowanie i uwierzytelnianie dostępu do każdego pliku z danymi, monitorowanie konfiguracji serwerów.

Procedury: analiza ryzyka przed powierzeniem, weryfikacja dostawcy pod kątem zdolności zabezpieczenia danych (art. 28 RODO), audyt zapisany w umowie i faktycznie wykonany, zgoda na podwykonawców, udział IOD; dla dostawców krytycznych – plan ciągłości bez ich systemu: Bruksela, Heathrow i Berlin ratowały odprawę ręcznie i online z dodatkowym personelem, Bruksela prosiła linie o odwołanie połowy odlotów.

Źródła: UODO, komunikat z 21.07.2025; decyzja Prezesa UODO DKN.5130.4179.2020 (23.06.2025); RODO (rozporządzenie 2016/679); RTX, formularz 8-K (SEC, 24.09.2025); AP (21.09.2025)

Umowy, monitorowanie i audyt dostawców

Co wpisać do umowy z dostawcą krytycznym

Wzorzec: rozporządzenie 2024/2690, pkt 5.1.4 (wiąże podmioty z art. 8b KSC, dla pozostałych to dobra praktyka):

- wymogi cyberbezpieczeństwa dla produktu lub usługi;
- kompetencje, szkolenia i sprawdzenie przeszłości pracowników dostawcy;
- zgłaszanie incydentów bez zbędnej zwłoki – w terminie, który pozwoli zdążyć z wczesnym ostrzeżeniem w 24 h;
- prawo do audytu albo do otrzymywania sprawozdań z audytu;
- postępowanie z podatnościami i zasady podwykonawstwa;
- obowiązki dostawcy przy rozwiązaniu umowy: zwrot i usunięcie danych, pomoc w przejściu.

Przy danych osobowych dodatkowo umowa powierzenia (art. 28 RODO).

Monitorowanie

- ocena przy wyborze i okresowo – częściej dla dostawców krytycznych;
- przegląd sprawozdań z poziomu usług, incydentów i zmian u dostawcy (ISO/IEC 27001:2022, zał. A 5.22);
- przegląd kont i dostępuów zdalnych dostawcy: konta imienne, dostęp na czas prac, uwierzytelnianie wieloskładnikowe.

Audyt dostawcy krytycznego

- kwestionariusz i dowody: certyfikat z zakresem, podsumowanie testu penetracyjnego, plan ciągłości;
- audyt zdalny lub na miejscu, gdy dowody nie wystarczają;
- starsze umowy: przegląd i aneksy.

Podstawa dobrych praktyk: ISO/IEC 27001:2022, zał. A 5.19–5.23.

Źródła: rozporządzenie wykonawcze Komisji (UE) 2024/2690; ISO/IEC 27001:2022; RODO (rozporządzenie 2016/679)

Ćwiczenie 3: który dostawca jest krytyczny?

Spółka Metalpol — przykład szkoleniowy. Producent komponentów, 180 pracowników, podmiot ważny. Prosimy uszeregować dostawców od najbardziej do najmniej krytycznego i wpisać na czacie cztery litery, np. „C A B D”.

A. Chmurowy system kadrowo-płacowy (SaaS)

Dane wszystkich pracowników, w tym PESEL i numery rachunków; przy awarii wypłaty można przez kilka dni przygotować ręcznie. Umowa: 40 tys. zł rocznie.

B. Serwis sterowników linii produkcyjnej

Stały zdalny dostęp VPN do sieci produkcyjnej przez wspólne konto bez uwierzytelniania wieloskładnikowego; linia daje 70% przychodu. Umowa: 30 tys. zł rocznie.

C. Dostawca tonerów i materiałów biurowych

Zamówienia przez sklep internetowy, bez dostępu do systemów spółki. Umowa: 90 tys. zł rocznie.

D. Agencja prowadząca stronę-wizytówkę

Hosting u agencji, bez sklepu, formularzy i danych klientów. Umowa: 25 tys. zł rocznie.

☐ **Klucz odpowiedzi (po głosowaniu): B A D C**

B — krytyczny

Uprzywilejowany dostęp do sieci produkcyjnej bez MFA i wpływ na główną działalność. Do umowy: konta imienne, dostęp na żądanie z MFA, zgłaszanie incydentów, prawo audytu.

A — istotny

Dane osobowe wszystkich pracowników (umowa powierzenia, art. 28 RODO); proces może krótko działać ręcznie.

D — niski

Ryzyko wizerunkowe (podmiana strony), bez danych i bez wpływu na produkcję.

C — najniższy

Brak dostępu do systemów i danych. Najwyższa wartość umowy nie oznacza najwyższego ryzyka.

Wniosek: o krytyczności decydują wpływ na usługę, dostęp i zastępowalność — nie wartość umowy.

Źródła: przykład szkoleniowy — spółka i dostawcy fikcyjni; ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252)

KPI i KRI

KPI (kluczowy wskaźnik efektywności) pokazuje, czy zabezpieczenia działają. **KRI** (kluczowy wskaźnik ryzyka) ostrzega, że ryzyko rośnie. Podstawa: polityki i procedury oceny skuteczności środków (art. 8 ust. 1 pkt 2 lit. h KSC; art. 21 ust. 2 lit. f NIS2) i nadzór kierownika (art. 8d pkt 3 KSC).

Obszar	KPI – przykład	KRI – przykład
Tożsamość	% kont uprzywilejowanych i dostępów zdalnych z MFA	konta uprzywilejowane bez MFA; aktywne konta byłych pracowników
Podatności	% krytycznych podatności usuniętych w ustalonym terminie	krytyczne podatności otwarte po terminie; systemy bez wsparcia producenta
Kopie zapasowe	% udanych testów odtworzenia	dni od ostatniego udanego odtworzenia systemu krytycznego
Incydenty	czas wykrycia i czas reakcji; zgłoszenia 24 h / 72 h w terminie	liczba incydentów poważnych; incydenty powtarzające się
Ludzie	% personelu po szkoleniu; % zgłoszeń w symulacji phishingu	% kliknięć w symulacji phishingu
Dostawcy	% dostawców krytycznych ocenionych w ostatnich 12 miesiącach	dostawcy krytyczni z dostępem bez MFA lub bez wymagań w umowie

241

dni

Średnio od naruszenia do jego wykrycia i opanowania — najkrócej od 9 lat (IBM, 2025)

- ☐ **Zasada dla zarządu:** kilka wskaźników z progami (zielony / żółty / czerwony), właścicielem i trendem zamiast kilkadziesiątu wykresów. Polityka oceny skuteczności określa, co się mierzy, jak, kiedy i kto analizuje wyniki (rozporządzenie 2024/2690, pkt 7.2).

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); dyrektywa NIS2 (2022/2555); IBM Cost of a Data Breach 2025 (30.07.2025); rozporządzenie wykonawcze Komisji (UE) 2024/2690

Audyty wewnętrzne i testy penetracyjne

	Audyt	Test penetracyjny
Pytanie	Czy działamy zgodnie z wymaganiami i własnymi zasadami?	Czy atakujący przełamie zabezpieczenia?
Metoda	wywiady, dokumenty, próbki dowodów	kontrolowany atak w uzgodnionym zakresie, na podstawie pisemnej zgody
Wynik	niezgodności i zalecenia	podatności z oceną ryzyka i dowodami
Podstawa	art. 15 KSC; ISO/IEC 27001:2022 rozdz. 9.2	art. 8 ust. 1 pkt 2 lit. b i h KSC; ISO/IEC 27001:2022 zał. A 8.8 i 8.29

Audyt wewnętrzny i audyt z art. 15 KSC

Audyt wewnętrzny sprawdza SZBI między audytami zewnętrznymi; audytor nie ocenia własnej pracy. Obecne KRI wymaga od podmiotów realizujących zadania publiczne audytu wewnętrznego bezpieczeństwa informacji co najmniej raz w roku (§ 19 ust. 2 pkt 14; rozporządzenie traci moc 23.02.2027).

- podmiot kluczowy: co najmniej raz na 3 lata, pierwszy do 3.04.2028; kopia raportu do organu w 3 dni robocze (ust. 1–1a);
- akredytowana jednostka oceniająca zgodność albo co najmniej dwóch uprawnionych audytorów; audytorem nie może być osoba realizująca w podmiocie zadania z art. 8 i 9–13 (ust. 2–2a);
- podmiot ważny: na nakaz organu, np. po incydencie poważnym (ust. 1b).

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); ISO/IEC 27001:2022; rozporządzenie wykonawcze Komisji (UE) 2024/2690; rozporządzenie RM w sprawie KRI (Dz.U. 2024 poz. 773); CERT Polska, Raport roczny 2025 (8.04.2026)

Testy penetracyjne

- ustawa nie określa ich częstotliwości; rozporządzenie 2024/2690 każe ustalać zakres i częstotliwość testów według oceny ryzyka i dokumentować wyniki (pkt 6.5.2);
- **skan podatności to nie test penetracyjny**: skaner automatycznie szuka znanych luk i błędów konfiguracji — bezpłatnie np. w moje.cert.pl (system Artemis CERT Polska); pentester ręcznie próbuje przełamać zabezpieczenia i łączy słabości w scenariusz ataku;
- raport bez planu usunięcia podatności to koszt, a nie bezpieczeństwo.

Ćwiczenia, symulacje i ciągłe doskonalenie

Plan, którego nikt nie przeciwiczył, zawodzi w pierwszej godzinie. Ustawa o KSC wymaga testowania planów ciągłości, awaryjnych i odtworzenia (art. 8 ust. 1 pkt 2 lit. f), a podmiot ważny publiczny — przygotowania i testowania procedury na wypadek awarii lub incydentu (zał. nr 4 pkt I.12).

HSE — irlandzka publiczna służba zdrowia (ransomware Conti, 2021)

Ransomware uruchomiono po 8 tygodniach obecności przestępców w sieci; antywirus wykrył ich narzędzia, ale działał tylko w trybie monitorowania. PwC: brak udokumentowanego planu reagowania na incydent cyber i ćwiczeń.

British Library (ransomware Rhysida, 2023)

Wejście przez serwer terminalowy bez MFA, wyłączony z wdrożenia MFA m.in. ze względu na koszt; ok. 600 GB plików trafiło do dark webu. Wniosek raportu: ćwiczyć plany na utratę wszystkich systemów, a ryzyka akceptowane operacyjnie zgłaszać kierownictwu.

Gotowe scenariusze bez kosztów

NCSC Exercise in a Box (20 ćwiczeń, m.in. ransomware i łańcuch dostaw) · pakiety CISA Tabletop Exercise (ponad 100 scenariuszy, także dla wodociągów, samorządów i ochrony zdrowia). W Polsce ćwiczenie KSC-EXE 2025 (26.11.2025) sprawdzało procedury podmiotów krajowego systemu cyberbezpieczeństwa. **Rytm:** plan reagowania ćwiczony co najmniej raz w roku (CISA CPG 2.0).

Ciągłe doskonalenie (ISO/IEC 27001:2022, rozdz. 10)

Każdy incydent, „prawie incydent”, audyt, test i ćwiczenie kończy się działaniem korygującym z właścicielem i terminem. Źródła usprawnień to także ostrzeżenia CERT Polska o podatnościach (art. 8 ust. 1 pkt 3 KSC) i zmiany: nowe systemy, dostawcy i przepisy. Przegląd przez kierownika kończy się decyzjami: co poprawiamy, za ile, kto i do kiedy (art. 8d pkt 1–3 KSC).

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); PwC: Conti cyber attack on the HSE (3.12.2021); British Library: Learning Lessons from the Cyber-Attack (8.03.2024); NCSC UK: Exercise in a Box; CISA Tabletop Exercise Packages; Ministerstwo Cyfryzacji: KSC-EXE 2025 (27.11.2025); CISA Cybersecurity Performance Goals 2.0 (11.12.2025); ISO/IEC 27001:2022

Ciekawostka 4: „Radio-Stop” pod Szczecinem

Piątek 25.08.2023, godz. 21:23: ktoś nadał przez radiotelefon sygnał „Radio-Stop” na liniach kolejowych prowadzących do Szczecina Głównego. Do 23:30 ponad 20 pociągów miało opóźnienia, a ruch towarowy przywrócono przed 2:00. Czynności prowadziła ABW.

Dlaczego to było możliwe

Analogowy sygnał nie jest szyfrowany i nie wymaga uwierzytelnienia – nadać go może każdy, kto ma radiotelefon.

Skala zjawiska

Dwa dni później, na Podlasiu, sygnał zatrzymał 18 pociągów. W lipcu 2026 r. sąd drugiej instancji skazał jednego ze sprawców na rok więzienia, a drugiego na 16 tys. zł grzywny. Ok. 720 nieuprawnionych nadań sygnału „Alarm” w 2023 r. i ok. 900 w 2024 r. W styczniu 2025 r. cyfrowa łączność GSM-R działała na ok. 1,6 tys. z planowanych 13,8 tys. km linii.

 **Lekcja dla Państwa:** polecenie bez uwierzytelnienia wykona każdy, kto zna protokół. Stare systemy sterowania i łączności trzeba ująć w rejestrze aktywów i w testach bezpieczeństwa, a tam, gdzie nie da się ich szybko wymienić – stosować środki zastępcze i monitorowanie.

Źródła: RMF24 (26.08.2023); TVN24 (26.08.2023 i 10.07.2026); Notes from Poland za Niebezpiecznik (29.08.2023); Kolejowy Portal (20.01.2025)

Podsumowanie Modułu II i przerwa obiadowa

Najważniejsze z Modułu II

SZBI

To zarządzanie ryzykiem całej organizacji, a nie projekt działu IT (art. 8 i 8d KSC).

Ciągłość działania

Przećwiczone plany i kopia, której przestępca nie skasuje – offline lub niezmiennalna, z testem odtworzenia.

Minimum techniczne

Łatki według ryzyka (najpierw systemy dostępne z internetu), osobne konta administratorów, logi poza urządzeniem i alerty obsługiwane przez całą dobę.

Dostawcy

Odpowiedzialność za łańcuch dostaw zostaje u Państwa; o krytyczności decyduje wpływ i dostęp, nie wartość umowy.

Nadzór

Wskaźniki KPI i KRI, audyty, testy penetracyjne i przećwiczone plany pokazują zarządowi, czy system działa.



Przerwa obiadowa 12:15–12:45

Po przerwie, 12:45–15:00: Moduł III – Incydenty, pracownicy i współczesne zagrożenia.

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); RODO (rozporządzenie 2016/679); CERT Polska, Raport roczny 2025 (8.04.2026)