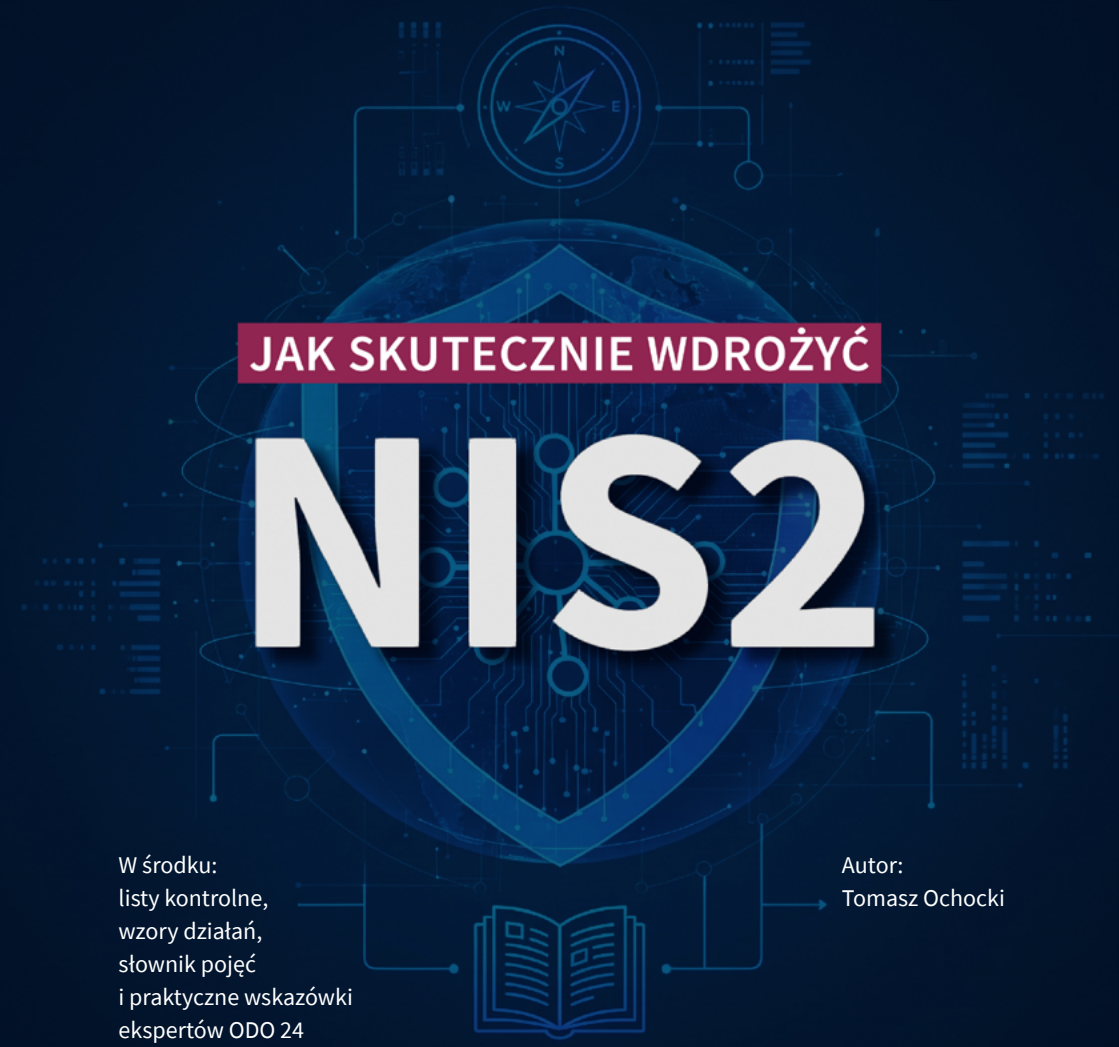
ODO 24

JAK SKUTECZNIE WDROŻYĆ NIS2



W środku:
listy kontrolne,
wzory działań,
słownik pojęć
i praktyczne wskazówki
ekspertów ODO 24

Autor:
Tomasz Ochocki

PRAKTYCZNY PRZEWODNIK
DLA FIRM

Wydanie I: Warszawa, 2026
Wydawca: ODO 24 sp. z o.o.
Skład: Enzo.pl

KONTAKT: WWW: ODO24.pl • **E-mail:** biuro@ODO24.pl

Spis treści

Cyberbezpieczeństwo to nie opcja – to konieczność

W erze cyfrowej transformacji bezpieczeństwo danych i systemów informatycznych przestało być jedynie zagadnieniem technicznym. Stało się fundamentem stabilności biznesowej, zaufania klientów i ciągłości działania każdej nowoczesnej organizacji. Dyrektywa NIS2 to odpowiedź Unii Europejskiej na ten zmieniający się krajobraz zagrożeń – i jest to odpowiedź stanowcza.

Dla wielu polskich firm nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (UKSC), wdrażająca unijną dyrektywę NIS2, może wydawać się kolejnym biurokratycznym obowiązkiem. Nic bardziej mylnego. To zestaw reguł, których celem jest stworzenie „wspólnej tarczy" chroniącej europejską gospodarkę przed cyberatakami, awariami infrastruktury i przerwami w dostawach usług.

O czym jest ten poradnik?

Jako eksperci ODO 24 na co dzień wspieramy firmy w budowaniu systemów bezpieczeństwa. Wiemy, że język ustaw bywa skomplikowany, a wymagania techniczne – przytłaczające. Dlatego przygotowaliśmy poradnik, w którym tłumaczymy złożone przepisy na język biznesu.

W tym opracowaniu:

- → **Wyjaśniamy**, czym różnią się podmioty kluczowe od podmiotów ważnych oraz jak sprawdzić, do której grupy należy Twoja firma.
- → **Wskazujemy** konkretne działania, które musi podjąć zarząd, aby uniknąć osobistej odpowiedzialności za zaniedbania.
- → **Dajemy narzędzia** – od procedur zarządzania ryzykiem, przez plany ciągłości działania, aż po gotowe listy kontrolne, które znajdziesz w dodatkach.

Dyrektywa NIS2 wymaga zmiany myślenia. Nie chodzi już tylko o to, by gasić pożary (reagować na incydenty), lecz o to, by systemowo im zapobiegać.

Wymaga to między innymi analizy ryzyka, weryfikacji łańcucha dostaw i regularnego testowania zabezpieczeń.

Czy Twoja firma jest gotowa na te zmiany? Zapraszamy do lektury. To najlepszy moment, aby z pomocą ekspertów zadbać o bezpieczną przyszłość Twojej organizacji.

Rozdział 1. Rewolucja NIS2 i nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (UKSC) – co zmieniają nowe przepisy

W świecie cyberbezpieczeństwa rok 2016 wydaje się odległą epoką. To wtedy weszła w życie pierwsza dyrektywa NIS. Od tego czasu krajobraz zagrożeń zmienił się diametralnie – pandemia przyspieszyła cyfryzację, wojna w Ukrainie pokazała realność cyberwojny, a ataki typu ransomware stały się codziennością biznesową.

Odpowiedzią Unii Europejskiej na te wyzwania jest **dyrektywa NIS2**. Nie jest to jedynie aktualizacja starych przepisów. To zupełnie nowe podejście, które ma na celu zbudowanie jednolitego, wysokiego poziomu cyberbezpieczeństwa w całej Wspólnocie.

Czym jest dyrektywa NIS2 i dlaczego jest ważna?

Dyrektywa NIS2 (Network and Information Security Directive 2) to akt prawny, który zobowiązuje państwa członkowskie UE do wprowadzenia rygorystycznych zasad ochrony cyfrowej. Jej poprzedniczka (NIS1)

dotyczyła wąskiej grupy operatorów usług kluczowych (z sektora energii, zdrowia, transportu, bankowości i finansów, zaopatrzenia w wodę oraz infrastruktury cyfrowej). Dyrektywa NIS2 znacząco rozszerza ten zakres.

Dlaczego ta zmiana jest kluczowa dla Twojej firmy?

Ponieważ bezpieczeństwo cyfrowe przestało być problemem wyłącznie działu IT. Stało się wyzwaniem biznesowym, operacyjnym i prawnym. Dyrektywa NIS2 przenosi ciężar odpowiedzialności na wyższy poziom organizacji i wymaga, aby bezpieczeństwo było integralną częścią każdego procesu biznesowego – od produkcji, przez HR, aż po łańcuch dostaw.

Ewolucja zagrożeń

Kiedyś (NIS1)	***Dziś (NIS2)***
Głównym celem ataku było wykradzenie danych z banku lub sparaliżowanie elektrowni. Przepisy skupiały się na punktowej ochronie największych graczy.	*Hakerzy atakują mniejsze podmioty (np. dostawcę oprogramowania księgowego lub firmę produkującą żywność), aby za ich pośrednictwem dostać się do większych celów lub sparaliżować łańcuch dostaw. Dlatego dyrektywa NIS2 obejmuje parasolem ochronnym znacznie szerszy rynek – w tym Twoich dostawców i klientów.*

Wdrożenie dyrektywy NIS2 w Polsce – nowelizacja ustawy o KSC

Dyrektywa unijna wyznacza cel, ale to prawo krajowe określa sposób jego realizacji. W Polsce dyrektywa NIS 2 została wdrożona w drodze nowelizacji **ustawy o krajowym systemie cyberbezpieczeństwa (UKSC).**

To właśnie znowelizowana ustawa o KSC stanowi bezpośrednią podstawę prawną dla Twojej firmy. Nakłada ona nowe obowiązki, definiuje terminy raportowania incydentów oraz określa wysokość kar. Choć proces legislacyjny w Polsce opóźnił się względem unijnego terminu (październik 2024), nowelizacja została ogłoszona, a nowe przepisy w pełni już obowiązują.

NIS1 a NIS2 – co się zmienia?

Nowe przepisy to nie kosmetyka, lecz zmiana filozofii. Oto pięć kluczowych obszarów, w których dyrektywa NIS2, a za nią nowelizacja UKSC, rewolucjonizuje podejście do bezpieczeństwa:

1. **Szerszy zakres podmiotowy:** Dyrektywa NIS2 obejmuje sektory, które wcześniej były pomijane, takie jak produkcja żywności, chemikalia, gospodarka odpadami czy usługi pocztowe.
2. **Nowa kategoryzacja:** Zamiast skomplikowanego procesu wyznaczania „operatorów usług kluczowych” decyzją administracyjną dyrektywa NIS2 wprowadza jasną zasadę wielkości (size-cap rule). Jeśli jesteś średnim lub dużym przedsiębiorstwem w objętym sektorze –

podlegasz przepisom automatycznie. W niektórych sektorach nowymi regulacjami będą objęte także mikro- i małe firmy oraz podmioty niebędące przedsiębiorcami.

3. **Bezpieczeństwo łańcucha dostaw:** To nowość – firmy muszą teraz nie tylko dbać o własne podwórko, lecz także weryfikować bezpieczeństwo swoich dostawców i podwykonawców.
4. **Osobista odpowiedzialność zarządu:** Dyrektywa NIS2 wprost wskazuje, że organy zarządzające mogą być pociągnięte do odpowiedzialności (w tym finansowej i dyscyplinarnej) za rażące zaniedbania w cyberbezpieczeństwie.
5. **Rygorystyczne raportowanie incydentów:** Wprowadzono ścisłe ramy czasowe zgłaszania incydentów (24 godziny na wczesne ostrzeżenie), co wymusza posiadanie sprawnych procesów monitoringu.

Kiedyś (NIS1)	***Dziś (NIS2)***
Wąska grupa sektorów, rozmyta odpowiedzialność, reaktywność, niskie kary.	*Wiele nowych sektorów (m.in. ścieki, żywność, przemysł), osobista odpowiedzialność zarządu, prewencja i łańcuch dostaw, wysokie kary (do 10 mln euro lub 2% obrotu – dla podmiotów kluczowych, do 7 mln euro lub 1,4% obrotu – dla podmiotów ważnych).*

Podejście all-hazards (wszystkie zagrożenia)

Dyrektywa NIS2 promuje podejście, które wykracza poza same cyberataki. Twoja firma musi być odporna na wszystkie zagrożenia (all-hazards approach), które mogą zakłócić działanie systemów informatycznych.

Oznacza to, że musisz brać pod uwagę również:

→ klęski żywiołowe (np. powodzie, pożary serwerowni),

→ błędy ludzkie (np. nieumyślne skasowanie danych przez pracownika),

→ awarie techniczne (np. przerwy w dostawie prądu, awarie łączy),

→ problemy w łańcuchu dostaw (np. upadłość kluczowego dostawcy IT).

Podejście all-hazards w praktyce

Wyobraź sobie firmę produkcyjną.

Scenariusz A (cyberatak):

Hakerzy szyfrują dane produkcyjne. Dyrektywa NIS2 i nowelizacja UKSC wymaga posiadania kopii zapasowych (backupów) offline, aby było możliwe odtworzenie systemu.

Scenariusz B (pożar):

Pożar niszczy serwerownię w biurze. Podejście all- hazards według dyrektywy NIS2 i nowelizacji UKSC wymaga, aby kopie zapasowe były przechowywane w innej lokalizacji (np. w chmurze lub drugim oddziale), co zapewni ciągłość działania mimo fizycznego zniszczenia sprzętu.

Wniosek:Procedury muszą chronić ciągłość biznesu niezależnie od przyczyny awarii.

Podsumowanie

Wejście w życie nowelizacji UKSC to moment zwrotny. Firmy, które potraktują te zmiany jako okazję do uporządkowania procesów, zyskają przewagę konkurencyjną i zaufanie rynku. Natomiast te, które zignorują nowe obowiązki, narażą się na poważne ryzyko finansowe i prawne.

Rozdział 2. Kwalifikacja podmiotów – czy Twoja firma podlega nowym przepisom

W poprzedniej wersji przepisów (NIS1) sytuacja była stosunkowo prosta: organizacja czekała na decyzję administracyjną. Jeśli otrzymała pismo potwierdzające, że jest operatorem usługi kluczowej, musiała działać. Jeśli nie – problem jej nie dotyczył.

Wraz z dyrektywą NIS 2 i nowelizacją UKSC ta zasada przestała obowiązywać.

Nowe przepisy wprowadzają mechanizm **samoidentyfikacji**. To Ty, jako przedsiębiorca, masz obowiązek sprawdzić, czy podlegasz ustawie o KSC, a następnie zgłosić się do wykazu. Niewiedza nie zwalnia z odpowiedzialności. Brak rejestracji sam w sobie jest naruszeniem przepisów i może skutkować karami – także bezpośrednio dla zarządu.

Krok 1: Wielkość ma znaczenie (zasada size-cap)

Pierwszym filtrem jest wielkość przedsiębiorstwa. Zgodnie z nowelizacją UKSC przepisy obejmują przede wszystkim **średnie i duże przedsiębiorstwa.**

Aby dowiedzieć się, czy Twoja firma spełnia kryteria, sprawdź poniższe progi:

1. **Średnie przedsiębiorstwo** – zatrudniasz co najmniej 50 pracowników oraz Twój roczny obrót lub bilans przekracza 10 mln euro.
2. **Duże przedsiębiorstwo** – zatrudniasz co najmniej 250 pracowników oraz Twój roczny obrót przekracza 50 mln euro (lub bilans 43 mln euro).

Jeśli spełniasz te warunki **oraz** działasz w jednym z sektorów wymienionych poniżej – podlegasz przepisom dyrektywy UKSC.

Kiedy mała firma podlega znowelizowanym przepisom UKSC?

Istnieją wyjątki od reguły wielkości. Nawet jeśli jesteś mikro- lub małym przedsiębiorstwem, podlegasz przepisom, jeśli:

→ jesteś dostawcą usług zaufania (np. podpisu elektronicznego),

→ jesteś dostawcą usług DNS lub rejestru nazw domen, w tym najwyższego poziomu (TLD),

→ jesteś jedynym dostawcą usługi krytycznej dla społeczeństwa lub gospodarki w danym państwie,

→ awaria Twojej firmy mogłaby zagrozić bezpieczeństwu publicznemu lub zdrowiu,

→ jesteś dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa (dotyczy co najmniej małego przedsiębiorcy),

- → państwo zidentyfikowało Cię jako podmiot krytyczny, podmiot kluczowy lub podmiot ważny,
- → jesteś podmiotem publicznym wskazanym w załączniku nr 1 do UKSC w sektorze podmiotów publicznych lub jesteś samorządową jednostką budżetową, samorządowym zakładem budżetowym, samorządową instytucją kultury albo spółką wykonującą zadania o charakterze użyteczności publicznej – jeśli realizujesz zadanie publiczne z wykorzystaniem systemów informacyjnych,
- → nie jesteś przedsiębiorcą, ale jesteś podmiotem wskazanym w załączniku nr 1 lub 2 do UKSC z nazwy albo przez określenie rodzaju,
- → jesteś operatorem obiektu energetyki jądrowej lub jego inwestorem, który uzyskał decyzję zasadniczą,
- → jesteś przedsiębiorcą komunikacji elektronicznej.

Krok 2: Sektor działalności – podmioty kluczowe a podmioty ważne

Dyrektywa NIS2 i nowelizacja UKSC dzieli firmy na dwie kategorie – podmioty kluczowe i podmioty ważne. Różnią się one stopniem krytyczności dla państwa oraz rygorem nadzoru.

A. Podmioty kluczowe (key entities)

To podmioty należące do sektorów o fundamentalnym znaczeniu dla funkcjonowania państwa. Awaria w tych sektorach może sparaliżować

życie społeczne.

- → **Energetyka** (wydobywanie kopalin, energia elektryczna, ciepło, ropa i paliwa, gaz, energetyka jądrowa, wodór)
- → **Transport** (lotniczy, kolejowy, wodny, drogowy)
- → **Bankowość i infrastruktura rynków finansowych**
- → **Ochrona zdrowia** (podmioty lecznicze, laboratoria referencyjne UE, podmioty udzielające świadczeń opieki zdrowotnej będące podwykonawcą dla podmiotów kluczowych lub podmiotów ważnych w sektorze ochrony zdrowia, infrastruktura IT i administracja zdrowia, producenci, importerzy i dystrybutorzy farmaceutyków, producenci wyrobów medycznych, apteki ogólnodostępne)
- → **Woda** (zaopatrzenie w wodę pitną, odprowadzanie i oczyszczanie ścieków)
- → **Infrastruktura cyfrowa** (IXP, dostawcy usług chmurowych, dostawcy usług DNS, w tym TLD, centra danych, dostawcy treści CDN, usługi zaufania, podmioty świadczące usługi rejestracji nazw domen, przedsiębiorcy komunikacji elektronicznej)
- → **Zarządzanie usługami ICT** (dostawcy usług zarządzanych – MSP i MSSP)
- → **Przestrzeń kosmiczna** (infrastruktura naziemna wspierająca świadczenie usług kosmicznych, Polska Agencja Kosmiczna)
- → **Podmioty publiczne** (centralne instytucje publiczne, administracja rządowa i samorządowa)

B. Podmioty ważne (important entities)

To podmioty należące do sektorów istotnych dla gospodarki. Zakłócenia w tych sektorach są dotkliwe, ale nie paraliżują natychmiastowo funkcjonowania państwa.

- → **Usługi pocztowe i kurierskie**
- → **Inwestycje energetyki jądrowej**
- → **Gospodarowanie odpadami** (zbieranie, transport, przetwarzanie, sortowanie, nadzór, postępowanie z miejscami unieszkodliwiania, sprzedaż odpadów, pośrednictwo w obrocie odpadami)
- → **Produkcja, wytwarzanie i dystrybucja chemikaliów**
- → **Produkcja, przetwarzanie i dystrybucja żywności** (hurtowa, przemysłowa)
- → **Produkcja przemysłowa** (wyroby medyczne, wyrób maszyn, pojazdów, sprzętu elektrycznego, elektronicznego, optycznego, medycznego)
- → **Dostawcy usług cyfrowych** (platformy handlowe online, wyszukiwarki, serwisy społecznościowe)
- → **Badania naukowe** (organizacje badawcze, podmioty edukacyjne, instytucje badawcze, specjalistyczne centra naukowo-szkoleniowe)

1. *Czy jesteś średnim albo dużym przedsiębiorstwem?*
> TAK > Idź dalej.

2. *Czy działasz w sektorze z listy A?*
> TAK > Jesteś podmiotem kluczowym.

3. *Czy działasz w sektorze z listy B?*
> TAK > Jesteś podmiotem ważnym.

Krok 3: Różnice w nadzorze

Wiesz już, do której grupy należy Twoja firma. Co to oznacza w praktyce? Główna różnica dotyczy sposobu, w jaki organy nadzorcze będą Cię kontrolować.

Podmioty kluczowe – NADZÓR PEŁNY (ex ante i ex post)

→ Organ nadzorczy nie musi czekać na incydent. Może przeprowadzić kontrolę w dowolnym momencie, aby sprawdzić Twoje procedury i przestrzeganie obowiązków wynikających z ustawy o KSC.

→ Musisz przeprowadzać regularne audyty bezpieczeństwa (co 3 lata).

Podmioty ważne – NADZÓR NASTĘPCZY (ex post)

→ Organ nadzorczy interweniuje zazwyczaj dopiero wtedy, gdy otrzyma zgłoszenie o incydencie lub ma dowody na nieprzestrzeganie przepi-

sów.

→ Działasz, dopóki coś się nie stanie – ale gdy się stanie, trzeba być przygotowanym i mieć dokumenty, które to potwierdzą.

Różnica w praktyce:

Szpital (podmiot kluczowy): *Może spodziewać się audytora, który sprawdzi dokumentację BCP (ciągłości działania), nawet jeśli systemy działają bez zarzutu.*

Fabryka mebli (podmiot ważny – produkcja): *Prawdopodobnie nie będzie miała rutynowej kontroli, dopóki nie padnie ofiarą ransomware i nie zgłosi tego faktu. Wtedy organ nadzorczy sprawdzi, czy fabryka miała wdrożone środki bezpieczeństwa. Jeśli nie – może zostać na nią nałożona dotkliwa kara.*

Obowiązek rejestracji

Jeśli Twoja firma jest podmiotem kluczowym lub podmiotem ważnym, masz określony termin na zgłoszenie jej do wykazu.

1. **Termin:** Masz 6 miesięcy od momentu spełnienia kryteriów (lub od wejścia w życie ustawy o KSC) na złożenie wniosku o wpis do wykazu.
2. **Gdzie:** Rejestracja odbywa się przez system teleinformatyczny Mini-

sterstwa Cyfryzacji.

3. **Zakres danych:** We wniosku musisz podać m.in. dane firmy, aktualne dane kontaktowe, listę adresów IP oraz dane osób wyznaczonych do kontaktu w sprawach cyberbezpieczeństwa.

Podsumowanie

Kwalifikacja podmiotu to fundament. Błędne założenie, że „mnie to nie dotyczy”, jest najprostszą drogą do problemów prawnych.

Nadal nie masz pewności, czy podlegasz dyrektywie NIS2?

Przepisy bywają skomplikowane, a granica między podmiotem kluczowym a podmiotem ważnym nie zawsze jest oczywista. Jednak nie musisz analizować ustawy o KSC samodzielnie.

Przygotowaliśmy bezpłatny, interaktywny test, który w kilka minut pomoże Ci zweryfikować status Twojej firmy. Wystarczy odpowiedzieć na kilka prostych pytań, aby otrzymać wstępną ocenę. W niektórych przypadkach konieczna może być także dalsza, pogłębiona analiza.

Zeskanuj kod QR lub kliknij w link i sprawdź teraz:

W kolejnym rozdziale omówimy, co zmiana przepisów oznacza dla prezesów, dyrektorów i członków zarządu.

Rozdział 3. Odpowiedzialność zarządu – nowe zasady gry

Przez lata w wielu firmach panowało niepisane przekonanie: „Cyberbezpieczeństwo? To problem dyrektora IT. Ja zarządzam biznesem". Gdy dochodziło do wycieku danych, zarząd wyrażał ubolewanie, a konsekwencje ponosił szef działu informatyki.

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa kończy z tym modelem.

Nowe przepisy wprowadzają fundamentalną zmianę: **cyberbezpieczeństwo staje się prawnym obowiązkiem kadry zarządzającej (C-level).** Nowelizacja UKSC wprost wskazuje, że organy zarządzające ponoszą osobistą odpowiedzialność za naruszenia. Nie można się już zasłaniać brakiem wiedzy technicznej ani delegowaniem zadań.

Koniec z delegowaniem odpowiedzialności

Oczywiście prezes firmy nie musi osobiście konfigurować firewalli ani instalować antywirusów. Zadania techniczne nadal wykonują specjaliści. **Jednak odpowiedzialność za skuteczność tych działań pozostaje na górze.**

Zgodnie z nowelizacją UKSC organy zarządzające podmiotów kluczowych i podmiotów ważnych mają trzy główne obowiązki:

1. **Zatwierdzanie środków:**
   To zarząd musi zaakceptować i podpisać politykę analizy ryzyka oraz plan postępowania z ryzykiem. Podpis pod tymi dokumentami oznacza: „Rozumiem zagrożenia i akceptuję sposób, w jaki firma się przed nimi broni".
2. **Nadzór:**
   Zarząd musi aktywnie nadzorować wdrażanie środków bezpieczeństwa. Nie wystarczy raz w roku zapytać: „Czy jesteśmy bezpieczni?". Wymagane jest regularne raportowanie i weryfikowanie, czy działania są rzeczywiście realizowane.
3. **Odpowiedzialność:**
   W razie incydentu organ nadzorczy nie zapuka do drzwi administratora sieci, lecz do gabinetu prezesa.

Co to znaczy w praktyce?

Jeśli firma padnie ofiarą ataku ransomware, ponieważ nie zaktualizowała systemów, a zarząd nie zapewnił budżetu na te aktualizacje lub nie wymagał raportów o stanie zabezpieczeń, wina leży po stronie zarządu. Tłumaczenia w rodzaju: „Dyrektor IT mówił, że jest w porządku" – nie będą skuteczną linią obrony.

Obowiązkowe szkolenia dla zarządu

Ustawodawca przewidział argument: „Ale ja nie jestem informatykiem, nie znam się na tym". Dlatego nowelizacja UKSC nakłada na kadrę zarządzającą obowiązek odbywania szkoleń.

Nie chodzi o naukę kodowania. Chodzi o to, by członkowie organów zarządzających potrafili w szczególności:

→ zidentyfikować ryzyko cybernetyczne dla biznesu,

→ ocenić, czy środki proponowane przez dział IT są adekwatne,

→ zrozumieć wpływ cyberzagrożeń na finanse i reputację firmy.

Uwaga: Ustawa o KSC wymaga, aby kadra zarządzająca zapewniała podobne szkolenia również pracownikom. Świadomość bezpieczeństwa musi płynąć z góry.

Sankcje za naruszenie obowiązków – kary finansowe to nie wszystko

Naruszenie obowiązków wynikających z nowelizacji UKSC wiąże się z surowymi sankcjami. Są one wzorowane na systemie znanym z RODO, ale w niektórych aspektach przewidziano rozwiązania idące znacznie dalej.

1. Gigantyczne kary finansowe

Organ nadzorczy (np. Minister Cyfryzacji lub KNF) może nałożyć administracyjną karę pieniężną. Jej wysokość zależy od kategorii podmiotu:

Kategoria podmiotu	Maksymalna kara finansowa
Podmiot kluczowy	Do 10 000 000 euro lub 2% rocznego światowego obrotu (wyższa kwota)
Podmiot ważny	Do 7 000 000 euro lub 1,4% rocznego światowego obrotu (wyższa kwota)

Kary mogą być nakładane nie tylko za wyciek danych, lecz także za niewykonywanie obowiązków, m.in. za **brak wdrożenia odpowiednich procedur** (np. brak analizy ryzyka) czy **niezgłoszenie incydentu w terminie.**

Organ może nałożyć karę w wysokości do **100 000 000 zł**, jeśli podmiot kluczowy lub podmiot ważny narusza przepisy znowelizowanej UKSC, co powoduje:

- → bezpośrednie i poważne cyberzagrożenie dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi,
- → zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług.

Kary pieniężne mogą zostać nałożone także na kierowników podmiotów kluczowych i podmiotów ważnych – w kwocie niewiększej niż 300% otrzymywanego przez ukaranego wynagrodzenia obliczanego według

zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop.

2. Opcja atomowa – zawieszenie w funkcjach (tylko podmioty kluczowe)

To najbardziej kontrowersyjny i dotkliwy mechanizm przewidziany w nowelizacji UKSC. W przypadku rażących i powtarzających się naruszeń w podmiocie kluczowym organ nadzorczy może wystąpić o:

- → **tymczasowe zawieszenie certyfikacji lub zezwolenia** na prowadzenie działalności,
- → **tymczasowy zakaz pełnienia funkcji kierowniczych** (np. CEO, członka zarządu) w tym podmiocie.

Oznacza to, że prezes może zostać odsunięty od zarządzania własną firmą, dopóki nie zostaną naprawione uchybienia w cyberbezpieczeństwie. To potężne narzędzie dyscyplinujące, które zmienia cyberbezpieczeństwo w „być albo nie być" dla kadry menedżerskiej.

Podsumowanie

Nowelizacja UKSC wymusza profesjonalizację zarządzania bezpieczeństwem. Zarząd nie musi wiedzieć, jak skonfigurować firewall, ale musi rozumieć, że firewall jest potrzebny, zapewnić na niego budżet, a także rozliczać dział IT z jego działania.

Lista „to-do” dla członka zarządu

- ❒ Zapisz się na szkolenie z cyberbezpieczeństwa dla kadry menedżerskiej.
- ❒ Zażądaj audytu otwarcia (ustalenie, gdzie jesteśmy).
- ❒ Wpisz bezpieczeństwo IT jako stały punkt agendy posiedzeń zarządu.

W kolejnym rozdziale przejdziemy do konkretów: jak zbudować fundament bezpieczeństwa, czyli jak zarządzać ryzykiem.

Rozdział 4. Fundament systemu – zarządzanie ryzykiem

Wiele firm popełnia błąd, zaczynając budowanie cyberbezpieczeństwa od zakupów. Pojawiają się: drogi firewall, zaawansowany system antywirusowy i coraz bardziej skomplikowane hasła. A potem okazuje się, że hakerzy dostali się do sieci przez niezabezpieczoną drukarkę, a pożar w serwerowni zniszczył jedyną kopię danych.

Znowelizowana ustawa UKSC odwraca tę logikę. Jest **neutralna technologicznie**. Nie mówi: „musisz kupić sprzęt marki X", lecz: **„zastosuj środki adekwatne do ryzyka".**

Aby dobrać środki adekwatne do ryzyka, najpierw musisz wiedzieć, co Ci grozi. Właśnie temu służy zarządzanie ryzykiem.

Czym jest zarządzanie ryzykiem w ujęciu UKSC

Zarządzanie ryzykiem to proces, który pozwala odpowiedzieć na cztery pytania:

1. Co mamy cennego? (aktywa)
2. Co nam grozi? (zagrożenia)
3. Jaka jest skala skutków? (ocena ryzyka)
4. Co zrobimy, żeby straty były jak najmniejsze? (postępowanie z ryzykiem)

Analiza ryzyka to podstawa. Bez niej każde wydane euro na bezpieczeństwo jest wydatkiem „na ślepo". Zgodnie z nowelizacją UKSC proces ten musi być udokumentowany, powtarzalny i – co najważniejsze – **zaakceptowany przez zarząd.**

Proces zarządzania ryzykiem krok po kroku

Nie musisz wymyślać koła na nowo. Możesz oprzeć się na standardach, np. ISO 27001 lub ISO 27005. Oto uproszczony schemat działania:

Krok 1: Inwentaryzacja (co mamy cennego?)

Nie da się chronić czegoś, o czym nie wiesz, że istnieje. Spisz aktywa organizacji, takie jak:

→ sprzęt – serwery, laptopy, urządzenia produkcyjne (OT), telefony,

→ oprogramowanie – systemy ERP, CRM, bazy danych,

→ informacje – dane klientów, receptury, plany finansowe,

→ ludzie – kluczowi specjaliści.

Krok 2: Identyfikacja zagrożeń (co nam grozi?)

Zagrożenia to nie tylko hakerzy. Musisz uwzględnić także:

→ cyberataki – ransomware, phishing, DDoS,

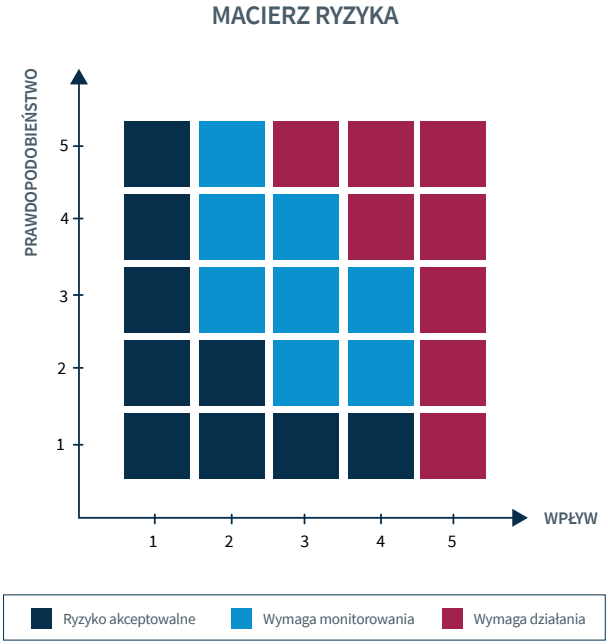
→ zagrożenia fizyczne – pożar, powódź, brak prądu, kradzież sprzętu,

→ czynnik ludzki – błąd pracownika, sabotaż, niedostępność kluczowego personelu (np. w czasie pandemii).

Krok 3: Ocena ryzyka (jaka jest skala skutków?)

Dla każdego zidentyfikowanego zagrożenia określ dwa parametry:

1. **prawdopodobieństwo** – jakie jest prawdopodobieństwo, że do tego dojdzie? (niskie/średnie/wysokie).
2. **wpływ** – jak dotkliwe dla firmy będą skutki finansowe, operacyjne lub wizerunkowe?



Krok 4: Plan postępowania z ryzykiem – co zrobimy, żeby straty były jak najmniejsze?

Po zidentyfikowaniu ryzyk musisz podjąć decyzję, jak z nimi postępować. Masz cztery możliwości:

1. **Mitygacja (zmniejszenie):** Wdrażasz zabezpieczenia, np. instalujesz system gaśniczy w serwerowni lub szyfrujesz dyski. To najczęstsza reakcja.
2. **Unikanie:** Rezygnujesz z ryzykownego działania, np. przestajesz używać przestarzałego oprogramowania, którego nie da się zabezpieczyć.
3. **Transfer (przeniesienie):** Przerzucasz skutki na inny podmiot, np. wykupujesz ubezpieczenie od cyberryzyk lub zlecasz proces firmie zewnętrznej z gwarancją SLA.
4. **Akceptacja:** Świadomie decydujesz, że ryzyko jest małe, a koszt zabezpieczeń zbyt duży, np. akceptujesz ryzyko awarii drukarki.

Decyzja biznesowa, nie techniczna

Zagrożenie: *Awaria serwera pocztowego.*

Opcja A (mitygacja): *Budujemy zapasową serwerownię za 500 tys. zł. Poczta działa zawsze.*

Opcja B (akceptacja): *Akceptujemy, że w razie awarii nie mamy dostępu do poczty przez 4 godziny. Koszt: 0 zł.*

Nowelizacja UKSC dopuszcza wybór opcji B, pod warunkiem że zarząd podejmie świadomą decyzję opartą na analizie oraz ją udokumentuje, np. podpisze oświadczenie: „Tak, rozumiemy ryzyko braku poczty i je akceptujemy (apetyt na ryzyko)".

Apetyt na ryzyko (risk appetite)

Apetyt na ryzyko to kluczowe pojęcie w kontekście dyrektywy NIS2. Żadna firma nie jest w pełni bezpieczna, dlatego zarząd musi określić **poziom tolerancji.**

→ Jak długo możemy nie działać? (RTO)

→ Ile danych możemy stracić? (RPO)

→ Jakie straty finansowe jesteśmy w stanie ponieść?

Poziom tolerancji określa granice akceptowalnego ryzyka rezydualnego. Wszystko, co przekracza ten poziom, musi zostać dodatkowo zabezpieczone.

Dokumentacja – tarcza dla zarządu

W świecie audytów NIS2 obowiązuje prosta zasada: **jeśli coś nie jest udokumentowane, to nie istnieje.**

Dlatego musisz posiadać:

→ metodykę – opis sposobu oceny ryzyka (tak aby wyniki były porówny-

walne z roku na rok),

- → raport z analizy ryzyka – listę zidentyfikowanych zagrożeń wraz z ich oceną,
- → plan postępowania z ryzykiem – listę działań naprawczych, harmonogram, budżet i osoby odpowiedzialne.

Dokumenty te muszą być **podpisane przez zarząd**. To jest Wasza polisa ubezpieczeniowa w razie kontroli – potwierdza, że działaliście z należytą starannością.

Podsumowanie

Zarządzanie ryzykiem to nie jednorazowe działanie, lecz proces. Zagrożenia ewoluują: zmienia się skład zespołu, pojawiają się nowe technologie (np. AI), wybuchają konflikty zbrojne. Dlatego przegląd analizy ryzyka powinien odbywać się **minimum raz w roku** lub po każdej dużej zmianie w firmie.

Gdy mamy już zmapowane ryzyka, musimy ustalić zasady gry – o tym jest kolejny rozdział.

Rozdział 5. Polityka bezpieczeństwa informacji – fundament zgodności

Wiemy już, co nam grozi (dzięki analizie ryzyka). Ustalmy więc, jak się przed tym bronić. Temu służy **polityka bezpieczeństwa informacji (PBI)**.

W wielu firmach polityki pozostają martwymi dokumentami: tworzy się je tylko pod audyt, a potem chowa do szuflady. W świetle dyrektywy NIS2 takie podejście jest niebezpieczne. Jeśli dojdzie do incydentu, organ nadzorczy poprosi o dokumenty. Gdy okaże się, że pracownicy ich nie znają, a opisane w nich zasady to fikcja, zarząd poniesie odpowiedzialność za brak nadzoru.

Polityka bezpieczeństwa informacji to „konstytucja" każdej firmy w zakresie cyberbezpieczeństwa. To deklaracja zarządu: „Tak chronimy nasze dane i systemy – i zapewniamy na to budżet".

Porządek w papierach – dokumentacja normatywna i operacyjna

Nowelizacja ustawy o KSC wymaga udowodnienia, że system cyberbezpieczeństwa działa w praktyce. Aby nie utonąć w morzu papierów, warto podzielić dokumentację na dwie grupy. To podział, który zrozumie każdy audytor.

1. Dokumentacja normatywna (zasady gry)

Odpowiada na pytanie: **Jak mamy postępować?** To zbiór reguł, procedur i instrukcji, np.:

- → polityka bezpieczeństwa informacji (PBI) – dokument nadrzędny, strategia,
- → procedury, np. procedura nadawania uprawnień, procedura zgłaszania incydentów, procedura tworzenia kopii zapasowych,
- → instrukcje – dokumenty „krok po kroku", np. jak skonfigurować VPN na laptopie.

2. Dokumentacja operacyjna (dowody działania)

Odpowiada na pytanie: **Czy to zrobiliśmy?** To zapisy potwierdzające, że procedury działają, np.:

- → logi systemowe (kto, kiedy się logował),
- → rejestry (incydentów, upoważnień, sprzętu),

→ raporty z przeglądów i audytów,

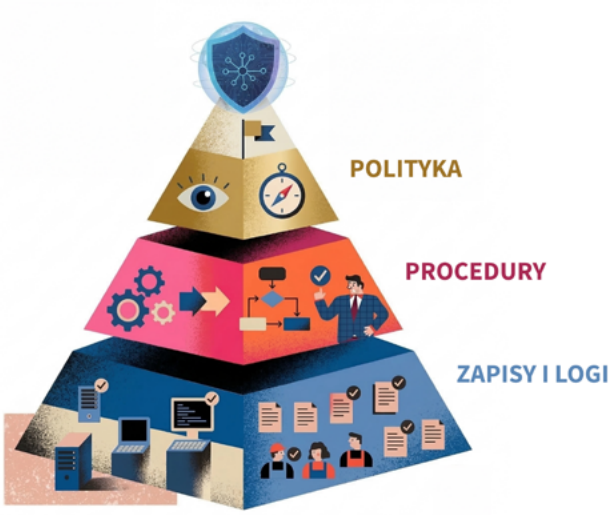
→ protokoły zniszczenia nośników danych.

Piramida dokumentacji:

→ Szczyt: Polityka (Strategia / Co chcemy osiągnąć? / Zatwierdza zarząd)

→ Środek: Procedury (Taktyka / Jak to robimy? / Zatwierdza kierownictwo)

→ Podstawa: Zapisy i logi (Dowody / Potwierdzenie wykonania / Generowane przez pracowników i systemy)



Co musi zawierać polityka bezpieczeństwa informacji

Nowelizacja UKSC nie narzuca jednego wzoru polityki bezpieczeństwa informacji. Można jednak oprzeć się na normie ISO 27001. Zgodnie z nią dobra polityka bezpieczeństwa informacji powinna regulować następujące kluczowe obszary:

1. **Zarządzanie dostępem:** Kto ma dostęp do danych? Warto stosować zasadę wiedzy koniecznej (need-to-know) – pracownik ma dostęp tylko do tego, co jest mu niezbędne do pracy.
2. **Bezpieczeństwo fizyczne:** Kto może wejść do biura i serwerowni? Jak chronimy laptopy przed kradzieżą?
3. **Zarządzanie dostawcami:** Jakie zasady obowiązują przy weryfikacji zewnętrznych firm IT i podczas współpracy z nimi?
4. **Bezpieczeństwo pracy zdalnej:** Jakie są zasady korzystania z VPN oraz zasady BYOD (lub czy obowiązuje zakaz używania prywatnego sprzętu do celów służbowych)?
5. **Zarządzanie zasobami (asset management):** Czy mamy aktualną inwentaryzację sprzętu i oprogramowania? Trzeba wiedzieć, co jest w organizacji, aby móc to chronić.
6. **Kryptografia:** Jakie są zasady szyfrowania dysków i bezpiecznego przesyłania plików?

Procedura a życie

Zły zapis: „Hasła muszą być zmieniane co 30 dni” (w praktyce pracownicy dodają tylko cyfrę na końcu, co obniża bezpieczeństwo).

Dobry zapis zgodny z nowelizacją UKSC: „Stosujemy silne hasła i obowiązkowe uwierzytelnianie wieloskładnikowe (MFA/2FA) do wszystkich systemów kluczowych”.

Ludzie i role – kto za co odpowiada

Największym grzechem w zarządzaniu bezpieczeństwem jest brak właściciela procesu. Stwierdzenie „wszyscy dbamy o bezpieczeństwo” w praktyce oznacza, że nikt za nic nie odpowiada.

Dokumentacja musi precyzyjnie przypisywać role i odpowiedzialności. Kluczowa jest tu zasada **rozdziału obowiązków** (segregation of duties). Chodzi o to, aby unikać konfliktu interesów oraz błędów.

Przykłady poprawnego rozdziału ról

→ **Administrator IT** – konfiguruje system i nadaje uprawnienia (ale tylko na wniosek).

→ **Przełożony / właściciel biznesowy** – decyduje, kto ma dostać uprawnienia (akceptuje wniosek).

→ **Audytor / inspektor bezpieczeństwa** – sprawdza, czy administrator nadał uprawnienia zgodnie z decyzją przełożonego.

W mniejszych firmach, w których nie ma rozbudowanych działów, funkcję kontrolera może pełnić firma zewnętrzna podczas okresowego audytu.

Cykl życia polityki bezpieczeństwa informacji – przegląd i aktualizacja

Stworzenie dokumentacji to dopiero początek. Dokument, którego nie aktualizujemy, szybko staje się bezużyteczny. Zgodnie z wytycznymi ENISA przegląd polityki bezpieczeństwa informacji powinien odbywać się:

- → **cyklicznie** – minimum raz w roku (czy polityka nadal odpowiada potrzebom naszej firmy?),
- → **po incydencie** – jeśli doszło do ataku, to sygnał, że procedury mogły być nieskuteczne, a więc trzeba je poprawić,
- → **przy zmianach** – takich jak wdrożenie nowego systemu ERP, przeprowadzka biura, zmiana struktury organizacyjnej.

Każda zmiana w polityce bezpieczeństwa informacji musi zostać **ponownie zatwierdzona przez zarząd**. Data i podpis na dokumencie stanowią dla audytora potwierdzenie, że zarząd sprawuje nadzór.

Podsumowanie

Polityka bezpieczeństwa informacji to nie biurokracja, lecz instrukcja obsługi bezpieczeństwa Twojej firmy. Dobre procedury ułatwiają życie (pracownicy wiedzą, co robić), a złe – paraliżują pracę.

Mając ustalone zasady (politykę) i znając zagrożenia (ryzyka), musimy przygotować się na moment, gdy mimo wszystko coś pójdzie nie tak. Czas omówić zarządzanie incydentami.

Rozdział 6. Zarządzanie incydentami – wyścig z czasem

W cyberbezpieczeństwie obowiązuje smutna zasada: **nie pytaj „czy" dojdzie do ataku, lecz „kiedy" to nastąpi.** Nawet najlepiej zabezpieczona organizacja może paść ofiarą błędu ludzkiego lub nowej, wcześniej nieznanej luki (zero-day).

Nowelizacja UKSC zmienia podejście do kryzysu. Skoro nie da się uniknąć wszystkich ataków, musisz być mistrzem w ich wykrywaniu i raportowaniu. Nowe przepisy nakładają na firmy kaganiec czasowy – a zegar zaczyna tykać w momencie wykrycia problemu.

Co jest incydentem, a co tylko zdarzeniem

Nie każda awaria to incydent w rozumieniu UKSC. Przepalona żarówka w serwerowni to zdarzenie. Pożar serwerowni to incydent.

Aby nie paraliżować pracy działu IT i organów nadzorczych, musisz wdrożyć **system kategoryzacji**. Nowelizacja UKSC nakazuje raportować tzw. **poważne incydenty**. Incydent uznaje się za poważny, jeśli:

→ powoduje lub może powodować poważne obniżenie jakości usług lub

przerwanie ciągłości ich świadczenia (np. zatrzymanie produkcji, brak dostępu do kont bankowych),

→ powoduje straty finansowe organizacji lub jej klientów,

→ stwarza zagrożenie dla innych osób przez wywołanie poważnej szkody materialnej lub niematerialnej (np. wyciek danych pacjentów).

Kiedy dzwonić na alarm?

Sytuacja A: *Pracownik zapomniał hasła i zablokował sobie konto. To jest zdarzenie. Rozwiązuje je helpdesk. Nie zgłaszasz tego do CSIRT.*

Sytuacja B: *W nocy nastąpiło 500 nieudanych prób logowania na konto administratora z adresu IP w Chinach, a rano system działa wolniej. To jest incydent. Istnieje podejrzenie ataku. Uruchamiasz procedurę reagowania.*

Oś czasu: 24 h – 72 h – 1 miesiąc

Sednem nowych przepisów są krótkie terminy raportowania incydentów. Procedura raportowania jest trójstopniowa, a czas biegnie nieubłaganie.

1. **Wczesne ostrzeżenie (24 godziny od wykrycia):** To sygnał: mamy problem. W tym czasie musisz zgłosić do właściwego CSIRT (np. CSIRT NASK), że doszło do incydentu.

Co musisz wiedzieć:

→ kiedy incydent wystąpił i kiedy został wykryty,

→ jak długo trwał (lub trwa),

→ czy jest to atak celowy,

→ czy incydent może mieć skutki transgraniczne (wpłynąć na inne kraje UE).

Cel: Umożliwienie oceny, czy incydent nie rozleje się na inne podmioty.

2. **Zgłoszenie właściwe (72 godziny od wykrycia):** To czas na konkrety – emocje opadły, a technicy pracują.

Co musisz wiedzieć:

→ jaka jest wstępna ocena powagi, przyczyn i skutków incydentu,

→ jakie wskaźniki kompromitacji (IoC) wykryliście (np. z jakiego adresu IP nastąpił atak),

→ jak przebiegał incydent,

→ jaki jest zakres incydentu – jak wpływa na usługi świadczone przez

Twoją firmę i inne podmioty, ilu osób dotyczy, jaki zasięg geograficzny obejmuje,

→ jakie podjęto działania zapobiegawcze i naprawcze.

Cel: Przekazanie informacji technicznych, które pomogą innym się bronić.

3. **Raport końcowy (1 miesiąc od zdarzenia):** To tzw. post mortem.

Co musisz wiedzieć:

→ jaki był szczegółowy przebieg incydentu,

→ jakie zakłócenia i szkody incydent spowodował,

→ czy wystąpiły skutki transgraniczne (jeśli tak – jakie),

→ jaka była przyczyna źródłowa (root cause analysis),

→ jakie środki zaradcze wdrożono, by sytuacja się nie powtórzyła.

Cel: Podsumowanie przyczyn i skutków incydentu oraz wykazanie wdrożonych działań korygujących i zapobiegawczych.

Uwaga: Jeśli nie masz gotowych szablonów zgłoszeń i listy kontaktowej do CSIRT, w stresie możesz nie zdążyć z przygotowaniem raportu w ciągu 24 godzin.

Procedura działań wewnętrznych – wykryj, zrozum, reaguj

Raportowanie na zewnątrz to jedno, ale najważniejsze jest opanowanie sytuacji wewnątrz firmy. Procedura zarządzania incydentami powinna przypominać instrukcję dla strażaków:

1. **Wykrywanie (monitoring):** W obszarze IT musisz mieć oczy dookoła głowy. Systemy logowania i monitoringu (np. SIEM) powinny działać 24/7. Bez logów nie da się ustalić, co się stało.
2. **Triage (segregacja):** Nadaj incydentowi priorytet. Czy to tylko fałszywy alarm, czy już krytyczne zagrożenie?
3. **Izolacja (powstrzymanie):** Szybko odseparuj źródło problemu, np. odłącz zainfekowane serwery od Internetu, aby wirus się nie rozprzestrzeniał.
4. **Analiza i naprawa:** Usuń wirusa, załataj lukę i przywróć dane z backupu.
5. **Lekcje (lessons learned):** Po wszystkim spotkaj się z zespołem i zapytaj: „Dlaczego to się stało i co poprawiamy w naszych procedurach?”.

Rola CSIRT

W Polsce funkcjonują trzy główne Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT):

→ **CSIRT GOV (ABW)** – dla administracji rządowej i infrastruktury kry-

tycznej,

- → **CSIRT MON** – dla wojska i podmiotów podległych MON lub przez niego nadzorowanych oraz przedsiębiorców realizujących zadania na rzecz Sił Zbrojnych,
- → **CSIRT NASK** – dla pozostałych podmiotów, w tym większości firm prywatnych, samorządów, jednostek naukowo-badawczych, uczelni i spółek komunalnych.

Krajowy system cyberbezpieczeństwa obejmuje także **CSIRT sektorowe** – powołane dla wybranych sektorów gospodarki.

Musisz wiedzieć, któremu CSIRT podlegasz.

Współpraca z CSIRT to nie tylko obowiązek, lecz także realne wsparcie. Zespół może przekazać Ci wytyczne, jak poradzić sobie z atakiem.

Podsumowanie

Zarządzanie incydentami zgodnie z dyrektywą NIS2 to test sprawności organizacyjnej. Wymaga **procedur, monitoringu i ćwiczeń**. Pamiętaj: w trakcie ataku nikt nie ma czasu na czytanie przepisów. Musisz mieć gotowe scenariusze działania (playbooki).

A co, jeśli incydent zniszczył dane lub systemy? Wtedy do gry wchodzą plany ciągłości działania, o których przeczytasz w kolejnym rozdziale.

Rozdział 7. Ciągłość działania i backupy (BCP i DRP)

Wyobraź sobie, że przychodzisz do firmy w poniedziałek rano. Serwery nie działają, telefony milczą, a na ekranach komputerów wyświetla się żądanie okupu (ransomware). Produkcja stoi, ciężarówki nie wyjeżdżają, faktur nie da się wystawić.

Pytanie brzmi: **Jak długo Twoja firma przetrwa w takim stanie?** Godzinę? Dzień? Tydzień?

Nowelizacja UKSC kładzie ogromny nacisk na odporność (resilience). Nie chodzi tylko o to, by unikać ciosów, lecz o to, by po ich przyjęciu wstać z desek i walczyć dalej. W tym pomagają BCP i DRP – dwa kluczowe pojęcia dotyczące ciągłości działania i odtwarzania po incydencie.

Różnice między BCP a DRP

Choć te skróty bywają używane zamiennie, oznaczają dwa różne dokumenty:

1. **BCP (Business Continuity Plan) – plan ciągłości działania**, czyli instrukcja dla biznesu, która opisuje, jak pracować, gdy systemy nie działają.

Przykład: Jeśli nie działa system do fakturowania, BCP wskazuje: „Przechodzimy na ręczne wypisywanie druków, które wprowadzimy do systemu po usunięciu awarii".

2. **DRP (Disaster Recovery Plan) – plan odzyskiwania po awarii**, czyli instrukcja dla IT, która opisuje, jak naprawić systemy i odzyskać dane.

   Przykład: DRP wskazuje: „Przywracamy kopię zapasową z chmury na serwer zapasowy w lokalizacji B".

Matematyka przetrwania – RTO i RPO

Aby stworzyć sensowny plan, zarząd musi podjąć decyzję biznesową i określić dwa parametry – RTO i RPO. Nie są to liczby techniczne. To wartości, które pokazują, ile pieniędzy firma jest gotowa stracić.

1. **RTO (Recovery Time Objective) – cel czasu odzyskiwania**, czyli maksymalny czas, przez jaki system może nie działać.

   Pytanie zarządu: „Po jakim czasie przestoju zbankrutujemy lub stracimy kluczowych klientów?".

2. **RPO (Recovery Point Objective) – cel punktu odzyskiwania**, czyli maksymalna ilość danych, jaką możemy bezpowrotnie stracić (mierzona w czasie).

   Pytanie zarządu: „Czy utrata danych z ostatniej godziny pracy to katastrofa? A z ostatniego dnia?".

RTO i RPO w praktyce

Sklep internetowy (e-commerce)

- *RTO musi być krótkie (np. 4 godziny). Każda godzina przestoju to realna strata przychodu.*
- *RPO musi być bliskie zeru. Utrata zamówień z ostatniej godziny oznacza chaos i niezadowolonych klientów.*

Archiwum państwowe

- *RTO może wynosić nawet 48–72 godziny. Katastrofy nie będzie, jeśli archiwum zostanie zamknięte na dwa dni.*
- *RPO może wynosić 24 godziny. Jeśli stracimy skany z jednego dnia, wykonamy je ponownie jutro.*

Wniosek: Koszt zabezpieczeń dla sklepu będzie wysoki, a dla archiwum – niski. Nowelizacja UKSC wymaga adekwatności.

Święty Graal – kopie zapasowe (backupy)

Zgodnie z nowelizacją UKSC zarządzanie kopiami zapasowymi to obowiązek, a nie opcja. Ale samo posiadanie backupu nie wystarczy – kopia musi być **odporna na atak**.

W dobie ransomware hakerzy najpierw szukają backupów, żeby je usunąć lub zaszyfrować, a dopiero potem atakują główny system. Jak się

bronić?

Złota zasada 3–2–1

→ Miej co najmniej **3** kopie danych.

→ Przechowuj je na **2** różnych nośnikach (np. dysk serwera + taśma lub chmura).

→ Zadbaj, aby **1** kopia znajdowała się **poza firmą** (off-site) lub była odłączona od sieci (offline).

Kopia offline to jedyna pewna ochrona przed ransomware. Jeśli dysk nie jest podłączony do sieci, haker nie może go zaszyfrować.

Testowanie – kopia nietestowana to brak kopii

Najczęstszy grzech firm to brak testów odtwarzania kopii zapasowych. System backupu działał latami („zielona lampka się świeciła"), ale gdy doszło do awarii, okazało się, że pliki są uszkodzone i nie da się ich odtworzyć.

Wymogi nowelizacji UKSC w zakresie testowania

→ **Regularność** – testuj odtwarzanie danych (restore test) minimum raz na kwartał.

→ **Weryfikacja** – sprawdzaj, czy kopie są kompletne i czy sumy kontrolne się zgadzają.

→ **Symulacje** – raz w roku zrób próbny alarm (fire drill). Wyłącz testowo

główny system i spróbuj przywrócić działanie firmy z systemów zapasowych.

Redundancja – nie wkładaj wszystkich jajek do jednego koszyka

Ciągłość działania oznacza także eliminowanie pojedynczych punktów awarii (single point of failure).

→ Jeśli masz jedną serwerownię – co zrobisz, gdy zaleje ją woda?

→ Jeśli masz jednego dostawcę Internetu – co zrobisz, gdy koparka przetnie kabel?

Nowelizacja UKSC zachęca do stosowania rozwiązań redundantnych (zapasowych), np. łączy od dwóch różnych operatorów czy serwerów w chmurze jako zaplecza dla infrastruktury lokalnej.

Podsumowanie

Inwestycja w ciągłość działania to kosztowna polisa, z której masz nadzieję nigdy nie skorzystać. Jednak w świetle nowelizacji UKSC brak tej polisy oznacza naruszenie obowiązków.

Masz już plan na wypadek, gdy zawiodą Twoje systemy. Ale co, jeśli zagrożenie przyjdzie z zewnątrz – od zaufanego partnera? O tym w kolejnym rozdziale poświęconym bezpiecznemu łańcuchowi dostaw.

Rozdział 8. Bezpieczny łańcuch dostaw

W cyberbezpieczeństwie funkcjonuje powiedzenie: **jesteś tak bezpieczny, jak Twój najsłabszy dostawca.**

Historia zna przypadki, w których gigantyczne korporacje – z budżetami liczonymi w miliardach dolarów – zostały zhakowane, ponieważ napastnicy weszli do ich sieci bocznym wejściem: przez systemy dostawcy klimatyzacji lub małej firmy sprzątającej, która miała dostęp do sieci Wi-Fi.

Dyrektywa NIS2 i nowelizacja UKSC podchodzą do tego problemu stanowczo. Nakłada na podmioty kluczowe i podmioty ważne obowiązek dbania nie tylko o własne podwórko, lecz także o bezpieczeństwo produktów i usług kupowanych od dostawców. W pewnych sytuacjach dostawca może zostać uznany za dostawcę wysokiego ryzyka, co oznacza konieczność wycofania określonego sprzętu lub usług. Musisz więc zacząć wymagać od swoich partnerów biznesowych tyle samo, ile państwo wymaga od Ciebie.

Nowa rzeczywistość – kontrola najwyższą formą zaufania

Do tej pory relacje z dostawcami opierały się głównie na cenie i jakości. Teraz dochodzi trzeci filar – **bezpieczeństwo**. Zgodnie z nowelizacją UKSC musisz uwzględnić podatności specyficzne dla każdego dostawcy.

Etapy procesu oceny dostawców

1. **Identyfikacja:** Kto dostarcza nam usługi IT, oprogramowanie, sprzęt?
2. **Ocena ryzyka:** Jak bardzo krytyczny jest ten dostawca? Co się stanie, jeśli zostanie zhakowany?
3. **Wymagania:** Jakie warunki musi spełnić ten dostawca, żebyśmy z nim współpracowali?

Kategoryzacja dostawców – nie każdy jest tak samo ważny

Nie musisz z taką samą surowością audytować dostawcy papieru do drukarek jak dostawcy usług chmurowych. Aby nie utonąć w biurokracji, podziel dostawców na kategorie:

1. **Dostawcy krytyczni:** Ich awaria zatrzymuje Twój biznes (np. dostawca ERP, firma hostingowa, dostawca energii). Wymagają najwyższego nadzoru i audytów.
2. **Dostawcy strategiczni:** Są ważni, ale ich awaria jest zarządzalna

(np. dostawca oprogramowania HR, obsługa prawna). Wymagają solidnych umów i jasno określonych wymagań bezpieczeństwa.

3. **Dostawcy rutynowi:** Mają mały wpływ na bezpieczeństwo sieci (np. dostawca mebli biurowych). Wymagają podstawowej weryfikacji.

Umowy – Twój najsilniejszy oręż

W momencie podpisywania umowy masz największą siłę przetargową. To wtedy warto zadbać o zapisy, które ochronią Cię w przyszłości. Dyrektywa NIS2 wymusza aktualizację kontraktów z dostawcami usług ICT.

Umowa z dostawcą powinna obejmować:

→ **klauzulę audytową** – prawo do audytu dostawcy i sprawdzenia, czy naprawdę robi backupy, tak jak obiecał,

→ **zgłaszanie incydentów** – obowiązek poinformowania Cię o incydencie po stronie dostawcy w ściśle określonym czasie (np. 24 godziny), jeśli incydent może wpłynąć na Twoje dane,

→ **SLA (Service Level Agreement)** – gwarancję dostępności usług oraz czasu naprawy,

→ **zasady podwykonawstwa** – wskazanie, czy dostawca korzysta z podwykonawców, oraz zobowiązanie, że spełniają oni wymagania bezpieczeństwa,

→ **exit plan (zakończenie współpracy)** – zasady zwrotu danych w czytelnym formacie oraz ich trwałego usunięcia z serwerów dostawcy po rozwiązaniu umowy.

Umowa a rzeczywistość

Błąd: *Podpisujesz umowę z software house'em na stworzenie aplikacji. Umowa reguluje tylko cenę i termin oddania dzieła.*

Ryzyko: *Aplikacja ma luki bezpieczeństwa, a wykonawca twierdzi, że ich usunięcie jest dodatkowo płatne.*

Podejście NIS2: *Umowa wymaga security by design. Wykonawca musi dostarczyć raport z testów bezpieczeństwa przed odbiorem, a naprawa luk krytycznych jest w cenie wdrożenia.*

Pułapka vendor lock-in (uzależnienie od dostawcy)

Dyrektywa NIS2 zwraca uwagę na ryzyko uzależnienia się od jednego dostawcy technologii. Jeśli cały Twój biznes opiera się na unikalnym systemie małej firmy, a ona nagle zbankrutuje lub zostanie przejęta przez wrogi podmiot – masz problem.

Jak się bronić?

→ **Dywersyfikacja** – tam, gdzie to możliwe, zapewnij alternatywę (np. łącza od dwóch różnych operatorów).

→ **Otwarte standardy** – używaj technologii, które pozwalają na łatwą

migrację danych (np. unikaj niszowych lub zamkniętych formatów plików).

→ **Dostęp do kodu źródłowego** – w przypadku kluczowego oprogramowania dedykowanego zadbaj o tzw. depozyt kodu (escrow), aby mieć do niego dostęp, gdy dostawca zniknie z rynku.

Polityka bezpieczeństwa łańcucha dostaw

Wszystkie powyższe zasady musisz spisać w formie **polityki bezpieczeństwa łańcucha dostaw**. Dokument ten powinien określać:

→ jakie kryteria musi spełnić nowy dostawca (np. posiadać certyfikat ISO 27001),

→ jak często weryfikowani są obecni dostawcy,

→ kto w firmie odpowiada za akceptację umów pod kątem bezpieczeństwa.

Rejestr dostawców i usługodawców

Zgodnie z zasadą „nie możesz zarządzać czymś, o czym nie wiesz", musisz prowadzić aktualny rejestr dostawców i usługodawców. Powinien on zawierać:

→ nazwę dostawcy i dane kontaktowe,

→ opis dostarczanej usługi (np. „utrzymanie serwerów"),

→ kategorię krytyczności (wysoka/średnia/niska),

→ datę ostatniej weryfikacji bezpieczeństwa.

Podsumowanie

Łańcuch dostaw to system naczyń połączonych. Dyrektywa NIS2 wymusza solidarność: Ty wymagasz od dostawców, a Twoi klienci (zwłaszcza jeśli jesteś podmiotem kluczowym) – od Ciebie. Wdrożenie tych zasad to nie tylko obowiązek prawny, lecz także sygnał dla rynku: jesteśmy bezpiecznym partnerem biznesowym.

Dotarliśmy prawie do końca. W ostatnim rozdziale zbierzemy całą wiedzę w prostą mapę drogową – pięć kroków, które musisz wykonać, by spać spokojnie.

Rozdział 9. Mapa drogowa wdrożenia NIS2 – podsumowanie

Przebrnęliśmy przez paragrafy, definicje i techniczne wymogi. Tyle obowiązków może przytłaczać – to naturalne. Wdrożenie wymogów nowelizacji UKSC jest dużym przedsięwzięciem, porównywalnym z wdrożeniem RODO w 2018 roku.

Na szczęście da się to poukładać krok po kroku. Stare biznesowe porzekadło mówi: **Jak zjeść słonia? Po kawałku!**

Eksperci ODO 24 opracowali sprawdzoną metodologię, która porządkuje wszystkie zadania. Zamiast chaotycznych zakupów sprzętu i pisania w pośpiechu procedur proponujemy podejście procesowe. Oto Twoja mapa drogowa w pięciu krokach.

Krok 1: Audyt zerowy (gdzie jesteśmy)

Zanim ruszysz w podróż, musisz wiedzieć, z jakiego punktu startujesz. Audyt zerowy (gap analysis) to „zdjęcie rentgenowskie" Twojej firmy.

Działanie:

→ przegląd obecnego stanu bezpieczeństwa,

→ sprawdzenie, jakie procedury już masz (np. z RODO lub ISO 9001), a jakich brakuje,

→ weryfikacja zabezpieczeń IT.

Wynik:
raport otwarcia pokazujący lukę między stanem obecnym a wymogami dyrektywy NIS2, czyli Twoja lista zadań.

Krok 2: Analiza ryzyka (co nam grozi)

Ten krok jest fundamentem, bez którego nie wolno Ci przejść dalej. Szczegóły opisaliśmy w rozdziale 4.

Działanie:

→ inwentaryzacja aktywów (sprzęt, ludzie, procesy),

→ identyfikacja zagrożeń,

→ określenie prawdopodobieństwa i skutków.

Wynik:
raport z analizy ryzyka i plan postępowania z ryzykiem, zatwierdzone przez zarząd – wiesz już, co musisz chronić w pierwszej kolejności.

Krok 3: Wdrożenie środków (budowa tarczy)

Dopiero gdy masz wyniki analizy ryzyka, możesz dobrać środki ochronne. Pamiętaj: muszą być one **adekwatne i proporcjonalne.**

Działanie:

→ techniczne – wdrożenie MFA, szyfrowania, systemów backupu oraz monitoringu sieci,

→ organizacyjne – ustalenie struktury odpowiedzialności, powołanie zespołu reagowania na incydenty.

Wynik:
działający system bezpieczeństwa, który realnie mityguje zidentyfikowane ryzyka.

Krok 4: Dokumentacja i procedury (zasady gry)

To etap, w którym utrwalamy wdrożone środki w postaci oficjalnych dokumentów.

Działanie:
opracowanie polityki bezpieczeństwa informacji, planów ciągłości działania (BCP i DRP), polityki łańcucha dostaw oraz procedur operacyjnych.

Wynik:
kompletna dokumentacja normatywna, dzięki której pracownicy wiedzą, jak postępować, a audytor ma co sprawdzać.

Krok 5: Szkolenia i świadomość (czynnik ludzki)

Nawet najlepszy firewall nie pomoże, jeśli pracownik kliknie w link w podejrzanym e-mailu, a prezes nie zrozumie raportu o ryzyku.

Działanie:

→ dla zarządu – obowiązkowe szkolenia z cyberbezpieczeństwa (wymóg prawny!),

→ dla pracowników – szkolenia z cyberhigieny (w tym phishing, hasła, RODO).

Wynik: zbudowanie human firewall – świadomego zespołu, który stanowi pierwszą linię obrony.

WSKAZÓWKA EKSPERTA ODO 24

Nie traktuj tych kroków jako jednorazowego działania. ***Cyberbezpieczeństwo to proces, a nie stan.*** *Po zakończeniu kroku 5 w kolejnym roku wracasz do kroku 1 – audytu i przeglądu. To cykl Deminga (PDCA: Plan–Do–Check–Act), na którym opiera się cała dyrektywa NIS2.*

Korzyści z wdrożenia NIS2 – dlaczego warto zrobić to dobrze

Wdrożenie wymogów dyrektywy NIS2 to koszt i wysiłek. Ale to także inwestycja, która zwraca się w trzech walutach:

1. **Bezpieczeństwo prawne:** Unikasz gigantycznych kar finansowych i odpowiedzialności osobistej zarządu. Śpisz spokojnie.
2. **Ciągłość biznesu:** W razie ataku ransomware Twoja konkurencja może mieć przestój nawet przez 2 tygodnie. Ty – dzięki planom BCP i backupom – wracasz do działania po 4 godzinach.
3. **Wizerunek i zaufanie:** Klienci (zwłaszcza duzi gracze podlegający dyrektywie NIS2) będą weryfikować swoich dostawców. Certyfikat zgodności lub audyt bezpieczeństwa to dziś przepustka do lukratywnych kontraktów.

Podsumowanie

Zmiany są nieuchronne. Jak głosi przysłowie: Najlepszy moment, aby zasadzić drzewo, był 20 lat temu. Drugi najlepszy moment jest teraz.

Teraz jest najlepszy moment, aby zadbać o bezpieczną przyszłość Twojej organizacji. Nie musisz robić tego samodzielnie. Eksperci ODO 24 są gotowi przeprowadzić Cię przez każdy z pięciu kroków – od audytu po szkolenia. Zabezpiecz swój biznes już dziś.

Dodatki

Dodatek A. Słownik pojęć – cyberbezpieczeństwo w pigułce

Dyrektywa NIS2 i noweliacja UKSC wprowadzają specyficzny język, którym od teraz musi posługiwać się nie tylko dział IT, lecz także zarząd.

→ **Analiza ryzyka** – proces identyfikacji zagrożeń (np. atak hakerski, pożar) i oceny, jak bardzo są one prawdopodobne oraz jakie straty mogą przynieść firmie. Fundament wdrożenia wymogów nowelizacji UKSC.

→ **BCP (Business Continuity Plan)** – plan ciągłości działania. Instrukcja biznesowa określająca, jak firma ma funkcjonować w trakcie awarii, zanim systemy zostaną naprawione (np. przejście na obsługę ręczną).

→ **CSIRT (Computer Security Incident Response Team)** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego. Państwowe jednostki (CSIRT NASK, CSIRT GOV, CSIRT MON oraz CSIRT sektorowe), do których firmy muszą zgłaszać poważne incydenty.

→ **Cyberhigiena** – podstawowe praktyki zwiększające bezpieczeństwo, takie jak regularna zmiana haseł, nieklikanie w podejrzane linki, aktualizowanie oprogramowania.

→ **DRP (Disaster Recovery Plan)** – plan odzyskiwania po awarii. Techniczna instrukcja dla IT opisująca, jak przywrócić systemy i dane

z kopii zapasowych.

- **Incydent poważny** – zdarzenie, które powoduje lub może spowodować znaczne zakłócenia w świadczeniu usług lub straty finansowe lub które zagraża innym podmiotom. Wymaga zgłoszenia do CSIRT.
- **IoC (Indicators of Compromise)** – wskaźniki kompromitacji. Cyfrowe ślady (np. podejrzane wpisy w logach) sugerujące, że doszło do ataku.
- **MFA (Multi-Factor Authentication)** – uwierzytelnianie wieloskładnikowe. Logowanie wymagające czegoś więcej niż hasła (np. kodu SMS, tokena). Wymóg stanowczo zalecany w ramach zarządzania ryzykiem.
- **Podmiot kluczowy** – firma z sektora krytycznego (np. energetyka, zdrowie, bankowość). Podlega pełnemu nadzorowi i regularnym audytom.
- **Podmiot ważny** – firma z sektora istotnego (np. produkcja, żywność, usługi pocztowe). Podlega nadzorowi następczemu (gdy dojdzie do incydentu).
- **Ransomware** – złośliwe oprogramowanie, które szyfruje dane firmy i żąda okupu za ich odblokowanie.
- **RPO (Recovery Point Objective)** – maksymalna ilość danych, jaką firma może stracić (np. z ostatniej godziny). Parametr wpływający na częstotliwość wykonywania backupów.
- **RTO (Recovery Time Objective)** – maksymalny czas, przez jaki system może nie działać po awarii, zanim firma poniesie krytyczne straty.
- **Ryzyko rezydualne** – ryzyko, które pozostaje nawet po zastosowaniu zabezpieczeń. Zarząd musi je formalnie zaakceptować.

Dodatek B. Lista kontrolna dla zarządu (governance)

Cel:

Weryfikacja, czy organy zarządzające dopełniły obowiązków, aby uniknąć osobistej odpowiedzialności prawnej i finansowej.

STATUS PRAWNY I ORGANIZACJA

- ❒ **Kwalifikacja:**
  Przeprowadzono analizę, czy firma jest podmiotem kluczowym lub podmiotem ważnym.
- ❒ **Rejestracja:**
  Firma została zgłoszona do wykazu podmiotów krajowego systemu cyberbezpieczeństwa.
- ❒ **Budżet:**
  Zatwierdzono budżet na cyberbezpieczeństwo (wdrożenia, szkolenia, audyty) na bieżący rok.
- ❒ **Zasoby:**
  Wyznaczono osobę odpowiedzialną za kontakt z CSIRT i koordynację bezpieczeństwa (np. CISO lub pełnomocnika).

ODPOWIEDZIALNOŚĆ OSOBISTA

- ❒ **Szkolenia:**
  Członkowie zarządu odbyli udokumentowane szkolenie z zakresu

cyberbezpieczeństwa.

- ❒ **Decyzje:**
  Zarząd zapoznał się z wynikami analizy ryzyka i podpisał akceptację ryzyka rezydualnego.
- ❒ **Dokumentacja:**
  Polityka bezpieczeństwa informacji została formalnie zatwierdzona (podpisana) przez zarząd.

NADZÓR I RAPORTOWANIE

- ❒ **Agenda:**
  Temat cyberbezpieczeństwa został wpisany jako stały punkt posiedzeń zarządu (np. raz na kwartał).
- ❒ **KPI:**
  Ustalono, jakie wskaźniki bezpieczeństwa mają być raportowane do zarządu (np. liczba incydentów, status wdrożenia zaleceń poaudytowych).

Dodatek C. Inwentaryzacja dokumentacji (gap analysis)

Cel:

Szybki przegląd braków w dokumentacji wymaganej przez ustawę o KSC. Zaznacz, co już jest w Twojej firmie.

DOKUMENTACJA NORMATYWNA (ZASADY)

- ☐ Polityka bezpieczeństwa informacji (dokument nadrzędny)
- ☐ Metodyka analizy ryzyka
- ☐ Raport z analizy ryzyka i plan postępowania z ryzykiem
- ☐ Polityka bezpieczeństwa łańcucha dostaw
- ☐ Plan ciągłości działania (BCP)
- ☐ Plan odzyskiwania po awarii (DRP)
- ☐ Procedura zarządzania incydentami
- ☐ Polityka kontroli dostępu i zarządzania tożsamością
- ☐ Polityka haseł i uwierzytelniania (MFA)
- ☐ Zasady pracy zdalnej i bezpieczeństwa urządzeń mobilnych (BYOD)
- ☐ Procedura tworzenia i testowania kopii zapasowych (backupów)
- ☐ Procedura zarządzania podatnościami (aktualizacje/patchowanie)

DOKUMENTACJA OPERACYJNA (DOWODY)

- ☐ Rejestr incydentów bezpieczeństwa
- ☐ Rejestr aktywów (inwentaryzacja sprzętu i oprogramowania)
- ☐ Rejestr dostawców usług IT (wraz z ich kategoryzacją)
- ☐ Listy obecności ze szkoleń pracowników (świadomość/cyberhigiena)
- ☐ Raporty z testów odtwarzania kopii zapasowych
- ☐ Logi systemowe (przechowywane przez określony czas)

Dodatek D. Reagowanie na incydent (panic button)

Cel:

Ściąga dla zespołu kryzysowego – kluczowe kroki i terminy w pierwszych godzinach ataku.

FAZA 1: IDENTYFIKACJA I POWSTRZYMANIE (natychmiast)

1. **Potwierdź:** Czy to fałszywy alarm, czy realny atak?
2. **Odizoluj:** Odłącz zainfekowane urządzenia od sieci (Wi-Fi/LAN), ale nie odłączaj ich od zasilania (możesz utracić dowody w pamięci RAM).
3. **Zabezpiecz dowody:** Zrób zdjęcia komunikatów, zabezpiecz logi.
4. **Uruchom sztab:** Zwołaj zespół reagowania na incydenty.

FAZA 2: RAPORTOWANIE OBOWIĄZKOWE (zegar tyka!)

→ **Do 24 godzin – wczesne ostrzeżenie**
Gdzie: Właściwy CSIRT (np. CSIRT NASK).
Co: Zgłoszenie podejrzenia ataku. Kiedy atak wystąpił i został wykryty, jak długo trwał? Czy jest celowy? Czy może mieć skutki dla innych krajów?

→ **Do 72 godzin – zgłoszenie incydentu**
Co: Wstępna ocena dotkliwości, przyczyn i skutków. Wskaźniki kompromitacji (IoC). Jak przebiegał incydent i jaki jest jego zakres – jak wpływa na usługi świadczone przez Ciebie i inne podmioty, ilu osób dotyczy, jaki zasięg geograficzny obejmuje? Jakie działania zapobie-

gawcze i naprawcze są podejmowane?

→ **Do 1 miesiąca – raport końcowy**
Co: Szczegółowy opis incydentu, zakłóceń i szkód, które spowodował. Przyczyna źródłowa (root cause). Zastosowane środki naprawcze. Skutki transgraniczne – jeśli wystąpiły.

FAZA 3: ODZYSKIWANIE

1. Oczyść systemy ze złośliwego oprogramowania.
2. Zmień wszystkie hasła administracyjne.
3. Przywróć dane z czystej kopii zapasowej (zgodnie z planem DRP).
4. Monitoruj sieć pod kątem powtórnego ataku.

Dodatek E. Weryfikacja dostawcy (vendor check)

Cel: Ocena bezpieczeństwa dostawcy usług IT przed zawarciem umowy.

PRZED WSPÓŁPRACĄ

- ☐ Czy dostawca posiada certyfikaty bezpieczeństwa ISO 27001, SOC 2?
- ☐ Czy dostawca udokumentował wdrożenie własnej analizy ryzyka?
- ☐ Czy dostawca gwarantuje, że dane są przechowywane na terenie EOG (Europejskiego Obszaru Gospodarczego)?

ZAPISY W UMOWIE

- ☐ **Prawo do audytu:** Czy mamy prawo sprawdzić bezpieczeństwo dostawcy (osobiście lub przez audytora)?
- ☐ **Incydenty:** Czy dostawca zobowiązuje się zgłosić nam incydent bezpieczeństwa w określonym czasie (np. w ciągu 24 godzin)?
- ☐ **SLA:** Czy określono gwarantowany czas dostępności usługi i czas naprawy awarii?
- ☐ **Podwykonawcy:** Czy dostawca musi uzyskać naszą zgodę na zmianę kluczowych podwykonawców?
- ☐ **Kary umowne:** Czy przewidziano kary za naruszenie zasad bezpieczeństwa lub wyciek danych?
- ☐ **Exit plan:** Czy określono, w jaki sposób odzyskamy nasze dane po zakończeniu umowy?

ODO 24 – Kompleksowo zarządzamy bezpieczeństwem danych i ryzykiem

Wdrożenie wymogów nowelizacji UKSC to proces, który wymaga połączenia wiedzy prawnej, technologicznej i organizacyjnej. Nie musisz przechodzić przez to samodzielnie.

Jesteśmy liderem na rynku ochrony danych i bezpieczeństwa informacji. Od lat wspieramy polskie firmy w budowaniu odporności biznesowej.

Jak możemy Ci pomóc?

- ☑ Audyt zgodności z NIS2 / UKSC– sprawdzimy, co już masz, a czego Ci brakuje.
- ☑ Analiza ryzyka – przeprowadzimy profesjonalny proces identyfikacji i oceny zagrożeń.
- ☑ Dokumentacja – przygotujemy szyte na miarę polityki, procedury i plany BCP/DRP.
- ☑ Szkolenia – przeszkolimy zarząd, kadrę IT oraz wszystkich pracowników (szkolenia stacjonarne i e-learning).
- ☑ Wsparcie bieżące – przejmiemy funkcję IOD lub doradcy ds. cyberbezpieczeństwa.

Masz pytania? Skontaktuj się z nami.

Zapraszamy do skorzystania z bezpłatnych poradników i kalkulatorów ryzyka dostępnych na stronie ODO24.pl.

Co dalej?

Wdrożenie NIS2

Jeśli potrzebują Państwo wsparcia w tym procesie, chętnie służymy pomocą. Dysponujemy odpowiednimi kompetencjami i zasobami, aby Państwa w tym wesprzeć. Zapraszamy do zapoznania się z naszą ofertą.

Marcin Kuźniak
tel. +48 690 957 665

Cezary Lutyński
tel. +48 690 957 609

ODO 24 sp. z o.o.
22 740 99 96
oferty@odo24.pl
ul. Kamionkowska 45
03-812 Warszawa
KRS: 0000434350