3.6.2025

Esencja z webinaru

NIS2 – 5 elementów, które zdecydują o sukcesie wdrożenia.

Dziękuję za udział w webinarze

Jeśli uważasz, że przekazałem wiedzę w sposób rzetelny
to dodaj proszę swoją opinię na wizytówce ODO 24 w Google.

Z góry dziękuję 😊

Jeśli potrzebujesz dodatkowego wsparcia merytorycznego – zachęcam do skorzystania z bezpłatnych porad prawnych i IT.

Tomasz Ochocki
Koordynator Zespołu Merytorycznego

Linki do źródeł wiedzy, inspiracji i nie tylko

Linki
NIS2 – 5 elementów, które zdecydują o sukcesie wdrożenia • Zobacz nagranie webinaru. • Zobacz prezentację z webinaru.
Polecamy • Jak wdrażać NIS2 - ciągłość działania • Jak wdrażać NIS2 - łańcuch dostaw • Jak wdrażać NIS2 - polityka bezpieczeństwa informacji • Jak wdrażać NIS2 - zarządzanie incydentami • Jak wdrażać NIS2 - zarządzanie ryzykiem • NASK: Dyrektywa NIS2
W czym możemy pomóc • Wdrożenie NIS2 – nowe wymogi dla cyberbezpieczeństwa. • Zarządzanie zgodnością z AI **(nowość)** • Analiza ryzyka i DPIA – zgodnie z RODO
Bezpłatne konsultacje • Porozmawiaj z naszymi doradcami  Marcin Kuźniak umów spotkanie  Cezary Lutyński umów spotkanie

Pytania i odpowiedzi

Szanowni Państwo,
dziękuję za udział w webinarium i przesyłam odpowiedzi na zadane za pomocą czatu pytania. Jednocześnie uczulam, że odpowiedzi tych nie należy traktować jako „prawdy objawionej", gdyż – z uwagi na formę zadawania pytań – są to raczej wskazówki, sformułowane w oparciu o skromne informacje na temat stanu faktycznego.

W jakich organizacjach wymagane jest stosowanie przepisów dyrektywy NIS2?

Kwestia, w jakich konkretnie organizacjach stosowanie przepisów dyrektywy NIS2 będzie wymagane w Polsce, zostanie ostatecznie rozstrzygnięta w ustawie o krajowym systemie cyberbezpieczeństwa (KSC), której projekt jest obecnie w trakcie prac legislacyjnych. Poniższe informacje opierają się wyłącznie na założeniach wynikających bezpośrednio z dyrektywy NIS2 (UE) 2022/2555 i mogą ulec doprecyzowaniu na poziomie krajowym.

Zgodnie z dyrektywą NIS2, obowiązki w zakresie cyberbezpieczeństwa będą miały zastosowanie do:

- Podmiotów kluczowych (essential entities), czyli m.in.:
  - dostawców usług energetycznych (elektroenergetyka, gazownictwo, ciepłownictwo),
  - podmiotów z sektora transportu (kolej, lotnictwo, żegluga, drogowy),
  - dostawców usług zdrowotnych (w tym szpitale, laboratoria, dostawcy e-zdrowia),
  - dostawców usług wodnych (zaopatrzenie w wodę i oczyszczanie ścieków),
  - dostawców usług cyfrowych (np. DNS, rejestry domen, chmura),
  - administracji publicznej (wybrane podmioty administracji centralnej i samorządowej).
- Podmiotów ważnych (important entities), czyli m.in.:
  - dostawców usług pocztowych i kurierskich,
  - producentów urządzeń elektronicznych, komputerowych, optycznych, medycznych,
  - podmiotów z sektora żywności i chemikaliów,
  - usług doradczych i badawczych istotnych dla infrastruktury krytycznej,
  - dostawców niektórych usług ICT na rzecz podmiotów kluczowych.

  Zasadniczo dyrektywa stosuje się do organizacji zatrudniających powyżej 50 pracowników lub osiągających roczny obrót/przychód powyżej 10 mln euro. Wyjątkiem są organizacje działające w sektorach szczególnie wrażliwych – w ich przypadku obowiązki mogą mieć zastosowanie niezależnie od wielkości.

Jaką rolę odgrywa IOD w procesie wdrażania dyrektywy NIS 2 w organizacji?

Rola Inspektora Ochrony Danych (IOD) w procesie wdrażania dyrektywy NIS 2 w organizacji rodzi zasadne pytania — zwłaszcza w kontekście ryzyka konfliktu interesów.

Zgodnie z art. 38 ust. 6 RODO, IOD może wykonywać inne zadania i obowiązki, ale tylko pod warunkiem, że nie prowadzą one do konfliktu interesów. W praktyce oznacza to, że IOD nie powinien pełnić funkcji związanych z określaniem celów i sposobów przetwarzania danych osobowych, ponieważ osłabia to jego niezależność i obiektywizm.

Dyrektywa NIS 2 nakłada na organizacje liczne obowiązki w zakresie cyberbezpieczeństwa, m.in. przeprowadzanie ocen ryzyka, wdrażanie środków technicznych i organizacyjnych czy zgłaszanie incydentów. Jeśli jednak IOD zostanie zaangażowany w te procesy w sposób decyzyjny, pojawia się problem: w praktyce oceni działania, które sam wcześniej zaplanował lub wdrożył. To klasyczny przykład konfliktu interesów.

Potwierdzają to także decyzje Prezesa UODO, w których jasno wskazano, że powierzanie IOD zadań mogących prowadzić do konfliktu interesów stanowi naruszenie przepisów RODO (np. tutaj). IOD nie może bowiem jednocześnie projektować rozwiązań (np. w zakresie cyberbezpieczeństwa) i być ich późniejszym kontrolerem. Taka podwójna rola podważa jego bezstronność i naraża organizację na ryzyko zarzutu naruszenia przepisów.

Dlatego angażowanie IOD w projekt NIS 2 powinno ograniczać się do roli doradczej i nadzorczej — bez powierzania mu zadań decyzyjnych czy wykonawczych w zakresie cyberbezpieczeństwa. Tylko w ten sposób organizacja może zapewnić jego niezależność, a jednocześnie uniknąć potencjalnych konfliktów interesów.

Czy w organizacji powinno się wyznaczyć dedykowany zespół lub osobę odpowiedzialną za wdrożenie i późniejsze utrzymanie rozwiązania — na wzór roli pełnionej przez IOD w obszarze ochrony danych?

Z perspektywy zarządczej wyznaczenie dedykowanego zespołu lub osoby odpowiedzialnej za wdrożenie oraz późniejsze funkcjonowanie rozwiązania, na wzór roli IOD, jest zdecydowanie zalecane. Przede wszystkim pozwala to jasno przypisać odpowiedzialność za koordynację działań, podejmowanie decyzji operacyjnych oraz raportowanie postępów, co jest kluczowe dla skutecznego zarządzania projektem. Dedykowana rola zapewnia spójność działań między działami, dzięki czemu organizacja unika chaosu i dublowania prac. Ważne jest także, aby ktoś nie tylko wdrożył rozwiązanie, ale prowadził jego stały nadzór, oceniał skuteczność i monitorował zgodność z przyjętymi standardami. Taki układ pozwala zarządowi lepiej kontrolować ryzyka, weryfikować realizację celów oraz szybko reagować na potencjalne problemy. Formalne przypisanie tej odpowiedzialności wzmacnia też kulturę organizacyjną, pokazując, że organizacja poważnie traktuje temat i inwestuje nie tylko w spełnianie wymogów formalnych, ale przede wszystkim w realne podniesienie poziomu bezpieczeństwa i zgodności.

Czy inspektor ochrony danych (IOD) może pełnić funkcję pełnomocnika zarządu (ds. NIS2)?

Inspektor ochrony danych (IOD) teoretycznie może pełnić funkcję pełnomocnika Zarządu, ale należy wziąć pod uwagę kilka kluczowych kwestii. Przede wszystkim, zgodnie z wymogami RODO, IOD powinien być niezależny i nie może podejmować działań, które mogłyby prowadzić do konfliktu interesów. Funkcja pełnomocnika Zarządu, zwłaszcza w obszarze wdrożenia i utrzymania przepisów, może wiązać się z podejmowaniem decyzji dotyczących zarządzania ryzykiem lub wdrażania środków technicznych i organizacyjnych, co może kolidować z rolą nadzorczą IOD.

Jeśli jednak zakres obowiązków pełnomocnika Zarządu nie będzie naruszał zasad niezależności, teoretycznie jest to możliwe. W praktyce jednak, ze względu na uniknięcie konfliktów interesów, zaleca się rozdzielenie tych ról.

Czy istnieją obecnie wytyczne, szablony lub matryce, które mogą wspierać analizę ryzyka w kontekście wdrażania dyrektywy NIS 2? Podczas webinaru sprzed kilku miesięcy wspominali Państwo o możliwości połączenia analizy ryzyka RODO i NIS 2 w ramach jednego narzędzia. Czy ta opcja nadal pozostaje aktualna i rekomendowana?

Tak, istnieją wytyczne wspierające analizę ryzyka w kontekście wdrażania dyrektywy NIS 2. Przykładem jest dokument ENISA pt. „Implementing Guidance on Commission Implementing Regulation (EU) 2024/2690” (październik 2024), który zawiera praktyczne wskazówki, przykłady dowodów, mapowanie do standardów międzynarodowych (m.in. ISO, NIST) oraz odniesienia do krajowych ram zarządzania ryzykiem cyberbezpieczeństwa. Dodatkowo, treść Rozporządzenia Komisji Europejskiej z 17 października 2024 r. (C(2024) 7151) również określa techniczne i metodyczne wymagania dotyczące analizy ryzyka zgodnej z NIS 2.

W praktyce dokumenty te odwołują się do normy ISO/IEC 27005, którą my przyjmujemy jako punkt wyjścia do opracowywania analiz ryzyka na gruncie RODO. Ta norma daje solidną metodologiczną podstawę, która pozwala skutecznie zintegrować analizę ryzyka zarówno pod kątem ochrony danych osobowych, jak i cyberbezpieczeństwa.

Tak, rekomendujemy naszym klientom integrowanie analiz ryzyk wynikających z NIS 2 i RODO w jednym spójnym narzędziu. Pozwala to na efektywniejsze zarządzanie ryzykiem, unikanie dublowania prac i zapewnienie zgodności z oboma reżimami prawnymi, przy jednoczesnym optymalnym wykorzystaniu zasobów organizacji.

Dodatkowo, już teraz przygotowujemy szkolenie dedykowane wdrażaniu NIS 2. Serdecznie zapraszamy do udziału, gdy tylko pojawi się ono w naszej ofercie 😊

Czy funkcję pełnomocnika zarządu ds. NIS2 może pełnić osoba z działu IT?

Tak, funkcję pełnomocnika zarządu ds. NIS2 może pełnić osoba z działu IT, pod warunkiem że posiada odpowiednie kompetencje, wiedzę oraz umocowanie formalne do realizacji tej roli.

Z perspektywy zarządczej kluczowe jest, aby pełnomocnik był w stanie skutecznie koordynować wdrożenie wymogów NIS2, rozumiał zarówno aspekty techniczne, jak i organizacyjne oraz potrafił komunikować się z zarządem i innymi działami. Informatyk może mieć dużą przewagę dzięki znajomości systemów i technologii, ale ważne jest, aby dodatkowo rozumiał wymogi prawne, zarządcze oraz związane z zarządzaniem ryzykiem.

Rekomendujemy również, aby organizacja upewniła się, że pełnomocnik nie wchodzi w konflikt interesów, np. jeśli w swojej codziennej roli podejmuje decyzje operacyjne, które później sam musiałby nadzorować lub oceniać w kontekście zgodności z NIS2.

Bardzo proszę o wskazanie, w jaki sposób można uwzględnić wszystkie istotne zagrożenia, aby analiza ryzyka była możliwie pełna i kompleksowa.

Nie ma możliwości przewidzenia wszystkich możliwych zagrożeń, ponieważ ryzyko z definicji dotyczy także zdarzeń nieprzewidywalnych lub o niskim prawdopodobieństwie, które trudno zidentyfikować zawczasu. Jednak dobra analiza ryzyka powinna być możliwie wyczerpująca i systematyczna — to znaczy, że:

- Opiera się na uznanych standardach — np. ISO/IEC 27005, które wskazuje, jak prowadzić identyfikację zagrożeń, biorąc pod uwagę kontekst organizacji, jej zasoby, systemy, procesy i otoczenie.
- Uwzględnia różne źródła zagrożeń — techniczne, organizacyjne, ludzkie, prawne, środowiskowe, zewnętrzne (np. dostawcy, partnerzy) i wewnętrzne (np. pracownicy, systemy).
- Korzysta z dostępnych danych — takich jak rejestry incydentów, raporty audytowe, dane branżowe, analizy trendów zagrożeń, raporty CERT, publikacje ENISA, krajowe raporty o stanie cyberbezpieczeństwa.
- Jest regularnie aktualizowana — analiza ryzyka nie jest „jednorazowym" ćwiczeniem, ale procesem cyklicznym, który wymaga weryfikacji w miarę zmian w organizacji, otoczeniu prawnym i technologicznym oraz pojawienia się nowych typów zagrożeń.
- Używa podejścia „all hazards" — czyli patrzy szeroko, nie tylko na cyberataki, ale też np. na ryzyko przerw w dostawie energii, awarii sprzętu, błędów ludzkich czy zdarzeń losowych.
- Zawiera fazę konsultacji eksperckich — często najlepsze identyfikacje zagrożeń powstają we współpracy zespołów wielobranżowych: IT, prawników, compliance, operacji, a nie wyłącznie w działach technicznych.

Jak skutecznie poradzić sobie z tym wyzwaniem, gdy zarząd deklaruje brak czasu na zaangażowanie?

Jeśli zarząd „nie ma czasu", warto od razu powiedzieć jasno: NIS2 nie przewiduje dla zarządu taryfy ulgowej. Członkowie zarządu ponoszą osobistą odpowiedzialność za nadzorowanie wdrożenia środków bezpieczeństwa, a dodatkowo dyrektywa przewiduje dla nich obowiązkowe szkolenia z zakresu cyberbezpieczeństwa.

Co zrobić praktycznie? Po pierwsze — zorganizować krótkie, konkretne szkolenie dla zarządu, np. w formule 30-45 minutowej, nastawionej na świadomość obowiązków i ryzyk. Po drugie — wyznaczyć pełnomocnika ds. NIS2, który zajmie się codziennym koordynowaniem działań, a zarząd będzie angażował się tylko przy kluczowych decyzjach. Po trzecie — dostarczać zarządowi krótkie, rzeczowe raporty: nie oczekujmy, że będą śledzić wszystkie szczegóły, ale muszą wiedzieć, co zatwierdzają i jakie ryzyka akceptują.

Wartość ODO 24 tkwi w merytoryce zespołu ekspertów

Ochrona danych osobowych

Bezpieczeństwo informacji

Szkolenia RODO

Sprawdź nas

Tomasz Ochocki
Koordynator
zespołu merytorycznego

ZAPYTAJ O OFERTĘ