trecom | cisco Partner

Jak skutecznie przygotować organizację **na NIS 2 i UoKSC?**

E-book autorstwa

Tomasza Matuły

Spis treści:

Disclaimer

Niniejszy dokument zawiera porady oraz rekomendacje wynikające z doświadczenia autora oraz dostępnych publicznie informacji. Zastosowanie w organizacji wskazań oraz strategii zawartych w niniejszym dokumencie powinno być w stosownych przypadkach skonsultowane ze specjalistami. Ani autor ani wydawca nie ponoszą odpowiedzialności za jakiekolwiek straty czy szkody wynikające z nieodpowiedniego wdrożenia zawartych w dokumencie rekomendacji. Informacje zaprezentowane w poniższym e-booku zostały przygotowane zgodnie ze stanem wiedzy dostępnym na dzień 22.08.2025 r.

Wytyczne związane z NIS 2 mogą ulec zmianie i/oraz doprecyzowaniu po faktycznej transpozycji dyrektywy NIS 2 do prawa krajowego t.j. aktualizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa (UoKSC).

1. Wstęp

Kilka słów od autora

18 października 2024 roku weszła w życie Dyrektywa NIS 2 (dyrektywa w sprawie środków na rzecz wysokiego, wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej) w całości zastępując obowiązującą dyrektywę NIS z 2016 roku. W Polsce NIS 2 do porządku prawnego wprowadzi nowelizacja Ustawy o Krajowym Systemie Cyberbezpieczeństwa. Prace nad nią wydłużyły się, ale wydaje się na dzień dzisiejszy (sierpień 2025), że dobiegają końca, a nowelizacja ustawy o KSC zostanie ostatecznie przyjęta na przełomie 2025 i 2026 roku.

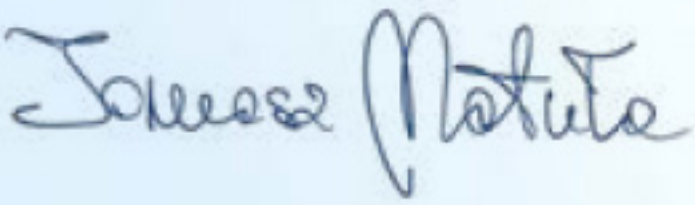
Z rozmów, warsztatów oraz szkoleń, które przeprowadziłem w ciągu ostatnich 12 miesięcy z wieloma CTIO, CISO i członkami Zarządów z ponad 50 różnych organizacji wiem, że duża część z nich wciąż posiada ograniczoną świadomość jak znaczące zmiany dla nich oraz ich organizacji wprowadza NIS 2 i nowelizacja UoKSC. **Część organizacji czeka z rozpoczęciem prac dostosowawczych do formalnego uchwalenia nowej UoKSC. Biorąc pod uwagę ilość i wagę zmian oraz obowiązków nakładanych na firmy i organizacje uważam, że to błąd.**

Warto przygotować się na nadchodzące zmiany wykonując już teraz ocenę aktualnego poziomu dojrzałości swojej organizacji w obszarze cyberbezpieczeństwa i na tej podstawie zaplanować co musimy zrobić, by w ciągu najbliższych kilkunastu miesięcy przygotować się do spełnienia wymagań NIS 2 i nowelizacji UoKSC. Wydaje się, że wiele firm i organizacji ma dużo lub bardzo dużo do zrobienia w najbliższym czasie...

Dyrektywa NIS 2 i znowelizowana UoKSC są w moim przekonaniu szansą na wzmocnienie cyberbezpieczeństwa naszych firm, organizacji i wszystkich obywateli. Są jednocześnie szansą dla osób odpowiedzialnych za cyberbezpieczeńswo (CISO, CSO, CIO, w których odpowiedzialności jest cybersecurity) na wzmocnienie pozycji security oraz zwiększenie "atencji" ze strony Zarządzających czy Zarządów swoich organizacji (a jest to często poważnym wyzwaniem).

Celem niniejszego opracowania jest przedstawienie "w pigułce" czym jest dyrektywa NIS 2, kogo obejmuje, jakie obowiązki nakłada na organizacje oraz jak się przygotować na dostosowanie się do jej wymagań.

Miłej lektury,



2. W skrócie - najważniejsze informacje o NIS 2

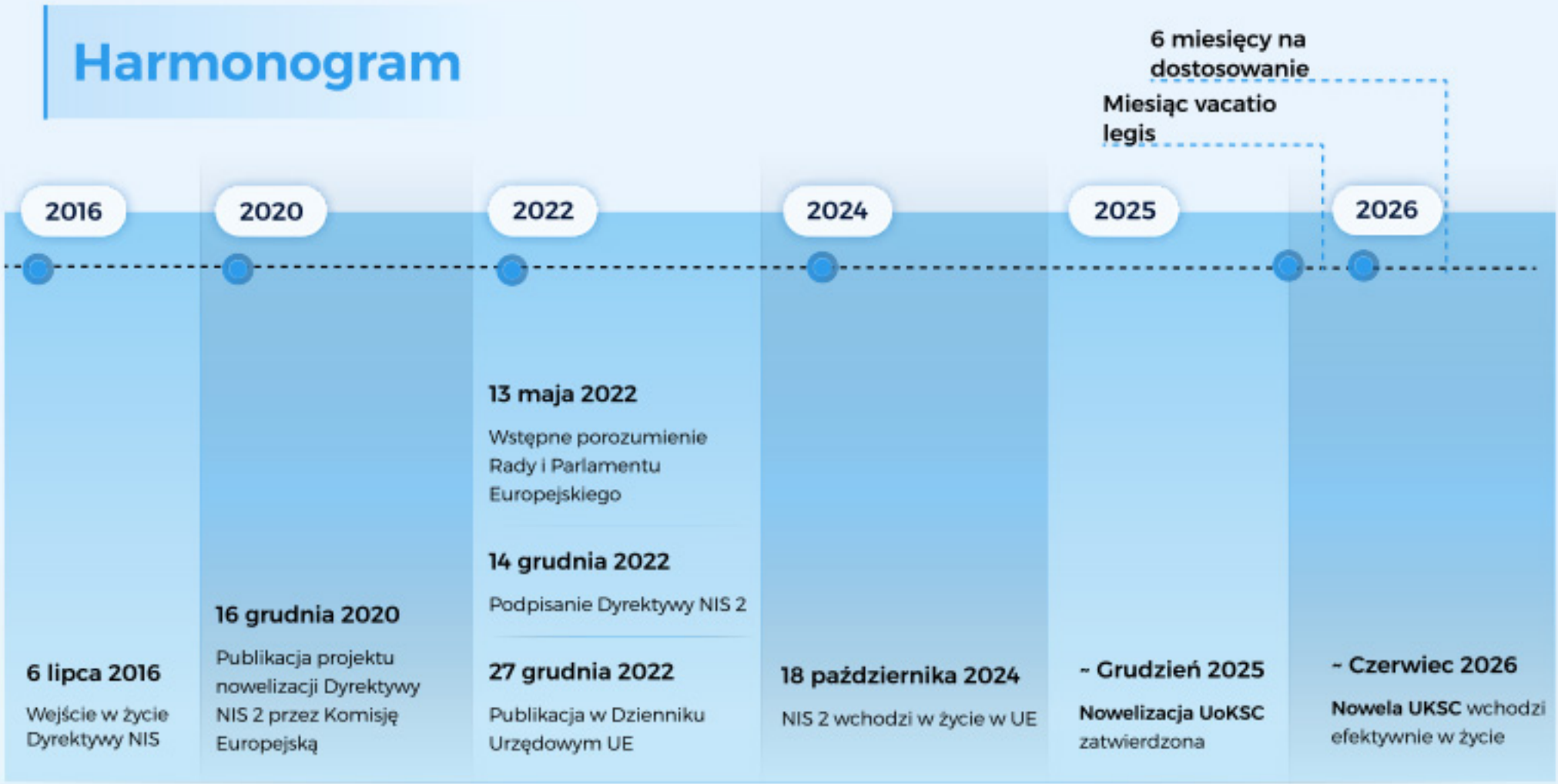
Cel

Dyrektywę NIS 2 wdrożono dla:

1. **Zwiększenia ochrony i odporności przed cyberzagrożeniami** firm oraz organizacji w UE, a także nas – obywateli.

2. **Zwiększenia umiejętności reagowania na kryzysy** związane z cyberbezpieczeństwem oraz odbudowy po nich.

Harmonogram



Sektory i podmioty

Dyrektywa NIS 2 znacząco rozszerza zakres obejmowanych nią sektorów i podmiotów. Dotyczy zarówno komercyjnych firm, jak i organizacji typu administracja publiczna czy służba zdrowia. Do NIS 2 dostosować się będą musiały podmioty:

1. o odpowiedniej wielkości - czyli mające minimum 50 pracowników i roczny obrót powyżej 10 mln euro
2. organizacje operujące w określonych sektorach uznanych jako istotne dla UE, m.in.
   - z sektorów istotnych dla gospodarki i społeczeństwa np.: energetyka, transport, ochrona zdrowia
   - z sektorów cyfrowych np. dostawcy usług społecznościowych, usług pocztowych
   - świadczące usługi transgraniczne np. dostawcy usług chmurowych i usługi centrów danych

3. Powody i cel wdrożenia NIS 2, korzyści

Dlaczego wdrożono dyrektywę NIS 2?

Temat cyberbezpieczeństwa był zawsze ważny dla Unii Europejskiej. Żeby zwiększyć poziom bezpieczeństwa w krajach UE wprowadzono w 2016 r. dyrektywę NIS.

Kontrole i audyty funkcjonowania NIS z 2016 r. przyniosły dwa kluczowe wnioski.

Po pierwsze: państwa członkowskie wdrażały przepisy unijne w zakresie bezpieczeństwa w różnym zakresie. Nie zawsze były one wzajemnie spójne, a krajowa egzekucja przepisów dotyczących cyberbezpieczeństwa często nie była na zadowalającym poziomie.

Po drugie: świat otaczający nas jako obywateli, organizacje i firmy od 2016 r. bardzo się zmienił:

1. W zakresie cyfryzacji naszego życia mamy do czynienia z rewolucją - lawinowy wzrost wykorzystania cyfrowych usług powszechnych np. bankowość, usługi typu e-government, e-commerce.
2. Postępująca konwergencja obszarów automatyki przemysłowej, Internetu Rzeczy i Przemysłowego Internetu Rzeczy z rozwiązaniami IT.
3. Transformacje do rozwiązań Przemysł 4.0, sieci nowej generacji 5G, czy transformacja do sieci definiowanych programowo itp.
4. Postępujące odmiejscowienie pracy, upowszechnienie pracy zdalnej i hybrydowej, ale też usług transgranicznych w UE.
5. Masowe upowszechnienie rozwiązań i usług chmurowych czy Software as a Service.

Po trzecie: zmieniający się świat przyniósł skokowy wzrost ilości cyberzagrożeń, zagrażających nie tylko nam jako obywatelom, firmom, ale i stabilności całych regionów, ciągłości działania usług czy infrastruktury krytycznej z punktu widzenia kraju. Agresywni cyberprzestępcy działający w celu wzbogacenia czy na zlecenie wrogich państw to od dłuższego czasu przykra rzeczywistość.

W 2024 r. do polskich CERT-ów trafiło 600 990 zgłoszeń.

Z czego 103 449 zostały zakwalifikowane jako incydenty bezpieczeństwa. To wzrost o 29% w skali roku! Według Microsoft Digital Defense Report - Polska zajmuje 3. miejsce w Europie (po Ukrainie i Wielkiej Brytanii) i 9. na świecie pod względem narażenia na ataki ze strony organizacji cyberprzestępczych sponsorowanych przez obce państwa (głównie Rosję).

> **Treść tego rozdziału dostępna jest również w formie nagrania. Kilknij tutaj aby obejrzeć.**

Jaki jest cel dyrektywy NIS 2?

Głównym celem dyrektywy NIS 2 jest **ustanowienie minimalnych wymagań,** które państwa członkowskie Unii Europejskiej powinny wdrożyć, aby skutecznie ograniczyć ryzyko incydentów cyberbezpieczeństwa oraz zwiększyć bezpieczeństwo obywateli, firm i organizacji. Innymi słowy, skorzystają na tym wszyscy obywatele, ponieważ nasze otoczenie cyfrowe stanie się po prostu bezpieczniejsze. Korzyści odczują także firmy, zwłaszcza te świadczące usługi transgraniczne, które dotychczas musiały zmagać się z różnicami w przepisach dotyczących cyberbezpieczeństwa w poszczególnych krajach.

Jakie korzyści przyniesie skuteczne wdrożenie dyrektywy NIS 2?

Konkretne korzyści ze stosowania się do zaleceń dyrektywy NIS 2 to m.in.:

1. Zwiększenie **ochrony i odporności na cyberzagrożenia.**

2. Zwiększenie zdolności, **umiejętności do reagowania na incydenty i kryzysy cyberbezpieczeństwa oraz odbudowy po nich** - bardzo ważne, ponieważ trzeba mieć świadomość, że poważne incydenty i kryzysy cyber będą miały miejsce, a kluczem jest umiejętność szybkiego, skutecznego zareagowania oraz minimalizacja ich skutków.

3. Zwiększenie **bezpieczeństwa i ochrony danych osobowych** w cyberprzestrzeni.

4. Wzrost **zaufania do cyfrowego rynku UE** i konkurencyjności europejskich podmiotów cyfrowych na arenie globalnej.

4. Kogo obejmie dyrektywa NIS 2?

Dyrektywa NIS 2 obejmuje znacznie więcej sektorów i podmiotów niż NIS. Co ważne, NIS 2 dotyczy zarówno komercyjnych firm, jak i organizacji typu administracja publiczna czy służba zdrowia.

Odpowiadając krótko na pytanie, dostosować się do NIS 2 będą musiały:

- organizacje operujące w określonych sektorach uznanych jako istotne dla UE oraz
- organizacje o odpowiedniej wielkości (size cap rule).

Jakie sektory zostały uznane jako istotne z punktu widzenia UE i Państwa?

1. **Świadczące usługi transgraniczne** np. dostawcy usług DNS, podmioty świadczące usługi rejestracji nazw domen, dostawcy usług chmurowych, przetwarzania na brzegu sieci i usługi centrów danych.
2. **Z sektorów istotnych dla gospodarki i społeczeństwa** np.: energetyka, transport, infrastruktura rynku finansowego, ochrona zdrowia, dostarczanie wody pitnej, zarządzanie odpadami, produkcja chemiczna i jądrowa.
3. **Z sektorów cyfrowych** np. dostawcy usług społecznościowych, usług udostępniania danych czy treści, usług wyszukiwania internetowego i usług pocztowych.

Sektor finansowy, czyli m.in. bankowość i ubezpieczenia nie podlega pod NIS 2, ale tylko dlatego, że pokrywa go siostrzana regulacja DORA jako „lex specialis".

Size Cap Rule

Wielkość organizacji objętych NIS 2 jest precyzyjnie określona. Dyrektywą objęte są wszystkie organizacje, które przekroczą pułap dla średnich przedsiębiorstw (size cap rule).

> 50 pracowników i roczny obrót > 10 mln EUR

NIS 2 co do zasady nie dotyczy małych organizacji, czyli tych poniżej 50 pracowników i 10 mln euro rocznego przychodu.

Wyjątki od size cap rule (organizacje objęte NIS 2 bez względu na wielkość): dostawcy usług zaufania, jednostki administracji publicznej, jedyny dostawca usługi w kraju, dostawy usług zarządzanych w zakresie cyberbezpieczństwa.

Czy do size cap rule liczą się tylko osoby zatrudnione na UoP?

Do liczby zatrudnionych należy wliczać również osoby współpracujące na podstawie umów innych niż umowa o pracę (np. umowa zlecenie, umowa o dzieło, kontrakt B2B) — pod warunkiem, że można je uznać za pracowników.

Ma to miejsce w szczególności wtedy, gdy osoby te:

- świadczą pracę wyłącznie na rzecz jednego podmiotu,
- wykonują ją pod nadzorem,
- pracują w miejscu i czasie wskazanym przez zlecającego lub zamawiającego usługę.

Do liczby zatrudnionych **nie należy** wliczać osób zatrudnionych przez agencję pośrednictwa pracy.

Co w przypadku firm międzynarodowych?

W przypadku firm międzynarodowych do size cap rule będzie wliczała się liczba pracowników wykonujących obowiązki zawodowe na terenie Polski.

Podmioty kluczowe i ważne

Biorąc pod uwagę dwa kryteria, czyli wielkość i istotność, podzielono podmioty podlegające pod NIS 2 na **kluczowe i ważne.**

Według treści dyrektywy NIS 2 wszystkie podmioty publiczne to podmioty kluczowe. Polski ustawodawca w projekcie nowelizacji UoKSC wprowadził jednak podział na dwie kategorie: **podmioty publiczne kluczowe i ważne.** Podział wynika ze zgłoszonych w konsultacjach społecznych uwag. Dla małych podmiotów publicznych, np. domy kultury, biblioteki, muzea, szkoły czy przedszkola spełnienie wymogów narzucanych na podmioty kluczowe byłoby niemożliwe w praktyce.

Podmioty kluczowe

> 250 pracowników i roczny obrót > 50 mln EUR i następujące sektory (sektory kluczowe):

- **Energia**
  - Wydobywanie kopalin
  - Energia elektryczna
  - Centralne ogrzewanie i chłodzenie
  - Ropa i paliwa
  - Gaz, wodór, jądrowa
- **Ochrona zdrowia**
  - Świadczenia i zdrowie publiczne
  - Produkcja i dystrybucja
- **Infrastruktura cyfrowa**
  - Data Center
  - Usługi łączności elektronicznej
  - Dostawcy usług chmurowych
  - Dostawcy usług DNS
- **Transport**
  - Lotniczy
  - Kolejowy
  - Wodny
  - Drogowy
- **Woda pitna - zaopatrzenie i dystrybucja**
- **Zbiorowe odprowadzanie ścieków**
- **Administracja publiczna***
- **Przestrzeń kosmiczna**
- **Zarządzanie usługami ICT**
  - Dostawcy Usług Zarządzanych
  - Dostawcy Usług Zarządzanych w zakresie bezpieczeństwa

*Administracja publiczna z wyłączeniem podmiotów publicznych ważnych.

Jeśli firma nie spełnia warunku wielkości, ale działa w wyżej wymienionym sektorze to zostanie objęta NIS 2 jako podmiot ważny.

Podmioty kluczowe - przykłady

Przykład 1: Firma ACME działa w energetyce (sektor wyszczególniony jako kluczowy), zatrudnia 100 pracowników oraz generuje obrót roczny 30 mln euro nie będzie podmiotem kluczowym (nie spełnia warunku wielkości). Firma ta zostanie objęta NIS 2, ale jako podmiot ważny.

Przykład 2: Firma HealX działa w sektorze opieki zdrowotnej (sektor wyróżniony jako kluczowy), zatrudnia 300 pracowników oraz generuje obrót roczny 25 mln EUR (spełnia tylko jeden z wymienionych warunków wielkości = nie spełnia warunków wielkości). Firma ta zostanie objęta NIS 2, ale jako podmiot ważny.

Podmioty ważne

> 50 pracowników i roczny obrót > 10 mln EUR i następujące sektory (sektory ważne):

- **Usługi pocztowe i kurierskie**
- **Badania naukowe**
- **Gospodarowanie odpadami**
  - Zbieranie odpadów
  - Transport odpadów
  - Przetwarzanie odpadów
  - Sprzedaż lub pośrednictwo
- **Dostawcy usług cyfrowych**
  - Wyszukiwarki sieciowe
  - Platformy e-commerce
  - Platformy sieci społecznościowych
- **Administracja publiczna**
  - Samorządowe jednostki budżetowe
  - Samorządowe zakłady budżetowe
  - Samorządowe instytucje kultury
  - Spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej (w rozumieniu ustawy o gospodarce komunalnej) przy wykorzystaniu systemów informacyjnych
- **Produkcja**
  - Produkcja, wytwarzanie i dystrybucja chemikaliów
  - Produkcja, wytwarzanie i dystrybucja żywności
  - Wyroby medyczne
  - Wyroby medyczne do diagnostyki in vitro
  - Produkty komputerowe
  - Produkty elektroniczne i optyczne
  - Sprzęt elektroniczny
  - Maszyny i urządzenia
  - Pojazdy samochodowe, przyczepy i naczepy

Jeśli firma nie spełnia warunku wielkości, ale działa w wyżej wymienionym sektorze to nie zostanie objęta NIS 2.

Podmioty ważne - przykłady

Przykład 3: Firma Barone Sanitation działa w sektorze gospodarowania odpadami (sektor wymieniony jako ważny), zatrudnia 40 pracowników i generuje obrót roczny 8 mln EUR (nie spełnia warunku wielkości). Firma ta nie zostanie objęta dyrektywą NIS 2.

Przykład 4: Firma Komputerki działa w sektorze produkcji produktów komputerowych (sektor wymieniony jako ważny), zatrudnia 52 pracowników i generuje obrót roczny 8 mln EUR (spełnia tylko jeden z wymienionych warunków wielkości = nie spełnia warunków wielkości). Firma ta nie zostanie objęta dyrektywą NIS 2.

UWAGA NA WYJĄTKI!

Nawet małe lub mikroprzedsiębiorstwa muszą spełniać obowiązki wynikające z NIS 2, jeśli mają kluczową rolę dla społeczeństwa, gospodarki lub konkretnych sektorów. Mogą to być np.:

- dostawcy usług zaufania
- podmiot będący jednostką administracji publicznej lub podmiot będący jedynym dostawcą usługi w kraju

- dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa zostaną uznani jako Podmioty Kluczowe jeśli co najmniej spełniają wymogi dla małego przedsiębiorcy: >10 pracowników i roczny obrót >2mln euro

Szczegółowa lista wyjątków najprawdopodobniej zostanie zawarta w treści nowelizacji UoKSC.

UWAGA NA ŁAŃCUCH DOSTAW!

W NIS 2 uwzględniono bezpieczeństwo łańcucha dostaw.

- Firmy i organizacje będą musiały wskazać wszystkie podmioty zaangażowane w dostarczanie produktów lub usług związanych z cyberprzestrzenią, takich jak producenci, dostawcy, dystrybutorzy, integratorzy itp.
- Dla wszystkich swoich bezpośrednich dostawców firmy i organizacje muszą przeprowadzać Risk Assessment i monitorować bezpieczeństwo współpracy z nimi.

To wywoła efekt „domina" - firma nieobjęta NIS 2, a będąca dostawcą firmy objętej NIS 2 będzie najprawdopodobniej zmuszona dostosować się w dużym stopniu do regulacji.

Dlaczego to ważne?

Nawet najmniejszy dostawca usług może stanowić drogę wejścia do organizacji docelowej.

Przykładem może być **atak ransomware na amerykańską sieć supermarketów Target** z 2013 roku. Atakujący wykorzystali phishing, aby wykraść poświadczenia z firmy dostarczającej usługi ogrzewania i klimatyzacji w sklepach. Dzięki temu atakujący dostali się do systemów Target i wykradli dane klientów. Cyberprzestępcom udało się ukraść dane 40 milionów kart kredytowych i debetowych oraz dane 70 milionów klientów. Całkowity koszt ataku dla Target szacowany jest na ponad 250 milionów dolarów, z czego 18,5 miliona wynosiły odszkodowania dla klientów, których dane wyciekły.

Obowiązek samorejestracji

Firmy spełniające warunki podmiotów kluczowych lub ważnych będą miały obowiązek dokonania samorejestracji w systemie teleinformatycznym S46 w ciągu trzech miesięcy od wejścia w życie nowelizacji UoKSC lub spełnienia wymogów (np. przekroczenie size cap).

Podmiot zobowiązany będzie do przekazania m.in.:

- zakresu wykorzystywanych adresów IP,
- zakresu wykorzystywanych domen internetowych,
- danych co najmniej 2 osób do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa (dla podmiotów publicznych - ważnych - 1 osoba),
- deklaracji o statusie mikroprzedsiębiorcy, małego przedsiębiorcy lub średniego przedsiębiorcy,
- informacji o państwach członkowskich, w których wykonywana jest działalność, wraz z określeniem wykonywanej działalności,
- informacji o zawarciu umowy z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa.

Informacje składane są pod rygorem odpowiedzialności karnej za złożenie fałszywego oświadczenia.

Sektor kluczowy - wykaz podmiotów podlegających pod NIS 2

Sektory kluczowe				
Sektor	**Podsektor lub przykład podmiotu**	**Podmioty małe i mikro***	**Podmioty średnie****	**Podmioty duże*****
Energetyka	Energia elektryczna	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
	Systemy ciepłownicze lub chłodnicze	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
	Ropa naftowa	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
	Gaz	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
	Wodór	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
Transport	Lotniczy	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
	Kolejowy	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
	Wodny	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
	Drogowy	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
Bankowość	Instytucje kredytowe (stosują także DORA)	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
Infrastruktura rynków finansowych	Operatorzy systemów obrotu, kontrahenci centralni (CCP) (stosują także DORA)	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
Opieka zdrowotna	M.in. świadczeniodawcy, laboratoria referencyjne, podmioty produkujące leki, substancje oraz określone wyroby medyczne	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
Woda pitna	Dostawcy i dystrybutorzy „wody przeznaczonej do spożycia przez ludzi"	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
Ścieki	Podmioty zbierające, odprowadzające lub oczyszczające ścieki komunalne, bytowe lub przemysłowe	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
Infrastruktura cyfrowa	Dostawcy punktu wymiany ruchu internetowego	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
	Dostawcy usług chmurowych	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
	Dostawcy usług ośrodka przetwarzania danych	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
	Dostawcy sieci dostarczania treści	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
	Dostawcy publicznych sieci łączności elektronicznej	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy	Nie wdraża NIS 2
	Dostawcy publicznie dostępnych usług łączności elektronicznej	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy	Nie wdraża NIS 2
	Dostawcy usług zaufania (stosują także rozporządzenie 910/2014)	NIS 2 - Podmiot kluczowy	NIS 2 - Podmiot kluczowy	NIS 2 - Podmiot kluczowy
	Dostawcy usług DNS, z wyłączeniem operatorów głównych serwerów nazw	NIS 2 - Podmiot kluczowy	NIS 2 - Podmiot kluczowy	NIS 2 - Podmiot kluczowy
	Rejestry nazw TLD	NIS 2 - Podmiot kluczowy	NIS 2 - Podmiot kluczowy	NIS 2 - Podmiot kluczowy
Zarządzanie usługami ICT (między przedsiębiorstwami)	Dostawcy usług zarządzanych	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy
	Dostawcy usług zarządzanych w zakresie bezpieczeństwa****	NIS 2 - Podmiot kluczowy	NIS 2 - Podmiot kluczowy	NIS 2 - Podmiot kluczowy
Podmioty administracji publicznej (nie mają do nich zastosowania kryteria wielkości i obrotu)	Podmioty administracji publicznej na szczeblu centralnym	NIS 2 - Podmiot kluczowy	NIS 2 - Podmiot kluczowy	NIS 2 - Podmiot kluczowy
	Podmioty administracji publicznej na szczeblu regionalnym	NIS 2 - Podmiot ważny	NIS 2 - Podmiot ważny	NIS 2 - Podmiot ważny
Przestrzeń kosmiczna	Operatorzy infrastruktury naziemnej w zakresie usług związanych z kosmicznymi podmiotami prywatnymi, które wspierają świadczone usługi kosmiczne (z wyjątkiem dostawców publicznych sieci łączności elektronicznej)	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot kluczowy

* **Małe i mikro** – mniej niż 50 pracowników oraz maksymalnie 10 mln € obrotu (lub sumy bilansowej) rocznie.

** **Średnie** – mniej niż 250 pracowników oraz maksymalnie 50 mln € obrotu (lub 43 mln € sumy bilansowej) rocznie.

*** **Duże** – co najmniej 250 pracowników lub ponad 50 mln € obrotu (lub 43 mln € sumy bilansowej) rocznie.

**** Co najmniej spełnia wymogi dla małego przedsiębiorcy >10 pracowników i roczny obrót >2mln euro.

Sektor ważny - wykaz podmiotów podlegających pod NIS 2

Sektory ważne				
Sektor	**Podsektor lub przykład podmiotu**	**Podmioty małe i mikro***	**Podmioty średnie****	**Podmioty duże*****
Usługi pocztowe i kurierskie	Operatorzy usług pocztowych	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot ważny
Gospodarowanie odpadami	Przedsiębiorstwa zajmujące się gospodarowaniem odpadami	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot ważny
Produkcja i wytwarzanie chemikaliów	Przedsiębiorstwa zajmujące się gospodarowaniem odpadami	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot ważny
Produkcja i przetwarzanie żywności	Przedsiębiorstwa spożywcze w rozumieniu rozporządzenia (WE) nr 178/2002	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot ważny
	Produkcja wyrobów medycznych	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot ważny
	Produkcja komputerów, wyrobów elektronicznych i optycznych	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot ważny
	Produkcja urządzeń elektrycznych	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot ważny
	Produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot ważny
	Produkcja pojazdów samochodowych	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot ważny
	Produkcja pozostałego sprzętu transportowego	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot ważny
Dostawcy usług cyfrowych	Dostawcy internetowych platform handlowych, wyszukiwarek internetowych, dostawcy platform usług sieci społecznościowych	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot ważny
Badania naukowe	—	Nie wdraża NIS 2	NIS 2 - Podmiot ważny	NIS 2 - Podmiot ważny

* **Małe i mikro** – mniej niż 50 pracowników oraz maksymalnie 10 mln € obrotu (lub sumy bilansowej) rocznie.

** **Średnie** – mniej niż 250 pracowników oraz maksymalnie 50 mln € obrotu (lub 43 mln € sumy bilansowej) rocznie.

*** **Duże** – co najmniej 250 pracowników lub ponad 50 mln € obrotu (lub 43 mln € sumy bilansowej) rocznie.

Treść tego rozdziału dostępna jest również w formie nagrania. Kilknij tutaj aby obejrzeć.

5. Kary i sankcje

W NIS 2 wymienione są trzy rodzaje kar: są to kary finansowe, sankcje dotyczące działalności samej organizacji oraz odpowiedzialności top managementu.

Kary finansowe

Jeśli chodzi o **kary finansowe to dla podmiotów kluczowych** wynoszą one:

- Co najmniej 10 000 000 EUR lub 2 % całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego, przy czym zastosowanie będzie mieć kwota wyższa.

Natomiast dla **podmiotów ważnych kary wynoszą:**

- Co najmniej 7 000 000 EUR lub 1,4 % całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego, przy czym zastosowanie będzie mieć kwota wyższa.

Polski ustawodawca wprowadził **dodatkową karę finansową** do 100 000 000 PLN **dla podmiotów kluczowych i ważnych**, jeżeli podmiot naruszy przepisy ustawy i spowoduje bezpośrednie, ekstremalnie poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, życia i zdrowia ludzi, wywołania poważnej szkody majątkowej itp.

Zawieszenie certyfikacji i zezwoleń

Drugą z sankcji określoną w NIS 2 jest możliwość **zawieszenia certyfikacji czy zezwoleń na usługi lub działania świadczone przez organizację**. Możemy sobie wyobrazić, że w przypadku znaczącego naruszenia firma może otrzymać czasowy zakaz świadczenia usług czy działalności.

Odpowiedzialność kierownika podmiotu

Trzecia sankcja dotyczy odpowiedzialności kierownika podmiotu, czyli:

- Złożenia przez firmę **publicznego oświadczenia** określającego osobę fizyczną i prawną odpowiedzialną za naruszenie oraz charakter tego naruszenia.
- Czasowy **zakaz pełnienia funkcji kierowniczych** w podmiocie na poziomie dyrektora generalnego, przedstawiciela prawnego oraz każdej innej osoby uznanej za odpowiedzialną za naruszenie. Ważne jednak, że zakaz pełnienia funkcji zarządczych w podmiocie kluczowym nie może doprowadzić do całkowitego uniemożliwienia funkcjonowania tego podmiotu.

  Oznacza to, że organ nadzoru musi uwzględniać konieczność zapewnienia minimalnego poziomu działalności podmiotu, aby umożliwić mu wdrożenie środków naprawczych.

- **Sektor prywatny - kara pieniężna do 300% średniego miesięcznego wynagrodzenia** danego kierownika podmiotu. Nie chodzi tu o średnią krajową, tylko faktyczne wynagrodzenie danej osoby.
- **Sektor publiczny - kara pieniężna do 100% średniego miesięcznego wynagrodzenia** danego kierownika podmiotu. Nie chodzi tu o średnią krajową, tylko faktyczne wynagrodzenie danej osoby.

Dyrektywa nie tylko "straszy" organy zarządzające sankcjami. Wymaga również wzięcia odpowiedzialności za cyberbezpieczeństwo organizacji oraz odbycia szkoleń z tego zakresu.

W dyrektywie NIS 2 jest m.in. zdanie mówiące o tym, że kierownik podmiotu odpowiada za:

„Wprowadzenie odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych dla zapobiegania lub minimalizowania wpływu incydentów cybernetycznych."

Doprecyzowując oznacza to, że **kierownik podmiotu zobligowany jest do:**

- oceny ryzyk cybernetycznych i ich wpływu na działalność podmiotu,
- zatwierdzania środków zarządzania ryzykiem cyberbezpieczeństwa,
- nadzorowania ich wdrażania.

W NIS 2 jest jednocześnie przewidziany obowiązek **regularnego odbywania szkoleń** przez kierownika podmiotu dla zdobycia wiedzy i umiejętności, umożliwiających im:

- identyfikację zagrożeń i ocenę ryzyk cybernetycznych,
- ocenę praktyk zarządzania ryzykiem cyberbezpieczeństwa,
- ocenę ich wpływu na działalność podmiotu.

Nowelizacja UoKSC nakłada na kierownika podmiotu obowiązek wykonywania wyżej wymienionych szkoleń **minimum raz w roku.**

> **Treść tego rozdziału dostępna jest również w formie nagrania. Kilknij tutaj aby obejrzeć.**

Kim jest kierownik podmiotu?

W moich rozmowach dotyczących NIS 2, często słyszę, że powyżej opisana odpowiedzialność dotyczy osób zarządzających działami IT lub cyberbezpieczeństwem w organizacji, czyli CTO, CIO, CISO. **To błąd!**

W nowelizacji UoKSC wyżej wymieniona odpowiedzialność dotyczy kierownika podmiotu. Kim jest **KIEROWNIK PODMIOTU** definiuje ustawa o rachunkowości. Zgodnie z nią kierownikiem podmiotu zależnie od formy prawnej i rodzaju podmiotu jest prezes, dyrektor generalny, rektor, dyrektor szpitala, starosta, wójt itd.

W przypadku, gdy kierownikiem podmiotu jest organ wieloosobowy i nie została wskazana osoba odpowiedzialna, odpowiedzialność ponoszą wszyscy członkowie tego organu.

Równie często powtarzającym się mitem jest twierdzenie, że wyżej wymienione obowiązki i odpowiedzialność można zdelegować na kierownika IT, CTO, CIO, CISO itp. **To nieprawda.**

Kierownik podmiotu może zdelegować zarządzanie cyberbezpieczeństwem i wdrażanie wymogów NIS 2 odpowiednim osobom, jednak wyżej wymieniona odpowiedzialność, w tym kary, zawsze pozostają na kierowniku podmiotu.

Nadzór i kontrole nad spełnieniem wymagań

W ramach projektu nowelizacji UoKSC wprowadzającej NIS 2 w Polsce możemy wyróżnić trzy tryby kontroli.

Nadzór następczy – czyli kontrola przeprowadzana w podmiotach kluczowych i ważnych po wystąpieniu incydentu bezpieczeństwa. Dotyczy zarówno podmiotów kluczowych, jak i ważnych. Za jej realizację odpowiadają osoby wyznaczone przez właściwe ministerstwo ze wsparciem CSIRT sektorowych I poziomu krajowego.

Nadzór prewencyjny (proaktywny) – to cykliczne kontrole w podmiotach kluczowych oraz ważnych, sprawdzające czy organizacja spełnia wymagania wynikające z dyrektywy NIS 2 oraz znowelizowanej UoKSC. Ten rodzaj kontroli będzie stosowany głównie wobec podmiotów kluczowych i, podobnie jak w pierwszym przypadku, przeprowadzany przez przedstawicieli odpowiedniego ministerstwa ze wsparciem CSIRT sektorowych I poziomu krajowego.

Kontrole doraźne – przeprowadzane w podmiotach kluczowych w uzasadnionych przypadkach w związku z wystąpieniem poważnego incydentu, naruszeniem dyrektywy lub w innych przypadkach. Kontrola doraźna może być prowadzona także w celu sprawdzenia, czy podmiot usunął wcześniej stwierdzone uchybienia lub wykonał zalecenia pokontrolne.

W najnowszej wersji projektu nowelizacji UoKSC doprecyzowane zostały **zasady wydawania decyzji w zakresie środków nadzoru**, m.in. wskazano, że:

- środek nadzoru nie może być stosowany dłużej niż 14 dni od daty doręczenia decyzji o jego zastosowaniu,
- jednak, gdy podmiot kluczowy nie podjął wskazanych działań, organ właściwy ds. cyberbezpieczeństwa może ponownie wydać decyzje na kolejne 14-dniowe okresy do czasu usunięcia uchybień,
- organ właściwy ds. cyberbezpieczeństwa uchyla decyzję w sprawie środków nadzoru (na wniosek lub z urzędu) po usunięciu uchybień lub zaprzestaniu naruszeń,
- organ nadzoru, kierując do podmiotu kluczowego pismo z ostrzeżeniem o naruszeniu, musi wskazać termin, w jakim podmiot powinien podjąć określone działania naprawcze. Wcześniej przepisy nie regulowały tego w sposób precyzyjny,
- informacje o wydanych decyzjach w zakresie środków nadzoru będą publikowane w Biuletynie Informacji Publicznej organu nadzorczego. Wyjątek stanowią informacje prawnie chronione, które nie podlegają upublicznieniu.

Nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa

MAPA OBOWIĄZKÓW I ODPOWIEDZIALNOŚCI

(SZBI) Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w systemie informacyjnym (Art. 8).

- Prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem.
- Wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych.
  - Polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne.
  - Bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym **testowanie systemu informacyjnego.**
  - Bezpieczeństwo fizyczne i środowiskowe uwzględniające kontrole dostępu.
  - Bezpieczeństwo zasobów ludzkich.
  - Bezpieczeństwo i ciągłość łańcucha dostaw produktów, usług i procesów ICT.
  - Wdrażanie, dokumentowanie, testowanie i utrzymywanie **planów ciągłości działania, planów awaryjnych, oraz planów odtworzenia działalności.**
  - Objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi **systemem monitorowania w trybie ciągłym.**
  - Polityki i procedury oceny skuteczności środków technicznych i organizacyjnych.
  - Edukacja z zakresu cyberbezpieczeństwa dla personelu podmiotu.
  - Podstawowe zasady cyber higieny.
  - Polityki i procedury stosowania kryptografii i szyfrowania (w stosownych przypadkach).
  - Stosowanie bezpiecznych środków komunikacji... (w s.p.) uwzględniających uwierzytelnianie wieloskładnikowe.
  - Zarządzanie aktywami.
  - Polityki kontroli dostępu.
- Zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego.
- Zarządzanie incydentami.
- Stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego.
  - Stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym.
  - Regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji.
  - Ochrona przed nieuprawnioną modyfikacją w systemie informacyjnym.
  - Niezwłoczne podejmowanie działań po ostrzeżeniu podatności lub cyberzagrożeń, w tym również czasowe ograniczenie ruchu sieciowego przychodzącego... mając na uwadze konieczność minimalizacji skutków ograniczenia dostępności... usług.
- UWAGA: Podmioty publiczne-ważne.
  - Nie są objęte obowiązkiem wdrożenia pełnego SZBI.
  - Zamiast tego zobowiązane są do wdrożenia uproszczonego SZBI zgodnego z wymogami określonymi w załączniku nr 4 do ustawy.

KIEROWNIK PODMIOTU obowiązki i odpowiedzialności (Art. 8 c, d, e).

- Ponosi odpowiedzialność za wykonywanie obowiązków w zakresie cyberbezpieczeństwa przez podmiot.
  - UWAGA: Brak możliwości delegacji odpowiedzialności na CIO, CTIO, CISO itp.
- Podejmuje decyzje w zakresie przygotowania, wdrażania, stosowania, przeglądu i nadzoru SZBI.
- Planuje adekwatne środki finansowe na realizację obowiązków z zakresu cyberbezpieczeństwa.
- Przydziela zadania z zakresu cyberbezpieczeństwa w tym podmiocie i nadzoruje ich wykonanie.
- Zapewnia, że personel podmiotu jest świadomy obowiązków z zakresu cyberbezpieczeństwa i zna wewnętrzne regulacje podmiotu w tym zakresie.
- Zapewnia zgodność działania podmiotu z przepisami prawa oraz z wewnętrznymi regulacjami podmiotu.
- Obligatoryjnie raz w roku lub częściej odbywa szkolenie w zakresie wykonywania obowiązków.

Obowiązek samo rejestracji (Art. 7)

- Zgłoszenia dokonuje Kierownik Podmiotu
- Poprzez złożenie wniosku w systemie S46 (Art. 46)
- W terminie 3 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny
- Wpis z urzędu dokonywany tylko dla
  - Przedsiębiorcy telekomunikacyjni
  - Dotychczasowi Operatorzy Usług Kluczowych
  - Dostawcy usług zaufania
  - Podmioty publiczne

Wyznaczenie osób odpowiedzialnych zautrzymywanie kontaktów z podmiotami Krajowego Systemu Cyberbezpieczeństwa (Art. 9)

- Podmiot kluczowy i ważny
  - Wyznacza co najmniej dwie osoby
- Podmiot kluczowy i ważny będący mikro- lub małym przedsiębiorcą
  - Wyznacza co najmniej jedną osobę

Opracowanie, stosowanie i aktualizacja dokumentacji dot. bezpieczeństwa systemu informacyjnego (Art. 10)

- Dokumentacja normatywna
- Dokumentacja operacyjna

Powołanie wewnętrznej struktury odpowiedzialnej za cybersec lub zawarcie umowy z dostawcą usług zarządzania w zakresie cybersec (Art. 14).

Przeprowadzanie audytu bezpieczeństwa systemu informacyjnego (Art. 15).

- Tylko podmioty kluczowe.
- Pierwszy audyt w ciągu 24 miesięcy.
- Kolejne audyty raz na trzy lata.
- Organ właściwy ds. cyberbezpieczeństwa może zawsze nakazać przeprowadzenie audytu ad hoc w drodze decyzji.

Informowanie o cyberzagrożeniu, incydencie użytkowników usług (Art. 11, ust. 2a i 2b).

- Na których poważne cyberzagrożenie może mieć wpływ, o możliwych środkach zapobiegawczych, które użytkownicy ci mogą podjąć.
- O samym poważnym cyberzagrożeniu, jeżeli nie spowoduje to zwiększenia poziomu ryzyka dla bezpieczeństwa systemów informacyjnych.
- O incydencie poważnym, jeżeli ma on niekorzystny wpływ na świadczenie tych usług.

Obowiązek obsługi incydentów, zgłaszania incydentów poważnych i współdziałanie przy obsłudze incydentu poważnego (Art. 11, 12, 13).

- Zapewnienie obsługi incydentów.
- Zapewnienie obsługi incydentów.
- Zapewnienie dostępu do informacji o rejestrowanych incydentach właściwemu CSIRT.
- Klasyfikacja incydentów poważnych.
- **Zgłoszenie wczesnego ostrzeżenia o incydencie poważnym.**
  - Do CSIRT sektorowy.
  - Nie później niż w ciągu 24 godz. od wykrycia.
- **Zgłoszenie incydentu poważnego.**
  - Do CSIRT sektorowy.
  - Nie później niż w ciągu 72 godz. od wykrycia.
- Przekazanie sprawozdania okresowego.
  - Tylko gdy wnioskuje o to właściwy CSIRT sektorowy.
- **Przekazanie sprawozdania końcowego z obsługi incydentu poważnego.**
  - Do CSIRT sektorowy.
  - Nie później niż **w ciągu 1 miesiąca** od wykrycia.
- Współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT.
- Usuwanie podatności, o których mowa w art. 32 ust. 2 oraz informowanie o nich.
  - CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie podmiotu, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego lub krytycznego.

6. Obowiązki firm - zarządzanie ryzykiem

NIS 2 wskazuje, że wszystkie podmioty muszą **„podejmować odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania zagrożeniami dla bezpieczeństwa cybernetycznego sieci i systemów informatycznych."**

Mówiąc prościej te środki oznaczają zatrudnionych specjalistów, wdrożone procesy i procedury, systemy i rozwiązania techniczne itd. Jak mądrze zdecydować o dobrze środków technicznych i organizacyjnych dla danej organizacji?

WDROŻENIE SZBI

Dyrektywa NIS 2 i nowelizacja UoKSC nakłada na podmioty kluczowe i ważne obowiązek wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Organizacje muszą dokumentować środki techniczne i organizacyjne, np. polityki bezpieczeństwa, zarządzanie dostępem czy ciągłość działania. SZBI powinien być nie tylko wdrożony, ale również **utrzymywany, aktualizowany i kontrolowany.** SZBI można wdrożyć w oparciu o dowolny framework, a w załączniku do UoKSC ma się znaleźć mapowanie obowiązków na wybrane normy np. ISO czy NIST.

Podmioty publiczne-ważne nie są objęte obowiązkiem wdrożenia SZBI. Zamiast tego zobowiązane są do wdrożenia uproszczonego SZBI zgodnego z wymogami określonymi w załączniku nr 4 do ustawy. Oprócz obowiązkowych wymagań, załącznik 4 zawiera też dodatkowe, nieobowiązkowe propozycje zabezpieczeń, które mogą pomóc lepiej chronić się przed cyberzagrożeniami.

SZACOWANIE RYZYK

Właściwym podejściem, niezależnie od wielkości firmy czy instytucji, jest przeprowadzenie szacowania ryzyk (w tym cybernetycznych) oraz identyfikacja tych najbardziej krytycznych. Wymienione wcześniej środki muszą zapewniać poziom bezpieczeństwa powiązany z i wynikający wprost z występujących w danej organizacji ryzyk. To dlatego w projekcie nowelizacji UoKSC zawarty jest obowiązek szacowania ryzyka czyli identyfikacji cyber ryzyk, ich analizy, a finalnie ich oceny i priorytetyzacji.

Dyrektywa NIS 2 wymaga posiadania przez organizację udokumentowanych, aktualizowanych analiz i ewaluacji ryzyk systemów informacyjnych. Szacowanie ryzyk składa się z:

1. Identyfikacji ryzyk, w tym cyber i ich poziomu,
2. Analizy tych ryzyk i wybranie tych najistotniejszych,
3. Opracowania planu mitygacji najbardziej krytycznych z nich.

Dobrze przygotowana, przedyskutowana i uzgodniona z Zarządem oraz udokumentowana analiza cyber ryzyk zapewnia nam spełnienie w tym zakresie wymagania NIS 2, ale przede wszystkim jest najlepszym sposobem na przekonanie Zarządu do wagi obszaru cyber, w tym potrzebnych nakładów finansowych.

Pamiętajmy, by w oszacowaniu budżetu i środków na minimalizację cyber ryzyk wykorzystać specyfikę naszej organizacji, raporty o zagrożeniach czy przypadki cyber ataków na podobne do naszej organizacje. Należy wziąć pod uwagę koszty przestojów, niedostępności usług, utratę produkcji, dodać odzyskiwanie danych i wysiłki potrzebne do przywrócenia normalnego działania, a także uwzględnić szacunkowe koszty kar NIS 2 i szkody dla powiązanych przedsiębiorstw itp.

POLITYKI BEZPIECZEŃSTWA

Kolejny obowiązek to posiadanie udokumentowanej i aktualizowanej polityki bezpieczeństwa organizacji. Polityka bezpieczeństwa systemu informacyjnego:

- wynika ze strategii i celów biznesowych oraz je uzupełnia,
- określa cele i zobowiązanie do ciągłej poprawy,
- zobowiązuje do zapewnienia odpowiednich zasobów w tym budżetu,
- określa funkcje, obowiązki i uprawnienia,
- zawiera wykaz dokumentacji, w tym wykaz polityk tematycznych,
- określa KPI monitorowania jej wdrażania oraz poziomu dojrzałości,
- została formalnie zatwierdzona przez Kierownika Podmiotu,
- zawiera informację o terminie przeglądu i ewentualnej aktualizacji samej polityki - rekomendujemy wykonywanie przeglądu co roku.

Jak szybko zweryfikować czy obszar zarządzania ryzykiem i polityk bezpieczeństwa jest pod kontrolą?

Rekomenduję by zadać sobie samemu następujące pytania - **mini lista kontrolna:**

1. Czy krytyczne procesy i ich zasoby są znane, udokumentowane, określono dla nich najważniejsze ryzyka, a środki bezpieczeństwa są określone i wdrożone?
2. Czy zasoby teleinformatyczne objęte zakresem zostały zidentyfikowane, są monitorowane, a podatności i zagrożenia są zarządzane?
3. Czy polityki bezpieczeństwa, procedury są dokumentowane, komunikowane i cyklicznie oceniane?
4. Czy wdrożono proces monitorowania i zgłaszania incydentów bezpieczeństwa i reagowania na nie? Czy jest on udokumentowany?
5. Czy wiem jakich mam dostawców oraz czy zidentyfikowano zagrożenia dla łańcucha dostaw i wdrożono środki minimalizujące je?

CIĄGŁOŚĆ DZIAŁANIA I ZARZĄDZANIE KRYZYSOWE

Dyrektywa NIS 2 odnosi się do "ciągłości działania i zarządzania kryzysowego" w swoich środkach zarządzania ryzykiem.

Liczy się realna gotowość naszej organizacji do przywracania normalnego działania po wystąpieniu sytuacji nadzwyczajnej czy kryzysowej. Kluczowe jest tu **posiadanie planów ciągłości działania i zarządzania kryzysowego.**

Równie ważne jest **cykliczne testowanie planów ciągłości działania i zarządzania kryzysowego.** Nawet najlepiej opracowany dokument będzie bezużyteczny, jeśli pracownicy nie będą potrafili skorzystać z niego w sytuacji kryzysowej.

> **Treść tego rozdziału dostępna jest również w formie nagrania. Kilknij tutaj aby obejrzeć.**

INCYDENTY BEZPIECZEŃSTWA

NIS 2 wprowadza dwa rygorystyczne obowiązki dotyczące incydentów bezpieczeństwa:

1. Obowiązek zgłaszania incydentów i raportowanie ich statusu:

- bez zbędnej zwłoki i co ważne w czasie nie dłuższym niż 24 godziny od powzięcia wiedzy o poważnym incydencie czy zagrożeniu cybernetycznym musimy dokonać **wczesnego ostrzeżenia,** w którym musimy wskazać, czy poważny incydent został przypuszczalnie wywołany działaniem bezprawnym, czy działaniem w złym zamiarze oraz czy mógł wywrzeć wpływ transgraniczny,
- następnie, bez zbędnej zwłoki, w ciągu 72 godzin od powzięcia wiedzy o poważnym incydencie – **zgłoszenie incydentu**, z aktualizacją wcześniejszych informacji i wskazaniem wstępnej oceny poważnego incydentu, jego dotkliwości i skutków, a tam, gdzie to ma zastosowanie także wskaźników integralności systemu.

2. Obowiązek przedstawienia raportu końcowego < 1 miesiąc po złożeniu pierwszego raportu, po zgłoszeniu incydentu. Raport końcowy powinien zawierać:

- szczegółowy opis incydentu, jego wagi, wpływu i dotkliwości oraz skutków,
- rodzaj zagrożenia, pierwotna przyczyna, która prawdopodobnie była źródłem incydentu,
- zastosowane i wdrażane środki zaradcze ograniczające ryzyko,
- wskazanie transgranicznych skutków incydentów.

Podmioty ważne-publiczne nie są zobowiązane do przekazywania wczesnych ostrzeżeń i raportów końcowych. Podmioty publiczne-ważne mają jedynie obowiązek **dokonania zgłoszenia incydentu poważnego**. Sposób zgłaszania nie ulega zmianie – podmioty te powinny zgłosić incydent poważny niezwłocznie, nie później niż w terminie 72 godzin od jego wykrycia

Poważny incydent bezpieczeństwa to takie zdarzenie, które:

- spowodowało lub może spowodować dotkliwe zakłócenia operacyjne usług lub straty finansowe dla danego podmiotu,
- wpłynęło lub jest w stanie wpłynąć na inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe i niemajątkowe,
- ma znaczący wpływ na świadczenie usług,
- wszelkie istotne zidentyfikowane zagrożenia cybernetyczne, które mogły potencjalnie skutkować istotnym incydentem (zdarzenia potencjalnie wypadkowe).

Można przypuszczać, że specyfikacja UoKSC dla poważnego incydentu bezpieczeństwa będzie związana z liczbą użytkowników dotkniętych zakłóceniem podstawowej usługi, czasem trwania incydentu i obszarem geograficznym dotkniętym incydentem. Zasady klasyfikacji incydentów jako poważne określone zostaną po wejściu w życie znowelizowanej UKSC, w rozporządzeniu Rady Ministrów, które precyzować będzie progi uznania incydentu za poważny.

Jak sprawdzić, czy jesteśmy przygotowani do zgłaszania i raportowania incydentów bezpieczeństwa?

Rekomenduję by zadać sobie samemu następujące pytania - **mini lista kontrolna:**

1. Czy moja organizacja wykrywa i reaguje na incydenty w trybie operacyjnym, codziennie? Czy jestem odpowiednio szkolony w tym zakresie?
2. Czy wykrywam na bieżąco podatności, zagrożenia i zdarzenia security. Jaka jest ich jakość? Czy proces ten jest zautomatyzowany?
3. Czy moja organizacja jest w stanie zidentyfikować przyczynę źródłową incydentu? Czy obejmuje to czas i ścieżkę ataku?
4. Czy mam zdefiniowany, zakomunikowany i przećwiczony proces komunikacji w zakresie incydentów NIS 2?
5. Czy jestem w stanie na żądanie uprawnionych organów dostarczyć dowody?

Do kogo firmy i instytucje mają zgłaszać incydenty bezpieczeństwa?

Incydenty poważne, ich status i raporty musimy zgłaszać do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego, czyli CSIRT. Odbywać się to będzie przy użyciu systemu S46, który służyć będzie do komunikacji dwustronnej z CSIRTami.

Zgłoszenia należy wysyłać do odpowiedniego CSIRTu sektorowego, o ile taki został utworzony. Obecnie istnieją następujące CISRITy sektorowe:

- CSIRT CeZ - dla sektora ochrony zdrowia, w ramach Centrum e-Zdrowia.
- CSIRT INFRASTRUKTURA - dla sektora transportu i dostępu do wody, powołany przez Ministerstwo Infrastruktury.
- CSIRT Energia - dla sektora energii, tworzony przez Ministerstwo Klimatu i Środowiska.

W czerwcu 2025 r. Ministerstwo Cyfryzacji ogłosiło utworzenie CSIRTu Cyfra - dla sektora infrastruktury cyfrowej. Planowana operacyjność tej jednostki to czerwiec 2026 r.

Jeśli nie istnieje odpowiedni CSIRT sektorowy, incydenty należy zgłaszać do:

- CSIRT GOV - dla sektorów związanych z obronnością i bezpieczeństwem,
- CSIRT MON - dla instytucji administracji publicznej,
- CSIRT NASK - dla pozostałych podmiotów, głównie sektora cywilnego i prywatnego.

Treść tego rozdziału dostępna jest również w formie nagrania. Kilknij tutaj aby obejrzeć.

7. Bezpieczeństwo łańcucha dostaw

Jak interpretować „łańcuch dostaw”?

Łańcuch dostaw przede wszystkim obejmuje firmy, z którymi współpracujemy, w szczególności wszystkich naszych podwykonawców i usługodawców. Będą to przykładowo kancelarie prawne, ale też dostawcy usług chmurowych, agencja ochrony fizycznej, ale i software house'y, uczestniczące w tworzeniu dla nas aplikacji.

Do łańcucha dostaw zaliczyłbym również np. biblioteki i pakiety oprogramowania typu open-source lub innych firm, które są wymagane do funkcjonowania naszych aplikacji i operacji.

Kolejny przykład to wykorzystywana infrastruktura firm trzecich, a nawet zewnętrzni dostawcy zarządzanych usług bezpieczeństwa takich jak SOC. W przypadku firm, gdzie funkcjonuje Automatyka Przemysłowa łańcuch dostaw obejmować będzie serwis stron trzecich, które konfigurują i konserwują sprzęt przemysłowy.

Dobrze przygotowana, przedyskutowana i uzgodniona z Zarządem oraz udokumentowana analiza cyberryzyk zapewnia nam spełnienie w tym zakresie wymagania NIS 2, ale przede wszystkim jest najlepszym sposobem na przekonanie Zarządu do wagi obszaru cyber, w tym potrzebnych nakładów finansowych.

> **Treść tego rozdziału dostępna jest również w formie nagrania. Kilknij tutaj aby obejrzeć.**

Według wielu ekspertów **uwzględnienie w NIS 2 bezpieczeństwa łańcucha dostaw jest jedną z najważniejszych zmian jakie przynosi NIS 2.** Dlatego, że w dzisiejszym świecie większość firm i organizacji funkcjonuje w ekosystemie wielu firm, podwykonawców oraz partnerów publiczno-prywatnych. Ten ekosystem jest tak bezpieczny jak jego najsłabsze ogniwo.

Z tego powodu NIS 2 wprowadza dwie kategorie obowiązków dotyczących bezpieczeństwa łańcucha dostaw.

Pierwsza kategoria obowiązków

To obowiązek przeprowadzenia **risk assessmentu** dla wszystkich bezpośrednich dostawców i podwykonawców (tzw. Tier1), czyli zbadania i udokumentowania jakie cyberryzyka niesie współpraca z danym dostawcą, na ile jest to bezpieczne oraz określenie w jaki sposób zminimalizujemy te ryzyka, jakie środki czy rozwiązania wdrożymy. Ten assessment ma być oczywiście później aktualizowany.

Druga kategoria obowiązków

To obowiązki związane z **operacyjnym monitorowaniem i sprawdzaniem bezpieczeństwa.** Do tej kategorii wchodzą:

- proces wykrywania i reagowania na incydenty bezpieczeństwa, jak i technologie to wspierające
- cykliczne testy penetracyjne i audyty bezpieczeństwa włącznie z zarządzaniem podatnościami,
- kontrola jak bezpieczny jest proces tworzenia oprogramowania u naszego partnera.

Należy zwrócić uwagę na **„efekt domina”** - firma nieobjęta NIS 2, a będąca dostawcą firmy objętej NIS 2 będzie zmuszona w dużym stopniu dostosować się do obowiązków.

8. Ocena skuteczności środków zarządzania ryzykiem

NIS 2 wymaga, by organizacja wdrożyła procedury służące ocenie skuteczności środków zarządzania ryzykiem jako takim, w tym cybernetycznym. Wśród tych sposobów, procedur możemy wymienić kilka podstawowych metod:

Audyty bezpieczeństwa

Ważnym sposobem oceny skuteczności środków zarządzania ryzykiem cybebezpieczeństwa są audyty bezpieczeństwa. Są one **niezależnymi i obiektywnymi analizami** wdrożonych procesów bezpieczeństwa oraz procedur operacyjnych.

Podmioty kluczowe zobowiązane są do wykonania pierwszego audytu w ciągu pierwszych dwóch lat od wdrożenia nowelizacji ustawy, następnie audyt ma być powtarzany co 3 lata. Moim zdaniem to zdecydowanie zbyt rzadko - **rekomenduje wykonywanie audytu (i wdrażanie odpowiednich środków na jego podstawie!) raz na rok.**

Zazwyczaj punktem wyjścia do nich są standardy, normy np. ISO oraz przepisy prawa. Audyt bezpieczeństwa daje dobry wgląd w aktualny poziom bezpieczeństwa w organizacji, wskazując jednocześnie obszary wymagające poprawy czy doskonalenia.

Plany ciągłości działania i zarządzania kryzysowego

By być przygotowanym na wystąpienie sytuacji nadzwyczajnej, kryzysowej, w tym cyberkryzysu np. atak ransomware na naszą firmę i zaszyfrowanie większości komputerów i serwerów, kluczowe jest posiadanie **planów ciągłości działania i zarządzania kryzysowego**.

Równie ważne jest cykliczne testowanie planów ciągłości działania i zarządzania kryzysowego (co, powiedzmy sobie szczerze, nie dzieje się w dużej ilości organizacji). Nawet najlepiej przygotowany dokument będzie bezużyteczny, jeśli nie będziemy w stanie skutecznie przywrócić działania organizacji po wystąpieniu sytuacji nadzwyczajnej, takiej jak cyberatak.

Testy penetracyjne i testy bezpieczeństwa

Testy penetracyjne pozwalają sprawdzić odporność infrastruktury i systemów naszej organizacji na cyberataki. Testy weryfikują zastosowane rozwiązania, wyszukują wystąpienie podatności w naszej sieci, serwisach webowych, infrastrukturze chmurowej czy aplikacjach mobilnych. Szczególnym przypadkiem testów bezpieczeństwa są **testy kodu źródłowego** wykorzystywanych aplikacji i występujących w nim luk i podatności.

Testy socjotechniczne

Testy te dotyczą **pracowników i współpracowników organizacji.** Pozwalają one na weryfikację czy pracownicy i współpracownicy:

- znają i stosuje dobre praktyki związane z przetwarzaniem informacji?
- korzystają z sieci Internet w sposób z zachowaniem odpowiedniej czujności?
- potrafią rozpoznać typowe, najbardziej popularne metody działania cyberprzestępców?

Symulacje ataków hakerskich

Zazwyczaj takie testy wykonywane są według podobnego schematu, jakim posługują się cyberprzestępcy i skupiają się na weryfikacji błędów bezpieczeństwa, które mogą zostać wykorzystane do osiągnięcia celu.

Tutaj zazwyczaj zewnętrzna firma wykonująca takie symulacje koncentruje się na scenariuszach wykorzystywanych podczas prawdziwych ataków. Tego typu symulacje zazwyczaj mają dwie części:

- **blackbox** - gdzie testujący, którzy wcielają się w rolę atakujących mają minimalną wiedzą o atakowanej infrastrukturze organizacji,
- **whitebox** - gdzie testujący, którzy wcielają się w rolę atakujących mają dostęp do konfiguracji testowanej.

Kliknij tutaj, żeby zobaczyć symulację ataku hakerskiego Sekurak i Trecom.

Ćwiczenia red team i blue team

To są jeszcze bardziej zaawansowane nie tylko testy, ale **skomplikowane ćwiczenia** mające za zdanie ocenić cały system cyberochrony (ludzie, procesy i technologie) i w efekcie znaleźć niezauważone wcześniej luki.

Ćwiczenia te polegają na tym, że „czerwona" drużyna pentesterów atakuje, na przykład naszą infrastrukturę sieciową czy aplikację finansową, a zadaniem „niebieskiej" drużyny jest skuteczna obrona.

9. Cyberhigiena i szkolenia

NIS 2 wskazuje na obowiązek wykonywania cyklicznych szkoleń dla pracowników i współpracowników, co ważne wszystkich szczebli.

Moduły szkoleniowe w zakresie podnoszenia cyber świadomości użytkowników muszą być dostosowane do specyfiki organizacji. Wspomniane wcześniej testy socjotechniczne są również zaliczane są do proaktywnej edukacji. Takie testy pozwalają określić na jakie obszary cyber ochrony musimy zwrócić szczególną uwagę w danej organizacji.

Kluczowe jest jednak, aby nie skupiać się bezrefleksyjnie tylko na odbyciu szkolenia (zwykle w formie e-learningu), po to by „odbębnić" wymagany obowiązek ponieważ to zwykle przynosi zły efekt. Byle jakimi szkoleniami nie zwiększamy świadomości naszych pracowników. Dlatego tak ważny jest w moim przekonaniu

Program Security Awareness

Czyli całościowe, holistyczne podejście, według którego w organizacji staramy się uzyskać stan, w którym wszyscy czują się odpowiedzialni za bezpieczeństwo i ochronę informacji od zarządu, po biznes i wszystkich pracowników. Budowanie świadomości to proces długi, to raczej maraton niż bieg na 400m, obejmujący wiele zagadnień, i musi się odbywać na poziomie strategicznym jak i operacyjnym.

Kilknij tutaj, aby obejrzeć materiał z Tomaszem Matułą o programach security awareness.

10. Rozwiązania technologiczne

NIS 2 właściwie nie wskazuje konkretnych rozwiązań technologicznych security, które powinny być stosowane przez organizacje.

Punktem wyjścia jest tu następujący zapis dyrektywy:

„Kluczowe i ważne podmioty podejmują odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykiem stwarzanym dla bezpieczeństwa systemów sieciowych i informatycznych, z których podmioty te korzystają przy świadczeniu swoich usług."

Wspomniane wyżej **środki i obowiązki** omówiliśmy w większości w poprzednich rozdziałach. Wymieńmy je wszystkie w jednym miejscu. Są to:

1. Szacowanie ryzyka i polityki bezpieczeństwa systemów informatycznych
   - Określenie ryzyk i ich poziomu
   - Plan mitygacji ryzyk security
2. Obsługa incydentów security i informowanie o nich (zapobieganie, wykrywanie i reagowanie na incydenty)
3. Plany ciągłości działania i zarządzania kryzysowego
4. Bezpieczeństwo łańcucha dostaw
5. Polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem cyberbezpieczeństwa
6. Bezpieczeństwa w pozyskiwaniu, rozwijaniu i utrzymywaniu sieci i systemów informatycznych, w tym ujawnianie i zarządzanie podatnościami
7. Stosowanie kryptografii i szyfrowania oraz uwierzytelniania wieloskładnikowego lub ciągłego

Treść tego rozdziału dostępna jest również w formie nagrania. Kilknij tutaj aby obejrzeć.

Ponieważ firmy i instytucje są różne pod względem wielkości, sektora, tego czym się zajmują, dlatego jakie konkretne środki organizacyjne, procesowe oraz rozwiązania technologiczne wdrożą **musi wynikać** z analizy zagrożeń i ryzyk, określenia ich poziomu i naszego apetytu na ryzyko. Niezbędne i wdrażane konkretne cyber rozwiązania technologiczne mogą być inne dla sklepu internetowego, inne dla firmy produkcyjnej, a inne dla szpitala.

Bardzo szczegółowo zabezpieczenia zarówno procesowe oraz technologiczne opisują frameworki takie jak **ISO 27001**, a w szczególności **ISO 27002** czy **NIST**.

Dlaczego w dyrektywie NIS 2 wymienione jest wprost wykorzystanie kryptografii, szyfrowania oraz uwierzytelniania wieloskładnikowego lub ciągłego?

Regulator przyjął, że zarówno wykorzystanie kryptografii i szyfrowania oraz uwierzytelniania wieloskładnikowego to absolutne podstawy, które powinny być stosowane przez zdecydowaną większość firm, instytucji i organizacji.

11. Ujawniane i zarządzanie podatnościami

Zarządzanie podatnościami w infrastrukturze teleinformatycznej, aplikacjach i systemach to jeden z podstawowych wymogów bezpieczeństwa, ale ten obowiązek dotyczy trochę innego obszaru.

W NIS 2 jest następujący zapis:

„Producent lub dostawca produktów lub usług ICT powinien również wprowadzić procedury niezbędne do otrzymywania informacji o podatnościach na zagrożenia od stron trzecich".

Odnosi się on do **skoordynowania na poziomie UE procesu ujawniania podatności** i stworzenia unijnej bazy podatności - publicznie znanych luk w produktach ICT i usługach ICT, która to baza ma być obsługiwana przez ENISA.

Producenci lub dostawcy produktów i usług teleinformatycznych, będą zobligowani do umożliwienia przyjmowania podatności zgłaszanych przez osoby czy podmioty z zewnątrz. Proces ten, czyli Vulnerability Disclosure Policy (VDP) ma stworzyć strukturyzowany kanał udostępniany przez organizację każdemu, kto może zgłosić do niej problem związany z bezpieczeństwem cyfrowym.

Innymi słowy, jest to bezpieczny sposób, aby osoby trzecie wiedziały, gdzie i jak zgłaszać podatności w produktach czy usługach ICT do danej jednostki.

Treść tego rozdziału dostępna jest również w formie nagrania. Kilknij tutaj aby obejrzeć.

trecom | Cisco Partner

Potrzebujesz pomocy w obszarze NIS 2 lub UoKSC?

Umów się na bezpłatną konsultację i otrzymaj konkretne rekomendacje. Skontaktuj się ze swoim przedstawicielem handlowym lub napisz na poniższy adres e-mail.

marketing@trecom.pl

O Trecom

Jako Trecom od ponad 25 lat rozwijamy, optymalizujemy i utrzymujemy złożone systemy IT. Jesteśmy jednym z liderów rynku polskiego w segmencie sieci, cyberbezpieczeństwa, systemów AV, UC oraz data center. Nasz zespół składa się z ponad 115 inżynierów i architektów.

Posiadamy ponad 70 partnerstw technologicznych z wiodącymi dostawcami technologii oraz obszerną ofertę szkoleń. Rozbudowane portfolio rozwiązań przekłada się na niemal nieograniczone możliwości projektowe.

Nasza oferta obejmuje audyt, doradztwo, projektowanie, wdrażanie oraz utrzymywanie infrastruktury IT oraz cyberbezpieczeństwa. Wspieramy naszych klientów również poprzez usługi zarządzane – SOC, NOC i Centrum Wsparcia.