



Cybersecurity

Cloud&Data Center

T Business

NIS 2

**– REWOLUCJA W OBSZARZE
CYBERBEZPIECZEŃSTWA**

NIS 2 – NOWE STANDARDY

1 CO TO JEST NIS 2?

Dyrektywę NIS 2 (znaną jako dyrektywa UE 2022/2555), będącą przełomowym aktem prawnym, wprowadzono w celu **zwiększenia poziomu cyberbezpieczeństwa w Unii Europejskiej**. Zastępuje ona Dyrektywę NIS z 2016 r. Ustawodawca **wdraża bardziej rygorystyczne rozwiązania**, które będą skuteczniej chronić sektory infrastruktury krytycznej przed cyberatakami.



NIS 2 TO:

- Dyrektywa określająca standardy zarządzania ryzykiem oraz incydentami cyberbezpieczeństwa, do wdrożenia których zobowiązane są wskazane w niej instytucje publiczne oraz przedsiębiorstwa.
- NIS 2 wchodzi w życie 17.10.2024r.



2 WYBIERZ T BUSINESS

T Business wspiera organizacje we wdrażaniu oraz rozwijaniu rozwiązań z zakresu kompleksowej ochrony przed cyberzagrożeniami.

Zgodnie z modelem **IDENTIFY-PROTECT-DEFEND** nasi eksperci dokonają analizy stanu bezpieczeństwa firmy i przygotują strategię specjalnie dostosowaną do profilu jej działalności. Pomogą również osiągnąć zgodność z najnowszymi wymogami prawnymi dotyczącymi cyberochrony, w tym z Dyrektywą NIS 2.

WYMAGANIA NIS 2	DEDYKOWANE ROZWIĄZANIE	DLACZEGO T BUSINESS?
<p>Analiza ryzyka oraz polityka bezpieczeństwa systemów informatycznych</p>	<ul style="list-style-type: none"> ▪ vCISO 	<ul style="list-style-type: none"> ▪ Zarządzanie Programem Bezpieczeństwa ▪ Analiza stanu bezpieczeństwa, przygotowanie planu i schematu działania ▪ Ustalenie najlepszych praktyk w zakresie zasad i procedur, które zgodne są z ramami cyberbezpieczeństwa NIS2 i innymi obowiązującymi regulacjami branżowymi
<p>Zapobieganie, wykrywanie incydentów i reagowanie na nie</p>	<ul style="list-style-type: none"> ▪ Security Operations Center (SOC) ▪ XDR ▪ Cyber Guard ▪ Email Protection ▪ AntyDDoS ▪ vCISO 	<ul style="list-style-type: none"> ▪ Usługi wspierane analitykami SOC oraz analitykami wykrywającymi zagrożenia w cyberprzestrzeni ▪ Usługi poprawiające bezpieczeństwo podczas korzystania z Internetu ▪ Planowanie reagowania na incydenty związane z cyberbezpieczeństwem
<p>Zapewnienie ciągłości działania i zarządzanie kryzysowe</p>	<ul style="list-style-type: none"> ▪ MetroCluster ▪ Disaster Recovery as a Service ▪ Backup ▪ AntyDDoS ▪ vCISO 	<ul style="list-style-type: none"> ▪ Usługi zwiększające dostępność zasobów ▪ Eliminowanie przerw wynikających z niedostępności systemów
<p>Zapewnienie bezpieczeństwa w pozyskiwaniu, rozwijaniu oraz utrzymywaniu sieci i systemów informatycznych, zarządzanie podatnościami</p>	<ul style="list-style-type: none"> ▪ Zarządzanie Podatnościami (Vulnerability Management) ▪ Dostawa i wdrożenie rozwiązań z zakresu automatyzacji testów pozwalających na wykrywanie podatności ▪ Dostawa i wdrożenie rozwiązań z zakresu cyberbezpieczeństwa przez wykwalifikowany personel przy zapewnieniu zgodności z normami (ISO itp.) ▪ vCISO 	<ul style="list-style-type: none"> ▪ Ocena stanu infrastruktury teleinformatycznej ▪ Badanie bezpieczeństwa i zabezpieczeń aplikacji WEB ▪ Analiza nadzoru nad punktem styku z Internetem ▪ Weryfikacja sposobu ochrony systemów pocztowych ▪ Ocena stanu kultury bezpieczeństwa ▪ Wykrywanie podatności
<p>Podstawowe praktyki higieny cybernetycznej i szkolenia z zakresu cyberbezpieczeństwa</p>	<ul style="list-style-type: none"> ▪ Security Awareness (Program podnoszenia świadomości cyberzagrożeń) ▪ Mobile Device Management (MDM) 	<p>Szkolenie podnoszące świadomość bezpieczeństwa pozwala zmniejszyć ryzyko podatności na ataki wykorzystujące socjotechnikę. Pomagamy zmieniać zachowania pracowników. Celem jest podniesienie odporności na najnowsze zagrożenia socjotechniczne i taktyki naruszania biznesowej poczty elektronicznej.</p>

3 CELE NIS 2

Podstawowym celem wdrożenia dyrektywy NIS 2 jest osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii Europejskiej. Nowe standardy, które wprowadza Dyrektywa, wpłyną na zwiększenie bezpieczeństwa organizacji oraz ich infrastruktury.

CELE SZCZEGÓŁOWE:



Wyznaczenie nowych ram współpracy między państwami.



Zapewnienie wysokiego poziomu odpowiedzialności za środki zarządzania ryzykiem.



Poprawa poziomu rozumienia głównych zagrożeń oraz zbiorowej zdolności reagowania na nie.



Nałożenie na przedsiębiorstwa obowiązku zgłaszania incydentów.

4 KOGO DOTYCZY NIS 2?

Dyrektywą NIS 2 objęte zostały podmioty publiczne oraz prywatne, które:

- prowadzą działalność w sektorach wskazanych w dyrektywie jako kluczowe i ważne,
- kwalifikują się jako średnie przedsiębiorstwa lub przekraczają pułapy dla średnich przedsiębiorstw.

Sektory objęte dyrektywą NIS 2

SEKTOR KLUCZOWY

(high critical – Aneks 1)

- Energetyka
- Transport
- Bankowość
- Infrastruktura rynku finansowego
- Opieka zdrowotna
- Woda pitna
- Ścieki
- Infrastruktura cyfrowa
- Administracja publiczna
- Przestrzeń kosmiczna
- Zarządzanie usługami ICT

SEKTOR WAŻNY

(critical – Aneks 2)

- Usługi pocztowe i kurierskie
- Gospodarowanie odpadami
- Produkcja, wytwarzanie i dystrybucja chemikaliów
- Produkcja, wytwarzanie i dystrybucja żywności
- Produkcja
- Dostawcy usług cyfrowych
- Badania naukowe

NIS 2 obejmuje podmioty, w których liczba pracowników wynosi co najmniej 50 i/lub roczna suma bilansowa przekracza 10 mln euro.

5 KORZYŚCI

Spełnienie wymagań **NIS 2** wiąże się z wieloma korzyściami dla podmiotów kluczowych i ważnych. Do najważniejszych należą:

- **zwiększenie poziomu cyberbezpieczeństwa,**
- **ograniczenie ryzyka** wystąpienia incydentów bezpieczeństwa cybernetycznego,
- **ochrona** przed negatywnymi skutkami incydentów bezpieczeństwa cybernetycznego, poprawa reputacji.

6 NADZÓR

Podmioty kluczowe oraz ważne przestrzegają takich samych reguł Dyrektywy NIS 2. Różnica polega na stosowaniu systemu nadzoru.

Wobec podmiotów kluczowych stosuje się systemy nadzoru ex ante (proaktywny) i ex post (reaktywny), natomiast w przypadku podmiotów ważnych stosuje się system nadzoru ex post (reaktywny, uproszczony).



7 WYMAGANIA

DYREKTYWA NIS 2 WPROWADZA 3-STOPNIOWE RAPORTOWANIE:



Wczesne ostrzeżenie
(early warning) –
w ciągu 24 godz.
wysłanie wczesnego
ostrzeżenia, a tym
samym ograniczenie
rozprzestrzeniania
incydentu.



Zgłoszenie incydentu
(notification) –
w ciągu 72 godz.
wstępna ocena
skutków incydentu.



**Sprawozdanie
końcowe** (final report)
– nie później niż
miesiąc po wstępnej
ocenie przygotowanie
szczegółowego
raportu końcowego
(tzw. lessons learned).

7 KLUCZOWYCH ELEMENTÓW, KTÓRE MUSZĄ ZOSTAĆ UWZGLĘDNIONE PRZEZ ORGANIZACJĘ W CELU ZGODNOŚCI Z NIS 2:

- analiza ryzyka i polityki bezpieczeństwa systemów informatycznych,
- ciągłość działania i zarządzania kryzysowego,
- bezpieczeństwo łańcucha dostaw,
- bezpieczeństwo pozyskiwania, rozwijania i utrzymywania sieci oraz systemów informatycznych (w tym obsługi i ujawniania podatności),
- polityka i procedury (testowanie i audyt) służące ocenie skuteczności środków zarządzania ryzykiem cyberbezpieczeństwa,
- wykorzystywanie kryptografii i szyfrowania,
- obsługa incydentów (zapobieganie, wykrywanie i reagowanie na incydenty).

8 JAKIE KARY GROŻĄ ZA NIEPRZESTRZEGANIE NIS 2?

Od października 2024 r. **Dyrektywa NIS 2** będzie obowiązywała we wszystkich państwach członkowskich UE. Niezastosowanie się do wymogów tej dyrektywy może skutkować surowymi karami i oznaczać będzie m.in. „Twoja organizacja łamie prawo”.

Dyrektywa stanowi, że kadry zarządzające muszą podjąć odpowiednie środki w zakresie cyberbezpieczeństwa – w przeciwnym razie osoby odpowiedzialne w organizacji (pracownicy wyższego szczebla) mogą zostać pociągnięte do osobistej odpowiedzialności.

Kary finansowe za nieprzestrzeganie NIS 2:

Podmioty kluczowe:

10 mln euro

lub 2% łącznego rocznego obrotu.

Podmioty ważne:

7 mln euro

lub 1,4% łącznego rocznego obrotu.

W obu przypadkach zastosowanie ma wyższa kwota.

9 JAK PRZYGOTOWAĆ SIĘ DO WDROŻENIA NIS 2?

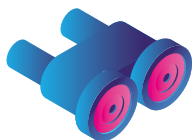
Aby dobrze przygotować organizację do wdrożenia **Dyrektywy NIS 2**, należy:



Powołać osobę lub zespół odpowiedzialny za nadzorowanie procesu dostosowania do NIS 2



Oceń ryzyko cyberbezpieczeństwa, zagrożenia, opracować mitygacje dla zidentyfikowanych ryzyk



Wdrożyć środki kontroli tak, aby ograniczyć zidentyfikowane zagrożenia i ochronić zasoby krytyczne



Edukować personel w zakresie cyberbezpieczeństwa

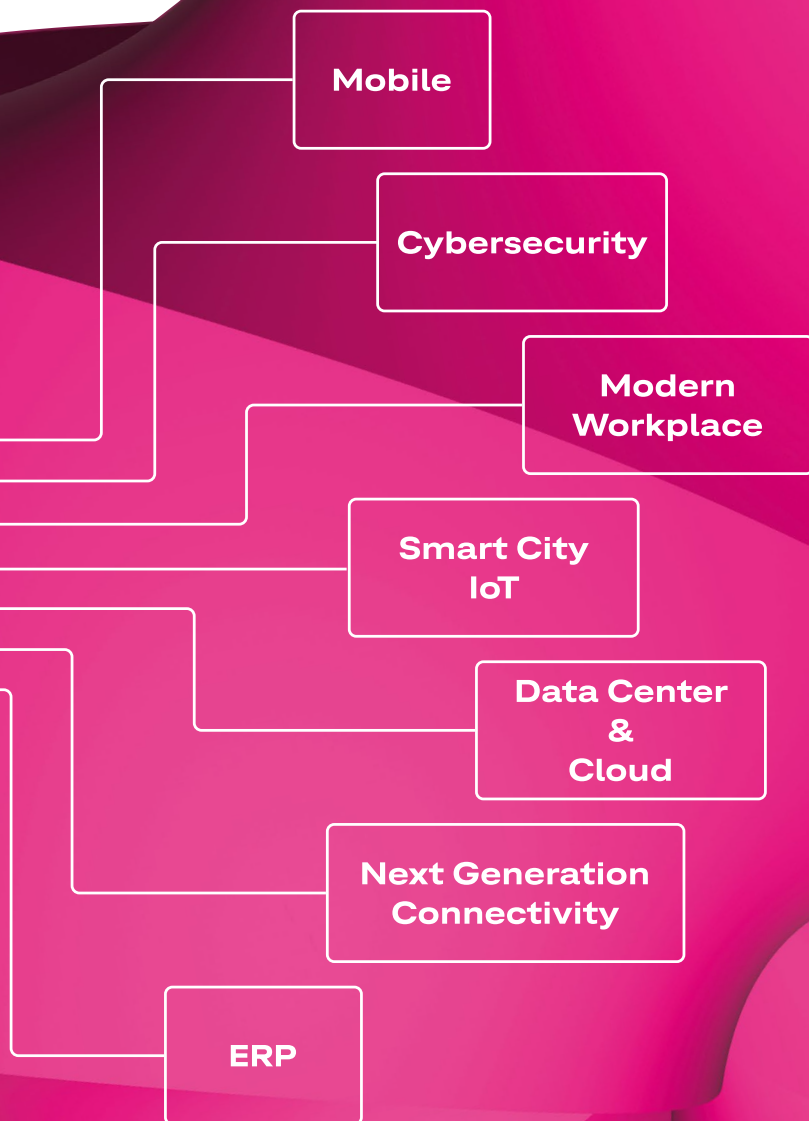


Opracować plan skutecznego reagowania na incydenty

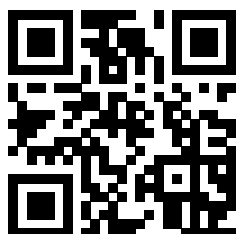
Obowiązkiem podmiotu jest przeprowadzenie we własnym zakresie oceny, czy w oparciu o wskazane w Dyrektywie NIS 2 kryteria jest on podmiotem kluczowym czy ważnym.

KOMPLEKSOWE USŁUGI

DLA DUŻYCH I ŚREDNICH FIRM



Dowiedz się więcej



T-Mobile Polska S.A.
ul. Marynarska 12, 02-674 Warszawa

Więcej informacji o usługach: www.biznes.t-mobile.pl