Cyberbezpieczeństwo w świetle Dyrektywy NIS2

Nowe Standardy dla Przedsiębiorstw od 2024

KILKA SŁÓW O MNIE

Marcin Chlebowski

Prezes Zarządu

eximo PROJECT

Wiceprezes Zarządu ds. nowych technologii

Pracodawcy Pomorza i Kujaw

NIS2. DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2022/2555 z dnia 14 grudnia 2022 r.

w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii,

https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32022L2555

Cel NIS2 ?

Zwiększenie poziomu cyberbezpieczeństwa na terenie Unii Europejskiej

Harmonizacja przepisów w państwach członkowskich:

Wzmocnienie współpracy i zdolności reagowania na incydenty

Horyzony czasowy

2016
Wejście w zycie Dyrektywy NIS

2020
Nowelizacja dyrektywy NIS

2022
Podpisanie Dyrektywy NIS2

2024.04.24
nowelizacja KSC

2024.10.18
NIS2 wchodzi w życie

Kogo obejmuje NIS2 ?

Podmioty kluczowe:

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

Energetyka
- Energia elektryczna
- Centralne ogrzewanie i chłodzenie
- Ropa
- Gaz
- Wodór

Bankowość
Infrastruktura rynków finansowych
Opieka zdrowotna
Woda pitna
Ścieki
Administracja publiczna
Przestrzeń kosmiczna
Transport
- Powietrzny
- Kolejowy
- Wodny
- Lądowy

Zarządzanie usługami ICT
Infrastruktura cyfrowa
- Data Center
- Usługi łączności elektronicznej
- Dostawcy usług chmurowych
- Dostawcy usług DNS

Kogo obejmuje NIS2 ?

Podmioty ważne:
50 pracowników i roczny obrót >
10 mln EUR i następujące branże:

Produkcja
- Wyroby medyczne
- Wyroby medyczne do diagnostyki in vitro
- Produkty komputerowe
- Produkty elektroniczne i optyczne
- Sprzęt elektryczny
- Maszyny i wyposażenie
- Pojazdy samochodowe, przyczepy i naczepy
- Inny sprzęt transportowy

Usługi pocztowe i kurierskie
Gospodarowanie odpadami
Produkcja, wytwarzanie i dystrybucja chemikaliów
Produkcja, przetwarzanie i dystrybucja żywności
Badania naukowe
Dostawcy cyfrowi
- Wyszukiwarki sieciowe
- Platformy e-commerce
- Platformy sieci społecznościowych

Kogo obejmuje NIS2 ?

Podmioty kluczowe i podmioty ważne z	Wielkość
podsektora produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro	44
sektora administracji publicznej	27905
sektora badań naukowych	169
sektora bankowości i infrastruktury rynków finansowych	547
sektora dostawców usług cyfrowych	40
sektora energii	365
sektora gospodarowania odpadami	276
sektora infrastruktury cyfrowej z wyłączeniem podsektora komunikacji elektronicznej	462
podsektora komunikacji elektronicznej	3784
sektora poczty	280
sektora produkcja, przetwarzanie i dystrybucja żywności	1204
sektora produkcja, wytwarzanie i dystrybucja chemikaliów	214
sektora produkcji, z wyłączeniem wyrobów medycznych	1120
sektora ścieków	102
sektora transportu	450
sektora transportu wodnego	11
sektora wody pitnej	268
sektora zarządzania ICT	43
sektora zdrowia	1248

38532

Obowiązki

Podmiot

„prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem”

Podmiot

„bezpieczeństwo i ciągłość łańcucha dostaw …”

Kary i sankcje

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.

Kary i sankcje

Drugą z sankcji określoną w NIS 2 jest możliwość **zawieszenia certyfikacji czy zezwoleń na usługi lub działania świadczone przez organizację**.

Firma może otrzymać czasowy zakaz świadczenia swoich usług czy działalności.

Obowiązki

Zarząd

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

organy zarządzające są zobligowane do:

- oceny ryzyk cybernetycznych i ich wpływu na działalność podmiotu
- zatwierdzanie środków zarządzania ryzykiem cyberbezpieczeństwa
- nadzorowanie ich wdrażania

obowiązek regularnego odbywania szkoleń przez ograny zarządzające dla zdobycia wiedzy i umiejętności, umożliwiające im:

- identyfikację zagrożeń i ocenę ryzyk cybernetycznych
- ocenę praktyk zarządzania ryzykiem cyberbezpieczeństwa
- Ich wpływu na działalność podmiotu

Kary i sankcje

Trzecia sankcja dotyczy odpowiedzialności zarządów i top managementu, czyli:

• Złożenia **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

Podsumowanie

Wejście w życie NIS2 18.10.2024

Analiza ryzyka cybernetycznych

Odpowiedzialność zarządu

Bezpieczeństwo łańcucha dostaw

Q&A

Dziękuję!

marcin.chlebowski@eximoproject.pl

PROJECT eximo