

# Dyrektywa NIS, czyli nowe CYBERobowiązki firm

Czym jest Krajowy System Cyberbezpieczeństwa i co on oznacza dla działających w Polsce firm?

Grudzień 2018



## Purpurowy Informator – Źródło informacji

Z przyjemnością prezentujemy kolejną edycję „Purpurowego Informatora”, czyli cyklu analiz, w którym omawiamy ważne dla przedsiębiorców kwestie prawne, księgowe i kadrowe. Tym razem tematem naszego cyklu jest tzw. dyrektywa NIS, czyli unijna regulacja, na bazie której powstaje w Polsce Krajowy System Cyberbezpieczeństwa.

### Szanowni Państwo,

Na wiosnę bieżącego roku przez polskie firmy przetoczyła się „akcja RODO” – do 25 maja wszystkie przedsiębiorstwa w Polsce musiały dostosować się do nowych przepisów, jakie niosła ze sobą unijna dyrektywa o ochronie danych osobowych. Nowe przepisy zmuszały przedsiębiorców do żmudnej pracy nad procesami i bazami danych oraz nakładały wysokie kary, za ewentualne uchybienia.

Choć nie jest o tym aż tak głośno, właśnie rozpoczyna się w polskich firmach druga, pod wieloma względami podobna rewolucja związana z dostosowywaniem procedur wewnętrznych – tym razem chodzi o tzw. dyrektywę NIS (Network and Information Systems Directive). Nakłada ona na wiele przedsiębiorstw obowiązek wprowadzenia rygorystycznych zasad dotyczących cyberbezpieczeństwa.

W odróżnieniu od RODO, regulacje NIS nie dotyczą wszystkich firm, a tylko te, które mają wpływ na szeroko rozumiane bezpieczeństwo systemu gospodarczego w Polsce. Ale – jak pokazujemy na kolejnych stronach – ich również są co najmniej setki, a może nawet tysiące.

**Kogo obejmują nowe CYBERregulacje?  
Co się z nimi wiąże?  
Jakie są ewentualne kary?  
Zapraszamy do lektury raportu.**



**Jolanta Jackowiak**  
Partner  
Doradztwo Cybersecurity  
Departament Doradztwa  
Grant Thornton

# Czym jest Krajowy System CYBERbezpieczeństwa?

## **W sierpniu 2018 r. w życie weszła ustawa o Krajowym Systemie Cyberbezpieczeństwa, która implementuje w Polsce dyrektywę NIS.**

Ustawa ta określa, w jaki sposób tworzony jest w naszym kraju system, mający zapobiegać cyberatakom, które mogą być zagrożeniem dla działalności polskiej gospodarki czy polskiego państwa.

Trzon systemu mają stanowić instytucje państwowe, m.in. Ministerstwo Cyfryzacji, Rządowe Centrum Bezpieczeństwa, Ministerstwo Obrony Narodowej, Agencja Bezpieczeństwa Wewnętrznego czy Narodowy Bank Polski. To one mają tworzyć sieć wykrywania ataków informatycznych rodzące ryzyko dla bezpieczeństwa kraju oraz szybkiego reagowania na nie. Jednak w system włączane są również instytucje prywatne, tzn. firmy, które – jak zdecydowali twórcy regulacji – mają istotne znaczenie dla bezpieczeństwa kraju, np. firmy z branż takich jak energetyka, finanse, transport czy ochrona zdrowia.

Obecnie przedsiębiorstwa, które mają być objęte ustawą, są informowane o tym przez rząd. Uznawane są za tzw. dostawców usług kluczowych, a to oznacza, że będzie na nich spoczywał obowiązek pilnego dostosowania się do określonych wymogów bezpieczeństwa informatycznego. Aby spełnić pierwsze z nich, będą miały tylko 3 miesiące od dnia doręczenia decyzji.

Firmy będą musiały zapewnić odpowiednie środki techniczne i organizacyjne, ocenić ryzyko bezpieczeństwa i zakłócenia ciągłości świadczonej usługi oraz wdrożyć działania zabezpieczające, w tym monitorować poziom bezpieczeństwa i raportować incydenty do organów odpowiedzialnych za bezpieczeństwo na poziomie krajowym. Ponadto, przynajmniej co dwa lata poddawać się audytowi bezpieczeństwa i na wezwanie udostępniać raporty z audytu.



# Jakie sektory wchodzą w skład systemu?

Ustawa definiuje dziewięć sektorów gospodarki, które mają wyjątkowe znaczenie dla bezpieczeństwa kraju – sześć z nich to tzw. operatorzy

usług kluczowych, a trzy to tzw. operatorzy usług cyfrowych. To wśród nich identyfikowane są przedsiębiorstwa, które

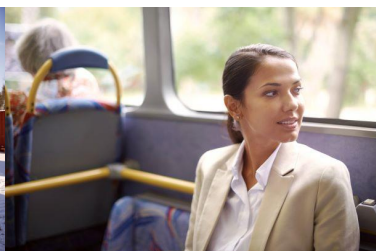
– ze względu na swoją rolę lub wielkość – muszą być objęte wymogami cyberbezpieczeństwa.

## Dostawcy usług kluczowych

**Energetyka**



**Transport**



**Finanse**



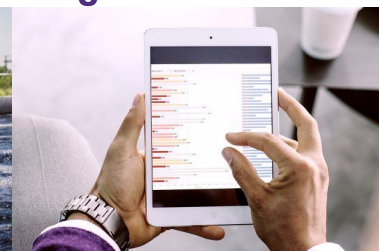
**Ochrona zdrowia**



**Woda pitna**



**Infrastruktura cyfrowa**



## Dostawcy usług cyfrowych

**Internetowe platformy cyfrowe**

**Usługi przetwarzania w chmurze**

**Wyszukiwarki internetowe**

# Jakie podmioty wchodzą w skład systemu?

## Energetyka



- Wydobywanie kopalin
- Produkcja, obrót, dystrybucja, przetwarzanie i magazynowanie energii elektrycznej, zarządzanie infrastrukturą elektryczną
- Wytwarzanie, obrót i dystrybucja ciepła
- Wytwarzanie, obrót i dystrybucja paliw płynnych
- Obrót, przesył, dystrybucja i magazynowanie gazu
- Produkcja urządzeń dla wyżej wymienionych działalności

## Transport



- Przewozy lotnicze, lotnisko i obsługa lotniska, kontrola powietrzna
- Przewozy kolejowe, zarządzanie infrastrukturą kolejową
- Zarządzanie portem, usługi żeglugi morskiej i śródlądowej, kontrola statków
- Zarządzanie infrastrukturą drogową, podmioty wdrażające ITS (inteligentne systemy transportowe)

## Finanse



- Bank krajowy
- Oddział banku zagranicznego
- Oddział instytucji kredytowej, SKOK-i
- Podmiot prowadzący rynek regulowany
- PWPW, BGK, BFG
- Instytucje płatnicze

# Jakie podmioty wchodzą w skład systemu?

## Ochrona zdrowia



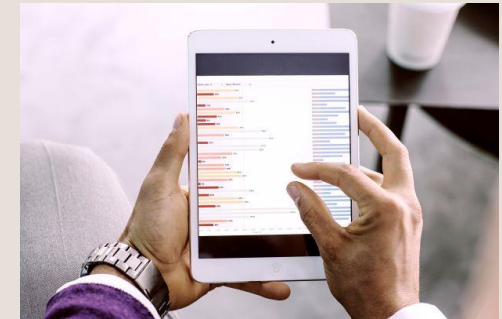
- Podmiot leczniczy
- Przedsiębiorca prowadzący aptekę ogólnodostępną
- Hurtownia farmaceutyczna
- Podmiot, który uzyskał pozwolenie na produkcję produktu leczniczego lub substancji czynnej
- Importer produktu leczniczego lub substancji czynnej
- Importer równoległy produktu leczniczego lub substancji czynnej

## Woda pitna



- Przedsiębiorstwo wodociągowo-kanalizacyjne

## Infrastruktura cyfrowa



- Podmiot świadczący usługi DMS (Domain Name System)
- Podmiot prowadzący punkt wymiany ruchu internetowego (IXP)
- Podmiot zarządzający TLD (Top Level Domain)

# Ile podmiotów czeka wprowadzenie wymogów NIS?

## Wariant minimalny (szacunek rządowy)

Jeśli spojrzeć na Ocenę Skutków Regulacji przygotowaną przez rząd w trakcie tworzenia ustawy o Krajowym Systemie Cyberbezpieczeństwa, w grono dostawców włączone zostanie 360 podmiotów. Najwięcej z nich to szpitale (131) i podmioty finansowe (47).

**Tabela 1:** Liczba podmiotów, które będą wskazane jako dostawcy usług kluczowych Krajowego Systemu Cyberbezpieczeństwa (szacunek według Oceny Skutków Regulacji dołączonych do ustawy)

|                                               |     |
|-----------------------------------------------|-----|
| Służba zdrowia                                | 131 |
| Bankowość i infrastruktura rynków finansowych | 47  |
| Zaopatrzenie w wodę pitną i jej dystrybucja   | 31  |
| Dostawcy usług cyfrowych                      | 25  |
| Transport drogowy                             | 24  |
| Wydobycie i dystrybucja gazu                  | 22  |
| Elektroenergetyka                             | 20  |
| Transport morski                              | 17  |
| Transport lotniczy                            | 15  |
| Transport kolejowy                            | 10  |
| Infrastruktura cyfrowa                        | 10  |
| Wydobycie i dystrybucja ropy naftowej         | 4   |
| Transport śródlądowy                          | 4   |

**RAZEM**

**360**

# Ile podmiotów czeka wprowadzenie wymogów NIS?

## Wariant urealniony

Jeśli jednak bliżej przyjrzeć się szacunkom dokonany przez rząd w ramach OSR, wyraźnie widać, że wyliczone 360 podmiotów to wynik znacząco niedoszacowany. Zgodnie z ustawą, do grona dostawców usług kluczowych mają być włączone np. hurtownie farmaceutyczne czy producenci i importerzy leków, tymczasem w OSR dla kategorii „Ochrona zdrowia” wpisano

jedynie szpitale. Dlatego postanowiliśmy również oszacować, ile podmiotów może być realnie objętych obowiązkami NIS.

Tam gdzie szacunki OSR wydawały się nieprecyzyjne, wykorzystaliśmy dane GUS, zakładając, że obowiązkami NIS objęte byłyby wszystkie średnie i duże podmioty (zatrudniające przynajmniej 50 osób) świadczący dane usługi.

Naszym zdaniem, nadal jest to szacunek dość ostrożny, ponieważ teoretycznie – zgodnie z ustawą do grona dostawców usług kluczowych mogą być włączone również małe przedsiębiorstwa, np. drobne apteki, zatrudniające zaledwie kilka osób.



# Ile podmiotów czeka wprowadzenie wymogów NIS?

## Wariant urealniony c.d.

Licząc w ten sposób, okazuje się, że łącznie obowiązki związane z dyrektywą NIS mogą dotyczyć ponad 2,1 tys. podmiotów.

**Tabela 2:** Liczba podmiotów, które będą wskazane jako dostawcy usług kluczowych Krajowego Systemu Cyberbezpieczeństwa (szacunek Grant Thornton na podstawie OSR i GUS)

|                                               |             |
|-----------------------------------------------|-------------|
| Służba zdrowia                                | 1304        |
| Zaopatrzenie w wodę pitną i jej dystrybucja   | 376         |
| Elektroenergetyka                             | 276         |
| Bankowość i infrastruktura rynków finansowych | 47          |
| Dostawcy usług cyfrowych                      | 25          |
| Transport drogowy                             | 24          |
| Wydobycie i dystrybucja gazu                  | 22          |
| Transport morski                              | 17          |
| Transport lotniczy                            | 15          |
| Transport kolejowy                            | 10          |
| Infrastruktura cyfrowa                        | 10          |
| <b>RAZEM</b>                                  | <b>2126</b> |

# Jakie są obowiązki dostawcy usług kluczowych?

## Najważniejsze obowiązki to:

- **wdrożenie systemu** zarządzania bezpieczeństwem,
- powołanie wewnętrznych **struktur** odpowiedzialnych za cyberbezpieczeństwo lub zawarcie umów z podmiotami świadczącym usługi z zakresu cyberbezpieczeństwa,
- systematyczne **szacowanie ryzyka** wystąpienia incydentu oraz zarządzanie tym ryzykiem,
- wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka **środków technicznych i organizacyjnych**, uwzględniających bezpieczeństwo IT, fizyczne i środowiskowe,
- wdrożenie **polityki** zarządzania incydentami i obsługi incydentów,
- **niezwłocznie zgłaszanie** CSIRT poważnych incydentów, nie później niż w ciągu 24 godzin od wykrycia,
- przeprowadzenie co najmniej raz na dwa lata **audytu bezpieczeństwa** teleinformatycznego,
- usuwanie **podatności** oraz informowanie o ich usunięciu organ właściwy do spraw cyberbezpieczeństwa,
- ustanowienie **nadzoru** nad dokumentacją dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, którą przechowuje przez co najmniej 2 lata. Dokumentacja powinna być zgodnie z normą PN ISO/IEC 27001 dla SZBI i z normą PN-EN ISO 22301 dla planu ciągłości działania usługi kluczowej.

# Jakie kary grożą za niewywiązanie się z obowiązków?

## Przewinienie / niedopatrzenie

## Kara (w zł)

- |                                                                                            |         |
|--------------------------------------------------------------------------------------------|---------|
| ▪ nie przeprowadza systematycznego szacowania ryzyka                                       | 150 000 |
| ▪ nie wdrożył systemu zarządzania bezpieczeństwem                                          | 100 000 |
| ▪ nie opracował dokumentacji                                                               | 50 000  |
| ▪ nie wykonuje obowiązków obsługi incydentu                                                | 15 000  |
| ▪ nie wyznaczył osoby odpowiedzialnej za cyberbezpieczeństwo świadczonych usług kluczowych | 15 000  |
| ▪ nie przeprowadził audytu                                                                 | 200 000 |
| ▪ nie usunął w wyznaczonym terminie nieprawidłowości stwierdzonych w wyniku kontroli       | 200 000 |
| ▪ uniemożliwia lub utrudnia wykonywanie czynności kontrolnych                              | 50 000  |

# Zapraszamy do kontaktu

Potrzebujesz wsparcia?  
**Jesteśmy do dyspozycji**

**Jolanta Jackowiak**

Partner

Doradztwo Cybersecurity

Departament Doradztwa

T+48 601 934 173

E [Jolanta.Jackowiak@pl.gt.com](mailto:Jolanta.Jackowiak@pl.gt.com)



Grant Thornton to jedna z wiodących organizacji audytorsko-doradczych na świecie. Wiedza, doświadczenie i zaangażowanie ponad 3000 partnerów oraz 50 000 pracowników Grant Thornton dostępne są dla klientów w 136 krajach. W Polsce działamy od 25 lat, a ponad 550-osobowy zespół oraz obecność w kluczowych aglomeracjach (Warszawa, Poznań, Katowice, Wrocław, Kraków i Toruń) pozwala nam wspierać w rozwoju ponad 1600 firm i organizacji rocznie.