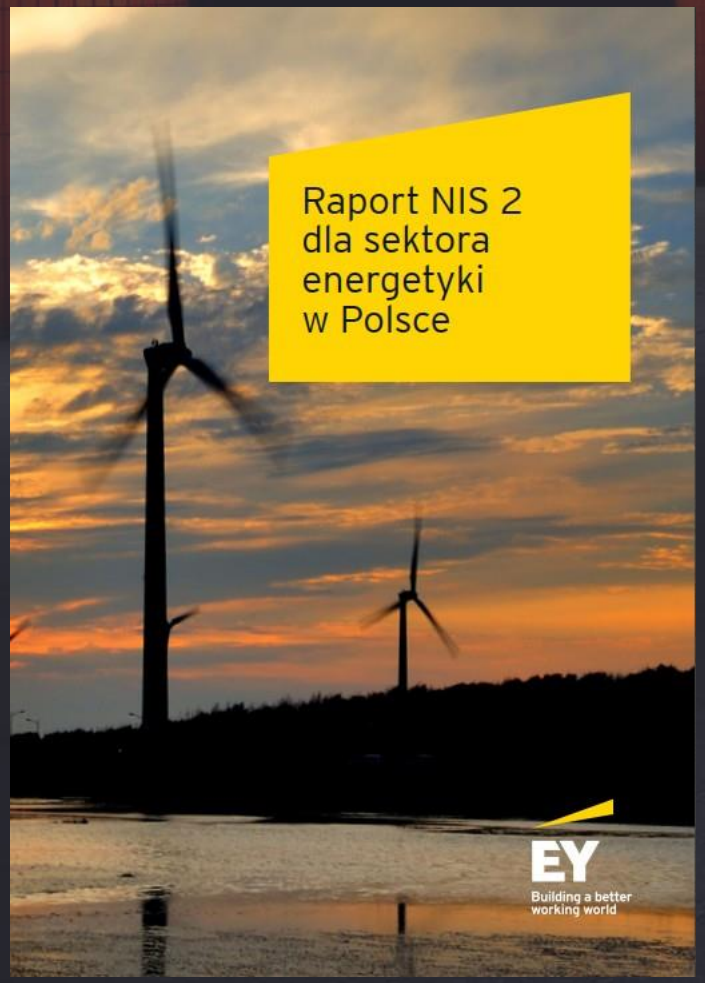
Raport NIS 2 dla sektora energetyki w Polsce

Justyna Wilczyńska-Baraniak, Partner, EY Law

CYBERGAZTERM
Międzyzdroje, 13 maja 2024

Building a better working world

Zapraszamy do pobrania Raportu NIS2 dla sektora energetyki w Polsce



Raport przygotowany przez Zespół Digital kancelarii EY Law Polska **„NIS 2 dla sektora energetyki w Polsce"** podejmuje analizę następujących tematów:

- Wyzwania dla sektora energetyki związane z implementacją dyrektywy NIS 2
- Propozycja rozwiązań dla sektora energetyki i w zakresie implementacji NIS 2 w Polsce
- Stan rynku energetycznego w Polsce

Portal Prawny NIS2

Pobierz raport za pomocą kodu QR

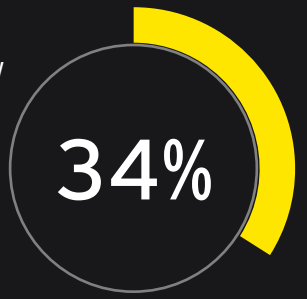
Raport dostępny będzie również od dzisiaj na stronie EY

Top 5 najważniejszych globalnych ryzyk biznesowych w 2023 roku:

1 Incydenty związane z cyberbezpieczeństwem

Przykłady: cyberprzestępczość, awaria IT, naruszenia danych, grzywny

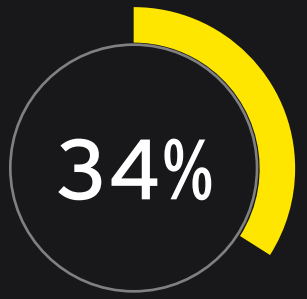
▶ od #1 w 2022 r. (44%)



2 Przerwa w działalności

Przykłady: zakłócenia w łańcuchu dostaw, pandemia, lockdown

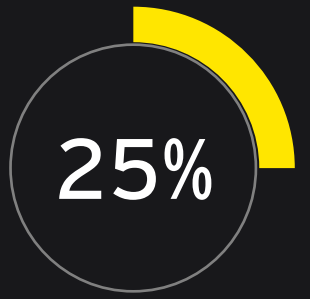
▶ od #2 w 2022 r. (42%)



3 Rozwój sytuacji makroekonomicznej

Przykłady: polityka pieniężna, programy oszczędnościowe

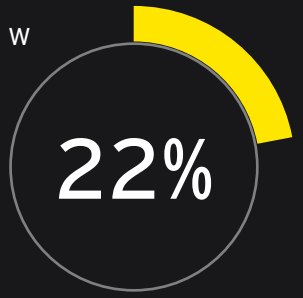
▲ od #10 w 2022 (11%)



4 Kryzys energetyczny

Przykłady: brak/przerwa w dostawach, wahania cen)

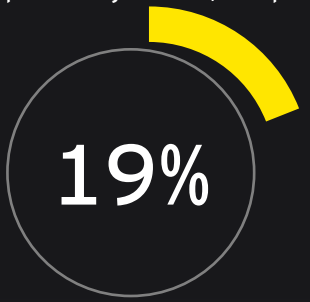
★ Nowość w 2023 roku



5 Zmiany w ustawodawstwie i rozporządzeniach

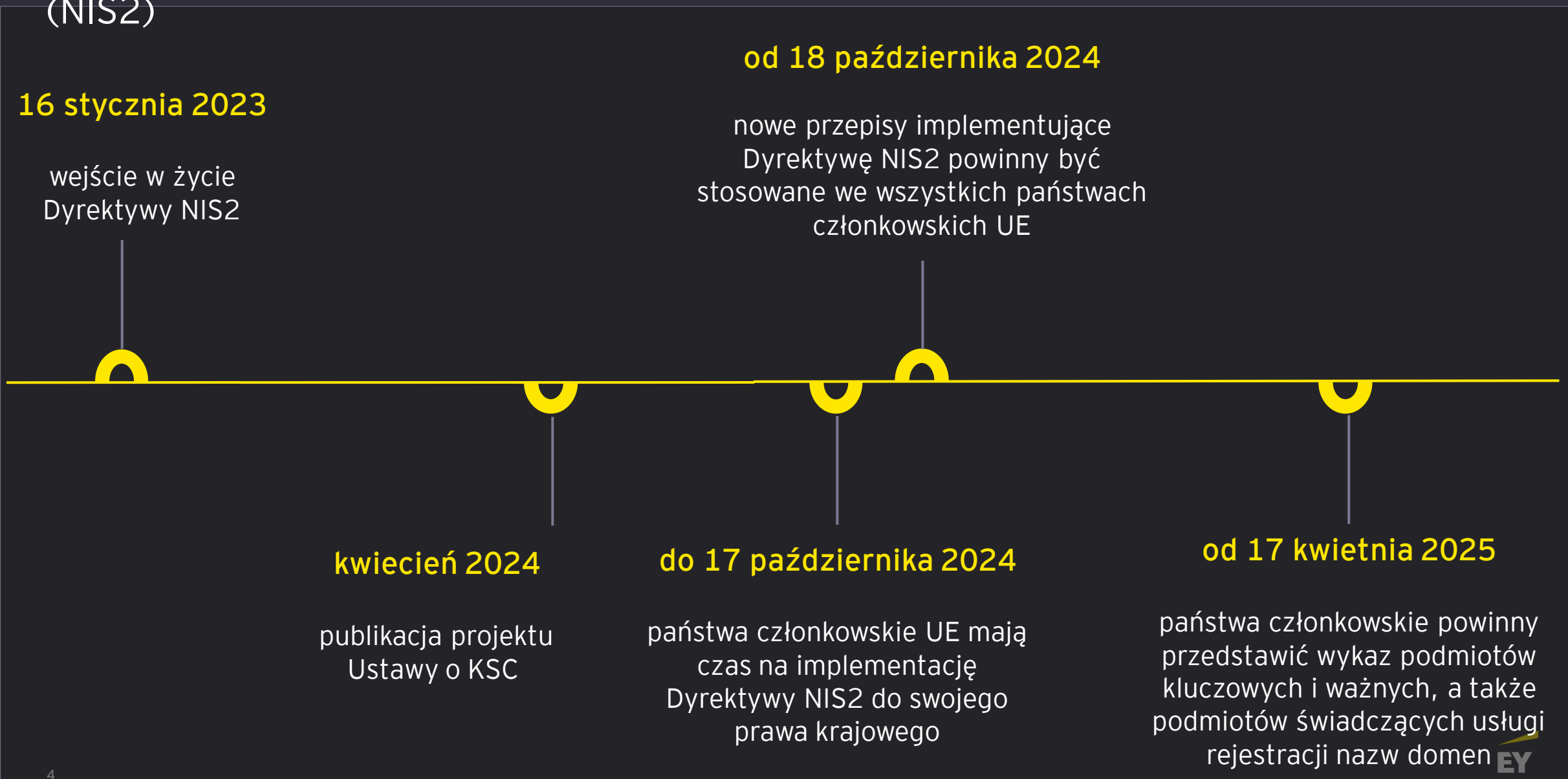
Przykłady: wojny handlowe i cła, sankcje gospodarcze, protekcjonizm, rozpad strefy euro)

▶ od #5 w 2022 (19%)



Źródło: Barometr Ryzyka Allianz 2023: coroczne badanie uwzględnia opinie 2 712 respondentów z 94 krajów i terytoriów.

Dyrektywa Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej (NIS2)



Podmioty z sektora energetyki objęte dyrektywą NIS a NIS2

Energia elektryczna

- przedsiębiorstwa energetyczne
- operatorzy systemów dystrybucyjnych
- operatorzy systemów przesyłowych

- wytwórcy urządzeń z elementami cyfrowymi
- wyznaczeni operatorzy rynku energii elektrycznej
- uczestnicy rynku
- operatorzy punktów ładowania

System ciepłowniczy lub chłodniczy

- operatorzy systemów ciepłowniczych lub chłodniczych

Ropa naftowa

- operatorzy ropociągów
- operatorzy instalacji służących do produkcji, rafinacji, przetwarzania, magazynowania i przesyłu ropy naftowej

- krajowe centrale zapasów

Gaz

- przedsiębiorstwa dostarczające gaz
- operatorzy systemów dystrybucyjnych
- operatorzy systemów przesyłowych
- operatorzy systemów magazynowania
- operatorzy systemów LNG
- przedsiębiorstwa gazowe

Wodór

- operatorzy instalacji służących do produkcji, magazynowania i przesyłu wodoru

Zidentyfikowane wyzwania związane z implementacją NIS 2

Obszar 1: Transpozycja NIS 2 i innych aktów z zakresu cyberbezpieczeństwa energetycznego do polskiego porządku prawnego	Obszar 2: Wypracowanie modelu zarządzania ryzykiem łańcucha dostaw ICT w sektorze energetycznym	Obszar 3: Digitalizacja sektora energetycznego	Obszar 4: Transformacja energetyczna państwa a cyberbezpieczeństwo
► Wysokie ryzyko "przeregulowania" sektora energetycznego na poziomie krajowym ► Zbieg przepisów NIS 2 z przepisami dyrektywy o odporności podmiotów krytycznych (Dyrektywa CER) ► Trwające prace nad projektem kodeksu sieci w zakresie cyberbezpieczeństwa transgranicznych przepływów energii elektrycznej ► Rozszerzony katalog podmiotów z sektora energetycznego zobowiązanych do dostosowania do wymogów dyrektywy NIS 2 ► Szczególna rola sektora energetycznego dla funkcjonowania Unii i państw członkowskich	► Wysokie koszty wypracowania modelu zarządzania łańcuchem dostaw ► Rosnąca liczba ataków w łańcuchu dostaw ► Brak oszacowania ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw w energetyce ► Ryzyko wykluczenia małych i średnich przedsiębiorstw (MŚP) z łańcucha dostaw ► Brak jednolitych standardów i certyfikacji	► Cyberbezpieczeństwo zastosowania technologii cyfrowych w energetyce ► Potencjalne zastosowanie Aktu w sprawie sztucznej inteligencji do rozwiązań sztucznej inteligencji (SI) w energetyce ► Zapewnienie bezpieczeństwa inteligentnych sieci energetycznych (smart grids) ► Dostarczanie produktów z elementami cyfrowymi dla sektora energetycznego w świetle projektu Cyber Resilience Act ► Wzmożona konsumpcja energii przez nowoczesne rozwiązania technologiczne	► Rozwój krajowej sieci elektroenergetycznej a jej bezpieczeństwo cybernetyczne ► Rosnąca liczba ataków cybernetycznych w Polsce ► Deficyt specjalistów z zakresu cyberbezpieczeństwa ► Konieczność reorganizacji działań krajowych organów ds. cyberbezpieczeństwa

Propozycja rozwiązań dla sektora energetyki i w zakresie implementacji NIS 2 w Polsce

Harmonizacja przepisów

Rekomendacja 1:
Harmonizacja przepisów implementujących dyrektywę NIS 2 z innymi przepisami w zakresie cyberbezpieczeństwa oraz charakterystyki sektora energetycznego

Podejście oparte na rzeczywistym i mierzalnym ryzyku

Rekomendacja 4:

Utworzenie systemu, w którym NIS 2 stanowi regulację ogólną dla cyberbezpieczeństwa i współgra z założeniami regulacji szczegółowych

Certyfikacja

Rekomendacja 2:
Potrzeba stosowania unijnej certyfikacji dotyczącej cyberbezpieczeństwa dla sektora energetycznego

Zasada proporcjonalności i minimalnej harmonizacji

Rekomendacja 5:
Ograniczenie zakresu dyrektywy na podstawie zasady proporcjonalności i minimalnej harmonizacji

Publiczny i prywatny sektor energetyczny

Rekomendacja 3:
Uwzględnienie różnic w objęciu dyrektywą NIS 2 pomiędzy publicznym a prywatnym sektorem energetycznym

Doświadczenia innych Państw w UE

Rekomendacja 6:
Bazowanie na doświadczeniu pozostałych państw członkowskich w implementacji NIS 2 w sektorze energetycznym

Podsumowanie

Sektor energetyczny odgrywa kluczową rolę z punktu widzenia planowania strategicznego oraz bezpieczeństwa państwa.

Sektor energetyczny jest celem licznych cyberataków

Inne sektory oraz infrastruktura krytyczna kraju są uzależnione od sektora energetycznego. Ewentualne przerwy w dostawach energii wywołane cyberatakami mogą zaburzyć działalność biznesową jak i bezpieczeństwo oraz komfort życia obywateli.

NIS2 powinno być transponowane w ramach harmonizacji minimalnej i stanowić ogólny akt prawny regulujący cyberbezpieczeństwo w Polsce.

Dziękuję za uwagę!

Justyna Wilczyńska-Baraniak

Partner, EY Law Poland

Justyna.Wilczynska-Baraniak@pl.ey.com
+48 519 098 119