Praktyczne kroki zgodności z NIS 2 w kontekście IT: obowiązki i plan działań

Adam Woźniak
Grant Thornton

Obowiązki przedsiębiorców wynikające z NIS2 - co regulują nowe przepisy i jak je raportować?

Co ogólnie narzuca na mnie NIS-2?

A może NIS-2 odnosi się do istniejących Standardów bezpieczeństwa?

Zgodność z Normą ISO27001

Bezpieczeństwo Informacji

Zgodność z Normą ISO22301

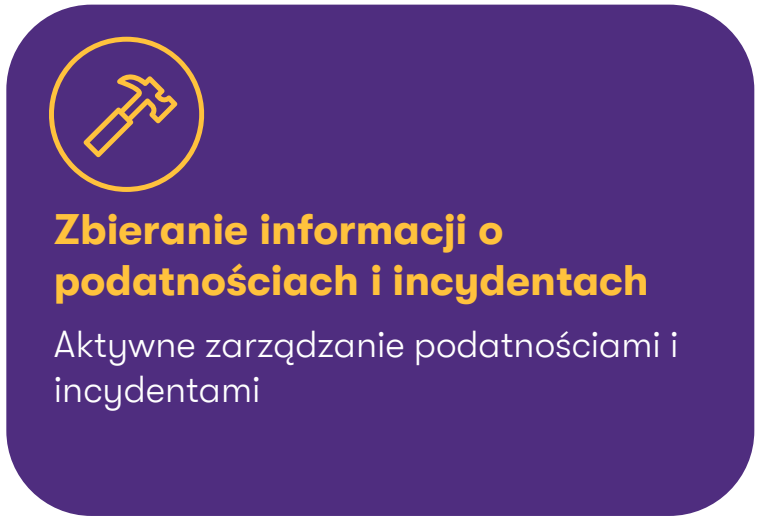
Bezpieczeństwo ciągłości działania

Zbieranie informacji o podatnościach i incydentach

Aktywne zarządzanie podatnościami i incydentami

Co ogólnie narzuca na mnie NIS-2?

A może NIS-2 odnosi się do istniejących Standardów bezpieczeństwa?



Zbieranie informacji o podatnościach i incydentach

Aktywne zarządzanie podatnościami i incydentami

A coś więcej?

- Wdrożenie proporcjonalnych do wielkości firmy środków zarządzania ryzykiem, uwzględniające również prawdopodobieństwo wystąpienia incydentów i ich dotkliwość
- Powiadamianie odbiorców usług o wystąpieniu incydentu
- Wdrożenie obowiązkowych szkoleń dla kadry kierowniczej w zakresie cyberbezpieczeństwa
- Monitorowanie systemów IT w trybie ciągłym

Zgłaszanie incydentów do odpowiednich organów, wskazanych przez regulatora

A czym są te normy i co wprowadzają?

ISO27001

- Zapewnia ramy dotyczące Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)
- Narzuca zasady, które organizacja musi bezwzględnie spełniać
- Sugeruje szereg zabezpieczeń, które należy wdrożyć celem osiągnięcia pożądanego poziomu bezpieczeństwa
- Wspiera rozwój świadomości użytkowników
- Efektywnie poprawia bezpieczeństwo procesów biznesowych
- Uspójnia podejście organizacji do zagrożeń

A czym są te normy i co wprowadzają?

ISO22301

- Zapewnia ramy dotyczące zarządzania ciągłością działania
- Wspiera zapobieganie występowania incydentów
- Wspiera w rozwiązywaniu incydentów, które wystąpiły
- Chroni ciągłość działania organizacji, w efekcie również całego sektora
- Uświadamia całą organizację o możliwych istniejących zagrożeniach
- Przygotowuje organizacje na najgorsze scenariusze

A czym są te magiczne „incydenty” w kontekście NIS-2?

- **Incydent** – Zdarzenie mogące naruszyć jedną z cech informacji (poufność, dostępność, integralność) w kontekście świadczonej usługi przez podmiot kluczowy lub ważny

- **Incydent poważny** – Incydent, który może mieć **istotny wpływ** na świadczenie usługi przez podmiot kluczowy lub ważny

Grant Thornton

Co mam zrobić z tymi incydentami?

Incydenty należy zgłaszać w dwóch trybach:

- Niezwłocznie (do 24h) – wczesne ostrzeżenie definiujące zagrożenie wraz z informacją o charakterze (np. działanie bezprawne)
- Niezwłocznie (do 72h) – faktyczne zgłoszenie incydentu wraz z wstępną oceną dotkliwości, skutków
- Sprawozdanie okresowe
- Sprawozdanie końcowe

Podsumowując – to co mam spełniać?

Należy zaprojektować i wdrożyć System Zarządzania Bezpieczeństwem Informacji

W tym polityk i procedur niezbędnych do oceny skuteczności środków zarządzania ryzykiem

Należy wdrożyć środki niezbędne do zarządzania ryzykiem ciągłości działania

Należy zaprojektować i zaimplementować proces zarządzania i obsługi incydentów, a także przede wszystkim – systemu zgłaszania incydentów poważnych

Należy zapewnić stosowne środki dotyczące bezpieczeństwa zasobów ludzkich, zarządzania aktywami i kontrolą dostępu

Podsumowując – to co mam spełniać?

Należy zapewnić stosowny proces w zakresie bezpieczeństwa procesu nabywania i rozwoju sieci i systemów IT

Należy zaprojektować i wdrożyć system szkolenia pracowników, w tym przede wszystkim managerów

Ocenić i wdrożyć praktyki związane z kryptografią i szyfrowaniem

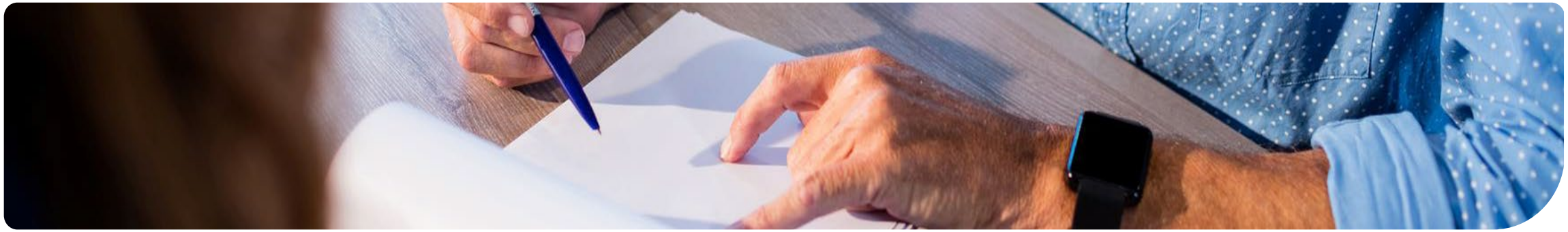
Przeszkody i wyzwania - jak krok po kroku przygotować swoją firmę na nowe obowiązki?

Jakie są przeszkody

1. Brak klarownej informacji dotyczącej ostatecznego wyglądu ustawy
2. Brak pewności kto będzie podlegał wymogom ustawy
3. Brak wystarczającej liczby dobrych specjalistów i konsultantów na rynku
4. Brak biegłej znajomości wymaganych przez regulację norm i standardów
5. Długi okres wdrażania wymagań
6. Wysokie koszty niezbędne do poniesienia celem wdrożenia wymagań
7. Obowiązek analizy i decyzji o podleganiu obowiązkom Dyrektywy po stronie organizacji
8. Mnogość regulacji

Problemy i wyzwania polskich firm w kontekście cyberzagrożeń

- Brak jasnych reguł i zasad bezpieczeństwa
- Brak rzetelnej analizy otoczenia regulacyjnego
- Brak osoby odpowiedzialnej za bezpieczeństwo
- Brak procedur zarządzania incydentami, podatnościami i procedur awaryjnych
- Nieprawidłowości w procesie utrzymania i aktualizacji systemów
- Niekompletne kopie zapasowe i brak kopii zapasowych w dodatkowej lokalizacji
- Przestarzała infrastruktura informatyczna
- Brak wieloczynnikowego uwierzytelnienia
- Brak testów bezpieczeństwa
- Nieprawidłowości w zarządzaniu dostawcami
- Brak ubezpieczenia od cyberzagrożeń
- Niska świadomość użytkowników i niewystarczające szkolenia w zakresie bezpieczeństwa
- Niezłomna wiara, że nas to nie dotyczy



Czy moja firma podlega pod NIS2? SPRAWDŹ w 2 minuty - Grant Thornton

Zapraszam do kontaktu

CLIENT WEEK
z Grant Thornton

Adam Woźniak

Executive Director
Grant Thornton
M +48 600 805 785
E adam.wozniak@pl.gt.com

Na co dzień dzielimy się wiedzą na:

GrantThornton.pl

Znajdą tam Państwo między innymi cykl artykułów dotyczących dyrektywy NIS2.

Zapraszamy też do zapisu na newsletter.