NIS 2 i nowela UoKSC

jak daleko jest rzeczywistość CyberSec w polskich firmach?

- 13 subiektywnych „grzechów głównych” polskich organizacji
- Dlaczego Zarządy i CTIOs obawiają się NIS 2, ale nie chcą się do tego przyznać ;-)?
- Fałszywe przekonania i fakty

Tomasz Matuła, Wisła, 04.11.2025

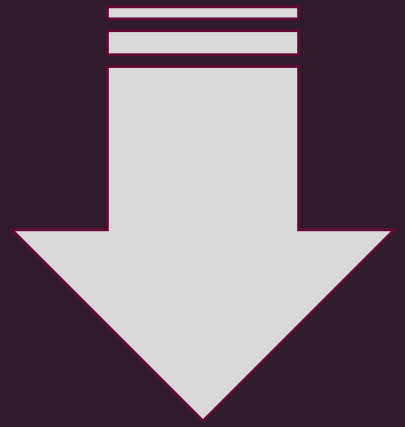
„Po co w ogóle wprowadzane są nowe regulacje?”

2016

6 lipca 2016 - wejście w życie Dyrektywy NIS

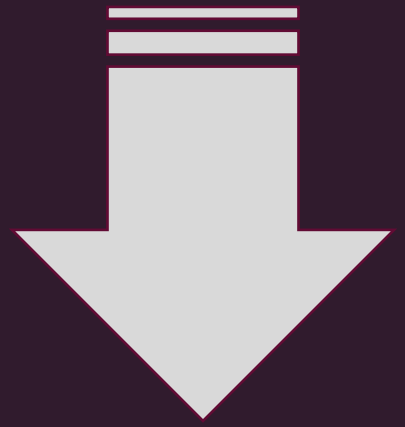
2024

18 października 2024 – NIS 2 wchodzi w życie w UE



❖ **„Grzech” nr 1:** wypieranie i lekceważenie zmieniającej się CYBER rzeczywistości przez TOP Management

„Kary $$$$$$ i odpowiedzialność zarządzających”



- **„Grzech” nr 2:** niechęć do brania odpowiedzialności przez Zarząd

„Zdecydowanie za dużo wymagań i obowiązków”

„Duże obciążenia administracyjne i proceduralne”

„Zdecydowanie za dużo wymagań i obowiązków”

1. Obowiązek samo rejestracji [Art. 7]
2. Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji 5→21 [Art. 8]
3. Wyznaczenie osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami Krajowego Systemu Cyberbezpieczeństwa [Art. 9]
4. Opracowanie, stosowanie i aktualizacja dokumentacji dot. bezpieczeństwa systemu informacyjnego [Art. 10]
5. Obowiązek obsługi incydentów, zgłaszania incydentów poważnych i współdziałanie przy obsłudze incydentu poważnego 10 [Art. 11-13]
6. Powołanie wewnętrznej struktury odpowiedzialnej za cybersec lub zawarcie umowy z dostawcą usług zarządzania w zakresie cybersec [Art. 14]
7. Audyt bezpieczeństwa systemu informacyjnego [Art. 15]
8. Informowanie użytkowników usług o cyberzagrożeniu, incydencie [Art. 11]

„Zdecydowanie za dużo wymagań i obowiązków”

Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w systemie informacyjnym

6 Wdrażanie, dokumentowanie, testowanie i utrzymywanie planów ciągłości działania… planów awaryjnych, oraz planów odtworzenia działalności …

5 Bezpieczeństwo i ciągłość łańcucha dostaw produktów, usług i procesów ICT

4 Bezpieczeństwo zasobów ludzkich

3 Bezpieczeństwo fizyczne i środowiskowe uwzględniające kontrole dostępu

2 Bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym testowanie systemu informacyjnego

1 Polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne

7 Objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym

8 Polityki i procedury oceny skuteczności środków technicznych i organizacyjnych

Wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i

9 Edukacja z zakresu cyberbezpieczeństwa dla personelu podmiotu

10 Podstawowe zasady cyber higieny

11 Polityki i procedury stosowania kryptografii, (w s.p.) szyfrowania

12 Stosowanie bezpiecznych środków komunikacji… (w s.p.) uwzględniających uwierzytelnianie wieloskładnikowe

13 Zarządzanie aktywami

14 Polityki kontroli dostępu

❖ **„Grzech” nr 3:** brak świadomego ZARZĄDZANIA obszarem cyberbezpieczeństwa i ochrony informacji

„Obowiązkowy cyber audyt zabije mój biznes”

Audyt bezpieczeństwa systemu informacyjnego [Art.15]

- ✓ **Podmioty kluczowe**
  - ✓ przeprowadzać audyt bezpie[illegible]raz na ~~dwa~~ trzy lata
  - ✓ pierwszy audyt w ciągu ~~12~~ 24 m[illegible]y
  - ✓ **Uwaga:** możliwy audyt ad hoc w drodze decyzji

❖ **„Grzech” nr 4:** podejście *„lepiej nie robić audytu zewnętrznego bo jeszcze coś wyjdzie i będę mieć problem”*

„Po co tak krótkie czasy zgłaszania incydentów”

Obsługa incydentów, zgłaszanie incydentów poważnych [Art.11, 12, 13]

Zgłoszenie incydentu poważnego

- nie później niż **w ciągu 72 godz.** od wykrycia

Przekazanie sprawozdania okresowego

Przekazanie sprawozdania końcowego z obsługi

Usuwanie podatności art. 32 ust. 2

Obsługa incydentów poważnych

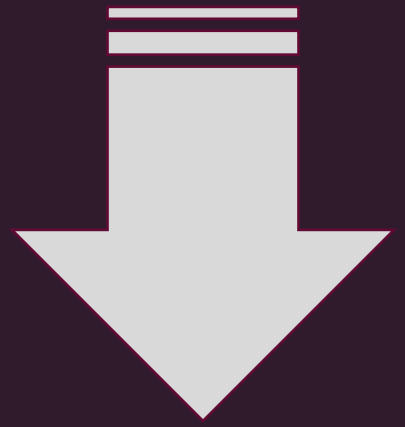
Zapewnienie obsługi incydentów

Klasyfikacja incydentów poważnych

Zgłoszenie wczesnego ostrzeżenia o incydencie

- ❖ **„Grzech” nr 5:** sprowadzenie ZARZĄDZANIA INCYDENTAMI do ich "obsługi"
- ❖ **„Grzech” nr 6:** brak pełnego monitorowania w trybie ciągłym i w czasie rzeczywistym

„Bardzo wysokie koszty dostosowania się”



- **„Grzech” nr 7:** wcześniejszy brak poważnego traktowania cyber zagrożeń, cyberbezpieczeństwa i ochrony informacji przez „Zarząd”

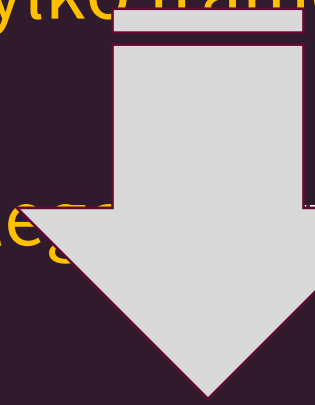
„Brak w NIS 2 i noweli UoKSC wskazań konkretnych cyber rozwiązań do wdrożenia”

- ✓To analiza ryzyka jest podstawą do wyboru zabezpieczeń i ich wdrożenia
- ✓Każda organizacja jest in
- ✓All Risks Approach
- ✓*System monitorowania, szyfrowanie, uwierzytelnianie wieloskładnikowe, …*

- ❖ **„Grzech” nr 8:** szacowanie cyber ryzyk traktowane „po macoszemu”

„Przecież wystarczy mieć (wdrożyć) ISO 27001”

- ✓W projekcie UoKSC zamiast odwołania do norm ISO, wprowadzono obowiązek ustanowienia SZBI w oparciu o dowolny framework
- ✓ISO 27001 lub NIST CSF to tylko frameworki, które mogą pomóc przy wdrożeniu SZBI
- ✓Wdrożenie SZBI w SI nie polega na wypełnieniu i przechowywaniu dokumentacji
- ✓SZBI powinien być jak ubranie szyte na miarę

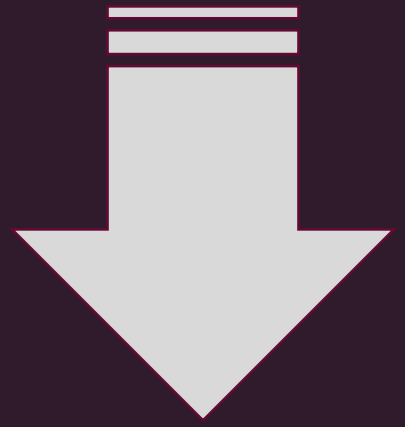


- ❖ **„Grzech” nr 9:** sprowadzenie wdrożenia ISO 27001 do przygotowania odpowiedniej dokumentacji
- ❖ **Mit:** przekonanie, że ISO 27001 zapewni zgodność z NIS 2 i nowelą UoKSC

„Przecież mam SIEM-a”

„Korzystam z usług SOC zewnętrznego”

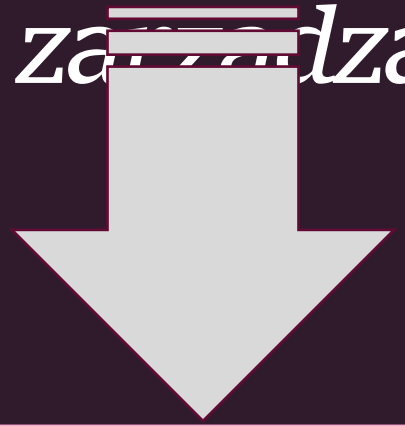
„Technologie/usługi NIS 2 ready”



- **„Grzech” nr 10:** brak kompleksowego monitorowania w trybie ciągłym i w czasie rzeczywistym ≠ SIEM !!!
- **Mit:** podpisanie umowy na usługi ”SOC” z firmą zewnętrzną zapewni spełnienie obowiązków NIS 2/UoKSC
- **„Grzech” nr 11:** przekonanie, że istnieją rozwiązania NIS 2 ready

„Ale my mamy plany ciągłości działania. Proces zarządzania kryzysowego na pewno też”

„Backup-em, kopiami zapasowymi i redundancją świetnie zarządzamy”



- **„Grzech” nr 12:** brak TESTOWANIA planów ciągłości działania oraz sytuacji kryzysowych w „realu”
- **„Grzech” nr 13:** brak regularnych testów odzyskiwania kopii zapasowych, systemów i aplikacji oraz redundancji

„Grzechy główne ;-)” wielu organizacji

- **Zarządy i TOP Management**
  - ✓wypieranie i lekceważenie zmieniającej się CYBER rzeczywistości
  - ✓brak poważnego traktowania cyber zagrożeń i cyber odporności
  - ✓niechęć do brania odpowiedzialności
  - ✓brak świadomego ZARZĄDZANIA obszarem cyberbezpieczeństwa i ochrony informacji

„Grzechy główne ;-)” wielu organizacji

- **CTIO i czasami CISO**
  - ✓brak świadomego ZARZĄDZANIA obszarem cybersec i ochrony inf.
  - ✓szacowanie cyber ryzyk traktowane po macoszemu
  - ✓sprowadzenie ZARZĄDZANIA INCYDENTAMI do ich "obsługi"
  - ✓brak pełnego monitorowania w trybie ciągłym i w czasie rzeczywistym
  - ✓przekonanie, że ISO 27001 zapewni zgodność z NIS 2 i UoKSC
  - ✓przekonanie, że istnieją rozwiązania NIS 2 ready
  - ✓brak TESTOWANIA planów ciągłości działania oraz sytuacji kryzysowych w „realu”
  - ✓brak regularnych testów odzyskiwania kopii zapasowych, systemów i aplikacji oraz redundancji

NIS 2 i nowela UKSC to również szanse dla organizacji oraz CTIO i CSO

Zapraszam do kontaktu

tomasz.matula@ictmasters.com