Zabezpieczenie ciągłości funkcjonowania placówki medycznej

Tomasz Kawa, Archer Sp. z o.o.
Marcin Klimowski, CISCO

KSC – co to jest?

- Krajowy System Cyberbezpieczeństwa (Polska)
- Najważniejszym celem jest przede wszystkim **zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych na poziomie krajowym**.
- Od lipca 2023 r. projekt skierowany do prac sejmowych (znany zarys i sporo szczegółów).
  ETA: koniec 2024 r., ma wejść w 2025 r.
- Certyfikacja kluczowych podmiotów (zgodnie z różnymi wymogami/standardami, w tym ISO-27001 czy zalecenia NIS2)

NIS2 - co to jest?

- **Dyrektywa UE dotycząca bezpieczeństwa sieci i informacji**
- Dotyczy podmiotów kluczowych i ważnych
- Państwa członkowskie mają obowiązek dostosować swoje ustawodawstwo do 17.10.2024 r.
- Istotne zmiany względem obowiązującego NIS1
- Brak oficjalnego procesu certyfikacji (np. w przeciwieństwie do ISO-27001)

Konsekwencje dla Was: żaden „papierek” od firm zajmujących się audytem NIS2 nie ma wagi prawnej

Kogo dotyczy NIS2?

PODMIOTY KLUCZOWE

- Administracja publiczna
- Energia
- Transport
- Bankowość
- **Zdrowie**

PODMIOTY WAŻNE

- Firmy powyżej 50 pracowników lub z obrotem powyżej 10M E, lub świadczące krytyczne usługi
- Poczta/firmy kurierskie
- Produkcja żywności
- Zarządzanie odpadami
- Dostawcy usług cyfrowych
- Produkcja elektroniki, sprzętu medycznego, pojazdów
- Badania naukowe

NIS2 a certyfikacja ISO-27001

CERTYFIKACJA ISO-27001

- Międzynarodowy standard zarządzania bezpieczeństwem informacji
- Obejmuje 2 fazy audytu
- Zakończony certyfikacją

NIS2

- Szczegółowe wymagania dla systemu ochrony zdrowia
- Raportowanie incydentów (24h SLA)
- Pełne zarządzanie ryzykiem łańcucha dostaw
- Zarządzanie kryzysowe (NIS sections: „crisis management” + „resilience requirements”)
- Bezpośrednia odpowiedzialność członków zarządu

NIS2 – odpowiedzialność i kary

- **Maksymalnie 10 mln euro dla podmiotów kluczowych**
- Maksymalnie 7 mln euro dla podmiotów ważnych
- Do wartości 2% lub 1.4% rocznego obrotu
- Dodatkowe kary
- Utrata certyfikacji/akredytacji
- **Odpowiedzialność osób fizycznych (kadry kierowniczej), włącznie z zakazem prowadzenia działalności gospodarczej**

W jakim miejscu są placówki medyczne?

NIS2 Kategorie

A: Zarządzanie ryzykiem	B: Ochrona przed atakami	C: Wykrywanie ataków	D: Minimalizacja szkód

NIS2 Szczegółowe cele

A1 Zarządzanie procesem	A2 Zarządzanie ryzykiem	B1 Polityki, procesy, procedury	B2 Uwierzytelnianie tożsamości	C1 Monitorowanie, przeglądanie alertów		D1 Odpowiedź na atak i przywracanie usług	
A3 Zarządzanie zasobami	A4 Łańcuchy dostaw	B3 Bezpieczeństwo danych	B4 Bezpieczeństwo systemów	C2 Proaktywne wykrywanie		D2 Wyciąganie wniosków	
		B5 Dostępność sieci i systemów	B6 Świadomość pracowników, szkolenia				

ŚREDNIEJ WIELKOŚCI SZPITAL

- Czy macie platformę, która zbiera i agreguje różne logi dotyczące bezpieczeństwa?
- Czy macie ludzi/zespół, który patrzy w te logi, wykrywa ataki i reaguje na nie?
- Czy macie zespół, który wyciąga wnioski, optymalizuje platformę (ulepsza „playbooki”)?

C1

Monitorowanie, przeglądanie alertów

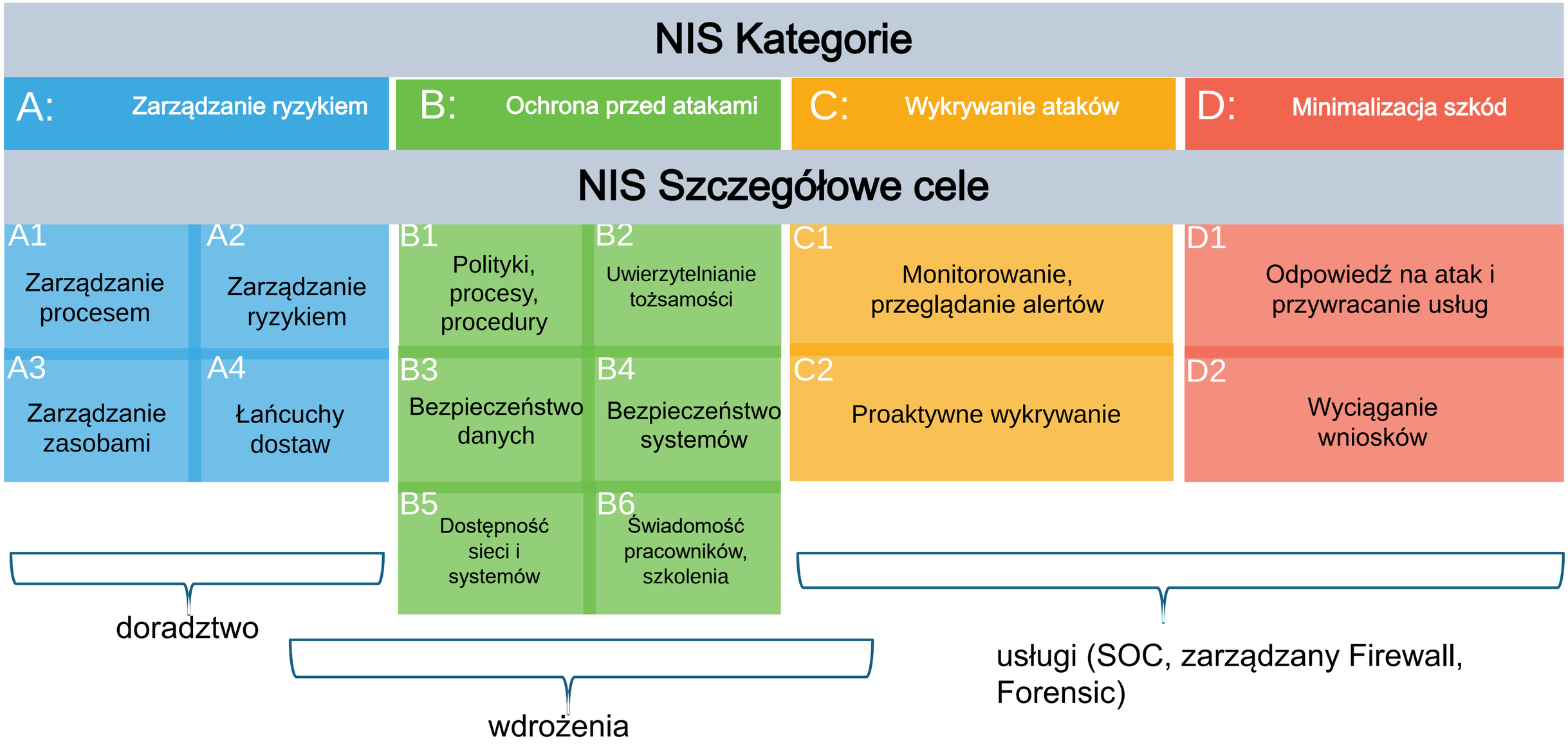
ŚREDNIEJ WIELKOŚCI SZPITAL

- Czy ten zespół jest w stanie zareagować w ciągu 24h i zgłosić incydent (wymaganie NIS2)?
- A co jeśli atak nastąpił w piątek o 22:00?
- Ilu ludzi musicie zatrudnić, aby spełnić to wymaganie?
- Ile czasu zajmie Wam przywracanie usług?
- Ile operacji/zabiegów będzie zagrożonych?
- Część Business Continuity Planu (np. brak zasilania, powódź)

D1

Odpowiedź na atak i przywracanie usług

W czym pomaga Archer?



KOMPETENCJE

Możemy pochwalić się najwyższymi kwalifikacjami w branży, które potwierdzają liczne certyfikaty:

KONTAKT

SKONTAKTUJ SIĘ Z NAMI

sales@archerit.pl

+48 786 808 772

www.archerit.pl