Wymagania bezpieczeństwa w małej lub średniej Organizacji – jak je spełnić wobec ograniczoności zasobów i możliwości.

Maciej Michalczak, CISSP, EMBA

Conotoxia / Cinkciarz.pl

Przedstawienie mojej Organizacji

Conotoxia Holding, w której funkcjonują jednostki organizacyjne świadczące usługi finansowe, między innymi spółki działające w Polsce **Cinkciarz.pl** oraz **Conotoxia**.

Wprowadzenie

Designed by Freepik

Strategia odporności i bezpieczeństwa cybernetycznego.

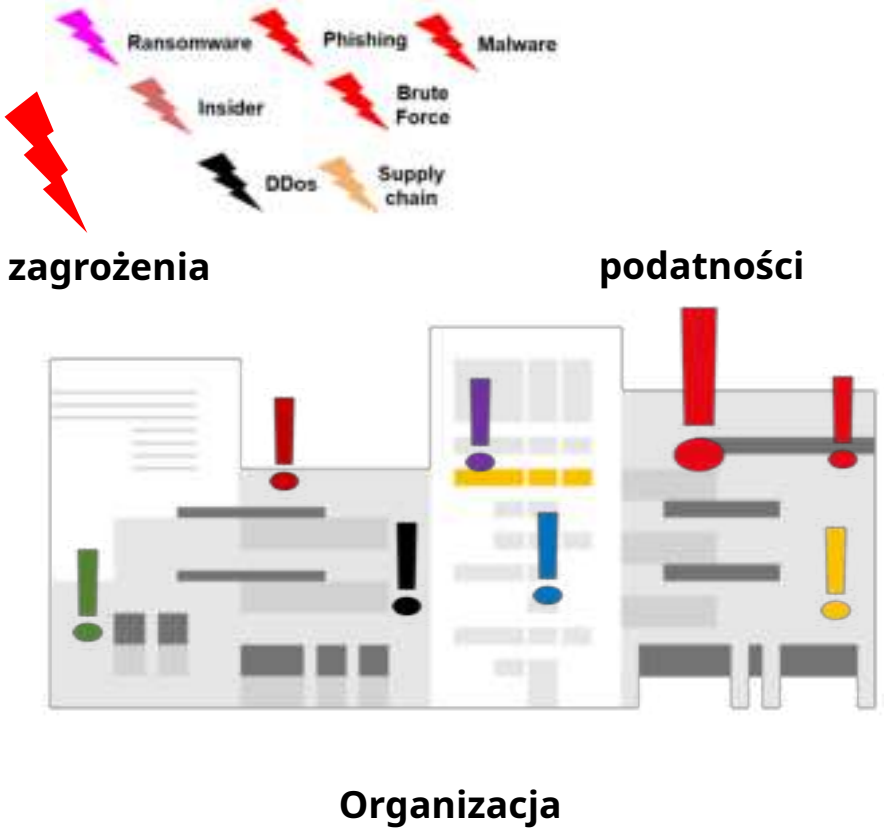
System bezpieczeństwa Organizacji:

- ❑ Budowa i utrzymanie ochrony
- ❑ Reakcja na incydenty i ataki cybernetyczne
- ❑ Testy i audyty gotowości

Trzy sposoby podejścia do bezpieczeństwa Organizacji

Określenie **źródeł wymagań**, specyficznych dla Organizacji, na podstawie których Organizacja definiuje **wymagania bezpieczeństwa**, które jest zobowiązana spełnić.

Zagrożenia i podatności



Identyfikacja **zagrożeń** dotyczących Organizacji:

- ❑ wiadomości prasowe
- ❑ raporty branżowe agencji (np. **ENISA**, **NASK**)
- ❑ badania, statystyki, rekomendacje dostawców (np. **Splunk**, **ESET**, **Cisco**)

Określenie **podatności** w zasobach Organizacji:

- ❑ testy bezpieczeństwa (wewnętrzne/zewnętrzne)
- ❑ informacje o znalezionych podatnościach w:
  - ❑ produktach i usługach od dostawców
  - ❑ używanym oprogramowaniu open-source

- ❑ Rekomendacje dla MŚP **CIS**, **FCC**, **NIST**

Zagrożenie + podatność + zasób = ryzyko

Identyfikacja i definicja **ryzyka** zazwyczaj wymaga:

- ❑ zidentyfikowania **zagrożenia**
- ❑ określenia **zasobu**
- ❑ wykrycia **podatności** na zasobie

Zdefiniowanie **poziomu ryzyka** wymaga określenia:

- ❑ **prawdopodobieństwa**
- ❑ **konsekwencji biznesowych**

Poziom **apetytu na ryzyko** vs. poziom ryzyka

Poziom ryzyka > apetytu na ryzyko Organizacji zazwyczaj wymaga obsługi danego ryzyka poprzez np. zbudowanie odpowiedniego procesu bezpieczeństwa lub mechanizmu kontrolnego sprowadzającego poziom danego ryzyka do poziomu apetytu na ryzyko.

Prawo i Regulacje

Działalność w oparciu o dane klientów:

- ❑ **GDPR / RODO**

na rynku regulowanym:

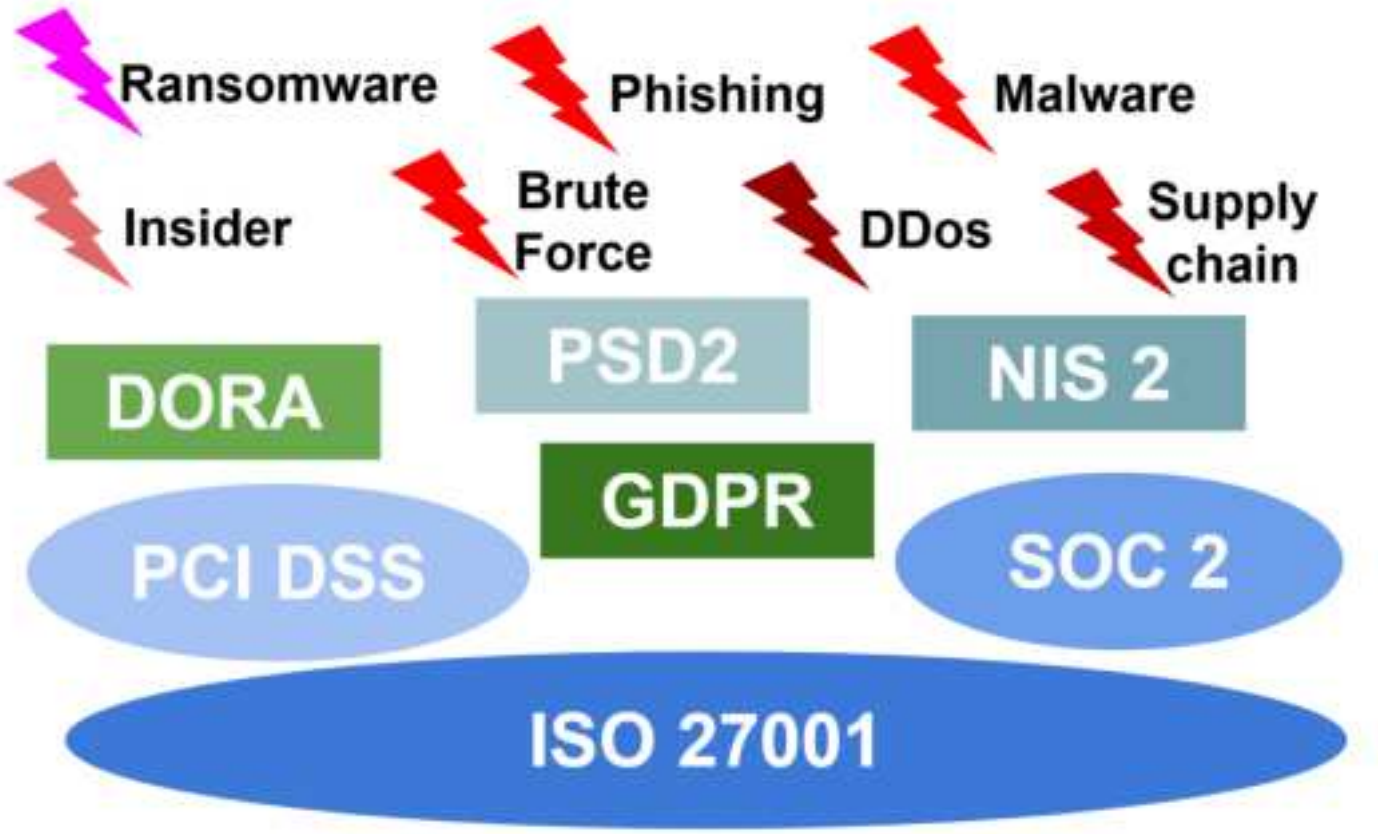
- ❑ finanse – **DORA**, **PSD2**, **UOUP**, **Rekomendacja D**
- ❑ służba zdrowia – **HIPPA** USA

ale też działalność jako sektorowy dostawca usługi krytycznej lub ważnej - **NIS2**

Standardy / Normy bezpieczeństwa

- Bazowy standard, np. **ISO/IEC 27001**
- … a kolejne standardy, o ile potrzebne jako rozszerzenia:
  - wspólna baza **mechanizmów kontrolnych**, specyficznych dla Organizacji
    wymaga mniej zasobów, ale trudniejsze zarządzanie
  - lub implementacja per standard/norma
    wymaga więcej zasobów, ale łatwiejsze zarządzanie

A może podejście hybrydowe …

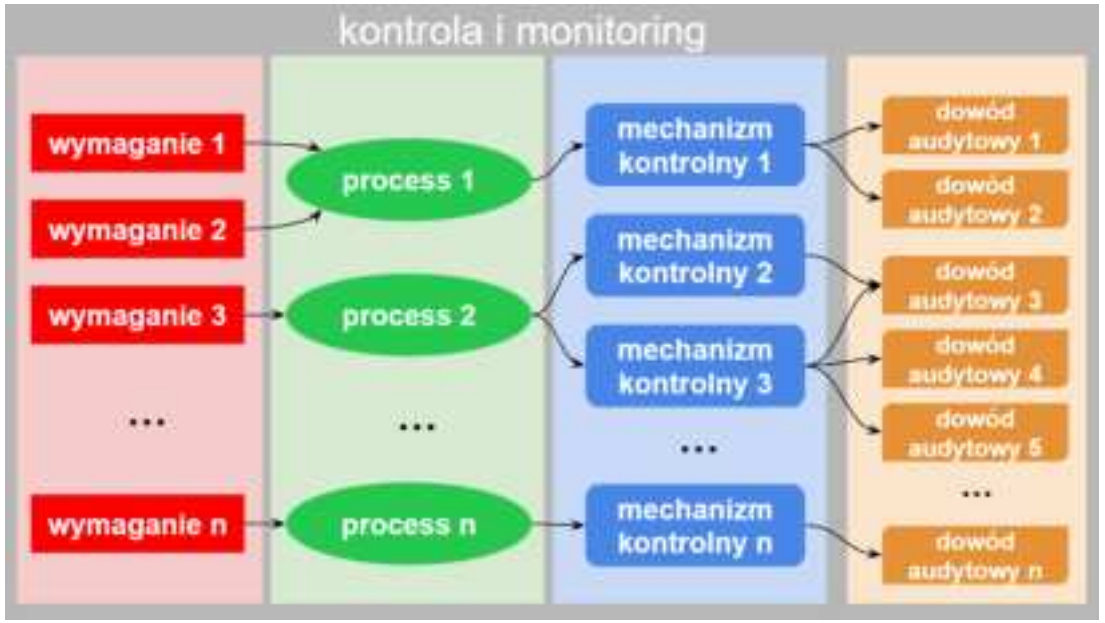


… przy którym Organizacja korzysta z wielu źródeł wymagań bezpieczeństwa, z wielu ich kategorii.

Zidentyfikowane źródła wymagań umożliwiają budowanie specyficznego dla Organizacji

katalogu wymagań bezpieczeństwa.

Katalog wymagań bezpieczeństwa dla Organizacji ...



... to miejsce w którym Organizacja może przechowywać **wszystkie** swoje wymagania bezpieczeństwa które zdecydowała się spełnić.

Wraz z wymaganiami, może być określony sposób ich realizacji, opis implementacji i użycia mechanizmów kontrolnych, definicja oczekiwań co do wyników, czy też w jaki sposób będzie monitorowany status zgodności ich działania.

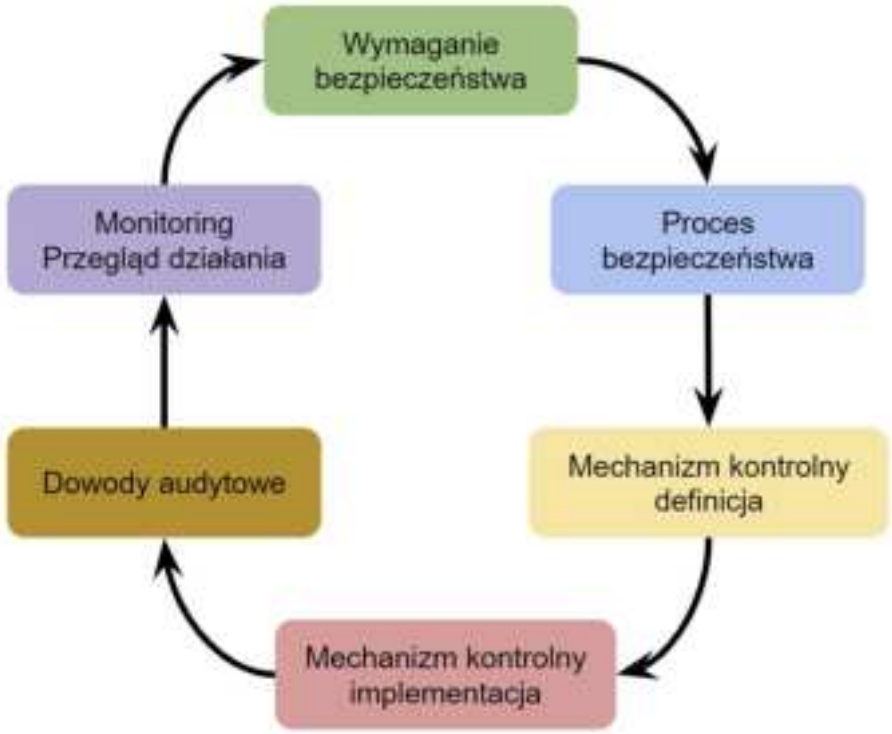
Realizacja wymagania bezpieczeństwa

Standaryzacja spełniania poszczególnych wymagań.

Realizacja np. poprzez procesy bezpieczeństwa (definicja z użyciem zasobów organizacji lub z wykorzystaniem dostawcy usługi **virtual CISO** - vCISO)

- ❑ wspierające procesy organizacyjne
  np. zarządzanie ryzykiem organizacji -> zarządzanie ryzkiem bezpieczeństwa informacji
- ❑ używające mechanizmów kontrolnych
  np. „trzy linie obrony”:
  analityk ryzyka (L1), manager/ISO (L2), audytor (L3)

Realizacja wymagania bezpieczeństwa (2)

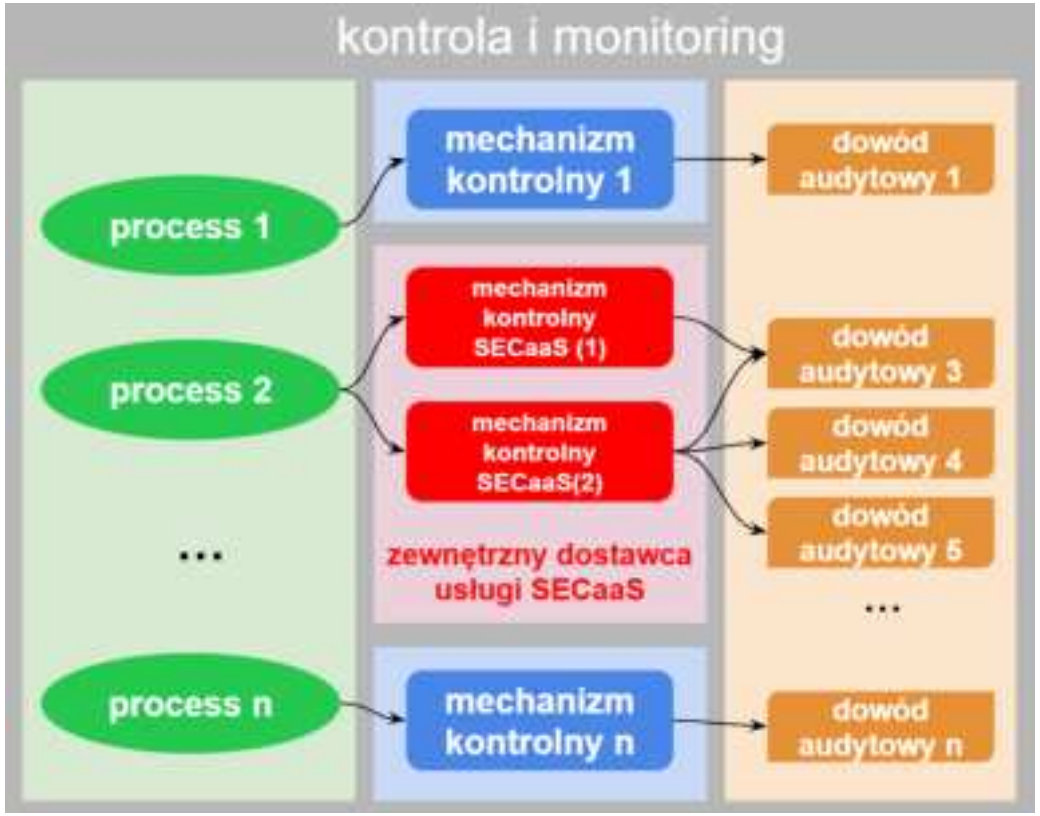


Mechanizmy kontrolne:

- ❑ zapewniają spełnienie wymagania bezpieczeństwa
- ❑ umożliwiają testowanie zgodności z wymaganiem
- ❑ wytwarzają określone dowody audytowe potwierdzające prawidłowe funkcjonowanie (np. kwartalne raporty audytowe)

Zarówno wymagania bezpieczeństwa (mogą ulec modyfikacji), jak też sposób działania mechanizmów kontrolnych powinny podlegać monitorowaniu oraz cyklicznym testom i przeglądom kontrolnym.

Implementacja mechanizmu kontrolnego



Optymalizacja użycia niezbędnych zasobów:

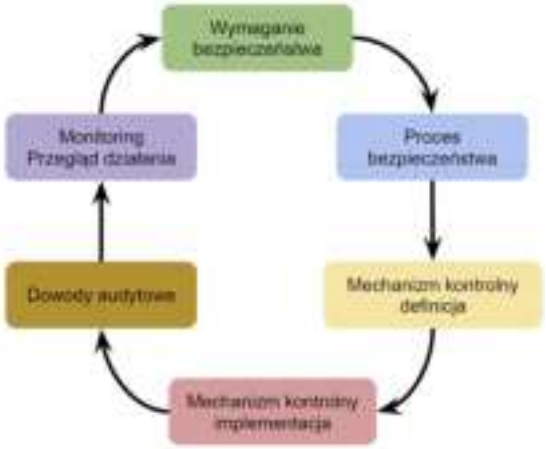
Organizacja może implementować mechanizmy kontrolne z wykorzystaniem swoich zasobów, lub
też zlecić implementację do dostawcy zewnętrznej usługi typu **SECaaS** (SECurity-as-a-Service).

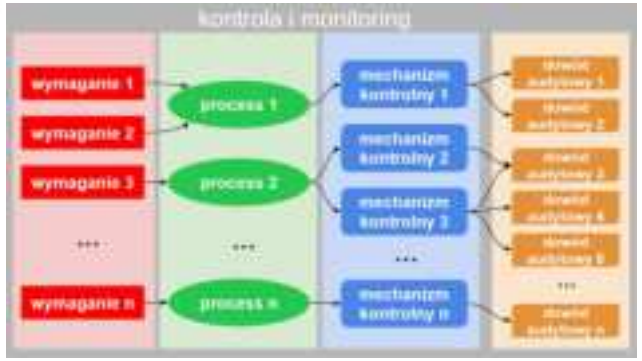
W takim przypadku, Organizacja wciąż pozostaje odpowiedzialna za prawidłowe funkcjonowanie mechanizmu, więc nie może odpuścić kontroli i monitorowania, np. dowodów audytowych.

Dobre praktyki / nasze doświadczenia

- wymagania – ważne dla Twojej Organizacji !
- zasada Pareto - 80/20 wciąż aktualna (szczególnie przy brakach zasobów i możliwości)
- właścicielstwo ! – określ „kto” za „co” odpowiada
- krytyczne zasoby dla biznesu … – zrób BIA
- … i zarządzaj ryzykiem które ich dotyczy
- standaryzacja – przy realizacji wymagań
- konsolidacja – wspólne mechanizmy kontrolne
- monitoring – działanie mechanizmów kontrolnych
- incydenty – były, są i będą, naucz się z nimi żyć, skutecznie obsługiwać i uczyć się z nich
- backupy – najważniejsza część planu przeżycia „po”
- testuj swoją odporność, ale też umiejętność podniesienia się w przypadku katastrofy

Podsumowanie





- ❑ Źródła wymagań
- ❑ Katalog wymagań i ich realizacja dla Organizacji
  - ❑ własnymi siłami
  - ❑ usługi vCISO jako alternatywa
- ❑ Procesy zarządzające cyberbezpieczeństwem
- ❑ Mechanizmy kontrolne
  - ❑ własnymi siłami
  - ❑ usługi SECaaS jako alternatywa
- ❑ Wyniki działania procesów i kontrolek
- ❑ Monitoring, testy i audyty

Dodatkowe materiały

NIST:
Small Business Cybersecurity Corner
CSF 2.0: Small Business Quick-Start Guide Overview

ENISA:
Cybersecurity guide for SMEs

CIS:
18 Security Controls as best practices you can use to strengthen your cybersecurity posture

ISACA:
The Essentiality of Cybersecurity for Small Businesses

Dziękuję za uwagę ☺ ☺ ☺ ☺ ☺

Linkedin:
https://www.linkedin.com/in/maciej-michalczak-9a05a89/