Praktyczne zasady audytu cyberbezpieczeństwa

Praktyczne zasady audytu cyberbezpieczeństwa
[Standardy zarządzania ryzykiem]

Wykładowca: Artur Cieślik
MBA, IRCA lead auditor ISO/IEC 27001
IRCA lead auditor ISO/IEC 22301
ISACA Certified Information Systems Auditor (CISA)
redaktor naczelny „IT Professional”
artur.cieslik@politykabezpieczenstwa.com.pl

Artur Cieślik
politykabezpieczenstwa.com.pl

- **Założyciel i główny ekspert ACSEC Sp. z o.o.:**
- Audytor wiodący normy ISO/IEC 27001 IRCA Certified Lead Auditor (nr w rejestrze: 6035034).
- Audytor wiodący normy ISO/IEC 22301 uzyskany zgodnie z IRCA.
- Certified Information Systems Auditor (CISA)
- Członek SABI – Stowarzyszenia Inspektorów Ochrony Danych.
- Członek IIA – Instytutu Audytorów Wewnętrznych IIA Polska
- Redaktor naczelny miesięcznika „IT Professional”.
- Członek rady programowej „ABI Expert”.
- Szkolenia i wykłady: Akademia Leona Koźmińskiego, Politechnika Wrocławska, Uniwersytet Ekonomiczny we Wrocławiu, Uniwersytet im. Kardynała Wyszyńskiego „IT Professional Academy” „Informacja Publiczna”, „Forbes Academy”, „IT w Administracji”.

Środki zarządzania ryzykiem w cyberbezpieczeństwie

- Przy uwzględnieniu najnowszego **stanu wiedzy** oraz, w stosownych przypadkach, odpowiednich **norm europejskich i międzynarodowych**, a także **kosztów** wdrożenia środki, o których mowa w akapicie pierwszym, zapewniają poziom bezpieczeństwa sieci i systemów informatycznych **odpowiedni do istniejącego ryzyka**.
- Oceniając proporcjonalność tych środków, należycie uwzględnia się **stopień narażenia** podmiotu na ryzyko, **wielkość podmiotu** i **prawdopodobieństwo** wystąpienia incydentów oraz ich dotkliwość, w tym ich **skutki** społeczne i gospodarcze

Środki zarządzania ryzykiem w cyberbezpieczeństwie

- Przy ustalaniu środków zarządzania ryzykiem w cyberbezpieczeństwie:
  - Identyfikujemy wszystkie zagrożenia(!)
  - Obejmujemy ochroną przed incydentami sieci i systemy informatyczne;
  - Obejmujemy ochroną przed incydentami środowisko fizyczne tych systemów.

Środki zarządzania ryzykiem w cyberbezpieczeństwie

- Środki zarządzania ryzykiem w cyberbezpieczeństwie obejmują co najmniej następujące elementy:
  - **politykę analizy ryzyka i bezpieczeństwa systemów informatycznych;**
  - obsługę incydentu;
  - ciągłość działania, np. zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej, i zarządzanie kryzysowe;
  - bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami;
  - bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku podatności i ich ujawnianie;

Środki zarządzania ryzykiem w cyberbezpieczeństwie

- Środki zarządzania ryzykiem w cyberbezpieczeństwie obejmują co najmniej następujące elementy:
  - **polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie;**
  - podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa;
  - polityki i procedury stosowania kryptografii i, w stosownych przypadkach, szyfrowania;
  - bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzanie aktywami;
  - w stosownych przypadkach - stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych.

Środki zarządzania ryzykiem w cyberbezpieczeństwie

Identify

- Uzyskanie informacji organizacyjnych, aby zarządzać ryzykiem cyberbezpieczeństwa w zakresie: systemów, zasobów, danych i możliwości zabezpieczenia

Protect

- Opracowanie i uruchomienie odpowiednich zabezpieczeń organizacyjnych, technicznych, personalnych, fizycznych w celu zapewnienia działania usług IT

Detect

- Opracowanie i uruchomienie działań niezbędnych do zidentyfikowania wystąpienia zdarzenia cyberbezpieczeństwa

Środki zarządzania ryzykiem w cyberbezpieczeństwie

Respond

- Opracowanie i wdrożenie działań niezbędnych w przypadku wykrycia zdarzenia cyberbezpieczeństwa

Recover

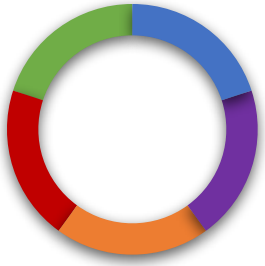
- Opracowanie i wdrożenie działań w celu utrzymania procedur i planów niezbędnych do przywrócenia uszkodzonych systemów, zasobów i danych w wyniku zdarzenia cyberbezpieczeństwa.

Zasady cyberbezpieczeństwa

Wytyczne i standardy:

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- ISO 22301:2019
- CIS Controls v.8.1
- NIST SP 800-115
- NIST SP 800-30

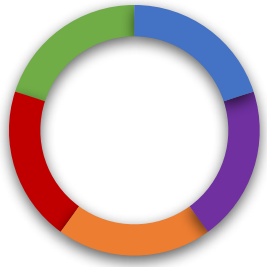
Obszary cyberbezpieczeństwa



Inwentaryzacja i kontrola aktywów	Inwentaryzacja i kontrola zasobów oprogramowania	Zarządzanie ryzykiem	Identyfikacja i uwierzytelnienie	Zarządzanie kontami	Kontrola dostępu, w tym zarządzanie uprawnieniami
Rozliczalność w systemie	Kryptografia i zabezpieczenia danych podczas transferu	Zarządzanie zmianą i konfiguracją	Rozwój oprogramowania i testowanie	Zabezpieczenia przed malware	Monitorowanie systemu
Zarządzanie logami	Zarządzanie podatnościami	Audyt i testowanie	Bezpieczeństwo sieci i usług	Nabywanie systemu i usług	Zarządzanie ciągłością działania

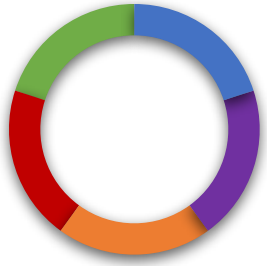
Bezpieczeństwo usług cloudowych	Bezpieczeństwo zewnętrznych usług IT	Zarządzanie i obsługa incydentów	Szkolenie w zakresie świadomości i umiejętności w zakresie bezpieczeństwa	Zarządzanie dostawcami

Organizacja audytu



- **Zakres zadań audytowych**
  - Audyt możemy podzielić na kilka obszarów:
    - Zarządzanie aktywami
    - Zarządzanie usługami IT
    - Funkcjonowanie środków organizacyjnych
    - Funkcjonowanie zabezpieczeń IT
    - Funkcjonowanie zabezpieczeń fizycznych
    - Zarządzanie dostawcami, w tym DC oraz cloud

Organizacja audytu



- **Metody**
  - Ocena na podstawie listy kontrolnej lub ankiety
  - Analiza stosowania procedur i dobrych praktyk
  - Analiza architektury bezpieczeństwa
  - Weryfikacja konfiguracji
  - Analiza logów zdarzeń związanych z bezpieczeństwem
  - Testowanie podatności
  - Testy penetracyjne

Organizacja audytu

- **Narzędzia – przykład listy pytań**

WSZYSTKIE OBSZARY BEZPIECZEŃSTWA

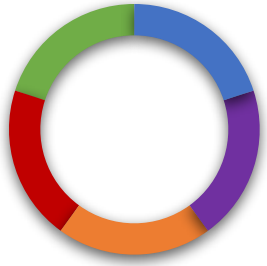
Obszar	Relacja	Uwagi	Punktacja
Zarządzanie ryzykiem	1		33%
Relacje z dostawcami	2		100%
Bezpieczeństwo zasobów ludzkich	3		33%
Kontrola Dostępu	4		33%
Ochrona aktywów	5		33%
Klasyfikacja i postępowanie z informacjami	6		33%
Zarządzanie incydentami bezpieczeństwa	7		0%
Kryptografia	8		33%
Bezpieczeństwo fizyczne i środowiskowe	9		33%
Przygotowanie, reakcja i zarządzanie kryzysowe	10		33%
Bezpieczeństwo operacji	11		66%
Bezpieczeństwo komunikacji	12		33%
Zarządzanie incydentami bezpieczeństwa	13		33%
Zarządzanie ciągłością działania	14		33%
Usługi chmurowe i wirtualizacja	15		33%
Audyt i zgodność	16		33%

TYLKO OBLIGATORYJNE OBSZARY BEZPIECZEŃSTWA

Obszar	Relacja	Uwagi	Punktacja
Zarządzanie ryzykiem	1		33%
Relacje z dostawcami	2		100%
Bezpieczeństwo zasobów ludzkich	3		33%
Kontrola Dostępu	4		33%
Ochrona aktywów	5		33%
Klasyfikacja i postępowanie z informacjami	6		33%
Zarządzanie incydentami bezpieczeństwa	7		0%
Kryptografia	8		33%
Bezpieczeństwo fizyczne i środowiskowe	9		33%
Przygotowanie, reakcja i zarządzanie kryzysowe	10		33%
Bezpieczeństwo operacji	11		66%
Bezpieczeństwo komunikacji	12		33%
Zarządzanie incydentami bezpieczeństwa	13		33%
Zarządzanie ciągłością działania	14		33%
Usługi chmurowe i wirtualizacja	15		33%
Audyt i zgodność	16		33%

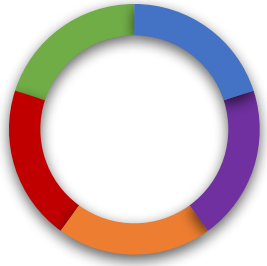
ACSEC

Organizacja audytu



- **Narzędzia – przykład listy CIS 8.1**
- Oznaczenia IG1, IG2 i IG3 odnoszą się do grup wdrożeniowych, które są podzbiorami kontrolek CIS, mających na celu zapewnienie właściwej ścieżki stopniowego doskonalenia stanu cyberbezpieczeństwa organizacji.

Organizacja audytu

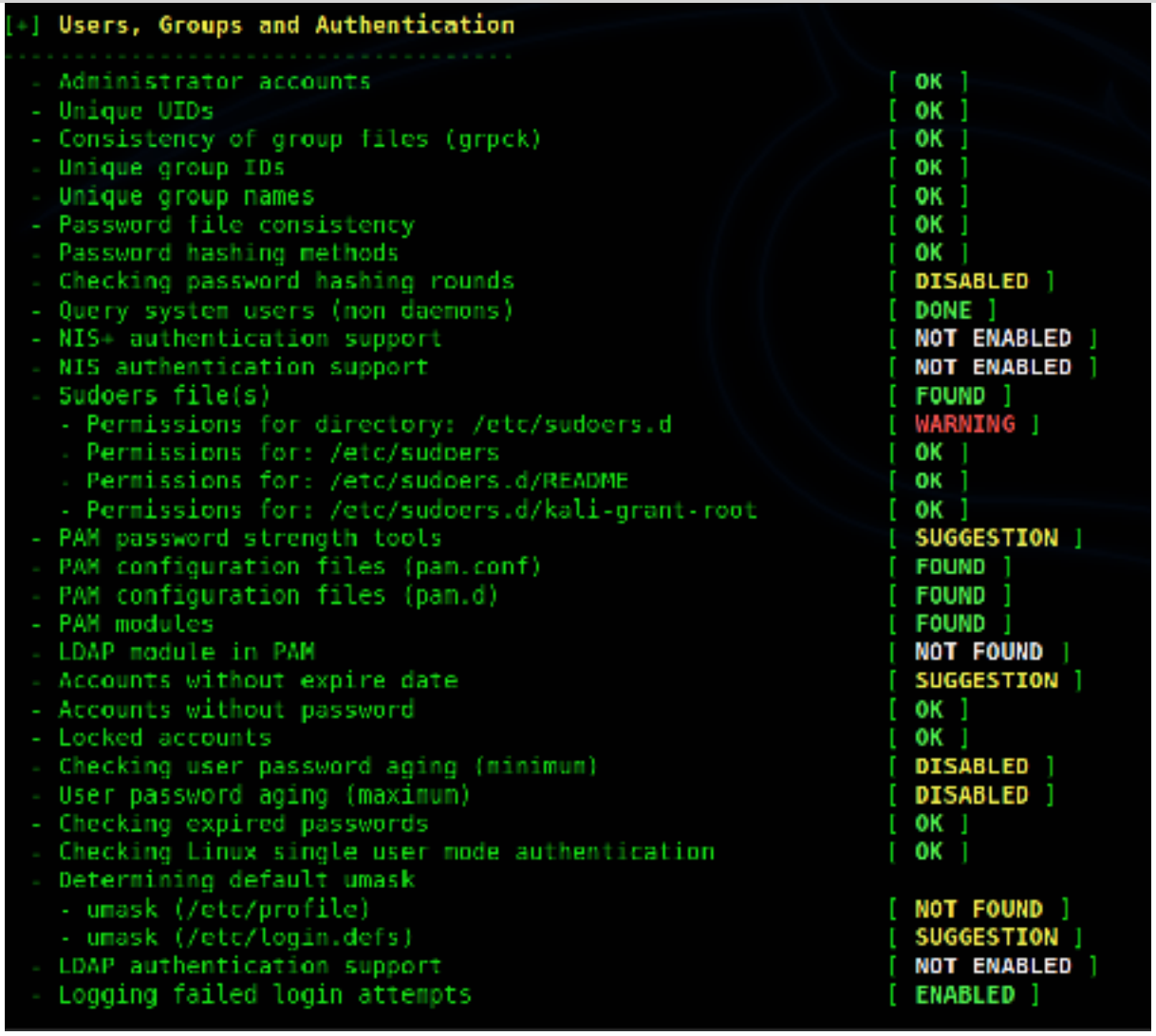


- **Narzędzia**
  - Narzędzia szacowania ryzyka np. The OWASP Risk Rating
  - Narzędzia analizy konfiguracji np. lynis, OpenSCAP, CIS Benchmark
  - Narzędzia do skanowania podatności np. OpenVAS, ZAP, Metasploit
  - Narzędzia do analizy logów: ELK Stack, Greylog

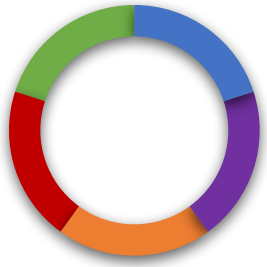
Organizacja audytu

- **Narzędzia –**

  przykład lynis

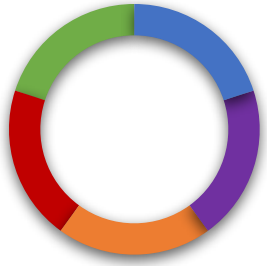


Organizacja audytu



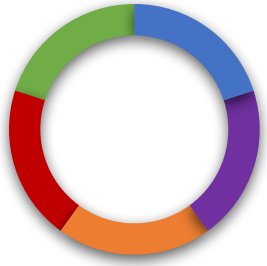
- **Analiza funkcjonowania procedur bezpieczeństwa**
  - Procedura zarzadzania ryzykiem.
  - Procedura prowadzenia rejestru zasobów informatycznych.
  - Procedura przydzielania, zwrotu sprzętu i oprogramowania.
  - Procedura korzystania z zasobów informatycznych przez użytkowników, w tym urządzeń mobilnych.
  - Procedura zarządzania konfiguracją.
  - Procedura zarządzania uprawnieniami do pracy w systemach teleinformatycznych;
  - Procedura monitorowania poziomu świadczenia usług.
  - Procedura niszczenia nośników informacji.
  - Procedura zarządzania zmianami.
  - Procedura stosowania środków kryptograficznych.
  - Procedura określania specyfikacji technicznych wymagań odbioru systemów IT.
  - Procedura zgłaszania i obsługi incydentów naruszenia bezpieczeństwa informacji.
  - Procedura wykonywania i testowania kopii zapasowych.
  - Procedura zarządzania ciągłością działania.

Organizacja audytu



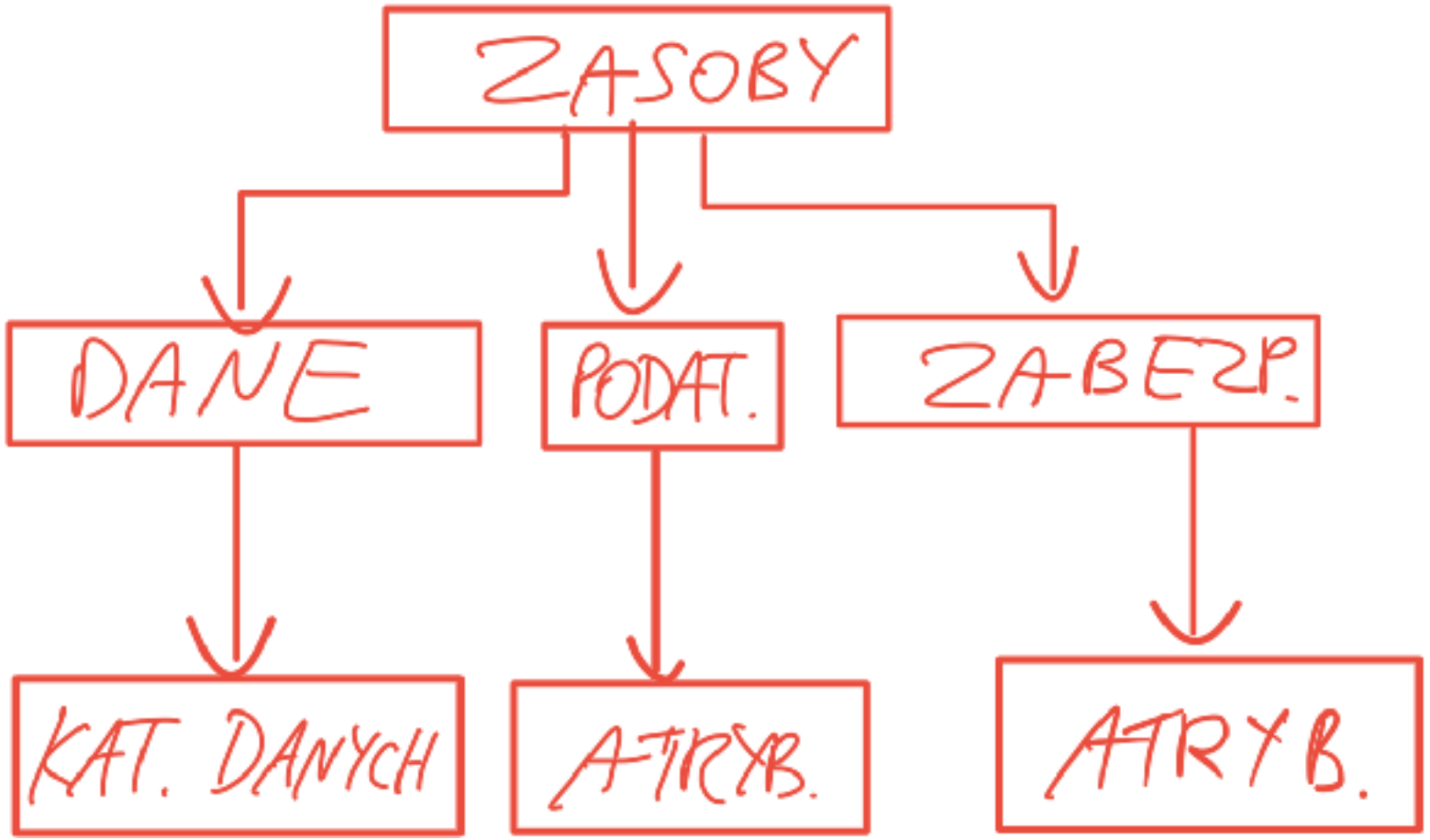
- **Analiza funkcjonowania procedur bezpieczeństwa**
  - Procedura monitorowania dostępu do zasobów IT, w tym prowadzenia logów systemowych.
  - Procedura zarządzania dokumentacją i zapisami.
  - Procedura audytu bezpieczeństwa informacji.
  - Procedura szkoleń.
  - Procedura pracy zdalnej.
  - Standardy zabezpieczeń.

Metody audytu - identify



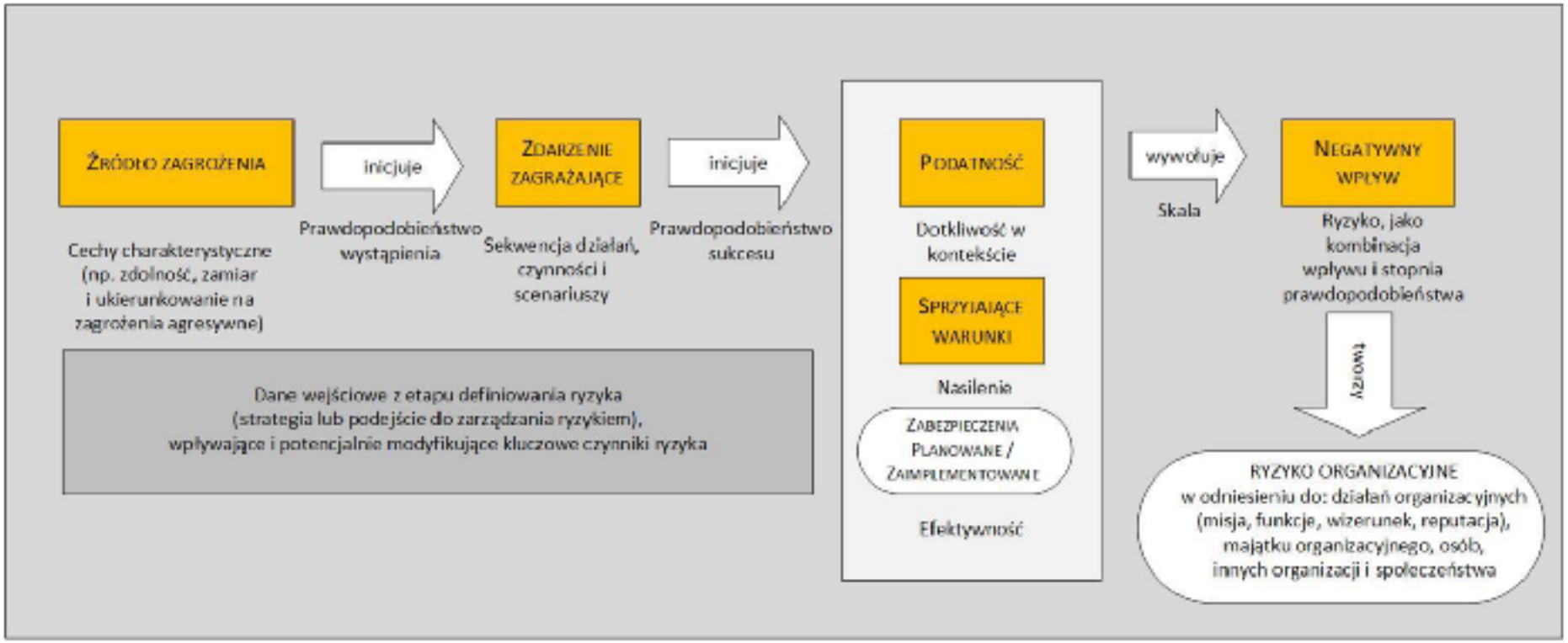
- Analiza zidentyfikowanych aktywów – jakie rodzaje informacji i procesów określono jako krytyczne
- Analiza przepływów danych – gdzie dane są przechowywane i w jaki sposób wykorzystywane
- Weryfikacja inwentaryzacja sprzętu i oprogramowania – czy wiadomo, jaką krytyczność mają poszczególne aktywa
- Identyfikacja podatności i zagrożeń aktywów
- **Weryfikacja szacowania ryzyka**
- Analiza podatności, zagrożeń, pentesty

Metody audytu - identify

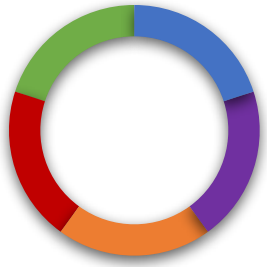


Szacowanie ryzyka

- Proces szacowania ryzyka zgodnie z NIST SP 800-30



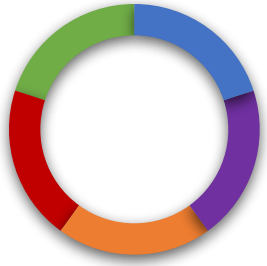
Szacowanie ryzyka – dobór zabezpieczeń



- Atrybuty cyberbezpieczeństwa
  - **Identify –** uzyskanie informacji organizacyjnych, aby zarządzać ryzykiem cyberbezpieczeństwa
  - **Protect –** opracowanie i uruchomienie odpowiednich zabezpieczeń prewencyjnych
  - **Detect –** opracowanie i uruchomienie działań niezbędnych do zidentyfikowania wystąpienia zdarzenia cyberbezpieczeństwa
  - **Respond –** opracowanie i wdrożenie działań niezbędnych w przypadku wykrycia zdarzenia cyberbezpieczeństwa
  - **Recover –** opracowanie i wdrożenie działań w celu utrzymania procedur i planów niezbędnych do przywrócenia uszkodzonych systemów, zasobów i danych w wyniku zdarzenia cyberbezpieczeństwa

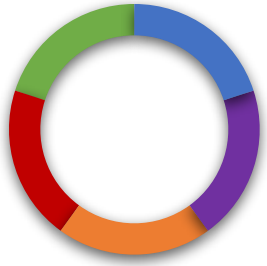
- **Preventive** – zabezpieczenie, które ma na celu zapobieganie wystąpieniu incydentu bezpieczeństwa informacji.
- **Detective –** zabezpieczenie stosowane w przypadku wystąpienia incydentu bezpieczeństwa informacji.
- **Corrective** – zabezpieczenie działające po wystąpieniu incydentu bezpieczeństwa informacji.

Szacowanie ryzyka



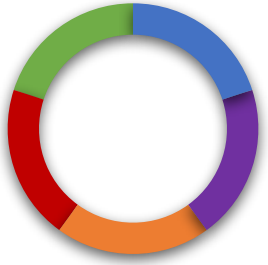
- Analiza scenariuszy zagrożeń
- Ocena skuteczności zabezpieczeń
- Ustalenie atrybutów zabezpieczeń
- Uwzględnienie możliwości wykrywania i reagowania na zdarzenia
- Stosowanie metodyki uwzględniającej cechy zagrożenia, podatności oraz stosowanych zabezpieczeń

Metody audytu - protect



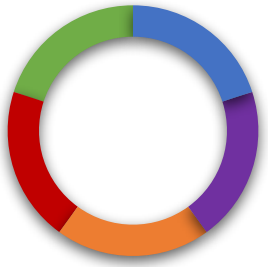
- Analiza zarządzania dostępem
- **Weryfikacja zabezpieczeń** dla krytycznych procesów/systemów na podstawie np. **ISO/IEC 27002:2022**, NIST SP 800-53 lub CIS
- Sprawdzenie funkcji wykorzystanych narzędzi i zmapowanie na wymagane rodzaje zabezpieczeń
- Sprawdzenie sposobu zarządzania podatnościami
- Sprawdzenie sposobu zarządzania patchami
- Weryfikacja poziomu świadomości użytkowników

Narzędzia cyberbezpieczeństwa



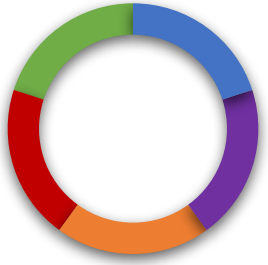
ISO/IEC 27002 control identifier	Control name	Information security properties	Cybersecurity concepts
5.15	Access control	#Confidentiality #Integrity #Availability	#Protect
5.18	Access rights	#Confidentiality #Integrity #Availability	#Protect
5.24	Information security incident management planning and preparation	#Confidentiality #Integrity #Availability	#Respond #Recover
5.25	Assessment and decision on information security events	#Confidentiality #Integrity #Availability	#Detect #Respond
5.26	Response to information security incidents	#Confidentiality #Integrity #Availability	#Respond #Recover
5.32	Intellectual property rights	#Confidentiality #Integrity #Availability	#Identify
6.3	Information security awareness, education and training	#Confidentiality #Integrity #Availability	#Protect
6.7	Remote working	#Confidentiality #Integrity #Availability	#Protect
7.9	Security of assets off-premises	#Confidentiality #Integrity #Availability	#Protect
8.2	Privileged access rights	#Confidentiality #Integrity #Availability	#Protect
8.7	Protection against malware	#Confidentiality #Integrity #Availability	#Protect #Detect
8.8	Management	#Confidentiality #Integrity #Availability	#Identify #Protect
8.12	Data leakage prevention	#Confidentiality	#Protect #Detect
8.15	Logging	#Confidentiality #Integrity #Availability	#Detect
8.16	Monitoring activities	#Confidentiality #Integrity #Availability	#Detect #Respond
8.18	Use of privileged utility programs	#Confidentiality #Integrity #Availability	#Protect
8.19	Installation of software on operational systems	#Confidentiality #Integrity #Availability	#Protect
8.20	Networks security	#Confidentiality #Integrity #Availability	#Protect #Detect
8.22	Segregation of networks	#Confidentiality #Integrity #Availability	#Protect
8.23	Web filtering	#Confidentiality #Integrity #Availability	#Protect
8.26	Application security requirements	#Confidentiality #Integrity #Availability	#Protect

Narzędzia cyberbezpieczeństwa



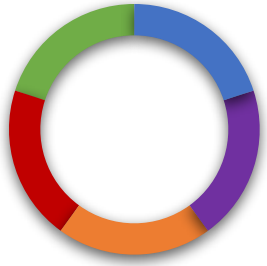
Nazwa systemu	Pkt. ISO/IEC 27001 Zał. A	NIST CSF	Opis ISO/IEC 27001 Zał. A
EDR (Endpoint Detection and Response)	8.7	#Protect #Detect	Protection against malware
	5.26	#Respond #Recover	Response to information security incidents
NDR (Network Detection and Response)	8.20	#Protect #Detect	Networks security
	5.26	#Respond #Recover	Response to information security incidents
XDR (Extenced Detection and Response)	8.7	#Protect #Detect	Protection against malware
	5.26	#Respond #Recover	Response to information security incidents
	8.20	#Protect #Detect	Networks security
NAC (Network Access Control)	8.20	#Protect #Detect	Networks security
	8.22	#Protect	Segregation of networks
UEBA (User Entity Behavior Analytics)	8.16	#Detect #Respond	
SIEM (Security Information and Event Management)	8.15	#Detect	Logging
	5.26	#Respond #Recover	Response to information security incidents
	8.16	#Detect #Respond	Monitoring activities
AV (Antivirus)	8.7	#Protect #Detect	Protection against malware
PAM (Privileged Access Management)	8.18	#Protect	Use of privileged utility programs
	8.2	#Protect	Privileged access rights
IAM (Identity and Access Management)	5.15	#Protect	Access control
	5.18	#Protect	Access rights
DLP (Data Loss Prevention)	8.12	#Protect #Detect	Data leakage prevention
	5.32	#Identify	Intellectual property rights

Narzędzia cyberbezpieczeństwa



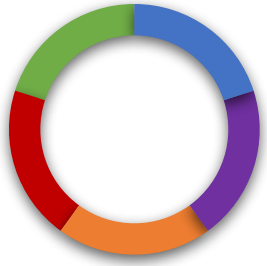
Nazwa systemu	Pkt. ISO/IEC 27001 Zał. A	NIST CSF	Opis ISO/IEC 27001 Zał. A
VPN (Virtual Private Network)	6.7	#Protect	Remote working
WAF (Web Application Firewall)	8.26	#Protect	Application security requirements
Sandbox	8.7	#Protect #Detect	Protection against malware
MDM (Mobile Device Management)	8.12	#Protect #Detect	Data leakage prevention
	7.9	#Protect	Security of assets off-premises
	8.7	#Protect #Detect	Protection against malware
SOAR (Security Orchestration Automation and Response)	8.7	#Protect #Detect	Protection against malware
	8.26	#Protect	Response to information security incidents
	5.7	#Identify #Detect #Respond	Threat intelligence
Vulnerability scanner	8.8	#Identify #Protect	Vulnerability management
Patch Management System	8.8	#Identify #Protect	Patch management
EMS (Endpoint Management System)	8.19	#Protect	Installation of software on operational systems
	5.32	#Identify	Intellectual property rights
Platforma szkoleniowa	6.3	#Protect	Information security awareness, education and training
TIP	5.7	#Identify #Detect #Respond	Threat intelligence
VPN (Virtual Private Network)	6.7	#Protect	Remote working
NGFW (Next-Generation Firewall)	8.22	#Protect	Segregation of networks
	8.23	#Protect	Web filtering
	8.32	#Protect	Change management
	5.23	#Protect	Information security for use of cloud services

Metody audytu - detect



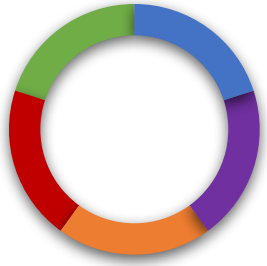
- Analiza procedur **wykrywania zdarzeń cyberbezpieczeństwa**
- Weryfikacja narzędzi i zasad wykrywania nieoczekiwanych przepływów danych
- Analiza narzędzi i procedur **monitorowania oraz przechowywania logów**
- Integracja procesu monitorowania z obsługą incydentów

Metody audytu - respond



- Weryfikacja planów reakcji na cyberincydent (CRP) oraz ich sposobów testowania – **upewnić się, że każda osoba zna swoje obowiązki związane z realizacją planu**
- Analiza wyników testowania planu (i wykonania podczas incydentu), **sprawdzenie aktualizacji planów na podstawie wyciągniętych wniosków po incydencie/testowaniu**
- Analiza procesu obsługi incydentu w przypadku wykrycia zdarzenia związanego z cyberbezpieczeństwem – **sposoby działania, zrozumienie zakresu i poziomu wpływu na organizację**
- Weryfikacja, czy plany uwzględniają **relacje zewnętrzne**

Metody audytu - recover



- Analiza procesu zarządzania ciągłością działania na podstawie ISO 22301
- Analiza planów ciągłości dla systemów na podstawie NIST SP 800-34
- Weryfikacja planów odzyskiwania zdolności działania i ich testowania
- Weryfikacja systemu kopii zapasowych **zgodnie z zasadą 3-2-1**
- Sprawdzenie wdrażania doskonaleń na podstawie wniosków z testów odzyskiwania i incydentów
- Analiza procedur komunikacji