ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

Reforma ochrony danych osobowych RODO/GDPR

Reforma ochrony danych osobowych (RODO/GDPR) – wyzwania dla organów państwa, sektora publicznego i przedsiębiorców.

Marek Abramczyk
CISA, CRISC, CISSP, LA 27001, LA 22301

Biblioteka Uniwersytetu Warszawskiego
Warszawa, 22.09.2017

Agenda

1	Zarządzanie zbiorami danych osobowych
2	Realizacja procesu identyfikacji zbiorów danych osobowych
3	Inwentaryzacja aktywów wspierających
4	Szacowanie ryzyka utraty bezpieczeństwa informacji

Agenda

1	Zarządzanie zbiorami danych osobowych
2	Realizacja procesu identyfikacji zbiorów danych osobowych
3	Inwentaryzacja aktywów wspierających
4	Szacowanie ryzyka utraty bezpieczeństwa informacji

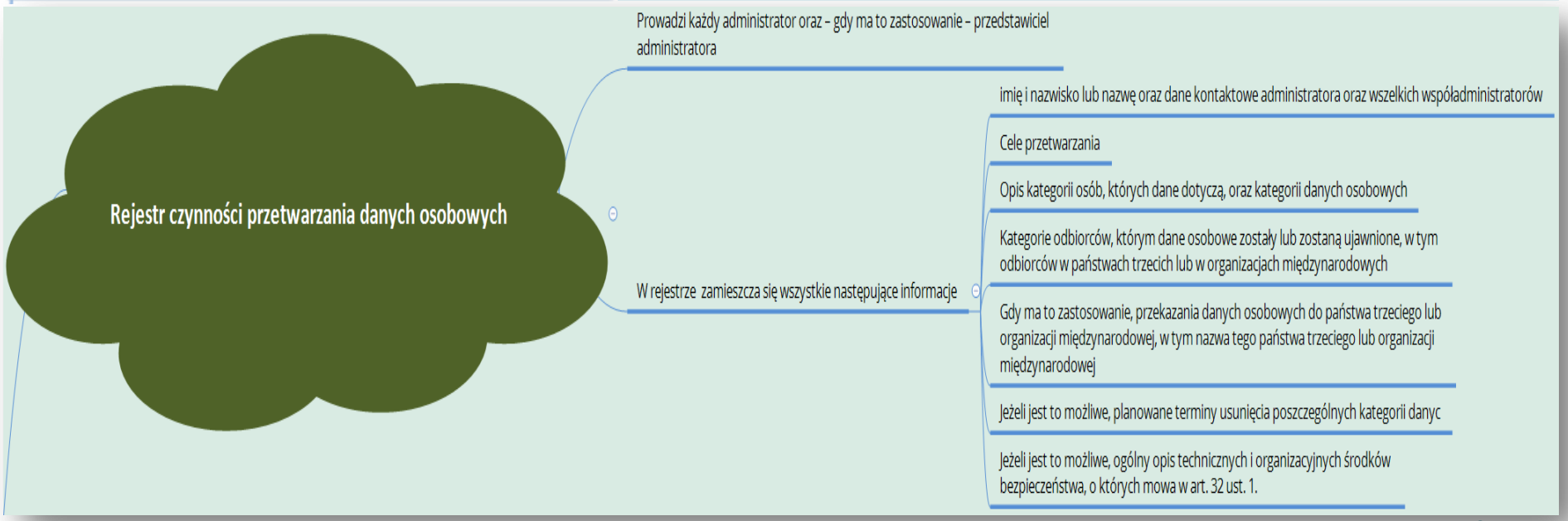
Wymagania prawne

Blok – Zarządzanie zbiorami danych osobowych

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

SEKCJA 1
OBOWIĄZKI OGÓLNE

Artykuł 30 Rejestrowanie czynności przetwarzania



Wymagania prawne

Blok – Zarządzanie zbiorami danych osobowych

Rozporządzenie Ministra Administracji i Cyfryzacji z **11 maja 2015** r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015, poz. 719)

Rejestr zbiorów danych

Wykaz zbiorów danych osobowych

Rozporządzenie ministra spraw wewnętrznych i administracji z dnia **29 kwietnia 2004** r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)

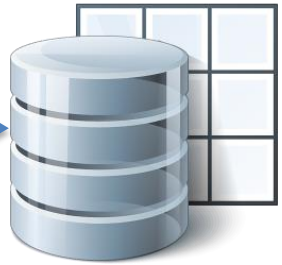
Role i odpowiedzialności

Blok – Zarządzanie zbiorami danych osobowych

Właściciele aktywów / danych w zakresie przypisanej odpowiedzialności odpowiadają za:

a) inwentaryzację aktywów/informacji,
b) klasyfikację aktywów/informacji,
c) okresowe przeglądy inwentaryzacji aktywów / zbiorów danych i ich aktualizacja,
d) udział w szacowaniu ryzyka utraty bezpieczeństwa informacji,
e) szkolenie użytkowników z zasad bezpiecznego korzystania z informacji,
f) nadzorowanie dostępu do danych (kontrola dostępu),
g) decydowanie o miejscach i metodach przetwarzania informacji ze zbioru danych.

współpraca
z
ABI / IOD



Rejestr zbiorów danych

Wykaz zbiorów danych osobowych

ABI WAY
ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

- Upoważnienia
- Podmioty upoważniane
- Udostępnienia
- Zbiory
  - Nowy zbiór
  - Rejestr zbiorów
  - Powiadom właścicieli zbiorów
- Systemy IT
- Identyfikatory
- Zabezpieczenia
- Rejestr umów
- Rejestr sprzeciwów
- Rejestr szkoleń
- Zgłoszenia do GIODO
- Miejsca przetwarzania
- Sprawdzenia

Zbiory zarejestrowane w systemie

Wykaz zbiorów UoODO | Wykaz zbiorów i lokalizacji | Właściciele zbiorów | Wykaz ogólny | Wykaz szczegółowy | Historia zdarzeń

1. kontrahenci		Szczegóły	Przenieś do kosza	Wykreśl z rejestru
2. Pracownicy		Szczegóły	Przenieś do kosza	Wykreśl z rejestru
3. Skazani	wykreślony	Szczegóły	Przenieś do kosza	
4. Zbiór danych kontaktowych do pracodawców		Szczegóły	Przenieś do kosza	Wykreśl z rejestru

Powrót

Administrator Systemu
(Gabinet Prezesa)
IP: 109.173.208.160
Zmiana hasla za dni: 1124

- Użytkownicy
  - Nowy użytkownik
  - Użytkownicy
  - Szukaj użytkownika
- Organizacja
- Dokumentacja
- Konfiguracja
- Kosz
- Informacje

Informacje dotyczące zbioru

Wydruk PDF

Nazwa zbioru:	kontrahenci
Właściciel zbioru danych osobowych:	Administrator Systemu (admin)
Rodzaj zbioru:	Stworzony w organizacji
Rejestracja w GIODO:	Niezarejestrowany w GIODO
Forma przetwarzania	Papierowa
Oznaczenie administratora danych:	Nazwa administratora: Podmiot Regon: 1231233 Miejscowo□ć Poznań Kod pocztowy: 51-234 Ulica: Kawiatkowskiego Nr domu: 3 Lokal: 1
Oznaczenie przedstawiciela administratora danych, o którym mowa w art. 31a ustawy:	Nie wskazano przedstawiciela
Podstawa prawna upoważniająca do prowadzenia zbioru danych:	- Zgoda osoby, której dane dotyczą.
Cel przetwarzania danych w zbiorze:	Sprzedaż produktów i usług
Opis kategorii osób, których dane są przetwarzane w zbiorze:	Osoby fizyczne
Oznaczenie	

Formularz rejestracji nowego zbioru

Krok 1

Dane o zbiorze

Nazwa zbioru:	
Właściciel zbioru danych osobowych:	[wybierz]
Rodzaj zbioru:	[wybierz]
Rejestracja w GIODO:	[wybierz]
Forma przetwarzania:	[wybierz]

Oznaczenie administratora danych:

- (•) - wykorzystaj dane zapisane w systemie (menu Konfiguracja)
- ( ) - użyj poniższych danych:

Nazwa administratora:

REGON:

Miejscowość:

Kod pocztowy:

Ulica:

Nr domu:

Lokal:

Oznaczenie przedstawiciela administratora danych, o którym mowa w art. 31a ustawy:

- (•) - brak przedstawiciela
- ( ) - wykorzystaj dane zapisane w systemie (menu Konfiguracja)
- ( ) - użyj poniższych danych:

Nazwa przedstawiciela:

Miejscowość:

Kod pocztowy:

Ulica:

Nr domu:

Lokal:

Agenda

1	Zarządzanie zbiorami danych osobowych
2	Realizacja procesu identyfikacji zbiorów danych osobowych
3	Inwentaryzacja aktywów wspierających
4	Szacowanie ryzyka utraty bezpieczeństwa informacji

Planowanie – zainteresowane strony i wymagane zasoby

Blok – Realizacja procesu identyfikacji zbiorów danych osobowych

ABI / IOD

- Koordynacja procesu
- Zbieranie danych
- Raportowanie
- Przygotowanie rejestru zbiorów danych

Wariant I

Każdy pracownik (przetwarzający informacje)

- (-) Trudniejsze w realizacji - koordynacja
- (-/+) Więcej danych analitycznych - czasochłonna
- (+) Możliwość wykorzystania danych na potrzeby systemów klasy DLP

Wariant II

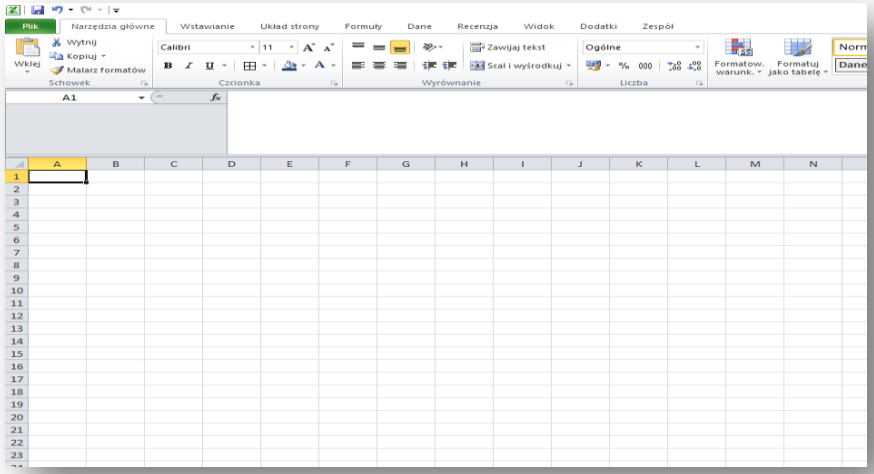
Przedstawiciele komórek organizacyjnych – departamenty, biura, zespoły

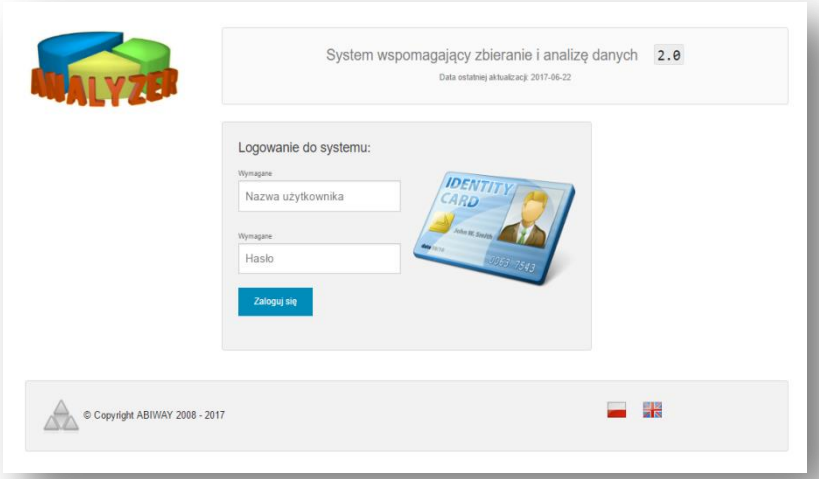
- (+) Łatwiejsze w realizacji
- (-) Mniejszy zbiór danych analitycznych

Planowanie – zainteresowane strony i wymagane zasoby

Blok – Realizacja procesu identyfikacji zbiorów danych osobowych

Narzędzia analityczne



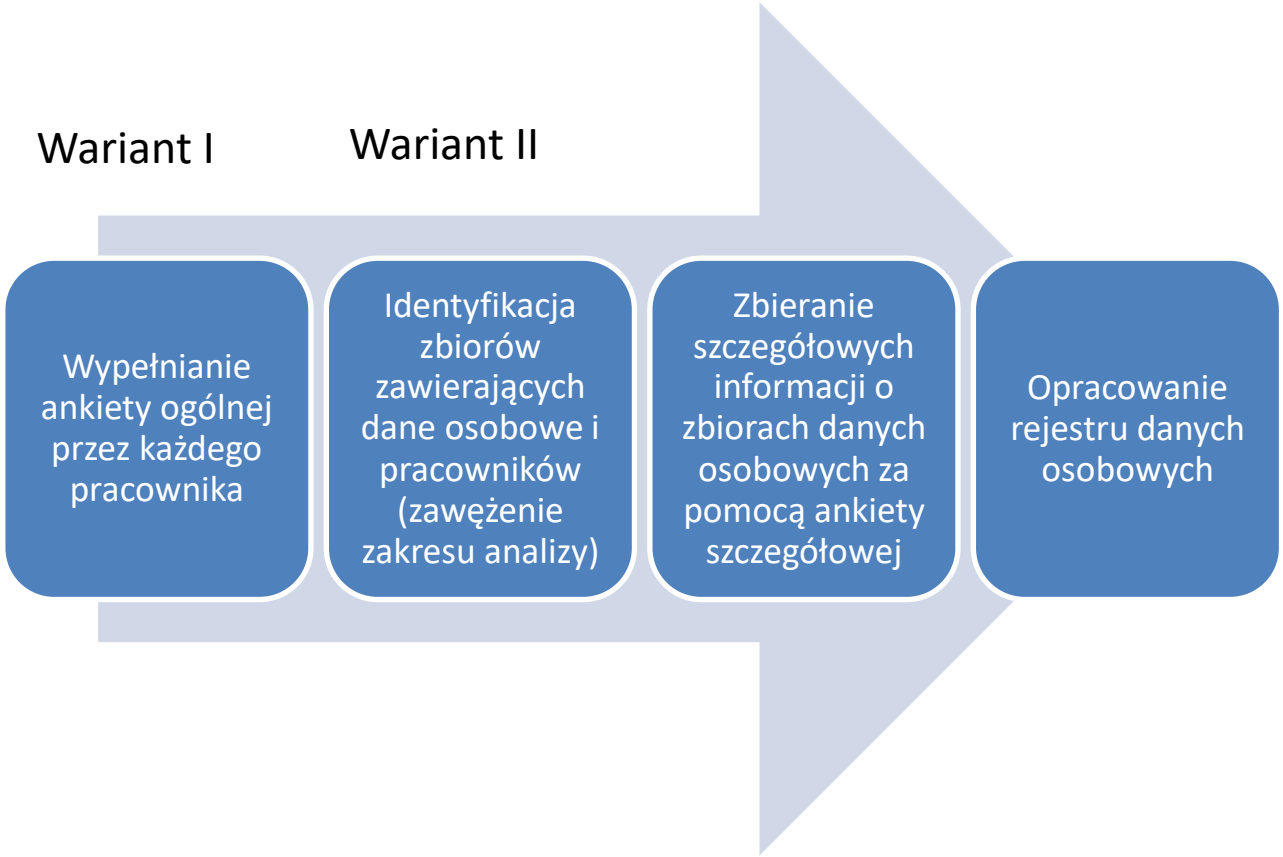


Oraz trochę czasu na przeprowadzenie analizy i uzupełnienie danych …

Planowanie – zainteresowane strony i wymagane zasoby

Blok – Realizacja procesu identyfikacji zbiorów danych osobowych

Kompleksowa i pełna inwentaryzacja zbiorów informacji



Metody identyfikacji

Blok – Realizacja procesu identyfikacji zbiorów danych osobowych

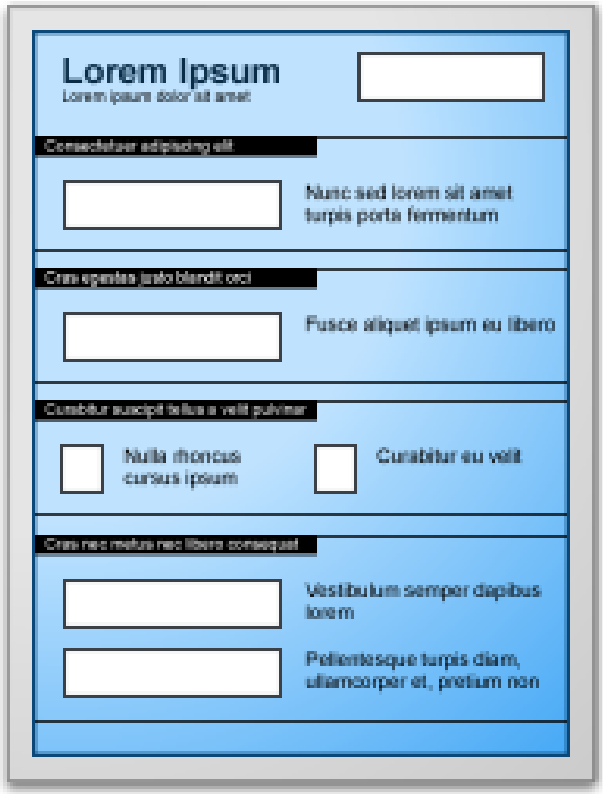
Proces identyfikacji zbiorów danych i ich klasyfikacja

1. Określić cele procesu identyfikacji zbiorów informacji
2. Uzyskać od kierownictwa wsparcie w zakresie organizacji procesu – zaangażowanie stron
3. Zdefiniować metodę inwentaryzacji i klasyfikacji zbiorów danych (formalna procedura)
4. Przygotować narzędzia do realizacji procesu (np. ankiety, narzędzia informatyczne)
5. Zidentyfikować właścicieli aktywów (procesów/informacji/aplikacji)
6. Rozdystrybuować standardowe szablony ankiet z instrukcją wypełnienia
7. Przygotować dane analityczne - zebrać, zagregować i uporządkować informacje z ankiet wg klucza w celu dalszej analizy
8. Grupować informacje, identyfikować zbiory danych (po celu przetwarzania i zakresie danych osobowych)
9. Sklasyfikować informacje i aplikacje
10. Opracować raport zawierający wykaz zbiorów danych
11. Przeszkolić użytkowników z utrzymania wykazu zbiorów danych
12. Eksploatować zatwierdzony schemat identyfikacji i klasyfikacji zbiorów danych
13. Rozwinąć i wdrożyć procedury audytu wewnętrznego
14. Okresowo przeglądać i aktualizować procedury identyfikacji zbiorów danych

Metody identyfikacji

Blok – Realizacja procesu identyfikacji zbiorów danych osobowych

1. Ankieta ogólna inwentaryzacji i klasyfikacji informacji
2. Ankieta wspomagająca proces identyfikacji zbiorów danych osobowych



Rejestr zadań

Aktywne

Inwentaryzacja i klasyfikacja informacji w [redacted] S.A. (2017)

Zadanie aktywne
Data rozpoczęcia: 2017-06-01
Data zakończenia: 2018-06-30

Wybierz zadanie

Identyfikacja i estymacja ryzyka ZSZ (2017)

Zadanie aktywne
Data rozpoczęcia: 2017-01-01
Data zakończenia: 2018-01-01

Wybierz zadanie

Nieaktywne

Brak zadań nieaktywnych.

Porzuć

Zadanie: Inwentaryzacja i klasyfikacja informacji w [redacted]. (2017)

Ankieta inwentaryzacji i klasyfikacji informacji w [redacted].

UWAGA: Przy wypełnianiu formularza w polach tekstowych należy unikać wpisywania znaków specjalnych typu np. „"'#$&/ |}{[]~`

Dane o wypełniającym

1 Departament lub biuro

[wybierz komórkę organizacyjną]

2 Zespół, sekcja lub samodzielne stanowisko (w przypadku braku należy wpisać słowo BRAK)

Tutaj wpisz tekst

3 Stanowisko zgłaszającego

[wskaż stanowisko]

Zbiory informacji przetwarzane na stanowisku pracy

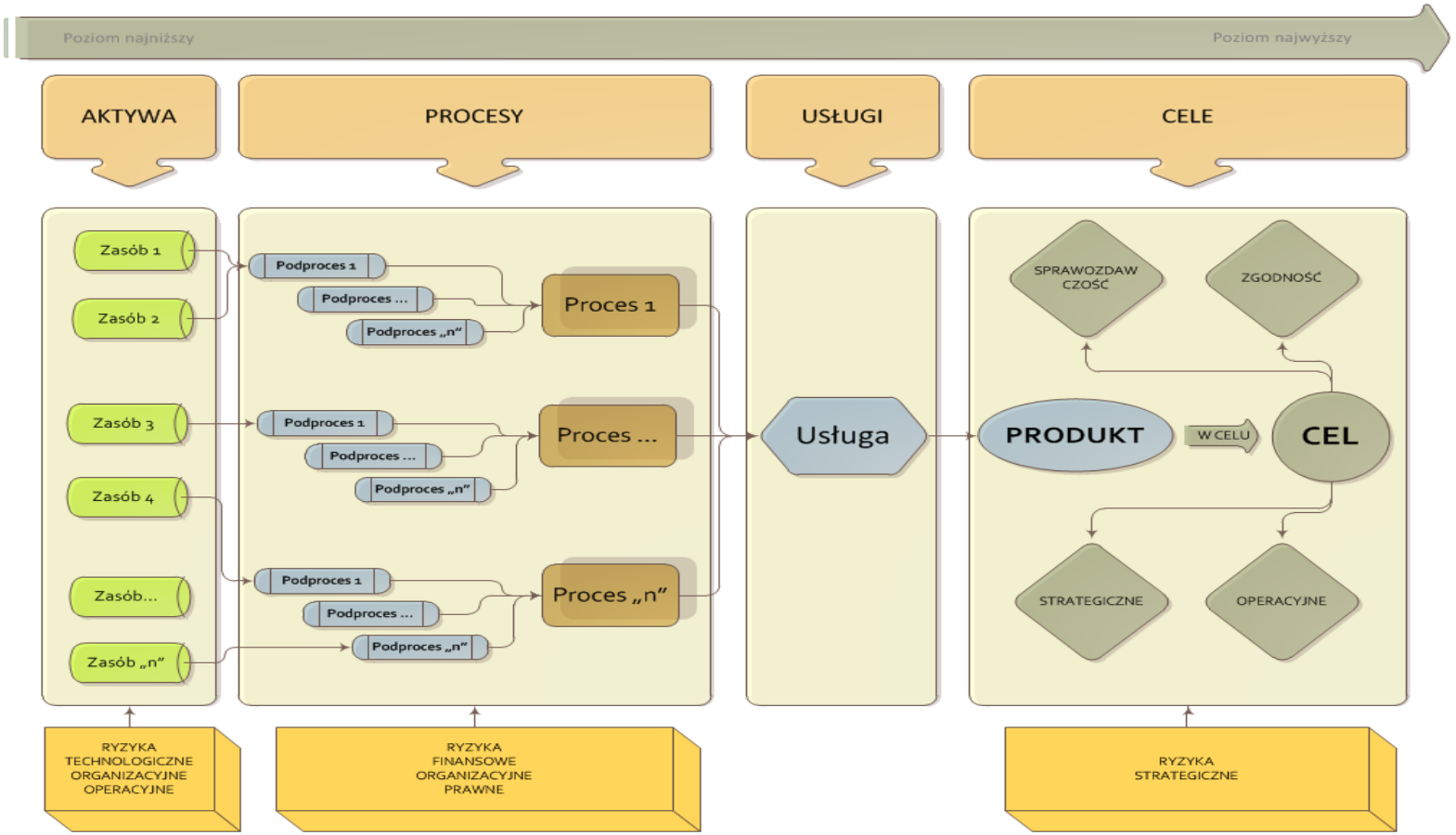
Agenda

1. Zarządzanie zbiorami danych osobowych
2. Realizacja procesu identyfikacji zbiorów danych osobowych
3. Inwentaryzacja aktywów wspierających
4. Szacowanie ryzyka utraty bezpieczeństwa informacji

Horyzont informacyjny organizacji

Blok – Inwentaryzacja aktywów wspierających

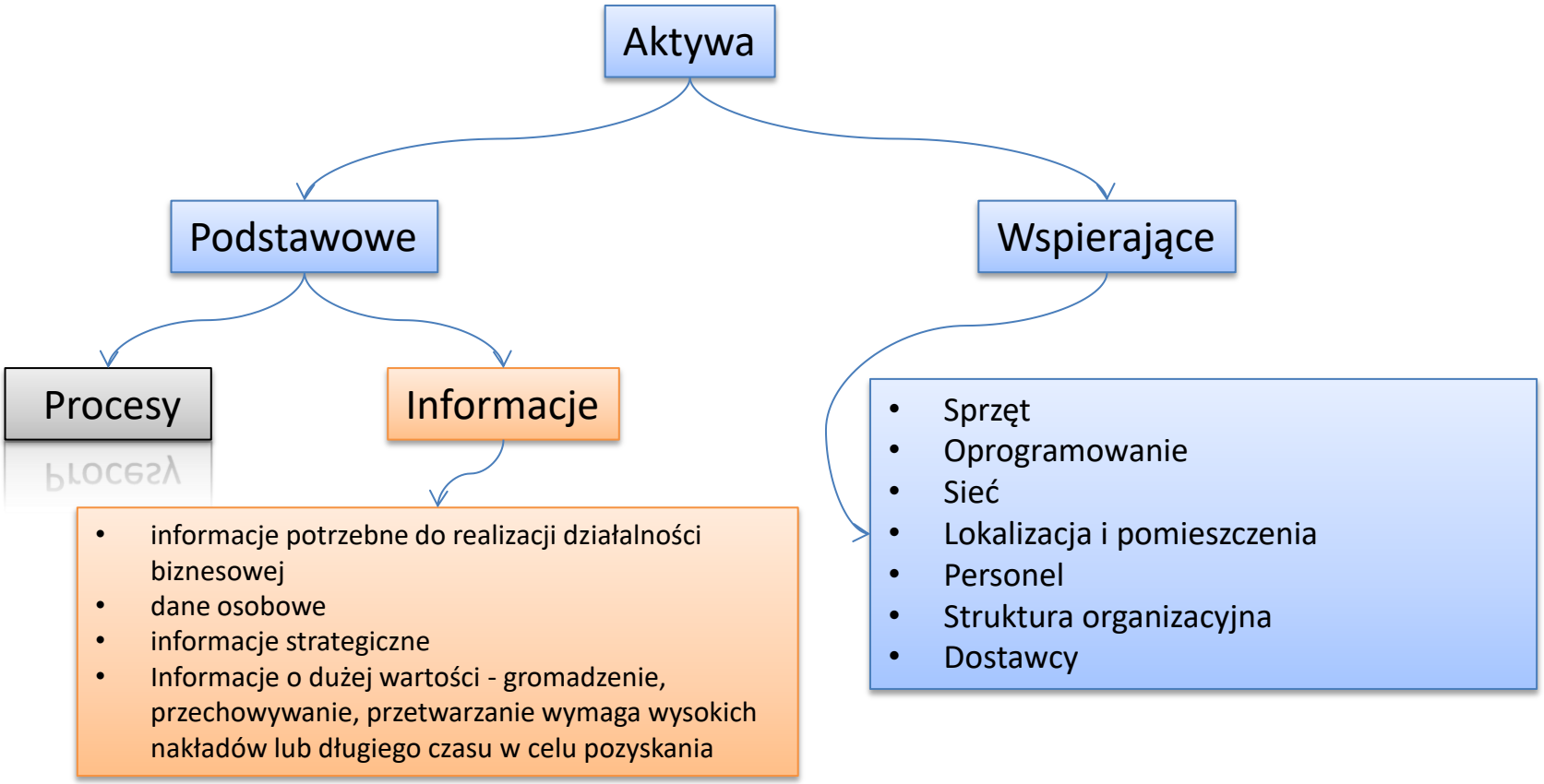
Informacje i dane przetwarzane w aktywach na różnych poziomach funkcjonowania organizacji



Aktywa – podstawowe / wspierające

Blok – Inwentaryzacja aktywów wspierających

PN-ISO/IEC 27001 oraz PN-ISO/IEC 27005



Aktywa wspierające - przykłady

Blok – Inwentaryzacja aktywów wspierających

Identyfikacja aktywów

Sieć:

- urządzenia
- protokoły transmisyjne
- interfejsy komunikacyjne
- usługi sieciowe

Personel:

- kierownictwo
- pracownicy
- administratorzy
- developerzy aplikacji

Aktywa wspierające - przykłady

Blok – Inwentaryzacja aktywów wspierających

Identyfikacja aktywów

Sprzęt:

- urządzanie przetwarzające dane
- urządzenia przenośne
- urządzenia stacjonarne
- urządzenia peryferyjne
- nośniki danych
- inne

Oprogramowanie:

- system operacyjny
- narzędzia administracyjne
- aplikacje biurowe / pudełkowe
- aplikacje biznesowe

Przykład inwentaryzacji aktywów

Blok – Inwentaryzacja aktywów wspierających

LP	Kategoria aktywu	Aktywo	Właściciel
1	Sieć	Urządzenia brzegowe – Checkpoint	Zespół ds. sieci
2	Sieć	Rutery CISCO	Zespół ds. sieci
3	Sieć	AP Wi-Fi	Zespół ds. sieci

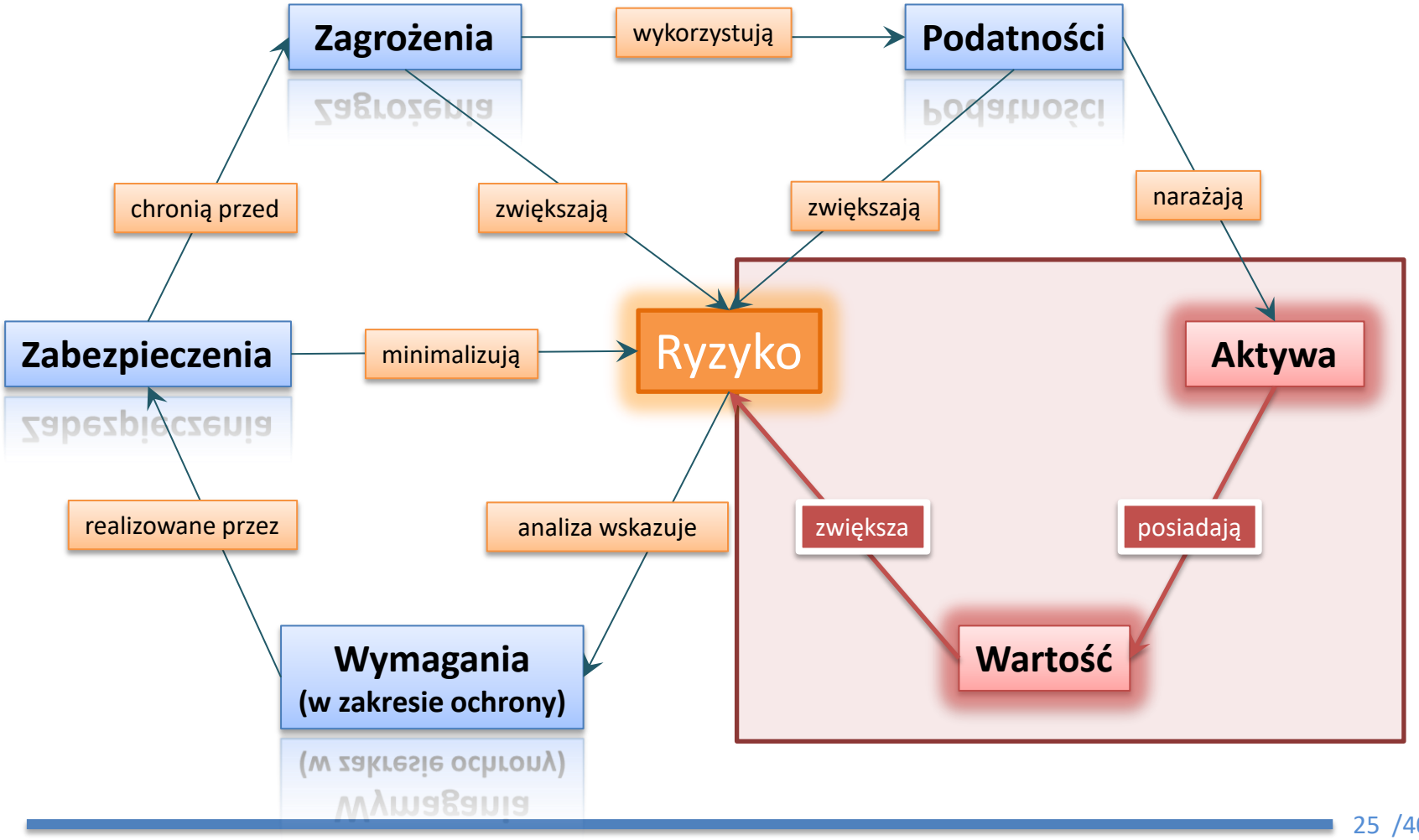
Od kilkudziesięciu do kilkuset pozycji

Agenda

1. Zarządzanie zbiorami danych osobowych
2. Realizacja procesu identyfikacji zbiorów danych osobowych
3. Inwentaryzacja aktywów wspierających
4. Szacowanie ryzyka utraty bezpieczeństwa informacji

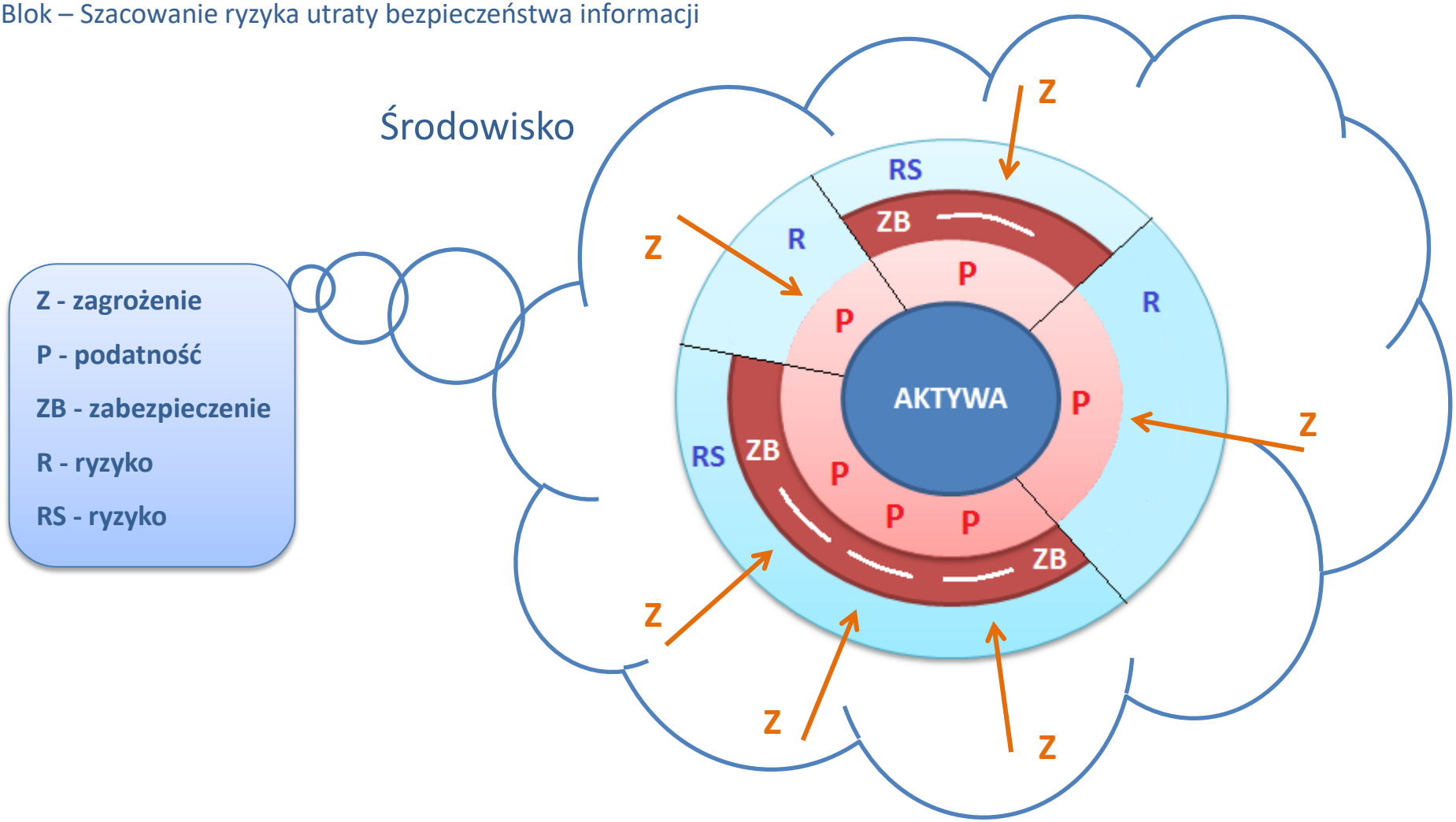
Zależności dotyczące ryzyka utraty bezpieczeństwa informacji

Blok – Szacowanie ryzyka utraty bezpieczeństwa informacji



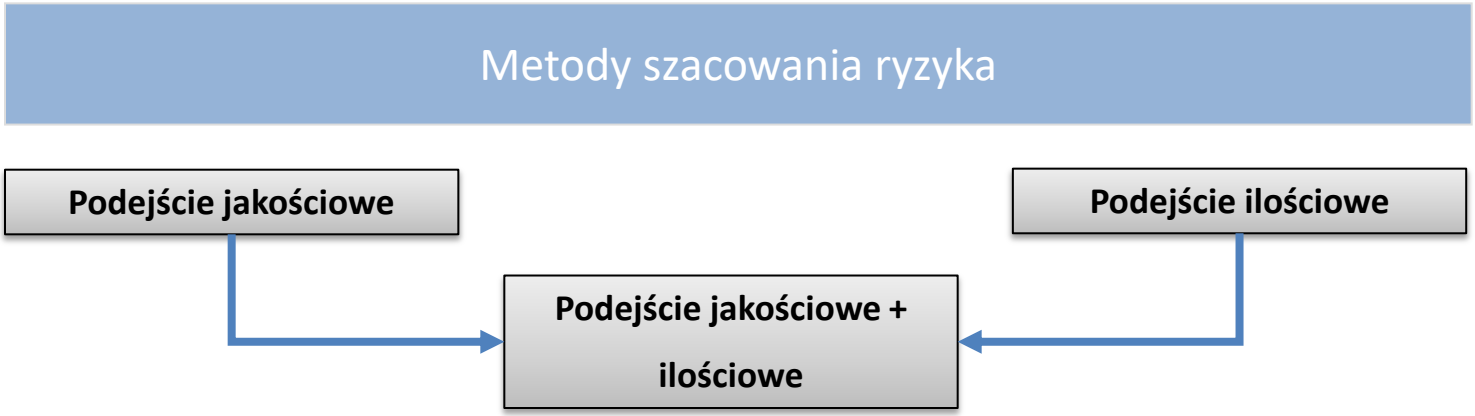
Zależności dotyczące ryzyka utraty bezpieczeństwa informacji

Blok – Szacowanie ryzyka utraty bezpieczeństwa informacji



Poziom ryzyka – metody określania

Blok – Szacowanie ryzyka utraty bezpieczeństwa informacji



Podejście jakościowe:

- wykorzystuje skalę klasyfikacji atrybutów oraz prawdopodobieństwa ich wystąpienia (np. Niskie, Średnie, Wysokie)
- skale mogą być dowolnie dopasowane do potrzeb organizacji

Podejście ilościowe:

- wykorzystuje skalę z wartościami numerycznymi do określenia konsekwencji oraz prawdopodobieństwa wystąpienia

Cyberatak

Blok – Szacowanie ryzyka utraty bezpieczeństwa informacji

Atak cybernetyczny - dowolny rodzaj działań ofensywnych stosowanych przez jednostki, grupy lub organizacje wspierane przez państwa narodowe i przez nie wyposażane, które atakują komputerowe systemy informatyczne, infrastrukturę, sieci komputerowe i / lub komputery osobiste za pomocą różnych złośliwych metod.

Ataki cybernetyczne są maskowane - zazwyczaj pochodzą z anonimowych źródeł, a ich głównym celem jest przejęcie kontroli nad zasobami poprzez nielegalne włamania do podatnych systemów.

Ataki cybernetyczne są ukierunkowane na kradzież, zmianę lub zniszczenie określonego celu.

Coraz częściej celem ataków staje się infrastruktura krytyczna.

Przykłady realnych zagrożeń

Blok – Szacowanie ryzyka utraty bezpieczeństwa informacji

2007

Atak cybernetyczny na Estonię – zmasowany atak prowadzony przez hakerów przeciwko Estonii od 17 maja 2007.

Według niektórych źródeł hakerzy powiązani byli z władzami Federacji Rosyjskiej, nie zostały jednak przedstawione żadne dowody potwierdzające tę tezę. W wyniku ataku zostały zablokowane serwery i strony Zgromadzenia Państwowego, agend rządowych, banków i mediów.

Przykłady realnych zagrożeń

Blok – Szacowanie ryzyka utraty bezpieczeństwa informacji

Stuxnet: Iran potwierdza atak na elektrownię atomową

Michał Chudziński 30-11-2010, 06:51

Doszło do sabotowania niektórych komponentów elektrowni atomowej poprzez wprowadzenie do nich złośliwego oprogramowania. Winnymi są, zdaniem Teheranu, państwa wrogo do niego nastawione.

2010

Zaawansowany robak Stuxnet jest znany od roku 2010. Został najprawdopodobniej stworzony przez siły kontrolowane przez CIA i Mossad.

Celem ataku była irańska elektrownia atomowa.

Zagrożenie traktowane jest niezwykle poważnie, gdyż ewentualne zniszczenie elektrowni atomowej mogłoby zagrozić nie tylko kruchemu pokojowi na Bliskim Wschodzie, ale także doprowadzić do katastrofy humanitarnej i ekologicznej.

W wyniku ataku Iran wstrzymał czasowo program wzbogacania uranu.

STUXNET w ataku na irańską elektrownię skorzystał z 4 luk 0day i był wycelowany w konkretne sterowniki PLC produkcji Siemensa.

Przykłady realnych zagrożeń

Blok – Szacowanie ryzyka utraty bezpieczeństwa informacji

W 2014 roku z powodu cyberataku ucierpiała huta stali w Niemczech – hakerzy doprowadzili do awaryjnego wygaszenia pieca i ogromnych zniszczeń w infrastrukturze sieci.

2014 - 2015

W grudniu 2015 roku cyberprzestępcy zaatakowali elektrownię na Ukrainie, pozbawiając prądu 103 miasta i miasteczka.

Przykłady realnych zagrożeń

Blok – Szacowanie ryzyka utraty bezpieczeństwa informacji

W ciągu ostatniego roku rosyjscy hakerzy atakowali brytyjskie media oraz podmioty działające w obszarze telekomunikacji i energii. Taką informację przekazał Ciaran Martin, szef Narodowego Centrum Cyberbezpieczeństwa (National Cyber Security Centre, NCSC).

2017

Specjaliści od cyberbezpieczeństwa odkryli nowego wirusa wymierzonego w firmy energetyczne na terenie Europy Zachodniej. Według ekspertów nowe złośliwe oprogramowanie posiada zaawansowane mechanizmy maskowania swojej obecności w zaatakowanych systemach.

BAD RABBIT

If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you'll be provided with a bitcoin account to transfer payment. The current price is on the right.

Once we receive your payment you'll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.

Time left before the price goes up

Price for decryption:

 = 0.05

Enter your personal key or your assigned bitcoin address.

Zadanie: Rejestr ryzyka utraty bezpieczeństwa informacji

Formularz służy do zbierania informacji na temat ryzyka utraty bezpieczeństwa informacji

1

Rodzaj aktywu

Tutaj wpisz tekst

Baza danych

2

Wartość aktywu

wartość 1 (informacje ogólnodostępne, systemy pomocnicze)

3 Zagrożenie

Tutaj wpisz tekst

4 Prawdopodobieństwo wystąpienia zagrożenia

Niskie (1)

5 Opis podatności

Tutaj wpisz tekst

6 Łatwość wykorzystania podatności

Niska łatwość wykorzystania podatności (1)

7

Opis konsekwencji

Tutaj wpisz tekst

8

Wartość skutków

Niskie skutki (1)

Dodaj nowe dane

Porzuć

Przykłady rejestru ryzyka

Blok – Szacowanie ryzyka utraty bezpieczeństwa informacji

Wynik zaawansowanego eksportu danych:

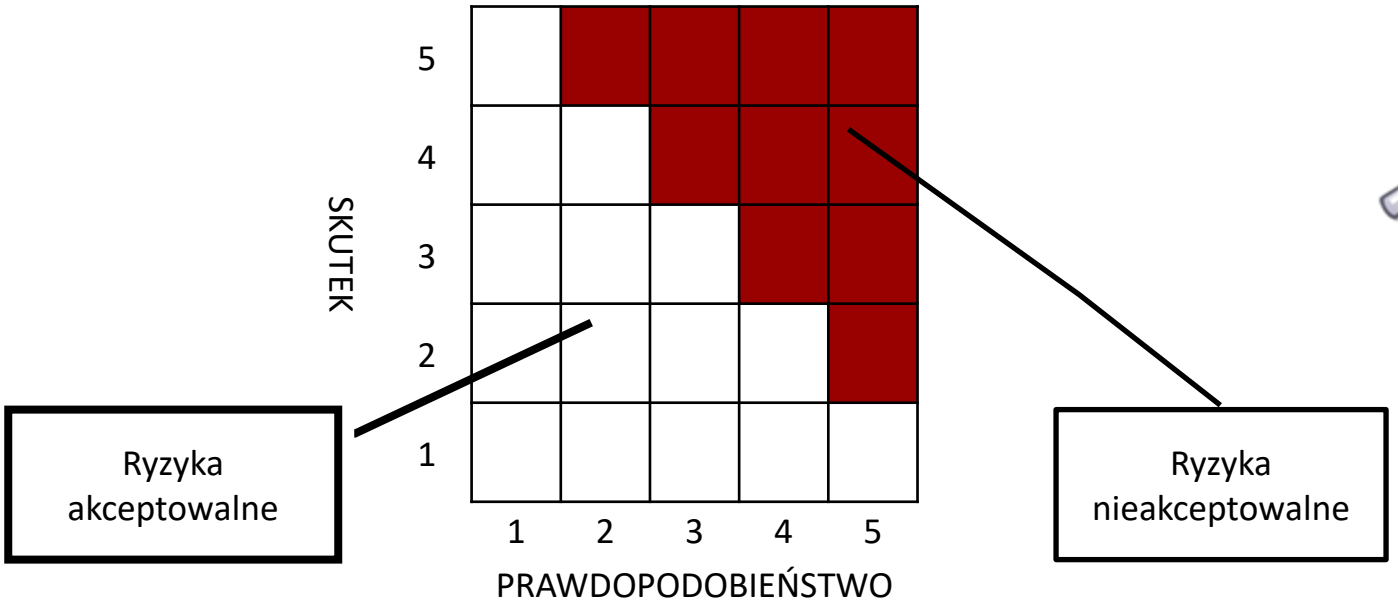
ID	Zgłosił	Właściciel	Status	Rodzaj aktywu	Wartość aktywu	Zagrożenie	Prawdopodobieństwo wystąpienia zagrożenia	Opis podatności	Łatwość wykorzystania podatności	Opis konsekwencji	Wartość skutków	Ryzyko	Plan postępowania
13	Marek Abramczyk	Właściciel danych nie został przypisany	Archiwum - zgloszenie zalatwione	Wizerunek	wartość 3 (informacje poufne, systemy krytyczne)	Negatywne opinie w mediach	Średnie (2)	Brak SZBI	Wysoka łatwość wykorzystania podatności (3)	Utrata wizerunku	Wysokie skutki (3)	54	
1	Marek Abramczyk	Marek Abramczyk	Archiwum - zgloszenie zalatwione	Serwery produkcyjne	wartość 3 (informacje poufne, systemy krytyczne)	Włamanie hakera	Niskie (1)	Brak aktualizacji OS	Wysoka łatwość wykorzystania podatności (3)	Utrata dostęności, integralności danych	Wysokie skutki (3)	27	
19		Właściciel danych nie został przypisany	Nowe zgłoszenie	Serwer AD	wartość 2 (informacje do użytku wewnętrznego, systemy ważne)	Awaria serwera	Niskie (1)	Brak procedury zarządzania zmianą	Średnia łatwość wykorzystania podatności (2)	Niedostępność AD	Średnie skutki (2)	8	

Postępowanie z ryzykiem

Blok – Szacowanie ryzyka utraty bezpieczeństwa informacji

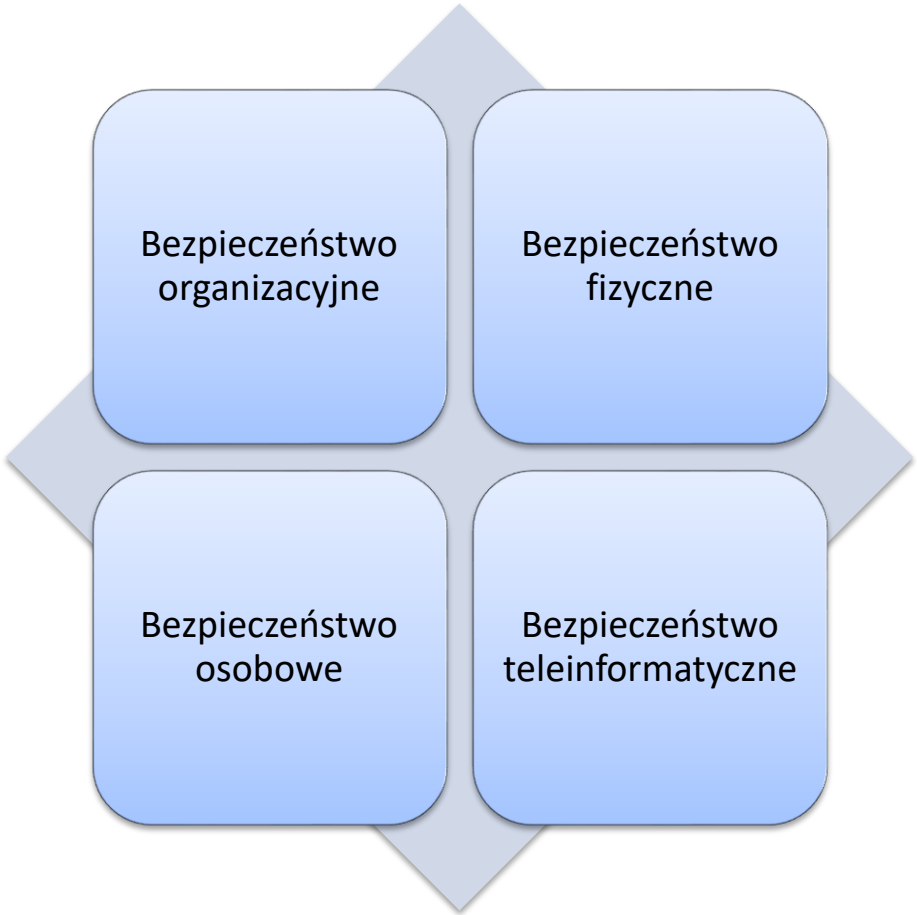
RANKING RYZYK

Apetyt na ryzyko - wielkość ryzyka, jakie organizacja jest gotowa podjąć w celu realizacji swoich zadań przy wykorzystaniu zidentyfikowanych aktywów.



Obszary bezpieczeństwa ISO/IEC 27002

Blok – Szacowanie ryzyka utraty bezpieczeństwa informacji



Dziękuję za uwagę