ANALIZA RYZYKA - PROPOZYCJA

Ocena poziomu ryzyka będzie wynikała z wyliczenia iloczynu trzech elementów: prawdopodobieństwa zmaterializowania się danego zagrożenia, podatności badanego aktywa/zasobu informacyjnego i skutku zmaterializowania się zagrożenia. Każdy z tych trzech parametrów będzie brany pod uwagę w kontekście konkretnego zagrożenia, które może naruszyć bezpieczeństwo konkretnego aktywa/zasobu informacyjnego.

Krok 1 – Zagrożenia

Dla danego zasobu/aktywu informacyjnego, związanego z analizowanym procesem, w zadaniu drugim celów szczegółowych, określone zostały zagrożenia, które będą generowały ryzyko. Krok 1 został zatem wykonany. Należy przejść do kroku drugiego.

KILKA USTALEŃ DEFINICYJNYCH:

Zagrożenie – to jakikolwiek czyn, zdarzenie, które może negatywnie wpłynąć na aktyw/zasób informacyjny potrzebny do realizacji danego procesu.

Zagrożenia, które warto brać pod uwagę oceniając ryzyko, są wielowymiarowe i różnorodne np.:

- Zagrożenia środowiskowe: powódź, burza, trzęsienia ziemi
- Zagrożenia organizacyjne: brak określonych procedur
- Zagrożenia związane z błędem ludzkim: przypadkowe usunięcie plików, przypadkowe wysłanie informacji do złego adresata
- Zagrożenia związane z błędem technicznym: awaria twardego dysku, awaria oprogramowania, awaria prądu.
- Zagrożenia z intencjonalnymi wrogimi działaniami: np. atak hakera w wyniku którego uzyskany został nielegalny dostęp do bazy danych, kradzież baz danych.

Zagrożenie może stanowić ryzyko dla zasobu tylko wtedy gdy istnieją podatności.

Podatność - jest to słabość aktywu/zasobu, którą owe zagrożenie może wykorzystać.

Podatności mogą dotyczyć wszystkich aktywów/zasobów: np. zasobów IT (np. brak aktualizacji oprogramowania), zabezpieczeń fizycznych (np. brak kontroli wejść do budynku), ludzi (np. brak kwalifikacji, znajomości polityk).

Źródło 1 ENISA.

Krok 2 – Analiza ryzyka

W kontekście każdego ryzyka, poddajemy analizie trzy elementy: prawdopodobieństwo, podatność, skutek. Wykorzystujemy do tego poniższe tabelki.

Badane kryterium		Wartość
(Pr) Prawdopodobieństwo	**Niskie** - mało realna szansa materializacji zagrożenia, podobne wypadki występowały w przeszłości w naszej organizacji (lub w	1

(możliwość wystąpienia zagrożenia)	organizacjach podobnego typu) bardzo rzadko (np. raz na dekadę).	
	Średnie – istnieje realna szansa, że zdarzenie się wydarzy. Zdarzenie wystąpiło w naszej organizacji (lub w podobnych organizacjach) w ciągu ostatnich pięciu lat.	2
	Duże - bardzo realne szanse wystąpienia zdarzenia. Zdarzenie wystąpiło w ostatnim roku w naszej organizacji (lub w organizacjach podobnego typu).	3

Badane kryterium		Wartość
(Po) Podatność *(słabość aktywa/zasobu)*	Słabości nie występują, lub jest ich mało, zabezpieczenia skuteczne.	1
	Słabości występują, zabezpieczenia są stosowane, ich skuteczność jest średnia.	2
	Występują bardzo liczne słabości, brak zabezpieczeń lub są one słabo skuteczne.	3

Badane kryterium		Wartość
(S) Skutek *(wpływ na organizację)*	Zmaterializowanie zagrożenia: - nie spowoduje długotrwałych utrudnień w pracy organizacji, - nie wpłynie negatywnie na reputacje (wizerunek) organizacji, - nie przyniesie strat finansowych.	1
	Zmaterializowanie zagrożenia: - spowoduje zakłócenia w funkcjonowaniu organizacji, - wpłynie negatywnie na reputacje (wizerunek) organizacji, - przyniesie koszty finansowe, - mogą wystąpić konsekwencje dyscyplinarne.	2
	Zmaterializowanie zagrożenia: - spowoduje długotrwałe zatrzymanie procesów realizowanych przez organizację/paraliż jej działania. Może nawet spowodować zniszczenie (aktywów/zasobów), - wywoła poważne, negatywne skutki dla reputacji (wizerunku) przedsiębiorstwa, - spowoduje duże straty finansowe, - przyniesie poważne konsekwencje prawne.	3

Następnie zastosować następujący wzór:

$$R = P_R \cdot P_O \cdot S$$

gdzie:
P_R - Prawdopodobieństwo
P_O - Podatność
S - Skutek

Każdemu elementowi ze wzoru, przypisujemy odpowiednią wartość punktową zgodnie z wcześniej dokonaną analizą.

Krok 3 - Ocena[1] ryzyka.

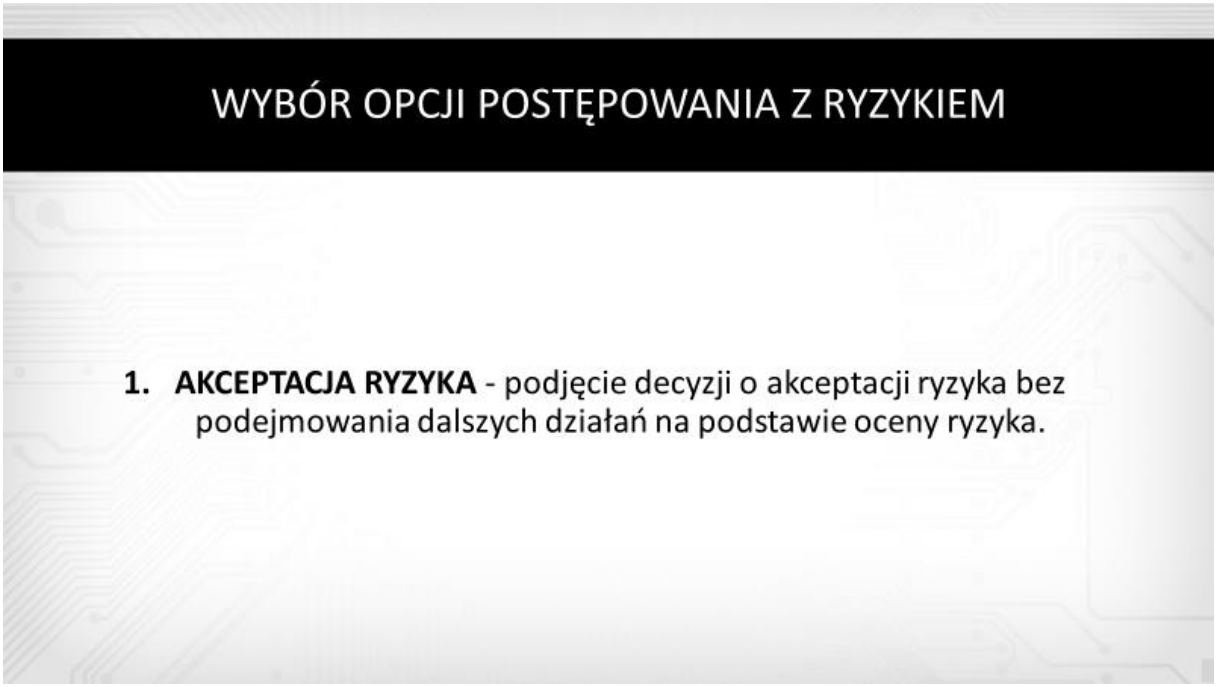
Porównujemy wynik poziomu ryzyka z przyjętą skalą.

Stosujemy poniższą tabelkę (zawiera ona wcześniej ustalone w organizacji poziomy akceptowalnego ryzyka).

Uzyskany rezultat jest punktem wyjścia do podjęcia decyzji związanych z działaniami jakie należy podjąć w stosunku do każdego ryzyka.

Klasa Kategorii	Kategoria Ryzyka	Wartość Ryzyka	Akceptacja Ryzyka Tak / Nie	Działania zapobiegawcze
1	Małe	1÷ 7	**TAK**	Ryzyko akceptowalne. Podejmowanie działań nie jest konieczne, zalecane jest utrzymywanie ryzyka na obecnym poziomie. Można podjąć działania doskonalące
2	Średnie	8 ÷ 17	**NIE**	Ryzyko nieakceptowalne. Należy podjąć działania prowadzące do zredukowania poziomu ryzyka.
3	Duże	**18 ÷ 27**	**NIE**	Ryzyko nieakceptowalne. Należy priorytetowo podjąć działania prowadzące do zredukowania poziomu ryzyka.

Strategie podstepowania z ryzykiem:



[1] Można użyć terminu „szacowanie ryzyka”, dla odróżnienia od nazwy całego procesu.

WYBÓR OPCJI POSTĘPOWANIA Z RYZYKIEM

2. UNIKANIE RYZYKA - unikanie działań lub warunków, które powodują powstanie określonych ryzyk.

WYBÓR OPCJI POSTĘPOWANIA Z RYZYKIEM

3. TRANSFER RYZYKA - transfer ryzyka do innej strony, która może skutecznie zarządzać ryzykiem.

WYBÓR OPCJI POSTĘPOWANIA Z RYZYKIEM

4. REDUKOWANIE RYZYKA - zredukowanie ryzyka **przez taki wybór zabezpieczeń**, aby ryzyko można było ponownie oszacować jako ryzyko do zaakceptowania.