OCENA RYZYKA

OCEN RYZYKA JEST ELEMENTEM STANDARDU CYBERBEZPIECZEŃSTWA PPBW DLA MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW ORAZ INSTYTUCJI PUBLICZNYCH, OPRACOWANEGO PRZEZ POLSKĄ PLATFORMĘ BEZPIECZEŃSTWA WEWNĘTRZNEGO.

SPIS TREŚCI

03

INFORMACJE WPROWADZAJĄCE

- Ocena ryzyka jest podstawowym procesem, który pozwala organizacji zapewnić bezpieczeństwo jej aktywów/zasobów informacyjnych, na poziomie adekwatnym do istniejącego poziomu ryzyka.
- Nie istnieje jedna, uniwersalna, ogólnie przyjęta metodyka oceny ryzyka. Wybór stosowanego podejścia powinien wiązać się ze specyfiką funkcjonowania organizacji i uwzględniać jej charakterystykę. Można zatem stworzyć autorską metodykę, lub dostosować istniejące. Ważna w tym kontekście jest konsekwencja w stosowaniu przyjętych założeń. Wyniki oceny ryzyka powinny być porównywalne w czasie.
- Ocena ryzyka powinna być prowadzona regularnie w wyznaczonych przez odpowiednie osoby w organizacji jednostkach czasu, dodatkowo po wprowadzeniu każdej poważnej zmiany, pojawieniu się nowego poważnego zagrożenia lub po wystąpieniu poważnego incydentu.
- Proces oceny ryzyka powinien być wciąż udoskonalany.

04

PRZYKŁADOWA METODYKA

UWAGA:

Poniżej przedstawione działania są wyłącznie propozycją metodyki jaką można zastosować, aby ocenić ryzyko w organizacji.

Proponowane podejście jest dwuetapowe (1).

Etap 1 służy zwiększaniu efektywności całego procesu oceny ryzyka. Pozwala zidentyfikować priorytety. Jego zastosowanie może znacząco zwiększyć produktywność szczególnie gdy organizacja dokonuje oceny po raz pierwszy. Działania te są rekomendowane dla MŚP przez ENISĘ(2). Przeprowadzenie procesu nie jest jednak koniecznie i można go pominąć przechodząc od razu do etapu 2.

Etap 2 to właściwa ocena ryzyka(3).

1) W standardzie PPBW nie opisano pierwszego etapu. Wynika on z tego, że jest to działanie opcjonalne.

2) ENISA ad hoc working group on risk assessment and risk management, Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs), 30/03/2006.

3) W standardzie stosowane jest określenie “szacowanie ryzyka” - znaczenie jest takie same, chodzi o fakt, że często wyrażenia stosuje się zamiennie, natomiast należy pamiętać, że będą one musiały być stosowane konsekwentnie i będzie trzeba dostrzec różnicę między całością procesu, a konkretnym działaniem realizowanym w Etapie 2, Fazie 3 (Faza 3: Ocena analizowanego ryzyka).

05

JAKIE KROKI PODJĄĆ ABY STWORZYĆ KLASYFIKACJE

ETAP 1

KROK 1
IDENTYFIKACJA PROCESÓW

KROK 2
OCENA ISTOTNOŚCI PROCESU

KROK 3
OKREŚLENIE KRYTYCZNOŚCI AKTYWÓW

KROK 4
USTALENIE PRIORYTETÓW

ETAP 2

KROK 1
ZAGROŻENIA

KROK 2
ANALIZA RYZYKA

KROK 3
OCENA RYZYKA

KROK 4
WYBÓR I REALIZACJA STRATEGII POSTĘPOWANIA Z RYZYKIEM

06

ETAP 1

Krok 1 – identyfikacja procesów, które są realizowane w organizacji

Należy zidentyfikować procesy, jakie są realizowane z organizacji. W praktyce może być to zrealizowane w grupach roboczych realizujących w organizacji określone zadania. Krok ten może być to ściśle połączony z inwentaryzacją aktywów/zasobów informacyjnych (Etap 1, Zadanie 1 według standardu PPBW). Identyfikacja procesów realizowanych w przedsiębiorstwie jest ściśle zespolone z aktywami/procesami istniejącymi w organizacji. Np. poczta e-mail oraz gromadzone CV są bezpośrednio związane z procesem rekrutacji, realizowanym w organizacji po to aby zatrudnić pracowników.

Krok 2 – określenie istotności zidentyfikowanych procesów

TYPOWE PROCESY REALIZOWANE W MAŁYCH I ŚREDNICH FIRMACH:

- **Produkcja**: rozumiana jako proces, którego realizacja służy wytworzeniu dóbr, które organizacja wytwarza (i sprzedaje, oferuje), lub zrealizowaniu usługi, którą dostarcza odbiorcom. Sedno funkcjonowania organizacji.
- **Finanse**: wszelkie operacje finansowe prowadzone przez firmę (wpłaty, przelewy za podatki, inwestycje itd.)
- **Kadry**: Wszelkie procesy związane z pracownikami, współpracownikami
- **Sprzedaż, dystrybucja, marketing**: Obsługa istniejących klientów, pozyskanie nowych

Następnie należy określić jaką wagę dla organizacji ma każdy proces z punktu widzenia celów jej działalności. Inaczej mówiąc, należy określić jak bardzo dane procesy są istotne do tego aby zrealizować dane zadanie i osiągnąć cel.

07

ETAP 1

Można przyjąć trójstopniową skalę: duża wartość, średnia, niska wartość. Przykładowo:

DUŻA WARTOŚĆ

- najważniejsze procesy z punktu widzenia organizacji, np. związane z oferowaniem najważniejszej usługi dla klienta,
- zakłócenie tych procesów może mieć katastrofalne skutki dla organizacji (np. z punktu widzenia strat finansowych lub wizerunkowych).

ŚREDNIA WARTOŚĆ

- procesy, które odgrywają ważną, lecz nie kluczową rolę dla organizacji. Są pomocnicze dla jej funkcjonowania,
- zakłócenia tych procesów przyniosą problemy i utrudnienia z punktu widzenia codziennego funkcjonowania organizacji.

NISKA WARTOŚĆ

- procesy, które nie mają dużego znaczenia dla organizacji,
- zakłócenia tych procesów wiążą się z trudnościami, ale nie prowadzą do poważnych konsekwencji.

08

ETAP 1

Krok 3 – Określenie stopnia krytyczności aktywów/zasobów ICT dla organizacji

Wpierw należy określić jak bardzo realizacja każdego ze zidentyfikowanych procesów jest zależna od właściwego funkcjonowania poszczególnych aktywów/zasobów ICT. Dla określenia zależności proponuje się przyjęcie trójstopniowej skali:

DUŻA WARTOŚĆ

- niewłaściwe funkcjonowanie aktywów/zasobów ICT bardzo poważnie zakłóci lub uniemożliwi realizację danego procesu,

ŚREDNIA WARTOŚĆ

- niewłaściwe funkcjonowanie aktywów/zasobów ICT doprowadzi do utrudnień związanych z realizacją procesu. Nie jest to jednak zakłócenie krytyczne,

NISKA WARTOŚĆ

- niewłaściwe funkcjonowanie aktywów/zasobów ICT w niewielkim stopniu utrudni realizację procesu.

09

ETAP 1

Określenie stopnia krytyczności aktywów/zasobów ICT dla organizacji następuje poprzez zestawienie wartości wcześniej zidentyfikowanych procesów ze stopniem ich zależności od systemów ICT.

UWAGA

To samo narzędzie/system może być wykorzystywane do różnych procesów i mieć różny poziom krytyczności. Ostatecznie bierzemy pod uwagę najwyższy poziom krytyczności.

RODZAJ PROCESU (np. rekrutacja)

WAGA PROCESU DLA ORGANIZACJI	ZALEŻNOŚĆ PROCESU DO AKTYWÓW/ZASOBÓW ICT		
	NISKA ZALEŻNOŚĆ	ŚREDNIA ZALEŻNOŚĆ	DUŻA ZALEŻNOŚĆ
NISKA WARTOŚĆ	Bardzo niski poziom krytyczności	Bardzo niski poziom krytyczności	Bardzo niski poziom krytyczności
ŚREDNIA WARTOŚĆ	Bardzo niski poziom krytyczności	Niski poziom krytyczności	Średni poziom krytyczności
DUŻA WARTOŚĆ	Niski poziom krytyczności	Średni poziom krytyczności	Bardzo wysoki poziom krytyczności

Krok 4 – Ustalenie priorytetów:

Wynik określenia stopnia krytyczności aktywów/zasobów ICT dla organizacji daje odpowiedź, które procesy i wykorzystywane dla ich realizacji narzędzia/systemy ICT, należy poddać w pierwszej kolejności dokładnej ocenie ryzyka. Może być ona przeprowadzona na przykład według metodyki zaproponowanej poniżej (Etap 2).

ETAP 2

Etap drugi to już właściwa ocena ryzyka, przeprowadzona według wybranej metodyki (Więcej patrz: ETAP 2 Standardu PPBW). Poniżej zaproponowany został przykład jak może wyglądać metodyka[4].

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, należy określić zagrożenia jakie będą generowały ryzyko. Zaleca się tworzenie listy zagrożeń, która będzie na bieżąco uzupełniana (w załączniku 1 PRZYKŁADOWA lista zagrożeń). Przy jej tworzeniu można posłużyć się rożnymi metodami. Analizą istniejących źródeł (raportów itd.), burzą mózgów, konsultacjami z ekspertami, ankietami itd.).

Warto skoncentrować się na kilkunastu, najważniejszych zagrożeniach i poddać je bardziej pogłębionej analizie. Jak wybrać kluczowe zagrożenia? Może być to decyzja właściciela aktywu, może być to wynik głosowania zespołu.

4) Modyfikowana Procedura oceny ryzyka bezpieczeństwa informacji, Załącznik do Zarządzenia Prezydenta Miasta Jastrzębie-Zdrój Nr Or.IV.0050.635.2015 z dnia 23 listopada 2015 w sprawie wprowadzenia w Urzędzie Miasta w Jastrzębiu-Zdroju „Procedury oceny ryzyka bezpieczeństwa informacji.

11

WYBRANE USTALENIA DEFINICYJNE

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

ETAP 2

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 (możliwość wystąpienia zagrożenia)	**Niskie** - mało realna szansa materializacji zagrożenia, podobne wypadki występowały w przeszłości w naszej organizacji (lub w organizacjach podobnego typu) bardzo rzadko (np. raz na dekadę).	1
	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

ETAP 2

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

ETAP 2

Następnie zastosować następujący wzór:
R = Pr · Po · S

gdzie:
Pr - Prawdopodobieństwo
Po - Podatność
S - Skutek

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

Krok 3 - Ocena (5) 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.

5) Można użyć terminu „szacowanie ryzyka", dla odróżnienia od nazwy całego procesu.

ETAP 2

Klasa Kategorii	Kategoria ryzyka	Wartość ryzyka	Akceptacja ryzyka	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.

ETAP 2

Krok 4 – Wybór i realizacja strategii postępowania z ryzykiem.

Należy wybrać i zrealizować strategię postępowania z ryzykiem. Dla ryzyka nieakceptowalnego istnieją 3 warianty decyzji:

- wdrożenie zabezpieczeń, które obniżą poziom ryzyka (np. poprzez eliminację podatności, obniżenie skutków materializacji zagrożenia),
- dokonanie transferu ryzyka do innych podmiotów takich jak np. ubezpieczyciel, dostawca, partner biznesowy,
- unikanie ryzyka – np. niepodejmowanie czynności, które mogą podnosić poziom ryzyka,
- akceptacja (retencja),
- sharing.

ETAP 2

Przykład - Kancelaria prawna

Proces biznesowy	Wartość dla biznesu	Zależność od ICT	Krytyczność aktywów/zasobów ICT
Doradztwo prawne (Produkcja)	**Duża wartość**	Baza danych związanych ze sprawami – duża zależność	Bardzo wysoki poziom krytyczności
		E-mail – średnia zależność	Średni poziom krytyczności
		Infrastruktura IT (hardware, system operacyjny, sieć) – duża zależność	Bardzo wysoki poziom krytyczności
		Aplikacja do śledzenia czasu – niska zależność	Niski poziom krytyczności
Marketing	**Niska wartość**	Strona www - średnia zależność	Bardzo niski poziom krytyczności
		Social media - niska zależność	Bardzo niski poziom krytyczności
Rekrutacja (Kadry)	**Średnia wartość**	Baza danych kandydatów – niska zależność	Bardzo niski poziom krytyczności
		E-mail – średnia zależność	Niski poziom krytyczności
		Portal rekrutacyjny – średnia zależność	Niski poziom krytyczności

UWAGA!

Jak widać na powyższym przykładzie, ten sam aktyw/zasób informacyjny (np. e-mail), dla różnych procesów może mieć różny poziom krytyczności. W takiej sytuacji należy przyjąć najwyższy zidentyfikowany poziom.

ETAP 2

Należy wykonać pogłębioną analizę ryzyka, w pierwszej kolejności dla bazy danych związanych z realizacją procesu doradztwa prawnego dla klientów kancelarii.

Jednym ze zidentyfikowanych zagrożeń będzie na przykład: - atak prowadzący do zaszyfrowania bazy danych.
Rozpoczynamy analizę ryzyka i podstawiamy dane pod wzór:
R = Pr · Po · S

gdzie:

Pr – prawdopodobieństwo – 2 – ze względu na charakter organizacji, wagę przetwarzanych informacji, oraz obserwując wydarzenia w podobnych podmiotów, istnieje realna szansa, że zdarzenie się wydarzy.

Zdarzenie wystąpiło w naszej organizacji (lub w podobnych organizacjach) w ciągu ostatnich pięciu lat.

Po – podatność - występują nieliczne słabości (np. częste zmiany pracowników, mających dostęp do bazy), istnieje wiele zabezpieczeń – (np. regularne backupy) – 1.

S – skutki - brak dostępu do bazy może być paraliżujący dla funkcjonowania kancelarii – 3.

Wynik: 2x1x3=6 – ryzyko niskie – akceptowalne.

ZAŁĄCZNIK 1. PRZYKŁADY[6]:

PRZYKŁADOWE ZAGROŻENIA:

1. Zainstalowanie złośliwego oprogramowania przez korespondencję elektroniczną prowadzące do uzyskania dostępu do aktywów/zasobów informacyjnych.
2. Zainstalowanie złośliwego oprogramowania przez korespondencję elektroniczną prowadzące do modyfikacji aktywów/zasobów informacyjnych.
3. Zainstalowanie złośliwego oprogramowania przez korespondencję elektroniczną prowadzące do usunięcia aktywów/zasobów informacyjnych.
4. Zainstalowanie złośliwego oprogramowania przez korespondencję elektroniczną prowadzące do zaszyfrowania aktywów/zasobów informacyjnych.
5. Zainstalowanie złośliwego oprogramowania przez stronę www elektroniczną prowadzące do uzyskania dostępu do aktywów/zasobów informacyjnych.
6. Zainstalowanie złośliwego oprogramowania przez stronę www prowadzące do modyfikacji aktywów/zasobów informacyjnych.
7. Zainstalowanie złośliwego oprogramowania przez stronę www prowadzące do usunięcia aktywów/zasobów informacyjnych.
8. Zainstalowanie złośliwego oprogramowania przez stronę www prowadzące do zaszyfrowania aktywów/zasobów informacyjnych.
9. Zainstalowanie złośliwego oprogramowania przez nośniki zewnętrzne prowadzące do uzyskania dostępu do aktywów/zasobów informacyjnych.
10. Zainstalowanie złośliwego oprogramowania przez nośniki zewnętrzne prowadzące do modyfikacji aktywów/zasobów informacyjnych.
11. Zainstalowanie złośliwego oprogramowania przez nośniki zewnętrzne prowadzące do usunięcia aktywów/zasobów informacyjnych.

6) Na podstawie m.in. TZ-Consultans Tadeusz Zawistowski, Metodyka oceny ryzyka do przygotowania sprawozdania za rok 2013; Krzysztof Liderman, Oszacowania jakościowe ryzyka dla potrzeb bezpieczeństwa teleinformatycznego, Biuletyn Instytutu Automatyki i Robotyki NR 19, 2003; MC, Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych, Warszawa 2015.

ZAŁĄCZNIK 1. PRZYKŁADY[6]:

PRZYKŁADOWE ZAGROŻENIA:

12. Zainstalowanie złośliwego oprogramowania przez nośniki zewnętrzne prowadzące do zaszyfrowania aktywów/zasobów informacyjnych.
13. Zainstalowanie złośliwego oprogramowania w instalowanym oprogramowaniu, prowadzące do uzyskania dostępu do aktywów/zasobów informacyjnych.
14. Zainstalowanie złośliwego oprogramowania w instalowanym oprogramowaniu, prowadzące do modyfikacji aktywów/zasobów informacyjnych.
15. Zainstalowanie złośliwego oprogramowania w instalowanym oprogramowaniu, prowadzące do usunięcia aktywów/zasobów informacyjnych.
16. Zainstalowanie złośliwego oprogramowania w instalowanym oprogramowaniu, prowadzące do zaszyfrowania aktywów/zasobów informacyjnych.
17. Zainstalowanie złośliwego oprogramowania w trakcie naprawy lub serwisu, prowadzące do uzyskania dostępu do aktywów/zasobów informacyjnych.
18. Zainstalowanie złośliwego oprogramowania w trakcie naprawy lub serwisu, prowadzące do modyfikacji aktywów/zasobów informacyjnych.
19. Zainstalowanie złośliwego oprogramowania w trakcie naprawy lub serwisu, prowadzące do usunięcia aktywów/zasobów informacyjnych.
20. Zainstalowanie złośliwego oprogramowania w trakcie naprawy lub serwisu, prowadzące do zaszyfrowania aktywów/zasobów informacyjnych.
21. Wykorzystanie luk w systemach urządzeń mobilnych, prowadzące do uzyskania dostępu do aktywów/zasobów informacyjnych.

ZAŁĄCZNIK 1. PRZYKŁADY[6]:

PRZYKŁADOWE ZAGROŻENIA:

22. Wykorzystanie luk w systemach urządzeń mobilnych, prowadzące do modyfikacji aktywów/zasobów informacyjnych.
23. Wykorzystanie luk w systemach urządzeń mobilnych, prowadzące do usunięcia aktywów/zasobów informacyjnych.
24. Wykorzystanie luk w systemach urządzeń mobilnych, prowadzące do zaszyfrowania aktywów/zasobów informacyjnych.
25. Atak zewnętrzny ograniczający dostęp do aktywów/zasobów informacyjnych typu DDoS.
26. Przejęcie aktywów/zasobów informacyjnych przesyłanych pocztą elektroniczną.
27. Podsłuchanie aktywów/zasobów informacyjnych przesyłanych siecią radiową.
28. Podsłuchanie aktywów/zasobów informacyjnych przesyłanych siecią tradycyjną.
29. Atak socjotechniczny w celu przejęcia aktywów/zasobów informacyjnych (phishing).
30. Nieuprawniony fizyczny dostęp do aktywów/zasobów informacyjnych.
31. Brak zasilania energetycznego uniemożliwiający korzystanie z aktywów/zasobów informacyjnych.
32. Zalanie wodą lub innymi substancjami z instalacji wewnętrznych uniemożliwiające korzystanie z aktywów/zasobów informacyjnych.
33. Zalanie wodą lub innymi substancjami z instalacji wewnętrznych niszczący aktywa/zasoby informacyjne.
34. Pożar niszczący aktywa/zasoby informacyjne.
35. Pożar uniemożliwiający korzystanie z aktywów/zasobów informacyjnych.
36. Katastrofa budowlana uniemożliwiająca korzystanie z aktywów/zasobów informacyjnych.
37. Katastrofa budowlana niszcząca aktywa/zasoby informacyjne.

ZAŁĄCZNIK 1. PRZYKŁADY:

PRZYKŁADOWE ZAGROŻENIA:

38. Powódź niszcząca aktywa/zasoby informacyjne.
39. Powódź uniemożliwiająca korzystanie z aktywów/zasobów informacyjnych.
40. Przegrzanie sprzętu uniemożliwiająca korzystanie z aktywów/zasobów informacyjnych.
41. Awaria sprzętu uniemożliwiająca korzystanie z aktywów/zasobów informacyjnych.
42. Niewydolne urządzenia (zbyt wolne, nieodpowiadające wymaganiom programowym) uniemożliwiające korzystanie z aktywów/zasobów informacyjnych.
43. Niestabilność łącza w usłudze dostępu do internetu uniemożliwiająca korzystanie z aktywów/zasobów informacyjnych.
44. Niewystarczająca przepustowość łącza w usłudze dostępu do internetu utrudniająca korzystanie z aktywów/zasobów informacyjnych.
45. Kradzież aktywów/zasobów informacyjnych z siedziby jednostki.
46. Kradzież mobilnych aktywów/zasobów informacyjnych.
47. Zgubienie aktywów/zasobów informacyjnych.
48. Podejrzenie aktywów/zasobów informacyjnych w siedzibie jednostki.
49. Podejrzenie aktywów/zasobów informacyjnych przetwarzanej na sprzęcie mobilnym.
50. Błędy uprawnionych użytkowników – niezapisanie aktywów/zasobów informacyjnych.
51. Błędy uprawnionego użytkownika – skasowanie aktywów/zasobów informacyjnych.
52. Błąd uprawnionego użytkownika – wysłanie informacji pocztą elektroniczną do nieuprawnionej osoby.
53. Celowe działanie uprawnionych użytkowników – zniszczenie aktywów/zasobów informacyjnych.

ZAŁĄCZNIK 1. PRZYKŁADY:

PRZYKŁADOWE ZAGROŻENIA:

54. Celowe działanie uprawnionych użytkowników – sprzedaż aktywów/zasobów informacyjnych.
55. Celowe działanie uprawnionych użytkowników – sabotaż aktywów/zasobów informacyjnych.
56. Celowe działanie uprawnionych użytkowników – nadużycie uprawnień.
57. Celowe działanie – zniszczenie aktywów/zasobów informacyjnych.
58. Zamach terrorystyczny.
59. Stosowanie korupcji oraz szantażu w celu wydobycia określonych informacji od wybranych pracowników firmy.
60. Infiltracja środowiska przez wyszukiwanie osób uważających się za pokrzywdzone przez pracodawcę, zwalnianych lub poszukujących zatrudnienia w innej komórce organizacyjnej.
61. Brak dostępu do aktywów/zasobów ze względu na nieobecność osób, które mają do nich uprawnienia.

PRZYKŁADOWE PODATNOŚCI:

1. Brak świadomości użytkowników na temat ryzyk (zagrożeń, podatności, skutków).
2. Brak znajomości zasad i procedur bezpieczeństwa.
3. Zbyt rzadko zmieniane hasła.
4. Zbyt słabe hasła.
5. Zbyt często zmieniane hasła.
6. Nieprzestrzeganie przez użytkowników zasad i procedur bezpieczeństwa.
7. Nieprawidłowe zarządzanie uprawnieniami użytkowników – nadanie nadmiernych uprawnień.
8. Nieprawidłowe zarządzanie uprawnieniami użytkowników – brak cofnięcia albo bardzo opóźnione cofnięcie uprawnień.
9. Błąd uprawnionego użytkownika – administratora – błędna konfiguracja dająca nadmierne uprawnienia.
10. Źle skonfigurowane, w tym otwarte porty.
11. Źle skonfigurowane systemy operacyjne.
12. Brak zabezpieczeń protokołów komunikacyjnych.

ZAŁĄCZNIK 1. PRZYKŁADY:

PRZYKŁADOWE PODATNOŚCI:

13. Korzystanie z nielicencjonowanego oprogramowania.
14. Nierzetelne kontrola rejestrowanych zdarzeń systemowych.
15. Korzystanie z prywatnych zasobów informacyjnych.
16. Brak lub złe umiejscowienie w systemie, lub brak aktualizacji oprogramowania typu AV.
17. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja zapór sieciowych (firewall).
18. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja oprogramowania IPS/IDS i jego sond.
19. Niewłaściwa konfiguracja mechanizmów bezpieczeństwa w sieciach WAN.
20. Brak monitorowania obciążenia serwerów.
21. Podatność użytkowników na oddziaływanie metod inżynierii społecznej w celu uzyskania informacji lub wprowadzenia kodu złośliwego.
22. Niewłaściwa konfiguracja mechanizmów bezpieczeństwa w sieciach LAN.
23. Brak nadzoru nad ruchem w sieci (QoS).
24. Brak nadzoru nad uprawnieniami użytkowników, uprawnienia nieadekwatne do zadań.
25. Brak kontroli dostępu fizycznego do elementów systemu.
26. Brak szyfrowania w łączach WAN.
27. Brak aktualizacji oprogramowania systemowego.

ZAŁĄCZNIK 1. PRZYKŁADY:

WIECEJ INFORMACJI NA TEMAT OCENY RYZYKA:

- ENISA ad hoc working group on risk assessment and risk management, Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs), 30/03/2006.
- Modyfikowana Procedura oceny ryzyka bezpieczeństwa informacji, Załącznik do Zarządzenia Prezydenta Miasta Jastrzębie-Zdrój Nr Or.IV.0050.635.2015 z dnia 23 listopada 2015 w sprawie wprowadzenia w Urzędzie Miasta w Jastrzębiu-Zdroju „Procedury oceny ryzyka bezpieczeństwa informacji.
- TZ-Consultans Tadeusz Zawistowski, Metodyka oceny ryzyka do przygotowania sprawozdania za rok 2013.
- Krzysztof Liderman, Oszacowania jakościowe ryzyka dla potrzeb bezpieczeństwa teleinformatycznego, Biuletyn Instytutu Automatyki i Robotyki NR 19, 2003.
- MC, Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych, Warszawa 2015.

POLSKA PLATFORMA
BEZPIECZEŃSTWA WEWNĘTRZNEGO

Polska Platforma Bezpieczeństwa Wewnętrznego

ul. Słowackiego 17/11
60-822 Poznań
www.ppbw.pl
tel.: (61) 663 02 21
e-mail: standard-cyber@ppbw.pl

Fundusze Europejskie Inteligentny Rozwój
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Projekt pt.: „Cyberbezpieczeństwo – standard PPBW dla MŚP i instytucji publicznych" współfinansowany ze środków Unii Europejskiej.