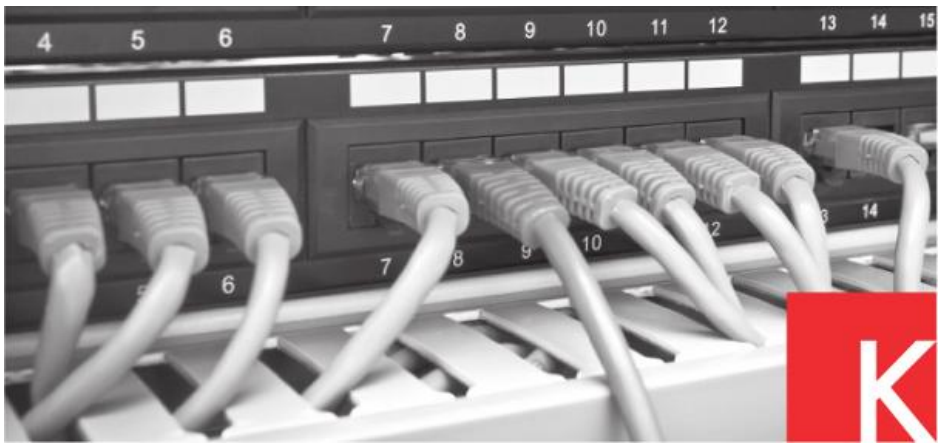
2012

Metodyka zarządzania ryzykiem w obszarze bezpieczeństwa informacji

Veracity

Niniejszy przewodnik dostarcza praktycznych informacji związanych z wdrożeniem metodyki zarządzania ryzykiem w obszarze bezpieczeństwa informacji.



Fundacja Veracity
2012-07-15

Spis treści

Wprowadzenie

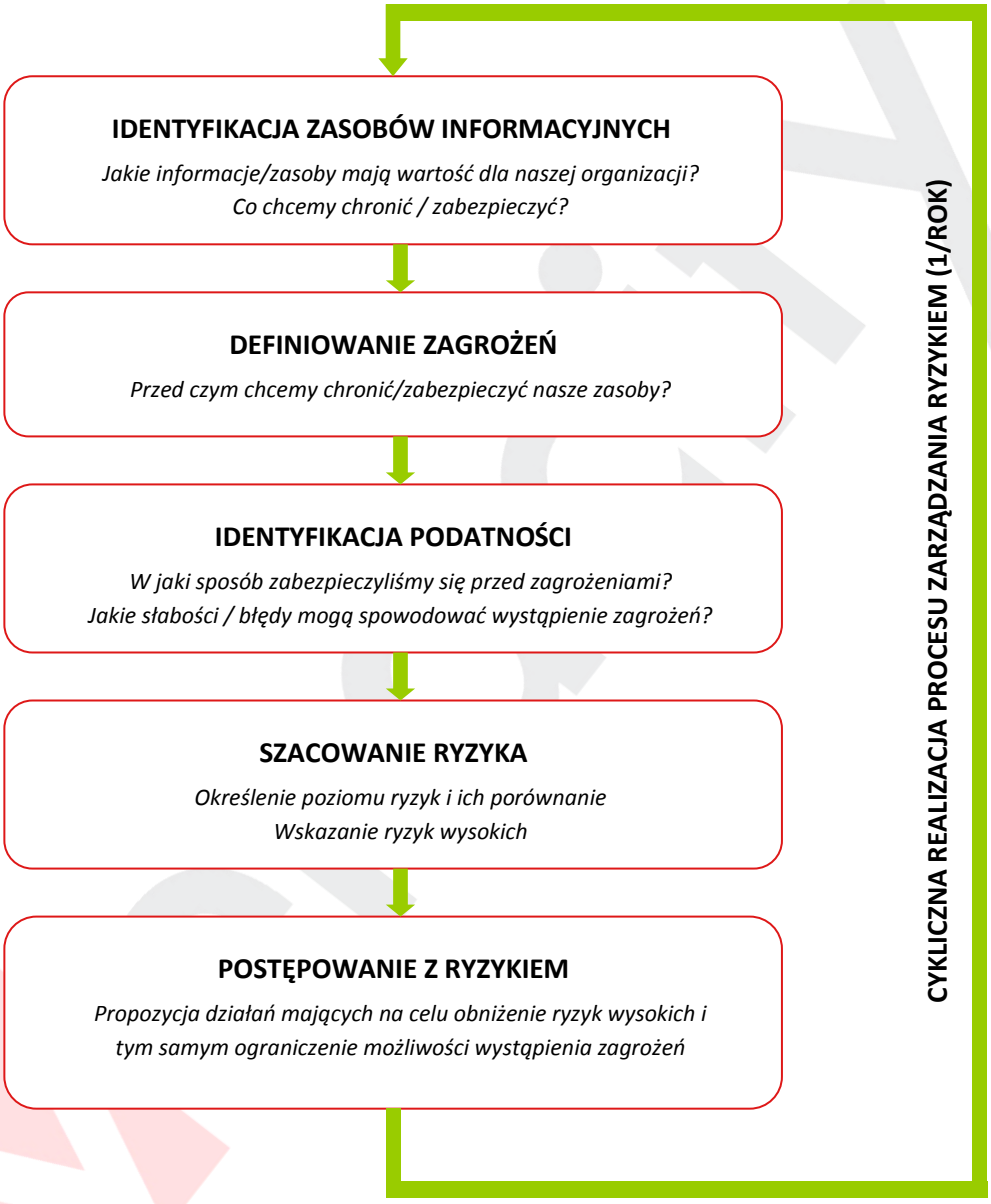
Proces zarządzania ryzykiem jest procesem cyklicznym realizowanym w celu zdefiniowania najważniejszych zagrożeń, które wpłynąć mogą negatywnie na informacje przetwarzane w naszej organizacji.

Opracowana metodyka zarządzania ryzykiem w obszarze bezpieczeństwa informacji określa główne etapy procesu zarządzania ryzykiem oraz role i odpowiedzialności w zakresie ich realizacji.

Przeprowadzenie procesu zarządzania ryzykiem pozwoli nam wdrożyć rozwiązania organizacyjne lub techniczne przede wszystkim w tych obszarach, które są kluczowe z punktu widzenia naszej organizacji, jak również w ujęciu najbardziej prawdopodobnych zagrożeń jakie mogą wystąpić w naszej organizacji.

Administrator Bezpieczeństwa – rola/osoba odpowiedzialna za obszar bezpieczeństwa informacji w naszej organizacji

Główne etapy procesu zarządzania ryzykiem



Identyfikacja zasobów informacyjnych

W pierwszym kroku procesu zarządzania ryzykiem, musimy określić jakie informacje przetwarzamy w naszej organizacji oraz jakie zasoby/systemy wykorzystujemy do ich przetwarzania. Mówiąc o informacjach najlepiej podzielić je w grupy tematyczne tworząc tzw. grupy informacji. Dla przykładu mogą to być m.in. informacje finansowo-księgowe, dane kadrowe, dane strategiczne, dane Klientów itp.

Za inwentaryzacje aktywów na poziomie poszczególnych komórek organizacyjnych odpowiedzialni mogą być ich kierownicy. Osoby na poziomie kierowników powinni być również wyznaczone jako Właściciele zasobów, którzy odpowiadają m.in. za określenie ważności danej grupy informacji i zasad postępowania z tą grupą informacji w naszej organizacji.

Mając wyznaczone grupy informacji wraz z właścicielami należy określić ważność tych grup informacji wg przyjętych kryteriów. Ocena ważności grup informacji powinna uwzględniać trzy aspekty bezpieczeństwa informacji a mianowicie poufność, integralność oraz dostępność i może przyjmować wartości liczbowe (np. 1-4) jak i opisowe/jakościowe np. krytyczne, ważne, wewnętrzne, ogólnodostępne. Ważność grupy informacji przekładać się będzie na skutek jej utraty w przypadku wystąpienia konkretnego zagrożenia (skutek utraty ważnych informacji jest proporcjonalnie większy do skutku utraty informacji mniej ważnych).

Dla poszczególnych informacji zaleca się również wskazać systemy informatyczne wykorzystywane do przetwarzania tych informacji.

Wynikiem etapu I jest lista grup informacji ocenionych pod względem ważności wraz z właścicielami zasobów oraz zasobami/systemami informatycznymi wykorzystywanymi do przetwarzania tych informacji.

Zebrane od kierowników dane Administrator Bezpieczeństwa uspójnia i przedstawia najwyższemu kierownictwu do zatwierdzenia.

Definiowanie zagrożeń

Realizacja etapu pierwszego pozwala nam zidentyfikować i ocenić zasoby informacyjne w naszej organizacji. Celem etapu drugiego jest zidentyfikowanie zagrożeń, które mogą wpłynąć na utratę poufności, integralności i dostępności tych zasobów. Zagrożenia to nic innego jak odpowiedź na pytanie co złego może stać się z naszymi informacji.

Etap ten zrealizowany może być przez Administratora Bezpieczeństwa przy wsparciu Właścicieli zasobów.

Zaleca się, aby zidentyfikować zagrożenia, których realizacja jest realna w środowisku w jakim funkcjonuje organizacja. Tym samym często uwzględniane będą zagrożenia typu pożar, kradzież, atak wirusowy, natomiast rzadziej zagrożenia typu erupcja wulkanu, trzęsienie ziemi. W praktyce lista zagrożeń nie powinna być zbyt rozbudowana. Stworzenie katalogu większego niż 20-30 zagrożeń spowoduje duże problemy podczas etapu szacowania ryzyka.

Administrator Bezpieczeństwa przedstawia listę zagrożeń do zatwierdzenia najwyższemu kierownictwu.

Identyfikacja podatności

Mając wiedzę o tym co chcemy chronić, jak również przed czym chcemy się chronić, przechodzimy do oceny aktualnego stanu naszej organizacji w kontekście tych zagrożeń. Analizujemy zabezpieczenia, które mają nas chronić przed zagrożeniami znajdującymi się na liście zagrożeń oraz ich skuteczność. Identyfikujemy słabości/podatności, które mogą być wykorzystane przez poszczególne zagrożenia. Przykładowo analizując zagrożenie ataku wirusowego sprawdzamy czy nasz system antywirusowy jest zainstalowany na wszystkich stacjach roboczych oraz czy jest prawidłowo zarządzany w tym aktualizowany. Przygotowane w etapie pierwszym zestawienie grup informacji z systemami informatycznymi pozwala teraz ocenić podatność danej grupy w kontekście poszczególnych systemów informatycznych.

Zebranie tych danych pozwala nam ocenić poziom podatności, który może być wyrażony liczbowo np. 1-3 lub 1-4 albo też jakościowo/słownie – prawdopodobieństwo niskie, średnie, wysokie, bardzo wysokie.

Ilość i skuteczność zabezpieczeń powoduje, że prawdopodobieństwo wystąpienia zagrożenia maleje, natomiast liczba zidentyfikowanych słabości/podatności wpływa na wzrost poziomu prawdopodobieństwa.

Na wartość prawdopodobieństwa wpływ mogą mieć również informacje o incydentach, które występowały w tym zakresie w przeszłości. Jeżeli zagrożenia w przeciągu ostatnich 2 lat wystąpiło kilka razy i w tym zakresie w naszej organizacji nie zaszły znaczące zmiany, oznacza to, że poziom prawdopodobieństwa powinien oscylować w górnych granicach.

W etap identyfikacji podatności zaangażowani są m.in. Administrator Bezpieczeństwa, Właściciele Zasobów, a także specjaliści jak administratorzy IT, którzy posiadają wiedzę pozwalającą ocenić i zweryfikować zabezpieczenia oraz znaleźć słabości/podatności w środowisku informatycznym.

Szacowanie ryzyka

Administrator Bezpieczeństwa na podstawie danych zebranych w etapach 1-3 dokonuje szacowania ryzyka.

Jednym z najprostszych a jednocześnie skutecznym rozwiązaniem do oceny poziomu ryzyka jest zastosowania prostej macierzy łączącej prawdopodobieństwo wystąpienia zagrożenia z jego skutkiem.

Przykładowa macierz ryzyka może wyglądać następująco:

Skutek \ Prawdopodobieństwo	1	2	3	4
1	N	N	N	N
2	N	N	S	S
3	N	S	S	W
4	S	S	W	W

Po podstawieniu danych do powyższej tabeli otrzymujemy wartości ryzyka:

- N – ryzyko niskie;
- S – ryzyko średnie;
- W – ryzyko wysokie.

Wartość ryzyka obliczamy dla każdej pary grupa informacji – zagrożenie.

Administrator Bezpieczeństwa przygotowuje raport z procesu analizy ryzyka, który przedstawia najwyższemu kierownictwu do akceptacji. W raporcie tym uwzględnić może również propozycje decyzji w zakresie akceptacji lub braku akceptacji poszczególnych ryzyk. W praktyce często przyjmuje się rozwiązanie, w którym ryzyko na poziomie niskim jest ryzykiem akceptowalnym, ryzyko na poziomie średnim może być zaakceptowane lub nie przez właścicieli zasobów lub administrator bezpieczeństwa, natomiast ryzyko na poziomie wysokim jest ryzykiem nieakceptowanych, chyba że decyzję tą zmieni najwyższe kierownictwo.

Postępowanie z ryzykiem

Po zatwierdzeniu raportu z analizy ryzyka i wyznaczeniu ryzyk nieakceptowanych, Administrator Bezpieczeństwa wraz z Właścicielami zasobów przygotowuje propozycję działań, które mają na celu ograniczyć poziom ryzyka.

Przygotowując te działania kierować się można trzema sposobami postępowania z ryzykiem nieakceptowanym:

- Minimalizacja ryzyka - podjęcie działań usuwających problemy mające wpływ na wystąpienie danego poziomu ryzyka dla zagrożenia np. instalacja klimatyzacji w serwerowni w której wysoka temperatura powodowała spadek wydajności serwerów
- Unikanie ryzyka - konieczność podjęcia działań mających na celu zaprzestanie działań/działalności powodującej powstanie zagrożenia o danym poziomie np. zaprzestanie korzystania z systemów operacyjnych Windows 95
- Transfer ryzyka - konieczność podjęcia działań mających na celu przekazanie odpowiedzialności w zakresie działań/działalności na podmioty zewnętrzne np. przekazanie utrzymania systemów IT firmie zewnętrznej i zapewnienie stosownych umów gwarantujących wysoki poziom bezpieczeństwa.

Wyznaczając działania należy w sposób czytelny je opisać, wskazać na jakie zagrożenie wpłynie wdrożenie danego działania, kto ma dane działanie zrealizować oraz w jakim terminie.

Jeśli organizacja chce być zgodna z wymaganiami normy ISO/IEC 27001 musi również wyliczyć wartości ryzyka szczątkowego, czyli wartość ryzyka jaka pozostanie po wdrożeniu przygotowanych działań. Jeżeli wyniki ryzyka szczątkowego są akceptowalne dla najwyższego kierownictwa, oznacza to, że przygotowane przez nas działania są wystarczające.

Plan postępowania z ryzykiem jest akceptowalny przez najwyższe kierownictwo.

Administrator Bezpieczeństwa jest odpowiedzialny za nadzorowanie realizacji działań z Planu postępowania z ryzykiem

Podsumowanie

Proces zarządzania ryzykiem realizowany jest cyklicznie – proponujemy przeprowadzać ten proces w cyklach rocznych. W przypadku, przeprowadzania procesu po raz kolejny realizacja poszczególnych etapów, będzie polegała przede wszystkim na aktualizacji danych zebranych przed rokiem z uwzględnieniem zmian jakie zaszły od czasu zakończenia procesu ryzyka w tym zmian w zakresie funkcjonowania organizacji, zmian w środowisku/otoczeniu organizacji, zmian prawa i innych wymagań/standardów/norm, zmian technicznych jak np. wdrożenie nowych systemów informatycznych itp.

Zaleca się stosowanie prostej i dostosowanej do organizacji metodyki, która spełni swój cel, czyli pozwoli skupić się najwyższemu kierownictwu na konkretnych problemach, które zagrażają utracie najważniejszych informacji dla organizacji.