Procedura szacowania ryzyka

w Zespole Szkół Ogólnokształcących nr 1

im. Zbigniewa Herberta w Lublinie

Cel procedury

Celem Procedury szacowania ryzyka jest:

* określenie zasad inwentaryzowania informacji chronionych,
* określenie zasad szacowania ryzyka.

Zakres obowiązywania

Niniejszy dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przetwarzanie (papierowej, elektronicznej i innej).

Terminologia

1. Ryzyko w bezpieczeństwie informacji – zwane dalej ryzykiem – potencjalna sytuacja mogąca wystąpić z określonym prawdopodobieństwem, w której określone zagrożenie wykorzysta podatność aktywa lub grupy aktywów w celu spowodowania strat dla organizacji.
2. Ryzyko szczątkowe – poziom ryzyka po wdrożeniu zabezpieczeń.
3. Poziom ryzyka akceptowalnego – poziom zapewniający, że ryzyka szczątkowe są świadomie zaakceptowane przez Dyrektora ZSO1.
4. Aktywo informacyjne – wszelkie informacje chronione w formie papierowej, elektronicznej i innej, przetwarzane (zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane i usuwane) w sposób tradycyjny lub w systemach informatycznych, będące własnością ZSO1.
5. Właściciel aktywa informacyjnego – Dyrektor ZSO nr 1 im. Zbigniewa Herberta w Lublinie lub Urząd Miasta Lublin.
6. Poufność informacji – atrybut bezpieczeństwa aktywa informacyjnego oznaczający, że dostęp do informacji powinny mieć jedynie osoby uprawnione.
7. Integralność – atrybut bezpieczeństwa aktywa i zasobu informacyjnego określający jakość informacji w aspekcie kompletności, spójności i wiarygodności danych.
8. Dostępność – atrybut bezpieczeństwa aktywa i zasobu informacyjnego oznaczającydostęp do informacji dla osób uprawnionych wtedy, kiedy jej potrzebują do przetwarzania.
9. Podatności – rozumiemy jako wady, luki lub słabości w strukturze fizycznej, organizacji działania Jednostki Organizacyjnej, procedurach, personelu, zarządzaniu, administrowaniu, sprzęcie lub oprogramowaniu (zasobu lub grupy zasobów), które mogą być wykorzystane przez zagrożenie do spowodowania strat.
10. Zagrożenie informacji – potencjalne działanie wobec aktywa i zasobu informacyjnego lub procesu, mogące wykorzystać określoną podatność, w celu spowodowania strat.
11. Prawdopodobieństwo wystąpienia zagrożenia – potencjalna możliwość lub częstość występowania zagrożenia.

**Identyfikacja i klasyfikacja informacji**

Inwentaryzacja i ocena wartości aktywów i zasobów jest niezbędna, aby określić, jakie aktywa i zasoby powinny podlegać ochronie. Identyfikacja umożliwia określenie rodzaju i miejsca ich przechowywania oraz przetwarzania. Ocena wartości aktywa i zasobu umożliwia zmierzenie zależności JednostkiOrganizacyjnej od danego aktywa i zasobu, a następnie przeprowadzenie identyfikacji i analizy ryzyka. Identyfikuje się te zasoby, od których zależy prawidłowe funkcjonowanie ZSO nr 1im. Z. Herberta w Lublinie. Przy wykonywaniu inwentaryzacji aktywów i zasobów uwzględnia się wymagania prawne wynikające z ustaw i rozporządzeń.

**Klasyfikacji zasobów dokonuje się zgodnie z zapisami Polityki Bezpieczeństwa Informacji.**

1. Metodyka identyfikacji aktywów informacyjnych:
2. inwentaryzacja oraz identyfikacja aktywów i zasobów informacyjnych,
3. określenie miejsc przetwarzania informacji,
4. zidentyfikowanie właścicieli zasobów,
5. wyszczególnienie zasobów oraz określenie istotności tych zasobów dla Jednostki Organizacyjnej,
6. klasyfikacja aktywów i zasobów informacyjnych przeprowadzona przez gestorów informacji.
7. Klasyfikacja zasobów informacyjnych jest przeprowadzona przez właścicieli informacji, czyli jej gestorów, w formularzu będącym załącznikiem nr 1 do niniejszej procedury. Klasyfikacja dokonywana jest w kontekście trzech podstawowych cech bezpieczeństwa informacji:
8. POUFNOŚCI, która oznacza, że dostęp do informacji powinny mieć jedynie osoby uprawnione
9. INTEGRALNOŚCI, która określa jakość informacji w aspekcie kompletności, spójności i wiarygodności danych
10. DOSTĘPNOŚCI, która oznacza dostępność informacji dla osób uprawnionych.

Ocenę istotności (wartości) aktywów informacyjnych i zasobów wykonuje się według skali numerycznej od 1 do 4, gdzie 4 oznacza najwyższą wagę. Dla każdego z atrybutów informacji przyjmuje się wartości ze skali. Ostatecznie dla każdego z aktywów informacyjnych kalkuluje się istotność zgodnie z poniższą formułą:

$$WA= P+I+D$$

gdzie:

WA – wartość aktywa

P – atrybut poufności aktywa podany w skali od 1 do 4

I – atrybut integralności aktywa podany w skali od 1 do 4

D – atrybut dostępności aktywa podany w skali od 1 do 4

Do oceny wartości zasobów przyjęto Tabelę Istotności Zasobów o 4-o stopniowej skali wartości. Wartości przypisuje się do atrybutu poufności, integralności oraz dostępności każdego z aktywów. Wartość 4 oznacza największą istotność bezpieczeństwa aktywa, np. poufność oceniona na 4 oznacza najwyższą wartość wymagań dla zachowania poufności rozpatrywanego aktywa. Analogicznie w tym przykładzie wartość 0 dla poufności oznacza brak wymagań dla zachowania poufności rozpatrywanego aktywa.

| Wartość liczbowa | Opis |
| --- | --- |
| 4 | Naruszenie bezpieczeństwa aktywa w zakresie danego atrybutu drastycznie zakłóca lub całkowicie uniemożliwia pracę z aktywem. Możliwa jest również poważna odpowiedzialność prawna i negatywny rozgłos medialny. |
| 3 | Naruszenie bezpieczeństwa aktywa w zakresie danego atrybutu może znacząco zakłócić pracę z aktywem. Możliwa jest również odpowiedzialność prawna lub negatywny rozgłos medialny. |
| 2 | Naruszenie bezpieczeństwa aktywa w zakresie danego atrybutu może utrudnić pracę z aktywem. Możliwy jest również negatywny rozgłos medialny. |
| 1 | Naruszenie bezpieczeństwa aktywa w zakresie danego atrybutu może w niewielkim stopniu utrudnić pracę z aktywem, jednak główne zadania w zakresie danego aktywą mogą być nadal realizowane. |
| 0 | Brak wymagań bezpieczeństwa w zakresie danego atrybutu. Oznacza to brak konieczności stosowania zabezpieczeń w danym obszarze. |

Przynależność aktywa informacyjnego do właściwej klasy zależy od wartości tego aktywa. Wartość WA aktywa informacyjnego oblicza się zgodnie z wzorem podanym powyżej.

Przyjmuje się 4 klasy ochrony informacji:

1. Klasa 1 – niski poziom ochrony. WA < 2
2. Klasa 2 – średni poziom ochrony. 8 > WA >= 2
3. Klasa 3 – wysoki poziom ochrony. 11 > WA >= 8
4. Klasa 4 – bardzo wysoki poziom ochrony. WA > =11

Efektem identyfikacji i klasyfikacji informacji powinien być Wykaz aktywów informacyjnych, będący wejściem do etapu analizy ryzyka dla bezpieczeństwa informacji.

Wykaz zidentyfikowanych aktywów i zasobów informacyjnych zawiera Załącznik nr 7.1 do niniejszej procedury. Zbiorczy wykaz aktywów i zasobów informacyjnych prowadzi Dyrektor ZSO nr 1 im. Z. Herberta w Lublinie.

Szacowanie ryzyka

Analiza ryzyk

Analizę ryzyka przeprowadza się w zakresie obszarów o największej istotności, w szczególności analizuje się ryzyka utraty wymaganego poziomu poufności, integralności oraz dostępności dla danych osobowych. Ryzyka szacuje się szczególnie dla danych osobowych w kontekście utraty praw lub wolności osób fizycznych zgodnie z art. 32 RODO. Należy założyć, że utrata wymaganego poziomu poufności, integralności lub dostępności danych osobowych może skutkować naruszeniem praw lub wolności osób fizycznych. Przyjmuje się, że powaga tego naruszenia jest adekwatna do poziomu ryzyka określanego zgodnie z niniejszą procedurą.

Na podstawie wyników analizy ryzyka opracowywane są plany postępowania z ryzykiem dla poziomu ryzyka większego niż akceptowalny. W przyjętym modelu jest to wartośćw większa lub równa 32. Analiza ryzyka jest przeprowadzana nie rzadziej niż raz do roku, w terminie określonym przez Dyrektora ZSO1. Ryzyka są monitorowane przez Inspektora Ochrony Danych oraz Administratora Systemu Informatycznego.

Analiza ryzyka przeprowadzana jest również po wprowadzeniu zmian mających wpływ na wymagany poziom poufności, integralności oraz dostępności aktywów informacyjnych.

Wzór Rejestru ryzyka Jednostki Organizacyjnej w bezpieczeństwie informacji jest załącznikiem nr 7.2 do niniejszej procedury.

Identyfikacja zagrożeń i podatności

Zagrożenie jest potencjalnym działaniem wobec aktywa i zasobu informacyjnego, mogącym wykorzystać określoną podatność, mającym na celu spowodowanie strat.

Należy rozpoznać zagrożenia dla bezpieczeństwa informacji przetwarzanych i przechowywanych w Jednostce Organizacyjnejoraz określić ich wpływ na bezpieczeństwo tychże informacji.

Należy brać pod uwagę następujące klasy zagrożeń w szczególności:

1. zewnętrzne – kryzys finansowy, zmiana prawa, klęski żywiołowe, siła wyższa,
2. ludzkie – kradzież, podsłuch, zgubienie, szpiegowanie, celowe działanie użytkownika, niecelowe działanie użytkownika, działanie intruza,
3. użytkownika – brak odpowiedniego przeszkolenia,
4. proceduralne – błędy w ochronie fizycznej i technicznej,
5. Sprzętu i oprogramowania – wady oprogramowania, awarie sprzętu,

Każde zdarzenie będące zagrożeniem dla zasobu powinno być powiązane z podatnością, którą należy rozumieć
w szczególności jakowadę, lukę lub słabość w strukturze fizycznej, zasobach materialnych, organizacji, procedurach, personelu, zarządzaniu, administrowaniu, sprzęcie lub oprogramowaniu (zasobu lub grupy zasobów), która może być wykorzystana przez zagrożenie w celu spowodowania strat.

Wyniki identyfikacji zagrożeń i podatności po przeprowadzanej analizie wraz z ich wartościami odpowiednich parametrów, przypisanymi do odpowiednich aktywów i zasobów informacyjnych przedstawione są Rejestrze ryzyk w bezpieczeństwie informacji.

Dobór zabezpieczeń

Cele stosowania zabezpieczeń i zabezpieczenia powinny być dobierane adekwatnie do wymagań prawnych i wyników analizy ryzyka dla bezpieczeństwa informacji.

Zabezpieczenia fizyczne, techniczne i organizacyjne dobierane są tak, aby uzupełniać się wzajemnie, zapewniając wspólnie wymagany poziom bezpieczeństwa informacji.

W doborze celów stosowania zabezpieczeń i zabezpieczeń należy kierować się zaleceniami Polskiej Normy PN-ISO/IEC27002:2014:12 oraz dobrymi praktykami.

Proces szacowania ryzyka

Każda miara powiązana z elementem bezpieczeństwa powinna być rozpatrywana w trzech niezależnych aspektach: poufności, integralności oraz dostępności. Wartości dla poufności, integralności oraz dostępności obliczane są niezależnie, stąd każdy element bezpieczeństwa charakteryzuje się trzema odrębnymi grupami parametrów podlegających identycznym obliczeniom i zasadom zgodnie z przyjętą metodyką analizy ryzyka zatwierdzoną w Jednostce Organizacyjnej.

Krok 1. Scenariusze wykorzystania podatności przez zagrożenie

Opis potencjalnego zdarzenia wykorzystania podatności przez zagrożenie jest kluczowy dla przeprowadzenia prawidłowej analizy. Powinny być rozpatrywane zdarzenia, których działanie prowadzi do utraty całkowitej bądź częściowej poufności, integralności oraz dostępności aktywa. Zdarzenia powinny być opisywane w szczególności za pomocą:

1. źródła ryzyka,
2. opisu podatności,
3. opisu zagrożenia,
4. nazwy aktywa/zasobu podlegającego zdarzeniu.

Krok 2 – prawdopodobieństwo wystąpienia zdarzenia

Dla każdego zdarzenia, w wyniku którego może zrealizować się rozpatrywane ryzyko, należy dobrać odpowiednie wartości prawdopodobieństwa. Podczas oceny prawdopodobieństwa wystąpienia zagrożenia wykorzystującego wskazaną podatność w celu spowodowania strat w zasobie, należy uwzględniać nie tylko potencjalne zajście zdarzenia w przyszłości, lecz również sytuacje z przeszłości.

Dla każdego prawdopodobieństwa należy dobrać wartości zgodnie z poniższą tabelą.

|  |  |
| --- | --- |
| Wartość | Opis |
| 4 | Realizacja raz w tygodniu |
| 3 | Realizacja raz na trzy miesiące |
| 2 | Realizacja raz na rok |
| 1 | Realizacja raz na dwa lata lub rzadziej |

Uwaga. Dla niektórych sytuacji przyjmuje się niezerowe wartości prawdopodobieństwa, pomimo że sytuacja występuje niezmiernie rzadko. Przykładem są: klęski żywiołowe, katastrofy naturalne, pożar, powódź.

Krok 3 – wpływ zagrożenia

Wpływ zagrożenia rozumiemy, jako skutki dla naszej organizacji w wyniku opisanego scenariusza zdarzenia. Tutaj wpływ rozumiemy, jako utratę bezpieczeństwa dla poufności, integralności oraz dostępności zasobu. Wartości wpływu dobieramy dla poufności, integralności oraz dostępności zgodnie z poniższą tabelą.

|  |  |
| --- | --- |
| **Wartość** | **Opis** |
| 4 | Bardzo poważne naruszenie bezpieczeństwa zasobu, które może rodzić konsekwencje prawne, wizerunkowe oraz dla ciągłości działania organizacji. Naruszenie dotyczy najważniejszych elementów zasobu. Naruszenie uniemożliwia korzystanie z zasobu.Osoby fizyczne, których dane osobowe są objęte naruszeniem, mogą odczuwać istotne lub nawet nieodwracalne konsekwencje. |
| 3 | W wyniku naruszenia poważnie zakłócone są procesy zależne od korzystania z zasobu. W wyniki zadziałania zagrożenia organizacja odczuwa poważne zakłócenie natury technicznej oraz organizacyjnej.Osoby fizyczne, których dane osobowe są objęte naruszeniem, mogą odczuwać istotne konsekwencje, które są w stanie rozwiązać z wieloma trudnościami. |
| 2 | Naruszone jest bezpieczeństwo zasobu, jednak nie rodzi ono konsekwencji prawnych, wizerunkowych i innych poważnych skutków dla organizacji.Osoby fizyczne, których dane osobowe są objęte naruszeniem, mogą odczuwać istotne niedogodności, które są w stanie rozwiązać pomimo kilku trudności |
| 1 | Naruszenie bezpieczeństwa ma ograniczone konsekwencje dla organizacji. Nie rodzi skutków prawnych, wizerunkowych czy dla ciągłości działania organizacji.Osoby fizyczne, których dane osobowe są objęte naruszeniem, praktycznie nie odczuwają skutków. |
| 0 | Brak wpływu |

Krok 4 – inwentaryzacja zabezpieczeń

Właściwa ocena sytuacji, w której może zadziałać zagrożenie, wymaga określenia stosowanych zabezpieczeń dla zasobu. Szczególnie istotna jest skuteczność stosowanych zabezpieczeń dla zapewnienia poufności, integralności oraz dostępności zasobu.

W przyjętej metodzie należy uwzględnić obecnie stosowane zabezpieczenia podczas określania wartości wpływu zagrożenia na aktywo.

Krok 5 – ocena ryzyka

Po dobraniu odpowiednich wartości i uwzględnieniu obecnego stanu zabezpieczeń, Arkusz kalkulacyjny automatycznie oblicza wartości ryzyk. Wartości ryzyk przyjmują wartości z przedziału od 1 do 64.

W przyjętej metodzie ryzyko zależy od wartości wpływu, prawdopodobieństwa oraz klasy ochrony aktywa. Należy oszacować ryzyko utraty poufności Rp, integralności Ri oraz dostępności aktywa Rd.

$$Rp= Wartość skutków z powodu utraty poufności\*Wartość prawdopodobieństwa\*Klasa aktywa(zależna od WA)$$

$$Ri= Wartość skutków z powodu utraty integralności\*Wartość prawdopodobieństwa\*Klasa aktywa(zależna od WA)$$

$$Rd= Wartość skutków z powodu utraty \*Wartość prawdopodobieństwa\*Klasa aktywa(zależna od WA)$$

Bardzo istotnym krokiem jest dobranie ryzyka akceptowalnego, poniżej którego wartości ryzyka będzie określać jako szczątkowe (rezydualne). Poziom ryzyka akceptowalnego należy określić na podstawie oszacowań ryzyka dla wszystkich przyjętych do analizy zagrożeń. Należy przyjąć poziom ryzyka akceptowalnego dla każdego z obszarów lub procesów organizacji, lub przyjąć globalną wartość ryzyka akceptowalnego. Wynik porównania wartości ryzyk dla zagrożeń i wartości ryzyka akceptowalnego jest podstawą procesu zarządzania ryzykiem, w którym powinniśmy reagować na ryzyka ponad akceptowalne na kilka sposobów np. stosując dodatkowe zabezpieczenia.

W przyjętym modelu należy kierować się poniższą mapą ryzyka.

|  |  |
| --- | --- |
| Skutki dla organizacji | Prawdopodobieństwo scenariusza zdarzenia |
| Niskie | Średnie | Wysokie | Bardzo wysokie |
| Bardzo wysokie | Od 24 do 32 | Od 32 do 40 | Od 40 do 48 | Powyżej 48 |
| Wysokie | Od 16 do 24 | Od 24 do 32 | Od 32 do 40 | Od 40 do 48 |
| Średnie | Od 8 do 16 | Od 16 do 24 | Od 24 do 32 | Od 32 do 40 |
| Niskie | Od 1 do 8 | Od 8 do 16 | Od 16 do 24 | Od 24 do 32 |

Ryzyka w kolorze niebieskim należy monitorować, czy nie zbliżają się do kolejnego obszaru. Kolorem pomarańczowym zaznaczono te ryzyka, którymi należy zająć się w dłuższym okresie czasu. Natomiast kolorem czerwonym zaznaczono te ryzyka, którymi należy zająć się natychmiast.

Postępowanie z ryzykiem

Dyrektor ZSS zatwierdzając Rejestr ryzyk w bezpieczeństwie informacji określa zasady postępowania z ryzykiem. Zgodnie z PN-ISO/IEC 27005:2014 stosuje się cztery warianty postępowania z ryzykiem:

1. Modyfikowanie ryzyka - polega na zredukowaniu poziomu ryzyka przez taki wybór zabezpieczeń, aby ryzyko szczątkowe można było ponownie oszacować jak ryzyko akceptowalne.
2. Zachowanie ryzyka - polega na podjęciu decyzji o zachowaniu ryzyka bez podejmowania dalszych działań, na podstawie oceny ryzyka.
3. Unikanie ryzyka - polega na unikaniu działań lub warunków, które powodują powstanie określonych ryzyk.
4. Dzielenie ryzyka - na podstawie oceny ryzyka zaleca się transfer ryzyka do innej strony, która może skutecznie zarządzać ryzykiem.

Wszystkie ryzyka o wartości poniżej akceptowanego poziomu ryzyka o wartości mniejszej niż 32 zostaną zachowane.
W przypadku poziomu ryzyka o wartości równej i większej 32 po wybraniu wariantu postępowania z ryzykiem należy przygotować plan postępowania z ryzykiem.

Plan postępowania z ryzykiem powinien zawierać:

1. Opis postępowania z ryzykiem,
2. wybrane zabezpieczenia,
3. wskazanie odpowiedzialności za realizację planu,
4. ewentualne koszty związane z realizacją planu,
5. w razie potrzeby harmonogram działań.

Plan postępowania z ryzykiem zatwierdza Dyrektor Zespołu Szkół Ogólnokształcących nr 1 im. Z. Herberta w Lublinie, a realizację monitoruje Inspektor Ochrony Danych.

Za wdrożenie planów odpowiedzialni są wyznaczeni przez Dyrektora ZSO nr 1 pracownicy.

Monitorowanie i przegląd ryzyka

Proces identyfikacji i analizy ryzyka w ZSO1 jest procesem ciągłym i monitorowanym w szczególności pod względem:

1. nowych lub zwiększonych zagrożeń pojawiających się zarówno na zewnątrz, jak i wewnątrz ZSO1,
2. szacowania prawdopodobieństwa występujących zdarzeń,
3. analizy nowych lub zwiększonych podatności mogących umożliwić zagrożeniom ich wykorzystanie,
4. analizy zwiększonych konsekwencji szacowanych zagrożeń, podatności, ryzyk, których agregacja może spowodować przekroczenie kryteriów akceptacji ryzyka.

Przebieg procesu monitorowania ryzyka sprawia, że należy zapewnić ciągłą dostępność zasobów organizacyjnych i technicznych, które mogą go realizować.

Proces monitorowania ryzyka polega na prowadzeniu przeglądu ryzyk w terminie wskazanym przez Dyrektora ZSO1 oraz na zgłoszeniu nowych i zmian w istniejących ryzykach w trakcie roku.

Monitorowanie i przegląd procesu zarządzania ryzykiem dotyczy w szczególności:

1. kontekstu prawnego i umownego Jednostki Organizacyjnej,
2. kryteriów szacowania ryzyka,
3. kategorii zasobów i ich wartościowania,
4. kryteriów akceptowania ryzyka,
5. kontrolowanie kosztów zarządzania ryzykiem.

Lista dokumentów związanych

1. Polityka Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin.

Załączniki

1. Załącznik nr 7.1 – Wzór Wykazu aktywów informacyjnych.
2. Załącznik nr 7.2 –Wzór Rejestru ryzyk ZSO nr 1 im. Z. Herberta w Lublinie w bezpieczeństwie informacji.