Aruba Cloud

Zarządzanie ryzykiem dla zapewnienia bezpieczeństwa informacji

SPIS TREŚCI

AlphaNet Spółka z o.o.
ul. Małobądzka 4a, 41-214 Sosnowiec
NIP: 644-318-61-65

1 POJĘCIA I DEFINICJE

Niniejszy rozdział zawiera definicje uznane za istotne dla przedstawienia modelu obliczania i zarządzania ryzykiem w zakresie bezpieczeństwa informacji.

***BIA (Business Impact Analysis)*:**

Analiza ekonomicznych, regulacyjnych i wizerunkowych skutków dla działalności związanych z utratą poufności, integralności i dostępności informacji związanych z danym procesem/usługą oraz jej przerwaniem.

Dostępność:

Zagwarantowanie dostępności niezbędnych systemów informatycznych i danych.

Zarządzanie ryzykiem dla bezpieczeństwa informacji

Ogół działań i procesów biznesowych opracowanych w celu identyfikacji, mierzenia, ograniczenia i monitorowania ryzyka związanego z utratą poufności, integralności i dostępności (CIA) danych i usług.

Skutek:

Negatywna konsekwencja wystąpienia co najmniej jednego zagrożenia.

Incydent:

Zdarzenie związane z cyberbezpieczeństwem, które z dużym prawdopodobieństwem narazi na szwank działalność gospodarczą i zagrozi bezpieczeństwu informacji.

Integralność:

Odnosi się to do ochrony danych i informacji przed zmianami ich treści, zarówno przypadkowymi, jak i celowymi.

Zagrożenie:

Potencjalna przyczyna (celowa lub przypadkowa) incydentu, który może doprowadzić do uszkodzenia systemu lub szkód dla organizacji, oddziałując na **p**oufność, **i**ntegralność i **d**ostępność informacji.

Zagrożeniami mogą być:

- „Cyberzagrożenia" – negatywnie oddziałują na firmę poprzez:
  - wykorzystanie systemu informatycznego lub jego komponentów (np.: atak hakerski);
  - prowadzenie działań związanych z zarządzaniem systemem informatycznym (np.: uszkodzenie przez personel wewnętrzny);
- Zagrożenia „niecybernetyczne" – negatywnie oddziałują na system informatyczny firmy poprzez:
  - bezpośredni wpływ na świadczenie usług systemu informatycznego (np. klęski żywiołowe, przerwy w świadczeniu usług wsparcia);
  - wpływ na sposób zarządzania systemem informatycznym (np. sposób wdrażania procesów informatycznych).

Aby scharakteryzować ryzyko związane z każdym zagrożeniem, musimy znać:

- Podatności komponentów systemu informatycznego lub miejsca, w których mogą urzeczywistnić się zagrożenia;
- Ekspozycję komponentów na zagrożenie, innymi słowy, jak łatwo zagrożenie może się urzeczywistnić (na przykład serwer, który udostępnia klientom usługę sieciową, jest bardziej narażony na ataki przeprowadzane przez Internet);
- Rodzaje konsekwencji, biorąc pod uwagę, że niektóre zagrożenia mogą z kolei być „nośnikami" innych zagrożeń (na przykład nieautoryzowany dostęp do serwera internetowego może umożliwić intruzowi kradzież danych, ale może również pozwolić na usunięcie, zmianę, popełnienie oszustwa itp.).

Możliwość lub prawdopodobieństwo wystąpienia:

Prawdopodobieństwo, że zagrożenie może mieć wpływ na jeden lub więcej komponentów informatycznych, wywierając negatywny wpływ na działalność w danym okresie czasu.

Ryzyko dla bezpieczeństwa informacji (zwane dalej również „ryzykiem")

Połączenie prawdopodobieństwa wystąpienia zagrożenia i oddziaływania na firmę w zakresie aktywów objętych analizą. W zależności od tego, kiedy jest mierzone, ryzyko można zdefiniować jako:

- Ryzyko potencjalne lub nieodłączne (**rRp**):

  Oznacza to maksymalne ryzyko, na jakie narażony jest dany składnik aktywów pod względem możliwości powstania zagrożenia, które może mieć wpływ na utratę poufności, integralności lub dostępności inf ormacji. Wszystkie komponenty uwzględniane w analizie usługi przyczyniają się do określenia ryzyka nieodłącznego: procesy, aplikacje, dane, infrastruktura i wreszcie, czynnik ludzki.

  Jest on zasadniczo wyrażany w postaci wartości, obliczanej w różny sposób w zależności od zastosowanej metodologii, w oparciu o sumę wszystkich możliwych zagrożeń, na które narażony jest składnik aktywów, przy uwzględnieniu odpowiedniego prawdopodobieństwa wystąpienia i jego wpływu.

  Innymi słowy, jest to ryzyko, na które dany składnik aktywów może być narażony ze względu na swój charakter i związane z nim zagrożenia. Na przykład komputer narażony w sieci publicznej bez żadnych środków zabezpieczających.

- Ryzyko rezydualne lub końcowe (**rRf**):

  Stanowi takie ryzyko, na jakie może być narażona usługa po zastosowaniu środków zaradczych mających na celu zmniejszenie ryzyka nieodłącznego.

- Końcowe ryzyko dopuszczalne (**rRfa**):

  Oznacza maksymalny próg ryzyka możliwy do zaakceptowania przez Organizację.

AlphaNet Spółka z o.o.
ul. Małobądzka 4a, 41-214 Sosnowiec
NIP: 644-318-61-65

Wszystkie podane powyżej wartości ryzyka należy uznać za dynamiczne, ponieważ podlegają zmianom w czasie, gdyż oddziałują na nie przykładowo następujące elementy:

- Ewolucja zagrożeń;
- Zmiana w zależności od wymaganych poziomów obsługi;
- Zmiany przepisów prawnych unijnych regulacji BMR;
- Zmiany organizacyjne, które mogą wpłynąć na słabości lub prawdopodobieństwo wystąpienia zagrożeń lub zmienić spowodowane przez nie skutki;
- Wzmocnienie lub osłabienie środków zabezpieczających.

Podstawowe zagrożenia:

Dotyczy to zagrożeń cybernetycznych związanych z każdym zasobem i każdym scenariuszem ryzyka.

Poufność:

Odnosi się do ochrony danych i informacji w celu ograniczenia ryzyka związanego z nieupoważnionym dostępem do informacji lub ich wykorzystaniem.

Docelowy punkt odzyskiwania (Recovery Point Objective):

Odnosi się to do dopuszczalnej utraty danych i jest maksymalnym okresem czasu między ostatnim zapisem danych z procesu a zdarzeniem powodującym zatrzymanie procesu.

Docelowy czas odzyskiwania (Recovery Time Objective):

Okres po wystąpieniu incydentu, w którym:

- Należy przywrócić Produkt lub Usługę, lub
- Należy wznowić działalność, lub
- Należy odzyskać zasoby.

Scenariusz ryzyka:

Połączenie dwóch lub więcej zagrożeń, które umożliwiają ich klasyfikację.

Podatność:

Nieodłączna słabość procesu, usługi lub aktywa, która, w przypadku wykorzystania przez jedno lub więcej zagrożeń, umożliwia naruszenie celów bezpieczeństwa informacji (poufności, integralności i dostępności). Przykłady to:

- Sieci niesegregowane;
- Wykorzystywanie protokołów nie chronionych przez szyfrowanie;
- Brak regularnych aktualizacji systemów operacyjnych;

AlphaNet Spółka z o.o.
ul. Małobądzka 4a, 41-214 Sosnowiec
NIP: 644-318-61-65

- Bazy danych z niezaszyfrowanymi danymi „wrażliwymi”;
- Brak aktualizacji definicji wirusów;
- Niemonitorowany dostęp fizyczny;
- Brak automatycznych systemów przeciwpożarowych;
- Niewydolne systemy zasilania awaryjnego;
- itp.

2 GŁÓWNE NORMY REFERENCYJNE

Głównymi normami przyjętymi w celu zapewnienia, że prowadzone działania są zgodne z międzynarodowymi najlepszymi praktykami w zakresie bezpieczeństwa, są te opisane w poniższych akapitach.

2.1 Norma ISO/IEC 27001

Norma ISO/IEC 27001 jest międzynarodową normą dotyczącą bezpieczeństwa i stanowi wzorzec służący do oceny poziomu bezpieczeństwa informacji, umożliwiający analizę komponentów zarówno technologicznych, jak i organizacyjnych, które przyczyniają się do zdefiniowania Systemu Zarządzania Bezpieczeństwem Informacji (ISMS).
Norma określa wymagania dla ISMS i pomaga identyfikować, zarządzać i minimalizować różnorodne zagrożenia, na które stale wystawione są informacje. Niniejsza norma ustanawia również środki kontroli w zakresie ochrony, które należy przyjąć w celu ochrony informacji poprzez zapewnienie ich bezpieczeństwa interesariuszom, w tym klientom organizacji.

2.2 Norma ISO/IEC 27002

Norma ISO/IEC 27002 określa wytyczne i ogólne zasady wdrażania odpowiedniego Systemu Zarządzania Bezpieczeństwem Informacji w organizacji.
W szczególności norma ISO/IEC 27002 stanowi międzynarodowy standard dotyczący bezpieczeństwa i jest wzorcem służącym do oceny aspektów organizacyjnych, proceduralnych, technologicznych i regulacyjnych bezpieczeństwa systemu informatycznego w celu:

- Przeprowadzenia krytycznej analizy usług oraz funkcjonalności, które dany system posiada lub powinien posiadać;
- Uwydatnienia luk w systemie;
- Wskazania odpowiednich działań umożliwiających osiągnięcie poziomu bezpieczeństwa określonego w celach.

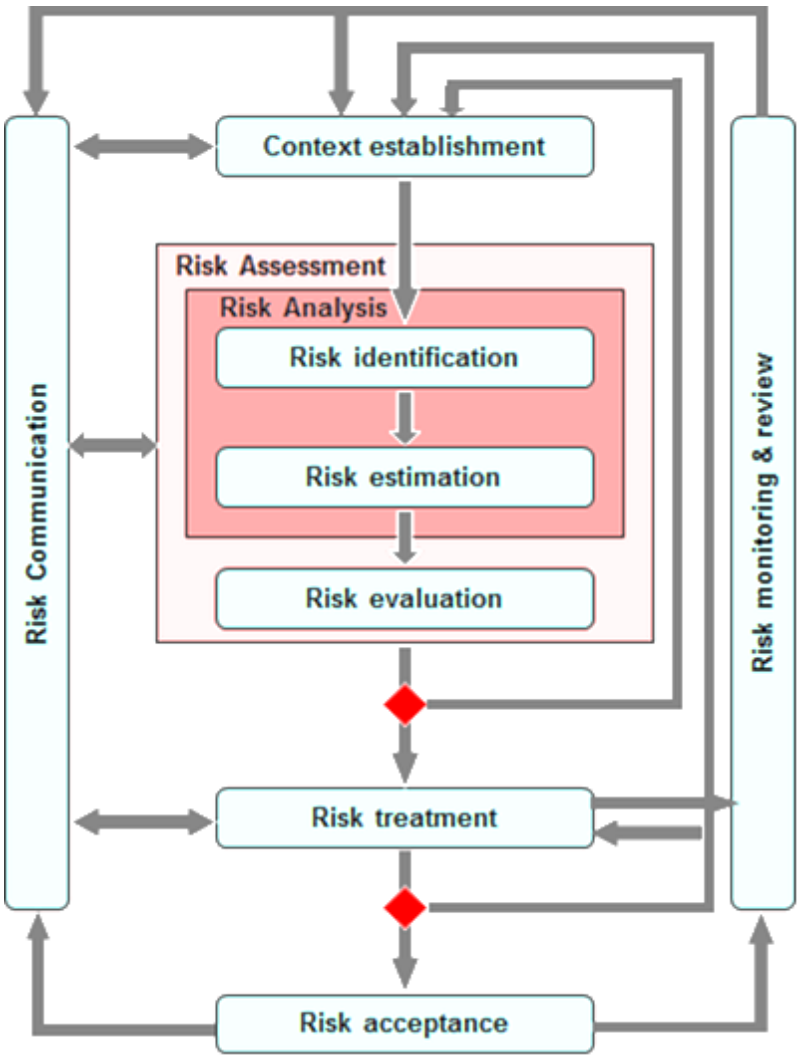
Należy zauważyć, że ISO/IEC 27002 identyfikuje środki kontroli w zakresie ochrony, których zastosowanie organizacja powinna rozważyć, jednak nie zastępuje samej analizy ryzyka.

2.3 Norma ISO/IEC 27005

Norma ISO/IEC 27005 opisuje proces zarządzania ryzykiem związanym z bezpieczeństwem informacji i związane z nim działania, potwierdzając ogólne zasady zawarte w ISO/IEC 27001.

Norma – zgodna z ISO 31000 – ma pomóc firmom zarządzać zagrożeniami dla bezpieczeństwa informacji podobnie jak zarządzają innymi rodzajami ryzyka.

Rysunek 1 przedstawia proces zarządzania ryzykiem przedstawiony w normie ISO/IEC 27005:11, który stanowił inspirację dla modelu przyjętego i opracowanego przez Grupę Aruba.



Rysunek 1 – ISO/IEC 27005: Proces zarządzania ryzykiem

3 METODYKA ZARZĄDZANIA ZAGROŻENIAMI DLA BEZPIECZEŃSTWA INFORMACJI

Dla Grupy Aruba informacje stanowią aktywa, które wymagają starannego zarządzania i mają strategiczne znaczenie dla ochrony i rozwoju działalności firmy.

W tym kontekście ryzyko cybernetyczne można zdefiniować jako każde niepewne zdarzenie, które może narazić na szwank jedną lub więcej z trzech następujących głównych właściwości aktywów informacyjnych firmy:

- **P**oufność (dane są dostępne dla osób nieuprawnionych);
- **I**ntegralność (dane mogą podlegać nieupoważnionym modyfikacjom i mogą zostać zmienione);
- **D**ostępność (nie można korzystać z systemu komputerowego);

W zależności od poziomu istotności, który jest ściśle zależny od rodzaju danych, których to dotyczy.

Ocena ryzyka uwzględnia następujące możliwe rodzaje oddziaływania:

- Ekonomiczne;
- Regulacyjne;
- Wizerunkowe.

Zarządzanie ryzykiem związanym z bezpieczeństwem informacji to proces oceny wzajemnych powiązań między aktywami, zagrożeniami i lukami w organizacji. Ten proces analityczny ma na celu identyfikację zagrożeń związanych z lukami i zagrożeniami występującymi w aktywach oraz stanowi podstawę do zdefiniowania skutecznego programu bezpieczeństwa.

Rozpatrywane kategorie ryzyka muszą być zgodne z typami mającymi zastosowanie dla danego kontekstu. Rozpatrywane ryzyko może zatem wynikać z zagrożeń wewnętrznych, zewnętrznych lub środowiskowych, jak również z umyślnych działań lub nieodpowiedniego zarządzania organizacją bądź zaniedbań poszczególnych osób.

Wartość ryzyka rozumiana jest jako funkcja wartości przedmiotowych aktywów, wartości zagrożeń i podatności na zagrożenia.

Wyniki analizy ryzyka dokumentuje się i obejmują one:

- Jasno sprecyzowaną identyfikację kluczowych zagrożeń;
- Ocenę potencjalnego wpływu, jaki każde ze zidentyfikowanych zagrożeń może mieć na firmę;
- Plan zalecanych działań w celu zmniejszenia ryzyka i przywrócenia go do akceptowalnego poziomu.

Groupa Aruba ustanawia model analizy jakościowej, ponieważ może on natychmiast zapewnić wysoki poziom świadomości na temat głównych zagrożeń związanych z technologiami informacyjno-komunikacyjnymi, które mają wpływ na dane środowisko technologiczne.

Przyjęta metodologia jest:

- Wykorzystywana przez Grupę w celu oszacowania wartości informacji w odpowiednich procesach i poziomów ryzyka, na jakie są narażone, tak aby można było zastosować odpowiednie środki ochronne;
- Ma zastosowanie również w przypadku opracowywania nowych rozwiązań infrastrukturalnych lub aplikacyjnych, które mają wpływ na bezpieczeństwo zarządzania danymi. W tym przypadku metodologia pozwala ocenić, na ile krytyczne są dane i zagrożenia, na jakie są one narażone, tak aby osoby odpowiedzialne za analizę ryzyka mogły, na etapie opracowywania i nabywania systemów komputerowych, wdrożyć odpowiednie zabezpieczenia minimalizujące ich podatność na zagrożenia.

Ocena ryzyka i analiza powiązań między aktywami, zagrożeniami i środkami zaradczymi odbywa się przy pomocy opracowanego wewnętrznie narzędzia, z wykorzystaniem informacji zgromadzonych podczas stosownych spotkań z osobami zaangażowanymi w analizowane procesy.
Metodologia oznacza, że można stworzyć model biznesowy, w którym opisane zostaną wszystkie podstawowe elementy niezbędne do kolejnych analiz, wraz z ich charakterystyką, strukturą hierarchiczną i związanymi z tym powiązaniami.

4 PROCES ZARZĄDZANIA RYZYKIEM

Poniżej opisano główne fazy przyjętego i stosowanego przez Grupę Aruba modelu analizy zarządzania ryzykiem związanym z bezpieczeństwem informacji.

4.1 FAZA 1 – Ustanowienie kontekstu

Pojęcie kontekstu analizy obejmuje modelowanie sytuacji firmy oraz identyfikację głównych biznesowych usług, procesów, makroprocesów i zaangażowanych aktywów.

Jeśli chodzi o identyfikację zasobów, zgodnie z normą ISO/IEC 27005 „Technologia informacyjna – techniki bezpieczeństwa – zarządzanie ryzykiem związanym z bezpieczeństwem informacji", rozróżnia się dwa odmienne typy:

- **Zasoby podstawowe** – informacje, procesy, makroprocesy i usługi o charakterze biznesowym;
- **Drugorzędne zasoby lub aktywa** – sprzęt, oprogramowanie, personel, sieć, lokalizacja i organizacja.

4.1.1 Identyfikacja usług, procesów i makroprocesów

W celu identyfikacji usług i procesów organizacji jako początkowe źródła odniesienia wykorzystuje się struktury organizacyjne ogłoszone i udostępnione za pośrednictwem wewnętrznego narzędzia do komunikacji korporacyjnej. Następnie poszczególne procesy, które przyczyniają się do świadczenia usług, grupuje się w makroprocesy specyficzne dla analizowanego kontekstu.

4.1.2 Identyfikowanie aktywów

Aby zapewnić precyzyjną identyfikację aktywów, postępujemy zgodnie z poniższymi wskazówkami:

1. **Określenie kategorii** aktywów informacyjnych (np. sprzęt, oprogramowanie, lokalizacja itp.), zgodnie z systemem klasyfikacji zdefiniowanym w normie ISO/IEC 27005;
2. **Przypisywanie wagi kategoriom** aktywów informacyjnych zgodnie ze strategią bezpieczeństwa firmy oraz wymaganiami o charakterze biznesowym, prawnym i umownym;
3. **Identyfikacja zależności** między kategoriami aktywów, które zostały skategoryzowane.

4.1.3 Relacje między makroprocesami i aktywami

Po zidentyfikowaniu aktywów określa się zależności między nimi a makroprocesami.

Zależności te oznaczają, że wartości oddziaływania w zakresie CIA mogą być powiązane z każdą kategorią aktywów (określone na podstawie wywiadów BIA), dzięki czemu można obliczyć podstawowe zagrożenia cybernetyczne związane z każdym z aktywów.

4.2 ETAP 2 – Analiza ryzyka

4.2.1 Ocena wpływu

Oceny oddziaływania (Business Impact Analysis) dokonują przedstawiciele Firmy zgodnie z metodą przyjętą w uzupełnieniu do podstawowych norm międzynarodowych (ISO 27005, ISO 22301).
Podczas fazy wywiadu BIA i przy użyciu wewnętrznie opracowanego narzędzia do gromadzenia informacji, menedżerowie poszczególnych działów firmy oceniają utratę poufności, integralności i dostępności informacji zarządzanych w ramach ich obszaru kompetencji w kontekście wpływów ekonomicznych, regulacyjnych i wizerunkowych, zgodnie z precyzyjnie zdefiniowanymi skalami oceny.

Jak określono w FAZIE 1, poszczególne procesy grupuje się w makroprocesy specyficzne dla analizowanego kontekstu. Oddziaływania związane z tymi makroprocesami oblicza się jako *„możliwie najgorszy scenariusz”* poszczególnych oddziaływań różnych, tworzących je procesów.

4.2.2 Identyfikacja i wycena aktywów

Identyfikacja aktywów stanowi punkt wyjścia, bez którego nie można właściwie i skutecznie zarządzać bezpieczeństwem firmy. Inwentaryzacja stanowi punkt wyjścia do klasyfikacji aktywów firmy i do analizy poziomu ryzyka, na jakie są narażone.

Celem tej fazy operacyjnej jest sporządzenie spisu inwentaryzacji aktywów informacyjnych lub sformalizowanie istniejących metodologii, uznanych przez firmę za „krytyczne" dla osiągnięcia celów biznesowych, wypełnienia zobowiązań umownych oraz przestrzegania ustawodawstwa i przepisów, którym podlega jej działalność.
Centralną wartość aktywów przedstawiają zwykle informacje (lub dane), które system przetwarza, pozostawiając zadanie ich przetwarzania lub ochrony pozostałym aktywom.
W tym kontekście, podczas wywiadów BIA przypisuje się wartość dla każdego aktywu i dla każdego z wymiarów bezpieczeństwa CIA (poufności, integralności i dostępności) mającego zastosowanie do kontekstu.

Wykorzystując informacje zebrane podczas wywiadów BIA, można zatem powiązać oddziaływania wynikające z makroprocesów, w których są one wykorzystywane, z każdym aktywem.

4.2.3 Analiza zagrożeń i ocena ich prawdopodobieństwa

Metodologia stosowana w procesie zarządzania ryzykiem bezpieczeństwa informacji określa dokonane w odpowiednim momencie określenie zagrożeń, które mają wpływ na przedmiotowe aktywa. Zagrożenia reprezentują wszystkie te elementy lub zdarzenia, które mogą zagrozić aktywom.
Celem takiego działania jest identyfikacja zagrożeń i podatności wpływających na zidentyfikowane i uwzględnione w procesie analizy ryzyka i zarządzania ryzykiem aktywa oraz ocena prawdopodobieństwa ich wystąpienia.
Aby upewnić się, że lista zagrożeń jest wyczerpująca, należy odnieść się do listy zagrożeń ujętych w normie ISO/IEC 27005, a także do uwag opracowanych i opublikowanych przez agencję ENISA po jej badaniach w tym zakresie.
Poszczególne zagrożenia następnie grupuje się w realistyczne scenariusze ryzyka dla analizowanego kontekstu.

4.2.4 Analiza środków zaradczych

Celem tego działania jest określenie środków zaradczych uznanych za niezbędne do objęcia scenariuszy ryzyka dotyczących aktywów zidentyfikowanych w poprzednim kroku.
Aby upewnić się, że lista jest wyczerpująca, Grupa Aruba wykorzystuje listę środków zaradczych w oparciu o najlepsze praktyki zawarte w Załączniku A do normy ISO/IEC 27001. W zależności od rodzaju analizowanej usługi, oceny dla konkretnych tematów można wzbogacić poprzez analizę dalszych czynności kontrolnych sugerowanych przez wiarygodne źródła, takie jak ENISA, AgID, NIST itp.
Po zdefiniowaniu listy kontroli bezpieczeństwa mapuje się je w odniesieniu do scenariuszy ryzyka, w których można je przeprowadzić, aby zmniejszyć prawdopodobieństwo wystąpienia konkretnych zagrożeń lub ich skutków.

Środki zaradcze zostały podzielone na:

- **Reaktywne** (r), mające na celu zmniejszenie wpływu;
- **Zapobiegawcze** (p), mające na celu zmniejszenie prawdopodobieństwa wystąpienia zagrożenia.

4.3 FAZA 3 – Ocena ryzyka

4.3.1 Model i metodyka ryzyka

Wartość ryzyka rozumie się jako funkcję $R = f(A, M, V)$, o wartości A przedmiotowych aktywów, wartości M zagrożeń i V podatności na zagrożenia.

W DRUGIEJ FAZIE procesu zarządzania ryzykiem bezpieczeństwa informacji można zdefiniować model ryzyka (*Modelowanie ryzyka*). Jest to proces wykorzystywany do identyfikacji potencjalnych zagrożeń i podatności, oceny prawdopodobieństwa ich wystąpienia w określonych okolicznościach, uporządkowania ich pod względem istotności i zmniejszenia ryzyka ich wystąpienia poprzez wdrożenie odpowiednich środków zaradczych.

Po zdefiniowaniu podstawowego kontekstu proces *Modelowania zagrożeń* obejmuje:

- Sporządzenie listy potencjalnych ataków/luk w zabezpieczeniach, która obejmuje sposoby, w jakie poufność, integralność i dostępność danych mogą zostać naruszone.
- Ocenę najbardziej prawdopodobnych ataków/luk w zabezpieczeniach, odrzucenie tych, które są mało prawdopodobne lub w zasadzie niemożliwe do zapobiegnięcia w każdym przypadku, a dla wszystkich innych zastosowanie środków kontrolnych lub zaradczych o charakterze technicznym lub proceduralnym.

4.3.2 Obowiązujące wymagania w zakresie bezpieczeństwa i poziom zgodności

Po zidentyfikowaniu wymogów bezpieczeństwa uznanych za mające zastosowanie w kontekście analizy (patrz punkt zatytułowany „Analiza środków zaradczych") ocenia się zakres, w jakim uwzględniono wymogi dotyczące 14 obszarów określonych w Załączniku A do normy ISO/IEC 27001.

Stopień zgodności każdego środka zaradczego wyraża się zgodnie z precyzyjnie określoną skalą wartości od „0", co oznacza brak środka zaradczego, do „4", w którym środek zaradczy został w pełni wdrożony.

W celu analizy poziomu zgodności mechanizmów kontrolnych wymaganych w Załączniku A do normy ISO/IEC 27001 wykorzystuje się informacje i dowody zebrane w ramach prowadzonych wewnętrznie określonych działań związanych z oceną.

4.3.3 Obliczanie podstawowego ryzyka nieodłącznego i rezydualnego

Na tym etapie oblicza się wartość nieodłącznych i rezydualnych zagrożeń bezpieczeństwa CIA (AS-IS (w stanie obecnym), planowanych i TO-BE (w stanie przyszłym)) związanych z analizowaną usługą.

Podstawowe występujące ryzyka nieodłączne dla każdego składnika aktywów i dla każdego scenariusza, zgodnie z opisaną powyżej logiką, oblicza się uwzględniając prawdopodobieństwo ich wystąpienia w poszczególnych scenariuszach ryzyka i ich potencjalny wpływ.
Po określeniu ryzyka nieodłącznego, w celu uzyskania ryzyka rezydualnego (AS-IS, planowanego i TO-BE), bierze się pod uwagę wartości związane ze środkami zaradczymi bezpieczeństwa niezbędnymi do przeciwdziałania scenariuszom ryzyka zidentyfikowanym na etapie audytu wewnętrznego, zarówno pod względem redukcji prawdopodobieństwa wystąpienia zagrożeń, jak i ograniczania ich skutków.

4.4 FAZA 4 – Postępowanie z ryzykiem

4.4.1 Analiza akceptowanego ryzyka

Jedną z koncepcji, którą należy się zająć, jeśli chodzi o zarządzanie ryzykiem, jest koncepcja akceptowanego ryzyka. Termin w ogólnym zarysie odnosi się do tych zagrożeń, z którymi z pewnych powodów nie można sobie poradzić w sposób dogodny lub którym w ogóle nie można zapobiec i które się zwyczajowo akceptuje.

Celem tego działania jest zatem zdefiniowanie kryterium, zgodnie z którym można po prostu zaakceptować kombinacje zagrożenie-aktywa wiążące się z niskim ryzykiem. Dlatego poza indywidualnymi przypadkami określa się próg, poniżej którego określone ryzyko jest po prostu uważane za koszt i nie podlega rozpatrzeniu.

4.4.2 Wyniki analizy: ryzyko rezydualne AS-IS

Prace związane z analizą i oceną ryzyka z uwzględnieniem zastosowanych środków zaradczych (ryzyko rezydualne) realizuje się poprzez wdrożenie:

- Oceny kontroli bezpieczeństwa w odniesieniu do najlepszych praktyk z Załącznika A do normy ISO/IEC 27001;
- Analizy wpływu utraty dostępności informacji, poufności i integralności w odniesieniu do danych usług;
- Analizy podatności i zagrożeń dla aktywów;
- Oceny aktualnego ryzyka dla bezpieczeństwa informacji i określenie porządku istotności.

4.4.3 Analiza rozbieżności i wybór środków zaradczych do wdrożenia

W wyniku przeprowadzonej analizy mającej na celu wyeliminowanie wszelkich istotnych zagrożeń/problemów w zakresie usług świadczonych przez Grupę Aruba oraz w celu ciągłego usprawniania ISMS, dane uzyskane z analizy przeprowadzonej w narzędziu do analizy ryzyka przetwarza się, aby zidentyfikować obszary ryzyka, dla których należy określić odpowiednie środki bezpieczeństwa.

W celu zidentyfikowania działań uznanych za niezbędne w celu poprawy i redukcji ryzyka okresowo określa się zatem analizę luk mającą na celu ocenę rozbieżności między obecnym poziomem stosowania środków ochrony a maksymalnym stosowanym poziomem.

4.4.4 Plan postępowania z ryzykiem – racjonalizacja interwencji

Działania zidentyfikowane w ramach analizy luk następnie grupuje się w konkretne inicjatywy projektowe i dokumentuje w ramach Planu postępowania z ryzykiem.

5 CZĘSTOTLIWOŚĆ PRZEPROWADZANIA ANALIZ

Proces zarządzania ryzykiem związanym z bezpieczeństwem informacji opracowuje się co 12 miesięcy lub częściej w przypadku wystąpienia istotnego zdarzenia, w tym między innymi:

- Nowych aktywów objętych zakresem Zarządzania ryzykiem;
- Nowych zagrożeń, zarówno wewnątrz, jak i na zewnątrz organizacji, a których nie oceniono;
- Możliwości wykorzystania przez zagrożenia nowych lub powiększonych luk w zabezpieczeniach;
- Przeglądu zidentyfikowanych już luk w celu określenia tych, które mogą być bardziej narażone na nowe lub ponownie pojawiające się zagrożenia;
- Zintensyfikowanych skutków lub konsekwencji zagrożeń dla aktywów, podatności na zagrożenia i ryzyka, które razem skutkują niedopuszczalnym ogólnym poziomem ryzyka;
- Szczególnie poważnych incydentów związanych z bezpieczeństwem.

Ponadto analizy mogą być przeprowadzane z różną częstotliwością, na przykład w zakresie zgodności z określonymi normami lub wymogami certyfikacyjnymi.