Mariusz SZCZĘSNY[1]

CO NOWEGO W ZARZĄDZANIU BEZPIECZEŃSTWEM INFORMACJI? STANDARD ISO 27002

Streszczenie

Niniejszy artykuł poświęcony został standardowi ISO 27002, który jest stosunkowo nowym standardem zawierającym wytyczne związane z wdrażaniem Systemu Zarządzania Bezpieczeństwem Informacji. Praca ta ma na celu opisanie samej normy, jej historii oraz najważniejszych wytycznych w sposób przystępny dla czytelników, którzy nie zajmują się problematyką bezpieczeństwa informacji.

Abstract

This article is dedicated to ISO 27002 standard which is a quite new standard that consist guidelines for implementation of Information Security Management System. The objective of this document is to describe the norm, its history and its most important guidelines in intelligible way for readers who don't take up information security.

1 WPROWADZENIE

ISO 27002 to międzynarodowa norma określająca wytyczne związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji (SZBI - ISMS ang. Information Security Management System).

Standard ten był po raz pierwszy opublikowany przez ISO (ang. *Organization for Standarization*) jako norma ISO 17799 w grudniu 2000 r., która stała się częścią serii norm ISO 27XXX.

ISO 27002 jest w swojej naturze wysokopoziomowym i szerokim standardem bezpieczeństwa informacji. Podejście takie zapewnia szerokie możliwości jego stosowania w wielu organizacjach. ISO 27002 jest jedynie standardem opisującym wytyczne do zarządzania bezpieczeństwem informacji. Generalnie jest to standard dający ogólny pogląd na tą problematykę, nie jest to na pewno standard techniczny, dokument opisujący rozwiązania i technologie czy opisujący sposoby testowania systemów bezpieczeństwa. ISO

[1] Mgr Mariusz Szczęsny jest menagerem produktu w Naukowej i Akademickiej Sieci Komputerowej.

27002 jest za to dobrą podstawą dla stosowania skutecznych zabezpieczeń w celu ochrony informacji w organizacjach.

2 DLACZEGO ISO 27002?

Bezpieczeństwo informacji z reguły poparte jest "dobrymi praktykami" oraz wytycznymi. Z racji tego, iż jest to wiedza praktyczna pochodząca często z różnych źródeł powiązanych zarówno z instytutami badawczymi jak również producentami systemów bezpieczeństwa, interpretacje i implementacje tych wytycznych nie zawsze są logiczne i konsekwentne. ISO 27002 jest próbą skodyfikowania i standaryzacji tych wytycznych w celu osiągnięcia takich korzyści, jak:

- utworzenie katalogu zabezpieczeń, który jest rozpoznawany na całym świecie, jako zaufany dla wielu organizacji,
- wyznaczenie miernika dającego możliwości ewaluacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
- stworzenie meta standardu dającego możliwości odnoszenia się do niego przez różne regulacje branżowe.

Dla wielu organizacji ISO 27002 może być:

- wręcz wymaganiem, jeżeli jest to organizacja przetwarzająca wrażliwe informacje,
- standardem, który wyeliminuje konieczność stosowania wielu regulacji branżowych,
- marketingowym narzędziem poświadczającym bezpieczeństwo przetwarzanych informacji.

3 HISTORIA STANDARDU

ISO 27002 jest w linii prostej potomkiem ISO 17799, który jest z kolei potomkiem brytyjskiego standardu BS 7799-1, który został opracowany przez British Standard Institute (BSI). Organizacja ta przyczynia się do rozwoju standardów w zakresie bezpieczeństwa informacji. W odpowiedzi na wymagania firm komercyjnych i instytucji, grupa robocza powołana w 1990 r. zajmująca się problematyką bezpieczeństwa informacji opublikowała już w 1993 r. procedury postępowania w zakresie zarządzania bezpieczeństwem informacji (ang. *Code of Practice for Information Security Management*). Dokument ten był podwaliną dla pierwszej wersji standardu BS 7799, który został opublikowany w 1995 r.

Pod koniec lat dziewięćdziesiątych w odpowiedzi na potrzeby zgłaszane przez firmy, BSI stworzył program akredytacji firm audytorskich zajmujących się oceną zgodności w zakresie normy BS 7799. Jednocześnie w tym samym czasie opublikowano nowe wersje standardu BS 7799, co miało miejsce w latach 1998, 1999, 2000 i 2002. W tym czasie bezpieczeństwo informacji stało się również ważne i znaczące dla firm używających technik komputerowych do przetwarzania informacji. W tamtych latach wiele organizacji stosowało standard BS 7799, jednocześnie też rosło zapotrzebowanie na opracowanie międzynarodowego standardu bezpieczeństwa informacji, który byłby szeroko rozpoznawany na całym świecie. To zapotrzebowanie spowodowało, iż w grudniu 2000 r. opublikowano pierwszy międzynarodowy standard bezpieczeństwa informacji – ISO 17799:2000. W celu zachowania nomenklatury nazewniczej z serii norm ISO 27000, ISO 17799 została zaktualizowana i wydana w czerwcu 2005 r. już jako ISO 27002.

Oba standardy zostały stworzone w celu osiągnięcia założonych celów, dlatego istotne jest zrozumienie różnic pomiędzy nimi.

Tabela 1. Podstawowe różnice pomiędzy ISO 27002 i ISO 27001

ISO 27001	ISO 27002
• Standard audytorski oparty o wymagania stawiane audytowi. • Lista zabezpieczeń organizacyjnych, które powinny zostać uwzględnione. • Używany do audytowania bezpieczeństwa organizacji oraz certyfikowania w zakresie SZBI.	• Wytyczne implementacyjne oparte o rekomendowane „dobre praktyki”. • Lista zabezpieczeń operacyjnych, które organizacja powinna rozważyć. • Używany do szacowania kompletności i spójności systemu zarządzania bezpieczeństwem organizacji.

4 OBSZARY ZABEZPIECZEŃ

ISO 27002 definiuje informacje przetwarzane w firmie jako ważne aktywa, które istnieją w wielu formach, które muszą być chronione w odpowiedni sposób. ISO 27002 definiuje bezpieczeństwo informacji jako ochronę tych informacji przed zagrożeniami w takim porządku, iż najważniejsze dla organizacji powinno być przede wszystkim zapewnienie ciągłości biznesu, zminimalizowanie ryzyka biznesowego a także maksymalizacja zwrotu z inwestycji. Podejście takie sprawia, iż zabezpieczenia opisane w normie ISO 27002 koresponduą z wieloma obszarami działalności firmy, takimi jak:

- bezpieczeństwo,
- bezpieczeństwo aplikacji,

- bezpieczeństwo platform komputerowych,
- bezpieczeństwo sieciowe,
- bezpieczeństwo fizyczne.

W celu osiągnięcia założonych celów, ISO 27002 identyfikuje jedenaście obszarów zabezpieczeń, 39 celów zabezpieczeń oraz 133 zabezpieczenia. Każde zabezpieczenie jest odpowiednio zdefiniowane, opisane wraz z wytycznymi do implementacji i wyjaśnieniem intencji jego stosowania.

Standard wskazuje również, które zabezpieczenia powinny być ważne dla organizacji z legislacyjnego punktu widzenia, które zaś z punktu widzenia bezpieczeństwa informacji.

Z legislacyjnego punktu widzenia najważniejsze to[2]:

- ochrona danych osobowych i prywatności,
- ochrona firmowych danych utrwalonych na różnych nośnikach,
- ochrona praw autorskich.

Z punktu widzenia bezpieczeństwa informacji:

- dokument polityki bezpieczeństwa,
- alokacja odpowiedzialności w zakresie bezpieczeństwa informacji,
- edukacja i szkolenia w zakresie bezpieczeństwa informacji,
- właściwe przetwarzanie informacji przez aplikacje,
- zarządzanie podatnościami technicznymi,
- zarządzanie ciągłością działania,
- zarządzanie incydentami bezpieczeństwa oraz udoskonalaniem systemów.

Najważniejsze obszary zabezpieczeń opisane w ISO 27002, cele zabezpieczeń oraz kluczowe atrybuty poszczególnych zabezpieczeń zostały opisane poniżej. Każdy obszar zabezpieczeń opisany w normie ISO 27002 posiada następujące sekcje, tj. cel zabezpieczenia, zabezpieczenie, wytyczne implementacyjne oraz dodatkowe informacje.

4.1 Polityka bezpieczeństwa[3]

Zabezpieczenie w postaci polityki bezpieczeństwa adresuje głównie zarządzanie w kontekście zgodności bezpieczeństwa informacji z wymaganiami biznesowymi, prawodawstwem oraz regulacjami. Polityka bezpieczeństwa jest to zatwierdzony przez zarząd firmy dokument, który powinien być opublikowany w organizacji w celu zade-

[2] ISO/IEC 27002:2005 – str. 10 – ISO Second Edition 2005-06-15.
[3] SO/IEC 27002:2005 – str. 19 – ISO Second Edition 2005-06-15.

monstrowania i podkreślenia odpowiedzialności zarządu za bezpieczeństwo informacji. Polityka bezpieczeństwa może być również częścią całościowego dokumentu polityki firmy. Przegląd polityki bezpieczeństwa oraz ciągły monitoring jej zgodności ze środowiskiem firmy realizowany jest z reguły przez wyznaczoną osobę, która bardzo często staje się właścicielem tego dokumentu. W ramach obszaru polityka bezpieczeństwa wyróżnione zostały następujące zagadnienia:

- dokument polityki bezpieczeństwa,
- przegląd polityki bezpieczeństwa.

4.2 Organizacja bezpieczeństwa informacji[4]

Organizacja w zakresie bezpieczeństwa informacji zapewnia możliwość zarządzania bezpieczeństwem informacji w sposób skoordynowany włączając w to działalność zarządu. Główny nacisk położony został tu na przywództwo w zakresie jasnego, bezpośredniego oraz autoryzowanego koordynowania prac związanych z zabezpieczeniem informacji przetwarzanych w organizacji. W obszarze tym opisano również alokację odpowiedzialności w zakresie bezpieczeństwa informacji, co oznacza m.in. ich przypisanie poszczególnym pracownikom w sposób pośredni, jak również bezpośredni np. w opisie stanowiska. Kolejne opisane zabezpieczenia to:

- proces autoryzacji nowej infrastruktury, w której będą przetwarzane informacje – każdy system, który będzie przetwarzał informacje, przed jego wprowadzeniem powinien być przetestowany pod kątem bezpieczeństwa,
- umowy o zachowaniu poufności – zrządzanie i utrzymanie bezpieczeństwa informacji w sytuacji kiedy informacje wychodzą poza obręb firmy,
- kontakt z władzami – relacje i zachowania w zakresie kontaktu z lokalnymi władzami, służbami jak również z wewnętrznymi zespołami odpowiedzialnymi za zarządzanie incydentami,
- kontakty z grupami interesu – relacje w zakresie kontaktu z zewnętrznymi grupami ekspertów specjalizującymi się w bezpieczeństwie informacji.

4.3 Strony trzecie[5]

Obszar ten odnosi się do identyfikacji ryzyk związanych ze współpracą ze stronami trzecimi – zabezpieczanie współpracy z klientami poprzez umowy z użytkownikami

[4] ISO/IEC 27002:2005 – str. 21 – ISO Second Edition 2005-06-15.
[5] ISO/IEC 27002:2005 – str. 26 – ISO Second Edition 2005-06-15.

systemu jak również zabezpieczenie współpracy z firmami trzecimi poprzez umowy serwisowe SLA (ang. *Service Level Agreement*).

4.4 Zarządzanie aktywami informacyjnymi[6]

Jest to obszar zabezpieczeń adresujący możliwości infrastruktury w zakresie ochrony aktywów informacyjnych firmy włączając w to inwentaryzację oraz mechanizmy utrzymujące rozliczalność w zakresie aktywów, przypisanych do nich właścicieli oraz zarządców. W obszarze tym zdefiniowano również właścicielstwo aktywów oraz akceptowalne ich używanie. Właścicielstwo aktywu może oznaczać przypisanie do:

- procesu biznesowego,
- zdefiniowanego zbioru operacji,
- aplikacji,
- zdefiniowanego zbioru danych.

Akceptowalne użycie aktywów firmowych w szczególności powinno obejmować zasady wysyłania korespondencji e-mail oraz użycia Internetu, jak również wytyczne w zakresie w używania urządzeń mobilnych.

4.5 Klasyfikacja informacji[7]

Klasyfikacja to mechanizm segregujący aktywa informacyjne w zakresie ich wpływu na działalność biznesową firmy. W obszarze tym opisano również konieczność stosowania standardu oznaczania aktywów informacyjnych w kontekście ich klasyfikacji, jak również konieczność wprowadzenia procesu obsługi informacji poczynając od jej wprowadzenia do firmy a kończąc na jej usunięciu.

4.6 Bezpieczeństwo zasobów ludzkich[8]

Jest to obszar zabezpieczeń umożliwiający organizacji niwelowanie ryzyk w zakresie ludzkich interakcji, które występują podczas przetwarzania informacji w organizacji, włączając w to m.in. klasyfikację pracowników w kontekście lokalnego prawa i uwarunkowań kulturowych z jednoczesnym zapewnieniem ich kwalifikacji przy dostępie do aktywów informacyjnych. Klasyfikacja taka może być oparta o aktywa informacyjne jak również opis stanowisk. Dodatkowo obszar ten precyzuje odpowiedzialność personelu

[6] ISO/IEC 27002:2005 – str. 31 – ISO Second Edition 2005-06-15.
[7] ISO/IEC 27002:2005 – str. 33 – ISO Second Edition 2005-06-15.
[8] ISO/IEC 27002:2005 – str. 35 – ISO Second Edition 2005-06-15.

w zakresie bezpieczeństwa informacji - pracownicy powinni być jasno poinformowani o swoich odpowiedzialnościach włączając w to procedury postępowania oraz zachowania poufności. Istotnym elementem tego obszaru są również szkolenia i edukacja personelu w zakresie bezpieczeństwa informacji. Każdy pracownik powinien przejść takie szkolenia, jak również powinien być zapewniony program ich aktualizacji i okresowego powtarzania.

Obszar ten to jedna z ważniejszych grup zabezpieczeń, która znajduje często zastosowanie w życiu codziennym firmy. Potwierdzeniem tego jest fakt, że m.in. zdefiniowano tu również zasady postępowania przy zwalnianiu pracowników oraz usuwanie praw dostępu do aktywów informacyjnych firmy.

4.7 Bezpieczeństwo fizyczne i środowiskowe[9]

Jest to obszar zabezpieczeń dedykowany do ochrony budynków i infrastruktury firmy. Wyróżnia się w nim ochronę budynków, terenu, wejść do firmy oraz wszelkich zagadnień związanych z bezpieczeństwem fizycznego dostępu do aktywów informacyjnych. Szczególną uwagę poświęcono m.in. takim zagadnieniom jak:

- ochrona przed zagrożeniami zewnętrznymi i środowiskowymi,
- praca w bezpiecznych obszarach (wyznaczone bezpieczne obszary firmy),
- zapewnienie ochrona siedziby firmy przed nieuprawnionym dostępem,
- zabezpieczenia w zakresie fizycznego dostępu,
- ochrona pomieszczeń i infrastruktury przed nieuprawnionym dostępem,
- kontrolowanego dostępu dla osób zewnętrznych i kontrahentów,
- bezpieczeństwo urządzeń,
- zapewnienie mediów niezbędnych dla przetwarzania informacji,
- ochrona infrastruktury kablowej firmy,
- serwisowanie urządzeń,
- bezpieczeństwo urządzeń mobilnych,
- bezpieczne wycofywanie urządzeń z eksploatacji lub ich powtórne użycie,
- kontrola infrastruktury używanej do pracy poza siedzibą firmy.

[9] ISO/IEC 27002:2005 – str. 41 – ISO Second Edition 2005-06-15.

4.8 Komunikacja oraz zarządzanie operacjami[10]

Ten obszar zabezpieczeń ma za zadanie umożliwienie organizacji bezpiecznej pracy na aktywach informacyjnych włączając w to procedury operacyjne lub odpowiednie zestawy procedur, które wspierają standardy i polityki przyjęte przez organizację. W obszarze tym wyróżniamy takie zagadnienia jak:

- kontrola zmian – proces umożliwiający zarządzanie zmianami i konfiguracją zabezpiecezń włączając w to zmiany samego systemu SZBI,
- zarządzanie incydentami – mechanizm zapewniający szybką i efektywną odpowiedź na występujące incydenty bezpieczeństwa,
- separacja uprawnień – segregacja i rotacja uprawnień, co zapewnia minimalizację potencjalnych kolizji czy niekontrolowanych wycieków informacji,
- planowanie pojemności systemów – mechanizm zapewniający stały monitoring pojemności systemów przetwarzających informacje, tak aby zapewnić im nieprzerwaną pracę,
- testy akceptacyjne – stosowanie metodyki umożliwiającej wprowadzanie zmian systemowych z zachowaniem poufności, integralności i dostępności informacji,
- złośliwy kod – stosowanie zabezpieczeń zapewniających ochronę przed infekcją systemów złośliwym kodem,
- sprzątanie pomieszczeń firmy - ustanowienie polityk, standardów, wytycznych i procedur zapewniających bezpieczeństwo aktywów informacyjnych podczas rutynowych prac sprzątających,
- zarządzanie sieciami – zabezpieczenia umożliwiające bezpieczną pracę przy wykorzystaniu infrastruktury sieciowej,
- nośniki danych – wprowadzenie zabezpieczeń umożliwiających bezpieczne przechowywanie i usuwanie nośników danych jak również dokumentów,
- wymiana informacji – ustanowienie zabezpieczeń zarządzających wymianą informacji włączając w to umowy z użytkownikami systemu oraz mechanizmy zapewniające transport informacji.

4.9 Kontrola dostępu[11]

Kontrola dostępu to jeden z najważniejszych obszarów zabezpieczeń stosowanych w standardzie ISO 27002. Umożliwia organizacji kontrolę dostępu do aktywów informa-

[10] ISO/IEC 27002:2005 – str. 41 – ISO Second Edition 2005-06-15.
[11] ISO/IEC 27002:2005 – str. 72 – ISO Second Edition 2005-06-15.

cyjnych w oparciu o przypisane reguły biznesowe oraz politykę bezpieczeństwa. Standard wyróżnia w tym obszarze takie zagadnienia, jak:

- wymagania biznesowe – kontrolowany dostęp do zasobów firmy w oparciu o wymagania i biznesowe i zasadę „wiedzy koniecznej”,
- zarządzanie użytkownikami – mechanizm zapewniający rejestrację oraz usuwanie użytkowników systemów, kontrolę i rozliczalność dostępu oraz uprawnień, jak rów-nież zarządzanie hasłami,
- odpowiedzialność użytkowników – uświadamianie użytkowników o odpowiedzialności w zakresie dostępu do aktywów informacyjnych firmy, włączając w to udostępnianie haseł dostępowych czy stosowanie nieautoryzowanych urządzeń,
- kontrola dostępu do sieci – autoryzowane używanie dostępu do serwisów sieciowych, włączając w to takie zabezpieczenia jak:
  - uwierzytelnianie węzłów sieciowych,
  - uwierzytelnianie zdalnych użytkowników,
  - definiowanie routingu w sieciach,
  - weryfikacja bezpieczeństwa urządzeń podłączanych do sieci,
  - segmentacja sieci,
  - kontrola połączeń sieciowych,
  - zapewnienie bezpieczeństwa serwisów sieciowych.
- kontrola dostępu do serwerów i stacji roboczych - są to m.in. takie zabezpieczenia jak:
  - automatyczne identyfikowanie stacji roboczych i terminali,
  - bezpieczne logowanie do systemów,
  - uwierzytelnianie użytkowników,
  - zarządzanie hasłami,
  - bezpieczne wykorzystywanie zasobów systemowych,
  - zapewnienie użytkownikom możliwości cichego alarmowania pod przymusem (np. przyciski alarmowe),
  - zapewnienie wygasania czasu połączeń dla stacji roboczych i użytkowników.
- kontrola dostępu do aplikacji - to limitowanie dostępu do aplikacji w oparciu o poziomy uprawnień,
- monitoring dostępu – to stałe monitorowanie dostępu do systemów w celu wykrywania nieautoryzowanych prób,
- urządzenia mobilne – to przede wszystkim zapewnienie polityk i standardów w zakresie bezpiecznego używania urządzeń mobilnych jak również stosowania bezpiecznego dostępu.

4.10 Rozwój i utrzymanie systemów[12]

Jest to obszar zabezpieczeń dedykowany dla zapewnienia organizacji możliwości adekwatnego pozyskiwania i utrzymywania systemów bezpieczeństwa, które mają za zadanie ochronę przetwarzanych informacji w firmie. W obszarze tym wyróżniono m.in.:

- wymagania co do systemów bezpieczeństwa – każda implementacja systemu czy wprowadzanie zmian do istniejącego systemu bezpieczeństwa powinny być realizowane z uwzględnieniem bezpieczeństwa informacji,
- wymagania co do bezpieczeństwa aplikacji - każde wdrożenie czy wprowadzanie zmian do aplikacji powinny być realizowane z uwzględnieniem zagadnień bezpieczeństwa informacji,
- kryptografię - stosowanie polityk, standardów i procedur w zakresie zarządzania ochroną kryptograficzną,
- integralność systemów – zapewnienie mechanizmów kontroli dostępu oraz weryfikacji integralności danych i aplikacji, włączając w to implementowane poprawki oraz aktualizacje.
- doskonalenie systemów bezpieczeństwa – zapewnienie mechanizmów kontroli zmian oraz przeglądów technicznych jako spójnego procesu w firmie.

4.11 Zarządzanie ciągłością działania[13]

W ramach tego obszaru zabezpieczeń standard zapewnia organizacji możliwości przeciwdziałania wszelkim przerwom w działalności operacyjnej. Wyróżnia się tu m.in. takie zagadnienia jak:

- planowanie ciągłości działania - stosowanie odpowiedniej strategii zapewnienia ciągłości działania opartej o analizę wpływu zagrożenia na biznes,
- testowanie ciągłości działania – testowanie planów zapewnienia ciągłości działania i dokumentowanie tego procesu,
- utrzymanie ciągłości działania – przegląd strategii oraz cykliczne weryfikowanie planów.

[12] ISO/IEC 27002:2005 – str. 89 – ISO Second Edition 2005-06-15.
[13] ISO/IEC 27002:2005 – str.107 – ISO Second Edition 2005-06-15.

4.12 Zgodność

Zgodność to bardzo istotny obszar zabezpieczeń definiowany przez standard ISO 27002. Umożliwia on organizacji zapewnienie zgodności z regulacjami, statutem, zobowiązaniami oraz wszelkimi wymaganiami odnośnie bezpieczeństwa informacji. Norma wyróżnia tu przede wszystkim takie zagadnienia jak:

- prawodawstwo, które w sposób pośredni lub bezpośredni dotyczy organizacji,
- prawo autorskie,
- ochrona informacji przechowywanych w firmie,
- chrona prywatności,
- ochrona przed niewłaściwym użyciem systemów przetwarzających informacje,
- regulacje w zakresie stosowania środków ochrony kryptograficznej,
- gromadzenie dowodów w celach dochodzeniowych,
- mechanizmy weryfikacji zgodności systemu przetwarzania informacji z założoną polityką bezpieczeństwa,
- audytowanie systemów w celu maksymalizowania efektywności stosowanych zabezpieczeń.

5 JAK WDROŻYĆ ISO 27002 W ŻYCIE?

Standard ten zawiera wytyczne jak wdrożyć wymagane zabezpieczenia zgodnie z założonymi wymaganiami biznesowymi. Norma ta w szczególności kładzie duży nacisk na znaczenie każdego zabezpieczenia w kontekście zidentyfikowanych ryzyk biznesowych, przed którymi to zabezpieczenie ma uchronić organizację. Oznacza to, że każda firma, które chce skorzystać z wytycznych standardu, musi sporządzić analizę ryzyka, dzięki której możliwy będzie dobór odpowiednich zabezpieczeń. Idąc dalej, ISO27002 podaje również wytyczne co do samego szacowania ryzyka, włączając w to:

- zakres analizy,
- analizę ryzyka,
- ewaluację ryzyka,
- postępowanie z ryzykiem.

Co do wymagań odnośnie kryteriów oceny jakości szacowania ryzyka, tym zagadnieniem zajmuje się norma ISO27001. Poniżej zaś w sześciu fazach opisany został proces doboru odpowiednich zabezpieczeń, który proponuje nam standard ISO 27002.

Faza 1 - Ustalenie zakresu ryzyka

ISO 27002 zostało zaprojektowane tak, aby dobór zabezpieczeń był naturalny dla organizacji. Zabezpieczenia mogą być wdrażane na różny sposób w zależności od wymagań operacyjnych firmy. Zakres ryzyk strategicznych dotyczy całej organizacji i z reguły skupiony jest na ich niwelowaniu w odniesieniu do usług świadczonych przez firmę. Z kolei zakres ryzyk taktycznych jest całościowym programem poświęconym niwelowaniu ryzyk w odniesieniu do procesów wspierających świadczenie usług. Identyfikowane są również ryzyka operacyjne, które dotyczą wszelkich aspektów operacyjnych firmy w zakresie przetwarzania informacji.

Faza 2 - Identyfikacja ryzyka

Ryzyka wynikają bezpośrednio z zagrożeń. Zagrożenie to negatywne wydarzenie w zakresie bezpieczeństwa informacji, które pojawia się, dlatego że wykorzystano odkrytą podatność. Zagrożenia mogą dotyczyć całej organizacji. Rozróżnia się zagrożenia taktyczne jak również operacyjne. Taktyczne dotyczą wprost podatności organizacyjnych, jak np. mało efektywne procedury, operacyjne zaś dotyczą podatności technicznych.

Faza 3 - Określanie ryzyka

Zagrożenia nie koniecznie muszą być kwalifikowane jako ryzyko. Zagrożenia zidentyfikowane w fazie 2 wraz z przypisanymi do nich podatnościami muszą zostać oszacowane pod kątem ich ważności i istotności w kontekście ryzyka, które niosą ze sobą dla dane-go środowiska firmy. Oszacowane ryzyka pozwalają organizacji na priorytetyzację ochrony przed zagrożeniami. Realizowane jest to z wykorzystaniem procesu analizy ryzyka.

Z kolei szacowanie ryzyk strategicznych opiera się głównie na procesach biznesowych całej organizacji. Nie wszystkie procesy biznesowe muszą z założenia posiadać ryzyka związane z przetwarzaniem informacji.

Szacowanie ryzyk taktycznych to nic innego jak poszukiwanie sposobów na niwelowanie ryzyk strategicznych. Szacowanie ryzyk operacyjnych to z kolei próba określenia celów zabezpieczeń dla ochrony aktywów informacyjnych firmy.

Faza 4 - Postępowanie z ryzykiem

Posiadając określone w fazie 3 ryzyka, przystępujemy do ich hierarchizowania oraz planowania postępowania z nimi. Wyróżniamy następujące możliwości postępowania z ryzykiem:

- unikanie ryzyka - możemy próbować uniknąć ryzyka poprzez np. zmianę lokalizacji centrum danych,
- transfer ryzyka - ryzyko może być przeniesione na podmiot, który posiada większą tolerancję w zakresie tego ryzyka, jak np. zakup polisy ubezpieczeniowej.
- akceptacja ryzyka - ryzyko może zostać zaakceptowane, gdyż jego poziom z biznesowego punktu widzenia może być akceptowalny dla organizacji. W takim przypadku niezbędne jest stałe monitorowanie tego ryzyka przez organizację.
- niwelowanie ryzyka - ryzyko może być niwelowane do akceptowalnego poziomu poprzez zastosowanie zabezpieczeń.

Faza 5 - Niwelowanie ryzyka

Cele stosowania zabezpieczeń ujęte w ISO 27002 pozwalają na łatanie podatności poprzez stosowanie opisanych zabezpieczeń. Identyfikacja właściwego celu zabezpieczeń oraz samego zabezpieczenia jest pierwszym krokiem do rozpoczęcia procesu niwelowania ryzyka powiązanego z daną podatnością.

Faza 6 - Pomiar efektywności zabezpieczeń

W zależności od rodzaju zabezpieczeń, istnieje wiele sposobów na pomiar ich efektywności. Ważne jest, aby taki pomiar był wykonywany permanentnie, aby jego wyniki były podwaliną do doskonalenia systemów zabezpieczeń.

6 PODSUMOWANIE

ISO 27002 to przewodnik sugerujący organizacjom jakie czynności powinny zostać podjęte w celu spełnienia wymagań międzynarodowego standardu w zakresie zarządzania bezpieczeństwem informacji. W obecnych czasach istnieje duże zapotrzebowanie na standaryzację zabezpieczeń w zakresie bezpieczeństwa informacji. Ten fenomen jest napędzany przez wiele czynników, takich jak chociażby popularność normy ISO 27001, czy popularność norm branżowych (SOX, PCI, HIPAA, GLBA itp.), ale nie tylko. Standaryzacja bezpieczeństwa informacji jest niezmiernie ważna dla dzisiejszego globalnego świata biznesu, który chce w bezpieczny i zaufany sposób wymieniać informacje, który chce korzystać w pełni z dobrodziejstw globalnej sieci, który również pragnie być konkurencyjny i szybko reagować na zmieniający się rynek.

Literatura

1. Norma ISO/IEC 27002:2005, Second Edition, 15.06.2005 r. – ISO Office, Geneva.

BAZY DANYCH I ZARZĄDZANIE SYSTEMAMI INFORMATYCZNYMI