Sylwia MIERZEJEWSKA
Katedra Procesów i Urządzeń Przemysłu Spożywczego
Politechnika Koszalińska

Zarządzanie bezpieczeństwem informacji

Streszczenie

Informacja jest obecnie bardzo cennym towarem, często wykradanym i nieuczciwie wykorzystywanym. Odpowiednio opracowane, wdrożone i eksploatowane Systemy Zarządzania Bezpieczeństwem Informacji umożliwiają ochronę danych wpływających na konkurencyjność firmy oraz wymaganych przepisami prawa. W pracy opisano formy zasobów informacyjnych oraz przedstawiono normy dotyczące SZBI.

Słowa kluczowe: *System Zarządzania Bezpieczeństwem Informacji, informacja*

Management of security information

Summary

Currently information is a very precious commodity stealing often and unfairly used. Properly designed, implemented and operated Systems Information Security Management enable data protection affect the competitiveness of the company or required by the laws. This paper describes the form of information resources and presents standards for ISMS.

Key words: *Information Security Management System, information*

Wprowadzenie

Szybki rozwój informatyzacji, nie tylko w instytucjach państwowych, zakładach pracy, ale również w gospodarstwach domowych, stwarza coraz większe zagrożenie związanie z bezpieczeństwem informacji. Dane osobowe, dane firmy, informacje technologiczne czy tajemnice państwowe są narażone na umyślne lub nieumyślne zagrożenia utraty bezpieczeństwa. Od początku rozwoju informatyzacji dużą uwagę przywiązuje się do ochrony ważnych danych stosując coraz lepsze komputery i zabezpieczenia antywirusowe, programy zapewniające szyfrowanie czy różne rozwiązania prawne (www.pkn.pl). Zagrożenia związane z bezpieczeństwem informacji można opisać za pomocą trzech elementów, jakimi są utrata poufności, ograniczenie dostępności naruszenie integralności informacji. Mogą one mieć charakter zdarzeń przypadkowych (błędy czynnika ludzkiego, awarie, błędy oprogramowania), mogą być powodowane przez czynniki naturalne (powódź, pożar), ale mogą być również wynikiem celowego działania człowieka (ataki hackerskie).

Celem opracowania jest przedstawienie zagrożeń związanych z nieprawidłowym dostępem do informacji, jako ważnego dobra, które musi być chronione oraz omówienie podstawowych norm i rozwiązań prawnych dotyczących bezpieczeństwa informacji.

Informacja

"*Informacja jest wartościowa i użyteczna wtedy, gdy mamy pewność, że pochodzi z wiarygodnego, bezpiecznego źródła, gdy jest dostępna w każdej chwili dla autoryzowanego użytkownika oraz gdy jest niedostępna dla postronnych osób, jeśli występuje taka potrzeba*" (Schweitzer, 2012).

Poczucie bezpieczeństwa jest podstawową potrzebą człowieka. Maslow (2016) w piramidzie potrzeb usytuował potrzeby bezpieczeństwa na drugim poziomie, zaraz po potrzebach fizjologicznych, polegających na zaspokojeniu głodu, picia, ogrzania się, schronienia czy odpoczynku. W związku z tym chronimy rzeczy, które mają dla nas wartość (zamykamy samochód, złoto i cenne przedmioty przechowujemy w sejfach, ubezpieczamy domy, itd.). Podobnie jest z potrzebą ochrony informacji o sobie samych. Zapominamy jednak często o danych osobowych i tajemnicach, a one również wymagają odpowiednich działań w celu ich zabezpieczenia.

Informacja (zasoby informacyjne) może występować w różnych formach zaczynając od baz danych, wydruków i odręcznych notatek, przez te przesyłane pocztą tradycyjną i elektroniczną, wyświetlane na stronach internetowych, a kończąc na informacjach przekazywanych ustnie w czasie rozmowy. Do ochrony baz danych czy poczty elektronicznej jesteśmy przyzwyczajeni. Natomiast informacje wypływające np. z rozmowy, zapisków ze spotkań nie są dostatecznie chronione.

Informację można sklasyfikować również ze względu na jej stan (stopień przetworzenia), jako: utworzona, otrzymana, składowana, usunięta, przetwarzana, transmitowana, wykorzystana (właściwie lub niewłaściwie), uszkodzona, zagubiona, skradziona. Informacja jest obecnie bardzo cennym towarem i coraz częściej staje się łupem złodziei. W obecnych czasach informacja wykradana jest najczęściej przez Internet (wirusy, programy łamiące hasła, blokujące dostęp do poczty elektronicznej, stron www). Aby właściwie chronić informacje trzeba stworzyć zbiór zasad (regulaminy, instrukcje i procedury itp.), obowiązujących przy przetwarzaniu i wykorzystaniu informacji w organizacji.

Polityka Bezpieczeństwa Informacji dotyczy całego procesu korzystania z informacji, niezależnie od sposobu jej przetwarzania (tj. zbierania, utrwalania, przechowywania, opracowywania, zmieniania, udostępniania i usuwania). Dotyczy wszystkich systemów przetwarzania informacji,

zarówno systemów prowadzonych klasycznie (archiwa, kartoteki, dokumenty papierowe) jak i systemów komputerowych. Praktyczne podejście do tematu ochrony informacji wiąże się z rozpoznaniem rzeczywistych potrzeb organizacji w zakresie ochrony informacji, oczywiście w zgodzie z polskim prawodawstwem. Zgodnie Ustawą z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji za tajemnicę przedsiębiorstwa rozumie się: "*nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, handlowe lub organizacyjne przedsiębiorstwa, co, do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności*" (Dz.U. 1993 nr 47 poz. 211). Z przytoczonej definicji wynika, że aby chronić tajemnice firmy muszą być spełnione trzy warunki, tj.:
- dane nie mogą być ujawnione publicznie;
- muszą posiadać pewną wartość;
- zarząd podjął niezbędne działania w celu zapewnienia ich poufności.

Jeżeli nie określimy, co stanowi tajemnicę firmy i nie poinformujemy o tym pracowników, mogą oni całkiem nieświadomie przekazać te informacje konkurencji lub innym nieuprawnionym osobom. Do informacji poufnych mających znaczącą wartość możemy zaliczyć między innymi: listę klientów i dostawców, złożone oferty, ceny, wyniki badań i sondaży, statystyki, biznesplany, budżety, plany kampanii reklamowych i wiele innych.

Przedsiębiorstwa mają różne zasoby informatyczne i niekiedy ich właściwa ochrona, oprócz spełnienia wymagań prawa, przyczynia się do wzrostu konkurencyjności. Dla przedsiębiorstwa najważniejsze są dane stanowiące tajemnicę zakładu i zarząd musi podjąć odpowiednie działania w celu ich ochrony. Nieprofesjonalne podejście do ochrony danych powinno być zastąpione działaniami opartymi na sprawdzonych metodach opisanych w normach ISO/IEC opracowywanych w podkomitetach ISO/IEC/JTC 1. Przedstawione tam metody i zasady uważane są za najlepsze i zaleca się je do powszechnego stosowania (www.pkn.pl).

Podstawowe normy w zakresie zarządzania bezpieczeństwem informacji

Bardzo ważną rolę w bezpieczeństwie informacji stanowią rozwiązania prawne, w których występują powołania na normy z omawianego zakresu. Podstawowymi normami w zakresie zarządzania bezpieczeństwem informacji i budowy systemów zarządzania bezpieczeństwem informacji są normy z rodziny ISO/IEC 27000:
– PN-ISO/IEC 27000:2014-11 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia.
– PN-ISO/IEC 27001:2014-12 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.
– PN-ISO/IEC 27002:2014-12 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji.
– PN-ISO/IEC 24762: 2010 Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie.

Norma PN-ISO/IEC 27000: 2014-11 jest niezbędna przy wdrażaniu i certyfikacji Systemów Zarządzania Bezpieczeństwem Informacji. Zawiera definicje stosowane we wszystkich normach z rodziny SZBI i może być stosowana we wszystkich typach organizacji niezależnie od wielkości i zakresu działalności.

Norma PN-ISO/IEC 27001: 2014-12 jest normą referencyjną. Stosowana na całym świecie uważana jest za podstawowy akt prawny dotyczący bezpieczeństwa informacji. Norma ta stanowi również podstawę certyfikacji SZBI. W normie określono wymagania o charakterze ogólnym dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji. Opisano wymagania dotyczące szacowania ryzyka i postępowania z ryzykiem w zakresie bezpieczeństwa informacji. W przypadku deklaracji na zgodność z powyższą normą wszystkie wymagania zawarte w punktach od 4 do 10 muszą być uwzględnione i żadne z wymagań nie może być pominięte.

Norma PN-ISO/IEC 27002: 2014-12 jest przeznaczona do stosowania przez organizacje, które zamierzają wybierać wdrażać powszechnie akceptowane zabezpieczenia informacji oraz opracować własne zalecenia w zakresie SZBI.

Norma PN-ISO/IEC 24762: 2010 jest podstawą w odzyskiwaniu newralgicznych danych po katastrofie. Katastrofa to nie tylko trzęsienie ziemi czy powódź, ale przyczyną utraty danych może być również niewielki pożar.

Podsumowanie

Rozwój technik informacyjnych, w tym tworzenie się społeczeństwa i kultury informacyjnej, powoduje wzrost zagrożeń związanych z bezpieczeństwem informacji i ochrony prywatności. Wpływa to rosnącą potrzebę stosowania coraz skuteczniejszych rozwiązań w zakresie bezpieczeństwa informacji. Przeszkoleni i świadomi swojej odpowiedzialności pracownicy są dużo lepszą ochroną informacji niż najlepsze zabezpieczenia.

Bibliografia

Maslow A. H., 2016. Motywacja i osobowość, Wydawnictwo Naukowe PWN, Warszawa ISBN: 9788301148096
PN-ISO/IEC 24762: 2010 Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie.
Schweitzer T., 2012. Normalizacja. Polski Komitet Normalizacyjny. ISBN 978-83-266-9555-1.
Dz.U. 1993 nr 47 poz. 211 Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji.
PN-ISO/IEC 27000:2014-11 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia.
PN-ISO/IEC 27001:2014-12 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania
PN-ISO/IEC 27002:2014-12 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji
www.pkn.pl

Sylwia Mierzejewska
Politechnika Koszalińska, Katedra Procesów i Urządzeń Przemysłu Spożywczego
ul. Racławicka 15-17, 75-336 Koszalin, e-mail: *sylwia.mierzejewska@tu.koszalin.pl*