PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
Technika, Informatyka, Inżynieria Bezpieczeństwa 2013, t. I

Dariusz Rydz, Marlena Krakowiak, Teresa Bajor
Politechnika Częstochowska
Al. Armii Krajowej 19, 42-200 Częstochowa, e-mail: rydz@wip.pcz.pl

ZAPEWNIENIE BEZPIECZEŃSTWA INFORMACJI W PRZEDSIĘBIORSTWACH

Streszczenie. W obecnych czasach przedsiębiorstwa prowadzące działalność gospodarczą narażone są na wiele niebezpieczeństw ze strony nieuczciwej konkurencji. Jednym z ważniejszych przeciwdziałań niekontrolowanego przepływu informacji jest stosowanie systemów zapewnienia bezpieczeństwa informacji. Informatyczne systemy bezpieczeństwa dla przedsiębiorstw są opracowywane według obowiązującej normy ISO 27001 [2]. W opracowanym systemie bezpieczeństwa przewidziane są między innymi procedury postępowania w przypadku naruszenia bezpieczeństwa informacji przedsiębiorstwa. Pozwala to na zapewnie, że informacje będące własnością przedsiębiorstwa nie przedostaną się do nieuczciwej konkurencji. Ważnym elementem poprawnego działania systemu opartego na bezpiecznym przepływie informacji jest prowadzenie szkoleń pracowników, którzy będą znać zasady postępowania w sytuacjach naruszenia bezpieczeństwa oraz zapoznają się ze sposobami przeciwdziałania takim sytuacjom.

Słowa kluczowe: informacja, bezpieczeństwo, ryzyko.

Cele i zasady zarządzania bezpieczeństwem informacji w przedsiębiorstwach

W obecnych czasach informacja będąca zasobem wiedzy przedsiębiorstw ma decydujący wpływ na jego bieżącą działalność i dalszy rozwój. Podstawowym założeniem zarządzania bezpieczeństwem informacji jest ochrona gromadzonej i przetwarzanej informacji. Dlatego powinna być chroniona zarówno przez kierownictwo, jak i pozostałych pracowników firmy. Niejednokrotnie firmy będące konkurencją dla przedsiębiorstwa proponują jej pracownikom zatrudnienie u siebie na znacznie korzystniejszych warunkach. Ma to często na celu pozyskanie informacji związanych z technologią czy też informacji o klientach konkurenta. Z tego względu w ostatnich latach obserwuje się ciągły wzrost

zainteresowania przedsiębiorstw coraz nowszymi udoskonalonymi systemami zarządzania bezpieczeństwem informacji.

Bezpieczeństwo informacji jest to zachowanie poufności, integralności i dostępności informacji. Poufność informacji jest zapewnieniem, że dostęp do informacji mają tylko osoby upoważnione. Pod pojęciem integralności informacji należy rozumieć zapewnienie dokładności i kompletności informacji oraz metod ich przetwarzania [2].

Celem działań związanych z zarządzaniem bezpieczeństwem informacji jest zachowanie poufności informacji chronionych, zapewnienie integralność informacji chronionych i jawnych oraz dostępność do nich, zapewnienie oczekiwanego poziomu bezpieczeństwa przetwarzanych informacji, ograniczenie do minimum występowania zagrożeń dla bezpieczeństwa informacji, gwarancja poprawnego i bezpiecznego funkcjonowanie systemów przetwarzania informacji, zapewnienie gotowości do podejmowania działań kryzysowych.

Polityka Bezpieczeństwa Informacji jest zbiorem dokumentów określających metody i zasady ochrony bezpieczeństwa informacji w przedsiębiorstwie [1].

Bezpieczeństwo informacji w przedsiębiorstwie w oparciu o normę ISO 27001

Informacja w obecnych czasach staje się coraz cenniejszym towarem. Posiadanie jak największych zasobów informacji pozawala zarówno na usprawnienie systemu zarządzania przedsiębiorstwem, jak i uzyskanie przewagi konkurencyjnej na rynku. Do zasobów informacji niezbędnych do prowadzenia opłacalnej działalności przedsiębiorstwa należą między innymi: dane, fakty i statystyki niezbędne do podejmowania konkretnych decyzji. Współczesna świadomość odnośnie do wartości informacji wymaga opracowania systemów bezpieczeństwa, które pozwolą na jej chronienie, gromadzenie i kontrolowane wykorzystanie. Należy jednak podkreślić, że systemy zarządzania bezpieczeństwem informacji ze względu na coraz bardziej złożoną postać stają się coraz droższe. Nie mniej jednak można powiedzieć, że przedsiębiorstwa są niemal zmuszone do ich stosowania, gdyż bez systemów zarządzania bezpieczeństwem informacji przedsiębiorstwo z góry jest skazane na niepowodzenie.

W Polsce stosowanie systemów zarządzania bezpieczeństwem informacji znalazło miejsce stosunkowo niedawno w odniesieniu do państw rozwiniętych. W dalszym ciągu spotyka się przedsiębiorstwa, w których jest ono jeszcze niewłaściwie zinterpretowane. W rezultacie prowadzi to do podejmowania błędnych decyzji przez personel zarządzający przedsiębiorstwem. Dla przykładu w momencie wprowadzenia w życie ustawy o ochronie danych osobowych, w wielu przedsiębiorstwach postrzegano ją, jako zbędne prawo,które często utrudnia pracę. Obecnie, gdy w wielu przypadkach dochodzi do sprzedawania

i wykorzystywania danych osobowych zarówno przez legalnie działające firmy, jak i przez organizacje przestępcze, problem poufności danych osobowych jest w pełni uzasadniony i wręcz niezbędny. System Zarządzania Bezpieczeństwem Informacji (SZBI), z ang. ISMS (Information Security Management System) jest opracowany zgodnie z obowiązującymi normami ISO/IEC 27000:2005 [2]. Odnosi się on do wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji.

Głównym zadaniem stawianym systemom zarządzania bezpieczeństwem informacji jest ochrona [2]:

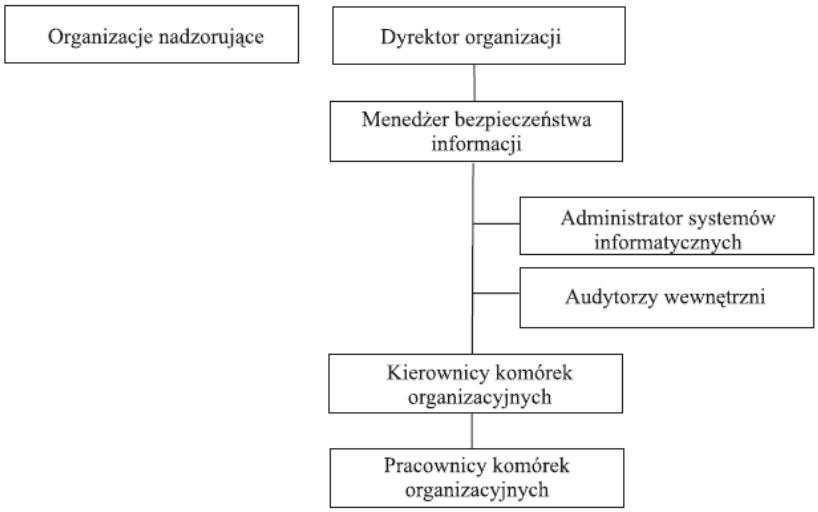
- danych o realizowanych kontraktach,
- danych finansowych przedsiębiorstwa,
- danych dostępowych do systemów IT,
- danych osobowych w oparciu o obowiązujące przepisy,
- danych dotyczących rozeznania rynku o ewentualnych zagrożeniach ze stron przedsiębiorstw konkurencyjnych dla firmy.

Kolejnym ważnym dla prawidłowego działania systemu zarządzania bezpieczeństwem informacji w przedsiębiorstwie jest przypisanie odpowiednim osobom uprawnień do korzystania z danych w nim zgromadzonych. I tak na przykład osobie pracującej na danym stanowisku przypisuje się uprawnienia, jakie są wymagane i niezbędne do realizacji jej obowiązków. A na przykład uprawnienia administracyjne przypisuje się kadrze zarządzającej przedsiębiorstwem. Podmiotami, które czynnie uczestniczą w systemie zarządzania bezpieczeństwem informacji, są głównie [3]: dyrektor organizacji, menedżer bezpieczeństwa informacji, administrator systemów informatycznych wraz z informatykami, audytorzy wewnętrzni, kierownicy komórek organizacyjnych oraz pracownicy.

Następnym problemem prawidłowego działania systemu bezpieczeństwa informacji jest ochrona przed wirusami. W tym celu stosuje się równolegle wiele technik na przykład [3]: oprogramowanie antywirusowe, systemy typu firewall, odpowiednią konfigurację systemu aktualizacji Windows.

W celu dotrzymania poufności informacji należy także określić zasady odpowiedzialności pracowników za utrzymanie w tajemnicy danych poufnych, do których dostęp został im powierzony. Poza tym właściwym podejściem jest przypisanie pracownikom kont i haseł dostępowych do informacji niezbędnych do wykonywania pracy. Podejście takie pozwala na monitorowanie, kto i kiedy miał dostęp do konkretnych informacji.

Na rysunku 1 przedstawiono przykładową strukturę zarządzania systemami bezpieczeństwa informacji [3].



Rys. 1. Przykładowy schemat struktur systemu zarządzania bezpieczeństwem informacji [3]

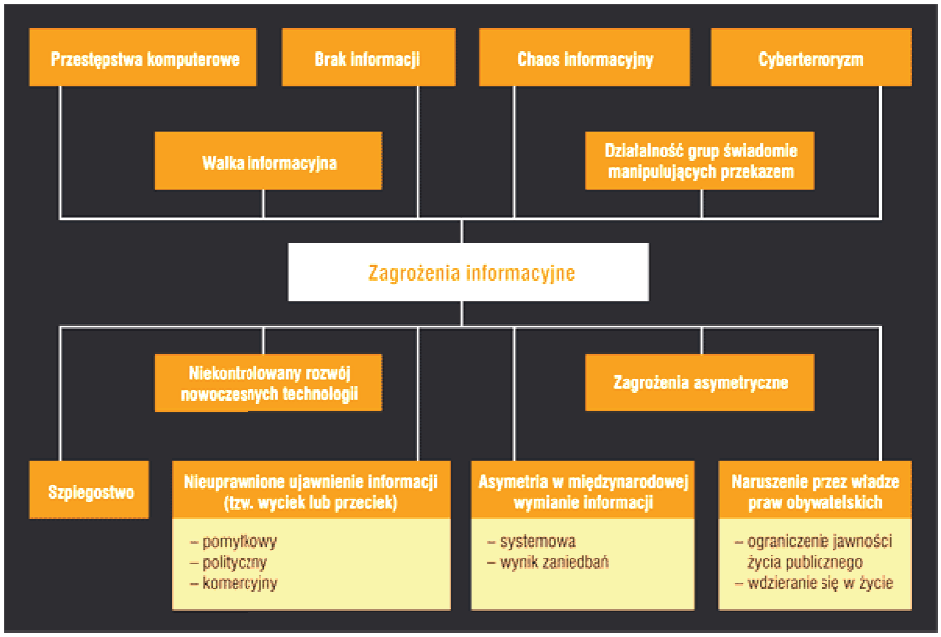
Wdrożenie systemu zarządzania bezpieczeństwem informacji jest procesem złożonym i trudnym. Przy jego wprowadzaniu należy korzystać z pomocy wysoko wykwalifikowanej kadry w zakresie informatycznym, dobrze znającej wymagania stawiane przez normę ISO 27001. Pomimo trudności wynikających z wdrażania systemu zarządzania bezpieczeństwem informacji, świadomość wagi informacji sprawiła, że niemal każde przedsiębiorstwo posiada lub jest zainteresowane wprowadzeniem takiego systemu.

Należy podkreślić, że wprowadzenie systemu zarządzania bezpieczeństwem informacji napotyka głównie problemy podczas jego wdrażania. Natomiast korzyści dla przedsiębiorstwa wynikające z jego wdrożenia to między innymi [2]:

- możliwość opracowania i usystematyzowanie wytycznych oraz dokumentacji w zakresie wymagań prawnych dotyczących bezpieczeństwa informacji,
- redukcja kosztów związanych z incydentami lub brakiem zgodności z wymogami prawnymi,
- spełnienie wymagań przepisów dotyczących bezpieczeństwa informacji,
- opracowanie zasad bezpieczeństwa informacji z rzeczywistymi potrzebami biznesowymi przedsiębiorstwa,
- określenie zadań, uprawnień i odpowiedzialności pracowników oraz menedżerów w zakresie bezpieczeństwa informacji,
- udoskonalenie systemu komunikacji w przedsiębiorstwie,
- wzrost wiarygodności organizacji jako zaufanego partnera biznesowego,
- zwiększenie bezpieczeństwa informacji klientów.

Zagrożenia dla systemów zarządzania bezpieczeństwem informacji

Działalność przedsiębiorstw krajowych i zagranicznych skupia się głównie na rozwoju i dążeniu do opracowania bądź pozyskiwania nowych innowacyjnych rozwiązań. W wyniku tych działań stają przed nowymi wyzwaniami i nowymi zagrożeniami, których niestety wciąż przybywa. Na rysunku 2 przedstawiono niektóre z zagrożeń informacyjnych dla przedsiębiorstwa.



Rys. 2. Podział zagrożeń informacyjnych [4]

Zagrożenia dla systemów zarządzania bezpieczeństwem informacji można również rozpatrywać pod kątem lokalizacji ich źródła. Wówczas można dokonać podziału na zagrożenia [4]:

– wewnętrzne, które powstają na terenie przedsiębiorstwa i obejmują:
  - utratę informacji wynikającą z uszkodzenia danych lub brakiem możliwości obsługi z powodu błędu lub przypadku,
  - utratę informacji wynikającą z uszkodzenia danych w wyniku celowego działania nieuczciwych użytkowników;

- zewnętrzne, które powstają poza terenem przedsiębiorstwa i obejmują zagrożenie związane z utratą bądź uszkodzeniem danych przez celowe lub przypadkowe działanie osób trzecich;
- fizyczne, w których zagrożenie utraty bądź uszkodzenia danych następuje z powodu wypadku, awarii, katastrofy lub innego nieprzewidzianego zdarzenia.

Podsumowanie

Przedsiębiorstwo poprzez wdrożenie systemu zarządzania bezpieczeństwem informacji staje się właścicielem narzędzia zapewniającego systemowe i kompleksowe podejście do bezpieczeństwa informacji. Niestety, ze względu na ciągłe dążenie do doskonalenia działalności przez przedsiębiorstwa konieczne są coraz częstsze modyfikacje systemu zarządzania bezpieczeństwem informacji (z uwagi na przyrastającą liczbę czynników mogących wpłynąć na jego skuteczność). Niezbędnym zatem staje się zatrudnianie wysoko wykwalifikowanej kadry posiadającej umiejętności zarówno w zakresie informatycznym, jak i dobrze znającej zasady wdrażania systemów zarządzania bazujących na normach ISO. Wymagania dla systemu zarządzania bezpieczeństwem informacji zostały określone w normie ISO 27001, która jest powszechnie stosowana w wielu krajach zarówno w Europie jak i na świecie.

Zainteresowanie systemami bezpieczeństwa informacji zarówno w kraju i za granicą wciąż rośnie. Można stwierdzić, że bez systemu zarządzania bezpieczeństwem informacji przedsiębiorstwo narażone jest na niepowodzenie.

Należy podkreślić, że wdrażane systemy zarządzania bezpieczeństwem informacji powinny posiadać możliwość szybkiej modyfikacji struktury, co pozwoli na swobodne zmiany w strukturach, jak i działalności przedsiębiorstwa.

Literatura

[1] pl.wikipedia.org/wiki/Polityka_bezpieczeństwa_informacji.
[2] http://www.iso.org.pl/iso-27001.
[3] Wawak S.: Podejście procesowe we wdrażaniu systemów zarządzania bezpieczeństwem informacji, Podejście procesowe w organizacjach, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, s. 127–135, 2009.
[4] Bączek P.: Zagrożenia informacyjne a bezpieczeństwo państwa polskiego, Wydawnictwo Adam Marszałek, Toruń 2006, s. 30.

Dariusz Rydz, Marlena Krakowiak, Teresa Bajor
Politechnika Częstochowska

PROVIDING INFORMATION SECURITY IN ENTERPRISES

Abstract

In present years companies providing are for many danger from site of uncontrolled competition. One of the most important reactions for uncontrolled flow information is application of providing information security systems. Information security systems for companies are made according to ISO 27001 [2]. In made security system among others are dealing procedures in case of interrupting the information security in the company. It allows ensuring will not be transferred to the unfair concurrent. Important element in correct working of the system based on safe information transfer is providing trainings for workers who will know the rules of what to do in situations of safety.

Keywords: information, security, risk.