Estera PIETRAS

ZAGADNIENIA ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W ORGANIZACJI

Słowa kluczowe:
ISO 27001, bezpieczeństwo informacji

1. Wstęp

W XXI wieku podstawą egzystencji stały się organizacje oparte na informacji, jednocześnie przyśpieszeniu uległ proces tworzenia społeczeństwa informacyjnego. Informacja stała się najbardziej pożądanym dobrem, zasobem o znaczeniu strategicznym.
Rosnąca wartość informacji powoduje znaczny wzrost zagrożeń dla instytucji rządowych, komercyjnych, stąd niezwykłej wagi problemem stała się ochrona systemów informacyjnych i przetwarzanie danych.
Organizacja systemu przepływu danych oraz wykorzystanie informacji w bieżącej i strategicznej działalności organizacji jest obecnie jednym z podstawowych problemów zarządzania, który w miarę dokonującego się postępu technologicznego uległ znacznej poprawie.
W dobie budowania społeczności informacyjnej, komunikowanie się za pomocą środków przekazu musi odbywać się w sposób natychmiastowy. Współczesna organizacja jest zobligowana do dbania o swoje informacje, gdyż one są jednym z czynników stanowiących przewagę nad innymi podmiotami. Bezpieczeństwo informacji jest nie tylko normą, lecz koniecznością i obowiązkiem [2].
Z pomocą dla organizacji świadomych znaczącej roli bezpieczeństwa i ochrony informacji w procesach realizacji misji i celów, obsługi klienta, przychodzi międzynarodowy standard ISO/IEC 27001:2014, stanowiący zbiór zaleceń, wymagań oraz dobrych praktyk, których zaimplementowanie do systemu bezpieczeństwa informacji gwarantuje jego niezawodność dla klientów, dostawców i osób trzecich. Nietrudno dostrzec, że dużą zaletą tej normy jest kompleksowe podejście do bezpieczeństwa informacji. Niniejsza norma międzynarodowa obejmuje również wymagania dotyczące szacowania i postępowania z ryzykiem dotyczącym bezpieczeństwa informacji, dostosowanych do potrzeb organizacji. Określone w niej wymogi są ogólne i mają zastosowanie do wszystkich organizacji, niezależnie od typu, wielkości i charakteru. Wyniki analizy certyfikacji ISO/IEC 27001 w sektorze przemysłu wskazują, że jest jeszcze wiele do zrobienia w tym obszarze. Podstawą takiego twierdzenia jest fakt, że 80% informacji różnego typu jest wykradana przez pracowników firmy.
Celem niniejszego artykułu jest zwrócenie uwagi czytelnika na pomysł systemu zarządzania bezpieczeństwem informacji opartego na identyfikacji zagrożeń oraz analizie ryzyka, ukierunkowanego na ustanawianie, wdrażanie, eksploatację, monitorowanie, utrzymanie i doskonalenie bezpieczeństwa informacji, poddawanego certyfikacji przez akredytowaną jednostkę certyfikującą. Ponadto w opracowaniu dokonano przeglądu rejestru certyfikatów ISO/IEC 27001:2014 przyznawanych organizacjom w Polsce, ze szczególnym uwzględnieniem przedsiębiorstw działających w sektorze przemysłu. Rozważania teoretyczne oparto o dane statystyczne dotyczące certyfikacji systemu ISO/IEC 27001. W artykule przedstawiono poszczególne etapy systemu ISMS.

2. Idea bezpieczeństwa informacji

W wyniku coraz większego uzależnienia od sieci, informacje są narażone na stale zwiększającą się liczbę i coraz większą różnorodność zagrożeń i podatności. Informacją jest każda wiadomość, powodująca jakąś reakcję i inicjująca określone działania, w samym systemie zarządzania lub jej otoczeniu. Niezależnie od tego, jaką formę przybiera lub za pomocą jakich środków jest udostępniana lub przechowywana, zaleca się, aby w odpowiedni sposób była chroniona. Poprzez bezpieczeństwo informacji rozumiemy ochronę przed szerokim spektrum zagrożeń w celu zapewnienia ciągłości działania minimalizacji ryzyka i maksymalizacji zwrotu z inwestycji oraz możliwości biznesowych. Innymi słowy bezpieczeństwo informacji zapewnia odpowiedni poziom poufności, dostępności i integralności danych [6]. W niektórych przedsiębiorstwach można zaobserwować brak świadomości pracowników mogący doprowadzić do ujawnienia istotnych informacji. Przykładem tego mogą być źle przetworzone dane księgowe czy projektowe, zagubienia nośników danych (np. laptopy, pendrivy, płyty CD), karteczki z hasłami przyklejone do monitora, ekrany monitorów zwrócone w stronę klientów, dokumenty leżące na biurku, które mogą zostać zabrane przez osoby niepowołane. Utrata tych danych może spowodować znaczne straty finansowe i znacząco wpłynąć na wizerunek firmy, co może przesądzić o jej konkurencyjności. Będąc tego świadomym, przedsiębiorstwa, które nie chcą zostać wyeliminowane z rynku uwzględniają w swoich strategiach elementy bezpieczeństwa informacji.
Normy PN-ISO/IEC 27001:2007 oraz PN-ISO/17799:2007 definiują „bezpieczeństwo informacji", jako „zachowanie poufności, integralności i dostępności informacji". Dodatkowo brane są pod uwagę atrybuty bezpieczeństwa takie jak: autentyczność, rozliczalność, niezaprzeczalność, niezawodność [7] (tab. 1).
Zgodnie z prezentowanymi w piśmiennictwie treściami informację uznaje się za bezpieczną, wówczas gdy zagwarantowane są wszystkie atrybuty jej bezpieczeństwa: poufność, spójność, dostępność, rozliczalność, autentyczność, niezaprzeczalność i niezawodność [6, 8]. Wobec powyższego, bezpieczeństwo informacji należy rozmieć wielowymiarowo, uwzględniając nie tylko wielość atrybutów informacji, podlegających ochronie, ale także różnorodność

Charakterystyka poszczególnych atrybutów bezpieczeństwa		
Poufność – zapewnienie, że informacja nie jest udostępniana bądź ujawniana osobom podmiotom i procesom nieuprawnionym	Integralność danych – zapewnienie, że dane nie zostały zamienione sposób nieautoryzowany, zapewnieniu dokładności i kompletności aktywów, czyli wszystkiego, co ma wartość dla organizacji	Integralność systemu – zapewnienie, że system realizuje swoje funkcje w sposób nienaruszony
Integralność – zapewnienie integralności danych i systemu	Dostępność – zakłada możliwość autoryzowanego wykorzystania danych i informacji w pożądanym czasie, właściwość bycia dostępnym	Autentyczność – zapewnienie, że tożsamość podmiotu bądź zasobu jest zgodna zdeklarowaną (dotyczy to użytkowników procesów, systemów)
Rozliczalność – wiąże się z jednoznacznym przypisaniem określonego zakresu działań do jednemu podmiotowi	Niezawodność – oznacza stałe spójne zamierzone zachowania oraz skutki	

Tab. 1. Atrybuty bezpieczeństwa informacji [6]

form ich występowania (np. w postaci pliku danych, wydruku, zapisu w formie elektronicznej i tradycyjnej, rekordu w bazie danych czy wiadomości przekazywanej ustnie). Problematyka bezpieczeństwa informacji w dzisiejszym świecie dotyczy podmiotu, który jest zagrożony poprzez brak informacji lub możliwość utraty zasobów informacyjnych. Natomiast bezpieczeństwo informacji to ochrona informacji będącej w posiadaniu tego właśnie podmiotu.

3. Sprawowanie kontroli nad bezpieczeństwem informacji

Zapewnienie bezpieczeństwa informacji rozumiane jest jako redukcja ryzyka i eliminowanie zagrożeń poprzez ochronę i wdrożenie skutecznych mechanizmów w tym zakresie. Systemowe zarządzanie bezpieczeństwem informacji SZBI opiera się nie tylko na wprowadzeniu zabezpieczeń technologii teleinformatycznych, ale przede wszystkim na odpowiednim zarządzaniu organizacyjnym i technicznym. SZBI formułuje cele i wymagania w zakresie bezpieczeństwa osobowego, fizycznego, prawnego. Zarządzanie bezpieczeństwem informacji ZBI polega na identyfikowaniu aspektów bezpieczeństwa i wprowadzeniu procedur i przeprowadzeniu działań doskonalących.

Wzrost świadomości wagi informacji i jej bezpieczeństwa znajduje swoje odzwierciedlenie w dynamicznym rozwoju standardów międzynarodowych dla systemów zarządzania bezpieczeństwem informacji i rosnącym zainteresowaniu przedsiębiorców tą problematyką. Najnowsze normy ISO/IEC 27001:20014-12 mogą i powinny być doskonałą wskazówką dla budowania bezpiecznej organizacji (tab. 2).

Norma ISO 27001 oparta jest na podejściu procesowym i wykorzystuje model Planuj – Wykonuj – Sprawdzaj – Działaj, który jest stosowany dla całej struktury procesów SZBI. Norma składa się z części podstawowej oraz załączników. Część podstawowa normy zajmuje się wymaganiami związanymi z ustanowieniem i zarządzaniem SZBI, wymaganą dokumentacją, odpowiedzialnością kierownictwa, wewnętrznymi audytami SZBI, przeglądami SZBI oraz ciągłym doskonaleniem SZBI. Wszystkie wymagania zdefiniowane w części podstawowej winny być spełnione. Określenie metody oraz przeprowadzenie analizy ryzyka jest podstawą ustanowienia oraz utrzymania SZBI.

ISO/IEC 27001 jest międzynarodowym standardem dotyczącym zarządzania bezpieczeństwem informacji, opublikowanym w 2005 r. przez ISO (International Organization for Standardization) i Międzynarodowy Komitet Elektrotechniczny (International Electrotechnical Commission), opracowanym na podstawie wycofanej już brytyjskiej normy BS7799-2:2002. Istnieją również wydane przez Polski Komitet Normalizacyjny polskie odpowiedniki obu standardów – wycofana norma PN-ISO/IEC 27001:2007 oraz PN-I-07799:2005.

Organizacje, w których funkcjonują jeszcze systemy zarządzania bezpieczeństwem informacji zgodne z ISO/IEC 27001:2005 lub PN ISO/IEC 27001:2007 miały czas maksymalnie do 01.10.2015 na przejście na nową normę.

Spełnienie wymagań normy oznacza zastosowanie wszystkich ww. zabezpieczeń. Nietrudno dostrzec, że dużą zaletą tej normy jest kompleksowe podejście do bezpieczeństwa informacji. Norma ta zajmuje się obszarem związanym z bezpieczeństwem fizycznym, teleinformatycznym, prawnym, przy czym nie określa szczegółowych rozwiązań, lecz podpowiada, co należy zrobić, ale nie precyzuje, w jaki sposób [2]. Wdrożony standard podnosi wiarygodność organizacji w oczach inwestorów i udziałowców, zapewniając bezpieczeństwo interesom klienta w wyniku poprawnie funkcjonującego systemu zarządzania informacją. Jednocześnie świadomi zagrożeń pracownicy, zachowają odpowiedni poziom jakości ochrony aktywów informacyjnych. Wiąże się to z odpowiednim wyedukowaniem pracowników poprzez szkolenia i zaznajomienie ich z dokumentami związanymi z bezpieczeństwem informacji.

Wymagania ISO/IEC 27001 zostały pogrupowane na:

- System zarządzania bezpieczeństwem informacji,
- Odpowiedzialność kierownictwa,
- Wewnętrzne audyty jakości,
- Przeglądy SZBI realizowane przez kierownictwo,
- Doskonalenie systemu zarządzania bezpieczeństwem informacji.

Numer normy	PN-ISO/IEC 27001:2014-12 - wersja polska
Tytuł	Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania
Data publikacji	02-12-2014
Liczba stron	30
Grupa cenowa	XZ
Sektor	STI, Sektor Technik Informacyjnych i Komunikacji
Organ Techniczny	KT 182, Ochrony Informacji w Systemach Teleinformatycznych
Wprowadza	ISO/IEC 27001:2013 [IDT]
Zastępuje	PN-ISO/IEC 27001:2007/Ap1:2010 - wersja polska, PN-ISO/IEC 27001:2007 - wersja polska
ICS	35.040

Tab. 2. Informacje dodatkowe ISO/IEC 27001:2014-12 - wersja polska [6]

Norma ISO/IEC 27001 stanowi model ISMS, który może być zastosowany przez każdą organizację, niezależnie od jej działalności, wielkości, statusu prawnego. Pozwala ona na ustanowienie, wdrożenie, eksploatowanie, monitorowanie, przegląd i ciągłe doskonalenie systemu.

3.1. Zalety wdrożenia systemu SZBI

Wdrożenie SZBI zapewnia organizacji szereg korzyści, m.in. adekwatny do zagrożeń, wymagań biznesowych i wymagań wynikających z przepisów prawa poziom ochrony wszystkich informacji. Dobór zabezpieczeń na podstawie wyników analizy ryzyka zapewnia natomiast efektywność kosztową.
Istnieje zdecydowana przewaga korzyści, jakie daje SZBI, czego przykładem jest poniższa tabela 3. Przedstawia ona porównanie funkcjonowania przedsiębiorstwa przed i po wprowadzeniu systemu.

3.2. Planuj: Ustanawianie ISMS

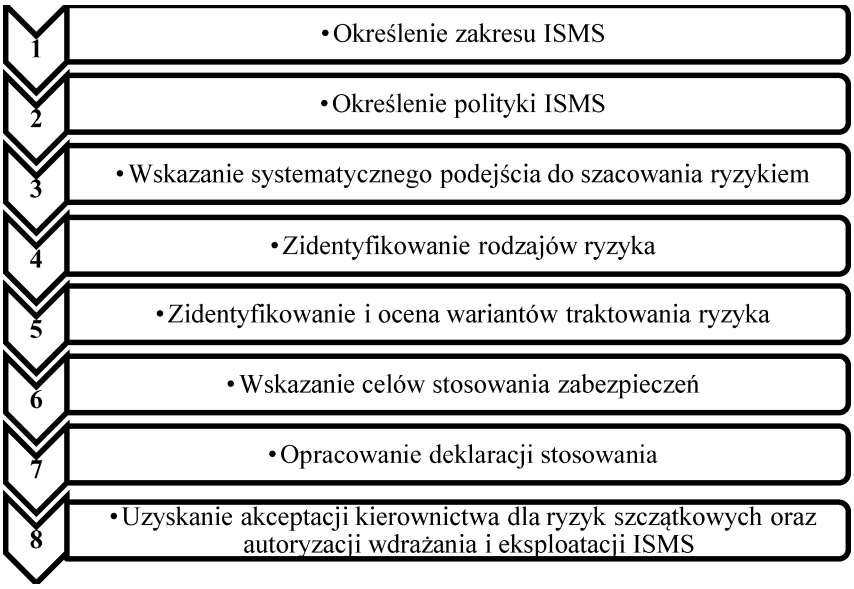
Podczas podjęcia decyzji o wdrożeniu ISMS konieczne jest uwzględnienie następujących po sobie procesów. Poszczególne jego etapy prezentuje rysunek 1.
Na dowolnym modelu każda organizacja może zaprojektować własny, indywidualny ISMS Jednak w przypadku wybrania ISO/IEC 27001 konieczne jest spełnienie wszystkich wymogów. Dopuszczalne są wyłączenia odnoszące się do zabezpieczeń. Konieczne jest ustanowienie granic systemu. Wiodącym dokumentem w ISMS jest polityka bezpieczeństwa i przy jej definiowaniu należy zapewnić charakterystykę prowadzonej działalności, aktywa i technologię.
Kolejnym etapem we wdrażaniu i ustanawianiu ISMS jest identyfikacja ryzyka, która polega na wskazaniu zasobów oraz przypisaniu do nich zagrożeń, podatności oraz skutków wystąpienia niebezpieczeństwa.
Norma definiuje również konieczność analizy i oceny ryzyka. Odbywa się to poprzez:
- wyznaczenie strat i szkód wynikających z naruszenia bezpieczeństwa informacji w organizacji,
- określenie realnego prawdopodobieństwa wystąpienia niekorzystnego zdarzenia,
- oszacowanie poziomu wyznaczonych rodzajów zagrożeń,
- ustalenie, czy ryzyko jest na poziomie akceptowalnym.

Kolejnym wymaganiem dyktowanym przez normę w zakresie ISMS jest identyfikacja oraz ocena wariantów traktowania ryzyka. Wyróżnia się następujące możliwości:
- wdrożenie stosownych zabezpieczeń,
- unikanie ryzyka,
- akceptowanie ryzyka,
- transfer ryzyka (np. na ubezpieczyciela).

Wszystkie zabezpieczenia, które trzeba bezwzględnie wdrożyć w ramach ISMS, określone zostały w załączniku A do normy – należy jednak mieć na uwadze, iż ich lista nie jest kompletna i w szczególnych przypadkach może zaistnieć konieczność zastosowania dodatkowych zabezpieczeń.

Brak wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji	Korzyści z wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji
Brak koordynacji polityki bezpieczeństwa pomiędzy różnymi jednostkami organizacyjnymi organizacji (departament IT, ochrona fizyczna, pion ochrony informacji niejawnych)	Standaryzacja bezpieczeństwa informacji w całej organizacji – stworzenie odpowiednich struktur nadzorczych
Koncentracja na zabezpieczeniach	Koncentracja na analizie ryzyka
Wydatki na bezpieczeństwo traktowane jako koszt działania	Wydatki na bezpieczeństwo traktowane jako inwestycja (możliwość wyznaczenia wskaźnika zwrotu z inwestycji)

Tab. 3. Porównanie funkcjonowania przedsiębiorstwa przed i po wprowadzeniu SZBI do przemysłu



Rys. 1. Etapy ustanawiania ISMS [4]

Zestawienie wszystkich zaimplementowanych zabezpieczeń wraz z uzasadnieniem ich wyboru należy określić w tzw. deklaracji stosowania ISMS [7].

3.3. Wykonuj: Wdrażanie i stosowanie ISMS

Proces wdrożenia i eksploatacji systemu obejmuje:

I. Przeprowadzenie szkoleń dla pracowników, zapoznanie ich z podstawowymi zasadami bezpieczeństwa informacji.
II. Wdrożenie planu postępowania z ryzykiem i dokumentacji systemowej.

Przeprowadzenie szkoleń uświadamiających pracownikom powody wdrożenia systemu, nałożenie na nich dodatkowych obowiązków ma duże znaczenie dla skuteczności stosowania przyjętych zasad. Sukces całego projektu będzie polegał na widocznym zaangażowaniu kierownictwa w dany projekt i poważne traktowanie przyjętych procedur. Zdarza się, że choć firma posiada wiedzę i środki do samodzielnego projektowania systemu, zatrudnia konsultantów z zewnętrznej firmy. Zwraca tym uwagę na istniejący problem.

Za przykłady działań związanych z wdrożeniem zabezpieczeń technicznych można uznać:

- zakup oprogramowania antywirusowego umożliwiającego zdalne zarządzanie na stacjach roboczych,
- zakup i wdrożenie monitoringu pomieszczeń,
- zakup oprogramowania do audytu legalności oprogramowania [10].

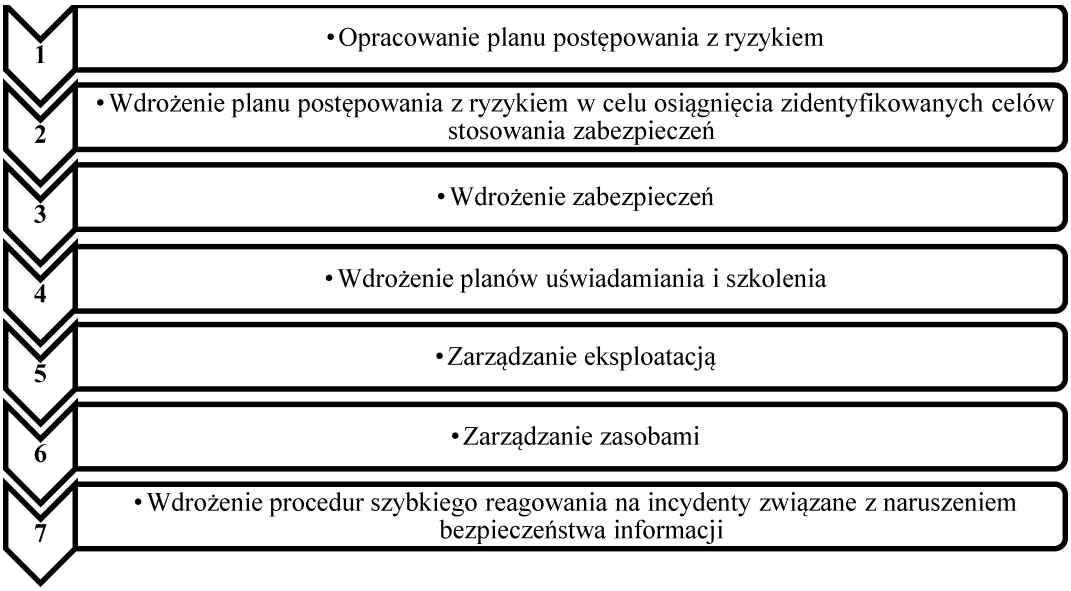
Wdrożenie i eksploatację można przedstawić w sposób graficzny, co pokazano na rysunku 2.

3.4. Sprawdź: Monitorowanie i przegląd ISMS

Działający system zarządzania bezpieczeństwem informacji powinien podlegać monitorowaniu i przeglądom, aby można było na bieżąco wykrywać błędy, naruszenia bezpieczeństwa oraz uzyskiwać informacje o skuteczności systemu.

Ponadto prawidłowe funkcjonowanie sytemu jest w znacznej mierze uzależnione od szkoleń, uświadamiania pracowników do postępowania zgodnego z przyjętymi zasadami stanowiącymi podstawę funkcjonowania systemu. Niezbędne jest ustawiczne weryfikowanie i przestrzeganie procedur, np. na drodze okresowych audytów wewnętrznych. W ramach systemu zarządzania bezpieczeństwem informacji konieczne jest:

- wykonywanie regularnych przeglądów efektywności ISMS przy uwzględnieniu wyników audytów bezpieczeństwa, rezultatów pomiarów efektywności,
- mierzenie efektywności zabezpieczeń w celu weryfikacji ich zgodności z wymaganiami bezpieczeństwa,
- dokonywanie przeglądu szacowania ryzyka w zaplanowanych odstępach czasu.



Rys. 2. Zasady wdrażania i eksploatacji ISMS oraz norma 2007 [5]

Wszystkie te wymagania zapewnią natychmiastowe wykrywanie błędów w wynikach przetwarzania i identyfikacji naruszeń bezpieczeństwa [10].

3.5. Działaj: Utrzymanie i doskonalenie ISMS

Procedury reagowania na błędy, incydenty oraz niezgodności wykryte na drodze przeglądów muszą skutkować podjęciem działań korygujących lub prewencyjnych. Procedury działań korygujących powinny również być udokumentowane. Poza działaniami korygującymi, w miarę możliwości powinny być również podjęte działania prewencyjne w celu ochrony przed powstaniem niezgodności w przyszłości. Przykładowo: jeśli coroczny audyt wewnętrzny wykazał dużo niezgodności, to należy rozważyć częstsze przeglądy bezpieczeństwa.

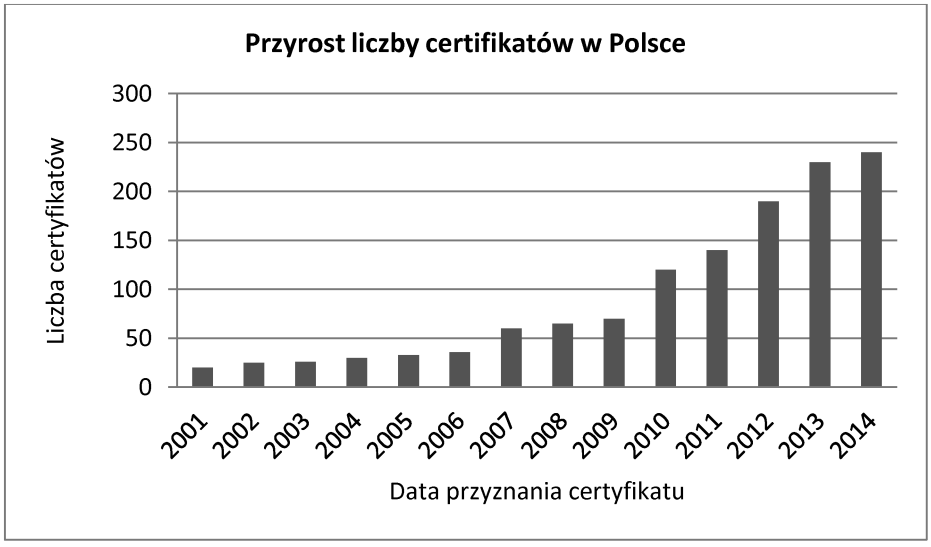
4. Działalność w przemyśle w oparciu o system bezpieczeństwa informacji ISO/IEC 27001:2014-12

Coraz więcej organizacji w Polsce dostrzega konieczność ochrony posiadanych informacji. Osiągnięcie i utrzymanie właściwego poziomu bezpieczeństwa w czasach, w których nowe zagrożenia pojawiają się praktycznie każdego dnia, nie jest zadaniem łatwym. Dochodzi także do zdarzeń nagłych awarii, które utrudniają lub wręcz uniemożliwiają funkcjonowanie procesów biznesowych. Najodpowiedniejszym podejściem jest więc wdrożenie adekwatnego i efektywnego systemu zarządzania opartego o sprawdzone, międzynarodowe normy ISO/IEC 27001 w zakresie bezpieczeństwa przetwarzanych informacji oraz zapewnienia ciągłości działania organizacji zgodnie z wytycznymi. Nie należy przy tym zapominać o niezwykle ważnym walorze biznesowym – normy ISO są uznawane i rozpowszechniane na całym świecie, więc ich dostępność w bezpośredni sposób wiąże się z podniesieniem prestiżu i pozycji organizacji, która w profesjonalny sposób zarządza bezpieczeństwem. Pozytywna ocena niezależnej jednostki, przyznającej certyfikaty, pozwoli jej znaleźć się o kilka kroków przed konkurencją, która tego, nadal unikalnego w naszym kraju, certyfikatu nie posiada. Jednostki, którym przyznano certyfikat zgodności z normą ISO/IEC 27001, mogą „reklamować się" jako organizacje przywiązujące najwyższą wagę do wartości bezpieczeństwa informacji poprzez wdrożenie niezbędnych środków ostrożności przeciwdziałających takim zagrożeniom jak: nieuprawniony dostęp czy nieautoryzowana modyfikacja.

Poniżej (rys. 3) zamieszczono podstawowe statystyki, prezentujące rozwój i obecny kształt rynku ISO/IEC 27001, ISO/IEC 20000, ISO 22301 i BS 25999 w Polsce. Wykresy są generowane według aktualnie dostępnych danych i odzwierciedlają wszystkie zmiany wprowadzone do rejestru.

Niezwykle istotną kwestią jest zapewnienie właściwego poziomu bezpieczeństwa informacji w przemyśle. Fundamentem nowoczesnego zarządzania w firmie przemysłowej jest przetwarzanie informacji, magazynowanie jej i wysyłanie dalej. Informacja stanowi źródło ciągłości działania w firmie przemysłowej. Nie wszystkie podmioty przemysłowe jednak chcą chronić w sposób należyty tę informację. Rysunek 4. obrazuje skalę rejestru certyfikatów ISO/IEC 27001 przyznanych firmom w Polsce, z podziałem według branż.

Z zebranych danych wynika, iż w Polsce jednie 9% przedsiębiorstw działających w sektorze przemysłu posiada świadectwo doskonale zorganizowanego systemu zarządzania bezpieczeństwem informacji, zgodnego z międzynarodowym standardem ISO/IEC 27001. Największy odsetek przedsiębiorstw wdrażających ISMS zgodny z ISO/IEC 27001 przypada branżom zdefiniowanym jako pozostałe usługi (53%) oraz integratorzy IT. Fakt ten może dowodzić, iż w polskiej gospodarce nadal panuje przekonanie, że bezpieczeństwo informacji to domena głównie informatyki. Należy jednak mieć nadzieję, iż w niedalekiej przyszłość świadomość organizacji w Polsce w zakresie konieczności kształtowania bezpiecznych warunków gromadzenia, przetwarzania oraz przepływu informacji będzie wzrastać, co będzie przekładać się również na liczbę posiadanych certyfikatów ISO/IEC 27001 przez przedsiębiorstwa i instytucje reprezentujące różne gałęzie gospodarki, w tym przemysł [12].



Rys. 3. Przyrost liczby certyfikatów w Polsce w latach 2001-2014 [12]

Rys. 4. ISO/IEC 27001 przyznawanych organizacjom w Polsce, z podziałem według branż [12]

Z tabeli 2 wynika, że AGI Media Warszawa Sp. z o.o. była pierwszą firmą na polskim rynku zajmującą się przemysłem, która zdecydowała się na certyfikację systemu zarządzania bezpieczeństwem informacji, zgodnego z ISO/IEC 27001. Jak możemy przeczytać na stronie internetowej Spółki zapewnienie bezpieczeństwa w całym łańcuchu świadczonych usług jest jednym z jej priorytetów. Spółka szczególną troskę przywiązuje do dbałości o poufność informacji, odpowiednie zabezpieczenie danych swoich klientów przed niekontrolowanym wyciekiem oraz dobry poziom komunikacji na linii firma-klient [11].

5. Podsumowanie

Każda organizacja chciałaby dysponować jednym z najważniejszych zasobów, jakim jest informacja. O ile są informacje mniej istotne, o mniejszym znaczeniu dla samej organizacji, o tyle są również informacje o znaczeniu wręcz strategicznym, które wymagają stosownej ochrony. Dlatego jednym z podstawowych zadań i wyzwań, przed jakimi stoi każda organizacja, jest ochrona informacji. Bezpieczeństwo informacji jest procesem ciągłym, w ramach którego organizacje starają się udoskonalić mechanizmy zapewniające im poczucie bezpieczeństwa. Odzwierciedlenie rozumienia i traktowania bezpieczeństwa informacji jako kluczowego obszaru zainteresowań organizacji można znaleźć w ich działaniach podejmowanych w obliczu zagrożenia. Procedury związane z ochroną i bezpieczeństwem przetwarzania informacji niewątpliwie wysoko cenią klienci w sektorze przemysłu [2]. Znane powiedzenie mówi, że czas to pieniądz. Może dobrze by było je zmodyfikować na czas i informacja to pieniądz. Informacja o sposobach działania firmy, o kontaktach handlowych, o stosowanych technologiach i wielu innych sprawach stanowi o konkurencyjności danej firmy na rynku. Większość działań zmierzających do zapewnienia bezpieczeństwa skupia się jedynie na ochronie budynku albo pieniędzy w kasie. Takie inicjatywy są potrzebne, ale niestety nie są wystarczające. Z niniejszego artykułu wynika, że liczba certyfikacji systemu zarządzania bezpieczeństwem informacji zgodnych z normą ISO/IEC 27001:2014-12 przyznawanych organizacjom przemysłowym w Polsce jest niewielka. Nie świadczy to jednak o tym, iż organizacje nie wykorzystują rozwiązań w niej zawartych jako wzorca do budowania własnego systemu bezpieczeństwa informacji. Opór organizacji przed procesem certyfikacji często wynika z jego złożoności i trudności w zastosowaniu [9].

Literatura:

[1] Barczak A., Sidoruk T., *Bezpieczeństwo systemów informatycznych zarządzania*. Dom Wydawniczy Bellona, Warszawa 2003.
[2] Jańczak J., Nowak A., *Bezpieczeństwo informacyjne Wybrane problemy*. Akademia Obrony Narodowej, Warszawa 2012.

Lp.	Organizacja	Data cert.	Standard
1.	AGI Media Warszawa Sp. z o.o.	2008-08-01	ISO/IEC 27001
2.	Elektromontaż Poznań S.A.	2009-03-09	ISO/IEC 27001
3.	Elektrotim S.A.	2009-04-10	ISO/IEC 27001
4.	Fujitsu Technology Solutions Sp. z o.o.	2011-05-05	ISO/IEC 27001
5.	GAZOPROJEKT S.A.	2010-01-19	ISO/IEC 27001
6.	KOKSOWNIA PRZYJAŹŃ Sp. z o.o.	2012-10-15	ISO/IEC 27001
7.	Megachemie Sp. z o. o.	2011-04-18	ISO/IEC 27001
8.	TINES S.A.	2011-04-18	ISO/IEC 27001
9.	Wojskowe Zakłady Mechaniczne S.A.	2009-12-08	ISO/IEC 27001

Tab. 2. Zestawienie certyfikowanych przedsiębiorstw z branży przemysłowej

[3] Kifner T., *Polityka bezpieczeństwa i ochrony informacji*. Wydawnictwo Helion, 1999.
[4] Łuczak J., Tyburski M., *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*. Wyd. Uniwersytetu Ekonomicznego w Poznaniu, Poznań 2010.
[5] Molski M., Łacheta M., *Przewodnik audytora systemów informatycznych*. Wydawnictwo Helion, Gliwice 2007.
[6] Nowak A., Scheffs W., *Zarządzanie bezpieczeństwem informacyjnym*. Wydawnictwo AON, Warszawa 2010.
[7] PN-ISO/IEC 27001:2007, *Technika informatyczna – Technika bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji, Wymagania*. PKN, Warszawa 2007.
[8] Prauzner T., *Technologia informacyjna – wybrane problemy społeczne*, [w:] *Wybrane problemy edukacji informatycznej i informacyjnej*, red. W. Walat. „Edukacja – Technika – Informatyka", Rocznik Naukowy Nr 3/2012, cz. 2. Wyd. FOSZE, Rzeszów 2012, s. 39-45.
[9] 12. Wołowski F., Zawiła-Niedzwiecki J., *Bezpieczeństwo systemów informacyjnych Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi*. Wydawnictwo edu-Libri s.c., Kraków 2012.
[10] *Wybrane problemy zarządzania bezpieczeństwem informacji*, red. J. Brdulak, P. Sobczak. Oficyna Wydawnicza Szkoły Głównej Handlowej, Warszawa 2014.
[11] www.asg-worldwide.com, PN-ISO/IEC 27001:2014-12 – wersja polska (dostęp 04.05.2016).
[12] www.iso27000.pl (dostęp 04.05.2016).

ISSUES OF INFORMATION SECURITY MANAGEMENT IN AN ORGANIZATION

Key words:
ISO 27001, security of information

Abstract:
One of the basic human needs, the primary and essential is a sense of security. It plays a special role in the life of the individual and social group for example in the family. This wouldn't possible without certain information by which you can get significant knowledge about the impact of security for human life. Many scientists claim that the information is the basis of community particularly those in the workplace, which organized it's protection by all possible means, protecting the company against unauthorized disclosure. A special role in this case played by the company management actually managing information security.
The results of the analysis of the certification ISO/IEC 27001 in the industrial sector shows that there is still much to be done in this area. The basis for such a claim is that 80% of information of various types is stolen by employees.
Theoretical considerations based on statistical data for the certification of ISO / IEC 27001. This article presents the different stages of ISMS system.
The purpose of this article is to alert the reader to the idea of information security management system based on identification of threats and risk analysis, directed on the establishment, implementation, operation, monitoring, maintenance and improving information security, subjected to certification by an accredited certification unit.

Mgr inż. Estera PIETRAS
Instytut Przeróbki Plastycznej i Inżynierii Bezpieczeństwa
Wydział Inżynierii Produkcji i Technologii Materiałów
Politechnika Częstochowska
estera.pietras@wp.pl