

Istota zarządzania bezpieczeństwem informacji

W dzisiejszych czasach strategię działania przedsiębiorstwa na rynku wyznaczają zasoby informacyjne. To informacja i umiejętność jej pozyskania stają się kluczowymi czynnikami, które warunkują sukces w prowadzeniu biznesu, a także utrzymaniu konkurencyjności. Informacja jest częścią majątku firmy, tak samo jak np. środki trwałe i chociażby tylko z tego powodu powinna być odpowiednio chroniona przed zagrożeniami. Wydostanie się na zewnątrz informacji dotyczących stosowanych w przedsiębiorstwie technologii, dystrybucji produktów, sposobów zarządzania personelem czy też informacji o strategicznych klientach może skutkować tym, że firma stanie się „przejrzysta i przezroczysta” dla konkurentów. Aby temu zapobiec powstała nowa dziedzina nauki – zarządzanie bezpieczeństwem informacji, rozwiązująca problemy związane z zapewnieniem i utrzymaniem odpowiedniego poziomu bezpieczeństwa dla instytucji.

System zarządzania bezpieczeństwem informacji to systematyczne podejście do zarządzania kluczowymi informacjami firmy w celu zapewnienia ich bezpieczeństwa. Obejmuje on ludzi, procesy, infrastrukturę i systemy informatyczne. System zarządzania bezpieczeństwem informacji może być wdrożony w organizacjach różnego typu, niezależnie od wielkości i charakteru działalności. Opiera się na podejściu procesowym (tak jak system zarządzania jakością czy środowiskiem) i może być integrowany z innymi systemami zarządzania.

Wszystkie aspekty związane z definiowaniem, osiąganiem i utrzymywaniem poufności, integralności i dostępności zawierają normy PN-ISO/IEC 17799 i PN-I-07799. Normy stosuje się w odniesieniu do systemu zarządzania bezpieczeństwem informacji (funkcjonuje tu skrót angielski: ISMS - Information Security Management System). PN-ISO/IEC 17799 i PN-I-07799 zostały stworzone tak, aby umożliwić instytucji dopasowanie lub zintegrowanie swojego systemu zarządzania bezpieczeństwem informacji z wymaganiami powiązanych systemów zarządzania. Normy opierają się na modelu zarządzania tzw. model koła Deminga: „Planuj – Wykonaj – Sprawdź - Działaj” (PDCA) jako część podejścia do tworzenia, wdrażania i zwiększania efektywności systemu zarządzania bezpieczeństwem informacji w instytucji.

Wymagania normy dotyczą ustanawiania, wdrażania, eksploatacji, monitorowania, przeglądu, utrzymywania i doskonalenia udokumentowanego systemu zarządzania bezpieczeństwem informacji w całościowym kontekście ryzyk biznesowych. Zapisy normy dotyczą informacji „papierowej”, informacji przechowywanej w systemach informatycznych oraz wiedzy poszczególnych pracowników. Zakres stosowania normy przedsiębiorstwo ustala sobie samo. Organizacje mogą chronić np.: różnego rodzaju nośniki informacji, systemy przetwarzania (system księgowy), ewidencję wartości niematerialnych i prawnych, aplikacje informatyczne, bazy danych czy też dane osobowe.

Normy zawierają opis zabezpieczeń, które należy stosować w celu ograniczenia ryzyka utraty informacji. PN-ISO/IEC 17799 i PN-I-07799 są kompleksowe i obejmują wszystkie aspekty bezpieczeństwa informacji, zwracając uwagę na sprawy najistotniejsze, a mianowicie: ważne jest posiadanie ważnej zapory sieciowej (sprawnego firewalla), zabezpieczenie fizycznego dostępu do niej, istnienie procedur regulujących sposób tworzenia reguł na tej zaporze, procedury kontroli jej skuteczności oraz wyznaczenie osób odpowiedzialnych za ten element systemu zabezpieczenia.

Przedsiębiorstwa mogą liczyć na szereg korzyści, jeżeli zdecydują się zastosować metodologię zarządzania bezpieczeństwem informacji zgodną z normami PN-ISO/IEC 17799 i PN-I-07799, np.:

- bezpieczeństwo wszystkich informacji korporacyjnych (zwiększenie wartości firmy),
- realizacja celów przedsiębiorstwa poprzez eliminowanie zagrożeń,
- uporządkowanie przetwarzanych informacji,
- wiarygodność firmy na rynku poprzez zapewnienie klientom, że ich informacja znajduje się pod właściwą ochroną,
- jasne określenie uprawnień i odpowiedzialności pracowników,
- zgodność z wymaganiami prawnymi (ustawą o ochronie danych osobowych, ustawą o dostępie do informacji publicznych, ustawą o ochronie informacji niejawnych, ustawą o prawie autorskim i prawach pokrewnych), a co się z tym wiąże uniknięcie kar za naruszenie bezpieczeństwa informacji,
- zabezpieczenie informacji na wypadek awarii czy katastrofy,
- pełna integracja z systemem zarządzania jakością i systemem informatycznym w przedsiębiorstwie.

Stale rośnie liczba uzyskiwanych certyfikatów potwierdzających zgodność systemu zarządzania bezpieczeństwem informacji z

PN-ISO/IEC 17799 i PN-I-07799. Coraz więcej przedsiębiorców zauważa, że wdrożenie wytycznych normy daje możliwość zmniejszenia do minimum ryzyka utraty, zatajenia czy też zafałszowania informacji.