



Bezpieczeństwo informacji

Czy chronisz istotne aktywa twojej firmy?

Normy dotyczące bezpieczeństwa informacji to nowoczesne standardy zachowania poufności, integralności i dostępności informacji.



MANAGING RISK

DNV



Bezpieczeństwo informacji

W dzisiejszych czasach informacja to majątek firmy, który jest równie ważny jak inne składniki kapitału przedsiębiorstwa, a zatem wymaga odpowiedniej ochrony. Przecieki informacji, np. do mediów lub konkurencji, stały się powszechnym problemem. Występują one zarówno za sprawą personelu, poprzez internet, jak też spowodowane mogą być zaniedbaniami.

Incydenty naruszenia bezpieczeństwa informacji mają miejsce pomimo zakrojonych na szeroką skalę różnorodnych działań, wdrażanych przez firmy i organizacje w celu zabezpieczenia systemów komputerowych. Jednak podejście do kwestii bezpieczeństwa z czysto technicznej perspektywy zazwyczaj nie wystarcza. Artykuły z pierwszych stron codziennych gazet świadczą o skali problemu bezpieczeństwa informacji:

- Twarde dyski z istotnymi informacjami sprzedane studentowi
- Skradziony laptop z tylnego siedzenia samochodu
- Zdjęcia promocyjne opublikowane przedwcześnie w prasie
- Brakujące dwa słowa w projekcie ustawy
- Dane ubezpieczonych z ZUS znalezione na śmietniku
- Falszywe wiadomości e-mail z „banków” z prośbą o podanie istotnych informacji nt. konta bankowego
- Kluczowy pracownik współpracujący z prasą
- Opublikowane w internecie tajne informacje



NIE POZWÓL, BY WAŻNE INFORMACJE WYMKNĘŁY CI SIĘ Z RĄK

Zarządzając bezpieczeństwem informacji ograniczamy ryzyko i unikamy sytuacji, które narażają organizację na prawne konsekwencje:

- W nowoczesnych firmach informacje najczęściej przetwarzane są w formie elektronicznej, a kapitał intelektualny to często 70-90% aktywów
- Zapewnienie poufności, integralności i dostępności informacji jest niezbędne do efektywnego działania każdej organizacji
- Bezpieczeństwo i zaufanie są kluczowymi aspektami w rozwoju handlu, produkcji i usług
- Zwiększa się ilość przypadków zagrożenia bezpieczeństwa, przestępstw komputerowych i terroryzmu
- Organizacje stały się bardziej podatne na zagrożenie bezpieczeństwa informacji z powodu internetowych sieci informatycznych.

Analiza przypadków naruszenia bezpieczeństwa informacji powinna skłonić do pytań:

- Jaki jest ich wpływ i rzeczywisty koszt biznesowy?
- Jakie są zagrożenia i ryzyko?
- W jaki sposób postępować w przypadku ich wykrycia?
- Dlaczego wdrażać system zarządzania bezpieczeństwem informacji?
- Dlaczego certyfikować system?

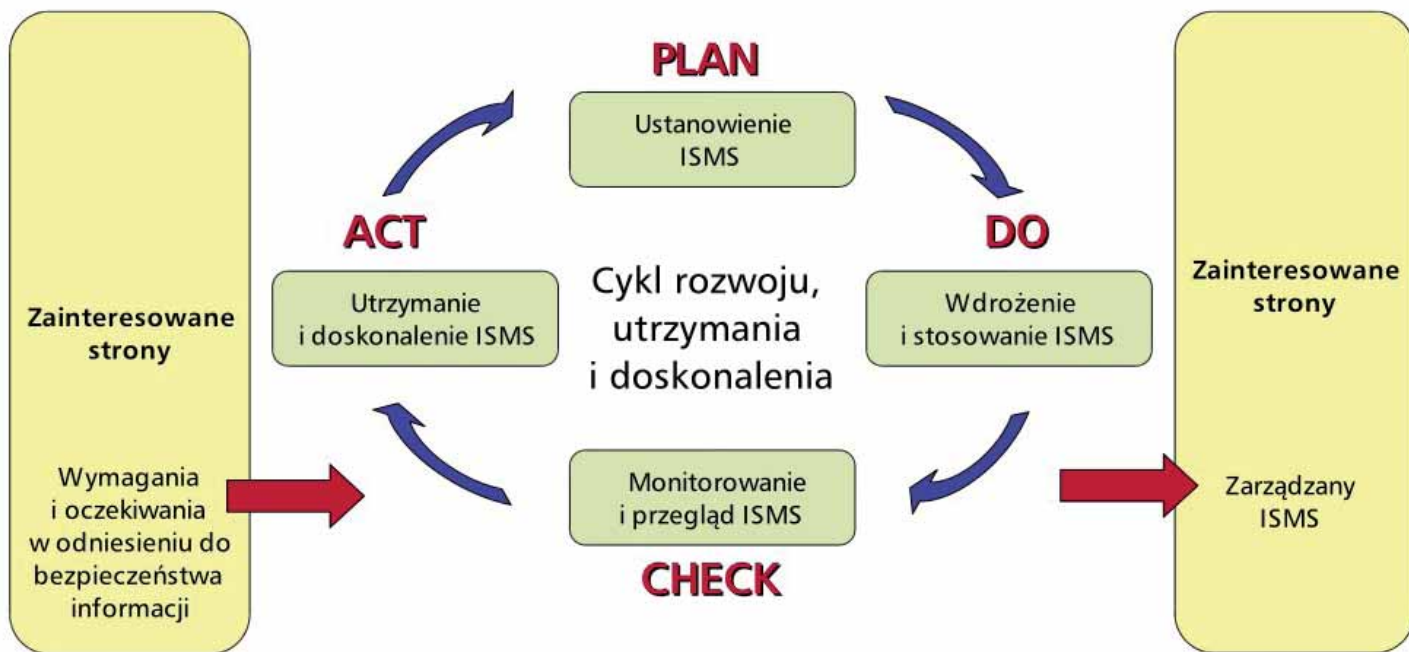
WDRAŻAJĄC ISO 27001, CHRONISZ LUDZI, TECHNIKI I POMYSŁY

Znajdująca się dziś w naszym posiadaniu olbrzymia ilość informacji zwiększa zapotrzebowanie na uniwersalną normę w dziedzinie zarządzania bezpieczeństwem informacji. Dotyczy to przede wszystkim przedsiębiorstw, dla których bezpieczeństwo informacji stanowi kwestię o zasadniczym znaczeniu, np. towarzystw ubezpieczeniowych, banków, operatorów telekomunikacyjnych, całej branży IT, instytucji zaufania publicznego, jednostek badawczych, czy ogólnie firm usługowych. Przedsiębiorstwa budowlane, energetyczne czy firmy konsultingowe również muszą chronić tajemnice handlowe, wzory przemysłowe, plany rozwoju i ogólne zasoby informacji istotnych dla firmy.

Podstawowym założeniem ISO 27001 jest zapobieganie, ochrona i odpowiednie standardy reagowania. Norma obejmuje wszystkie kategorie informacji, tzn. zarówno informacje związane z przedsiębiorstwem, jego aktywami, kontrahentami i pracownikami, jak i informacje dotyczące produktów. Uwzględnia ona informacje zapisane w postaci cyfrowej, dokumenty zapisane na papierze, oraz kładzie nacisk na bezpieczeństwo komunikacji werbalnej.

W jaki sposób organizacja może uzyskać pewność, że personel utrzymuje i rozwija swoje kompetencje?

W jaki sposób firma może ograniczyć do minimum utratę istotnych informacji, gdy pracownik odchodzi?



Norma ISO27001 powstała w odpowiedzi na zapotrzebowanie ze strony przemysłu, władz i przedsiębiorczości na wspólne zasady, które umożliwiłyby firmom opracowanie, wdrożenie i skuteczną ocenę praktyk w zakresie zarządzania bezpieczeństwem informacji oraz sprzyjałyby atmosferze zaufania w kontaktach między przedsiębiorstwami.

Norma szeroko definiuje pojęcie bezpieczeństwa informacji, uwzględniając zagadnienia od rozwoju kompetencji personelu aż po środki techniczne służące ochronie przed włamaniami komputerowymi.

Bezpieczeństwo informacji ma na celu ochronę wartościowych informacji przed nieautoryzowanym dostępem lub zmianą. Systemowe podejście odnosi się do zabezpieczenia informacji w zakresie:

Poufności - zapewnienia, że informacja jest dostępna jedynie osobom upoważnionym

Integralności - zapewnienia dokładności i kompletności informacji oraz metod jej przetwarzania

Dostępności - zapewnienia, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów zawsze wtedy, gdy jest to potrzebne.

11 GŁÓWNYCH OBSZARÓW, KTÓRE POWINNY ZOSTAĆ OBJĘTE DZIAŁANAMI SYSTEMOWYMI

Obszary, które pozwalają na stworzenie podstaw zarządzania bezpieczeństwem informacji:

1. Polityki bezpieczeństwa informacji
2. Organizacja bezpieczeństwa informacji
3. Zarządzanie aktywami
4. Bezpieczeństwo zasobów ludzkich
5. Bezpieczeństwo fizyczne i środowiskowe
6. Zarządzanie systemami i sieciami
7. Kontrola dostępu
8. Pozyskiwanie, rozwój i utrzymanie systemów informatycznych
9. Zarządzanie incydentami naruszenia bezpieczeństwa informacji
10. Zarządzanie ciągłością działania
11. Zgodność

SPECYFIKACJA SYSTEMÓW ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Zasadniczym celem wdrażania Systemu Zarządzania Bezpieczeństwem Informacji jest ochrona informacji.

U podstaw tego procesu leży identyfikacja aktywów informacyjnych, które należy chronić, oraz decyzja odnośnie stopnia ochrony. Aktywa podlegające ochronie obejmują zazwyczaj informacje zapisane w postaci cyfrowej, dokumenty zapisane na papierze oraz środki trwałe, takie jak komputery i sieci. Aktywami określa się również personel i wiedzę, które należy traktować jako majątek firmy.



Wymagania certyfikacyjne obejmują sześć kroków:

1. Ustanowienie i udokumentowanie Polityk Bezpieczeństwa Informacji
2. Zdefiniowanie Zakresu Systemu Zarządzania Bezpieczeństwem Informacji
3. Przeprowadzenie Analizy Ryzyka
4. Udokumentowanie Deklaracji Stosowania
5. Opracowanie Planów Postępowania z Ryzykiem i Planów Ciągłości Biznesu
6. Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji

System Zarządzania Bezpieczeństwem Informacji wdrożony przez firmę w oparciu o identyfikację zagrożeń podlega kontroli na zasadach zbliżonych do kontroli innych systemów zarządzania (ISO 9001, ISO 14001 itp.).

Obok typowego procesu nadzoru systemu zarządzania jednostka certyfikująca musi ocenić, czy zidentyfikowane zagrożenia są realne, oraz czy stopień ochrony wybrany przez firmę jest adekwatny do tych zagrożeń.

Ponadto niezbędne jest dokonanie oceny Deklaracji Stosowania, opisującej wymagania odnośnie wdrażanych zabezpieczeń.

DLACZEGO CERTYFIKOWAĆ SYSTEMY ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI?

Jakie są korzyści z wdrożenia i certyfikacji systemu zarządzania bezpieczeństwem informacji?

- Podniesienie poziomu świadomości w zakresie bezpieczeństwa informacji w całej organizacji
- Zapewnienie odpowiedniej ochrony kapitałowi wiedzy
- Zapewnienie ciągłości pracy przedsiębiorstwa i ograniczenie do minimum potencjalnych strat firmy poprzez ochronę informacji przed szeregiem zagrożeń
- Zapewnienie zgodności z normą opisującą wymagania odnośnie bezpieczeństwa informacji i równoczesna ochrona informacji o istotnym znaczeniu
- Zapewnienie poczucia pewności kontrahentom, którzy powierzają certyfikowanym organizacjom swoje informacje
- Umocnienie przewagi konkurencyjnej, poprzez wzbudzenie zaufania do firmy ze strony pracowników, partnerów i klientów
- Motywowanie kierownictwa do przykładowego przestrzegania dobrych praktyk w zakresie bezpieczeństwa informacji
- Stworzenie poczucia bezpieczeństwa kierownictwu, które może zaufać systemowym mechanizmom ochrony kluczowych aktywów firmy.



KTO MOŻE UBIEGAĆ SIĘ O CERTYFIKAT?

Postępowanie certyfikacyjne może zostać przeprowadzone w odniesieniu do organizacji, działu, placówki lub innego typu podjednostki, a następnie rozszerzone na całą jednostkę, o ile funkcjonuje w niej określony system zarządzania, który spełnia odpowiednie wymagania normy. Zakres dokumentacji systemu zarządzania oraz zastosowanych zabezpieczeń zaczerpniętych z normy ISO27001 zależy od wielkości i stopnia złożoności organizacji, realizowanych procesów oraz sektora rynkowego, w którym dana organizacja działa.

WYBIERZ DNV JAKO PARTNERA W PROCESIE CERTYFIKACJI

- Det Norske Veritas jest niezależną fundacją, powstałą w 1864 roku. Od początku swego istnienia stawia przed sobą zadanie, którym jest ochrona życia, własności i środowiska
- DNV jako pierwsza jednostka otrzymała akredytację na certyfikację wg wymagań normy BS 7799-2 (poprzedniczka ISO27001)
- DNV jest prekursorem w certyfikacji systemów zarządzania bezpieczeństwem informacji w Polsce
- DNV wspiera i bierze udział w pracach Podkomitetu Technicznego PKN ds. Systemów Zarządzania Bezpieczeństwem Informacji

- DNV jest organizacją, której naczelnym dobrem jest własność intelektualna i wiedza.
- Pracownicy DNV oprócz specjalistycznych szkoleń i wykształcenia mają praktyczne doświadczenie w certyfikacji systemów zarządzania bezpieczeństwem informacji
- DNV oferuje szkolenia i warsztaty obejmujące interpretację wymagań normy oraz warsztaty dla audytorów
- Wszystkie audyty i szkolenia prowadzone są przez polskich audytorów wiodących i wykwalifikowanych wykładowców
- Ponad 70 000 certyfikatów na świecie zostało wydanych przez DNV
- Dziś DNV zatrudnia 6 000 pracowników w 100 krajach, na wszystkich kontynentach. Wszędzie tam troszczymy się o naszych Klientów, dostarczając im rozwiązań doskonalących ich działalność biznesową.



DNV - PEWNOŚĆ I ZAUFANIE

DNV to niezależna, autonomiczna fundacja, której celem jest ochrona życia, majątku oraz środowiska naturalnego.

Jesteśmy przedsiębiorstwem opartym na wiedzy, którego najważniejszymi zaletami są kreatywność, wiedza oraz doświadczenie pracowników.

Nasza działalność polega na udzielaniu firmom pomocy w zakresie zarządzania ryzykiem. Na świecie DNV uznawana jest za jeden z wiodących i najbardziej szanowanych organów zajmujących się certyfikacją systemów zarządzania. Posiadamy 80 akredytacji w różnych państwach, a do tej pory na całym świecie wydaliśmy ponad 70 tysięcy certyfikatów systemów zarządzania.

Det Norske Veritas Poland Sp. z o.o.
ul. 3 Maja 67-69
81-850 Sopot
tel. +48 58 51 15 020
certification.pl@dnv.com
www.dnv.pl