

## Bezpieczeństwo danych

ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych<sup>1</sup>

### Wprowadzenie

Zgodnie z art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. 2002 r. nr 101 poz. 926, z późn. zm.; dalej jako: ustawa), administrator danych osobowych zobowiązany jest do zapewnienia ochrony przetwarzanych danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Jakość zapewnianej ochrony powinna być odpowiednia do zagrożeń oraz kategorii danych nią objętych. Ponadto zgodnie z art. 38 ustawy administrator danych zobowiązany jest zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

Ten ostatni wymóg, pomimo że umieszczony został w rozdziale 5 ustawy dotyczącym zabezpieczenia przetwarzanych danych, odnosi się nie tylko do kwestii bezpieczeństwa, ale również – odpowiednich funkcjonalności przyjętego systemu przetwarzania. Funkcjonalności te wynikają z kolei nie tylko z potrzeby zapewnienia bezpieczeństwa danych, ale również

z konieczności zapewnienia określonych właściwości oraz warunków umożliwiających administratorowi realizację zobowiązań wobec podmiotów danych wynikających z art. 32 i 33 ustawy i § 7 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. nr 100 poz. 1024; dalej jako: rozporządzenie). Wymagane w przywołanych przepisach obowiązki sprowadzają się m.in. do zapewnienia i udostępniania – na żądanie osoby, której dane są przetwarzane – informacji o:

- dacie, od kiedy przetwarza się w zbiorze jej dane osobowe, oraz treści tych danych,
- źródle, z którego pochodzą dane jej dotyczące, chyba że administrator jest obowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej,
- sposobie i zakresie udostępniania jej danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
- sposobie, w jaki zebrano dane.

<sup>1</sup> <https://edugiodo.giodo.gov.pl/mod/resource/view.php?id=39>

Ogólnie przez pojęcie zapewnienia ochrony przetwarzanym danym należy rozumieć działanie mające na celu zabezpieczenie przed czymś złym, niekorzystnym, niebezpiecznym. W odniesieniu do danych osobowych będą to działania mające na celu zapewnienie, aby były one pozyskiwane i przetwarzane zgodnie z przepisami prawa. Oznacza to między innymi, że powinny być one wykorzystywane tylko w określonym celu, zabezpieczone przed nieuprawnionymi zmianami, ujawnieniem nieupoważnionym osobom, zniszczeniem, utratą lub uszkodzeniem.

Czynności podejmowane w ramach tych działań oraz zastosowane środki techniczne i organizacyjne będą zależne od środowiska, w jakim dane są przetwarzane.

W niniejszym opracowaniu zostały omówione zagadnienia związane z zapewnieniem ochrony danych przetwarzanych przy użyciu systemów informatycznych. Pojęcie „ochrony danych” należy w tym przypadku utożsamiać z pojęciem „bezpieczeństwa informacji”, stosowanym w literaturze z zakresu bezpieczeństwa teleinformatycznego. Według normy PN-ISO/IEC-17799:20051 przez bezpieczeństwo informacji należy rozumieć zachowanie poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności. Wymienione właściwości, wg definicji zawartych w PN-1-13335-12, polegają odpowiednio na:

- Poufność – zapewnieniu, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,
- Integralność – zapewnieniu, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- Dostępność – zapewnieniu bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot,
- Rozliczalność – zapewnieniu, że działania podmiotu mogą być przy pisane w sposób jednoznaczny tylko temu podmiotowi,
- Autentyczność – zapewnieniu, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji),
- Niezaprzeczalność – braku możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,
- Niezawodność – zapewnieniu spójności oraz zamierzonych zachowań i skutków.

Należy zwrócić uwagę, że zapewnienie a następnie wykazanie określonych właściwości wymaga często zastosowania określonych środków i jednoczesnego spełnienia wielu warunków. Zapewnienie np. niezaprzeczalności podpisu elektronicznego (wykazanie, że dany dokument elektroniczny podpisała określona osoba) wymaga udowodnienia, że dany dokument nie został zmieniony (integralność), a złożony podpis należy do danej osoby (uwierzytelnienie).

Gdy do przetwarzania danych osobowych wykorzystuje się systemy informatyczne, zadania dotyczące zapewnienia określonych właściwości przenoszone są na odpowiednie wymagania

dotyczące właściwości tych systemów. Dodatkowy problem, jaki wówczas powstaje, polega na zapewnieniu skuteczności i ciągłości zachowywania przez systemy informatyczne wymaganych właściwości. Właściwości te mogą być utracone na skutek błędów popełnionych przez administratora systemu lub celowych działań osób nieupoważnionych do ingerowania w dany system informatyczny. W konsekwencji, oprócz działań mających na celu ochronę przetwarzanych danych, należy zapewnić również ochronę systemu informatycznego, którego użyto do ich przetwarzania. Stąd też w przepisach wykonawczych do ustawy, wydanych na podstawie delegacji zawartej w art. 39a, określone zostały wymagania dotyczące nie tylko polityki bezpieczeństwa, ale również systemu informatycznego oraz sposobu zarządzania nim.

### Co to jest bezpieczeństwo?<sup>2</sup>

Przedstawienie problematyki bezpieczeństwa systemów komputerowych systemów komputerowych należy rozpocząć od zdefiniowania pojęcia bezpieczeństwa. Niestety trudno skonstruować uniwersalną i jednoznaczną definicję tego pojęcia, która pokryłaby wszystkie oczekiwania stawiane w tej dziedzinie systemom komputerowym. Literatura przedmiotu podaje bardzo dużo, często znacznie odbiegających od siebie definicji.

Def.

**System komputerowy jest bezpieczny**, jeśli jego użytkownik może na nim polegać, a zainstalowane oprogramowanie działa zgodnie ze swoją specyfikacją. W myśl tej definicji, możemy system uznać za bezpieczny, jeśli np. można od niego oczekiwać, że wprowadzone na stałe dane nie zostaną utracone, nie ulegną zniekształceniu i nie zostaną pozyskane przez nikogo nieuprawnionego - ufamy, że system będzie przechowywał i chronił dane.

Bezpieczeństwo jest elementem szerszego kontekstu, nazywanego wiarygodnością systemu komputerowego. W kontekście tym wyróżnia się w sumie cztery atrybuty wiarygodności:

System wiarygodny:

- dyspozycyjny (available) = dostępny na bieżąco
- niezawodny (reliable) = odporny na awarie
- bezpieczny (secure) = zapewniający ochronę danych
- bezpieczny (safe) = bezpieczny dla otoczenia, przyjazny dla środowiska

### Czynniki decydujące o znaczeniu bezpieczeństwa

---

<sup>2</sup> [http://wazniak.mimuw.edu.pl/index.php?title=Bezpiecze%C5%84stwo\\_system%C3%B3w\\_komputerowych\\_-\\_wyk%C5%82ad\\_1:Wprowadzenie\\_do\\_problematyki\\_bezpiecze%C5%84stwa\\_system%C3%B3w\\_komputerowy\\_ch](http://wazniak.mimuw.edu.pl/index.php?title=Bezpiecze%C5%84stwo_system%C3%B3w_komputerowych_-_wyk%C5%82ad_1:Wprowadzenie_do_problematyki_bezpiecze%C5%84stwa_system%C3%B3w_komputerowy_ch)

O doniosłości problematyki bezpieczeństwa dla współczesnej cywilizacji decyduje przede wszystkim wszechobecność technik komputerowych. W szczególności rozważyć należy następujące zagadnienia:

- rola systemów informatycznych (szczególnie sieci) dla funkcjonowania współczesnej cywilizacji jest nie do przecenienia; nie ma już praktycznie obszaru działalności człowieka, w którym żadne elementy techniki komputerowej (bądź szerzej mikroprocesorowej) nie byłyby obecne. Jako drobny przykład niech posłuży telefonia komórkowa, towarzysząca dziś człowiekowi niemal ciągle i wszędzie;
- trudności związane ze skonstruowaniem i eksploatacją systemu spełniającego wysokie wymagania w zakresie bezpieczeństwa (niedoskonałości technologii, konfiguracji i polityki bezpieczeństwa) stwarzają niebezpieczeństwo niedopracowanego pod względem bezpieczeństwa i niezawodności produktu informatycznego lub nieodpowiedniego pod owym względem wykorzystania tego produktu;
- elementarny konflikt interesów występujący pomiędzy użytecznością systemu a ryzykiem związanym z jego wykorzystaniem rodzi szereg pragmatycznych problemów (często całkowicie pozatechnicznych) związanych z oczywistymi utrudnieniami we wdrożeniu i użytkowaniu systemów o podwyższonym bezpieczeństwie.

### Zagrożenia bezpieczeństwa

Zagrożenia bezpieczeństwa mają różną naturę. Mogą być najzupełniej przypadkowe lub powstać w efekcie celowego działania. Mogą wynikać z nieświadomości lub naiwności użytkownika, bądź też mogą być motywowane chęcią zysku, poklasku lub odwetu. Mogą pochodzić z zewnątrz systemu lub od jego środka. Większość działań skierowanych w efekcie przeciwko bezpieczeństwu komputerowemu jest w świetle aktualnego prawa traktowana jako przestępstwa.

Możemy tu wyróżnić w szczególności:

- włamanie do systemu komputerowego
- nieuprawnione pozyskanie informacji
- destrukcja danych i programów
- sabotaż (sparaliżowanie pracy) systemu
- piractwo komputerowe, kradzież oprogramowania
- oszustwo komputerowe i fałszerstwo komputerowe
- szpiegostwo komputerowe

Istotne jest, iż w przypadku jurysdykcji większości krajów europejskich, praktycznie wszystkie przypadki naruszające bezpieczeństwo wyczerpują znamiona przestępstw określonych w obowiązującym prawie.

W Polsce w szczególności mają tu zastosowanie:

**artykuły 267-269 Kodeksu Karnego**

**Art. 267<sup>3</sup>**

1. Kto bez uprawnienia uzyskuje informację dla niego nieprzeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym.

3. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1 lub 2 ujawnia innej osobie.

4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

**Art. 268**

1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Jeżeli czyn określony w § 1 dotyczy zapisu na komputerowym nośniku informacji, sprawca podlega karze pozbawienia wolności do lat 3.

3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

**Art. 269**

1. Kto na komputerowym nośniku informacji niszczy, uszkadza, usuwa lub zmienia zapis o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub administracji samorządowej albo zakłóca lub uniemożliwia automatyczne gromadzenie lub przekazywanie takich informacji, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając nośnik informacji lub niszcząc albo uszkadzając urządzenie służące automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji.

---

<sup>3</sup> [http://www.computerworld.pl/artykuly/311156\\_5/Komputerowi.detektywi.html](http://www.computerworld.pl/artykuly/311156_5/Komputerowi.detektywi.html)

## artykuł 287 Kodeksu Karnego

### Art. 287

1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji lub zmienia, usuwa albo wprowadza nowy zapis na komputerowym nośniku informacji, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
2. W wypadku mniejszej wagi sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
3. Jeżeli oszustwo popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

Jednym z najczęstszych przypadków wykorzystania computer forensics jest naruszenie zasad obowiązującej umowy o pracę poprzez celowe usunięcie danych. Ścigane jest to z art. 287 par. 1 kodeksu karnego.

W świetle regulacji kodeksu pracy wymazanie lub kradzież danych może stanowić podstawę do rozwiązania umowy o pracę przez pracodawcę bez wypowiedzenia w trybie art. 52 par. 1 pkt. 1 kodeksu pracy, gdyż takie zachowanie stanowi ciężkie naruszenie obowiązków pracowniczych.

Zgodnie z art. 114 kodeksu pracy pracownik, który wskutek niewykonania lub nienależytego wykonania obowiązków pracowniczych ze swej winy wyrządził pracodawcy szkodę, ponosi odpowiedzialność materialną. Pracownik ponosi odpowiedzialność za szkodę w granicach rzeczywistej straty poniesionej przez pracodawcę i tylko za normalne działania lub zaniechania, z którego szkoda wynikła. Odszkodowanie ustala się w wysokości wyrządzonej szkody, jednakże co do zasady nie może ono przewyższać kwoty trzymiesięcznego wynagrodzenia pracownika w chwili wyrządzenia szkody. Zgodnie z art. 122 kodeksu pracy jeżeli szkoda wyrządzona przez pracownika została umyślnie, pracownik jest zobowiązany do jej naprawienia w pełnej wysokości.

Ponadto art. 11 ustawy o zwalczaniu nieuczciwej konkurencji (Dz.U. 197 poz. 1661 z 2002 r.) określa, iż czynem nieuczciwej konkurencji jest przekazanie, ujawnienie lub wykorzystanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa. Art. 11 ustawy stosuje się również do osób, które świadczyły pracę na podstawie stosunku pracy lub innego stosunku prawnego - przez okres trzech lat od jego ustania, chyba że umowa stanowi inaczej albo ustał stan tajemnicy. Art. 23 wyżej wymienionej ustawy stanowi, iż "kto, wbrew ciążącemu na nim obowiązkowi w stosunku do przedsiębiorcy, ujawnia innej osobie lub wykorzystuje we własnej działalności gospodarczej informacje stanowiące tajemnicę przedsiębiorstwa, jeżeli wyrządza to poważną szkodę przedsiębiorcy podlega karze grzywny, karze ograniczenia wolności albo pozbawienia wolności do lat 2".

***Zazwyczaj przestępstwa te nie są ścigane z oskarżenia publicznego, lecz na wniosek pokrzywdzonego.***

W kontekście bezpieczeństwa komputerowego powszechnie spotyka użycie popularnego terminu hacker na określenie osoby podejmującej atak. Termin ten oryginalnie nie posiadał wydźwięku pejoratywnego. Wg „The Hacker's Dictionary” (Guy L. Steele et al.) hacker jest to osoba, której sprawia przyjemność poznawanie szczegółowej wiedzy na temat systemów komputerowych i rozszerzanie tej umiejętności, w przeciwieństwie do większości użytkowników, którzy wolą uczyć się niezbędnego minimum; osoba, która entuzjastycznie zajmuje się programowaniem i nie lubi teorii dotyczącej tej dziedziny.

### **Komponenty systemu informatycznego w kontekście bezpieczeństwa**

Elementarne składniki systemu informatycznego jakie należy wyróżnić przy omawianiu problematyki bezpieczeństwa to:

- stanowisko komputerowe i infrastruktura sieciowa
- system operacyjny i usługi narzędziowe
- aplikacje użytkowe

### **Ogólne problemy konstrukcji zabezpieczeń**

Problematyka bezpieczeństwa, jak każda dziedzina, podlega pewnym ogólnym prawom, niektórym sformalizowanym, innym - nieformalnym. Można wyróżnić pewne truizmy obowiązujące podczas projektowania i realizowania zabezpieczeń.

Niektóre z nich to:

- Nie istnieje absolutne bezpieczeństwo. Wiąże się to z wieloma przyczynami. Jedną z nich jest fakt, iż nigdy nie jesteśmy w stanie przewidzieć z góry wszystkich możliwych zagrożeń, tym bardziej że często należy opracowywać zabezpieczenia z odpowiednim wyprzedzeniem. Szybki rozwój technologii informatycznych implikuje powstawanie coraz to nowych zagrożeń. Czas reakcji na nie nigdy nie jest zerowy i w związku z tym nawet dla najlepiej opracowanego systemu zabezpieczeń istnieje ryzyko powstania okresu dezaktualizacji zastosowanych mechanizmów bezpieczeństwa. Ewolucja zagrożeń pociąga za sobą wyścig atakujących i broniących („policjantów i złodziei”). Innym istotnym powodem niemożliwości osiągnięcia 100% bezpieczeństwa jest ludzka słabość, w szczególności omylność projektantów, programistów, użytkowników systemów informatycznych, skutkująca błędami w oprogramowaniu systemowym i aplikacyjnym oraz niewłaściwym lub niefrasobliwym jego wykorzystaniu.

Skoro zatem nie mamy 100% bezpieczeństwa, jaki jego poziom można uznać za zadowalający? Otóż wydaje się, że najwłaściwszą odpowiedzią na to pytanie jest - taki, który



okaże się dla atakującego na tyle trudny do sforsowania, wymagając operacji żmudnych lub czasochłonnych, iż uczyni to atak nieatrakcyjnym lub nieekonomicznym (lub oczywiście nieopłacalnym wg innego kryterium obranego przez atakującego). Zatem należy na tyle utrudnić włamywaczowi atak, aby z niego zrezygnował widząc marne, choć nadal niezerowe, szanse powodzenia.

- Napastnik na ogół nie pokonuje zabezpieczeń, tylko je obchodzi. Przeprowadzenie skutecznego ataku na jakikolwiek aktywny mechanizm zabezpieczeń jest raczej czasochłonne i stosowane tylko w ostateczności. Zwykle mniej kosztowne i szybsze jest znalezienie luki w środowisku systemu informatycznego, zabezpieczonego owym mechanizmem niż łamanie jego samego, która to luka pozwoli skutecznie wtargnąć do systemu nie jako „z boku” zabezpieczeń. Przy tej okazji warto wspomnieć, że okazuje się niezmiennie od wielu lat, iż większość ataków przeprowadzanych na systemy informatyczne realizowana jest „od środka”, czyli przez zaufanych, poniekąd, użytkowników systemu, którzy znając system jakim się posługują niewątpliwie łatwiej mogą znaleźć i wykorzystać luki bezpieczeństwa.
- Nie należy pokładać zaufania w jednej linii obrony. Z poprzedniej obserwacji wynika, że obejście aktywnego mechanizmu zabezpieczeń często bywa możliwe i może istotnie narażać bezpieczeństwo całego systemu. W związku z tym, naturalną konsekwencją tego jest konstruowanie wielopoziomowych zabezpieczeń poprzez budowanie kolejnych swoistych „linii obrony”, z których każda po przejściu poprzedniej stanowić będzie, przynajmniej potencjalnie, kolejną zaporę dla atakującego.
- Złożoność jest najgorszym wrogiem bezpieczeństwa. Skomplikowane systemy są trudne do opanowania, również pod względem bezpieczeństwa. Istotnym usprawnieniem zarządzania systemem jest jego modułarna konstrukcja, dająca szansę na zwiększenie kontroli nad konfiguracją i funkcjonowaniem systemu. Dotyczy to również wielopoziomowych zabezpieczeń.
- System dopóty nie jest bezpieczny, dopóki nie ma pewności że jest. Bardzo łatwo popełnić błąd zakładając zupełnie inaczej - dopóki brakuje odnotowanych symptomów, iż bezpieczeństwo systemu zostało naruszone, możemy spać spokojnie. Zaobserwowanie ataku nie jest trywialne nawet w systemie poprawnie monitorowanym. Ponadto symptomy ataku zwykle występują dopiero po jego zakończeniu, kiedy to może być zbyt późno by przeprowadzać akcję ratunkową, kiedy ucierpiały już newralgiczne składniki systemu, poufne dane lub reputacja firmy.

Wzrost poziomu bezpieczeństwa odbywa się kosztem wygody. Użytkownicy systemu pragną przede wszystkim efektywności i wygody swojej pracy.

## Strategia bezpieczeństwa



Opracowanie skutecznych zabezpieczeń jest problemem bardzo złożonym. Wymaga uwagi i systematyczności na każdym etapie. Niewątpliwie decydujące znaczenia ma etap projektowy, na którym popełnione błędy mogą być nienaprawialne w kolejnych etapach. Etap projektowy powinien rozpocząć się od wypracowania strategii firmy dotyczącej bezpieczeństwa (i to nie wyłącznie systemu informatycznego). Polega to w ogólnym schemacie na odpowiedzi na następujące pytania:

- „Co chronić?” (określenie zasobów)
- „Przed czym chronić?” (identyfikacja zagrożeń)
- „Ile czasu, wysiłku i pieniędzy można poświęcić na należną ochronę” (oszacowanie ryzyka, analiza kosztów i zysku)

9

### **Określenie zasobów = „Co chronić?”**

Zasoby jakie mogą podlegać ochronie obejmują m.in. (w zależności od typu instytucji, dziedziny działalności itp.):

- sprzęt komputerowy
- infrastruktura sieciowa
- wydruki
- strategiczne dane
- kopie zapasowe
- wersje instalacyjne oprogramowania
- dane osobowe
- dane audytu
- zdrowie pracowników
- prywatność pracowników
- zdolności produkcyjne
- wizerunek publiczny i reputacja

### **Identyfikacja zagrożeń = „Przed czym chronić?”**

Zagrożenia jakie należy rozważyć stanowią m.in.:

- włamywacze komputerowi
- infekcje wirusami
- destruktywność pracowników / personelu zewnętrznego
- błędy w programach
- kradzież dysków / laptopów (również w podróży służbowej)
- utrata możliwości korzystania z łączy telekomunikacyjnych
- bankructwo firmy serwisowej / producenta sprzętu
- choroba administratora / kierownika (jednoczesna choroba wielu osób)

- powódź

### **Polityka bezpieczeństwa**

Polityka bezpieczeństwa stanowi element polityki biznesowej firmy. Jest to formalny dokument opisujący strategię bezpieczeństwa.

Jej realizacja podlega oczywistym etapom:

- zaprojektowanie
- zaimplementowanie
- zarządzanie (w tym monitorowanie i okresowe audyty bezpieczeństwa)

10

Szczególnie godnym podkreślenia jest etap 3. odzwierciedlający ciągłą ewolucję jaką przechodzą działalność firmy, środowisko rynkowe jej funkcjonowania, zagrożenia i technologie obrony. Wymaga to ciągłego "trzymania ręki na pulsie".

### **Zakres**

Zakres tematyczny jaki powinna obejmować polityka bezpieczeństwa to:

- definicja celu i misji polityki bezpieczeństwa
- standardy i wytyczne których przestrzegania wymagamy
- kluczowe zadania do wykonania
- zakresy odpowiedzialności

### **Specyfikacja środków**

Polityka bezpieczeństwa winna definiować środki jej realizacji obejmujące takie elementy jak:

- ochrona fizyczna
- polityka proceduralno-kadrowa (odpowiedzialność personalna)
- mechanizmy techniczne

### **Normy i zalecenia zarządzania bezpieczeństwem**

Istnieje wiele dokumentacji poświęconej realizacji polityki bezpieczeństwa, w tym również norm i standardów międzynarodowych, którymi należy posługiwać się przy opracowywaniu własnej polityki bezpieczeństwa. Pod tym względem kanonem jest norma ISO/IEC Technical Report 13335 (ratyfikowana w naszym kraju jako PN-I-13335).