Polityka bezpieczeństwa informacji

Główne zagadnienia wykładu

Bezpieczeństwo systemów informatycznych

Polityka bezpieczeństwa

Zbigniew Suski BSI – polityka bezpieczeństwa informacji 1

Polityka Bezpieczeństwa Informacji

Jest zbiorem zasad i procedur obowiązujących przy zbieraniu, przetwarzaniu i wykorzystaniu informacji w organizacji. Dotyczy ona całego procesu korzystania z informacji, niezależnie od sposobu jej gromadzenia i przetwarzania.

Zbigniew Suski BSI – polityka bezpieczeństwa informacji 2

Podstawowe zasady opracowywania polityki

- Inicjatywa w zakresie bezpieczeństwa informacji musi wyjść ze strony kierownictwa organizacji.
- Ostateczną odpowiedzialność za bezpieczeństwo informacji ponosi kierownictwo.
- Tylko, gdy kierownictwo jest zainteresowane bezpieczeństwem, zadania w tym zakresie są traktowane poważnie.
- Wszystkie strategie i procedury powinny odzwierciedlać potrzeby ochrony danych niezależnie od przyjmowanej przez nie formy - dane powinny być chronione niezależnie od nośnika, na którym występują.
- W skład zespołu d/s zarządzania bezpieczeństwem muszą wejść przedstawiciele praktycznie wszystkich komórek organizacyjnych.
- Każdy powinien sobie uświadomić sobie własną odpowiedzialność za utrzymywanie bezpieczeństwa.

Zbigniew Suski BSI – polityka bezpieczeństwa informacji 3

Zadania zespołu d/s bezpieczeństwa

- Ustalenie celów bezpieczeństwa oraz opracowanie polityki gwarantującej osiągnięcie założonych celów.
- Ustalenie zakresu obowiązków osób odpowiedzialnych za bezpieczeństwo.
- Doradzanie i kontrola w zakresie osiągania celów bezpieczeństwa przy opracowywaniu koncepcji bezpieczeństwa.
- Opracowanie planu wdrażania przedsięwzięć bezpieczeństwa określonych w koncepcji bezpieczeństwa.
- Nadzór nad realizacją planu wdrażania przedsięwzięć bezpieczeństwa.
- Nadzór nad informowaniem pracowników o działaniach w zakresie bezpieczeństwa.
- Kontrola efektywności przedsięwzięć bezpieczeństwa w toku pracy organizacji.
- Określanie zasobów niezbędnych do realizacji założonych procesów wdrażania bezpieczeństwa.

Zbigniew Suski BSI – polityka bezpieczeństwa informacji 4

Obowiązki pełnomocnika d/s bezpieczeństwa

- Współdziałanie w ustalaniu koncepcji bezpieczeństwa.
- Informowanie kierownictwa i zespołu d/s zarządzania bezpieczeństwem o przebiegu procesów bezpieczeństwa.
- Ustalenie dróg przepływu informacji od lokalnych pełnomocników i przetworzenie tej informacji.
- Odpowiedzialność i nadzór nad realizacją wybranych przedsięwzięć bezpieczeństwa.
- Planowanie i koordynacja szkoleń w zakresie bezpieczeństwa.
- Utrzymywanie założonego stopnia bezpieczeństwa (kontrole) w trakcie działania organizacji.
- Analizowanie i reagowanie na zdarzenia naruszające bezpieczeństwo.

Zbigniew Suski BSI – polityka bezpieczeństwa informacji 5

Schemat postępowania

- **Planowanie**
  - Zaprojektowanie polityki bezpieczeństwa.
  - Określenie pożądanego poziomu bezpieczeństwa.
  - Powołanie zespołu d/s zarządzania bezpieczeństwem.
  - Opracowanie polityki bezpieczeństwa.
  - Opracowanie koncepcji bezpieczeństwa.
- **Realizacja**
  - Wdrożenie przedsięwzięć bezpieczeństwa.
  - Szkolenie personelu w zakresie bezpieczeństwa.
- **Eksploatacja**
  - Utrzymywanie bezpieczeństwa w toku pracy organizacji.

Zbigniew Suski BSI – polityka bezpieczeństwa informacji 6

Audyt bezpieczeństwa

- Rozpoznanie problemu przetwarzania informacji w organizacji (przede wszystkim określenie podstawy prawnej).
- Rozpoznanie rodzajów informacji przetwarzanych w organizacji.
- Analiza obiegu poszczególnych grup informacji i rozpoznanie systemów przetwarzania informacji.
- Analiza zagrożeń i ryzyka przetwarzania informacji.
- Ocena stosowanych systemów zabezpieczeń.

Zbigniew Suski BSI – polityka bezpieczeństwa informacji 7

Ryzyko

IEC 61508:

Pod pojęciem ryzyka należy rozumieć miarę stopnia zagrożenia dla tajności, integralności i dostępności informacji wyrażona jako iloczyn prawdopodobieństwa wystąpienia sytuacji stwarzającej takie zagrożenie i stopnia szkodliwości jej skutków.

Zbigniew Suski BSI – polityka bezpieczeństwa informacji 8

Analiza ryzyka

- **Szacowanie ryzyka:**
  - Co chronić?
  - Przed czym chronić?
  - Jakie jest prawdopodobieństwo wystąpienia zagrożenia lub skutków zagrożenia?
- **Ocena akceptowalności ryzyka:**
  - Jaki jest stopień szkodliwości skutków zagrożenia?
  - Jakie są koszty zabezpieczeń?
  - Czy warto chronić?

Zbigniew Suski BSI – polityka bezpieczeństwa informacji 9

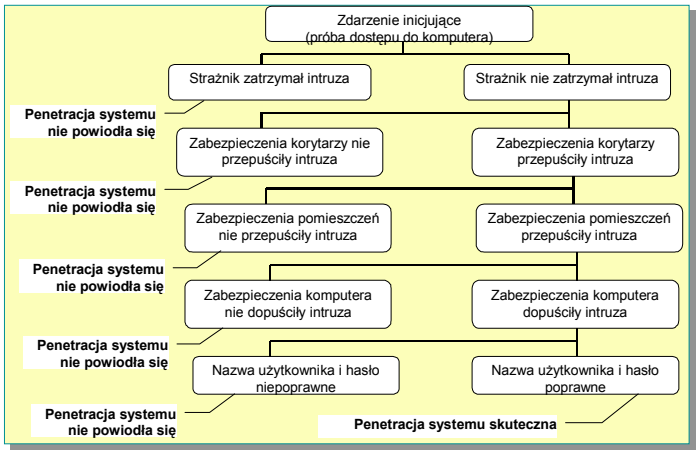
Przykład - założenia

Pracownicy pewnej instytucji dysponują kartami magnetycznymi z ich danymi osobowymi, służbowymi, zdjęciem i PINem. Karta służy jako przepustka okazywana wartownikowi przy wejściu. Wykorzystywana jest również jako klucz elektroniczny otwierający drzwi dostępne dla danego pracownika. System komputerowy jest chroniony następującymi zabezpieczeniami:

- **strażnik przy wejściu głównym,**
- **elektroniczne zabezpieczenia (czytnik kart) wejść do korytarzy,**
- **elektroniczne zabezpieczenia wejść do pomieszczeń służbowych,**
- **elektroniczne zabezpieczenia komputera,**
- **nazwa i hasło umożliwiające otwarcie sesji.**

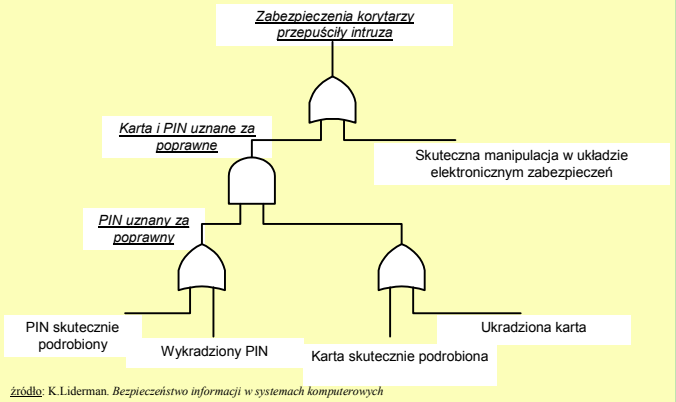
Zbigniew Suski BSI – polityka bezpieczeństwa informacji 10

Drzewo zdarzeń



Zbigniew Suski BSI – polityka bezpieczeństwa informacji 11

Drzewo błędów



źródło: K.Liderman. *Bezpieczeństwo informacji w systemach komputerowych*

Wady metody oceny ryzyka

- częsty brak danych do wyznaczania prawdopodobieństw zdarzeń elementarnych,
- trudności w ustaleniu pełnego zbioru kategorii ryzyka,
- niezdolność do badania skutków negatywnych o wspólnej przyczynie,
- nieuwzględnianie ryzyka wtórnego,
- nieuwzględnianie zagrożenia spowodowanego umyślnie,
- trudności w interpretacji wyników.

Zalety metody oceny ryzyka

- pomaga precyzyjniej identyfikować zagrożenia oraz ich przyczyny,
- stanowi podstawę do podejmowania decyzji administracyjnych i menedżerskich,
- systematyzuje proces oceny bezpieczeństwa systemu informacyjnego.

Realizacja polityki bezpieczeństwa

- Jakie informacje będą podlegać ochronie?
- Jakie systemy zostaną objęte polityką bezpieczeństwa?
- Jakie zadania realizowane przez w/w systemy mają związek z informacjami podlegającymi ochronie?
- Kto jest uprawniony do korzystania z zasobów?
- Na czym polega właściwe korzystanie z zasobów?
- Kto jest uprawniony do przydzielania praw dostępu?
- Kto ma uprawnienia *administratora*?
- Jaki jest zakres uprawnień i odpowiedzialności użytkowników?
- Jakie są uprawnienia *administratora* w porównaniu do uprawnień zwykłych użytkowników?

Plan realizacji przedsięwzięć

- Lista przedsięwzięć bezpieczeństwa realizowanych dla każdego systemu informatycznego.
- Zestawienie związanych z tym kosztów.
- Szczegółowy plan pracy, zawierający priorytety, budżet, harmonogram,
- listę niezbędnych akcji, projektów, itp.
- Określenie sposobu nadzoru i kontroli realizacji przedsięwzięć bezpieczeństwa,
- listę szkoleń niezbędnych do poprawnego wdrożenia przedsięwzięć bezpieczeństwa.

Tematyka szkoleń

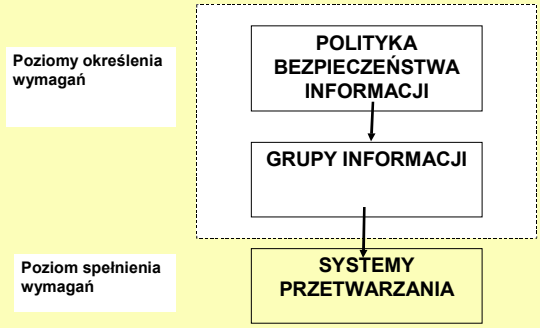
- Cele polityki bezpieczeństwa.
- Znaczenie polityki bezpieczeństwa dla firmy.
- Wybrane elementy koncepcji bezpieczeństwa.
- Omówienie konieczności i sposobów raportowania przypadków naruszania bezpieczeństwa.
- Omówienie konsekwencji nie przestrzegania polityki bezpieczeństwa.
- Plany implementacji i sprawdzania przedsięwzięć wyspecyfikowanych w polityce bezpieczeństwa.

Plan utrzymywania bezpieczeństwa

- Sposoby pielęgnacji i modyfikacji przedsięwzięć bezpieczeństwa.
- Sposoby kontroli przedsięwzięć.
- Sposoby sprawdzania wprowadzanych zmian na bezpieczeństwo.
- Sposoby reagowania na incydenty naruszania bezpieczeństwa.

Zbigniew Suski BSI – polityka bezpieczeństwa informacji 18

TISM - struktura polityki bezpieczeństwa



Total Information Security Management oraz skrót TISM jest przedmiotem rejestracji znaku towarowego w Głównym Urzędzie Patentowym RP. Autorem metodologii TISM jest *European Network Security Institute Sp. z o.o* (www.ensi.net). Dokumentacja TISM jest rozpowszechniana przez autora na zasadzie Licencji Darmowej Dokumentacji GNU - GNU Free Documentation Licence.

Zbigniew Suski BSI – polityka bezpieczeństwa informacji 19

Główne założenia TISM

Informacja

Wszelkie zapisy na papierze, w układach elektronicznych, na nośnikach magnetycznych, optycznych, itp. są reprezentacją informacji i podlegają ochronie

Własność informacji

Wszelkie informacje przekazywane i przetwarzane w organizacji, nie oznaczone jako należące do osób trzecich, będą traktowane jako własność organizacji

Podział informacji

Wszystkie informacje w organizacji dzielimy na jawne i "zastrzeżone dla danej organizacji"

Zbigniew Suski BSI – polityka bezpieczeństwa informacji 20

Główne założenia TISM

Ochrona informacji

Ochronie podlegają tylko informacje zastrzeżone

Dostęp do informacji zastrzeżonych

Dostęp do informacji zastrzeżonych przyznaje się w oparciu o rolę jaką dana osoba wypełnia w firmie

Zarządzanie informacjami zastrzeżonymi

Informacje zastrzeżone dzieli się na grupy

Każda grupa informacji zastrzeżonych posiada własny dokument Polityki Bezpieczeństwa

Każda grupa informacji zastrzeżonych musi posiadać Administratora grupy informacji i Administratora bezpieczeństwa grupy informacji

Zbigniew Suski BSI – polityka bezpieczeństwa informacji 21

Główne założenia TISM

System przetwarzania informacji zastrzeżonych

Informacje zastrzeżone mogą być przetwarzane, przechowywane lub przesyłane wyłącznie przy pomocy systemów, które spełniają warunki opisane w Polityce Bezpieczeństwa Grupy Informacji Zastrzeżonych

Każdy system przetwarzania informacji zastrzeżonych musi posiadać:

- *własną Politykę Bezpieczeństwa*
- *własne procedury przyznawania praw dostępu,*
- *własne procedury kryzysowe*

Każdy system przetwarzania informacji zastrzeżonych musi posiadać Administratora bezpieczeństwa systemu i Administratora systemu

Każdy system przetwarzania informacji zastrzeżonych musi przechodzić okresowe audyty bezpieczeństwa zlecane przez Zarząd organizacji

Zbigniew Suski BSI – polityka bezpieczeństwa informacji 22

Główne założenia TISM

Użytkownicy informacji zastrzeżonych

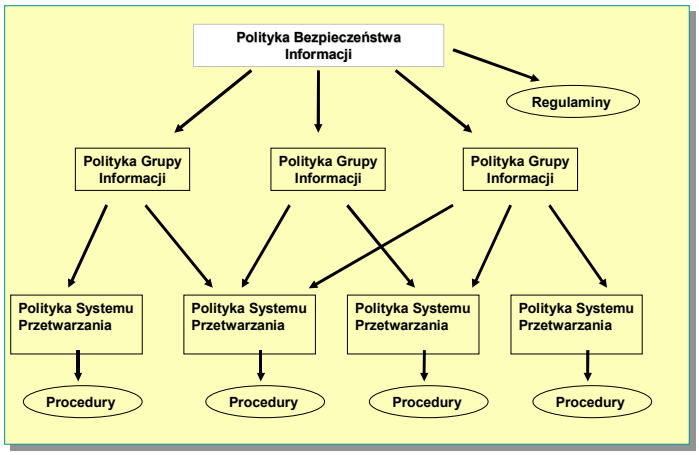
Użytkownikami informacji są wszystkie osoby, które mogą czytać, zmieniać, tworzyć lub kasować informacje zastrzeżone

Struktura zarządzania bezpieczeństwem informacji

Istnieją dwa piony zarządzania informacją - pion administracyjny i pion bezpieczeństwa, na wszystkich poziomach Polityki Bezpieczeństwa

Zbigniew Suski BSI – polityka bezpieczeństwa informacji 23

TISM - hierarchia dokumentów



Zbigniew Suski BSI – polityka bezpieczeństwa informacji 24