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.

Podstawowe zasady opracowywania polityki bezpieczeństwa:

- inicjatywa w zakresie bezpieczeństwa informacji musi wyjść ze strony kierownictwa,
- 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.

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.**

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.**

Schemat postępowania przy opracowywaniu polityki bezpieczeństwa

- **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

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.**

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.

Analiza ryzyka:

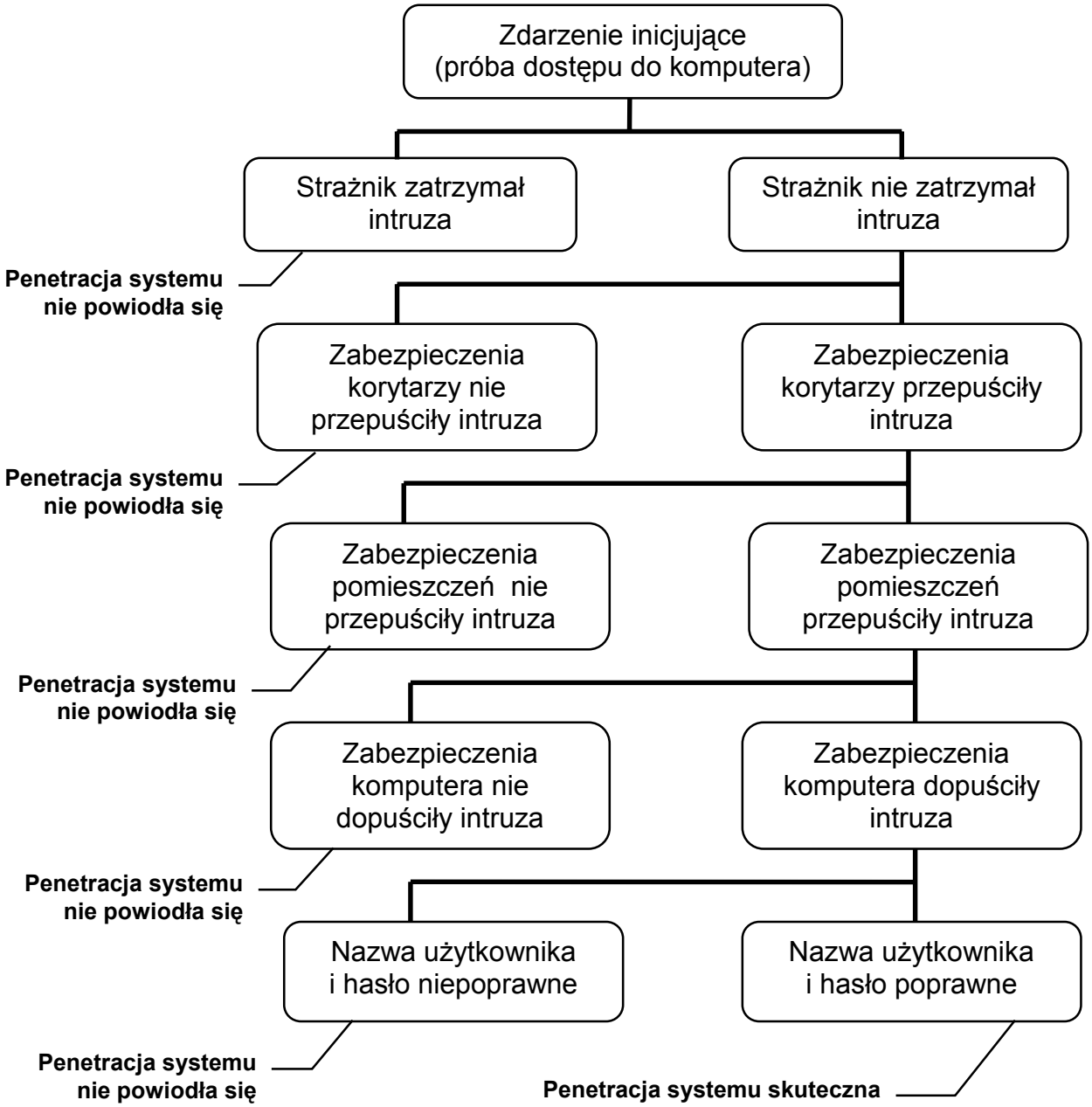
1. **Szacowanie ryzyka:**
   - **Co chronić?**
   - **Przed czym chronić?**
   - **Jakie jest prawdopodobieństwo wystąpienia zagrożenia lub skutków zagrożenia?**
2. **Ocena akceptowalności ryzyka:**
   - **Jaki jest stopień szkodliwości skutków zagrożenia?**
   - **Jakie są koszty zabezpieczeń?**
  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

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.**

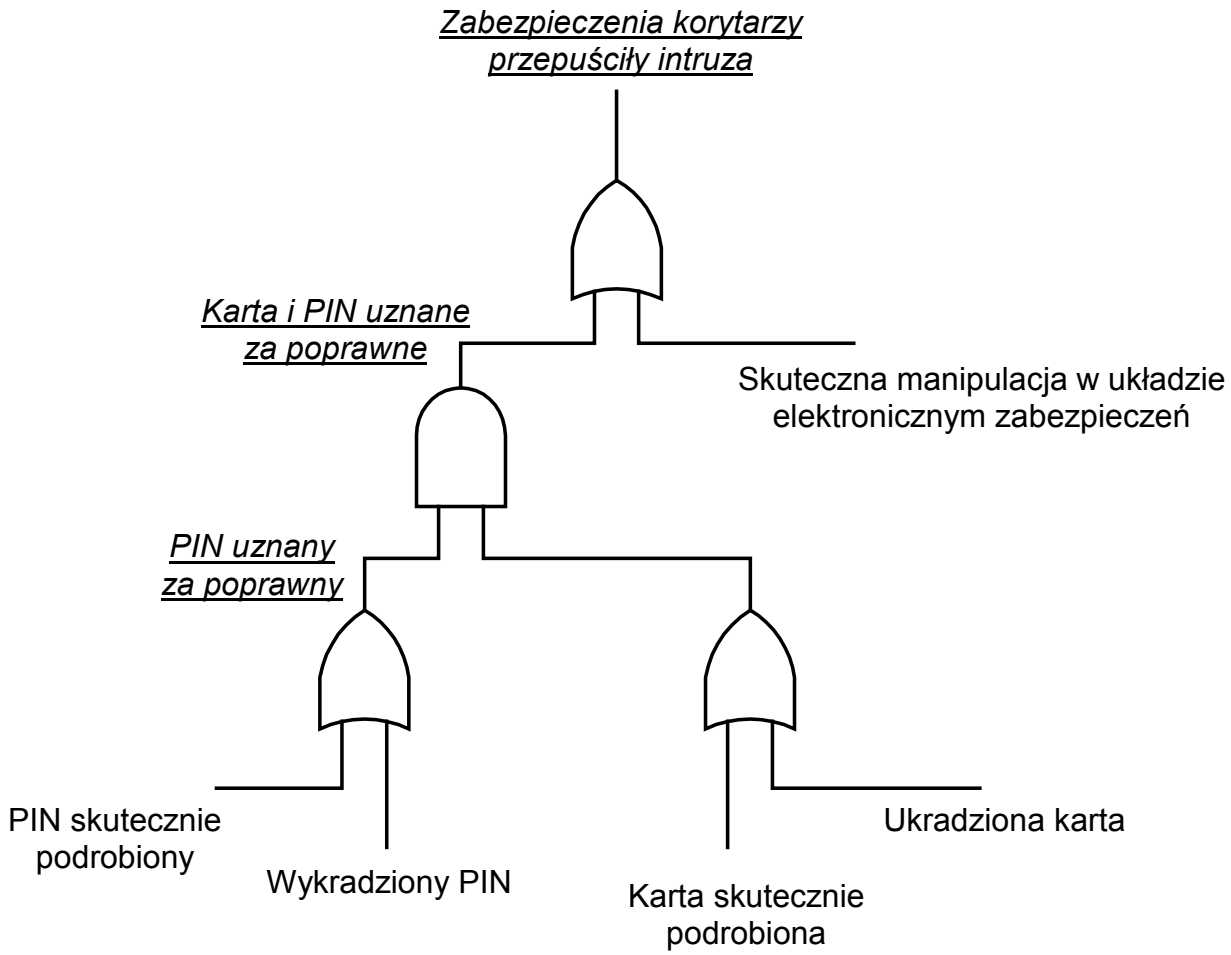
źródło: K.Liderman. *Bezpieczeństwo informacji w systemach komputerowych*

Drzewo zdarzeń dla próby fizycznego dostania się do komputera i uruchomienia sesji.



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

Drzewo błędów dla próby fizycznego dostania się do komputera i uruchomienia sesji.



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

Podstawowe kwestie do rozstrzygnięcia:

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

<u>Plan realizacji przedsięwzięć</u> powinien on zawierać:

- **listę 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.**

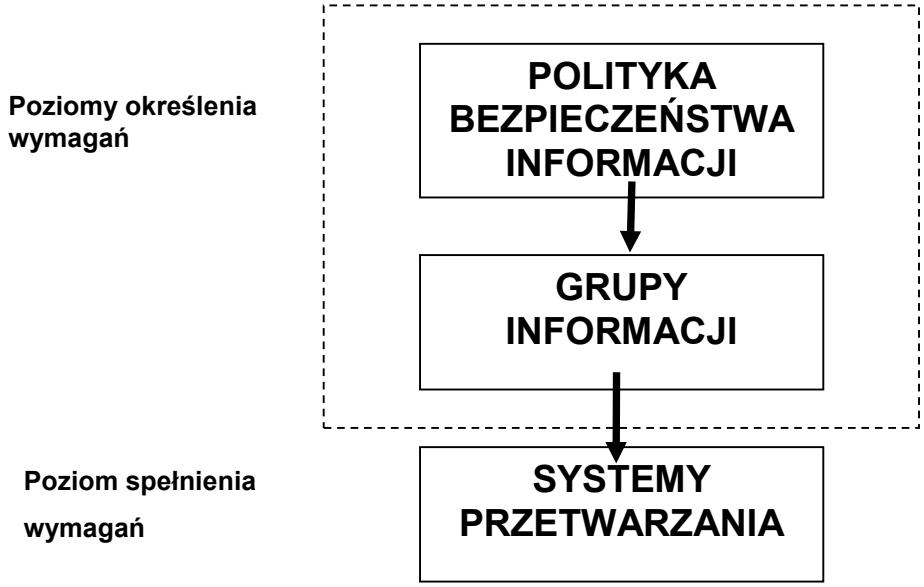
<u>Tematyka szkoleń</u> powinna obejmować:

- **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 powinien zawierać:

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

Struktura polityki bezpieczeństwa wg TISM



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.**

źródło: dokumentacja TISM

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"

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

Główne założenia TISM - *ciąg dalszy*

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

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:

- ***własna 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

Główne założenia TISM - *ciąg dalszy*

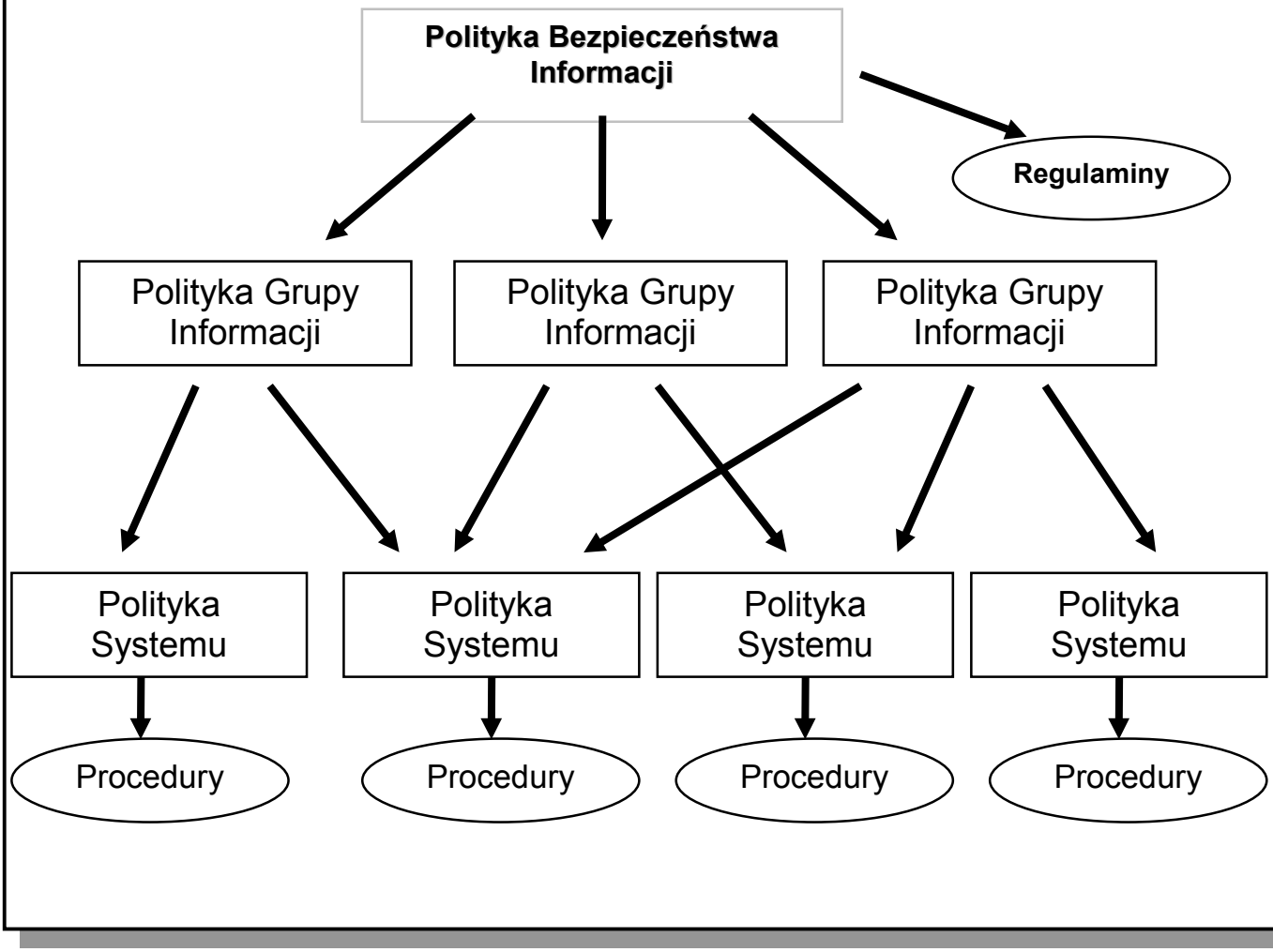
Użytkownicy informacji zastrzeżonych

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

Hierarchia dokumentów wg TISM



Schemat dokumentu Polityki Bezpieczeństwa grupy informacji zastrzeżonych (wg TISM)

1. Cel:

Polityka bezpieczeństwa grupy informacji zastrzeżonych jest wypełnieniem założeń dokumentu głównego Polityki Bezpieczeństwa Informacji w stosunku do danej grupy informacji zastrzeżonych.

2. Zakres

Określenie w stosunku do jakich informacji polityka ma zastosowanie (zdefiniowanie rodzajów i zakresu informacji zastrzeżonych należących do tej grupy).

3. Dostęp do informacji

Określenie poszczególnych ról dostępu do danej grupy informacji.
(spis ról i ich uprawnień)

4. Zarządzanie informacją

Określenie:

1. *Kto jest Administratorem grupy informacji: (imię, nazwisko, stanowisko lub wskazanie odpowiedniej uchwały Zarządu)*
2. *Kto jest Administratorem bezpieczeństwa grupy informacji: / imię, nazwisko, stanowisko lub wskazanie odpowiedniej uchwały Zarządu /*

5. Przetwarzanie informacji

Określenie w jakich systemach mogą być przetwarzane informacje zastrzeżone z tej grupy.
(Spis wszystkich dopuszczonych systemów)

6. Archiwizowanie informacji

Określenie systemu do tworzenia kopii bezpieczeństwa informacji zastrzeżonych należących do tej grupy.

7. Priorytety postępowania w sytuacjach kryzysowych

Określenie priorytetów postępowania w sytuacjach kryzysowych dla tej grupy.

źródło: dokumentacja TISM

Schemat dokumentu Polityki bezpieczeństwa systemu przetwarzania grupy informacji zastrzeżonych

1. Cel

Polityka bezpieczeństwa systemu przetwarzania jest wypełnieniem założeń dokumentu głównego Polityki Bezpieczeństwa Informacji oraz Polityki Bezpieczeństwa danej grupy informacji zastrzeżonych przez system przetwarzania tej grupy informacji zastrzeżonych.

2. Zakres

Określenie w stosunku do jakich elementów systemu oraz osób uczestniczących w systemie polityka ma zastosowanie.

3. Schemat systemu

Opis poszczególnych elementów systemu (schemat, dokumentacja).

4. Kontrola dostępu

Określenie:

1. *Czy system zapewnia, że do informacji zastrzeżonych mają dostęp wyłącznie upoważnione osoby poprzez zaimplementowane systemy:*
   1.1. Ochrony logicznej przy pomocy np. kont i haseł
   1.2. Ochrony fizycznej
2. *Czy system zapewnia, że upoważnione osoby mogą wykonywać wyłącznie dopuszczone operacje?*
3. *Czy wszystkie konta zdefiniowane w systemie mają określony czas ważności?*
4. *Czy wszyscy użytkownicy systemu zapoznali się i podpisali odpowiednie regulaminy użytkownika?*
5. *Czy wszelkie podzespoły, na których mogły być zapisane informacje zastrzeżone są przed opuszczeniem systemu kasowane (naprawa, zniszczenie itp.)?*

5. Integralność

Określenie:

1. *Czy system składa się wyłącznie z dopuszczonych do systemu elementów?*
2. *Czy system przed rozpoczęciem pracy przeszedł pomyślnie kontrolę bezpieczeństwa i jego konfiguracja została zatwierdzona?*
3. *Czy Stan systemu jest przez cały czas eksploatacji pod kontrolą?*
   3.1. Kontrola antywirusowa
   3.2. Kontrola instalacji i wymiany podzespołów i oprogramowania
   3.3. Kontrola integralności oprogramowania

6. Jednoznaczność operacji

Określenie:

1. *Czy system w jednoznaczny sposób umożliwia identyfikację osób, które dokonały zmiany w informacji zastrzeżonej*
2. *W jakiej postaci są dostępne informacje umożliwiające identyfikację osób dokonujących zmian w informacji zastrzeżonej*

źródło: dokumentacja TISM

źródło: dokumentacja TISM

Schemat dokumentu Polityki bezpieczeństwa systemu przetwarzania grupy informacji zastrzeżonych - *ciąg dalszy*

7. Zarządzanie bezpieczeństwem

Określenie:

1. *Czy system posiada mechanizmy pozwalające wykryć próby nieautoryzowanego dostępu do informacji zastrzeżonych lub wykonania nieuprawnionych operacji:*

8. Zarządzanie informacją

Określenie:

1. *Czy system zapewnia integralność danych przez cały czas przechowywania informacji.*
2. *Czy system posiada mechanizmy bezpowrotnego niszczenia informacji*

9. Administrator systemu i administrator bezpieczeństwa systemu

Określenie:

1. *Kto jest Administratorem systemu: /dane personalne lub wskazanie odpowiedniej uchwały Zarządu /*
2. *Kto jest Administratorem bezpieczeństwa systemu: /dane personalne lub wskazanie odpowiedniej uchwały Zarządu /*

10. Okresowe audyty bezpieczeństwa zlecane przez Zarząd firmy

Określenie:

1. *Czy system przechodzi okresowe audyty bezpieczeństwa zlecane przez Zarząd /częstość ich przeprowadzania/*
2. *Gdzie są dostępne dokumenty z okresowych audytów bezpieczeństwa zlecanych przez Zarząd.*

11. Sytuacje kryzysowe

Określenie działań:

1. *Powoływanie sztabu kryzysowego*
2. *Ustalenie działań i przyjęcie priorytetów (w kolejności ważności):*
   - *2.1. Zabezpieczenie informacji przed nieautoryzowanym dostępem*
   - *2.2. Zachowanie ciągłości działania*
   - *2.3. Zabezpieczenie informacji przed utratą*
   - *2.4. Ujęcie sprawców*
3. *Podanie listy stworzonych odpowiednich procedur dla przewidzianych sytuacji kryzysowych, np.:*
   - *3.1. Włamanie do systemu (nieautoryzowany dostęp)*
   - *3.2. Nadużywanie dostępnych praw*
   - *3.3. Następne sytuacje .....*

źródło: dokumentacja TISM

Schemat uniwersalnej procedury zakładania/modyfikacji/usuwania konta dostępu w systemie przetwarzania grup informacji zastrzeżonych[1]

CEL PROCEDURY

Celem niniejszej procedury jest określenie warunków i sposobu zakładania/modyfikacji/usuwania konta w systemie przetwarzania (nazwa)w sposób bezpieczny i kontrolowany, zgodnie z założeniami Polityki Bezpieczeństwa Informacji

WYMAGANIA

Istnienie następujących ról w strukturze firmy:
(Role te są opisane w Dokumencie Głównym Polityki Bezpieczeństwa)

- *Główny Administrator Bezpieczeństwa Informacji (GABI)*
- *Administrator Informacji (AI) dla wszystkich grup informacji przetwarzanych w systemie przetwarzania*
- *Administrator Bezpieczeństwa Informacji (ABI) dla wszystkich grup informacji przetwarzanych w systemie przetwarzania*
- *Administrator Bezpieczeństwa Systemu (ABS) systemu przetwarzania*

ZAKRES STOSOWANIA

Pracownicy działu (nazwa) firmy (nazwa)

OPIS

Procedura ma zapewnić, że zakładanie/modyfikacja/usuwanie konta w systemie przetwarzania (nazwa) odbywać się będzie w sposób zgodny z Polityką Bezpieczeństwa Informacji firmy (nazwa)

WEJŚCIE

Właściwie wypełniony wniosek (tzw.WZMUK) o założenie/modyfikację/usunięcie atrybutów konta w systemie przetwarzania(nazwa)

WYJŚCIE

Założone/zmodyfikowane/usunięte konto w systemie przetwarzania (nazwa)

STANDARD

Formularz „WZMUK”
„Wykaz praw dostępu do informacji”
Standard Przesyłania Haseł - Standardy
Rejestr Użytkowników Grupy Informacji - Standardy
Rejestr Użytkowników Systemu Przetwarzania – Standardy
Księga podpisów i pieczęci – Standardy
Standard Komunikacji miedzy AI, ABI, ABS, GABI – Standardy

PROCES

1. *Sprawdzić autentyczność podpisów ABI w Księdze Podpisów i Pieczęci*
   - *1.1. W przypadku braku zgodności skontaktować się osobiście z ABI w celu wyjaśnienia niezgodności.*
2. *Dokonać modyfikacji konta zgodnie z wytycznymi w „WZMUK” otrzymanym od ABI.*

KONIEC PROCEDURY

źródło: dokumentacja TISM

Literatura:

1. S. Garfinkel, G.Spafford. *Practical Unix and Internet Security.* O'Reilly & Associates 1996 (*tłum*. RM 1997).
2. V. Ahuja. *Network & Internet Security.* Academic Press 1996 (*tłum*. MIKOM 1997).
3. D. Atkins. *Internet Security: Professional Reference.* New Riders Publishing 1997 (*tłum*. LT&P 1997).
4. T. Kifner. *Polityka bezpieczeństwa i ochrony informacji*. Helion, Gliwice 1999.
5. L. Klander. *Hacker Proof*. Jamsa Press, 1997 (*tłum.* MIKOM 1998).
6. K. Liderman. *Bezpieczeństwo informacji w systemach komputerowych,* WAT Warszawa 1999.
7. *Total Information Security Management (TISM*), European Network Security Institute, Warszawa 2000. (www.ensi.net).