# Bezpieczeństwo systemów informatycznych - wstęp

*Materiały pomocnicze do wykładu*

**Bezpieczeństwo systemów informatycznych**

Pojęcia wstępne



## Literatura podstawowa

- **D. R. Ahmad i inni, *Hack Proofing Your Network*, Syngress Publishing Inc. 2002 (*tłum. Helion 2002 – pod tym samym tytułem).***
- **E. Amoroso. *Intrusion Detection.* AT&T Inc. 1999 (*tłum. RM 1999 - Wykrywanie intruzów).***
- **J. Scambray, S. McClure, G. Kurtz. *Hacking Exposed* McGraw-Hill 2001 (*tłum. Translator 2001 - Hakerzy - cała prawda).***
- ***M.* Strebe, Ch. Perkins. *Firewalls*. SYBEX Inc. 2000 (*tłum. MIKOM 2000 - Firewalls - ściany ogniowe).***



## Literatura dodatkowa

- **V. Ahuja. *Network & Internet Security.* Academic Press, Inc, 1996. (*tłum. MIKOM 1997 – Bezpieczeństwo w sieciach*).**
- **D. Atkins i inni. *Internet Security. Professional Reference.* New Riders Publishing, 1997 (*tłum. LT&P 1997 – Bezpieczeństwo Internetu*).**
- **S. Garfinkel, G. Spafford. *Practical Unix and Internet Security,* O'Reilly&Associates Inc. 1996. (*tłum. RM 1997 – Bezpieczeństwo w Unixie i Internecie*).**
- **M. Kaeo, *Designing Network Security,* CISCO Press 1999 (*tłum. MIKOM 2000 – Tworzenie bezpiecznych sieci).***
- **T. Kifner. *Polityka bezpieczeństwa i ochrony informacji.* Helion 1999.**
- **L. Klander. *Hacker Proof.* Jamsa Press, 1997. (*tłum. MIKOM 1998*).**
- **K. Liderman, *Bezpieczeństwo teleinformatyczne,* IAiR WAT 2001.**
- ***W.* Stallings, *Network and Internetwork Security Principles and Practice,* Prentice Hall 1994 (*tłum. WNT 1997 – Ochrona danych w sieci i intersieci w teorii i praktyce).***



## Zaliczenie ćwiczeń

Każdy student otrzymuje wstępnie 12 punktów kredytowych. Za każdą nieobecność na ćwiczeniach lub nie zaliczone ćwiczenie traci z tej puli 1 punkt. Na zakończenie ćwiczeń przeprowadzony zostanie sprawdzian z materiału będącego przedmiotem ćwiczeń. Można na nim uzyskać 10 punktów.

Ocena zaliczeniowa z ćwiczeń wynika bezpośrednio z ilości zdobytych punktów (sumy zachowanych punktów kredytowych i uzyskanych ze sprawdzianu):

dst : ( 12, 14 >
dst+: ( 14, 16 >
db : ( 16, 18 >
db+ : ( 18, 20 >
bdb : ( 20, 22 >



## Egzamin

Egzamin jest realizowany w formie testu zawierającego 25 pytań. Oceny:

dst : < 13, 14 >
dst+ : < 15, 16 >
db : < 17, 19 >
db+ : < 20, 22 >
bdb : < 23, 25 >

Za dobre i bardzo dobre wyniki uzyskane w trakcie ćwiczeń studenci uzyskują premię punktową na egzaminie wg reguły:

ocena bdb na zaliczeniu ćwiczeń: +5 pkt,
ocena db+ na zaliczeniu ćwiczeń: +3 pkt,
ocena db na zaliczeniu ćwiczeń: +2 pkt.

## Bezpieczeństwo

- Komputer jest bezpieczny, jeżeli jego użytkownik może na nim polegać, a zainstalowane oprogramowanie działa zgodnie ze stawianymi mu oczekiwaniami.

  *S. Garfinkel*
  *Bezpieczeństwo w Unixie i Internecie*

- Zaufanie:
  ufamy, że system będzie przechowywał i chronił nasze dane

- Kradzież informacji następuje w sposób ciągły i niewidoczny!



## Badania FBI i CSI (*Computer Security Institute*)

- 41% badanych potwierdziło włamanie do ich sieci lub użycie zasobów sieci przez niepowołane osoby;
- 37% stanowiły instytucje medyczne, a 21% instytucje finansowe.
- 50% ataków to szpiegostwo gospodarcze (wykradanie informacji biznesowych od konkurencji);
- 50% badanych nie miało opracowanej Polityki Bezpieczeństwa ochrony informacji ( z pozostałych 50% posiadających zasady ochrony informacji, aż połowa nie stosowała się do nich);
- 20% badanych nie wiedziało czy zostały zaatakowane czy też nie!



## Badania *Ernst&Young*

- 54% badanych firm poniosło straty w wyniku włamań;
- 78% firm odnotowało straty z powodu wirusów komputerowych;
- 42% firm odnotowało niszczące ataki z zewnątrz (destabilizacja systemu jest gorsza w skutkach niż samo włamanie do niego);
- 25% firm straciło w wyniku włamań ponad 250 tys. dolarów, a 15% ponad 1 mln dolarów.



## Wojna informatyczna

Określa techniki ataku na systemy komputerowe stosowane przez hakerów, szpiegów, terrorystów, wywiad wojskowy.



## Haker (hacker)

- Osoba, której sprawia przyjemność poznawanie szczegółowej wiedzy na temat systemów komputerowych i rozszerzanie tej umiejętności, w przeciwieństwie do większości użytkowników komputerów, którzy wolą nauczyć się niezbędnego minimum.
- Osoba, która entuzjastycznie zajmuje się oprogramowaniem i nie lubi teorii dotyczącej tej dziedziny.

*Guy L.Steele i inni – The Hacker's Dictionary*



## Kategorie bezpieczeństwa

- **Poufność** (*confidentiality*) – ochrona danych przed odczytem i kopiowaniem przez osobę nieupoważnioną. Jest to ochrona nie tylko całości danych, ale również ich fragmentów.
- **Spójność danych** (*integrity*) – ochrona informacji (również programów) przed usunięciem lub jakimikolwiek nieuprawnionymi zmianami. Np. zapisy systemu rozliczania, kopie zapasowe, atrybuty plików.
- **Dostępność** (*availability*) – ochrona świadczonych usług przed zniekształceniem i uszkodzeniem.

## Pomarańczowa Księga (*Orange Book*)

*Trusted Computer System Evaluation Criteria (TCSEC)*

- D - Ochrona minimalna (*Minimal Protection*)
- C1 - Ochrona uznaniowa (*Discretionary Protection*)
- C2 - Ochrona z kontrolą dostępu (*Controlled Access Protection*)
- B1 - Ochrona z etykietowaniem (*Labeled Security Protection*)
- B2 - Ochrona strukturalna (*Structured Protection*)
- B3 - Ochrona przez podział (*Security Domains*)
- A1 - Konstrukcja zweryfikowana (*Verified Design*)



## Inne „*kolorowe*" publikacje

Czerwona Księga
*Trusted Networking Interpretation*

zawiera kryteria oceny bezpieczeństwa sieci komputerowych

Zielona Księga
*Password Management Guideline*

zawiera wytyczne dotyczące stosowania i wykorzystania haseł



## Historia

- 1983 *Trusted Computer System Evaluation Criteria TCSEC - "Orange Book"*
- 1990 powołanie zespołu w ramach ISO
- 1991 *Information Technology Security Evaluation Criteria v. 1.2 (ITSEC)* (Francja, Niemcy, Holandia, Wielka Brytania)
- 1993 *Canadian Trusted Computer Product Evaluation Criteria v. 3.0 (CTCPEC)* łączący cechy ITSEC i TCSEC (Kanada)
- 1993 *Federal Criteria for Information Technology Security v. 1.0* (*FC*) (USA)



## Historia cd

- 1993 organizacje, które opracowały CTCPEC, FC, TCSEC, ITSEC podjęły wspólną pracę w ramach projektu o nazwie *Common Criteria* (*CC*) mającego na celu połączeniu ww. standardów.
- 1996 aprobata ISO dla wersji 1.0 CC (*Committee Draft*)
- 1997 wersja *beta* CC v. 2.0 - podstawa do opracowania normy ISO/IEC 15408 o nazwie *Evaluation Criteria for Information Technology Security.*
- 1998 podpisanie umowy o wzajemnym uznawaniu certyfikatów bezpieczeństwa wydawanych na podstawie CC.



## Historia cd

- 2000 Norma ISO/IEC 17799 :*2000 Code of Practice for Information Security Management* (Praktyczne zasady zarządzania bezpieczeństwem informacji)
- 2001 Raport techniczny ISO/IEC 13335TR

  PN-I 13335-1- Wytyczne do zarządzania bezpieczeństwem systemów informatycznych: terminologia, związki między pojęciami, podstawowe modele



## *Common Criteria*

- CC mają na celu wprowadzenie ujednoliconego sposobu oceny systemów informatycznych pod względem bezpieczeństwa. Określają co należy zrobić, aby osiągnąć zadany cel ale nie określają jak to zrobić.
- CC są katalogiem schematów konstrukcji wymagań związanych z ochroną informacji.
- CC odnoszą się do produktów programowych i sprzętowych.
- CC nie zalecają ani nie wspierają żadnej znanej metodyki projektowania i wytwarzania systemów.

## *Common Criteria*

**Wynikiem oceny jest dokument stwierdzający:**

- **zgodność produktu z określonym profilem ochrony lub,**
- **spełnienie określonych wymagań bezpieczeństwa lub,**
- **przypisanie do konkretnego poziomu bezpieczeństwa (*Evaluation Assurance Level*).**

Zbigniew Suski BSI - wstęp 18

## Norma ISO/IEC 17799

***2000 Code of Practice for Information Security Management***

- **Standard od grudnia 2000**
- **Dotyczy zarządzania a nie techniki**
- **Powinna być modyfikowana do lokalnych warunków**
- **Zawiera wymagania minimalne, uzgodnione w długiej drodze tworzenia normy, w wielu organizacjach mogą się okazać niewystarczające**
- **Będzie standardem w Polsce w 2003 roku**

Zbigniew Suski BSI - wstęp 19

## Norma ISO/IEC 17799

- **Rozdział 3 Polityka**
  ***zaangażowanie kierownictwa, wskazanie kierunków działania***
- **Rozdział 4 Działania organizacyjne**
  ***przemyślana, sprzyjająca celom struktura organizacyjna, współdziałanie i doskonalenie***
- **Rozdział 5 Klasyfikacja i kontrola zasobów**
  ***świadomość, co należy chronić i gdzie to jest***
- **Rozdział 6 Personel**
  ***świadomość, umiejętności, szkolenie***

Zbigniew Suski BSI - wstęp 20

## Norma ISO/IEC 17799

- **Rozdział 7 Zabezpieczenie fizyczne organizacji i otoczenia**
  ***ochrona fizyczna organizacji i jej otoczenia***
- **Rozdział 8 Zarządzanie działaniem urządzeń**
  ***sprawność działania urządzeń i usług***
- **Rozdział 9 Kontrola dostępu do informacji**
  ***uniemożliwienie dostępu do informacji przez osoby nieuprawnione, monitorowanie***
- **Rozdział 10 Opracowywanie i utrzymywanie systemów informatycznych**
  ***działanie w sytuacji zmian w oprogramowaniu***

Zbigniew Suski BSI - wstęp 21

## Norma ISO/IEC 17799

- **Rozdział 11 Zarządzanie ciągłością biznesu**
  ***działanie w sytuacjach awaryjnych***
- **Rozdział 12 Przestrzeganie**
  ***przestrzeganie przepisów prawa i ustalonych procedur***

Zbigniew Suski BSI - wstęp 22

## Raport techniczny ISO/IEC 13335TR

**PN-I 13335-1- Wytyczne do zarządzania bezpieczeństwem systemów informatycznych: terminologia, związki między pojęciami, podstawowe modele**

Zbigniew Suski BSI - wstęp 23

## Regulacje prawne w Polsce

- Ustawa z dn. 22.01.1999 ***O ochronie informacji niejawnych***. Dz. U. z dn. 8.02.1999.
- Ustawa z dn. 29.08.1997 ***O ochronie danych osobowych***. Dz. U. z dn. 29.10.1997.
- Rozporządzenie Prezesa Rady Ministrów z dn. 25.02.1999 ***W sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych***. Dz. U. z dn. 5.03.1999.
- Rozporządzenie MSWiA z dn. 3.06.1998 ***W sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych***. Dz. U. z dn. 30.06.1998.



## Kodeks Karny

**Art. 115.**

**Dokumentem jest każdy przedmiot lub zapis na komputerowym nośniku informacji, .**

**Art. 165.**

**Kto sprowadza niebezpieczeństwo dla życia lub zdrowia wielu osób albo dla mienia zakłócając, uniemożliwiając lub w inny sposób wpływając na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.**



## Kodeks Karny

**Art. 267.**

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



## Kodeks Karny

**Art. 268.**

**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 karze pozbawienia wolności do lat 2. Jeżeli czyn ten dotyczy zapisu na komputerowym nośniku informacji sprawca podlega karze pozbawienia wolności do lat 3.**



## Kodeks Karny

**Art. 269.**

**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 organizacji samorządowej albo zakłóca lub uniemożliwia automatyczne gromadzenie lub przekazywanie takich informacji, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.**

**Tej samej karze podlega, kto dopuszcza się takiego czynu, niszcząc albo wymieniając nośnik informacji lub niszcząc albo uszkadzając urządzenie służące automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji.**



## Kodeks Karny

**Art. 278.**

**Kto, bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy w celu osiągnięcia korzyści majątkowej podlega karze pozbawienia wolności od 3 miesięcy do lat 5.**

**Art. 287.**

**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.**

## Kodeks Karny

**Art. 292.**

**Kto, rzecz, o której na podstawie towarzyszących okoliczności powinien i może przypuszczać, że została uzyskana za pomocą czynu zabronionego, nabywa lub pomaga do jej zbycia albo tę rzecz przyjmuje lub pomaga do jej ukrycia, podlega grzywnie, karze ograniczenia wolności albo karze pozbawienia wolności do lat 2 (na mocy Art. 293. §1. przepis ten stosuje się również do programów komputerowych).**



## Ogólne zasady bezpieczeństwa

- **Skuteczność zabezpieczeń zależy od ludzi. Żaden system bezpieczeństwa nie obroni systemu informatycznego, jeżeli człowiek zawiedzie zaufanie.**
- **Nie ma bezwzględnej miary bezpieczeństwa. Poziom bezpieczeństwa można mierzyć tylko w odniesieniu do precyzyjnie określonych w tym zakresie wymagań stawianych systemowi.**
- **Nie istnieje żaden algorytm, który dla dowolnego systemu ochrony mógłby określić, czy dana konfiguracja jest bezpieczna.**
- **System bezpieczeństwa musi być systemem spójnym, tzn. muszą być stosowane łącznie różne metody ochrony, inaczej system bezpieczeństwa będzie posiadał luki.**



## Programowo-sprzętowe metody ochrony

- **stosowanie określonych procedur wytwarzania oprogramowania i sprzętu,**
- **stosowanie odpowiedniego oprogramowania systemowego i dodatkowego,**
- **stosowanie odpowiednich konfiguracji sprzętowych (UPS, nadmiarowość konfiguracji),**
- **stosowanie mechanizmów składowania,**
- **szyfrowanie informacji.**



## Metody ochrony fizycznej

- **Kontrola dostępu do obiektów i pomieszczeń**
- **Zabezpieczenie przeciw włamaniom**
- **Systemy przeciwpożarowe**

**Ma na celu:**

- **uniemożliwienie dostępu osobom niepowołanym,**
- **wykrycie i zapobieżenie rozprzestrzenianiu się ognia i wody,**
- **zapobieganie skutkom przerw w dostawach energii elektrycznej.**



## Urządzenia fizycznej kontroli dostępu

- **bariery mikrofalowe,**
- **bariery podczerwieni,**
- **systemy radarowe,**
- **wykrywacze zakłóceń w światłowodach**
- **sensory wibracyjne**
- **podsystemy włamania i napadu**
- **sygnalizatory pożaru i zalania**
- **systemy telewizji przemysłowej**
- **podsystemy kontroli dostępu**



## Organizacyjne metody ochrony

- **Regulaminy dla osób korzystających z systemów informatycznych**
- **Polityka bezpieczeństwa**
- **Polityka zakupu sprzętu i oprogramowania**

- **ISO 9001 - Model zapewnienia jakości w projektowaniu, pracach rozwojowych, produkcji, instalowaniu i serwisie.**
- **ISO 9002 - Model zapewnienia jakości w produkcji, instalowaniu i serwisie.**
- **ISO 9003 - Model zapewnienia jakości w kontrolach i badaniach końcowych**

## Wykładnia ISO dla wytwarzania oprogramowania

- **ISO 9000-3**

  ***Guideline for the application of ISO 9001 to the development, supplay and maintenance of software***

- **PN-ISO 9000-3**

  **Wytyczne do stosowania normy ISO 9001 podczas opracowywania, dostarczania i obsługiwania oprogramowania**



## Kadrowe metody ochrony

- **Sprawdzanie pracowników dopuszczonych do danych o szczególnym znaczeniu**
- **Przestrzeganie odpowiednich procedur zwalniania i zatrudniania pracowników,**
- **Motywowanie pracowników,**
- **Szkolenia.**



## Zasady ustalania zakresu obowiązków

- **Zasada wiedzy koniecznej - prawa muszą wynikać z obowiązków (nic więcej).**
- **Zasada minimalnego środowiska pracy - prawo dostępu tylko do pomieszczeń związanych z obowiązkami.**
- **Zasada dwóch osób - funkcje, które mogą być wykorzystane do złamania zabezpieczeń, należy podzielić a ich wykonanie przydzielić różnym osobom.**
- **Zasada rotacji obowiązków - szczególnie odpowiedzialne funkcje powinny podlegać rotacji.**