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

HACKER –

1. **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.**
2. **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. Niemożność skorzystania z systemu często daje taki sam efekt jak utrata danych.

Prawidłowość (*corretness*) – zapewnienie pracy systemu zgodnej z oczekiwaniami użytkowników. Dotyczy sprzętu i oprogramowania. Można to uważać za *prawidłowość danych i programów*.

Trusted Computer System Evaluation Criteria (TCSEC) - "Orange Book"

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)***

Czerwona Księga
Trusted Networking Interpretation
zawiera kryteria oceny bezpieczeństwa sieci komputerowych

Zielona Księga
Password Management Guideline
zawiera wytyczne dotyczące stosowania i wykorzystania haseł

Historia powstawania kryteriów oceny zabezpieczeń

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 i 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)

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 pomiędzy organizacjami z państw uczestniczących w projekcie CC, certyfikującymi produkty informatyczne, o wzajemnym uznawaniu certyfikatów bezpieczeństwa wydawanych na podstawie CC.

Charakterystyczne cechy zaleceń sformułowanych w *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.**
- **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 - EAL*).**

Struktura *Common Criteria*

Introduction and General Model

Security Functional Requirements

Security Assurance Requirements

W trakcie opracowywania znajduje się uzupełnienie CC w postaci ***Common Evaluation Methodology* (CEM)**, które ma stanowić zbiór metodyk prowadzenia procesu oceny.

Regulacje prawne w Polsce

1. Ustawa z dn. 22.01.1999 ***O ochronie informacji niejawnych***. Dz. U. z dn. 8.02.1999.
2. Ustawa z dn. 29.08.1997 ***O ochronie danych osobowych***. Dz. U. z dn. 29.10.1997.
3. 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.
4. 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 a przestępczość komputerowa :

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.

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.

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 a przestępczość komputerowa :

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.

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.

Art. 291.
Kto, rzecz uzyskaną za pomocą czynu zabronionego, nabywa lub pomaga do jej zbycia albo te rzecz przyjmuje lub pomaga do jej ukrycia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5 (na mocy Art. 293. §1. przepis ten stosuje się również do programów komputerowych).

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.**

Podsystemy i urządzenia:

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.**

Wytwarzanie sprzętu i oprogramowania wysokiej jakości może być jedną z metod podniesienia bezpieczeństwa informacji

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**

Zalecenia i normy ISO zawierają wymagania odnośnie różnych aspektów *zarządzania,* a nie wymagania na produkt. Specyfikują *co* należy zrobić ale nie mówią *jak* to zrobić.

Kadrowe metody ochrony:

- **sprawdzanie pracowników dopuszczonych do danych o szczególnym znaczeniu,**
- **przestrzeganie odpowiednich procedur zwalniania i zatrudniania pracowników,**
- **motywowanie pracowników,**
- **szkolenia.**

Zasady obowiązujące przy ustalaniu 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.**