






Bezpieczeństwo Systemów Informatycznych

dr inż. Michał Szychowiak






<https://www.cs.put.poznan.pl/mszychowiak>



Literatura podstawowa

-  William Stallings, Lawrie Brown, "Computer Security: Principles and Practice", IV ed., Pearson Education, 2018
-  William Stallings, Lawrie Brown, „Bezpieczeństwo systemów informatycznych. Zasady i praktyka”, wyd. IV, Helion, 2019
-  John Vacca, "Computer and Information Security Handbook", Morgan-Kaufmann, 2017
-  Mark Rhodes-Ousley, "Information Security. The Complete Reference", McGraw-Hill, 2013
-  Mark Stamp, "Information Security: Principles and Practice", Wiley, 2011

Literatura uzupełniająca

-  William Stallings, "Cryptography and Network Security: Principles and Practice", VII ed., Pearson Education, 2017
-  Bruce Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C", Wiley, (2015)
-  Niels Ferguson, Bruce Schneier, "Cryptography Engineering", Wiley, 2010
-  Czesław Kościelny, Mirosław Kurkowski, Marian Srebrny, "Modern Cryptography Primer", Springer-Verlag, 2013
-  Christof Paar, Jan Pelzl, "Understanding Cryptography", Springer-Verlag, 2010
- ...

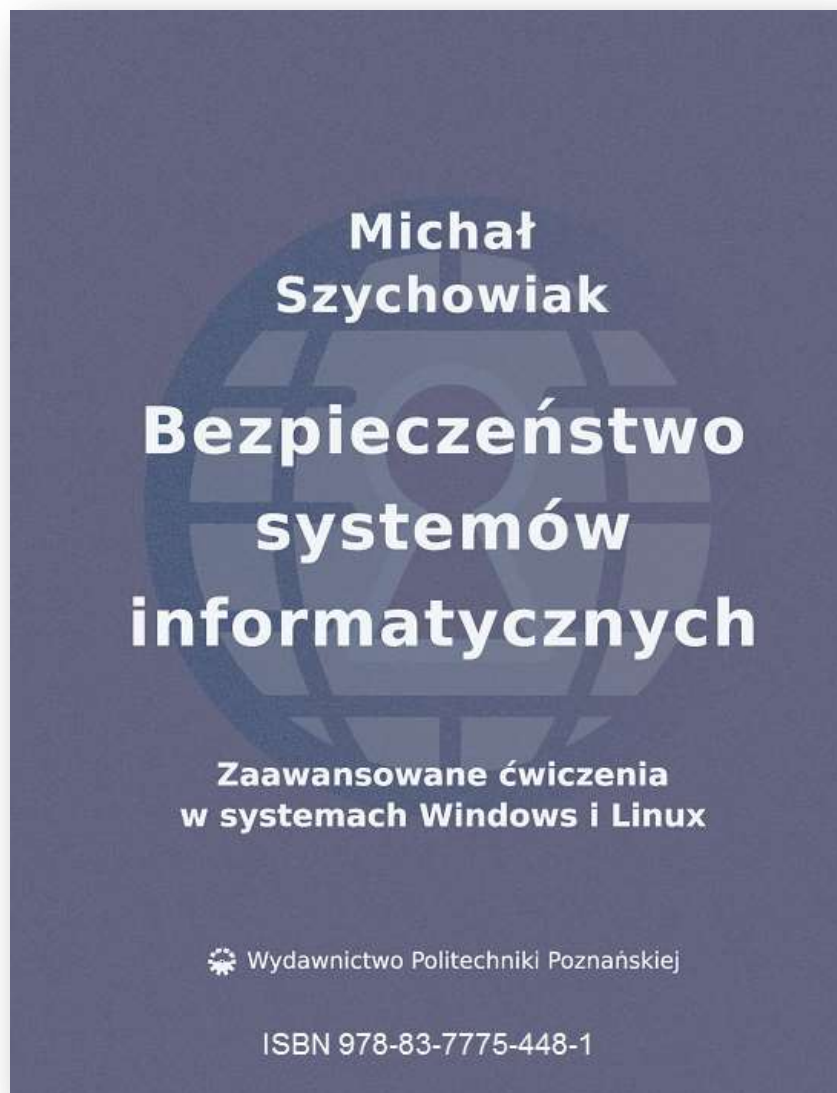
“the world was full of bad security systems designed by people who read *Applied Cryptography* [...] the weak points had nothing to do with the mathematics [...] Beautiful pieces of mathematics were made irrelevant through bad programming”.

Bruce Schneier

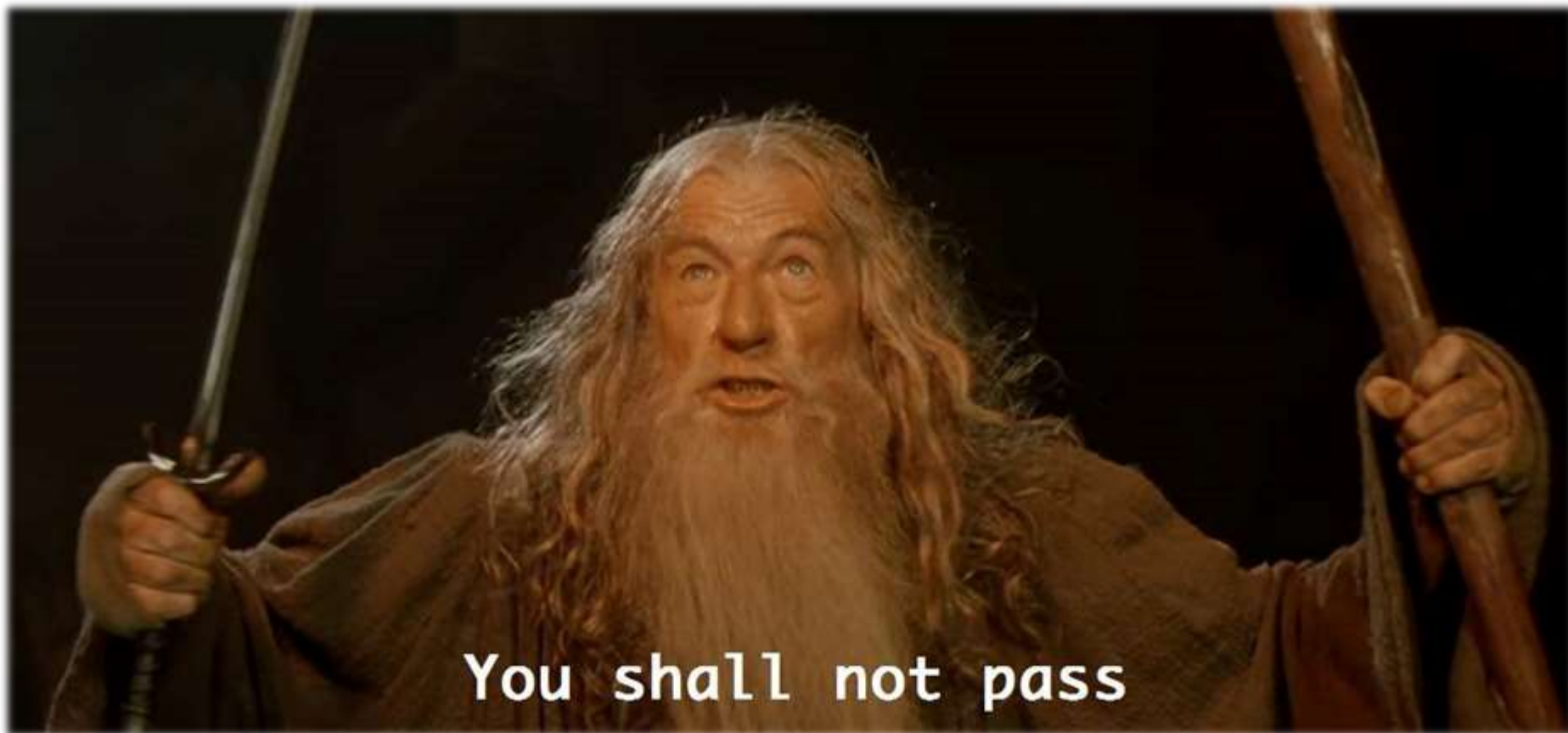


Literatura uzupełniająca

Laboratoria



Egzamin



Co to jest bezpieczeństwo?

Def.: **System informatyczny jest bezpieczny**, jeśli jego użytkownik może na nim polegać, a zainstalowane oprogramowanie działa zgodnie ze swoją specyfikacją.

Simson Garfinkel, Gene Spafford

Practical Unix and Internet Security

Możemy mówić, że system jest bezpieczny, jeśli np. zawsze można od niego oczekiwać, że wprowadzone dziś na stałe dane będą w nim jeszcze za tydzień, nie ulegną zniekształceniu i nie zostaną odczytane przez nikogo nieuprawnionego – ufamy, że system będzie przechowywał i chronił dane.

Wiarygodność

System wiarygodny =

bezpieczny (*secure*) = zapewniający ochronę danych



niezawodny (*reliable*) = odporny na awarie

dostępny (*available*) = dostępny na bieżąco

bezpieczny (*safe*) = bezpieczny dla otoczenia, przyjazny dla środowiska



Realne zagrożenia?

	Targeted Attacks	> 30,000
	New Malware	> 80 Million
	Web Attacks	~ 70 Million
	Identities Exposed	~ 200 Million
	Attacks Blocked	~ 2.4 Trillion



Zagrożenia

Zaciekła konkurencja

- w 1997 r. CIWARS (Centre for Infrastructural Warfare Studies) odnotował 2 incydenty (w Brazylii i w Australii), w których wzajemnie się zaatakowały (SYN flood) konkurujące ze sobą firmy ISP
- w 2009 r. malware SpyEye zwalcza wcześniejsze infekcje konkurenta Zeus
- w 2015 r. Poseidon group atakuje włoski Hacking Team i wykrada ich exploity

Hacktivity

Defacement:

- w 1997 r. grupa Damage Inc. zastąpiła witrynę Urzędu Rady Ministrów RP stroną proklamującą utworzenie Hackrepubliki Polskiej i Centrum Dezinformacyjnego Rządu z odsyłaczami do playboy.com



Zagrożenia

Cyberprzestępczość / cyberterroryzm

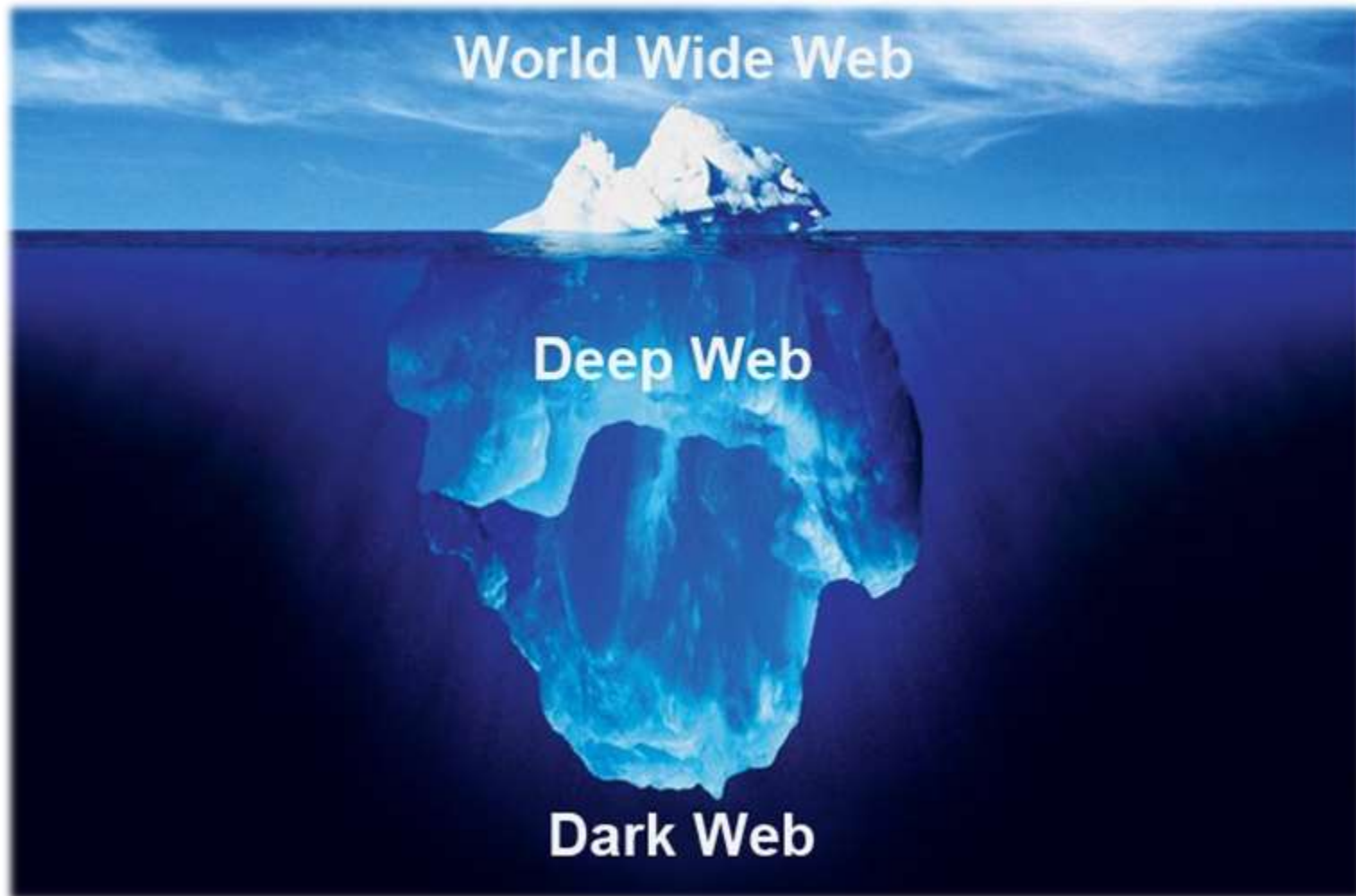
Targeted Attacks:

- 2014: Sony Picture Entertainment
- 2015: największa seria "skoków" na banki: ponad 1 mld USD, 100 banków w 30 krajach
- 2016: DynCyber Attack: Twitter, Netflix, Airbnb, Reddit, SoundCloud, ...
- ...

Advanced Persistent Threats (APT):

- 2010-13: sieć rządowa w Pakistanie
- 2013-14: Ukraina (CyberBerkut)
- 2016-17: <https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity>
- ...

Zagrożenia



Zagrożenia

Cybercrime-as-a-Service:

Usługa	Cena
Kradzione dane karty płatniczej	od kilku zł
Kradziony dostęp do konta bankowego	od kilkudziesięciu zł
Wysłanie miliona wiadomości spam	od kilkudziesięciu zł
Atak DoS	od kilkudziesięciu zł za 1 godzinę
Wynajęcie botnetu	od ok. 200 zł za 1 dzień
Oprogramowanie do ataku ransomware	od ok. 4000 zł za miesiąc
Przejęcie strony internetowej	od kilku zł
Dostęp do konta premium w serwisie streamingu filmów	kilka zł

wg. PTI "Bezpieczeństwo danych w sektorze publicznym"

Zagrożenia

Cybercrime-as-a-Service:

Please enter the amount you wish to purchase below and fill in the form.
(BTC value updates periodically via BTPAY)



USA VISA CREDIT CARD BALANCE \$2,000

Accepted at ATM worldwide
\$500 daily withdraw limit

\$90 (0.4001 BTC)

amount



USA VISA CREDIT CARD BALANCE \$5,000

Accepted at ATM worldwide
\$1,000 daily withdraw limit

\$170 (0.7557 BTC)

amount



EU VISA CREDIT CARD BALANCE €5,000

Accepted at ATM worldwide
€1,000 daily withdraw limit

\$210 (0.9335 BTC)

amount

Zagrożenia

Cybercrime-as-a-Service:

We get new lists every day!

80%+ working guarantee, we will replace if more than 20% dont work!

Product	Price	Quantity
100 PayPal accounts	100 USD = 0.434 ₿	<input type="text" value="1"/> X Buy now
100 Ebay accounts	100 USD = 0.434 ₿	<input type="text" value="1"/> X Buy now
100 CCs with CVV2	150 USD = 0.652 ₿	<input type="text" value="1"/> X Buy now

Zagrożenia



Cybercrime-as-a-Service:


ASSASSIN's COMMUNITY KILLERS LIST ABOUT INFO CONTACT Logout

SELECT VICTIM's LOCATION:

Europe • North America • Asia • South America • Australia • Africa

EUROPE

5000 € / person **HIRE**



Blacklord

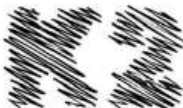
Confirmed Victims: (100+)

Age	16+
Gender	ANY
Extended Suffering	+
Photo/Video	+
CONTINENT	EUROPE, ASIA, AFRICA

POLITICIANS

(TOP-10)	-
----------	---

7500 € / person **HIRE**



K2


Confirmed Victims: (70+)

Age	20+
Gender	ANY
Extended Suffering	+
Photo/Video	+
CONTINENT	EUROPE, ASIA, AFRICA

POLITICIANS

(TOP-10)	-
----------	---

3000 € / person **HIRE**



HITMAN


Confirmed Victims: (70+)

Age	ANY
Gender	ANY
Extended Suffering	+
Photo/Video	+
CONTINENT	EUROPE, ASIA

POLITICIANS

(TOP-10)	-
----------	---

10000 € / person **HIRE**



Rodger D.

Confirmed Victims: (20+)

Age	16+
Gender	ANY
Extended Suffering	+
Photo/Video	+
CONTINENT	EUROPE, ASIA

POLITICIANS

(TOP-10)	-
----------	---





FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

- iOS
- Android
- Any OS



© dr inż. Michał Szychowiak, 2022

Hacker?

A photograph of a street sign for "Hackerstraße". The sign is rectangular with a dark border and a light background. The word "Hackerstraße" is written in large, bold, black letters. Below it, there is a small orange rectangular sticker with the text "FREE KEVIN" in black capital letters. The sign is mounted on a black metal pole. In the background, there are green trees and a building.

Hackerstraße

FREE KEVIN

8 - 7

Hacker?

Def: HACKER



1. 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;
2. osoba, która entuzjastycznie zajmuje się programowaniem i nie lubi teorii dotyczącej tej dziedziny.

Guy L. Steele et al.
The Hacker's Dictionary

 **white-hats:** pentesterzy, R/B-team, OSR (Offensive Security Research)

 **black-hats:** cracker, włamywacz, napastnik, atakujący, ...

Zagrożenia

Praktycznie wszystkie przypadki naruszające bezpieczeństwo w systemie informatycznym wyczerpują znamiona przestępstw określonych w obowiązującym prawie RP.

W szczególności mają tu zastosowanie:

- artykuły 267-269 KK
- artykuł 287 KK

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

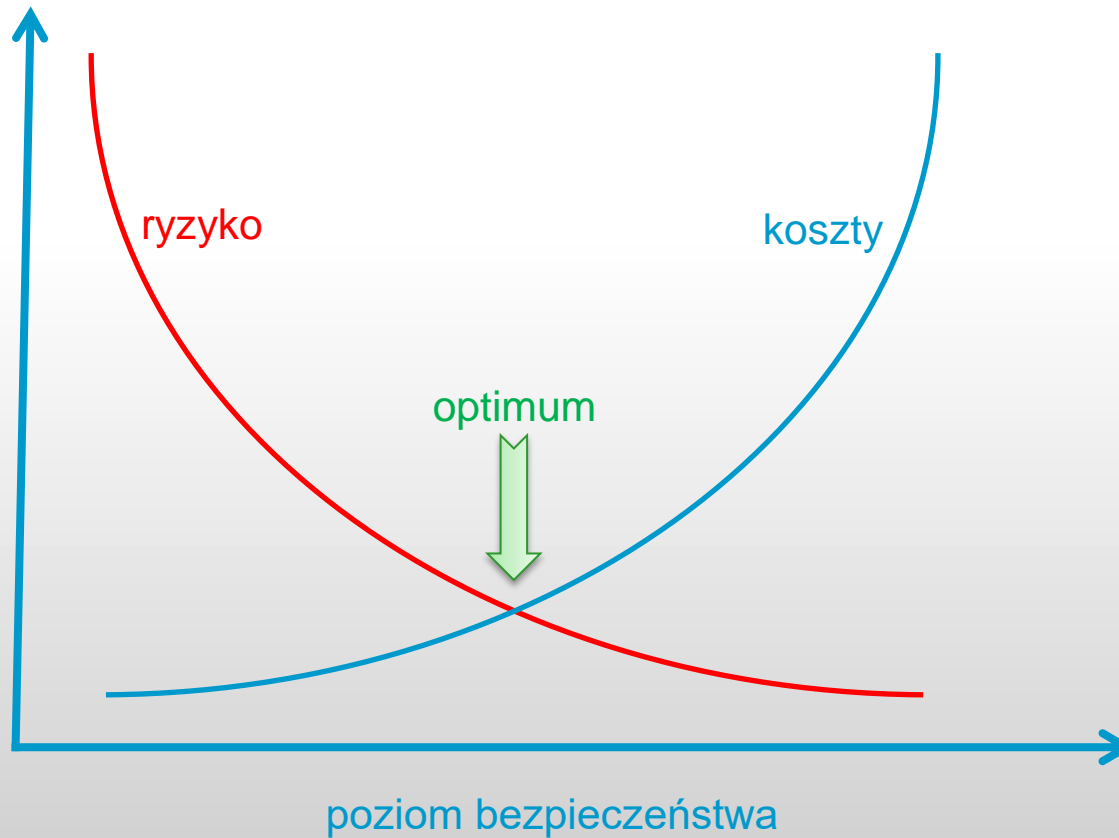


Bezpieczeństwo systemu informatycznego



1. Nie istnieje coś takiego, jak absolutne bezpieczeństwo.
2. Złożoność jest najgorszym wrogiem bezpieczeństwa.
3. Bezpieczeństwo musi być rozpatrywane w relacji z ekonomią.
4. System dopóty nie jest bezpieczny, dopóki nie ma pewności że jest.
5. Wzrost poziomu bezpieczeństwa odbywa się kosztem wygody.
6. Napastnik nie pokonuje zabezpieczeń, on je obchodzi.
7. Nie należy pokładać zaufania w jednej linii obrony (*defense in depth*).
8. Security by Design, by Default.

Bezpieczeństwo systemu informatycznego



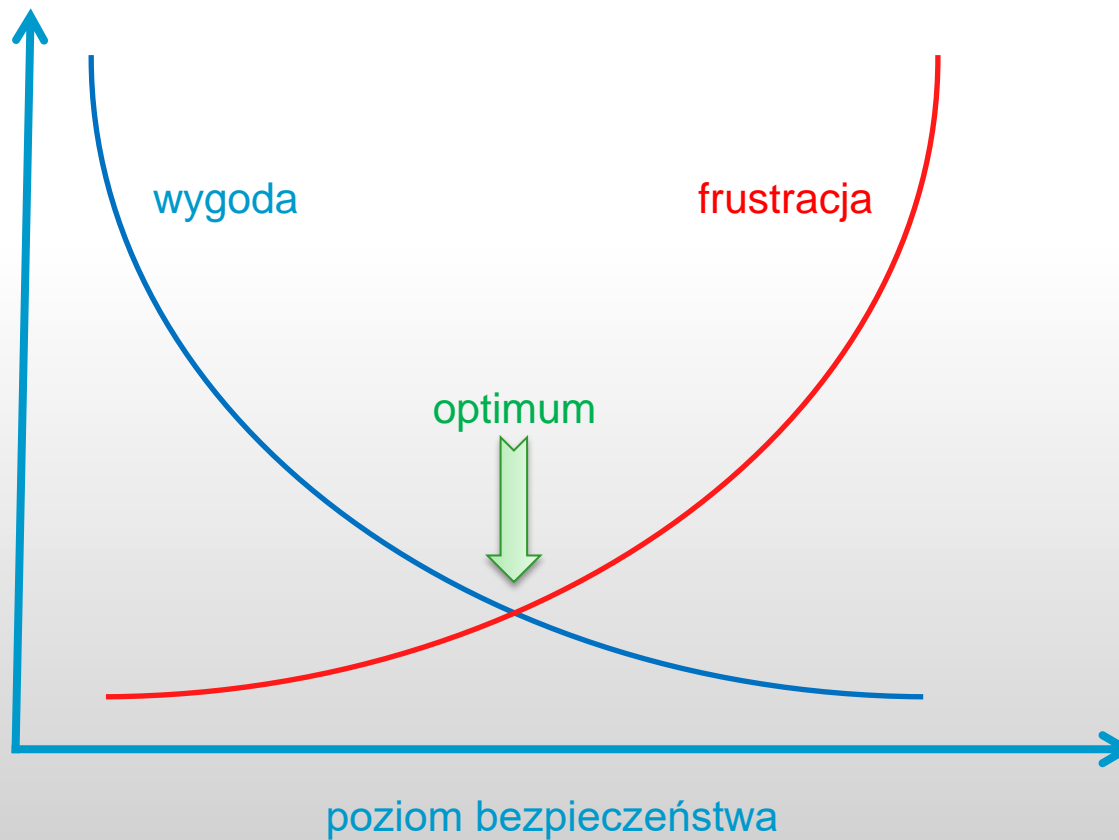
nomią.

ności że jest.

rygody.

ense in depth).

Bezpieczeństwo systemu informatycznego



nomią.
ności że jest.
wygody.
(sense in depth).

1. **Określenie zasobów = „Co chronić?”**
2. **Identyfikacja zagrożeń = „Przed czym chronić?”**
3. **Analiza ryzyka = „Ile czasu, wysiłku i pieniędzy można poświęcić na należną ochronę” (analiza kosztów i zysku)**



Polityka bezpieczeństwa

Polityka bezpieczeństwa

Polityka bezpieczeństwa

- ➔ element polityki [biznesowej] firmy



Etapy realizacji

1. zaprojektowanie
2. zaimplementowanie
3. zarządzanie (w tym okresowe audyty bezpieczeństwa)

Polityka bezpieczeństwa

Zakres

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

Specyfikacja środków

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

Polityka bezpieczeństwa



Normy i zalecenia zarządzania bezpieczeństwem

- PN-ISO/IEC 27000:2012 „Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia”
- PN-ISO/IEC 27001:2014-12 „Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania”
- PN-ISO/IEC 27005 „Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji”
- PN-ISO/IEC 24762:2010 „Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie”
- ...

Polityka bezpieczeństwa



Inne wymogi prawne w Polsce

- ➔ Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych – z późn. zmianami (tekst jednolity Dz. U. 2015 poz.2135)
- ➔ Rozporządzenie MSWiA z dnia 29 kwietnia 2004 r. w sprawie warunków technicznych i organizacyjnych (...) przetwarzania danych osobowych
- ➔ Rozporządzenie MAiC z 11 maja 2015 roku w sprawie sposobu realizacji zadań (...) przez administratora bezpieczeństwa informacji
- ➔ Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych
- ➔ Rozporządzenie Rady Ministrów z 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych
- ➔ Ustawa z 16 lipca 2004 r., Prawo telekomunikacyjne
- ➔ Ustawa z 29 sierpnia 1997 r., Prawo bankowe
- ➔ ...

1. **Określenie zasobów = „Co chronić?”**
2. Identyfikacja zagrożeń = „Przed czym chronić?”
3. Analiza ryzyka = „Ile czasu, wysiłku i pieniędzy można poświęcić na należną ochronę” (analiza kosztów i zysku)



Polityka bezpieczeństwa

Określenie zasobów = „Co chronić?”

- 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



1. **Określenie zasobów = „Co chronić?”**
2. **Identyfikacja zagrożeń = „Przed czym chronić?”**
3. **Analiza ryzyka = „Ile czasu, wysiłku i pieniędzy można poświęcić na należną ochronę” (analiza kosztów i zysku)**



Polityka bezpieczeństwa

Identyfikacja zagrożeń = „Przed czym chronić?”

- ➔ włamanie i kradzież poufnych danych
- ➔ infekcje wirusami
- ➔ kradzież sprzętu (np. w podróży służbowej)
- ➔ destruktywność pracowników / personelu zewnętrznego
- ➔ zablokowanie działania infrastruktury sieciowej
- ➔ utrata możliwości korzystania z łącz telekomunikacyjnych
- ➔ bankructwo firmy serwisowej / producenta sprzętu
- ➔ choroba administratora (jednoczesna choroba wielu osób)
- ➔ klęski żywiołowe (np. powódź)
- ➔ . . .



Model zagrożeń



Model zagrożeń

The Shark House in Oxford

NEWS, BY TOMO TAKA



Model zagrożeń

"All models are wrong, but some are useful"

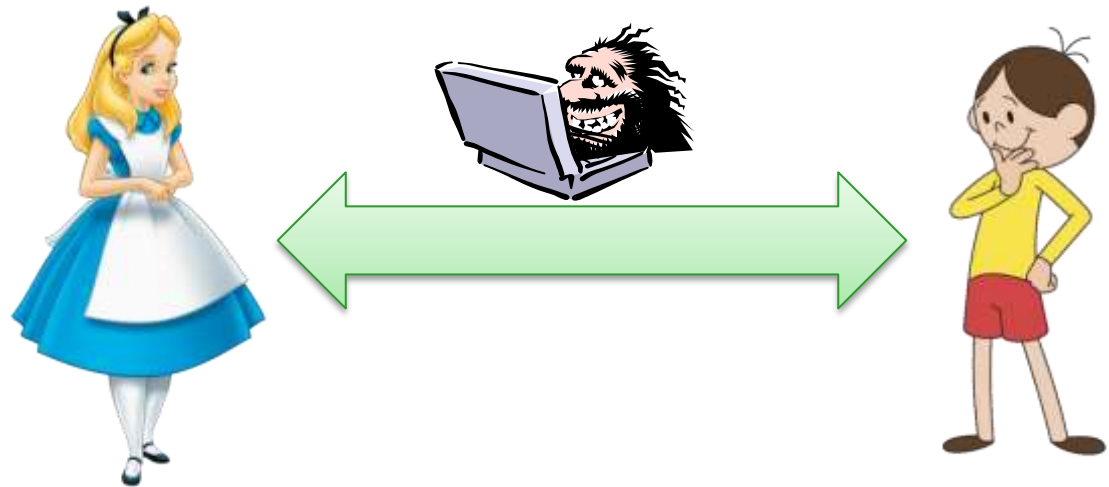
George E. P. Box



Atak na system informatyczny

Klasy ataków

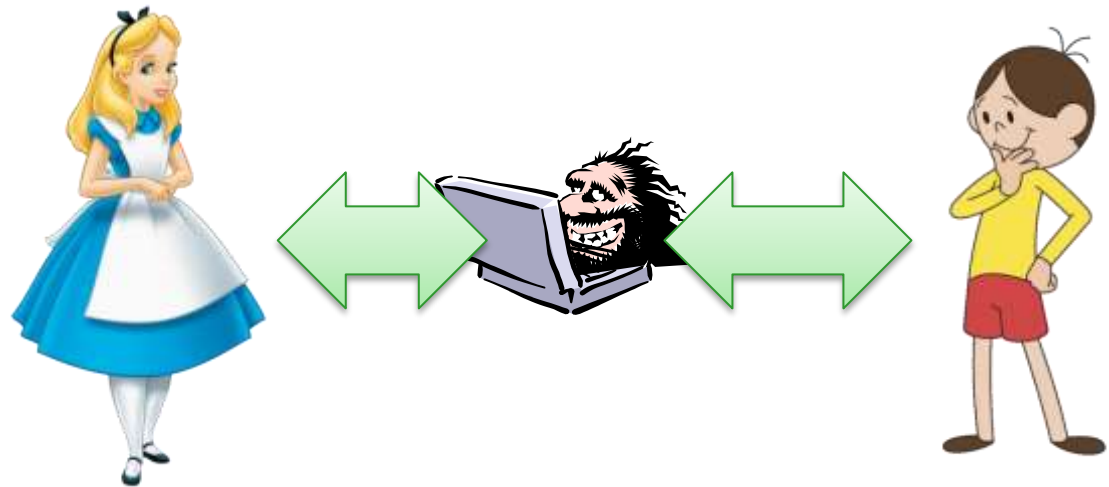
- pasywne / aktywne
- pasywny:



Atak na system informatyczny

Klasy ataków

- pasywne / aktywne
 - pasywny
 - aktywny:



Atak na system informatyczny

Klasy ataków

- ➔ pasywne / aktywne
 - ➔ pasywny
 - ➔ aktywny
- ➔ lokalne
 - ➔ atakujący już ma dostęp do systemu (konto) i próbuje zwiększyć swe uprawnienia

Atak na system informatyczny



Adversary Tactics and Techniques Knowledge Base
attack.mitre.org
Common Attack Pattern Enumeration and Classification
capec.mitre.org

Metody ataku elektronicznego

- podszywanie się (ang. *masquerading*),
fałszowanie tożsamości (ang. *spoofing*)
- podsłuch (ang. *eavesdropping*, *sniffing*)
- powtórzenie (ang. *replaying*)
- manipulacja (ang. *tampering*), przechwytywanie sesji (ang. *hijacking*)
- wykorzystanie luk w systemie (ang. *exploiting*)
- zablokowanie usług (ang. DoS = *Denial of Service*)
- DNS rebinding, web-pharming
- spam, scam, spim, blog spam, search spam
- phishing, spear-phishing, crab-phishing

} "Layer 8" attacks

Cyber Kill Chain



RECONNAISSANCE



WEAPONIZATION



DELIVERY

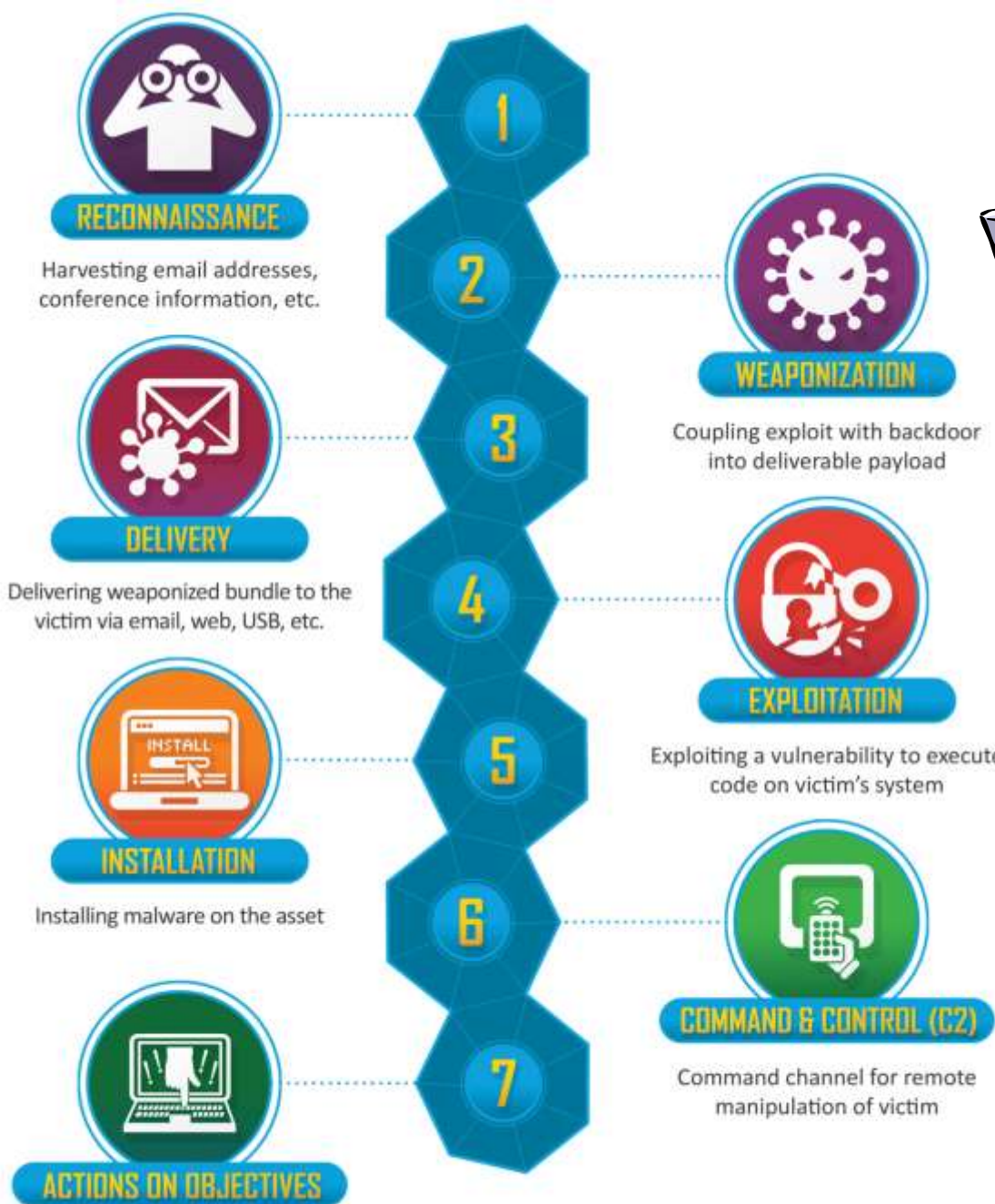


EXPLOITATION



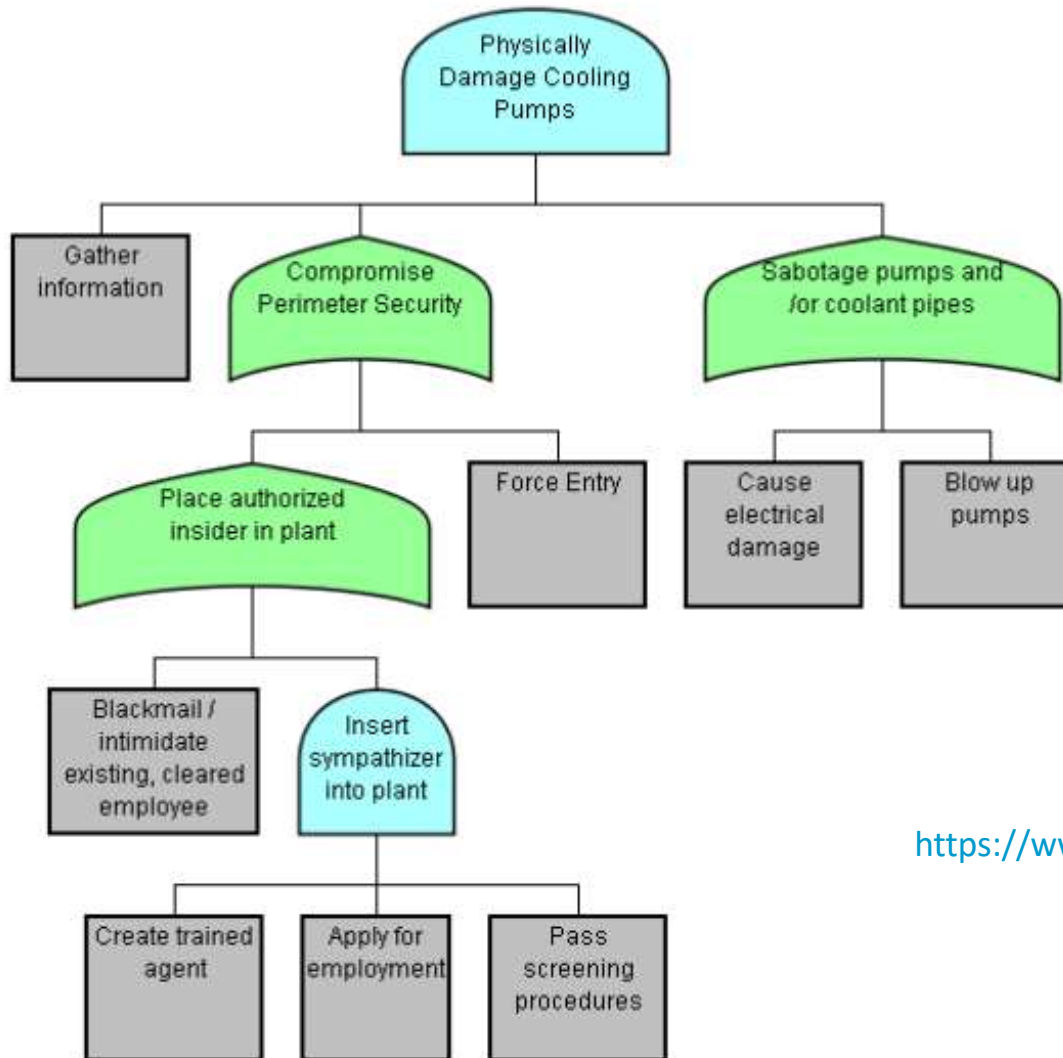
EXFILTRATION

➔ https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf



LockheedMartin

Attack tree



<https://www.amenaza.com>

MATRICES

Enterprise



PRE

Windows

macOS

Linux

Cloud



Network

Containers

Mobile



ICS

Reconnaissance

10 techniques

Resource Development

7 techniques

Initial Access

9 techniques

Execution

12 techniques

Persistence

19 techniques

Privilege Escalation

13 techniques

Defense Evasion

42 techniques

Active Scanning (3)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Access Token Manipulation (5)	BITS Jobs
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Domain Policy Modification (2)	Deploy Container
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Escape to Host	Direct Volume Access
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Event Triggered Execution (15)	Domain Policy Modification (2)
Search Victim-Owned Websites			System Services (2)	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Execution Guardrails (1)
			User Execution (3)	External Remote Services	Hijack Execution Flow (12)	Exploitation for Defense Evasion
			Windows Management Instrumentation	Hijack Execution Flow (12)	Process Injection (12)	File and Directory Permissions Modification (2)
				Implant Internal Image	Scheduled	Hide Artifacts (10)
						Hijack Execution Flow (12)
						Impair Defenses (9)
						Indicator Removal on

Atak na system informatyczny



Podstawowe fazy ataku

1. skanowanie (sondowanie, wyszukanie słabości)
2. wybór ataku (np. znaleziona podatność, dostępny exploit)
3. atak
4. modyfikacje systemu umożliwiające późniejszy powrót
5. zacieranie śladów
6. propagacja ataku

1. **Określenie zasobów = „Co chronić?”**
2. **Identyfikacja zagrożeń = „Przed czym chronić?”**
3. **Analiza ryzyka = „Ile czasu, wysiłku i pieniędzy można poświęcić na należną ochronę” (analiza kosztów i zysku)**



Polityka bezpieczeństwa

Zabezpieczenia



Złożoność problemu stosowania zabezpieczeń

➔ asymetria

Aby skutecznie zabezpieczyć system należy usunąć wszystkie słabości, aby skutecznie zaatakować – wystarczy znaleźć jedną.

➔ kontekst otoczenia systemu

Bezpieczeństwo powinno być rozważane w kontekście nie pojedynczego systemu informatycznego, ale całego otoczenia, w którym on się znajduje.

➔ zarządzanie i pielęgnacja

Zabezpieczenie systemu nie jest pojedynczą operacją, ale ciągłym procesem.

Zabezpieczenia



Złożoność problemu stosowania zabezpieczeń

1. Zasada naturalnego styku z użytkownikiem
2. Zasada spójności poziomej
3. Zasada spójności pionowej
4. Zasada minimalnego przywileju (*least privilege*)
5. Zasada bezpieczeństwa domyślnego (*security by default*)
 - zasada domyślnej odmowy dostępu (*deny by default*)
 - bezpieczna obsługa błędów (*fail-safe by default*)

Zabezpieczenia



Elementarne pojęcia

1. Identyfikacja (ang. *identification*)

- użytkownicy są identyfikowani w systemie za pomocą UID (*user identifier*)

2. Uwierzytelnianie (ang. *authentication*)

- proces weryfikacji tożsamości użytkownika; najczęściej opiera się na tym:
 - co użytkownik wie (*proof by knowledge*), np. hasło
 - co użytkownik ma (*proof by possession*), np. elektroniczną kartę identyfikacyjną

Доверяй но проверяй

Zabezpieczenia



Elementarne pojęcia

3. Autoryzacja (ang. *authorization*)

- ➡ proces przydzielania praw (dostępu do zasobów) użytkownikowi

4. Kontrola dostępu (ang. *access control*)

- ➡ procedura nadzorowania przestrzegania praw (dostępu do zasobów)

5. Poufność (ang. *confidentiality*)

- ➡ ochrona informacji przed nieautoryzowanym jej ujawnieniem

Zabezpieczenia



Elementarne pojęcia

6. Nienaruszalność / integralność (ang. *data integrity*)

- ochrona informacji przed nieautoryzowanym jej zmodyfikowaniem (ew. detekcja takiej modyfikacji)

7. Autentyczność (ang. *authenticity*)

- pewność co do pochodzenia (autorstwa i treści) danych

8. Niezaprzeczalność (ang. *nonrepudiation*)

- ochrona przed fałszywym zaprzeczeniem
 - przez nadawcę – faktu wysłania danych
 - przez odbiorcę – faktu otrzymania danych

Klasy bezpieczeństwa systemów komputerowych

Standardy certyfikacji:

- Trusted Computer System Evaluation Criteria (TCSEC “Orange Book”) – USA
<http://csrc.nist.gov/publications/history/dod85.pdf>; 1983-2000;
- Information Technology Security Evaluation Criteria (ITSEC) – EU
<http://www.cesg.gov.uk>; 1991-1997 (powstał głównie z angielskiego CESG2/DTIEC, francuskiego SCSSI i niemieckiego ZSIEC)
- Evaluation Assurance Levels (EAL) = ITSEC + TCSEC + CTCPEC (Canada) od 1996
Common Criteria (CC) for Information Technology Security Evaluation
od 1999 ISO/IEC 15408; od 2002 r. PN-ISO/IEC 15408; CC v.2.3 = ISO 18045;
akt. CC v.3.1 → <http://www.commoncriteria.org/cc/>

Klasy bezpieczeństwa systemów komputerowych

Sta



SA

1996

5;

