Model dogłębnej obrony

Marcin Szeliga
marcin@wss.pl

Agenda

- **Wprowadzenie**
- **Bezpieczeństwo jako proces**
- **Modelowanie zagrożeń**
  - Klasyfikacja zagrożeń
  - Ocena zagrożeń
  - Zarządzanie ryzykiem
- **Model dogłębnej obrony**

Wprowadzenie

- **Definicje:**
  - *Zdolność do unikania szkód będących wynikiem ryzyka, niebezpieczeństwa lub zagrożenia* (Cambridge Dictionary of English)
  - *zachowanie poufności, integralności i dostępności informacji* (PN-I 07799, PN ISO/IEC 17799)
- **…. w praktyce nieosiągalne**
- **Realny cel:**
  - *Zdolność do unikania zbyt wielkich szkód dzięki przewidywaniu ryzyka, niebezpieczeństw i zagrożeń* (Rafał Łukawiecki)

Wprowadzenie

Bezpieczne

W najlepszym wypadku

możemy wybrać dwie dowolne cechy

Funkcjonalne

Tanie

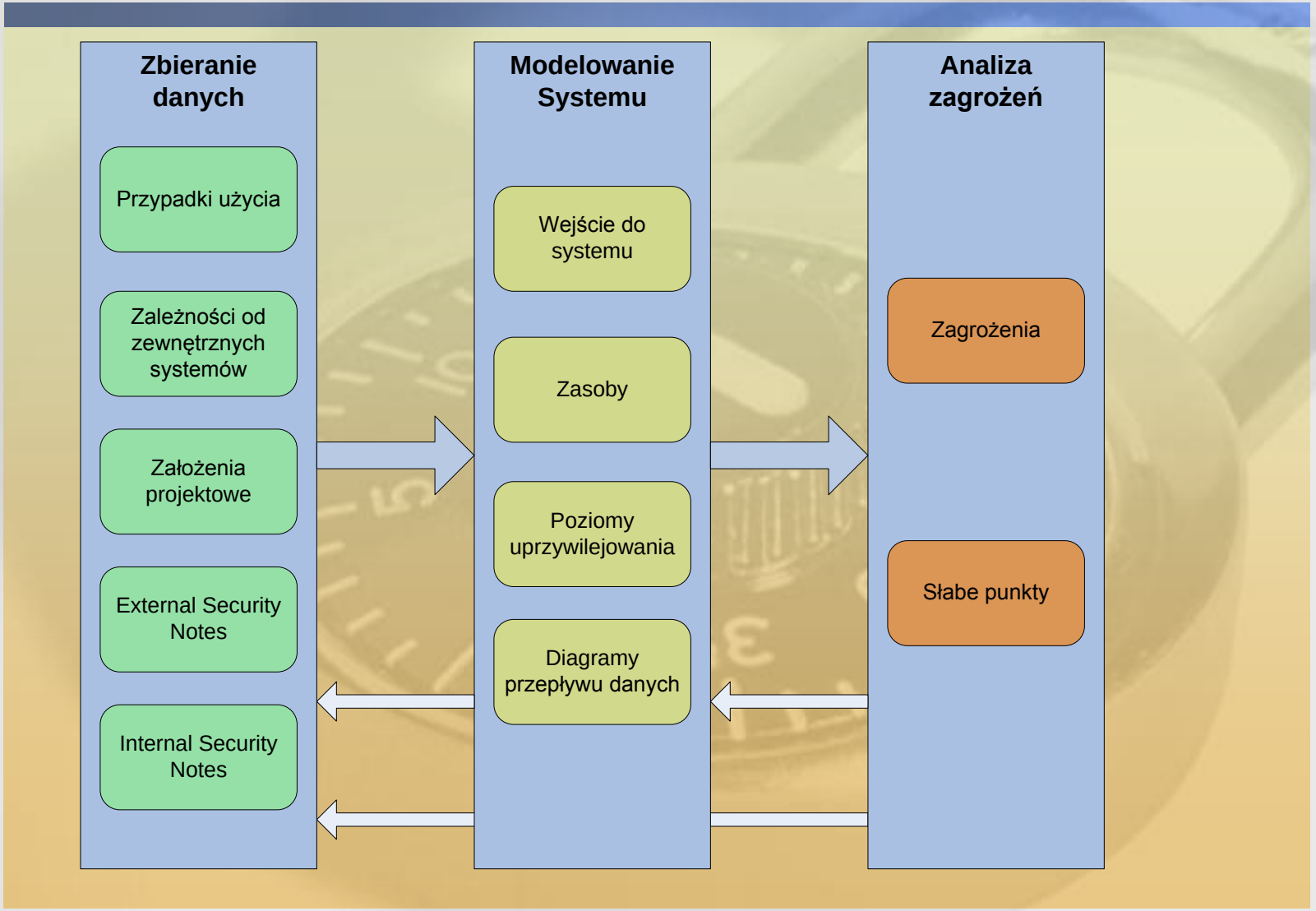
Wprowadzenie

- **Bezpieczeństwo = prostota + bezbłędność**
- **Bezpieczeństwo = technologia + ludzie + proces**
- **Zabezpieczenia muszą być opłacalne:**
  - Skoro 100% bezpieczeństwo jest niemożliwe, musimy zdecydować co i jakimi środkami chronić
  - Realna ocena dóbr i zagrożeń

Bezpieczeństwo jako proces

- Standardy:
  - Microsoft Operations Framework (MOF)
  - BS7799 i związane normy ISO 17799, 27001, 27002
  - OCTAVE (ang. Operationally Critical Threat, Asset and Vulnerability Evaluation) www.cert.org/octave
    - US Army, City Bank, …
- S3D:
  - Security by design
  - Security by deployment
  - Security by default

Modelowanie zagrożeń



Klasyfikacja zagrożeń

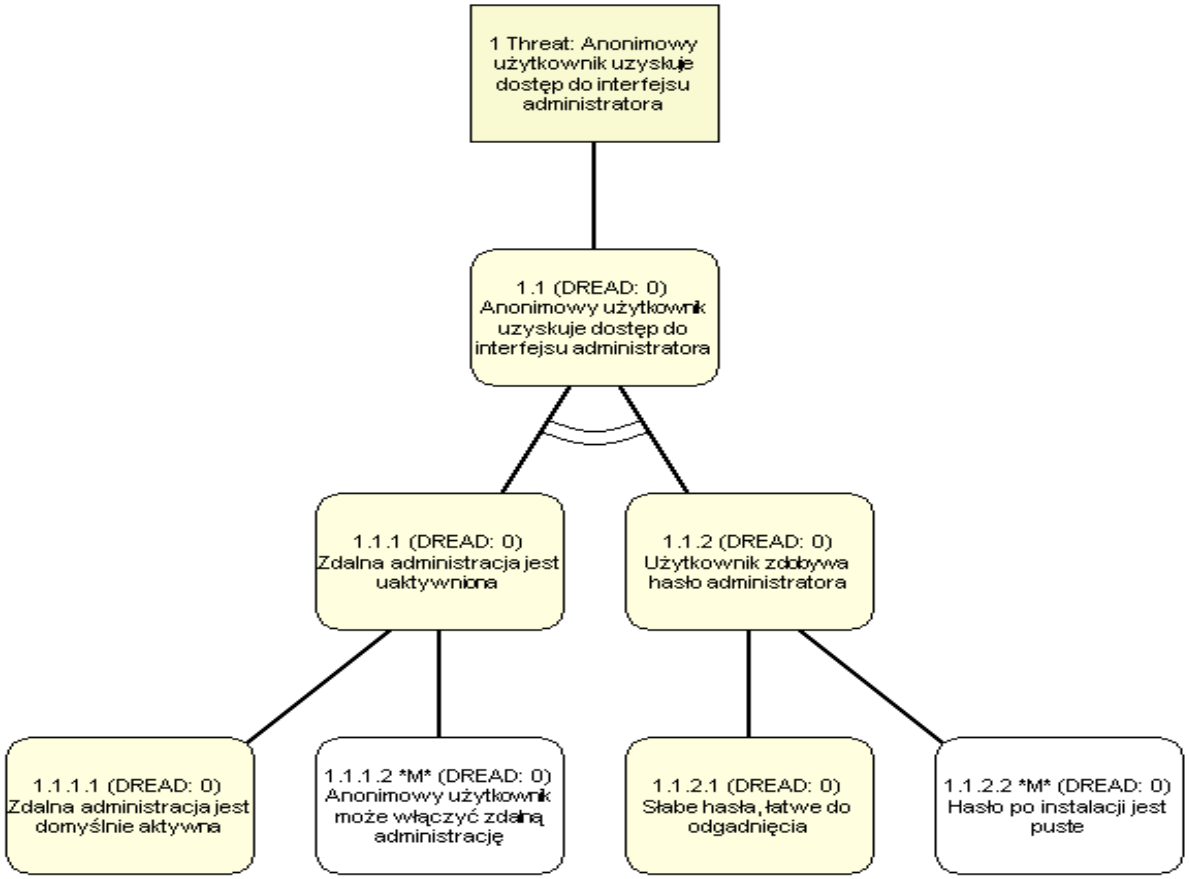
- Model STRIDE
  - S Spoofing identity (Fałszowanie tożsamości)
  - T Tampering with data (Modyfikowanie danych)
  - R Repudiability (Zaprzeczalność)
  - I Information disclosure (Ujawnienie danych)
  - D Denial of Service (Odmowa obsługi)
  - E Elevation of Privilege (Poszerzenie uprawnień)
- 5 z 6 zagrożeń może być zminimalizowanych za pomocą kryptografii

Ocena zagrożeń

- Wyznaczenie dóbr (<100)
- Ocena ryzyka utraty dóbr (model DREAD):
  - D — Damage potential (Potencjalne zniszczenia)
  - R — Reproducibility (Ryzyko odnowienia zagrożenia)
  - E — Exploitability (Podatność na atak)
  - A — Affected users (Poszkodowani użytkownicy)
  - D — Discoverability (Trudność wykrycia)

Threat	D	R	E	A	D	Total	Rating
Attacker obtains credentials	3	3	2	2	2	12	High
Injection of SQL commands	3	3	3	3	2	14	High

Drzewa zagrożeń (threat trees)



Zarządzanie ryzykiem

- Priorytet = zagrożenie * ryzyko
- Akceptacja ryzyka
  - Minimalizacja ewentualnych strat
- Minimalizacja ryzyka
  - Zmiana technologii
  - Zabezpieczenie systemu
  - Zablokowanie niebezpiecznych funkcji
  - Ostrzeżenie użytkowników
- Przeniesienie ryzyka na kogoś innego
- Rezygnacja z dóbr

Model dogłębnej obrony