Bezpieczeństwo w chmurze

Wydział Matematyki i Informatyki UAM

Semestr zimowy 2024/2025

Jan Helak, VML (jan.helak@vml.com)

TL;DR

Poznamy podstawy *Bezpieczeństwa* rozwiązań IT,
które działają w *Chmurze* (ang. Cloud Computing)

Warunki Zaliczenia

Projekt końcowy realizowany w zespołach 2-3 osobowych oceniany na podstawie następujących kryteriów:

1. Analiza wybranego zagrożenia CVE dla odbiorcy biznesowego oraz technicznego;
2. Prezentacja metod wykrycia zagrożenia CVE oraz sposobu jego usunięcia bądź minimalizacji;

Prowadzący Zajęcia

- Absolwent UAM w 2011 r.
- Dotychczas w karierze IT:
  - Operator Data Center
  - Administrator Linux / Unix
  - DevOps Engineer
- Obecnie pracuje w VML www.vml.com
- Lubi biegać długie dystanse

Prawdziwe Znaczenie Słów:

 ***Chmura*** 

 ***Bezpieczeństwo*** 

Shared Responsibility Model

- Modele Wspólnej Odpowiedzialności (Shared Responsibility Models) określają zakres odpowiedzialności dostawcy usług chmurowych i klienta;
- Najczęściej dostawcy usług chmurowych odpowiadają za bezpieczństwo infrastrukury, oraz częściowo za bezpieczeństwo niektórych usług;
- Klienci są odpowiedzialni za nadawanie odpowiednich uprawnień dostępu, zarządzanie aktualizacjami oraz spełnianie określonych polityk bezpieczeństwa;

Baza Podatności CVE

- Common Vulnerabilities and Exposures
- Zbiór publicznych informacji o podatnościach bezpieczeństwa
- Każda podatność ma przypisany unikalny identyfikator CVE
- Podatność CVE ma przypisany poziom krytyczności CVSS Common Vulnerability Scoring System
- Przykład: CVE-2021-44228
- Dane o podatnościach są przetwarzane m.in. przez NIST