POLITECHNIKA GDAŃSKA

# Wyzwania bezpieczeństwa nowoczesnych platform nauczania zdalnego

Paweł Lubomski

Gdańsk, 30 kwietnia 2015

# Szerokie grono odbiorców

**Platformy zamknięte:**
- studenci
- uczniowie
- kursanci kursów komercyjnych

**Platformy otwarte:**
- szeroko rozumiane społeczeństwo informacyjne
- osoby niepełnosprawne
- uniwersytety III wieku

**Platformy mieszane:**
- suma powyższych

stale rosnąca liczba użytkowników

**Przygotowanie kursu:**

- wiedza (know-how)

- poświęcony czas
- włożony wysiłek
- atrakcyjna oprawa

**Zagrożenia:**

- nielegalne i niekontrolowane
- powielanie i wykorzystywanie

**Systemy internetowe:**

- dostęp z wykorzystaniem przeglądarki WWW
- JavaScript
- AJAX
- rozwinięty CSS
- HTML5

# Charakterystyka technologiczna platform - urządzenia

**Szeroka gama obsługiwanych urządzeń:**

- komputery PC (niezależne od systemu operacyjnego)
- urządzenia mobilne (smartfony, tablety, …)

**Przetwarzanie w chmurze:**

- obciążenie przeniesione na serwery -> działa na słabszych urządzeniach

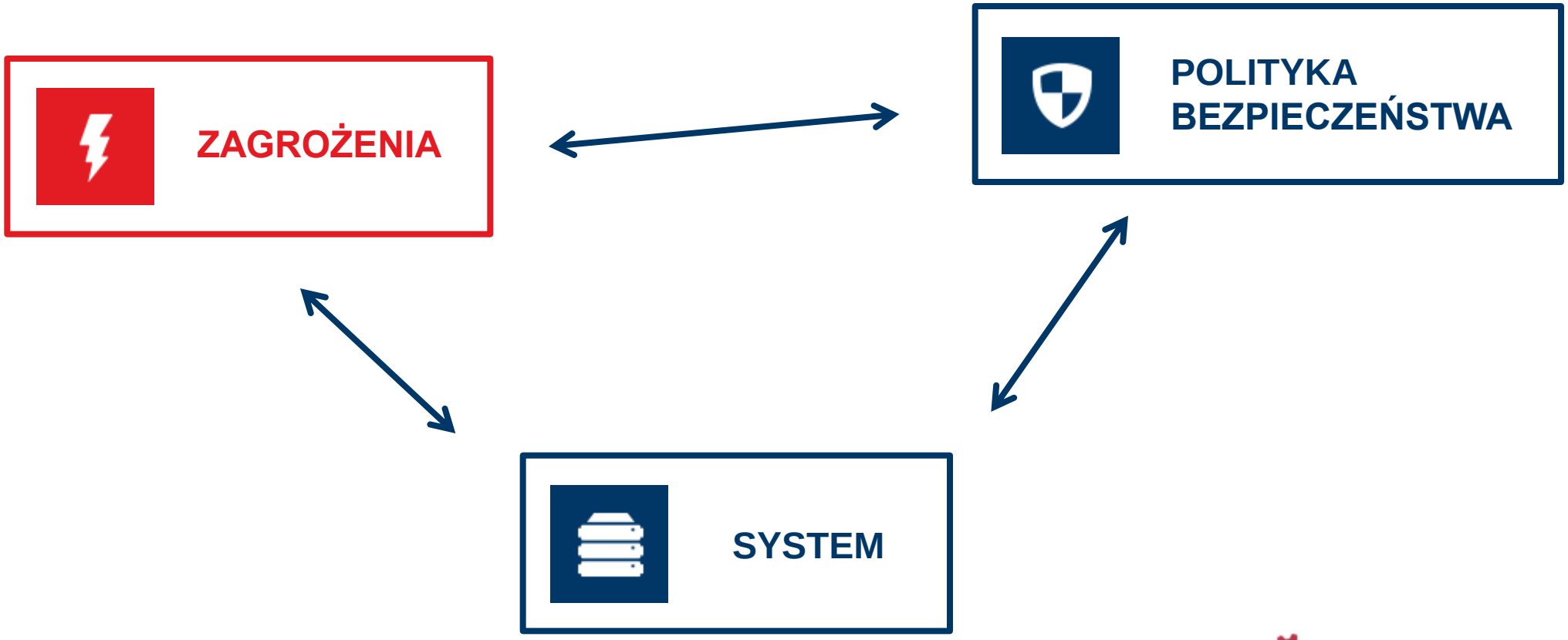
**Luźna interpretacja standardów przez różne urządzenia**

**Łączenie różnych źródeł i typów treści, np.**

- film + interakcja + kurs na platformie
- on-line film z wykładu połączony z prezentacją treści prezentacji i interaktywną tablicą

**Architektura usługowa (ang. SOA) – łączenie wielu usług od różnych dostawców**

# Środowisko działania systemu



**Polityka bezpieczeństwa** z perspektywy kontroli dostępu jest zbiorem reguł wyznaczanych przez organizację, które musi spełniać użytkownik otrzymujący dostęp do zasobu.

**Realizacja poprzez mechanizmy bezpieczeństwa:**

- zautomatyzowane, w pełni zaszyte w system
- częściowo zautomatyzowane
- manualne (procedury postępowania)

Wymagana ciągła **aktualizacja** i **usprawnianie**.

**Oprogramowanie:**
- skomplikowane
- produkowane coraz szybciej kosztem obniżenia jakości

Błędy w implementacji + cenne dane = **zagrożenia**

**Zagrożenia** podlegają klasyfikacji i kategoryzacji (CVE, CWE, NVD, OWASP Top Ten, …)

**Zagrożenia** występują również w sferze dostępności i niezawodności:
- utrata danych
- niedostępność systemu spowodowana awarią bądź przeciążeniem

## Jak zmierzyć brak incydentów?

### Audyt bezpieczeństwa

- analiza ryzyka wykrytych podatności (np. CVSS)
- priorytetyzacja usuwania podatności
- implementacja usprawnień w systemie
- kolejny audyt bezpieczeństwa

Wykonana z wykorzystaniem rozwiązań **open-source**.
**Silnie zintegrowana** z innymi centralnymi systemami Politechniki Gdańskiej.

Wyniesione uwierzytelnianie główne (+ dualny system uwierzytelniania)
- wygodne (pamięta się tylko jedno hasło)
- centralne zarządzanie uprawnieniami
- możliwość przezroczystego łączenia wielu usług wymagających uwierzytelnienia

Automatyczny przepływ uczestników i postępów pomiędzy platfromą eNauczanie, a systemem obsługi dydaktyki w Moja PG.

Osadzona na prywatnej chmurze w serwerowni Centrum Usług Informatycznych PG – serwery wirtualne pozwalają na elastyczne skalowanie pionowe (zwiększanie zasobów) i poziome (klastrowanie) => wzrost niezawodności działania (HA)

**Wykryto 8 podatności:**

- brak na poziomie wysokim
- 3 na poziomie średnim
- 5 na poziomie niskim

Podatności usunięte.

Zaplanowany **kolejny audyt bezpieczeństwa** oraz **testy wydajnościowe**.

**Ciągły rozwój platformy** oraz odkrywane coraz to nowsze zagrożenia.

**Potrzebny:**

- stały monitoring platformy
- okresowe audyty bezpieczeństwa
- okresowe testy wydajnościowe
- procedury na wypadek wystąpienia zagrożenia (naprawa jego skutków)


POLITECHNIKA
GDAŃSKA
111
LAT