

# Bezpieczeństwo portali: bramy personalizacji

Igor Margasiński

Instytut Telekomunikacji Politechniki Warszawskiej

Igor@Margasinski.com  
http://Margasinski.com

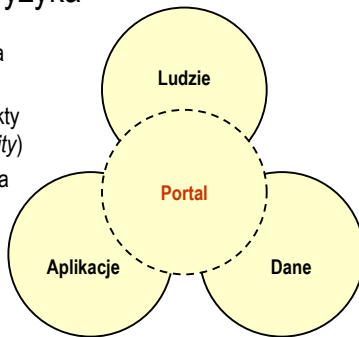
"Portale korporacyjne - zarządzanie treścią, informacją i wiedzą"  
Warszawa 27.01.2004 r.

## Plan prezentacji

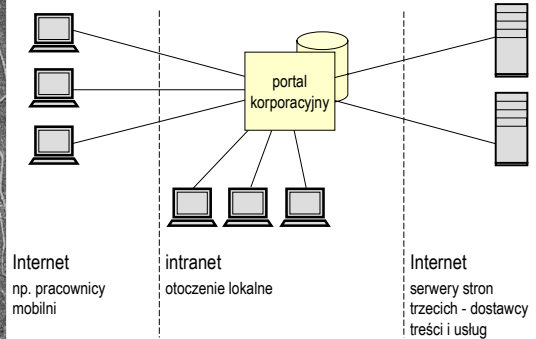
- ◆ Podstawowe aspekty bezpieczeństwa portali korporacyjnych
- ◆ Nowe kierunki – bezpieczeństwo portali jako źródło ich ewolucji
  - portale korporacyjne czyli *bramy personalizacji*
- ◆ Bezpieczeństwo a prywatność użytkowników
- ◆ Podsumowanie

## Analiza ryzyka

- ◆ Zagrożenia (*threats*)
- ◆ Słabe punkty (*vulnerability*)
- ◆ Następstwa (*impacts*)



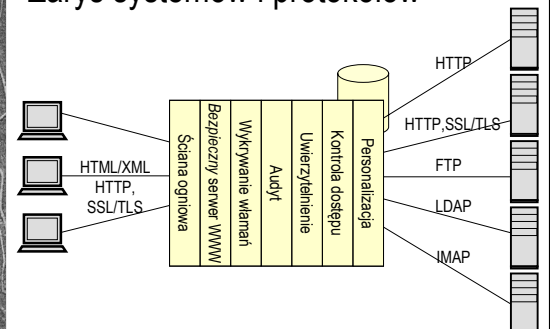
## Źródła zagrożeń



## Metody ochrony

- ◆ Użytkownicy
  - Uwierzytelnienie
  - Kontrola dostępu
  - Niezaprzeczalność
- ◆ Dane / treści, informacje, wiedza
  - Integralność
  - Poufność

## Zarys systemów i protokołów



## Bezpieczeństwo serwera WWW

- ◆ Wybór
  - platformy sprzętowej i programowej
  - Serwera WWW
- ◆ Wsparcie dla pożądaných protokołów i technologii związanych z bezpieczeństwem
- ◆ Konfiguracja
- ◆ Bezpieczeństwo w zakresie logiki aplikacji

## Ewolucja zabezpieczeń – u progu bram personalizacji

Tożsamości cyfrowe w oparciu o certyfikaty, PKI

Uwierzytelnienie z zastosowaniem SSO (*Single Sign-On*)

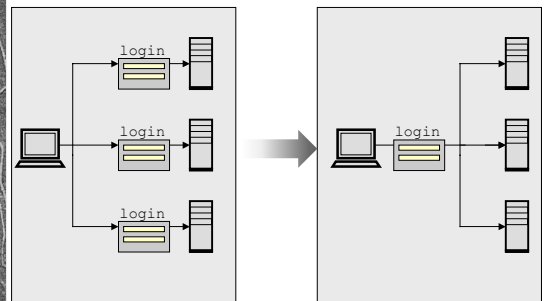
Kontrola dostępu (hierarchia grup, użytkowników, ról i profili)

Personalizacja, profilowanie użytkowników

## Single Sign-On

- ◆ Problem uwierzytelnienia w wielu systemach
- ◆ Wiele identyfikatorów użytkownika i haseł
  - Zapominanie
  - Próby zapisywania przez użytkowników danych wymaganych do uwierzytelnienia
- ◆ Koncepcja *Single Sign-On* – jednokrotne uwierzytelnienie do wielu systemów (geneza: sieci LAN)

## Schemat Single Sign-On



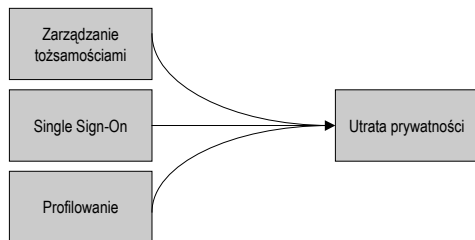
## Systemy Single Sign-On

- ◆ Kerberos (*tickets, tokens*)
- ◆ DCE – *Distributed Computing Environments*
- ◆ Infrastruktura klucza publicznego – PKI – *Public Key Infrastructure* (certyfikaty)
- ◆ LDAP – *Light Weight Directory Protocol*

## Personalizacja

- ◆ Dostosowanie treści i sposobu prezentacji do poszczególnych użytkowników, grup, itp. (*customization*)
- ◆ Zarządzanie dostępem użytkowników do Internetu – EMI – *Employee Internet Management*
  - poprzez analizę żądań (*pass-through*)
  - poprzez weryfikację otrzymywanych treści (*pass-by*)
- ◆ Profilowanie, śledzenie aktywności użytkowników

## Prywatność użytkowników



## Podsumowanie

- ◆ Rozwój mechanizmów bezpieczeństwa portali (takich jak zarządzanie tożsamościami, zarządzanie dostępem) oznacza obecnie nie tylko podwyższenie poziomu bezpieczeństwa, ale również:
  - jakościowe zmiany w funkcjonalności
  - wydajności pracy
  - wizerunku portali korporacyjnych
  - wprowadzenie nowych możliwości współdzielenia zasobów i współpracy użytkowników
  - uproszczenie interfejsu użytkownika
- ◆ Należy jednak pamiętać, że nadużywanie tych mechanizmów grozi całkowitym pozbawieniem użytkowników/pracowników prywatności w obrębie portalu
  - zniechęcanie i odstraszenie od korzystania z systemu

## Czy mają Państwo pytania?

**Igor Margasiński**

Instytut Telekomunikacji Politechniki Warszawskiej

Igor@Margasinski.com  
<http://Margasinski.com>