# Ekonomia bezpieczeństwa

Paweł Krawczyk pawel.krawczyk@hush.com

http://ipsec.pl/

# ŹRÓDŁA BEZPIECZEŃSTWA

- Zewnętrzne
  - Klienci – łańcuch odpowiedzialności, SLA
  - Przepisy prawa, konkurencja, reputacja
- Wewnętrzne
  - Klienci wewnętrzni – SLA
- Analiza ryzyka
  - *„10% szansy, że zapłacimy 10 mln zł kary”*
- Redukcja ryzyka jako inwestycja
  - *„unikniemy straty 1 mln zł za jedyne 100 tys. zł”*

# RACJONALNE BEZPIECZEŃSTWO

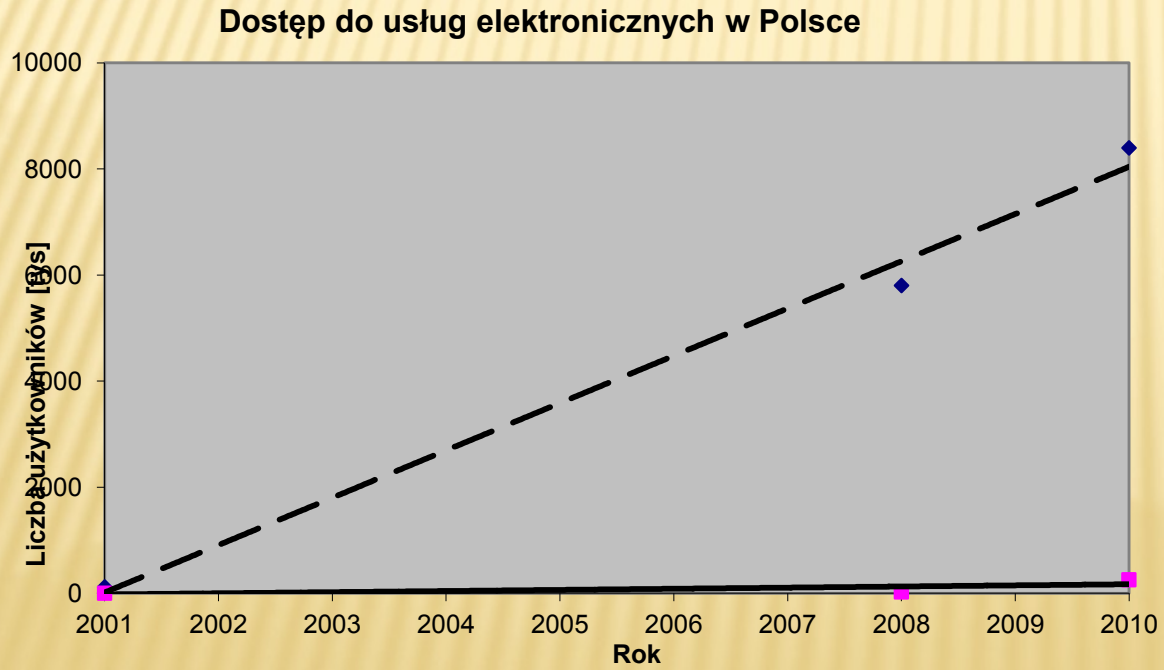
- Chroni przed zagrożeniami
- Nie kosztuje więcej niż chronione dobra
- Drogi do irracjonalności
  - Błędna ocena ryzyka
  - Błędny wybór zabezpieczeń
  - Automatyzm we wdrażaniu norm i zaleceń branżowych
- Skutki
  - Strata *pewna* zamiast *prawdopodobnej*
  - Chybione zabezpieczenia
  - Błędna alokacja zasobów
  - Wiecej, a nie mniej zdarzeń niepożądanych

# TECHNIKI UWIERZYTELNIANIA

- Sektor publiczny
  - Podpis kwalifikowany (2001-2010)
    - Wysoki poziom bezpieczeństwa
    - Niska używalność
    - Karta, sterowniki
- Prognozowane scenariusze
  - Zawieranie umów
  - Zakupy internetowe
  - Kupowanie nieruchomości przez Internet (!)
- Sektor prywatny
  - Hasła statyczne (~2000)
  - Hasła jednorazowe (~2002)
  - Hasła SMS (~2005)

# DOSTĘP DO USŁUG ELEKTRONICZNYCH W POLSCE

- Sektor prywatny
  - „Wystarczający poziom bezpieczeństwa”
  - 2010 – 8,4 mln
    - 22% obywateli
- Sektor publiczny
  - „Wysoki poziom bezpieczeństwa”
  - 2010 – 250 tys.
    - 0,94% obywateli




Źródła: Michał Polasik, “Bankowość internetowa”, 2001
IPSec.pl (2007-2010), Związek Banków Polskich (2008, 2010)

# E-DEKLARACJE

- 2008 – podpis kwalifikowany - 5 tys. PIT-37
- 2009 – bez p.k. – 78 tys.
- 2010 – 254 tys.
- 2011 – 700 tys.
- 2012 – 1,5 mln
- 2013 – 2,7 mln
- 2014 – 3,9 mln
- VAT-7 od 50 tys. (2008) do 5 mln (2013)

Źródło: http://www.finanse.mf.gov.pl/systemy-informatyczne/e-deklaracje/statystyka

# FAKTURY ELEKTRONICZNE

- 2001 dyrektywa UE
- 2005 polskie rozporządzenie o e-fakturach
  - Podpis kwalifikowany
- 2008 - 400 mln € oszczędności w Szwecji
  - Finlandia, Dania– bez podpisu lub prosty podpis cyfrowy
- 2008 Dania – 70% firm, 100% zamówień publicznych
- 2010 Polska – 10% firm
  - Możliwe oszczędności 15 mld zł (!)
- 2013 nowelizacja rozporządzenia
  - 20% firm

# GWARANCJE NA OPROGRAMOWANIE

- Niezawodne oprogramowanie istnieje
  - Formalne metody dowodzenia poprawności kodu
  - Języki: ADA SPARK, ATS, COQ, CompCert
  - Operacyjne: SELinux, AppArmor
- Ale tworzenie go jest bardzo kosztowne
  - Common Criteria EAL2 – od 50 tys. €, 12 miesięcy
  - Common Criteria EAL4 – od 150 tys. €, 18 miesięcy
- Czy chcemy **powszechnych** gwarancji na oprogramowanie?
  - Ja nie chcę! Wolę program za 300 zł, który działa *wystarczająco* dobrze

# BEZPIECZEŃSTWO A REGULACJA

Kilka rozpowszechnionych mitów

- *„Bezpieczeństwo jest najważniejsze”*
  - Ale 100% bezpieczeństwa = 0% aktywności
  - **Każde** działanie stanowi kompromis bezpieczeństwa
- *„Więcej bezpieczeństwa to lepiej”*
  - Ale to także większy koszt i mniejsza efektywność
- *„Tylko X zapewni wysoki poziom bezpieczeństwa”*
  - Ale czy **tutaj** potrzebujemy **wysokiego** poziomu?
    - Może wystarczy niski lub średni?