Problem szarej strefy e-dokumentu

Szara strona mocy e-dokumentu

XVII Forum Teleinformatyki **23.09.2011**

PWPW
TECHNOLOGIE IT

Marek Barszczyński
Pion Rozwiązań Informatycznych

Agenda

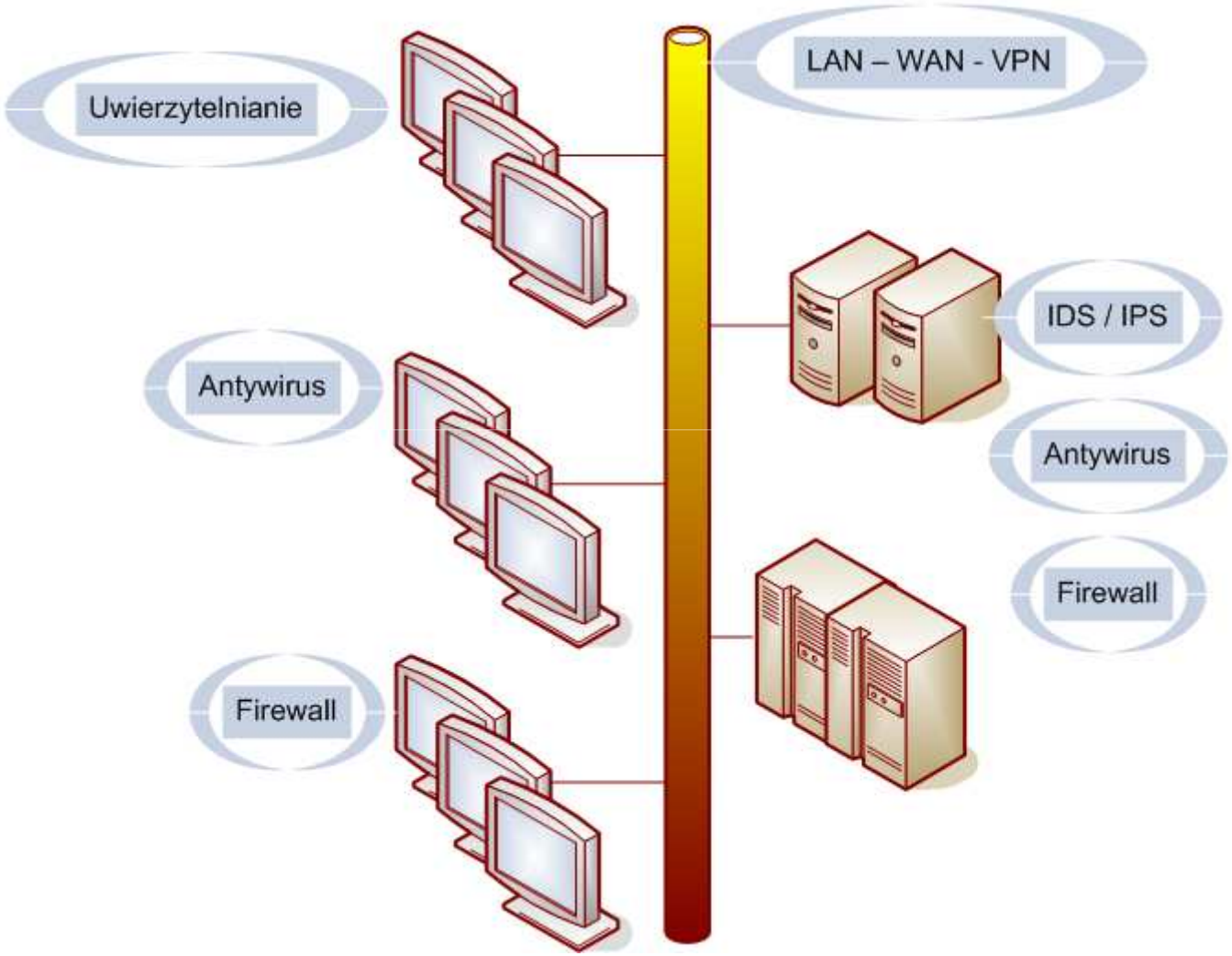
- E-dokument w obrocie gospodarczym
- Szara strona mocy – wycieki informacji
- Antidotum

E-dokument w obrocie gospodarczym

- Europejska Agenda Cyfrowa 2010
- Plan Informatyzacji Państwa do 2015
- Ustawy :
  - o informatyzacji,
  - o świadczeniu usług drogą elektroniczną,
  - o podpisach elektronicznych,
  - . . .
- Rozporządzenia :
  - Instrukcja Kancelaryjna i archiwum,
  - Elektroniczna Dokumentacja Medyczna,
  - Profil Zaufany,
  - . . .

E-dokument w obrocie gospodarczym

Szara strona mocy – wycieki informacji



Szara strona mocy – wycieki informacji

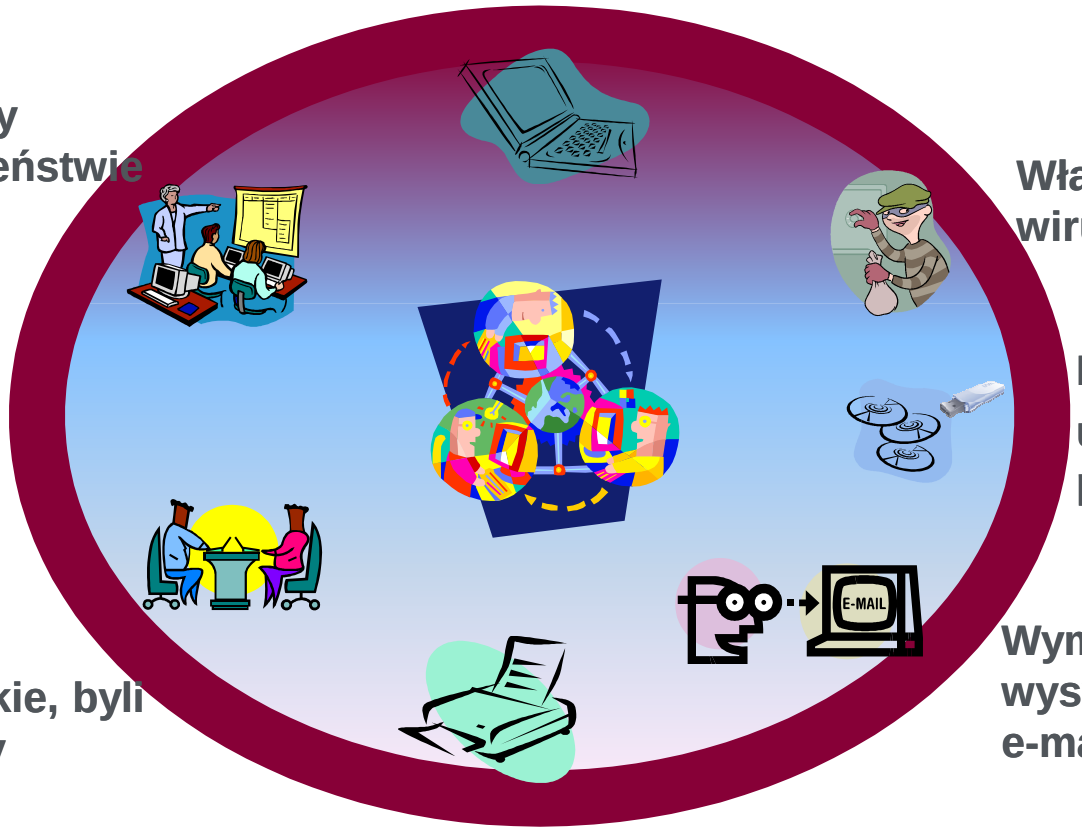
- Koncentrujemy się na statycznej ochronie sieci, serwerów, komputerów, aplikacji – a nie na ochronie informacji (dokumenty, zbiory danych, rysunki, zdjęcia, …)

- Statyczna ochrona danych jest konieczna ale obecnie już niewystarczająca – **informacja jest mobilna** – musimy zapewnić integralność, niezaprzeczalność i poufność w całym cyklu jej życia

Szara strona mocy – wycieki informacji

Utrata sprzętu (laptop, smartfon, pendrive, …)

Brak wiedzy o bezpieczeństwie danych



Włamania (hakerzy, wirusy, spyware, …)

Niezabezpieczone urządzenia przenośne i nośniki

Kontakty przyjacielskie, byli pracownicy

Wymiana plików, wysyłanie danych e-mailem

Wydruki i skanowanie

Szara strona mocy – wycieki informacji

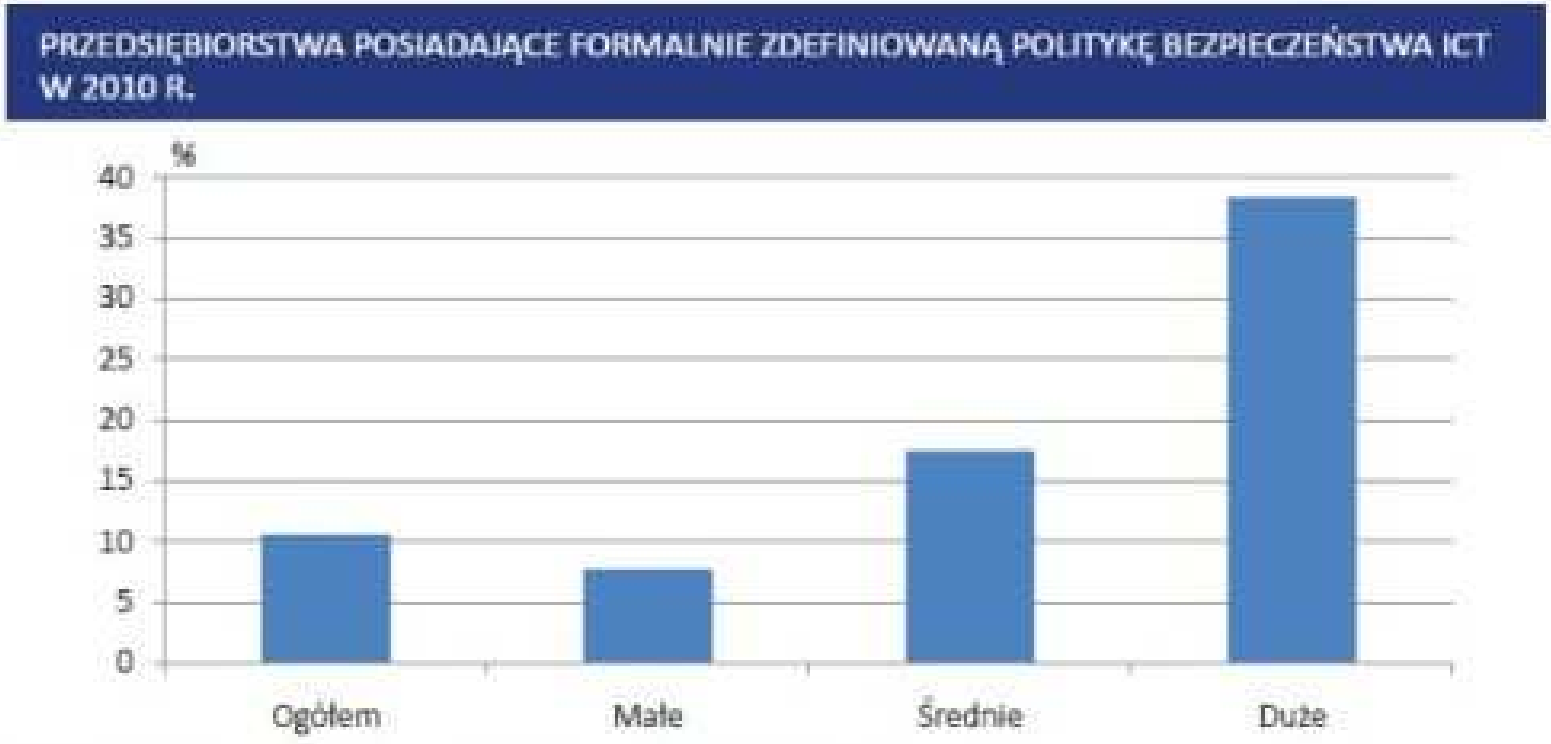
- W 2010 r. 77% przedsiębiorstw doświadczyło wycieku danych (wg. Check Point Software & Ponemon Institute)
- Wypływały dane o :
  - Klientach 52%
  - Własności intelektualnej 33%
  - Pracownikach 31%
  - Planach biznesowych 16%
- 2/3 zwalnianych pracowników kopiuje poufne dane
- 4/5 pracodawców nie przeprowadziło audytu dokumentów zwalnianych pracowników
- 1/2 ABI uważa, że brak jest wiedzy o bezpieczeństwie, standardach i politykach bezpieczeństwa

Antidotum

wg.raportu Check Point Software Technologies & Ponemon Institute

- Zebranie potrzeb dotyczących bezpieczeństwa danych w organizacji
- Klasyfikacja wrażliwych danych
- Dopasowanie polityk bezpieczeństwa do potrzeb organizacji
- Zabezpieczanie danych przez cały okres ich życia
- Eliminacja obciążenia wynikającego ze standardów
- Położenie nacisku na świadomość i zaangażowanie użytkowników

Antidotum

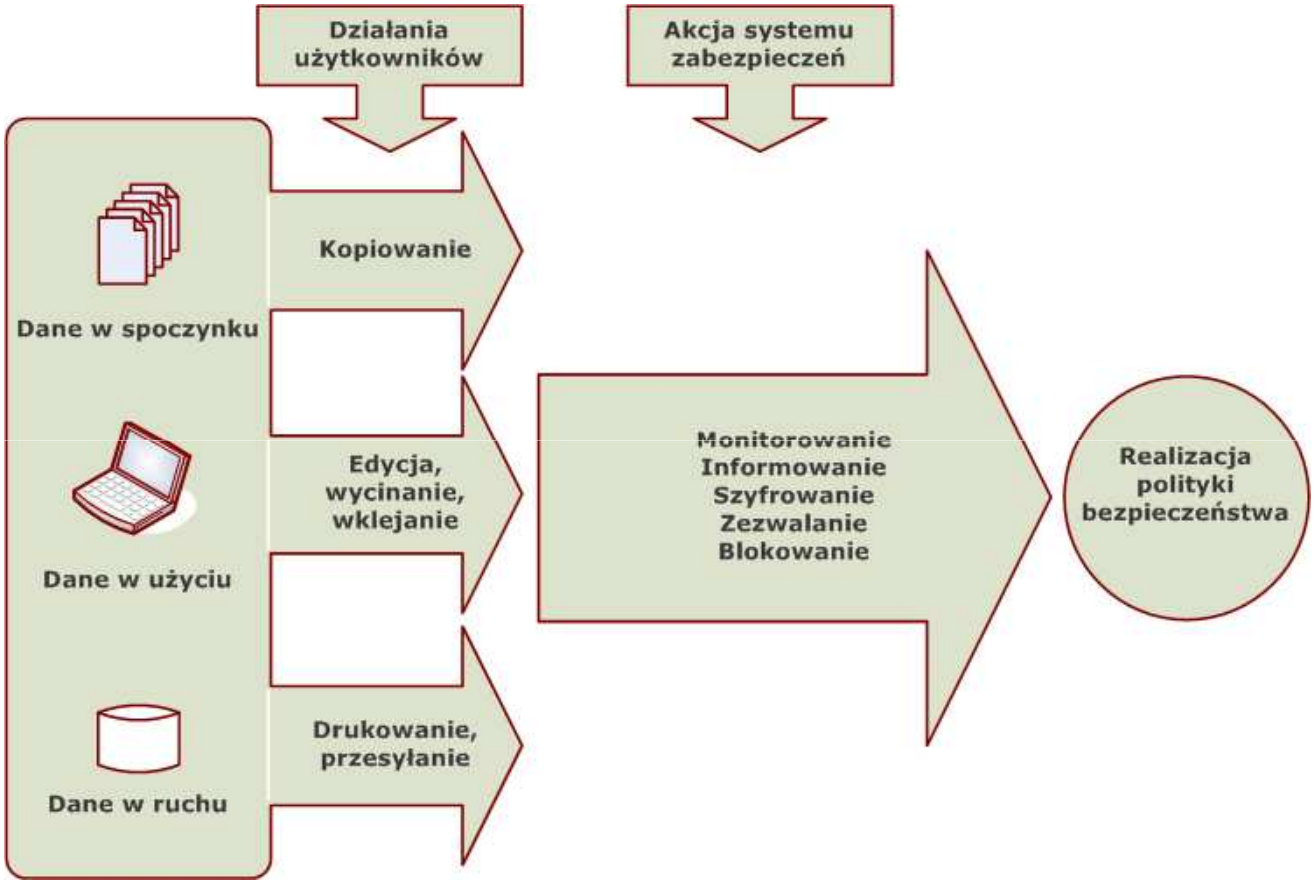


Źródło: *badanie Wskaźniki społeczeństwa informacyjnego*, GUS.

Antidotum

- ISO/IEC 27001 – Wymagania dla Systemów Zarządzania Bezpieczeństwem Informacji
- ISO/IEC 27002 – Praktyczne zasady zarządzania bezpieczeństwem informacji
- ISO/IEC 13335-1 – Wytyczne do zarządzania bezpieczeństwem informacji
- ISO/IEC 13335-2 – Planowanie
- ISO/IEC 13335-3 – Techniki zarządzania
- ISO/IEC 13335-4 – Wybór zabezpieczeń
- ISO/IEC 13335-5 – Zabezpieczenia dla połączeń z sieciami zewnętrznymi

Antidotum



technologia → procesy → ludzie → cel biznesowy

Antidotum

Rola trzeciej zaufanej strony w systemie bezpieczeństwa teleinformatycznego i uwierzytelniania

- Identyfikacja, autoryzacja, uwierzytelnianie
- Operator systemów zabezpieczenia informacji

Dziękuję za uwagę

- www.it.pwpw.pl
- m.barszczynski@pwpw.pl