Powiadamianie o naruszeniach ochrony danych osobowych

Sławomir Górniak

Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji

Konferencja: Reforma regulacji ochrony danych osobowych w Unii Europejskiej

Warszawa, 7 marca 2012

Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji

- Agencja Unii Europejskiej
- Ośrodek wiedzy n/t bezpieczeństwa sieci i informacji
- Centrum wymiany informacji i najlepszych praktyk pomiędzy państwami członkowskimi, instytucjami UE i firmami
- Zaangażowana w temat powiadamiania o naruszeniach ochrony danych

Naruszenia i powiadamianie

- Podstawy prawne UE
  - Dyrektywa o e-prywatności 2002/58/WE, Art. 4(3)
  - Projekt nowego rozporządzenia
- Naruszenie ochrony danych osobowych

  „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób”
- Powiadamianie

  „W przypadku naruszenia ochrony danych osobowych, administrator zgłasza organowi nadzorczemu takie naruszeniu bez nieuzasadnionej zwłoki i jeśli jest to możliwe, nie później niż w ciągu 24 godzin od momentu dowiedzenia się o tym naruszeniu.”

Sytuacja w 2010

- Ramy dyrektywy 2002/58/WE
- Różnice między państwami członkowskimi
- Uwagi organów nadzorczych
  - Ogólne poparcie dla powiadamiania o naruszeniach
  - Brak budżetu
  - Nacisk na edukację i prewencję
- Punkt widzenia firm telekomunikacyjnych
  - Akceptacja istniejącego porządku prawnego
  - Zaufanie do własnych procedur
  - Poczucie niesprawiedliwości
  - Potrzeba wsparcia w interpretacji legislacji

Sytuacja w 2010

- Punkty sporne
  - Ustalenie momentu rozpoczęcia procedury
  - Treść powiadomienia
  - Format powiadomienia
  - „Nieuzasadniona zwłoka”
  - Wykrywanie naruszeń i rola organów nadzorczych
  - Zaufanie do instytucji
- Wnioski
  - Powiadamianie nie zapewni ochrony danych od razu
  - Powiadamianie zapewni dostępność informacji o incydentach
  - Potrzeby organów nadzorczych i firm różnią się
  - **Brak jasnych wytycznych**

Zalecenia dot. technicznej implementacji Art.4

- Rola zarządzania ryzykiem
- Właściwe środki technologiczne i organizacyjne
- Plany reakcji na incydenty
- Detekcja i dwufazowa ocena incydentu
- Procedury powiadamiania
- Weryfikacja procedur
- Baza danych naruszeń

Plany na przyszłość

- Przygotowanie innych sektorów do powiadamiania o naruszeniach
- Piloty w krajach członkowskich
- Współpraca międzynarodowa
- Stworzenie centralnego punktu zbierającego dane o naruszeniach

Dziękuję za uwagę. Pytania?

Sławomir Górniak,
European Network and Information Security Agency
Technical Competence Department

Email: Slawomir.Gorniak@enisa.europa.eu

- Odnośniki
  - http://www.enisa.europa.eu/act/it/dbn
  - http://www.youtube.com/user/enisasta