

Microsoft®

CENTRUM INNOWACJI

Bezpieczeństwo Danych Osobowych

Zespół Bezpieczeństwa PCSS

Jakub Tomaszewski



Plan prezentacji

- Wprowadzenie

- Dane Osobowe
 - Definicja
 - Dane wrażliwe
 - Opinie i świadomość

- Ochrona danych osobowych
 - Akty prawne
 - Klauzule
 - Generalny Inspektor Ochrony Danych Osobowych
 - Europejski Inspektor Ochrony Danych
 - Ochrona we własnym zakresie

Plan prezentacji

- Metody wykorzystywania baz danych osobowych
 - Zgodne z prawem
 - Niezgodne z prawem

- Pozyskiwanie Danych Osobowych
 - Bazy otwarte
 - Wyszukiwarki
 - Socjotechnika

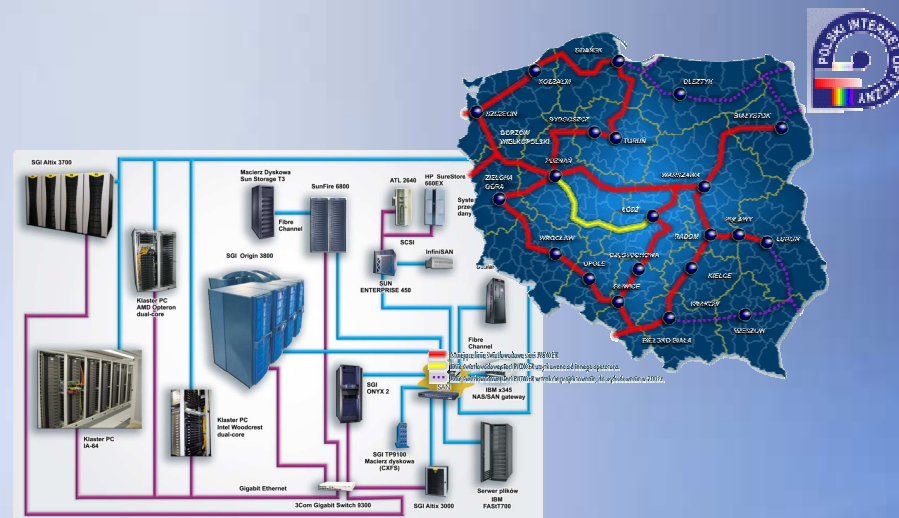
- Ciekawostki i przykłady

- Podsumowanie, pytania, ...

Wprowadzenie

PCSS

- Poznańskie Centrum Superkomputerowo-Sieciowe
 - Centrum obliczeniowe i składowania danych
 - Operator sieci PIONIER oraz POZMAN
 - Uczestnik projektów naukowo-badawczych
- Główne obszary zainteresowań:
 - Gridy, sieci nowej generacji, portale
 - Bezpieczeństwo sieci i systemów
- <http://www.pcass.pl>



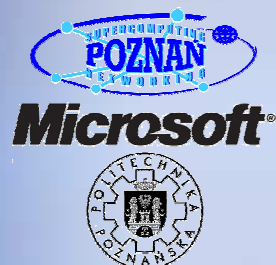
Zespół Bezpieczeństwa PCSS

- Dedykowany zespół istnieje od 1996 r.
- Podstawowy zakres prac Zespołu
 - Zabezpieczanie infrastruktury PCSS
 - Zadania bezpieczeństwa w projektach naukowo - badawczych
 - Szkolenie, transfer wiedzy
 - Badania własne
 - Audyty i doradztwo w zakresie bezpieczeństwa IT
- Najciekawsze badania z ostatnich lat
 - Bezpieczeństwo Instant Messengers (2004-05)
 - Badania sieci bezprzewodowych na terenie Poznania (2005)
 - Raport o bezpieczeństwie bankowości elektronicznej (2006)
 - Bezpieczeństwo serwerów WWW Apache i MS IIS (2007)
 - Raport o bezpieczeństwie zakupów internetowych (2008)
- <http://security.psnc.pl>



Centrum Innowacji Microsoft

- „Centrum bezpieczeństwa i usług outsourcingowych”




Partnerzy:

- Microsoft
- Poznańskie Centrum Superkomputerowo-Sieciowe
- Politechnika Poznańska



Zadania

- Bezpieczeństwo technologii Microsoft
 - Usługi hostingowe
 - Telemedycyna
- II Konferencja MIC: 13.05.08
 - <http://mic.psnc.pl>



Microsoft Centrum Innowacji

CENTRUM BEZPIECZEŃSTWA I USŁUG OUTSOURCINGOWYCH

<http://mic.psnc.pl>

Usługi dla uczelni, samorządów i firm:

- Referencyjna architektura usług hostingowych
- Audyty i szkolenia bezpieczeństwa
- Bezpieczeństwo technologii Microsoft
- Badania technologii multimedialnych
- Zdalne telekonsultacje medyczne

PARTNERZY



Microsoft



Dane Osobowe

Dane osobowe - definicja

Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Dane osobowe - dane wrażliwe

Są to dane dotyczące:

- Pochodzenia rasowego lub etnicznego
- Poglądów politycznych
- Przekonań religijnych lub filozoficznych
- Przynależności wyznaniowej, partyjnej lub związkowej
- Stanu zdrowia, kodu genetycznego, informacji o nałogach lub życiu seksualnym
- Skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym

Dane osobowe – opinie i świadomość

- **Opinie z życia wzięte**
 - “[...]kradzieży danych? A co tu kraść? Przecież wszystko dostępne jest... na tacy!?[...]”
 - “[...]Ludzie zaczęli się wstydzić nazwisk czy jak ? Kiedyś nikomu to nie przeszkadzało[...]
- **Ujawnianie danych na portalach społecznościowych**
 - **Imię i nazwisko, adres, numer telefonu**
 - **Wykształcenie, doświadczenie zawodowe**
 - **Pełne CV i listy motywacyjne**
- **Jeremy Clarkson [Top Gear] i jego dane osobowe**
 - **Strata 500 funtów, to niedużo za tego typu ignorację**

Ochrona Danych Osobowych

Ochrona Danych Osobowych akty prawne – polskie (1)

- **Konstytucja Rzeczypospolitej Polskiej** Art. 47, Art. 51
- **Ustawa z dnia 29 sierpnia 1997 r.** o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, ze zm.)
- **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.** w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)

Ochrona Danych Osobowych akty prawne – polskie (2)

- **Ustawa z dnia 27 lipca 2001 r.** o ochronie baz danych (Dz. U. z 2001 r. Nr 128, poz. 1402)
- **Ustawa z dnia 24 sierpnia 2007 r.** o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej (Dz. U. z 2007 r. Nr 165, poz. 1170)
- **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 15 listopada 2007 r.** w sprawie szczegółowego sposobu rejestrowania przypadków, w których uzyskano dostęp do danych przez Krajowy System Informatyczny (Dz. U. z 2007 r., Nr 223, poz. 1643)

Ochrona Danych Osobowych akty prawne – europejskie (1)

- **Dyrektywa 95/46/WE Parlamentu Europejskiego**
Zawiera definicje podstawowych terminów odnoszących się do dziedziny danych osobowych, ustala zasady zbierania, gromadzenia, przechowywania i udostępniania danych osobowych. Określa zasady i warunki zgodności przetwarzania danych osobowych z prawem oraz prawa osób, których dane dotyczą
- **Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r.** w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności (Dziennik Urzędowy Wspólnot Europejskich Serii L Nr 105 z dnia 13 kwietnia 2006 r.)

Ochrona Danych Osobowych akty prawne – europejskie (2)

- **Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r.** w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej (Dyrektywa o ochronie prywatności i komunikacji elektronicznej - aktualizowana).
- **Rekomendacja R (85)20 Komitetu Ministrów dla Państw Członkowskich** w sprawie ochrony danych osobowych używanych dla celów marketingu bezpośredniego, Rady Europy "Ochrona Danych Osobowych Wykorzystywanych dla potrzeb marketingu bezpośredniego" z 25 października 1985 r.
- **Rekomendacja R (81) 1 Komitetu Ministra dla Państw Członkowskich UE** w sprawie regulacji mających zastosowanie do zautomatyzowanych banków danych medycznych przyjęta przez Komitet Ministrów 23 stycznia 1981 r.

Klauzule dotyczące danych osobowych

- Curriculum Vitae, list motywacyjny
- Konkursy
- Ankiety
- Czy je czytamy? Czy wiemy, na co się zgadzamy?

Generalny Inspektor Ochrony Danych Osobowych

- **Organ powołany przez Sejm RP za zgodą Senatu**
- **Zajmuje się sprawami danych osobowych**
- **Kadencja – 4 lata**
- **Działa na podstawie ustawy z dnia 29 sierpnia 1997 r.**
- **Aktualny Inspektor - Michał Serzycki**
- **Siedziba - Warszawa**
- <http://www.giodo.gov.pl/>

Europejski Inspektor Ochrony Danych

- **Organ powołany przez Parlament Europejski i Radę UE**
- **Kadencja – 5 lat**
- **Kompetencje dotyczą instytucji i organów wspólnotowych**
- **Działa na podstawie Rozporządzenia Nr 45/2001 Parlamentu Europejskiego i Rady z 18 grudnia 2000 r**
- **Aktualny Inspektor - Peter J. Hustinx**
- **Siedziba - Bruksela**
- <http://www.edps.europa.eu/>

Sposoby ochrony danych we własnym zakresie

- **Podnoszenie własnej świadomości**
- **Weryfikacja obecności swoich danych w bazach**
- **Dokładne czytanie klauzul, które podpisujemy**
- **Ochrona przed wyciekami danych**
- **Polityka bezpieczeństwa w firmach**

Metody wykorzystywania baz Danych Osobowych

Wykorzystanie zgodne z prawem

- Rozsyłanie faktur, rachunków, ...
- Informowanie o spotkaniach, imprezach
- Reklama za zgodą
- Przesyłanie materiałów [np. prenumerat]
- Inne...

Wykorzystanie niezgodne z prawem

- **Spam**
- **Bezprawne sprzedawanie baz danych**
- **Podszywanie się - kradzież tożsamości**
- **Przestępstwa finansowe**

Pozyskiwanie Danych Osobowych

Bazy otwarte i półotwarte

- Krajowy Rejestr Długów
- Biuro Ewidencji Ludności i Dowodów Osobistych
- Książki telefoniczne

Wyszukiwarki

- **Curriculum Vitae filetype:pdf inurl:edu.pl**
- **Curriculum Vitae inżynier informatyk filetype:doc**
- **kontakty filetype:text inurl:ftp**
- **[imię, nazwisko, numer telefonu, email, numer gg ...]**

Socjotechnika

- **Wyłudzenia przez telefon, email, gg**
- **Podszywanie się pod osoby**
- **Phishing [Pharming]**
- **Szeroka dowolność scenariuszy socjotechnicznych**
- **Brak świadomości ludzi odpowiedzialnych za dane**

Ciekawostki i przykłady

Zadania w hakerskiej olimpiadzie

- Usunąć z Internetu wszystkie dane na swój temat
- Sfabrykować pełen zestaw fikcyjnych danych
- Stworzyć w Internecie historię konkretnej (fikcyjnej) osoby
- Fikcyjna firma
- <http://forums.hak5.org/index.php/topic,8038.0.html>

nasza-klasa.pl

- **Czy dane podawane na portalu to dane osobowe?**
- **Czy wiemy, na co się godzimy?**
- **Kto przegląda nasze dane?**
- **Automaty do wyciągania danych**

Dane osobowe a "ukierunkowany" spam

- Skuteczność "tradycyjnego" spamu – ułamek procenta
- Skuteczność "ukierunkowanego" spamu – kilkadziesiąt procent
- Czy dostaliśmy ofertę produktu, nad którym się zastanawialiśmy?
- Jak reklamodawca/producent do nas trafił?

Adres IP – daną osobową!

- Adres IP może bezpośrednio identyfikować osobę
- Dyrektywa 94/46/WE Parlamentu Europejskiego
- Potwierdzenie na stronach GIODO
- Co to oznacza dla przestępców (piratów, crackerów, ...)
- http://www.giodo.gov.pl/394/id_art/2028/j/pl/

Ile kosztują dane osobowe?

- **Karty kredytowe 0,50-5 USD**
- **Konta bankowe 30-400 USD**
- **Hasła do kont e-mail 1-350 USD**
- **Adresy e-mail 2-4 USD/MB**
- **Pełne dane osobowe 10-150 USD**
- **Numery SSN (social security numbers) 5-7 USD**

Tytuły prasowe

- **“Skradziono dane osobowe kilkuset tysięcy ludzi”**
- **“MON udostępnia dane osobowe kandydatów”**
- **“Kradzież danych osobowych na Uniwersytecie Kalifornijskim”**
- **“Nasze dane osobowe na śmietniku”**
- **“CyberLover wyłudza dane osobowe”**
- **“Dane osobowe 16 milionów moskwian w internecie”**
- **“Ukradł dane osobowe miliona Polaków”**

Podsumowanie

- **Dane osobowe to nasza własność, którą trzeba chronić!**
- **Nieodpowiednio wykorzystane mogą być dla nas wielkim problemem**
- **Najlepszym sposobem ochrony – podnoszenie świadomości**

Pytania, dyskusja



Dziękuję za uwagę :-)

Więcej informacji



Jakub Tomaszewski, PCSS:
bluerose@man.poznan.pl



Centrum Innowacji Microsoft:
<http://mic.psnc.pl>
mic-tech@lists.man.poznan.pl



PCSS:
<http://www.pcass.pl>



Zespół Bezpieczeństwa PCSS:
<http://security.psnc.pl>



8 marca

Dzień Kobiet

Wszystkiego najlepszego!!!