Organizacja środowiska pracy dla Administratora Bezpieczeństwa Informacji

w nawiązaniu do ochrony danych osobowych

Przemysław Rytka
Opiekun pracy: dr Ryszard Kossowski

Agenda

- Dlaczego taki temat?
- Dlaczego chronić?
- Krótko:
  - Źródła prawa,
  - Co to są dane osobowe,
  - ABI, ADO;
- Wymagania dot. ochrony wynikające z rozporządzenia,
- Moja propozycja organizacji ochrony danych osobowych,
- Kto powinien się zajmować ochroną,
- Krótki opis pracy dyplomowej.

Dlaczego taki temat?

- Brak ogólnodostępnych informacji,
- Brak wiedzy w firmach na ten temat,
  - Własne przykre doświadczenia wynikające z tego,
- Prawdopodobnie żaden prawnik nie napisałby pracy zrozumiałej dla informatyków (kodowanie!=szyfrowanie itp.).
- ?

Dlaczego chronić?

- KONSTYTUCJA RZECZYPOSPOLITEJ POLSKIEJ
- Art. 47 „Każdy ma prawo do ochrony prawnej życia prywatnego”
- Art. 51
  - Ust. 1. „Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby”
  - Ust. 2. „Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym”
  - Ust. 3. „Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa”
  - Ust. 4. „Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą”
  - Ust. 5. „Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa”

Dlaczego chronić?

- Niechęć do rozpowszechniania informacji o sobie (np. choroby),
- Możliwość podszycia się (Jeremy Clarkson☺),
- Życie codzienne: np. rekrutacja, spam.

Źródła prawa

- Ustawa z dnia 29.08.1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.),
- Ustawa z dnia 22.01.2004 r. o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz. U. Nr 33, poz. 285),
- 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. Nr 100, poz 1024).

Dane osobowe

- „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”,
- „Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań”.

Dane osobowe

- Dane wrażliwe
  - Dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym (art. 27 ust. 1 UODO).
  - Np.: Nałogi – hotel i rezerwacja pokoju dla palących lub nie.
- Dane zwykłe
  - Wszelkie inne dane osobowe.

ADO i ABI

- ADO (Administrator danych) – organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych
  - Np. zarząd spółki.
- ABI (Administrator bezpieczeństwa informacji) – wyznaczona przez administratora danych osoba nadzorująca przestrzeganie zasady zabezpieczeń danych osobowych, chyba że administrator danych sam wykonuje te funkcje.
  - Np. bardzo często jeden z informatyków☺

Jak chronić

- Obligatoryjne
  - Obowiązek stosowania wynika z przepisów prawa,
- Fakultatywne
  - Związane z analizą zagrożeń dla konkretnej jednostki organizacyjnej.

Zabezpieczenia wynikające z rozporządzenia

- Dokumentacja systemów,
- Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
- Polityka Bezpieczeństwa Informacji,
- Logowanie zdarzeń w systemach + raporty,
- ABI?

Polityka i Instrukcja

- Polityka bezpieczeństwa:
- Wykaz budynków, pomieszczeń lub części pomieszczeń…,
- Wykaz zbiorów danych osobowych + programów przetwarzających,
- Opis struktury zbiorów opisujący zawartość pól i powiązania,
- Sposób przepływu danych pomiędzy poszczególnymi systemami,
- Opis zabezpieczeń technicznych i organizacyjnych,

- Instrukcja:
- Procedury nadawania uprawnień,
- Metody i środki uwierzytelnienia + procedury,
- Zasady: rozpoczęcia, zawieszenia i zakończenia pracy z systemem, tworzenia kopii zapasowych
- Sposób, miejsce i okres przechowywania:
  - Elektronicznych nośników informacji zawierających dane osobowe,
  - Kopii zapasowych,
- Zasady działania oprogramowania antywirusowego,
- Zasady zapewnienia rozliczalności przekazywania danych osobowych,
- Zasady wykonywania przeglądów i konserwacji systemów oraz nośników informacji.

Zabezpieczenia wynikające z przepisów prawa

- Poziomy zabezpieczeń:
  - Podstawowy
    - Nie są przetwarzane dane osobowe określone w art. 27 Ustawy (wrażliwe)
    - Żaden z komponentów nie jest połączony z siecią publiczną
  - Podwyższony
    - Przetwarzane dane osobowe określone w art. 27 Ustawy (wrażliwe)
    - Żaden z komponentów nie jest połączony z siecią publiczną
  - Wysoki
    - Co najmniej jeden komponent systemu informatycznego jest połączony z siecią publiczną

Zabezpieczenia wynikające z rozporządzenia – poziom podstawowy

- Ograniczenie fizycznego dostępu do obszaru przetwarzania + upoważnienia,
- Logowanie dostępu do informacji,
- Indywidualne identyfikatory + uwierzytelnienie przed uzyskaniem dostępu,
- Zabezpieczenia antywirusowe,
- Zabezpieczenia przed awarią sieci zasilającej,
- Zmiana haseł co 30 dni. Hasła > 6 znaków,
- Kopie zapasowe – bezpiecznie przechowywane i usuwane po ustaniu użyteczności,
- Szyfrowanie danych na laptopach,
- Niszczenie informacji na nośnikach przed:
  - Likwidacją nośnika,
  - Przekazaniem nośnika,
  - Naprawą nośnika,
- Monitoruje to wszystko administrator☺

Zabezpieczenia wynikające z rozporządzenia – poziom podwyższony

- Wszystko z poziomu podstawowego,
- Hasła > 8 znaków, małe i wielkie litery oraz cyfry lub znaki specjalne,
- Dane wrażliwe przekazywane poza obszar zabezpiecza się w sposób zapewniający poufność i integralność tych danych (+informacja o zasadach w Instrukcji zarządzania systemem informatycznym).

Zabezpieczenia wynikające z rozporządzenia – poziom wysoki

- Wszystko z poziomu średniego,
- Fizyczne lub logiczne zabezpieczenia przed zagrożeniami z sieci publicznej, chroniące przed nieuprawnionym dostępem,
  - Jeśli logiczne, obejmują:
    - kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną,
    - kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych,
- Kryptograficzna ochrona danych uwierzytelniających przesyłanych przez sieć publiczną (ale już nie samych danych).

Jak chronić – powołanie ABI

- Art. 36 ust. 3
  - Administrator danych wyznacza administratora bezpieczeństwa informacji nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba że sam wykonuje te czynności.
- Art. 36 ust. 1
  - Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Jak chronić – powołanie ABI

- Nadzór:
  - Kontrola + kompetencje do przywrócenia stanu prawidłowego/ew. usunięcia nieprawidłowości (np. zarządzania, polecenia)
- Kontrola:
  - Ustalenie stanu faktycznego
  - Porównanie stanu faktycznego z wzorcem (stanem jaki powinien funkcjonować) i ustaleniu ewentualnych rozbieżności
  - Wyjaśnienie przyczyn powstania rozbieżności
  - Sformułowanie zaleceń pozwalających na uniknięcie podobnych rozbieżności w przyszłości

Jak chronić - normy

- ISO/IEC 27001,
- BS 7799,
- ISO/IEC 13335,
- Common Criteria,
- …

Jak chronić

- Analiza ryzyka
  - Dobór adekwatnych zabezpieczeń,
- PDCA – „Plan (Planuj) - Do (Wykonuj) - Check (Sprawdzaj) - Act (Działaj)”,
- Audyty:
  - Wewnętrzne,
  - Zewnętrzne:
    - 2 strony (my dostawcę usługi)
    - 3 strony (certyfikujący),
  - Testy penetracyjne (The Open Source Security Testing Methodology Manual – OSSTMM), The Open Web Application Security Project – OWASP),

Podmioty i osoby odpowiedzialne za ochronę danych

- Administrator danych,
- Podmiot, któremu administrator powierzył przetwarzanie danych,
- Administrator bezpieczeństwa informacji,
- Osoba upoważniona do przetwarzania danych osobowych:
  - Wszyscy pracownicy dopuszczeni do przetwarzania danych osobowych,
  - Także osoby z firm zewnętrznych są osobami przetwarzającymi dane osobowe np. osoby naprawiające sprzęt.

Krótki opis pracy dyplomowej

- To co w prezentacji tylko więcej☺,
  - „Tłumaczenie” dla informatyków przepisów prawa,
- Przykładowa analiza ryzyka,
- Przykładowe fragmenty procedur.

Pytania?