Jak zabezpieczać informacje w podmiotach przetwarzających dane osobowe

Jacek Biernacki

Jak cenne są dane przetwarzane przez organizację

- Bardzo cenne –jeżeli można je wykorzystać w celach biznesowych (i nie tylko) przez inne podmioty;
- Mało cenne – jeżeli są powszechnie dostępne, lub ich ujawnienie nie wywoła negatywnych skutków dla zainteresowanych;
- Możliwe do wyceny w ramach np. analizy ryzyka;
- Trudne do wyceny (bezcenne), np. utrata skutkuje utratą reputacji organizacji i zaprzestaniem działalności;

Jakie rodzaje / zakres informacji są przetwarzane przez organizację

- Biznesowe / strategiczne, plany rozwoju, inwestycji, ekspansji;
- Operacyjne / bieżące, finansowe, organizacyjne, personalne dot. pracowników organizacji;
- Dane osobowe dotyczące klientów, dane osobowe o charakterze wrażliwym;
- Dane gromadzone i przetwarzane na fizycznych nośnikach danych, przetwarzane i składowane lokalnie lub w zewnętrznych podmiotach;
- Dane gromadzone w postaci elektronicznej, przetwarzane lokalnie lub zdalnie, składowane lokalnie lub zewnętrznie w systemie upoważnionego podmiotu;

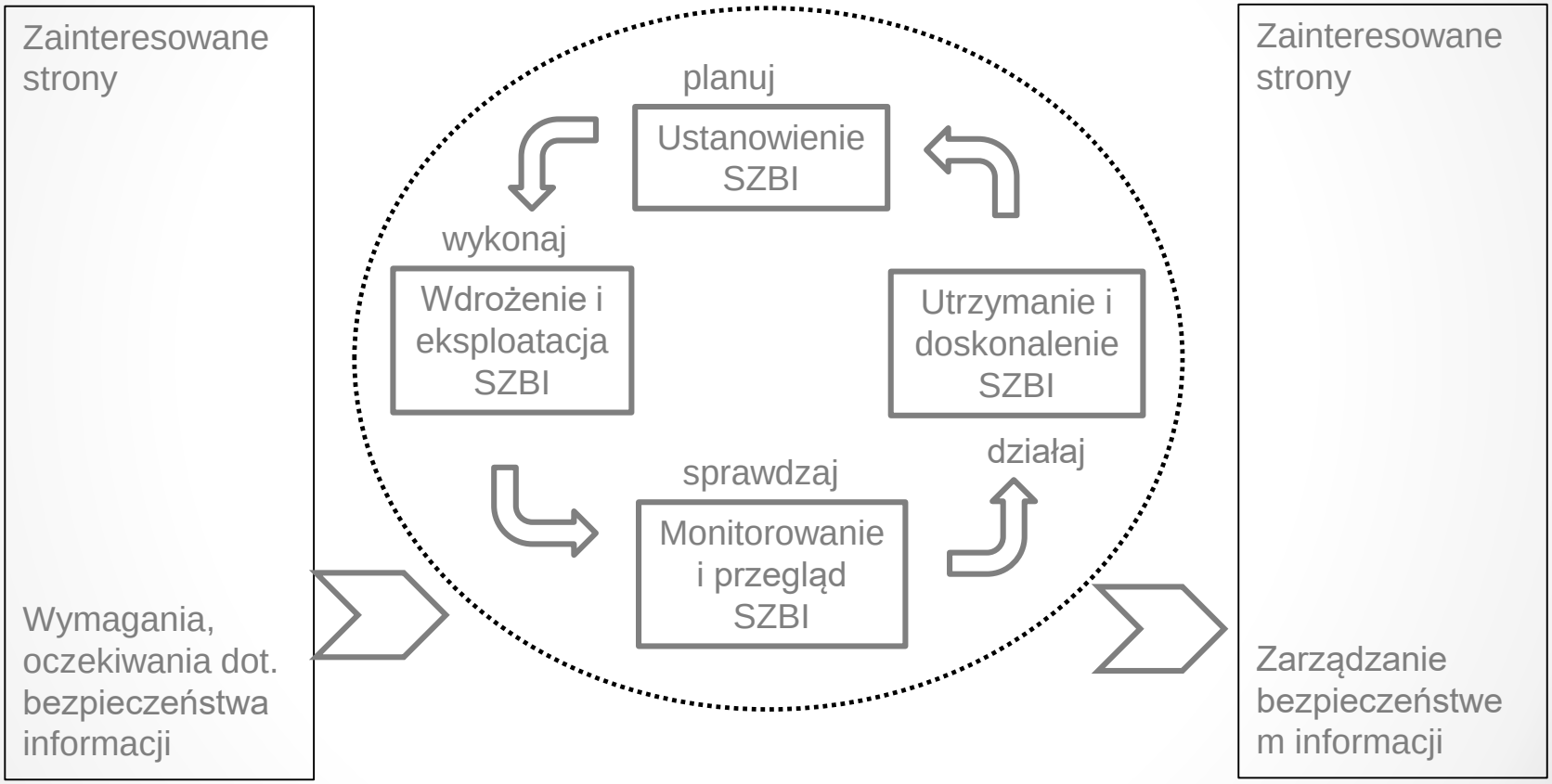
Co to jest bezpieczeństwo informacji

- bezpieczeństwo informacji (zgodnie z ISO 27001)

  to „zachowanie poufności, integralności i dostępności informacji. Dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność”

- Informacja jest bezpieczna, jeżeli zachowana jest co najmniej :
  - poufność – właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom,
  - integralność – właściwość polegająca na zapewnieniu dokładności i kompletności aktywów,
  - dostępność – właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.

System Zarządzania Bezpieczeństwem Informacji (SZBI)



- wg ISO

Zakres zagadnień SZBI

- Wynikający z normy ISO 27001
  - W sumie ponad 120 zagadnień szczegółowych w kilkunastu obszarach tematycznych
  - Polityki bezpieczeństwa informacji ,Organizacja bezpieczeństwa informacji
  - Bezpieczeństwo zasobów ludzkich, Zarządzanie aktywami
  - Kontrola dostępu , Kryptografia
  - Bezpieczeństwo fizyczne i środowiskowe, Bezpieczna eksploatacja
  - Bezpieczeństwo komunikacji, Pozyskiwanie, rozwój i utrzymanie systemów
  - Relacje z dostawcami, Zarządzanie incydentami związanymi z bezpieczeństwem informacji, Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania
  - Zgodność

Składowe systemu zarządzania bezpieczeństwem informacji

- Wymagania formalno–prawne
- Rozwiązania organizacyjne
- Rozwiązania techniczne

Zakres formalno- prawny

- Dyrektywy, Rozporządzenia EU, Ustawy
  - Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych
  - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG)
  - Projekt ustawy o ochronie danych osobowych (skierowany do Sejmu 04.2018);
- Normy, Standardy
  - Dotyczące bezpieczeństwa informacji / systemów informatycznych, ISO,seria 27000, COBIT;
- Polityki i regulaminy
  - Polityka bezpieczeństwa informacji, Kodeks postępowania;
- Procedury
  - Procedury operacyjne dotyczące zarządzania/ użytkowania systemów;

Zakres organizacyjny

- Osoby / role wymagane w zakresie zarządzani bezpieczeństwem informacji
  - Inspektora ochrony danych, Inspektor bezpieczeństwa informacji, Audytor, Administrator;
- Właściciele zasobów
  - Kierownicy komórek organizacyjnych, osoby wyznaczone za określony zakres przetwarzania danych;
- Zespoły
  - Zespół ds. wdrożenia (nowych rozwiązań), Zespół reagowania kryzysowego.

Rozwiązania techniczne

- System informatyczny własny
  - Zbudowany i zarządzany wewnętrznymi zasobami Organizacji / zewnętrznymi – outsourcing osobowy
  - Własna infrastruktura i licencjonowane oprogramowanie
  - Usługi świadczone na zewnątrz Organizacji w postaci serwisów
  - Wewnętrzne służby odpowiedzialne za utrzymanie i ochronę danych (w tym osobowych)
  - Wewnętrzne uregulowania dotyczące wszystkich obszarów bezpieczeństwa informacji;
- System informatyczny/ usługa od zewnętrznego dostawcy
  - System udostępniany zewnętrznie przez zewnętrznego dostawcę jako usługa (zwykle na zdefiniowany okres czasu), dane powierzone podmiotowi przetwarzającemu dane
  - Zewnętrzna infrastruktura i oprogramowanie / wewnętrznie stacje robocze, peryferia
  - Usługi świadczone na zewnątrz Organizacji w postaci serwisów udostępnianych przez podmiot przetwarzający dane osobowe
  - Wewnętrzne ograniczone służby odpowiedzialne za utrzymanie i ochronę danych (w tym osobowych)
  - Uregulowania wewnętrzne i zewnętrzne dotyczące obszarów bezpieczeństwa informacji / przetwarzania danych osobowych (Kodeks postępowania);

Zagrożenia

- Wewnętrzne
  - Mające swe źródło wewnątrz organizacji – pracownicy, rozwiązania programowe, infrastruktura, przepisy;
- Zewnętrzne
  - Mające swe źródło na zewnątrz organizacji – użytkownicy/ intruzi zewnętrzni, próby penetracji systemu, destabilizacji lub ograniczenia dostępu;
- Osobowe
  - Pracownicy Organizacji, pracownicy organizacji współpracujących / zewnętrznych posiadający dostęp do systemów;
- Techniczne
  - Podatności sprzętu i oprogramowania, awaria części zasobów uniemożliwiająca dalszą pracę, pojedynczy punkt awarii;
- Środowiskowe
  - Zagrożenia fizyczne, anomalie pogodowe;
- Wynikające z zakresu potencjalnego naruszenia bezp. danych
  - Naruszenie bezpieczeństwa pojedynczego rekordu, dużego zakresu danych;

Dokumenty - uwarunkowania

- Możliwie krótkie, zapisane językiem zrozumiałym dla odbiorców
- Adekwatne dla określonej grupy odbiorców w swojej treści i zakresie (użytkownicy, administratorzy, inspektorzy itd.)
- Zatwierdzone przez Kierownictwo organizacji i zarządzane przez uprawnione osoby
- Aktualne i dostępne dla wymaganych grup odbiorców

Personel - uwarunkowania

- W zakresie wykorzystania systemów / użytkownicy
  - Przeszkoleni w zakresie ochrony informacji
  - Zapoznani z wymaganymi dokumentami dotyczącymi ich zakresu działania
  - Wyposażeni w odpowiednie narzędzia, (identyfikacja i uwierzytelnienie, podpis elektroniczny)
  - Posiadający dostęp do odpowiednich narzędzi zgłaszania i eskalacji problemów / incydentów;
- W zakresie zarządzania systemami / personel zarządzający
  - Przeszkolony w zakresie ochrony informacji, technologii i systemów którymi zarządzają
  - Zapoznany z wymaganymi dokumentami dotyczącymi ich zakresu działania
  - Przyporządkowany do określonych ról ze wskazanym zakresem obowiązków/uprawnień
  - Posiadający odpowiednie zastępstwo na wypadek absencji
  - Wyposażony w odpowiednie narzędzia, zarządzanie, monitoring, audyt systemów, (ale również identyfikacja i uwierzytelnienie, podpis elektroniczny)
  - Posiadający dostęp do odpowiednich narzędzi zgłaszania i eskalacji problemów / incydentów, rozwiązywania problemów

Technologia - uwarunkowania

- Poufność informacji
  - Uprawnienia, mechanizm podwójnej kontroli (dwóch par oczu) w wybranych zakresach
  - Silne mechanizmy identyfikacji i uwierzytelnienia
  - Logowanie zdarzeń / audyt zdarzeń / aktywności użytkowników / systemów
  - Ochrona wewnętrzna / zewnętrzna, podsieci, strefy, firewall, ips;
- Integralność informacji
  - Podpis elektroniczny
  - Ograniczenia w zakresie modyfikacji / usuwania danych
  - Kontrola integralności danych;
- Dostępność informacji
  - Redundancja infrastruktury / system bez pojedynczego punktu awarii
  - Redundancja łączy
  - Kopie zapasowe, zarządzanie kopiami, przechowywanie;

Utrata bezpieczeństwa danych – przypadki / konsekwencje

- Holenderska firma DigiNotar (upadłość2011), wydawca certyfikatów SSL,
  - Atak wykryty po 1,5 miesiącu od ataku hakerów. Z DigiNotar skradziono ponad 500 certyfikatów SSL, w tym wystawione dla CIA, MI6 i Mossadu
- Rząd Królestwa Szwecji, utrata kontroli nad wrażliwymi danymi (2017)
  - Wyciekły szwedzkie dane dotyczące personelu wojskowego, osób w policyjnych bazach danych, osób w programie ochrony świadków oraz informacje dotyczące wojskowego sprzętu. Informacje zostały omyłkowo przesłane do osób w Czechach oraz Serbii podczas chaotycznej próby przeniesienia rządowych baz danych w ramach usług outsourcingowych
- NSA, ujawnienie tysięcy tajnych dokumentów (2013)
  - Edward Snowden były pracownik CIA i zleceniobiorca zatrudniony przez firmy Dell oraz Booz Allen Hamilton na umowach dla NSA, ujawnił na łamach prasy kilkaset tysięcy poufnych, tajnych i ściśle tajnych dokumentów NSA;

Dziękuję za uwagę

jacek@biernacki.co