

Bezpieczeństwo procesu przetwarzania danych

Michał Jakś

Oficer bezpieczeństwa ds.
IT



bezpieczeństwo



jakość



zaufanie

TALEX[®] S.A.

Bezpieczeństwo w procesie przetwarzania danych

Ochrona danych jest jednym z najważniejszych zadań zapewniających bezpieczeństwo organizacji (firmie), w głównej mierze polega na:

- zarządzaniu bezpieczeństwem,
- legalizacją i uwierzytelnianiem dostępu do danych,
- zarządzanie treścią.

Do zarządzanie bezpieczeństwem potrzebna jest tzw. polityka bezpieczeństwa.

Główną zasadą, którą należy się kierować podczas tworzenia zasad bezpieczeństwa, jest:

„zabronione jest wszystko, co nie zostało bezpośrednio dozwolone”.



Bezpieczeństwo w procesie przetwarzania danych

Ogólnie przyjęte zasady zabezpieczania systemów informatycznych

- Bezpieczeństwo informatyczne jest elementem ułatwiającym realizację misji organizacji.
- Bezpieczeństwo informatyczne jest integralnym elementem właściwego zarządzania.
- Bezpieczeństwo informatyczne powinno być efektywne pod względem kosztowym.
- Odpowiedzialność właścicieli systemu wybiega poza granice ich organizacji.
- Odpowiedzialność za bezpieczeństwo informatyczne oraz zasady rozliczania użytkowników powinny być jednoznaczne.
- Bezpieczeństwo informatyczne wymaga jasno zdefiniowanego i zintegrowanego podejścia.
- Skuteczność zabezpieczeń systemu powinna być okresowo weryfikowana.
- Bezpieczeństwo informatyczne jest ograniczone czynnikami społecznymi.

Zagrożenia w procesie przetwarzania danych

Główne zagrożenia:

- zewnętrzne:
 - włamania i kradzież urządzeń komputerowych
 - wirusy i robaki internetowe
 - ataki typu DoS
 - działania hackerów zmierzające do podmiany informacji przechowywanych w systemach
 - działania hackerów zmierzające do przejęcia kontroli nad systemami
- wewnętrzne:
 - błąd użytkownika
 - zanik zasilania
 - awaria sprzętu
 - błędy w oprogramowaniu systemowym, bazodanowym i aplikacyjnym
 - błąd administratora systemu



Straty spowodowane utratą danych/przestojem

75 procent firm z listy Fortune 1000 padło już ofiarą przypadkowej lub będącej wynikiem wrogiego działania utraty danych. Średni koszt, jaki ponosi tego rodzaju firma w wyniku utraty danych to 6,2 miliona dolarów. Dochodzi do tego ok. 4,1 miliona dolarów z tytułu utraconych możliwości biznesowych.

FBI/CSI-Study on Computer Crime and Computer Security, 2006

„Jednym z największych problemów współczesnych przedsiębiorstw jest utrata danych. Jedna trzecia respondentów badanych przez firmę McAfee wierzy, że incydent związany z utratą danych mógłby zdecydować o upadku ich firmy”



Straty spowodowane utratą danych/przestojem

10 największych kradzieży danych w 2007 roku

10: Monster.com Liczba ofiar: co najmniej 1,3 mln USD

9: Commerce Bank of Wichita Liczba ofiar: 20

8: **Indianapolis Power and Light** Liczba ofiar: ok. 3 tys.

Z zasobów zakładu energetycznego z Indianapolis ktoś ukradł kompletne dane ok. 3 tys. klientów - zawierające m.in. numery ubezpieczenia społecznego, dane teleadresowe itp. **Firma odkryła kradzież dopiero po 4 latach** (a w tym czasie dane zostały m.in. opublikowane w Internecie) to incydent ten z pewnością zasługuje na to, by trafić do naszego zestawienia.

7: TSA (Transportation Security Administration) Liczba ofiar: 3390

6: Shaw's Supermarket Liczba ofiar: 472

5: Swedish Urology Group Liczba ofiar: kilkaset

4: Nature Conservancy Liczba ofiar: 14 tys.

3: TSA (po raz drugi) Liczba ofiar: ok. 100 tys.

2: Urząd Podatkowy i Celny Jej Królewskiej Mości
Liczba ofiar: 25 mln.

1: TJX Liczba ofiar: miliony



Straty spowodowane utratą danych/przestojem

Najczęstsze przyczyny utraty danych

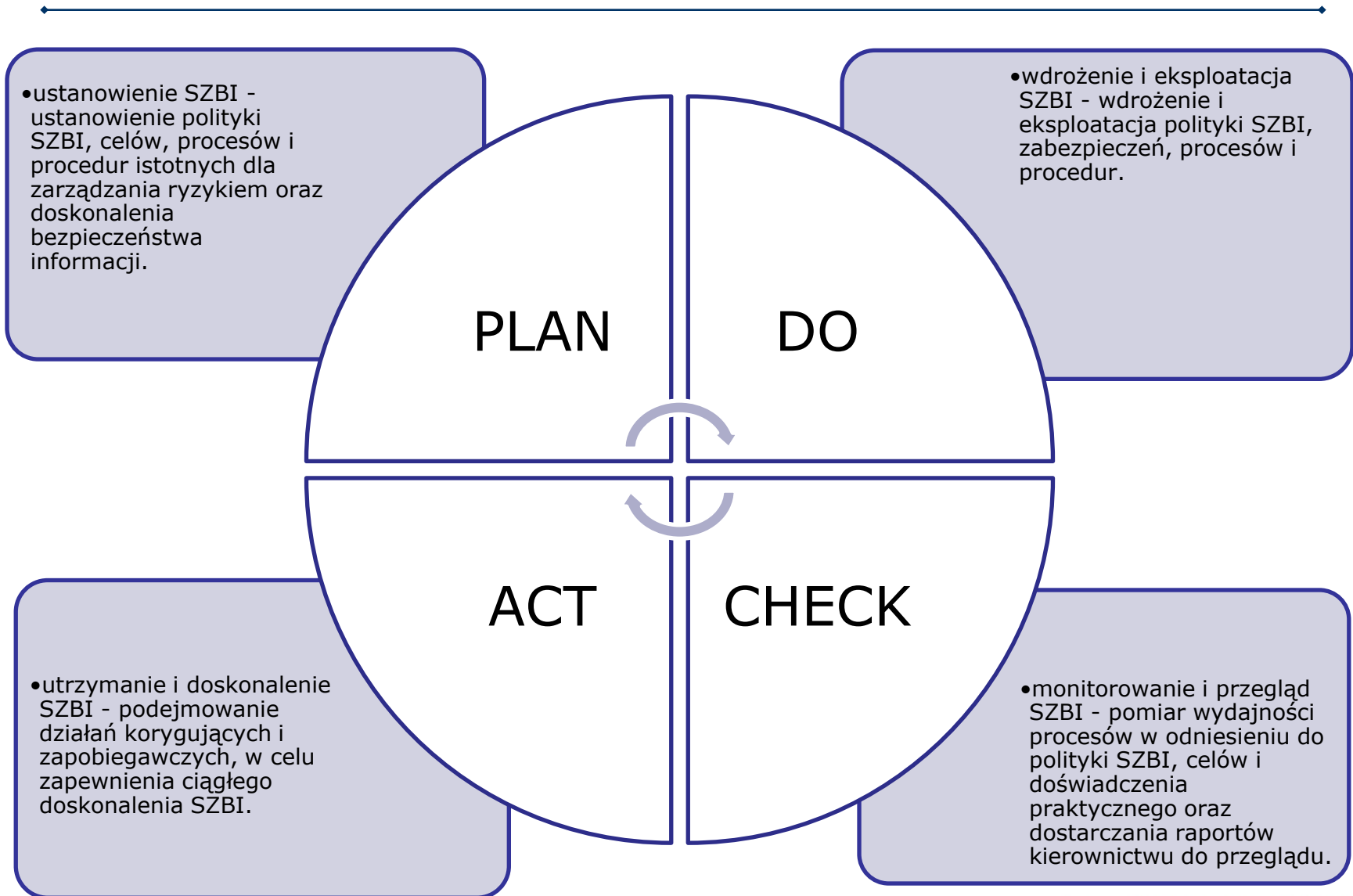


Źródło: IT Policy Compliance Group; opracowanie: IDG.pl

Norma ISO 17799

- ▶ Norma ISO 17799 "Praktyczne zasady zarządzania bezpieczeństwem informacji" została wydana w styczniu 2007 jako PN-ISO/IEC 17799:2007 i stanowi obowiązkowe uzupełnienie normy PN-ISO/IEC 27001:2007 „Systemy zarządzania bezpieczeństwem informacji. Wymagania” i jest to swoistą książką opijająca najlepsze praktyki z zakresu bezpieczeństwa informacji.
- ▶ Przez praktyków uważana za najlepsze opracowanie dotyczące systemowego podejścia do zarządzania bezpieczeństwem informacji.

Metody zabezpieczenia informacji



ISO27001 oraz 17799 jako zbiór dobrych praktyk w zakresie bezpieczeństwa informacji

Kluczową częścią normy ISO 27001:2005 jest załącznik A, który zawiera listę zabezpieczeń podzielonych na grupy:

- polityka bezpieczeństwa,
- organizacja bezpieczeństwa informacji,
- zarządzanie aktywami,
- bezpieczeństwo personelu,
- bezpieczeństwo fizyczne i środowiskowe,
- zarządzanie systemami i sieciami,
- kontrola dostępu do systemu,
- rozwój i utrzymanie systemu informacyjnego,
- zarządzanie incydentami bezpieczeństwa informacji,
- zarządzanie ciągłością działania,
- zapewnienie zgodności.

Norma ISO 17799 wywodzi się z brytyjskiego standardu bezpieczeństwa BS 7799. Stanowi zestaw wskazówek dla wdrożenia i utrzymania bezpieczeństwa informacji w przedsiębiorstwie.

- polityka bezpieczeństwa,
- kontrola dostępu do informacji,
- zabezpieczenia na poziomie organizacyjnym,
- klasyfikacja i kontrola zasobów,
- zarządzanie działaniem urządzeń informatycznych,
- przestrzeganie obowiązujących procedur i przepisów prawa,
- pracownicy,
- zabezpieczenie fizyczne organizacji i otoczenia,
- zarządzanie ciągłością,
- opracowywanie i utrzymywanie systemów informatycznych.

Bezpieczeństwo informacji

1. **Systemy kontroli dostępu**

Podstawą założeń bezpieczeństwa informacji jest kontrola dostępu do nich w taki sposób, aby była możliwość łatwej ochrony przed nieautoryzowanym dostępem, modyfikacją lub ujawnieniem sekretnych danych.

2. **Bezpieczeństwo sieci i urządzeń telekomunikacyjnych**

Telekomunikacja oraz sieci komputerowe zawierają w sobie dużą liczbę mechanizmów, urządzeń, oprogramowania oraz protokołów, które muszą się przenikać oraz integrować. Domena mówiąca o sieciach komputerowych jest jednym z trudniejszych i bardziej złożonych tematów.

3. **Praktyki zarządzania bezpieczeństwem**

Często słyszymy o wirusach zarażających miliony komputerów w sieci, powodujących milionowe straty, hackerach z całego świata, zdobywających dane o numerach kart kredytowych w instytucjach zarówno finansowych jak i w zwykłych firmach. Strony webowe wielkich korporacji są podmieniane z powodów politycznych, dla zabawy lub osobistych. Czytamy o świetnych hackerach, którzy trafili do więzienia za swoje cyber-czyny. To jest ta romantyczna część dotycząca bezpieczeństwa sieci i systemów komputerowych. Jednakże ten typ aktywności ma mało wspólnego z codziennymi zadaniami z jakimi spotyka się dział odpowiedzialny za bezpieczeństwo informacji w firmie. Mimo, że wirusy i hacking zajmują najwięcej miejsca w prasie (patrząc ze strony bezpieczeństwa), to największa uwaga przy tworzeniu działu ds. bezpieczeństwa sieci, informacji oraz systemów powinna być skupiona na zarządzaniu bezpieczeństwem.

4. **Projektowanie systemów i aplikacji**

Aplikacje oraz systemy projektowane są dla użytkownika końcowego. W trakcie projektowania przewiduje się szereg udogodnień oraz rozwiązań sprzyjających obsługującemu, nie zwraca się praktycznie żadnej uwagi na bezpieczeństwo projektowanej aplikacji czy systemu. Z reguły najpierw projektuje się funkcjonalność programu, a dopiero w późniejszym etapie jej bezpieczeństwo. Najlepszą praktyką przy tworzeniu aplikacji jest projektowanie bezpieczeństwa równoległe z projektowaniem funkcjonalności. Lepiej jest zaprojektować od początku bezpieczną aplikację niż potem dodawać dodatkowe rzeczy, które z reguły zmniejszają jej doskonałą funkcjonalność oraz pozostawiają wiele „dziur” w bezpieczeństwie.

5. **Kryptografia**

Kryptografia jest metodą przechowywania oraz transmisji danych w formie, w której będą one czytelne tylko dla osoby mającej do tego prawo i posiadającej odpowiednie hasła, klucze i inne dane umożliwiające odczytanie tych danych. Dzięki tej dziedzinie nauki nasze strategiczne dane pozostają bezpieczne na dysku lub niezagrożone „biegają” po publicznej lub prywatnej sieci komputerowej. Mimo, że głównym celem szyfrowania oraz mechanizmów je dostarczających jest ukrycie informacji przed niepożądanym przejęciem, podsłuchaniem lub odczytaniem, większość algorytmów można złamać, wystarczy tylko mieć odpowiednio dużo czasu, zasobów oraz zaangażowania. Wobec powyższego można przyjąć, że głównym zadaniem kryptografii jest spowodowanie, aby informacja była zaszyfrowana w taki sposób, by deszyfracja jej zajęła tak długi czas, zużyła tak dużo zasobów, żeby była już dla intruza nieprzydatna.

6. **Modele i architektury bezpieczeństwa**

Zagadnienie bezpieczeństwa systemów i informacji w organizacji zawiera wiele obszarów. Każdy z obszarów ma swoje słabe punkty, ale również różnego rodzaju środki zaradcze, dzięki którym jesteśmy w stanie zminimalizować ryzyko wystąpienia danego problemu. Brak zrozumienia oraz brak umiejętności zdefiniowania wszystkich obszarów wraz z ich słabymi punktami może doprowadzić do tego, że nawet najlepiej zabezpieczone dane, maszyny, programy, protokoły stają się łatwym celem ataku oraz mogą powodować, że system jako całość nie będzie w stanie się obronić przed intruzem. Dwie fundamentalne koncepcje bezpieczeństwa informacji w organizacji to – model bezpieczeństwa – który określa w jaki sposób bezpieczeństwo będzie implementowane w firmie i w jakiej postaci. Druga koncepcja opiera się na architekturze systemu komputerowego – która stanowi szkielet oraz strukturę systemu bezpieczeństwa firmy

7. **Operacyjne bezpieczeństwo**

Operacyjne bezpieczeństwo odnosi się do wszystkiego, co pomaga administratorowi utrzymać sieć, systemy komputerowe oraz środowisko pracy sprawnym i działającym w bezpieczny sposób. Systemy znajdują się w stanie operacyjnym z reguły zaraz po zakończeniu fazy projektu oraz wdrożenia. Zawiera się w tym również utrzymanie oraz wszystkie zadania związane z codzienną pracą personelu nad zaimplementowanym rozwiązaniem (systemem, siecią, aplikacją). Praca personelu obsługującego wdrożony produkt, to rutynowe czynności, które wpływają na ciągłość pracy systemów, sieci czy aplikacji i zapewniają jej dostępność oraz jakość na odpowiednio wysokim poziomie. Dzisiaj bezpieczna sieć czy program, za tydzień wcale już nie musi spełniać postawionych mu kryteriów, wtedy właśnie ma znaczenie pojęcie operacyjności, czyli ciągłego dbania o bezpieczeństwo zbudowanego rozwiązania.

Bezpieczeństwo informacji

8. **Planowanie ciągłości funkcjonowania organizacji oraz odtwarzania systemów**

Każdego dnia tysiące danych, informacji, wiadomości zostaje uszkodzonych, zniszczonych, wykradzonych. Setki, tysiące firm jest każdego dnia obiektem różnego rodzaju nieszczęść prowadzących do utraty danych – powodzie, pożary, tornada, ataki terrorystyczne czy wandalizm. Organizacje, które przetrwają katastrofy, to przeważnie firmy, które były przygotowane na to i miały odpowiednie plany na wypadek nieszczęścia. Jednak takich firm jest zaledwie nikły procent. Większość organizacji nie posiada takich planów, co oznacza, że w razie katastrofy, jaka przydarzyła się 11 września 2001 roku, firmy te będą zmuszone po prostu zamknąć swoje drzwi, gdyż nie będą w stanie kontynuować swojej działalności.
9. **Prawo, dochodzenie i etyka**
10. **Bezpieczeństwo fizyczne**

Bezpieczeństwo firmy nie kończy się na sprawnie działających komputerach, systemach, aplikacjach czy urządzeniach sieciowych, lecz odnosi się ono również do infrastruktury firmy oraz bezpieczeństwa fizycznego. Bezpieczeństwo fizyczne odkrywa inny rodzaj niebezpieczeństw, niedoskonałości materiałów, niedokładności ludzi oraz ryzyka z tym związanego. Fizyczne mechanizmy bezpieczeństwa zawierają projekty sieci, położenia okablowania, zabezpieczenia drzwi zamkiem, czytnikami kart, urządzeniami przeciwpożarowymi (gaśnice, gazy absorbujące tlen w pomieszczeniu), przeszkolenie personelu. Zadaniem fizycznych czynników mających wpływ na bezpieczeństwo jest ochrona ludzi, danych, urządzeń, systemów oraz zapewnienie funkcjonalności tychże

Wybór partnera w zakresie outsourcingu

Najważniejszym elementem jaki należy brać pod uwagę podczas wyboru firmy outsourcingowej jest jej rzetelna weryfikacja pod kątem jakości świadczonych usług, oraz dołności do właściwej realizacji kontraktu. Krytyczna jest także rzetelna analiza oferty i adekwatna ocena ryzyka. Częstym błędem popełnianym przez organizacje podczas dokonywania wyboru partnera jest kierowanie się wyłącznie ceną. Redukcja kosztów jest tylko jednym z elementów outsourcingu. Nawiązanie długofalowej współpracy z partnerem zewnętrznym powinno się odbyć na podstawie znacznie szerszego spektrum kryteriów.

Outsourcing infrastruktury IT

Bezpieczeństwo i ciągłość działania

CENTRUM ZAPASOWE

TALEX[®] S.A.

www.talex.pl

Bezpieczne Talex Data Center

- całodobowa ochrona fizyczna
- system wydzielonych stref wewnętrznych
- rozbudowany system antywłamaniowy
- system telewizji dozorowej (CCTV)
- nowoczesny system kontroli dostępu z elementami biometrii
- centralny system monitorowania bezpieczeństwa - wykrywanie i eskalacja incydentów
- rygorystyczna polityka bezpieczeństwa informacji potwierdzona certyfikatem ISO 27001:2005
- system wykrywania pożaru podłączony do systemu monitorowania straży pożarnej
- uzgodniona z Państwową Strażą Pożarną i wspólnie testowana procedura działań gaśniczych
- stałe urządzenia gaśnicze wykorzystujące gaz bezpieczny dla ludzi, sprzętu i środowiska
- materiały budowlane i wykończeniowe certyfikowane pod kątem wytrzymałości ogniowej



Outsourcing infrastruktury IT

Outsourcing IT

TALEX DATA CENTER

TALEX[®] S.A.

www.talex.pl

The image shows four hands cupping a small green plant growing from soil. The background is a green and white abstract design with light rays. The text 'Outsourcing infrastruktury IT' is in the top left, 'Outsourcing IT' is in the middle right, and 'TALEX DATA CENTER' is in large white letters at the bottom of the image area. Below the image is the Talex logo and the website address.

Bezpieczne Talex Data Center



Bezpieczne Talex Data Center

Wydajne systemy klimatyzacji i wentylacji zapewniające optymalne warunki pracy urządzeń

System przeciwpożarowy połączony z centralką najbliższej Straży Pożarnej; system gaśniczy wykorzystujący gaz FM-200

Strefa serwerów głównych - to tutaj przechowywane są najcenniejsze dane

System nadmiarowych UPS-ów gwarantujący podtrzymanie napięcia w przypadku wystąpienia awarii

Modułowe przestrzenie gwarantujące fizyczną i logiczną separację poszczególnych klientów czy systemów

Pomieszczenia monitoringu z dyżurującymi całą dobę specjalistami dbającymi o bezawaryjną pracę systemów

Całodobowa ochrona; kontrola dostępu oparta na rozwiązaniach biometrycznych

