Jakość danych w systemach informatycznych zakładów ubezpieczeń 25.III.2009

Aspekty normalizacyjne zarządzania incydentami bezpieczeństwa w kontekście integralności i dostępności danych

Janusz Cendrowski
Asseco Systems S.A.
Komitet Techniczny Nr 182

Skróty i definicje

- IB - Incydent bezpieczeństwa
- PBI – Polityka Bezpieczeństwa Informacji
- PZIB – Proces Zarządzania Incydentami Bezpieczeństwa
- JO - Jednostka organizacyjna
- IBTI - Inspektor bezpieczeństwa teleinformatycznego
- SZBI – System Zarządzania Bezpieczeństwem Informacji

Cel prezentacji

- Przedstawienie pojęcia incydentu w PN-ISO/IEC 27001 i PN-ISO/IEC 20000
- Przedstawienie normalizacyjnych aspektów zarządzania incydentami bezpieczeństwa w normach
  - PN-ISO/IEC 17799 (ISO/IEC 27002)
  - TR ISO/IEC 18044
- Przedstawienie powiązań procesu PZIB z innymi procesami w IT
- Interpretacja przepisów dotyczących ochrony informacji w zakresie zarządzania IB
- Uwaga techniczna
  - Znak (?) – wątpliwości prelegenta

Przepisy

- [UODO] – Ustawa z dnia 29.08.1997 o ochronie danych osobowych (Dz. U. Nr 133 poz. 883)
- [R1024] – Rozporządzenie Ministra SWiA z 29.04.2004 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)
- [UOIN] – Ustawa z dnia 22 stycznia 1999 o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95)
- [R1433] – Rozporządzenie Prezesa RM z dnia 25.08.2005 w sprawie określenia podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz.U. 171, poz. 1433)

Krótki przegląd - przepisy

- [UIDP] – Ustawa z dnia 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. Nr 64, poz. 565).
- [R1766] – Rozporządzenie RM z dnia 11.10.2005 w sprawie określenia minimalnych wymagań dla systemów teleinformatycznych (Dz.U.212, poz. 1766)
- [Zal_BTI] Zalecenia dotyczące bezpieczeństwa teleinformatycznego, ABW, wersja 1.1, Warszawa – grudzień 2006.
- [Zal_AZR] Szczegółowe zalecenia dotyczące analizy oraz zarządzania ryzykiem w systemach i sieciach teleinformatycznych, wersja 1.2, ABW, Warszawa – grudzień 2006.

Polskie normy

- [13335-1] – PN-I-13335-1:1999 Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa
- [27001] – PN-ISO/IEC 27001:2007 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania
- [17799] – PN-ISO/IEC 17799:2007 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji
- [20000]– PN-ISO/IEC 20000-1:2007 - Technika informatyczna - Zarządzanie usługami - Część 1: Specyfikacja; PN-ISO/IEC 20000-2:2007 - Technika informatyczna - Zarządzanie usługami - Część 2: Reguły postępowania.

Normy zagraniczne

- [18044] – TR ISO/IEC 180044 *Information technology – Security techniques – Information security incident management*

Problem

- Relacja bezpieczeństwa informacji do jakości danych
- Jakość danych rozumiana jako ich
  - Integralność
  - Dostępność
  - Autentyczność
- Jak reagować na incydenty, żeby zmniejszyć ich skutki i powtarzalność?

Definicje incydentów

- [20000]
  - **Incydent** – każde zdarzenie, które nie należy do standardowej operacji usługi i które powoduje lub może powodować przerwę w dostarczaniu tej usługi lub redukcję jej jakości
- [27001], [17799], [18044]
  - **incydent związany z bezpieczeństwem informacji** jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji

Definicje incydentów

	[20000]	[27001]
Co	Zdarzenie	Pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń
Cecha, sposób wykrycia	które nie należy do standardowej operacji **usługi**	związanych z **bezpieczeństwem** informacji,
Skutek	które powoduje lub może powodować **przerwę w dostarczaniu** tej usługi lub **redukcję jej jakości**	które stwarzają znaczne prawdopodobieństwo **zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji**

Rodzaje incydentów - przykłady

Tylko [20000] Incydent SLA	[20000] i [27001] Incydent SLA i IB	Tylko [27001] IB
Spadek wydajności spowodowany większą ilością użytkowników niż przewidziano	Awaria sprzętu (dostępność)	
Zablokowanie systemu spowodowane brakiem umiejętności użytkowników	Błąd /awaria/ oprogramowania Atak malware (integralność, dostępność)	
	Włamanie i usunięcie danych (integralność, dostępność)	Ujawnienie informacji, wykorzystanie w celach prywatnych (Naruszenie poufności)

Zarządzanie incydentami w [17799]

- Rozdział 13 [17799]
  - Zgłaszanie zdarzeń
    - Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji
    - Zgłaszanie słabości systemu bezpieczeństwa
  - Zarządzanie incydentami związanymi z bezpieczeństwem informacji
    - Odpowiedzialność i procedury
    - Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji
    - Gromadzenie materiału dowodowego

Zarządzanie incydentami w [17799]

- Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji
  - Niezwłoczne zgłaszanie zdarzeń związanych z bezpieczeństwem informacji poprzez odpowiednie kanały
  - Odpowiednie procedury
    - Poprawne zachowanie użytkownika
      - Opisanie szczegółów
      - Zakaz samodzielnej reakcji bez zgłoszenia (?)
    - Formularze zgłoszenia
    - Zwrotne informowanie
    - Proces dyscyplinarny
  - Zawsze dostępny punkt zgłoszenia
  - Również personel stron trzecich

Zarządzanie incydentami w [17799]

- Zgłaszanie słabości systemu bezpieczeństwa
  - Zgłaszanie zaobserwowanych lub podejrzewanych słabości bezpieczeństwa w systemach lub usługach przez wszystkich pracowników i reprezentantów stron trzecich.
  - Odbiorca zgłoszenia
    - Kierownictwo (?)
    - Dostawca usług
  - Zakaz testowania podatności na własną rękę

Zarządzanie incydentami w [17799]

- Odpowiedzialność i procedury w zakresie zarządzania IB
  - Szybka, skuteczna i uporządkowana reakcja
    - odpowiedzialność kierownictwa
    - procedury
  - Wykorzystanie systemów monitorowania
  - Różne procedury reagowania na różne IB
    - awarie systemów informacyjnych i utrata usługi
    - wystąpienie złośliwego kodu
    - odmowa usługi
    - błąd danych (?)
    - naruszenie poufności i integralności
    - niewłaściwe użycie systemów informacyjnych

Zarządzanie incydentami w [17799]

- Odpowiedzialność i procedury w zakresie zarządzania IB cd.
  - Analiza i identyfikacja przyczyny IB
  - Ograniczanie zasięgu
  - Działania naprawcze
  - Raportowanie
  - Gromadzenie i zabezpieczanie śladów audytowych lub podobnych dowodów
  - Nadzór nad działaniami odtwarzającymi

Zarządzanie incydentami w [17799]

- Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji
  - Mechanizmy umożliwiające liczenie i monitorowanie rodzajów, rozmiarów i kosztów incydentów związanych z bezpieczeństwem informacji.

Zarządzanie incydentami w [17799]

- Gromadzenie materiału dowodowego
  - Zgromadzenie, zachowanie i przedstawienie materiału dowodowego zgodnie z zasadami materiału dowodowego obowiązującymi w odpowiednim prawodawstwie
  - Procedury zbierania i przedstawiania materiału dowodowego na potrzeby postępowania
  - Dopuszczalność materiału dowodowego
    - Zgodność systemów informacyjnych z opublikowanymi normami lub praktycznymi zasadami tworzenia takiego materiału dowodowego
  - Zabezpieczania materiału dowodowego
    - Utrzymanie jakości i kompletności

Zarządzanie incydentami w [17799]

- Gromadzenie materiału dowodowego
  - „dla dokumentów papierowych: oryginał jest bezpiecznie przechowywany wraz z informacją, kto znalazł dokument, gdzie, kiedy i kto był świadkiem tego zdarzenia; każde śledztwo może wykazać, że oryginał nie został naruszony”
  - „dla dokumentów na nośnikach komputerowych: zaleca się utworzenie obrazu lub kopii (zależnie od stosownych wymagań) wszelkich nośników wymiennych; zaleca się zapisanie informacji znajdujących się na dyskach twardych lub w pamięci komputera, aby zapewnić ich dostępność; zaleca się zachowanie zapisów wszelkich działań podczas procesu kopiowania oraz aby proces ten odbywał się w obecności świadków; zaleca się przechowywanie oryginalnego nośnika i dziennika zdarzeń w sposób bezpieczny i nienaruszony (jeśli to niemożliwe, to co najmniej jeden obraz lustrzany lub kopię)”

Zarządzanie incydentami w [17799]

- Gromadzenie materiału dowodowego
  - Przeprowadzanie wszelkich działań śledczych na kopiach materiału dowodowego
  - Ochrona integralności wszystkich materiałów dowodowych
  - Nadzorowanie kopiowania materiałów przez zaufany personel
  - Zapisanie informacji
    - czas i miejsce kopiowania
    - podmiot wykonujący
    - narzędzia lub programy

Przykład procesu zarządzania IB

- Przykładowy proces zarządzania IB (PZIB)
  - Procedura zgłaszania IB
  - Procedura zgłaszania podatności
  - Procedura monitorowania usuwania skutków awarii, ataków malware i zdarzeń losowych
  - Procedury realizowane przez Pion IT (ich procesy)
    - Procedury reagowania na awarie
    - Itd. itp……
  - Procedura reagowania na naruszenie bezpieczeństwa
  - Procedura gromadzenia materiału dowodowego
- Właściciel procesu
  - Pion bezpieczeństwa organizacji

Powiązania z innymi procesami

- Proces HelpDesk –> PZBI
  - Zgłaszanie naruszeń bezpieczeństwa
  - Informowanie o incydentach, SLA które są IB
- Procesy utrzymania IT
  - Naprawianie awarii itp.
- Proces monitorowania -> PZIB
  - Bezpośrednie alarmy z systemów monitorowania
  - Bezpośrednie incydenty z systemów zarządzania zdarzeniami
  - Itd. itp..

Powiązania z innymi procesami

- PZIB -> Proces zarządzania ryzykiem
  - Uwzględnianie wniosków z IB w zarządzaniu ryzykiem
- PZIB -> Proces zarządzania konfiguracją
  - Natychmiastowa zmiana niebezpiecznej konfiguracji
- PZIB -> Proces zarządzania zmianami
  - Wniosek o zmianę
- PZIB -> Proces zarządzania ciągłością działania
  - Uruchamianie planu BCP

Zarządzanie incydentami w [18044]

- 4 procesy
  - Planowania i przygotowania
  - Stosowania
  - Przeglądu
  - Doskonalenia
  - => Model PCDA znany m.in. z [27001]

Zarządzanie incydentami w [18044]

- Planowania i przygotowania
  - Polityka zarządzania incydentami
  - Struktura zarządzania incydentami
    - ISIRT – Information Security Incident Response Team
    - Wsparcie z zewnątrz – np. CERT
  - Dostosowanie PZI do
    - Polityki Bezpieczeństwa Informacji
    - Polityką Zarządzania Ryzykiem
  - Opracowanie procedur
  - Szkolenie, uświadamianie
  - Testy

Zarządzanie incydentami w [18044]

- Stosowanie
  - Wykrywanie i raportowanie
    - Źródło – użytkownik lub system monitorujący
  - Zbieranie dodatkowych informacji w celu oceny
  - Reakcja
    - Tryb - natychmiastowa lub nie
    - Działania późniejsze – incydent „pod kontrolą”
    - Wdrożenie planów kryzysowych i planów BCP/DRP - incydent „poza kontrolą”
    - Komunikacja wewnętrzna oraz z organami ścigania i innymi zainteresowanymi podmiotami
    - Gromadzenie i analiza materiału dowodowego
    - Dokumentowanie działań i decyzji
    - Zamkniecie incydentu

Zarządzanie incydentami w [18044]

- Przegląd
  - Dalsza analiza materiałów dowodowych
  - Wnioski
  - Propozycje zmian w istniejących systemach (mechanizmach) zabezpieczeń
    - Warstwa techniczna
    - Warstwa organizacyjno-proceduralna
  - Propozycje zmian w zarządzaniu IB
    - Funkcjonowanie ISIRT
    - Zawartość procedur

Zarządzanie incydentami w [18044]

- Doskonalenie
  - Zmiany w zarządzaniu ryzykiem
  - Zmiany w organizacji bezpieczeństwa i samej PBI
  - Propozycje wdrożenia nowych systemów zabezpieczeń

Incydenty w przepisach

- [UOIN] - „naruszenie ochrony”
  - Art. 18, ust 9.
    - „Pełnomocnik ochrony podejmuje działania zmierzające do wyjaśnienia okoliczności naruszenia przepisów o ochronie informacji niejawnych, zawiadamiając o tym kierownika jednostki organizacyjnej, a w przypadku naruszenia przepisów o ochronie informacji niejawnych, oznaczonych klauzulą „poufne” lub wyższą, również właściwą służbę ochrony państwa”.
  - Art. 71, ust. 5, p. d)
    - Obowiązek informowania SOP przez jednostkę zlecającą przetwarzanie IN, o naruszeniach ochrony informacji niejawnych u zleceniobiorcy

Incydenty w przepisach

- [R1433]
  - Par. 4 Obowiązki Kierownika JO
    - p. 4 – analiza staniu bezpieczeństwa oraz zapewnienie usunięcia stwierdzonych nieprawidłowości
      - reagowanie na incydenty?
    - p. 6 – zawiadomienie SOP o incydencie bezpieczeństwa teleinformatycznego (klauzula „poufne” i wyższe))

Incydenty w przepisach

- Zalecenia [Zal_BTI]
  - System informowania o incydentach
    - obowiązek informowania IBTI o IB
  - Kontrole i audyty
    - prowadzone przez IBTI i administratorów w celu wykrycia IB
  - Wyjaśnianie okoliczności IB przez IBTI
  - Prawo żądania wsparcia od personelu IT
  - Pełnomocnik
    - działania i wnioski do kierownika JO w zakresie dodatkowych zabezpieczeń

Incydenty w przepisach

- Zalecenia [Zal_AZR]
  - Procedury zgłaszania i badania przyczyn IB
  - Świadome i efektywne reagowanie oraz wyciąganie wniosków
- [UODO] i [R1024]
  - ABI powinien nadzorować przestrzeganie zasad ochrony (art. 36 ust 3)
  - Brak przepisów dot. monitorowania bezpieczeństwa i reagowania na incydenty
- Dlaczego większość przepisów nie wykorzystuje polskich norm?

Przepisy o informatyzacji

- Ustawa o informatyzacji [UIDP] z 2005 r.
  - Możliwość kontroli [...] działania systemów TI, używanych do realizacji zadań publicznych
  - Rozporządzenie dot. minimalnych wymagań bezpieczeństwa [R1766]
    - § 2. Systemy teleinformatyczne używane przez podmioty publiczne do realizacji zadań publicznych 1) powinny spełniać właściwości i cechy w zakresie funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, określone w normach ISO zatwierdzonych przez krajową jednostkę normalizacyjną, na etapie projektowania, wdrażania i modyfikowania tych systemów;
    - => [17799], [20000]

Przepisy o informatyzacji

- Cd. [R1766]
  - § 3. 1. Podmiot publiczny opracowuje, modyfikuje w zależności od potrzeb oraz wdraża politykę bezpieczeństwa dla systemów TI używanych przez ten podmiot do realizacji zadań publicznych.
  - 2. Przy opracowywaniu polityki bezpieczeństwa, o której mowa w ust. 1, podmiot publiczny powinien uwzględniać postanowienia Polskich Norm z zakresu bezpieczeństwa informacji.

Poziomy zarządzania IB

- Poziom podstawowy
  - Wykorzystanie [17799] w zarządzaniu incydentami
    - Opracowanie kilku podstawowych procedur
- Poziom procesowy
  - Zbudowanie procesów w oparciu o [27001] i [17799] oraz częściowo [20000]
  - Budowa i certyfikacja SZBI na zgodność z [27001]
- Poziom dojrzały
  - Doskonalenie Procesu Zarządzania IB w oparciu o [18044]

- Dziękuję za uwagę
- Kontakt
  - cendrowskij@poczta.onet.pl