Warszawska Wyższa Szkoła Informatyki

Prezentacja do obrony pracy dyplomowej:

„Wzorcowa polityka bezpieczeństwa informacji dla organizacji zajmującej się testowaniem oprogramowania.”

Promotor: dr inż. Krzysztof Różanowski

Błażej Zawadzki

Album: 5325

21 czerwca 2012 roku

Cel i zakres pracy dyplomowej

- Przegląd aktów prawnych i norm dotyczących Bezpieczeństwa Informacji
- Prezentacja wymogów formalnych dla dokumentacji PBI
- Opracowanie sposobu inwentaryzacji i klasyfikacji zasobów
- Zaproponowanie wzorcowej Polityki Bezpieczeństwa Informacji dla działalności dotyczącej testowania oprogramowania:
  - szablonu dla dokumentów
  - propozycji rozporządzeń i decyzji ustanawiających PBI w organizacji
  - opracowanie kompletu niezbędnych procedur, regulaminów i instrukcji
- Przedstawienie definicji obowiązków wynikających z PBI

Polityka Bezpieczeństwa Informacji

- ***Polityka bezpieczeństwa informacji*** **- to zbiór spójnych, precyzyjnych reguł i procedur, według których organizacja buduje, zarządza oraz udostępnia swoje zasoby i systemy informacyjne i informatyczne. Polityka określa, które zasoby i w jaki sposób powinny być chronione.**

- Polityka powinna wskazywać możliwe rodzaje naruszenia bezpieczeństwa (jak np. utrata danych, nieautoryzowany dostęp itp.), scenariusze postepowania w takich sytuacjach oraz czynności, które pozwolą uniknąć ponownego wystąpienia takiego incydentu. Polityka bezpieczeństwa powinna dodatkowo definiować poprawne i niepoprawne metody korzystania z zasobów.

- Polityka bezpieczeństwa musi być dokumentem spisanym i znanym oraz zrozumianym przez wszystkich użytkowników zasobów informatycznych przedsiębiorstwa, w tym również klientów czy dostawców.

Polityka Bezpieczeństwa Informacji

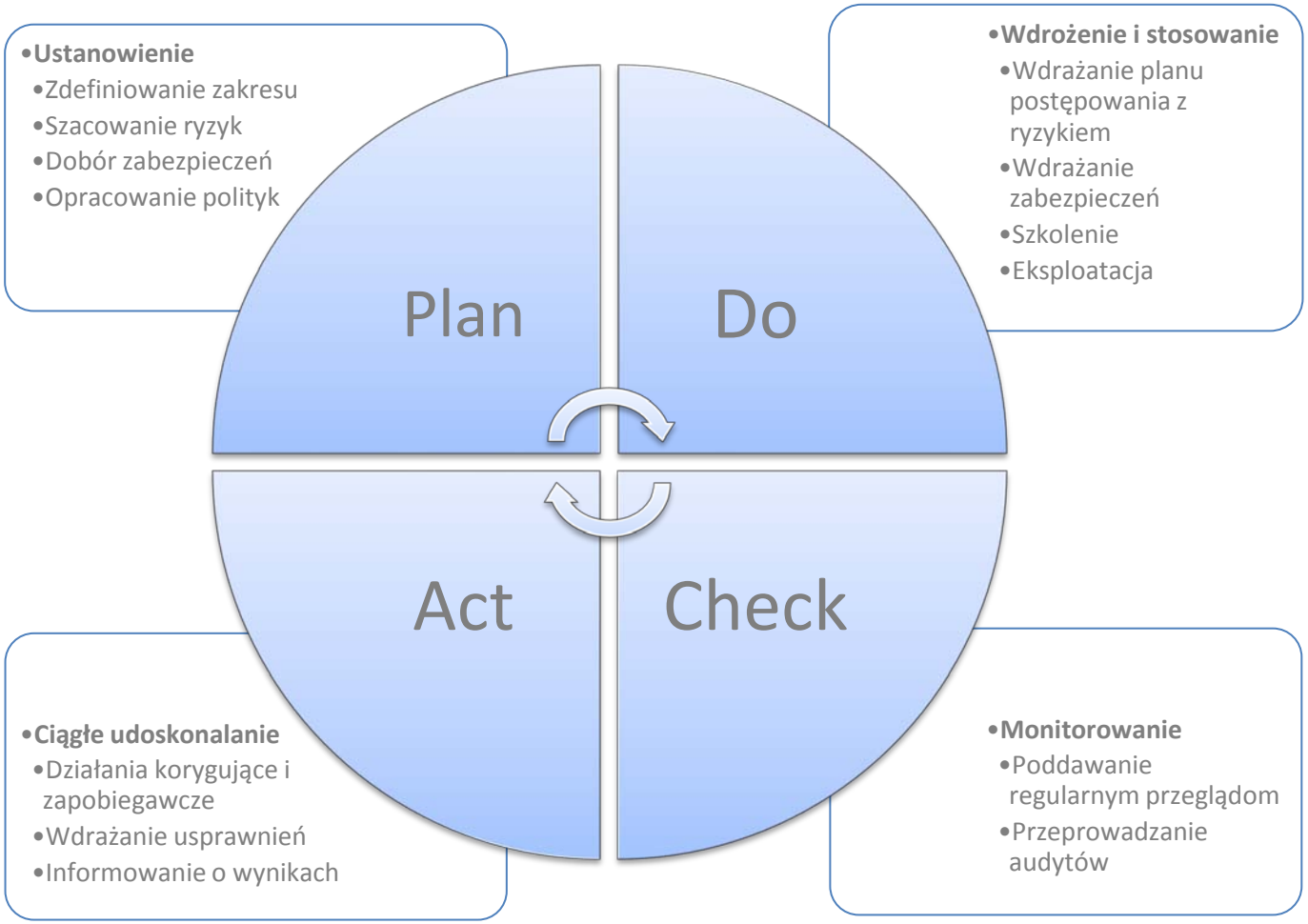
- Punktem wyjścia do spisania PBI jest dokładna analiza specyfiki działalności organizacji i jej otoczenia biznesowego

- Polityka powinna poruszać następujące zagadnienia:
  - co podlega ochronie?
    - informacja
    - systemy teleinformatyczne
    - itd.
  - identyfikacja zagrożeń
  - w jaki sposób chronimy krytyczne zasoby przedsiębiorstwa?
  - precyzyjne zdefiniowanie odpowiedzialności i obowiązków

Bezpieczeństwo informacji jako proces

- Zarządzanie bezpieczeństwem Informacji musi być procesem ciągłym
  - ustanowienie PBI i opracowanie systemu zabezpieczeń
  - wdrożenie zabezpieczeń i bieżące eksploatowanie
  - monitorowanie skuteczności przyjętych rozwiązań
  - utrzymywanie i doskonalenie

PDCA – cykl Deminga

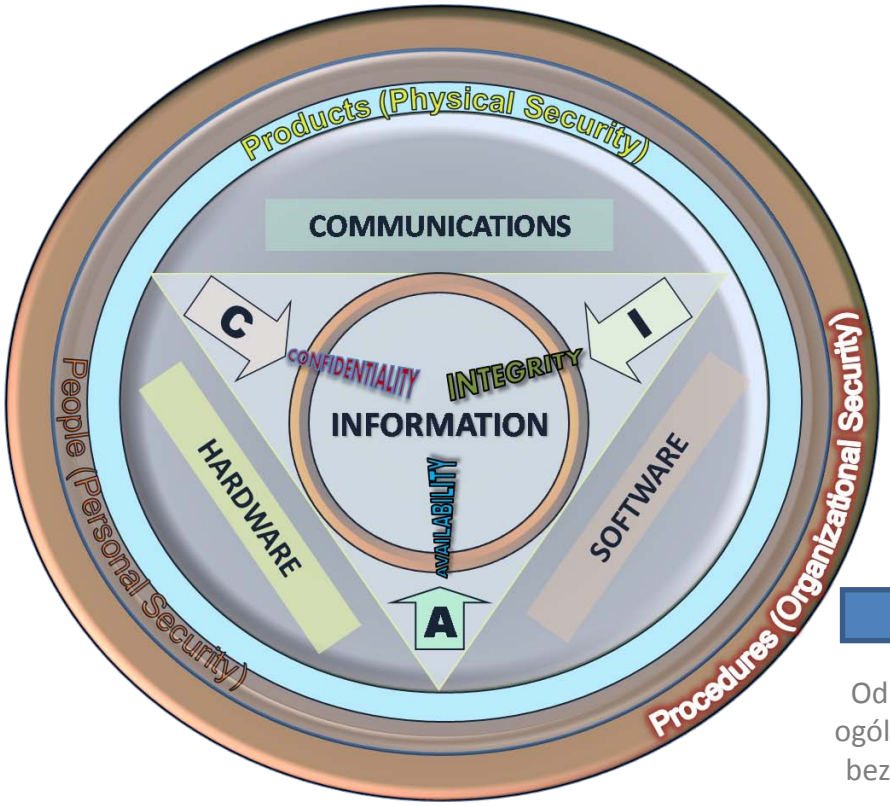


Cel PBI

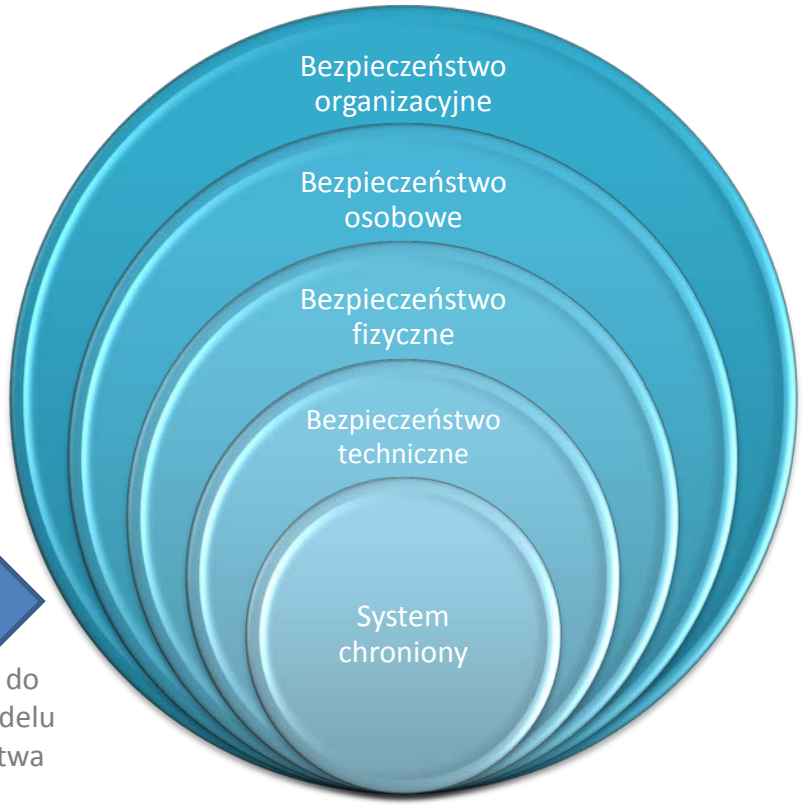
- Zbudowanie i opisanie jednorodnego systemu zabezpieczeń i rozwiązań mających zapewnić stan bezpieczeństwa teleinformatycznego (i szerzej bezpieczeństwa informacji)
- Atrybuty bezpieczeństwa informacji:
  - poufność
  - integralność
  - dostępność

  Dodatkowe atrybuty
  - autentyczność
  - rozliczalność
  - niezaprzeczalność
  - niezawodność

Poufność, Integralność i Dostępność (CIA – Confidentiality-Integrity-Availability)



Odniesienie do ogólnego modelu bezpieczeństwa



Źródło: http://en.wikipedia.org/wiki/CIA_triad#Key_concepts

Schemat PBI zaprezentowanej w pracy
– prezentacja warstwowa

- Dwa uzupełniające się dokumenty na najwyższym poziomie
  - Polityka Bezpieczeństwa Informacji – podstawy prawne oraz ogólne zasady i strategie bezpieczeństwa informacji
  - Politykę Bezpieczeństwa Systemu Informatycznego – ogólne procedury korzystania z zasobów informatycznych, tryby i zasady uzyskiwania dostępu do zasobów, procedury dotyczące wykonywania kopii zapasowych itd.
- Polityki dla poszczególnych grup informacji – konkretne rozwiązania i zabezpieczenia
- Regulaminy, procedury, instrukcje – szczegółowe opisy postepowania w konkretnych przypadkach

Polityka Bezpieczeństwa Informacji – plan dokumentu

- Definicja PBI
- Organizacja bezpieczeństwa informacji
- Zarządzanie aktywami
- Bezpieczeństwo osobowe
- Bezpieczeństwo fizyczne i środowiskowe
- Zarządzanie systemami i sieciami
- Kontrola dostępu do zasobów przedsiębiorstwa
- Rozwój i utrzymanie systemów
- Zarządzanie ciągłością działania
- Zarządzanie ryzykiem
- Zarządzanie incydentami bezpieczeństwa
- Powiązania i zgodność z aktami prawnymi i innymi dokumentami

Polityka Bezpieczeństwa Systemu Informatycznego
– plan dokumentu

- Definicja PBSI
- Fizyczny i logiczny dostęp do pomieszczeń przedsiębiorstwa, do systemów elektronicznych i do danych elektronicznych
- Szyfrowanie danych
- Sieć informatyczna przedsiębiorstwa
- Zabezpieczenia urządzeń, systemów i danych
- Przesył danych
- Kopie zapasowe i odtwarzanie danych
- Incydenty związane z naruszeniem bezpieczeństwa

Wykaz polityk i regulaminów opracowanych w ramach pracy dyplomowej

- Polityka Bezpieczeństwa Informacji – dokument główny
- Polityka Bezpieczeństwa Systemu Informatycznego
- Zasady Klasyfikacji Danych
- Regulamin Zdalnego Dostępu do Zasobów Informatycznych
- Regulamin Korzystania z Poczty Elektronicznej i Firmowego Komunikatora
- Procedura Zarządzania Ryzykiem

Pozostałe dokumenty opracowane w ramach pracy dyplomowej

- Szablon rozporządzenia ustanawiającego PBI w organizacji
- Wykaz definicji istotnych z dla PBI
- Wykaz aktów prawnych
- Wzór ewidencji aktywów sprzętowych
- Wzór dokumentacji sieci informatycznej przedsiębiorstwa
- Wykaz zatwierdzonych do użycia systemów operacyjnych
- Wzór formularzu incydentu bezpieczeństwa
- Szablon pliku do tworzenia dalszej dokumentacji PBI

Akty prawne, które muszą być uwzględnione przy tworzeniu PBI

- Dyrektywa Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie ramowych warunków Wspólnoty dla podpisu elektronicznego (99/93/WE)
- Rozporządzenie Ministra Finansów z dnia 31 października 2003 r. w sprawie szczegółowych zasad tworzenia, utrwalania, przechowywania i zabezpieczania dokumentów związanych z zawieraniem i wykonywaniem umów ubezpieczenia (Dz.U.2003.193.1889)
- 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.2004.100.1024)
- Rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczania danych informatycznych (Dz.U.2004.100.1023)
- Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U.05.171.1433)
- Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz.U.2002.128.1094)
- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U.2002.144.1204 z późniejszymi zmianami)
- Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U.2001.130.1450 z późniejszymi zmianami)
- Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (tekst jednolity Dz.U.05.196.1631)
- Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz.U.2001.128.1402 z późniejszymi zmianami
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.2002.101.926 z późniejszymi zmianami)
- Ustawa z dnia 16 lipca 2004 Prawo Telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późniejszymi zmianami)

Normy polskie i międzynarodowe

- ISO 18028 – Zarządzanie komunikacją
- ISO 18044 – Zarządzanie incydentami
- ISO/IEC 27002 (wcześniej ISO/IEC 17799 i BS 7799-1) Wytyczne związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem Systemy Zarządzania Bezpieczeństwem Informacji (SZBI – ISMS ang. Information Security Management System)
- ISO/IEC Guide 73 – Słownictwo dotyczące zarządzania ryzykiem
- ISO/IEC TR-13335-3:1998 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych
- ISO19011 – Wytyczne do auditów jakości i systemów środowiska
- PN-EN ISO 14001:2005 Systemy zarządzania środowiskowego. Wymagania i wytyczne stosowania
- PN-EN ISO 9001:2001 System zarządzania jakością. Wymagania
- PN-I-13335-1:1999 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych
- PN-ISO/IEC 15408-1:2002 Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych
- PN-ISO/IEC 17799:2007 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji
- PN-ISO/IEC 27001:2007 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania