

Część I. Podstawy zabezpieczenia informacji

1 Czym jest zabezpieczenie informacji?

Definicja zabezpieczenia informacji

Krótką historią zabezpieczeń

Zabezpieczenia fizyczne

Zabezpieczenia komunikacyjne

Zabezpieczenia emisji

Zabezpieczenia komputerowe

Zabezpieczenia sieci

Zabezpieczenia informacji

Dlaczego bezpieczeństwo polega na procesie, a nie na pojedynczych produktach

Programy antywirusowe

Kontrola dostępu

Firewalle (zapory ogniowe)

Elektroniczne identyfikatory

Dane biometryczne

Wykrycie włamania

Zarządzanie strategią

Tropienie słabych punktów

Szyfrowanie

Mechanizmy zabezpieczeń fizycznych

2 Typy ataków

Ataki dostępu

Węszenie

Podśluchiwanie

Przechwycenie

Jak przeprowadzane są ataki dostępu

Ataki modyfikujące

Zmiany

Dodawanie

Kasowanie

Jak przeprowadzane są ataki modyfikujące

Ataki pozbawienia usługi

Pozbawienie dostępu do informacji

Pozbawienie dostępu do aplikacji

Pozbawienie dostępu do systemów

Pozbawienie dostępu do komunikacji

Przeprowadzane są ataki pozbawienia usługi

Ataki zaprzeczenia

Maskarada

Zatajenie zdarzenia

Jak przeprowadzane są ataki zaprzeczenia

3 Usługi zabezpieczenia informacji

Utajnienie (Confidentiality)

Utajnienie zbiorów danych

Utajnienie informacji przepływającej

Utajnienie przepływu danych

Ataki, którym można zapobiec

Integralność (Integrity)

Integralność zbiorów danych

Integralność przepływu informacji

Ataki, którym można zapobiec

Dostępność (Availability)

Kopie zapasowe (Backup)

Przejęcie czynności przez urządzenie zastępcze

Odzyskiwanie systemu po awarii

Ataki, którym można zapobiec

Ustalanie odpowiedzialności

Identyfikacja i uwierzytelnianie

Inspekcja.

Ataki, którym można zapobiec

Część II. Przygotowanie terenu

4 Kwestie prawne dotyczące bezpieczeństwa informacji

Prawo karne w USA

- Oszustwo i nadużycie komputerowe (18 US Code 1030)
- Oszustwo za pomocą karty kredytowej (18 US Code 1029)
- Prawa autorskie (18 US Code 2319)
- Przechwycenie (18 US Code 2511)
- Dostęp do informacji elektronicznej (18 US Code 2701)
- Pornografia dziecięca
- Inne statuty kryminalne

Prawa stanowe

- Przykłady praw w innych krajach
 - Australia
 - Holandia
 - Zjednoczone Królestwo

Oskarżenie

- Gromadzenie dowodów
- Kontaktowanie się z organami ścigania

Kwestie cywilne

- Kwestie pracownicze
- Monitoring wewnętrzny
- Kwestie strategii
- Przenoszenie odpowiedzialności

Kwestie prywatności

- Informacje o klientach
- Informacje zdrowotne

5 Strategia firmy

Strategia jest ważna

- Określanie metod bezpieczeństwa
- Uwzględnianie wszystkich

Typy strategii

- Strategia informacyjna
- Strategia bezpieczeństwa
- Strategia korzystania z komputerów
- Strategia korzystania z Internetu
- Strategia korzystania z poczty
- Procedury administracji użytkownikami
- Procedura administracji systemu
- Procedura reakcji na incydent
- Procedura zarządzania konfiguracją
- Metodologia projektu
- Plany odzyskiwania systemów po awarii

Tworzenie odpowiedniej strategii

- Ustalenie co jest ważne
- Ustalenie tolerowanego zachowania
- Uwzględnianie udziałowców
- Ustalenie odpowiedniego zarysu
- Rozwój strategii

Wdrażanie strategii

- Uzyskanie poparcia
- Szkolenie
- Implementacja

Efektywne wykorzystanie strategii

- Nowe systemy i projekty
- Istniejące systemy i projekty
- Inspekcja
- Rewizja strategii

6 Zarządzanie ryzykiem

Czym jest ryzyko?

Słaby punkt

Zagrożenie

Zagrożenie + Słabe punkty = Ryzyko

Ustalanie ryzyka dla firmy

Ustalanie słabych punktów

Ustalanie realnych zagrożeń

Ustalanie środków zaradczych

Ustalanie ryzyka

Mierzenie ryzyka

Pieniądze

Czas

Środki

Reputacja

Stracone transakcje

Metodologia mierzenia ryzyka

7 Proces zabezpieczenia informacji

Oszacowanie

Sieć

Fizyczna ochrona

Strategie i procedury

Środki ostrożności

Uświadomienie

Ludzie

Ilość pracy

Nastawienie

Ustosunkowanie

Działalność

Wyniki oszacowania

Strategia

Wybieranie kolejności strategii

Uaktualnianie istniejących strategii

Wdrożenie

Systemy meldowania o bezpieczeństwie

Systemy uwierzytelniania

Bezpieczeństwo w Internecie

Systemy wykrycia włamania

Szyfrowanie

Fizyczna ochrona

Szkolenia uświadamiające

Inspekcja

Sprawdzanie ustosunkowania do strategii

Okresowa ocena oraz ocena nowych projektów

Testy włamania

8 Najlepsze praktyki zabezpieczania informacji

Zabezpieczenia w administracji

Strategie i procedury

Środki

Personel

Odpowiedzialność

Szkolenie

Plany awaryjne

Plany projektu bezpieczeństwa

Zabezpieczenia techniczne

Połączenia sieciowe

Ochrona antywirusowa

Uwierzytelnianie

Inspekcja

Szyfrowanie

Kopie zapasowe i odzyskiwanie

Ochrona fizyczna

Część III. Rozwiązania praktyczne

9 Architektura Internetu

Oferowane usługi

- Poczta
- Sieć
- Wewnętrzny dostęp do Internetu
- Dostęp z zewnątrz do systemów wewnętrznych
- Usługi kontroli

Usługi nieudzielane

Architektura komunikacji

- Dostęp przez jedno łącze
- Dostęp przez wielokrotne łącze do Jednego dostawcy
- Dostęp przez wielokrotne łącze do wielu dostawców

Strefa zdemilitaryzowana

- Ustalanie DMZu
- Jakie systemy umieścić w DMZ
- Odpowiednia architektura DMZ

Firewalle

- Typy firewalli
- Konfiguracje firewalli
- Ustalanie zestawu reguł firewalla

Przekład adresów sieciowych

- Czym jest przekład adresów sieciowych?
- Prywatna klasa adresów
- Statyczny NAT
- Dynamiczny NAT

Sieci partnerskie

- Zastosowanie sieci partnerskich
- Instalacja
- Kwestie adresowania

10 Wirtualne sieci prywatne

Wyznaczanie wirtualnej sieci prywatnej

VPN użytkownika

- Zalety VPNu użytkownika
- Problemy związane z VPNem użytkownika
- Zarządzanie VPNami użytkowników

VPN lokalizacji

- Zalety VPNu lokalizacji
- Problemy związane z VPNem lokalizacji
- Zarządzanie VPNami lokalizacji

Standardowe techniki VPN

- Serwer VPN
- Algorytmy szyfrowania
- System uwierzytelniania

11 Wymogi bezpieczeństwa w handlu elektronicznym

Usługi w handlu elektronicznym

- Różnice pomiędzy usługami handlu elektronicznego i zwykłymi usługami w DMZ
- Przykłady usług handlu elektronicznego

Dostępność

- Układ firma-konsument
- Układ firma-firma
- Czas globalny
- Wygoda klienta
- Koszt przerw w działaniu
- Rozwiązanie problemu dostępności

Bezpieczeństwo od strony klienta

- Bezpieczeństwo komunikacji
- Zapisywanie informacji w systemie klienta
- Zaprzeczenie

- Bezpieczeństwo od strony serwera
 - Informacje przechowywane w serwerze
 - Ochrona serwera przed atakiem
- Bezpieczeństwo aplikacji
 - Odpowiedni projekt aplikacji
 - Właściwe techniki programowania
 - Pokazać program światu
 - Zarządzać konfiguracją
- Bezpieczeństwo serwera baz danych
 - Lokalizacja baz danych
 - Komunikacja z serwerem handlu elektronicznego
 - Ochrona dostępu wewnętrznego
- Architektura handlu elektronicznego
 - Lokalizacja serwera i możliwości połączenia
 - Dostępność
 - Przegląd na okoliczność słabych punktów
 - Dane inspekcji i wykrywanie problemów

12 Szyfrowanie

- Koncepcje szyfrowania
 - Terminologia szyfrowania
 - Ataki na szyfrowanie
- Szyfrowanie z kluczem prywatnym
 - Czym jest szyfrowanie z kluczem prywatnym?
 - Szyfry zastępujące
 - Jednorazowe bloczki
 - Standard szyfrowania danych
 - Potrójny DES
 - Szyfrowanie hasła
 - Zaawansowany standard szyfrowania: Rijndael
 - Inne algorytmy z kluczem prywatnym
- Szyfrowanie z kluczem publicznym
 - Czym jest szyfrowanie z kluczem publicznym?
 - Wymiana klucza Diffiego-Hellmana
 - RSA
 - Inne algorytmy z kluczem publicznym
- Podpisy elektroniczne
 - Czym jest podpis elektroniczny?
 - Bezpieczne funkcje haszujące
- Zarządzanie kluczem
 - Tworzenie klucza
 - Rozpowszechnianie klucza
 - Certyfikacje kluczy
 - Ochrona kluczy
 - Unieważnianie klucza
- Zaufanie
 - Hierarchia
 - Sieć

13 Techniki hackerskie

- Motywacje hackera
 - Wyzwanie
 - Chciwość
 - Złośliwy zamiar
- Dawne techniki hackerskie
 - Otwarte współdzielenie
 - Złe hasła
 - Niemądre programowanie
 - Inżynieria społeczna
 - Przeciążenie bufora
 - Pozbawienie usługi

- Metody hackera o nieustalonym celu
 - Cele
 - Rekonesans
 - Metody ataku
 - Wykorzystanie naruszonych systemów
- Metody hackera o określonym celu
 - Cele
 - Rekonesans
 - Metody ataku
 - Wykorzystanie naruszonych systemów

14 Wykrycie włamania

- Rodzaje systemów wykrycia włamania
 - IDS systemowy
 - IDS sieciowy
 - Czy któryś rodzaj IDS jest lepszy?
- Zakładanie IDS
 - Określanie celu IDS
 - Zdecydowanie, co będzie monitorowane
 - Zdecydowanie, jak zareagować
 - Ustalanie progów
 - Wdrożenie systemu
- Zarządzanie IDS.
 - Co może powiedzieć IDS?.
 - Co mówi IDS?
 - Badanie podejrzanych zdarzeń

Cześć IV Przegląd Implementacji na różnych platformach

15 Kwestie bezpieczeństwa w systemie UNIX

- Ustawianie systemu
 - Pliki uruchamiania
 - Usługi dopuszczalne
 - Pliki konfiguracji systemu
 - Patche
- Zarządzanie użytkownikami
 - Dodawanie użytkowników do systemu
 - Usuwanie użytkowników z systemu
- Zarządzanie systemem
 - Inspekcja systemu
 - Pliki dzienników
 - Ukryte pliki
 - Pliki SUID i SGLD
 - Pliki do zapisywania przez wszystkich
 - Szukanie podejrzanych znaków

16 Kwestie bezpieczeństwa w systemie Windows NT

- Konfiguracja systemu
 - Ustawienia rejestru
 - Ustawienia konfiguracji systemu
- Zarządzanie użytkownikami
 - Dodawanie użytkowników do systemu
 - Ustawianie uprawnień plików
 - Usuwanie użytkowników z systemu
- Zarządzanie systemem
 - Inspekcja systemu
 - Dzienniki
 - Wypatrywanie podejrzanych oznak

17 Kwestie bezpieczeństwa w systemie Windows 2000

- Konfiguracja systemu .
 - Ustawienia zasad zabezpieczeń lokalnych
 - Konfiguracja systemu

- Zarządzanie użytkownikami
 - Dodawanie użytkowników do systemu
 - Ustawianie uprawnień plików
 - Usuwanie użytkowników z systemu
- Zarządzanie systemem
 - Polecenie Secedit
 - Inspekcja systemu
 - Dzienniki
 - Wypatrywanie podejrzanych oznak

Załączniki

A Plan projektu procesu

- Faza oszacowania
- Faza krytycznych poprawek
- Faza uaktualnienia
- Faza ciągłości pracy

B UNIX czy Windows: co jest bezpieczniejsze?

- Czasy się zmieniają
- Wirusy, konie trojańskie i robaki, o rany!
- Słabe punkty systemów operacyjnych a słabe punkty aplikacji
- Interaktywny czy nie interaktywny
- Z kodem źródłowym czy bez
- Umiejętności
- Wnioski

C Źródła dalszej wiedzy na temat bezpieczeństwa

D Scenariusze testujące procedurę reakcji na incydent

- Scenariusz 1 — Atak na stronę WWW
- Scenariusz 2 — Niewytłumaczalnie duży ruch w sieci
- Scenariusz 3 — Pliki zmodyfikowane przez nieznaną osobę
- Scenariusz 4 — Znalezienie nieautoryzowanej usługi w systemie
- Scenariusz 5 — Brakuje pliku dziennika w systemie
- Scenariusz 6 — Sieć jest zbyt wolna
- Scenariusz 7 — Atak na wewnętrzny router
- Scenariusz 8 — Atak wirusowy
- Scenariusz 9 — System wykrycia włamania melduje o ataku
- Scenariusz 10 — Wymuszenie