Bezpieczeństwo sieci bezprzewodowych

Specyfika Sieci 802.11

- Tryby pracy:
  - Ad-hoc
  - Infrastrukturalny
- Medium – fale radiowe
  - Agresor w łatwy sposób może uzyskać bezpośredni dostęp do medium transmisyjnego
- Kojarzenie w sieciach z wieloma punktami dostępowymi

Cele ataków

- Włamanie do sieci, dostęp do danych, podsłuchiwanie
- Wykorzystywanie atakowanej sieci (np. 'darmowy' dostęp do Internetu)
- Wykorzystanie sieci w nielegalny sposób (przeprowadzenie ataków sieciowych, spam, rozprzestrzenianie wirusów, włamania do innych systemów, omijanie zapór)

802.11 – Bezpieczeństwo L1

- ograniczenie zasięgu sieci:
  - regulacja mocy sygnału (bardziej zaawansowane AP mają taką możliwość)
- tłumienie sygnału:
  - farby metalizowane pochłaniające fale radiowe
  - reflektory paraboliczne
- odpowiedni dobór anten:
  - anteny dookólne – kąt promieniowania 360°
  - sektorowe – 180°
  - kierunkowe – zwykle kilkanaście do 30°

802.11 – Bezpieczeństwo L2

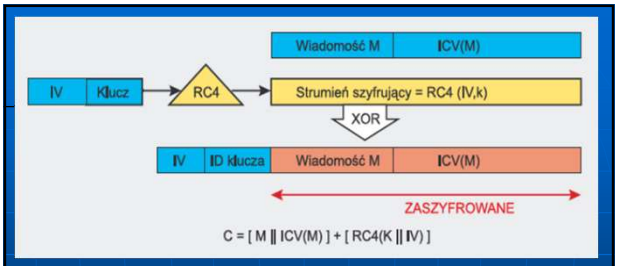
- Wyłączenie opcji rozgłaszania identyfikatora sieci SSID (*Service Set Identity*)
  - AP w ustalonych odstępach czasu wysyła ramki zarządzające *Beacon*, rozgłaszające informacje o sieci, w tym jej identyfikator SSID

802.11 – Bezpieczeństwo L2

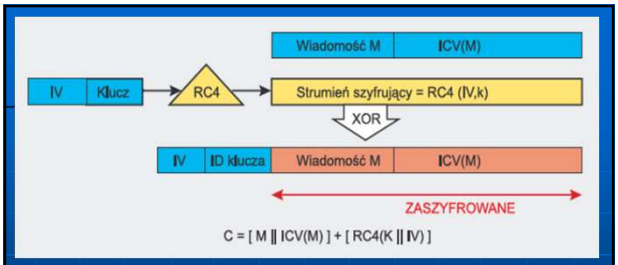
- Filtrowanie adresu MAC
  - AP akceptuje połączenia od adresów MAC zapisanych na liście
  - Wady: trudne logistycznie w dużych sieciach, problemy w sieciach mobilnych
- Szyfrowanie i uwierzytelnianie WEP (*Wired Equivalent Privacy*)
- Szyfrowanie i uwierzytelnianie WPA (*WiFi Protected Access*)

WEP

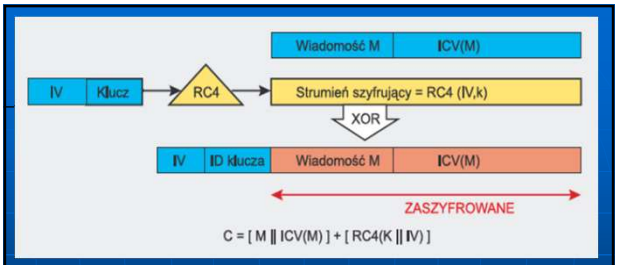
- Wykorzystywany jest algorytm RC4 – symetryczny, strumieniowy.
- Klucz 40 lub 104 bitowy jest wykorzystywany do wygenerowania jednorazowego klucza pseudolosowego o długości równej długości tekstu jawnego.
- Szyfrowanie sprowadza się do wykonania operacji XOR



- Z tajnego klucza (40 bitów) oraz jednorazowego wektora inicjacyjnego (24 bity) tworzony jest 64-bitowy klucz RC4.



- Algorytm RC4 generuje ciąg pseudolosowy
- Do wiadomości dołączana jest suma kontrolna (CRC)



- Szyfrowanie polega na wykonaniu operacji XOR na ciągu pseudolosowym oraz wiadomości
- Wektor inicjacyjny dołączany jest do wysyłanych danych (w postaci jawnej)

Bezpieczeństwo WEP

- W celu zwiększenia poufności możliwe jest rotacyjne używanie kilku (do 4) kluczy WEP
- Użycie klucza 128 (104) bitowego jest opcjonalne
- Jedynie dane oraz suma kontrolna są przesyłane w postaci zaszyfrowanej

Bezpieczeństwo WEP - poufność

- Łatwy atak metodą brutalną
- Atak FSM wykorzystuje słabość algorytmu – istnieją ”słabe” wektory inicjacyjne, powodujące, że z bajtów wynikowych można uzyskać informacje o kluczu. Do uzyskania odpowiedniej liczby słabych wektorów wystarczy przechwycenie około 5 -6 milionów pakietów.

Bezpieczeństwo WEP - integralność

- Niski poziom integralności – CRC pozwala na wykrycie jedynie pojedynczego przekłamania. Dodatkowo CRC nie obejmuje całej ramki, a jedynie obszar danych.
- Brak zabezpieczeń przed powtórzeniami

Standard 802.11i - WPA

- Podstawowe założenia: zwiększenie bezpieczeństwa przy pracy na starym sprzęcie (po wymianie oprogramowania)

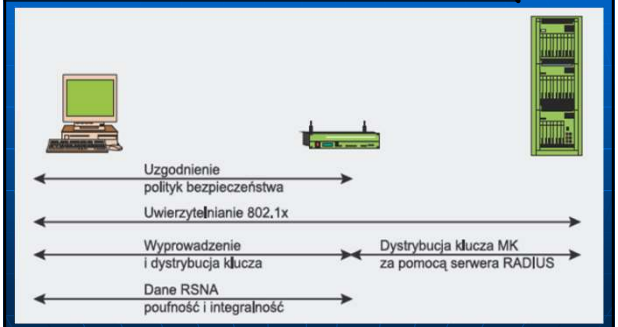
WPA = 802.11 + EAP + TKIP + MIC

- EAP – uwierzytelnianie
- TKIP – poprawa poufności algorytmu RC4
- MIC – mechanizm integralności – obejmuje nagłówek pakietu

Uwierzytelnianie WPA

- Personal – oparte na *pre-shared key* (PSK)
- Enterprise – oparte na RADIUS

Uwierzytelnianie Enterprise



Bezpieczeństwo WPA

- Dwa rodzaje uwierzytelniania:
  - WPA Enterprise – oparte na RADIUS
  - WPA Personal – oparte na ręcznej dystrybucji klucza
- Wyeliminowano słabe wektory IV, jednak nadal istnieją słabe klucze
- Możliwy atak słownikowy
- Możliwy atak na uwierzytelnianie (słabe hasła)

Bezpieczeństwo WPA

- Ataki MITM – podszywanie się pod punkt dostępowy
- Możliwe ataki DoS (zakłócenia, podrobienie nieszyfrowanych ramek do rozłączania i zmiany skojarzeń)

WPA 2

- Szyfrowanie – AES
- Dynamiczne zarządzanie kluczami

Zarządzanie Bezpieczeństwem Informacji

Polityka Bezpieczeństwa

Zarządzanie bezpieczeństwem informacji

- Inicjatywa zapewnienia bezpieczeństwa informacji musi wyjść od kierownictwa
- Odpowiedzialność za bezpieczeństwo teleinformatyczne ponosi kierownictwo
- Jeżeli kierownictwo nie troszczy się o realizację założeń bezpieczeństwa, nie będą one poważnie traktowane przez pracowników

Dokumenty

- **Polityka bezpieczeństwa** – dokument podstawowy, również o znaczeniu marketingowym
- Plan bezpieczeństwa – szczegóły wdrożenia koncepcji bezpieczeństwa (budowy systemu bezpieczeństwa)
  - dokument tajny, dostępny tylko dla osób odpowiedzialnych za bezpieczeństwo
- Instrukcja bezpieczeństwa – zawiera obowiązujące zasady i procedury, znany i rozumiany przez pracowników
- Plan odtwarzania ciągłości działania

Polityka bezpieczeństwa

- Rozporządzenie MSWiA z dnia 29 kwietnia 2004 r. nakłada obowiązek ochrony danych osobowych. Obowiązek ten dotyczy wszystkich instytucji i firm, nawet tych, które przetwarzają tylko dane osobowe tzw. 'pracownicze'.
- Zgodnie z wymogami w/w rozporządzenia do dnia 01-12-2004 należało opracować i wdrożyć Politykę Bezpieczeństwa (PB) i Instrukcję Zarządzania Systemem Informatycznym (IZSI).

Ważniejsze akty prawne i normy

- Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity - Dz. U. nr 101 z 2002 r. poz. 926, z późniejszymi zmianami).
- Rozporządzenie Ministra SWiA 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. Nr 100, poz. 1024).
- Norma ISO 27001 oraz 17799

Polityka bezpieczeństwa

- Polityka bezpieczeństwa (PB) obejmuje swoim zakresem nie tylko sieć komputerową przedsiębiorstwa czy instytucji, ale także całość zagadnień związanych z bezpieczeństwem danych będących w dyspozycji firmy.
- Polityka bezpieczeństwa organizacji definiuje poprawne i niepoprawne - w sensie bezpieczeństwa - sposoby wykorzystywania kont użytkowników i danych przechowywanych w systemie.

Realizacja polityki bezpieczeństwa

Polityka bezpieczeństwa wymaga ciągłych modyfikacji odzwierciedlających zmieniające się uwarunkowania pracy firmy, profilu działania, stosowanego sprzętu i oprogramowania.

- Analiza istniejących zasobów i zagrożeń.
- Opracowanie projektu i dokumentacji.
- Wdrożenie projektu.
- Ciągły nadzór, kontrola i modyfikacja istniejącej polityki.

Szkolenia i regulaminy

- Mechanizmy bezpieczeństwa będą skuteczne, jeżeli personel zostanie prawidłowo przeszkolony z zakresu bezpieczeństwa i zapoznany z regulaminem pracy, co zostanie udokumentowane podpisaniem oświadczenia.
- Użytkownicy sieci powinni dokładnie znać wytyczne odnośnie tego, co mogą oraz czego nie mogą dokonywać w procesie przetwarzania informacji.

Disaster Recovery

Po awarii/naruszeniu bezpieczeństwa:

- Efekt paniki, brak chłodnej oceny sytuacji
- Brak czasu na analizę dokumentacji
- Brak koordynacji działań

Nierozważna reakcja może spowodować większe straty niż sama awaria/incydent!

Rozwiązaniem jest opracowanie planu awaryjnego, realizowanego punkt po punkcie w wypadku katastrofy.

Disaster Recovery Plan

DRP zawiera:

- ocenę możliwych zagrożeń
- określenie, które elementy struktury firmy mają charakter kluczowy
- jakie są ich wymagania niezawodnościowe, np. dopuszczalny czas niedostępności
- jakie są zależności pomiędzy poszczególnymi jednostkami funkcjonalnymi w momencie kryzysu (efekt domina)

Ważnym mechanizmem w DRP są centra zapasowe lub internetowe centra danych umożliwiające składowanie danych w odległej lokalizacji.

Standaryzacja oceny bezpieczeństwa systemów komputerowych

Po co nam standardy

Standard – *wzorzec zatwierdzony przez autorytet (np. organizację standaryzacyjną) lub nieformalnie upowszechniony*

- Systematyzują proces oceny
- Ułatwiają wyznaczanie celów i rozliczalność
- Ułatwiają projektowanie i wytwarzanie

Standardy w bezpieczeństwie IT

- Miary gwarantowanej odporności
  - Klasy (TCSEC)
  - Stopnie (E1-E6 w ITSEC)
  - Poziomy uzasadnionego zaufania EAL (CC)
- Najlepsze praktyki (norma 27001)

Standaryzacja oceny bezpieczeństwa systemów komputerowych

- *Trusted Computer System Evaluation Criteria (TCSEC) - orange book* - 1983
- *Information Technology Security Evaluation Crirteria* (ITSEC) – 1991
- *Evaluation Criteria for Information Technology Security – ISO/IEC 15408 – Common Criteria - 1997*

Wymogi bezpieczeństwa TCSEC

- **Polityka bezpieczeństwa**. Musi istnieć jasna i dobrze zdefiniowana PB systemu. Ponadto muszą istnieć mechanizmy wymuszające jej realizację.
- **Opis obiektów**. Dla każdego obiektu systemu muszą być określone: poziom ochrony oraz prawa dostępu podmiotów.
- **Identyfikacja**. Podmioty muszą posiadać nazwę, aby możliwa była ich identyfikacja.

Wymogi bezpieczeństwa TCSEC

- **Audyt**. Informacje pochodzące z audytu muszą być gromadzone, rejestrowane i przechowywane w bezpieczny sposób w celu umożliwienia wykonania dokładnej analizy ewentualnych zagrożeń.
- **Pewność**. System komputerowy musi zawierać sprzętowe i/lub programowe mechanizmy zabezpieczeń, które można w sposób niezależny ocenić pod względem spełniania wymogów.

Wymogi bezpieczeństwa TCSEC

- **Ciągła ochrona**. Mechanizmy ochrony muszą być stale chronione przed nieautoryzowanym dostępem. W przeciwnym wypadku niemożliwe jest utrzymanie odpowiedniego poziomu ochrony.

TCSEC

- Ocena poziomu bezpieczeństwa systemu na bazie pomarańczowej księgi polega na zakwalifikowaniu go do którejś z siedmiu klas.
- Wyższe poziomy bezpieczeństwa zawierają wszystkie cechy poziomów niższych.

TCSEC - poziom D

- (*Minimal protection*) - najniższy poziom
- Poziom ten nie wymaga certyfikacji, oznacza brak zabezpieczeń.
- Przykładem jest procedura autoryzacji dostępu w Microsoft Windows 98. Do tej grupy należy również system DOS.

TCSEC - poziom C

- Definiowanie dostępu do obiektów poprzez indywidualne i grupowe prawa dostępu.
- Dostęp kontrolowany poprzez uwierzytelnianie.
- Obiekty systemu używane wielokrotnie nie zostawiają śladów
- Dostępne narzędzia umożliwiające sprawdzenie integralności systemu.
- Mechanizmy zabezpieczające muszą być przetestowane i działać zgodnie z instrukcją.
- Wymagana jest dokumentacja i sporządzenia testów systemu.

TCSEC – poziom B

- Kontrola dostępu do obiektów systemu oparta na zabezpieczeniu obowiązkowym (*Mandatory protection*).
- Wprowadzono etykietowanie podmiotów i obiektów (klauzule tajności): 'tajne', 'ściśle tajne', itp.
- Wymagany inspektor do spraw ochrony
- Podział elementów systemu na krytyczne i obojętne dla bezpieczeństwa systemu
- Procedury odtwarzania stanu systemu

TCSEC – poziom A

- *Verified design* – jedna klasa A1
- Zastosowanie narzędzi matematycznych do udowodnienia bezpieczeństwa
- Badanie wiarygodności całego cyklu projektowo - wdrożeniowego
- Sprzęt i oprogramowanie podlega specjalnej ochronie w trakcie transportu

Information Technology Security Evaluation Criteria - ITSEC

- Komisja Wspólnot Europejskich – 1991
- Ocena siły zabezpieczeń (niska, średnia, wysoka)
- Ocena poprawności realizacji (E1-E6)
- Stopień spełnienia wymagań funkcjonalnych – 10 klas funkcjonalności

ITSEC – cechy funkcjonalności

- kontrola dostępu do systemu (identyfikacja i uwierzytelnianie)
- kontrola dostępu do obiektów
- odpowiedzialność
- nasłuch
- ponowne wykorzystanie obiektów
- wierność (integralność danych, detekcja i prewencja)
- niezawodność pracy
- wymiana danych

Klasy funkcjonalności ITSEC

- **Klasy F-C1, F-C2, F-B1, F-B2, F-B3** odpowiadają klasom C1, C2, B1, B2, B3 TCSEC
- **Klasa F-IN** – zwiększone wymagania dotyczące integralności
- **Klasa F-AV** – zwiększone wymagania dotyczące niezawodności

Klasy funkcjonalności ITSEC

- **Klasa F-DI** – zwiększone wymagania dotyczące integralności danych w sieciach telekomunikacyjnych
- **Klasa F-DC** – zwiększone wymagania dotyczące tajności danych
- **Klasa F-DX** – zwiększone wymagania dotyczące tajności danych i integralności danych

Poziomy pewności ITSEC

- **E0** – brak odpowiedniej pewności.
- **E1** – istnienie nieformalnego opisu architektury bezpieczeństwa
- **E2** – nieformalny opis koncepcji szczegółowej, dowody testów, kontrola konfiguracji i proces nadzoru dystrybucji
- **E3** – dostarczenie szczegółowej koncepcji i kodu źródłowego

Poziomy pewności ITSEC

- **E4** – istnienie formalnego modelu polityki bezpieczeństwa
- **E5** – ścisła relacja między opisem formalnym koncepcji szczegółowej i kodem źródłowym
- **E6** – istnienie formalnego opisu architektury bezpieczeństwa kompatybilnej z modelem formalnym polityki bezpieczeństwa

ISO/IEC 15408 - Common Criteria

- Przyjęte jako standard NATO w 2001 roku (istnieje rejestr produktów NATO spełniających wymogi CC)
- Najnowsza wersja CC 3.1 obowiązuje od marca 2008 roku

Common Criteria

- CC są zaleceniami służącymi do jednolitego sposobu oceny systemów informatycznych pod względem bezpieczeństwa
- CC określają co należy zrobić, ale nie jak to zrobić
- CC mogą byś stosowane do wszystkich produktów informatycznych (sprzęt, oprogramowanie)

Common Criteria

- CC są przeznaczone dla użytkowników, projektantów oraz oceniających produkty informatyczne
- CC nie zalecają żadnej z metodyk projektowania czy wytwarzania

Common Criteria

- CC są zbudowane w postaci katalogu
- Pojęcia:
  - Klasa
  - Rodzina
  - Komponent
  - Element schematu konstrukcji wymagań

Common Criteria

Wynikiem oceny według CC jest:

- Stwierdzenie zgodności produktu (systemu) z określonym profilem zabezpieczeń
- Spełnienie wymagań określonych w zadaniach zabezpieczenia
- Przypisanie do któregoś z poziomów bezpieczeństwa *(Evaluation Assurance Level – Poziom Uzasadnionego Zaufania)*

ISO/IEC 15408

Norma składa się z 3 rozdziałów:

- Introduction and general model
  Ogólny model, zasady oceny
- Security functional requirements
  Katalog komponentów funkcjonalnych pogrupowanych w rodziny i klasy
- Security assurance requirements
  Katalog komponentów bezpieczeństwa związanych z procesami projektowania i wytwarzania

COBIT

- *Control Objectives for Information and Related Technology*
- Opracowany przez ISACA (*Information Systems Audit and Control Association*)
- Standard (metodyka) oceny bezpieczeństwa i audytu bezpieczeństwa IT
- Aktualna wersja: 4 (2007)

PN-ISO/IEC 27001
PN-ISO/IEC 17799

- *'best practices'*
- Zawartość
  - Zasady zarządzania bezpieczeństwem
  - SZBI
  - Zarządzanie ryzykiem bezpieczeństwa informacji
- Certyfikaty zgodności z normą

Zarządzanie Bezpieczeństwem Informacji

Analiza Ryzyka

Ryzyko wg. IEC 61508

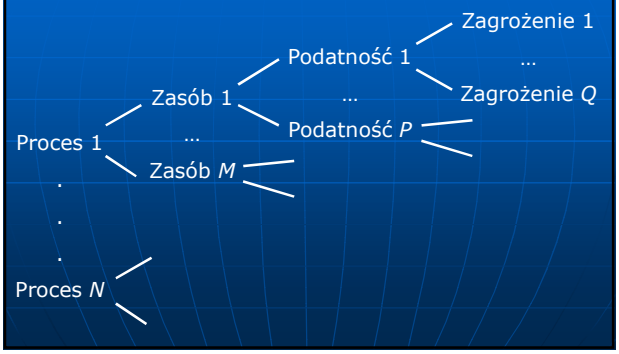
Miara stopnia zagrożenia dla tajności, integralności i dostępności informacji wyrażona jako iloczyn prawdopodobieństwa wystąpienia sytuacji stwarzającej takie zagrożenie i stopnia szkodliwości jej skutków

Analiza Ryzyka

- Identyfikacja zasobów,
- Określenie ich wartości,
- Identyfikacja możliwych zagrożeń oraz prawdopodobieństwa ich wystąpienia,
- Analiza metod przeciwdziałania uwzględniająca ich koszt.

Wykonywana cyklicznie, nie tylko w fazie projektowania !

Analiza ryzyka – etap I



Inwentaryzacja zasobów

Zasoby (wg. PN-ISO/IEC- 27001):

- Informacja: bazy danych, kartoteki, dokumentacje, umowy, podręczniki, …
- Oprogramowanie użytkowe
- Komputery, urządzenia teleinformatyczne, drukarki, …
- Urządzenia/systemy usługowe: zasilanie, łączność, oświetlenie, …

Lokalizacja zasobu, adres IP, właściciel

Zarządzanie ryzykiem

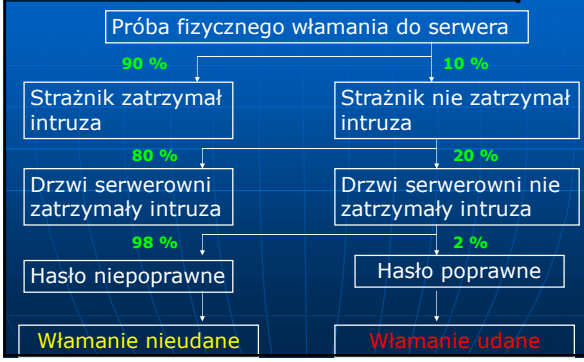
- Analiza ryzyka
  - Identyfikacja (zasobów, zagrożeń, podatności, potencjalnych strat)
  - Oszacowanie ryzyka
  - Ocena ryzyka
- Opracowanie zasad postępowania z ryzykiem (unikanie, kontrolowanie, transfer)
- Akceptacja ryzyka szczątkowego

Szacowanie ryzyka

- Określenie możliwości realizacji zagrożeń
- Metody:
  - Ilościowe – prawdopodobieństwo
  - Jakościowe – miary opisowe
- Mapy (matryce) ryzyka, drzewa zdarzeń
- Opis ryzyka:
  - *Possible maximum loss*
  - Prawdopodobieństwo realizacji
  - Okoliczności, w których możliwa jest realizacja

Mapa ryzyka

Drzewo zdarzeń



Szacowanie ryzyka – metoda jakościowa

	Poziom zagrożenia	Niski			Średni			Wysoki		
	Poziom podatności	N	Ś	W	N	Ś	W	N	Ś	W
Wartość zasobu	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Zarządzanie Bezpieczeństwem Informacji

Audyt bezpieczeństwa teleinformatycznego

Audyt bezpieczeństwa teleinformatycznego

- ABT to systematyczny, niezależny i udokumentowany proces przeprowadzany w celu uzyskania tzw. dowodów z audytu i dokonania na ich podstawie obiektywnej oceny - określenia w jakim stopniu są spełnione kryteria audytu (najczęściej określone jedną z norm).

Audyt bezpieczeństwa teleinformatycznego

- Założeniem jest szukanie zgodności (np. z określoną normą) a nie niezgodności czy braków (audyt nie jest kontrolą).
- Audyt musi być systematyczny oraz niezależny.
- Niezależność oznacza, że podmiot przeprowadzający audyt nie może być powiązany z audytowanym (np. zespołem budującym system zabezpieczeń, dostawcą sprzętu i oprogramowania, organizacją podlegającą audytowi).

Działania kluczowe audytu

- Planowanie - na ogół największy nakład pracy. Należy określić:
  - Zakres audytu, listy ocenianych obiektów
  - Metody audytu
  - Listy pytań audytowych (tzw. checklisty).
- Wykonywanie
- Raportowanie
- Działania korygujące i zamknięcie audytu

Zakres audytu

ABT obejmuje następujące zasoby i mechanizmy bezpieczeństwa:

- organizacyjne (procedury, struktury organizacyjne)
- fizyczne (zamki, płoty)
- techniczne (ppoż, monitoring, dostęp do obiektów – np. uwierzytelnianie biometryczne)
- programowe (zabezpieczenia systemów operacyjnych i aplikacji, kontrola dostępu, uwierzytelnianie, IPS, zapory ogniowe, itp.)
- ludzkie (świadomość procedur, obowiązków, zagrożeń, konsekwencji).

Podstawowe działania audytowe

1. Przygotowanie i wypełnienie checklisty
   - oznaczanie wymagań jako "spełnione", "niespełnione", "spełnione częściowo", "nie dotyczy„
   - wypełnianie na podstawie wywiadów, wizji lokalnych, kontroli i analizy dokumentów, wykonanych testów i badań

Podstawowe działania audytowe

2. Badanie systemów ochrony fizycznej, technicznej, programowej z wykorzystaniem narzędzi i testów penetracyjnych.

   Testy penetracyjne obejmują:
   - skanowanie i identyfikowanie systemów
   - badanie odporności na ataki DoS (tylko na wyraźne życzenie zleceniodawcy),
   - próby wykorzystania zidentyfikowanych podatności do przeprowadzenia szkodliwych działań z wewnątrz i z zewnątrz sieci,
   - podsłuchiwanie (sniffing).

Podstawowe korzyści z ABT

- stwierdzenie, czy system informatyczny został zabezpieczony zgodnie z ustaleniami między zleceniodawcą a wykonawcą budującym system zabezpieczeń (ocena wykonania umowy)
- wykazanie, że system spełnia wymagania określonych norm i standardów
- możliwość wystawienia certyfikatu bezpieczeństwa
- ocena jakości i skuteczności systemu bezpieczeństwa
- wyniki audytu można wykorzystać do wdrożenia odpowiednich zmian

Testy penetracyjne

- Symulowane ataki, uzgodnione (na ogół zamówione) przez właściciela celu
- Ich zadaniem jest wykrycie podatności (bez niszczenia celu)
- Przeprowadzane przez niezależne podmioty

Rodzaje testów penetracyjnych

- Bez wiedzy o testowanym systemie
- Z częściową wiedzą
- Z pełną (szczegółową) wiedzą

- Zewnętrzne
- Wewnętrzne

Metodyki testów

- Open Source Security Testing Methodology (OSSTM)
  - Omawia aspekty teleinformatyczne, fizyczne, prawne, związane ze świadomością użytkowników, podatnością na inżynierię socjalną
  - Opisuje planowanie audytów, obszary wymagające testowania, zasady raportowania
  - *Rules of Engagement* - ramy prawne i etyczne usług z dziedziny bezpieczeństwa teleinformatycznego

Realizacja testów

- Etap rozpoznania, testowanie typowych podatności, testy wg. Metodyki
- Narzędzia
- Opracowanie raportu