Zagrożenia i podatności bezpieczeństwa

16.1.1

Rodzaje zagrożeń

Przewodowe i bezprzewodowe sieci komputerowe są niezbędne w codziennych czynnościach. Osoby prywatne oraz organizacje często są zależne od swoich komputerów i sieci. Włamania do sieci mogą powodować kosztowne przerwy w jej działaniu. Ataki mogą być bardzo niszczycielskie i mogą doprowadzić do straty czasu i pieniędzy poprzez uszkodzenie lub kradzież ważnych danych.

Intruzi mogą uzyskać dostęp do sieci przez luki w oprogramowaniu, ataki sprzętowe czy nawet za pomocą mniej skomplikowanych metod, takich jak zgadywanie nazwy użytkownika i hasła. Intruzi, którzy uzyskali dostęp przez modyfikację oprogramowania czy wykorzystanie luki, są często nazywani podmiotami zagrożeń.

Po uzyskaniu dostępu do sieci podmiot zagrożenia może powodować cztery typy zagrożeń.

Kliknij każdy przycisk, aby uzyskać informacje o każdym zagrożeniu.

Kradzież informacji | Utrata i zmiana danych | Kradzież tożsamości | Blokada usługi

Kradzież informacji jest włamaniem się do komputera w celu

uzyskania poufnych informacji. Informacje mogą być wykorzystywane lub sprzedawane do różnych celów. Przykład: to kradzież zastrzeżonych informacji organizacji, takich jak dane dotyczące badań i rozwoju.

16.1.2

Rodzaje podatności bezpieczeństwa

Podatność to stopień słabości sieci lub urządzenia. Pewien stopień podatności jest związany z routerami, przełącznikami, komputerami stacjonarnymi, serwerami, a nawet urządzeniami bezpieczeństwa. Zazwyczaj atakowane są urządzenia sieciowe będące punktami końcowymi, takie jak serwery i komputery stacjonarne.

Istnieją trzy główne podatności lub luki: technologiczne, konfiguracyjne i dotyczące polityki bezpieczeństwa. Wszystkie trzy z tych źródeł podatności mogą pozostawić sieć lub urządzenie otwarte na różne ataki, w tym ataki złośliwego kodu i ataki sieciowe.

Kliknij każdy przycisk tabeli z przykładami i opisem każdego typu podatności.

Podatności technologiczne

Podatność	Opis
Niedoskonałości protokółu TCP/IP	• Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), i Internet Control Message Protocol (ICMP) są z natury niebezpieczne. • Simple Network Management Protocol (SNMP) i Simple Mail Transfer Protocol (SMTP) są związane z dziedziczoną niepewną strukturą TCP na którym został zaprojektowany.
Niedoskonałości systemu operacyjnego	• Każdy system operacyjny ma problemy z bezpieczeństwem, które muszą być uwzględnione. • UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8 • Podatności są udokumentowane w archiwach Computer Emergency Response Team (CERT) na stronie http://www.cert.org.
Niedoskonałości sprzętu sieciowego	Różne rodzaje urządzeń sieciowych, takich jak routery, zapory sieciowe i przełączniki mają słabe punkty bezpieczeństwa, które muszą być rozpoznawane i chronione . Ich słabości obejmują ochronę hasłem, brak uwierzytelniania, protokoły routingu i dziury zapory.

16.1.3

Bezpieczeństwo fizyczne

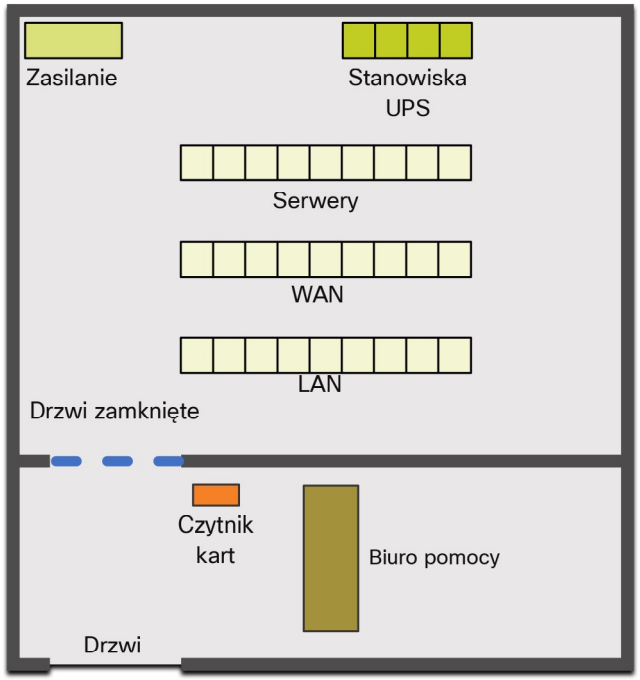
Równie ważnym zagrożonym obszarem sieci, który należy wziąć pod uwagę, jest fizyczne bezpieczeństwo urządzeń. Jeśli zasoby sieciowe mogą zostać fizycznie zagrożone, podmiot zagrożenia może zablokować użycie zasobów sieciowych.

Są cztery klasy zagrożeń fizycznych:

- **Zagrożenia sprzętowe -** Fizyczne uszkodzenia serwerów, routerów, przełączników, ciągów okablowania i stacji roboczych.
- **Zagrożenia środowiskowe -** Skrajne temperatury (za gorąco lub za zimno) lub skrajna wilgotność (zbyt duża wilgotność lub zbyt sucho).
- **Zagrożenia elektryczne -** Skoki napięcia, zbyt niskie napięcie (spadek napięcia zasilania), stan zasilania (szumy) oraz całkowita utrata mocy.
- **Zagrożenia związane z utrzymaniem -** Niewłaściwa obsługa kluczowych komponentów elektrycznych (wyładowania elektrostatyczne), brak krytycznych elementów zamiennych, złe okablowanie i słabe oznakowanie.

Należy stworzyć i wdrożyć dobry plan bezpieczeństwa fizycznego, aby rozwiązać te problemy. Rysunek pokazuje przykład fizycznego planu bezpieczeństwa.

Plan ochrony fizycznej ogranicza uszkodzenia sprzętu



- Zabezpiecz pomieszczenie z komputerami.
- Zastosuj środki fizycznego bezpieczeństwa, aby ograniczyć uszkodzenia sprzętu.

Krok 1. Zabezpiecz sprzęt i zapobiegnij nieautoryzowanemu dostępowi przez drzwi, z sufitu, podniesionej podłogi, przez okna, kanał i otwory wentylacyjne.

Krok 2. Monitoruj i kontroluj wejścia za pomocą rejestru elektronicznego.

Krok 3. Użyj kamery bezpieczeństwa.

16.1.4

Sprawdź, czy zrozumiałeś - Zagrożenia i podatności bezpieczeństwa

Sprawdź swoją wiedzę na temat zagrożeń i podatności bezpieczeństwa, wybierając NAJLEPSZĄ odpowiedź na poniższe pytania.

1. Jakie zagrożenie jest opisane, gdy podmiot zagrożeń wysyła wirusa, który może sformatować dysk twardy?

- utrata danych lub manipulacja
- zakłócenie usług
- kradzież tożsamości
- kradzież informacji

2. Jakie zagrożenie jest opisane, gdy podmiot zagrażający dokonuje nielegalnych zakupów online przy użyciu skradzionych informacji kredytowych?

- utrata danych lub manipulacja
- zakłócenie usług

- kradzież tożsamości
- kradzież informacji

3. Jakiego rodzaju zagrożenie opisano, gdy podmiot zagrożenia uniemożliwia użytkownikom uprawnionym dostęp do usług danych?

- utrata danych lub manipulacja
- zakłócenie usług
- kradzież tożsamości
- kradzież informacji

4. Jakie zagrożenie jest opisane, gdy podmiot zagrożenia kradnie dane z badań naukowych?

- utrata danych lub manipulacja
- zakłócenie usług
- kradzież tożsamości
- kradzież informacji

5. Jakie zagrożenie jest opisane, gdy podmiot zagrożeń przeciąża sieć, aby odmówiła innym użytkownikom dostępu do niej?

- utrata danych lub manipulacja
- zakłócenie usług
- kradzież tożsamości
- kradzież informacji

6. Jakie zagrożenie jest opisane, gdy podmiot zagrożenia zmienia rekordy danych?

- utrata danych lub manipulacja
- zakłócenie usług
- kradzież tożsamości

- kradzież informacji

7. Jakie zagrożenie jest opisane, gdy podmiot zagrożenia kradnie bazę danych użytkowników firmy?

- utrata danych lub manipulacja
- zakłócenie usług
- kradzież tożsamości
- kradzież informacji

8. Jakiego rodzaju zagrożenie opisano, gdy podmiot zagrażający podszywa się pod inną osobę w celu uzyskania informacji kredytowej o tej osobie?

- utrata danych lub manipulacja
- zakłócenie usług
- kradzież tożsamości
- kradzież informacji

Sprawdź

Rozwiązanie

Resetuj

16.0 Wprowadzenie

16.2 Ataki sieciowe