Bezpieczeństwo sieci

1.8.1

Zagrożenia bezpieczeństwa

Bez wątpienia słyszałeś lub czytałeś wiadomości o naruszeniach sieci firmowej, dając podmiotom zagrażającym dostęp do danych osobowych tysięcy klientów. Z tego powodu bezpieczeństwo sieci zawsze będzie priorytetem administratorów.

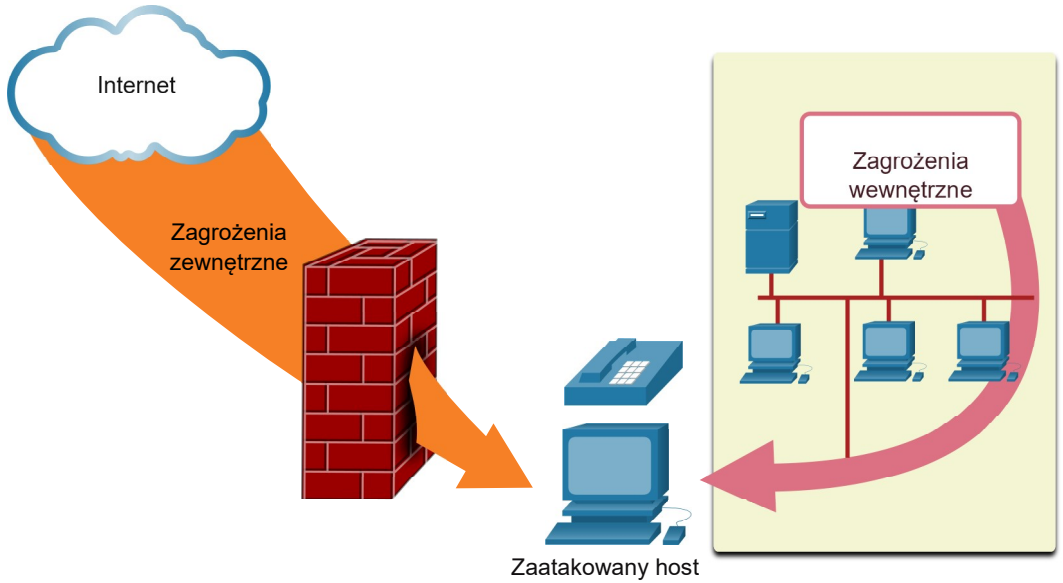
Bezpieczeństwo sieci jest integralną częścią sieci komputerowych, niezależnie od tego, czy sieć jest w domu z pojedynczym połączeniem z Internetem, czy jest korporacją z tysiącami użytkowników. Bezpieczeństwo sieci musi uwzględniać środowisko, a także narzędzia i wymagania sieci. Musi być w stanie zabezpieczyć dane, a jednocześnie zapewnić odpowiednią jakość usług, której oczekują użytkownicy sieci.

Zabezpieczenie sieci obejmuje: protokoły, technologie, urządzenia, narzędzia, techniki ochrony danych i uniknięcia zagrożeń. Wektory zagrożeń mogą być zewnętrzne lub wewnętrzne. Wiele współczesnych zagrożeń bezpieczeństwa sieci pochodzi z Internetu.

Istnieje kilka typowych zagrożeń zewnętrznych dla sieci:

- **Wirusy, robaki i konie trojańskie** - zawierają złośliwe oprogramowanie lub kod uruchamiany na urządzeniu użytkownika.
- **Spyware i adware** - Są to rodzaje oprogramowania, które są instalowane na urządzeniu użytkownika. Oprogramowanie to następnie potajemnie zbiera informacje o użytkowniku.
- **Ataki zero-day** - nazywane również atakami zero-hour, pojawiają się w pierwszym dniu, kiedy podatność staje się znana.
- **Ataki aktora zagrożeń** - Złośliwa osoba atakuje urządzenia użytkownika lub zasoby sieciowe.
- **Odmowa usługi** - ataki mające na celu spowolnienie lub zatrzymanie działania aplikacji i procesów działających w urządzeniu sieciowym.
- **Przechwytywanie i kradzież danych** - Ten atak przechwytuje prywatne informacje z sieci organizacji.
- **Kradzież tożsamości** - typ ataku polegający na kradzieży danych logowania użytkownika w celu dostępu do jego prywatnych danych.

Równie ważnym jest aby wziąć pod uwagę wewnętrzne źródła zagrożenia. Istnieje wiele przypadków, które pokazują iż najczęściej winni naruszeniu bezpieczeństwa sieci są użytkownicy wewnętrzni. Tego typu incydenty są spowodowane np. zagubionymi lub skradzionymi urządzeniami, przypadkowymi błędami pracowników, a w środowisku biznesowym możemy nawet mówić o celowych i szkodliwych działaniach przez niektórych zatrudnionych. Wraz ze zmieniającymi się strategiami BYOD dane korporacyjne są znacznie bardziej narażone. Dlatego przy opracowywaniu polityki bezpieczeństwa ważne jest, aby zająć się zarówno zewnętrznymi, jak i wewnętrznymi zagrożeniami bezpieczeństwa, jak pokazano na rysunku.



1.8.2

Rozwiązania bezpieczeństwa

Nie istnieje jedno rozwiązanie, które byłoby wstanie ochronić sieć przed wszystkimi istniejącymi zagrożeniami, dlatego też, zabezpieczenia powinny być implementowane w wielu warstwach, stosując przy tym więcej niż jeden system zabezpieczeń. Jeśli jeden składnik bezpieczeństwa nie zidentyfikuje i nie ochroni sieci, inne mogą sobie poradzić.

Zazwyczaj sieci domowe są chronione na poziomie podstawowym. Zazwyczaj wdrażasz je na urządzeniach końcowych, a także w punkcie połączenia z Internetem, a nawet możesz polegać na usługach zakontraktowanych u dostawcy usług internetowych.

Podstawowe elementy bezpieczeństwa dla sieci domowej lub dla małego biura:

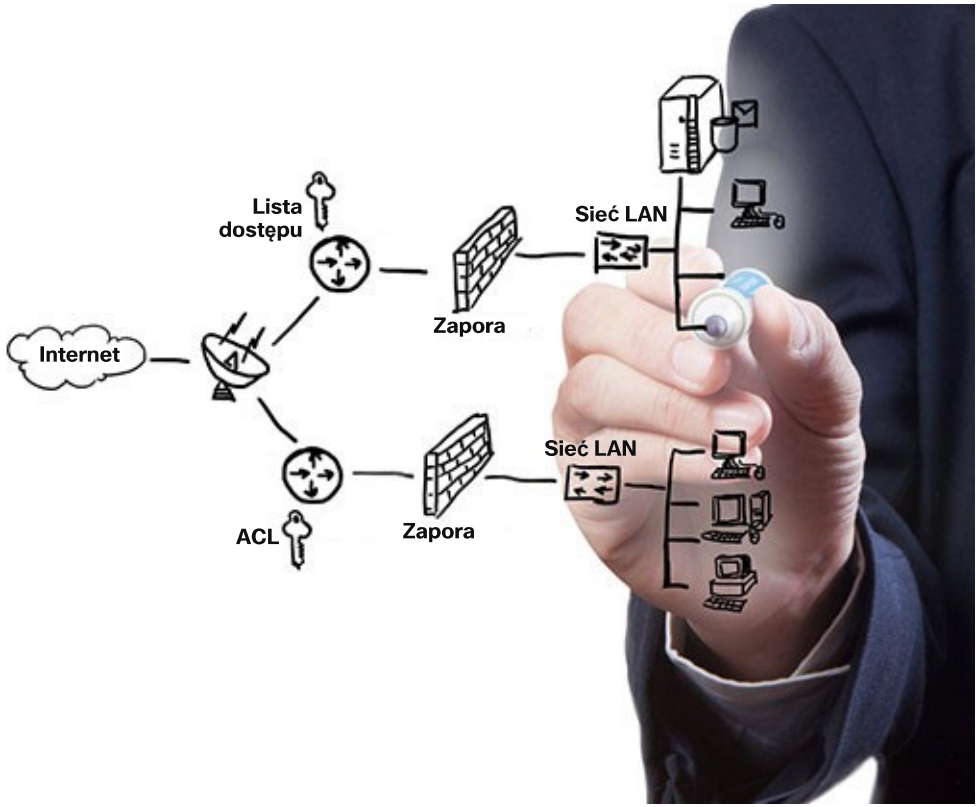
- **Oprogramowanie antywirusowe i antyszpiegowskie** - Te aplikacje pomagają chronić urządzenia końcowe przed zarażeniem złośliwym oprogramowaniem.
- **Zapory filtrujące** - zapora filtrująca blokuje nieautoryzowany dostęp do sieci i ruch z niej. Można tutaj wyróżnić zaporę na urządzeniu końcowym, którego celem jest zapobieganie nieautoryzowanemu dostępowi do systemu lub też podstawową usługę filtrowania uruchomioną na routerze domowym, chroniącą sieć wewnętrzną przed zagrożeniami z zewnątrz.

W przeciwieństwie do sieci domowych, zabezpieczenia w sieciach korporacyjnych składają się zazwyczaj wielu elementów, wbudowanych w sieć, celem monitorowania i filtrowania ruchu. Najlepiej byłoby, gdyby wszystkie te komponenty współpracowały ze sobą, co zminimalizowałoby konieczność obsługi i zwiększyłoby bezpieczeństwo. Większe sieci i sieci firmowe używają programów antywirusowych, antyszpiegowskich i zapór filtrujących, ale mają również inne wymagania bezpieczeństwa:

- **Dedykowane systemy zapór** - Zapewniają one bardziej zaawansowane funkcje zapory, które mogą filtrować duże ilości ruchu z większą szczegółowością.
- **Listy kontroli dostępu (ACL)** - Te dodatkowo filtrują dostęp i przekazywanie ruchu na podstawie adresów IP i aplikacji.
- **Systemy przeciwdziałania atakom (IPS)** - Identyfikują szybko rozprzestrzeniające się zagrożenia takie jak ataki zero-day lub zero-hour.
- **Wirtualne sieci prywatne (VPN)** – Zapewniają bezpieczny dostęp do organizacji dla pracowników zdalnych.

Wymagania dotyczące bezpieczeństwa muszą uwzględniać specyfikę środowiska sieci, różnego rodzaju aplikacji i wymagań obliczeniowych. Zarówno środowiska domowe jak i firmowe muszą być w stanie zabezpieczyć swoje dane, a jednocześnie zapewnić odpowiednią jakość usług, taką jakiej się oczekuje od każdej z technologii. Dodatkowo, bezpieczeństwo musi być implementowane w taki sposób, aby mogło być skalowalne i gotowe na zmiany w ciągle zmieniających się trendach sieciowych.

Badanie zagrożeń bezpieczeństwa i nauka technik obrony, powinna rozpocząć się od dogłębnego zrozumienia zasad przełączania i routowania.



Sprawdź swoją wiedzę na temat bezpieczeństwa sieci, wybierając NAJLEPSZĄ odpowiedź na poniższe pytania.

1. Który atak spowalnia lub powoduje awarię sprzętu i programów?

- Firewall
- Wirus, robak, koń trojański
- Zero-day lub zero-hour
- Wirtualna sieć prywatna (VPN)
- Odmowa usługi (DoS)

2. Która opcja tworzy bezpieczne połączenie dla pracowników zdalnych?

- ◯ Zapora
- ◯ Wirus, robak, koń trojański
- ◯ Zero-day lub zero-hour
- ◯ Wirtualna sieć prywatna (VPN)
- ◯ Odmowa usługi (DoS)

3. Która opcja blokuje nieautoryzowany dostęp do Twojej sieci?

- ◯ Zapora
- ◯ Wirus, robak, koń trojański
- ◯ Zero-day lub zero-hour
- ◯ Wirtualna sieć prywatna (VPN)
- ◯ Odmowa usługi (DoS)

4. Która opcja opisuje atak sieciowy, który ma miejsce pierwszego dnia po wykryciu luki w zabezpieczeniach?

- ◯ Zapora
- ◯ Wirus, robak, koń trojański
- ◯ Zero-day lub zero-hour
- ◯ Wirtualna sieć prywatna (VPN)
- ◯ Odmowa usługi (DoS)

5. Która opcja opisuje złośliwy kod działający na urządzeniach użytkownika?

- ◯ Zapora
- ◯ Wirus, robak, koń trojański
- ◯ Zero-day lub zero-hour
- ◯ Wirtualna sieć prywatna (VPN)
- ◯ Odmowa usługi (DoS)

Sprawdź

Rozwiązanie

Resetuj

Wprowadzenie do sieci