# Podstawowe informacje o zabezpieczeniach sieci dla średnich i małych firm

## Czym są zabezpieczenia sieci?

Zabezpieczenia sieci to inaczej wszelkie działania mające na celu ochronę sprawnego działania i integralności sieci oraz danych, obejmujące zarówno rozwiązania sprzętowe, jak i programistyczne. Skuteczne zabezpieczenia sieci umożliwiają zarządzanie dostępem do sieci. Ich zadaniem jest również przeciwdziałanie różnym zagrożeniem i udaremnienie im uzyskania dostępu do sieci oraz rozprzestrzeniania się w niej.

## Jak działają zabezpieczenia sieci?

Zabezpieczenia sieci składają się z wielu warstw rozwiązań ochronnych zarówno na obrzeżach, jak i w samej sieci. Każda warstwa zabezpieczeń wdraża własne zasady i mechanizmy kontrolne. Upoważnieni użytkownicy mogą uzyskiwać dostęp do zasobów sieciowych, jednak zabezpieczenia uniemożliwiają cyberprzestępcom dokonywanie włamań i ataków na sieć.

## Jakie korzyści zapewniają zabezpieczenia sieci?

Cyfryzacja całkowicie odmieniła nasz świat, zmieniając to, jak żyjemy, pracujemy, bawimy się i uczymy. Każda organizacja, która chce świadczyć usługi odpowiadające na potrzeby klientów i pracowników, musi chronić swoją sieć. Zabezpieczenia sieci pomagają również chronić zastrzeżone informacje przed próbami wykradzenia, są także jednym ze sposobów ochrony wizerunku firmy.

### 6 kroków, które można podjąć, aby zabezpieczyć swoją sieć

1. Monitoruj ruch przychodzący i wychodzący na firewallu oraz dokładnie analizuj raporty. Nie polegaj wyłącznie na alertach ostrzegających o potencjalnie niebezpiecznej aktywności w sieci. Upewnij się, że ktoś w zespole potrafi czytać dane i jest przygotowany do podejmowania niezbędnych działań.
2. Bądź na bieżąco z informacjami o nowych zagrożeniach, publikowanymi w Internecie. Na przykład witryna Trend Micro TrendWatch na bieżąco umieszcza informacje o pojawiających się zagrożeniach.
3. Przeprowadzaj regularne aktualizacje firewalla i oprogramowania antywirusowego.
4. Zapewnij pracownikom dostęp do ciągłych szkoleń, aby umożliwić im zapoznawanie się ze wszelkimi zmianami zasad dopuszczalnego użytkowania. Zachęcaj ich również do wykazywania nieustannej czujności wobec potencjalnych zagrożeń, nie tylko w ich bezpośrednim otoczeniu. Jeśli pracownik zauważy coś podejrzanego, na przykład brak możliwości szybkiego zalogowania się do konta pocztowego, powinien o tym niezwłocznie poinformować odpowiednią osobę.
5. Zainstaluj rozwiązanie zapewniające ochronę danych. Tego typu urządzenie pomoże chronić firmę przed utratą danych w wyniku naruszenia zabezpieczeń sieci.
6. Zastanów się nad zastosowaniem dodatkowych zabezpieczeń, oferujących skuteczniejszą ochronę sieci, a jednocześnie zwiększających możliwości działania firmy.

# Podstawowe informacje o zabezpieczeniach sieci dla średnich i małych firm

## Rodzaje zabezpieczeń sieci

### Kontrola dostępu

Nie każdy użytkownik powinien mieć dostęp do sieci. Aby powstrzymać potencjalnych cyberprzestępców, należy zastanowić się nad funkcją każdego użytkownika i urządzenia, a następnie wdrożyć odpowiednie zasady bezpieczeństwa. Można zablokować lub ograniczyć dostęp niezgodnych urządzeń końcowych do sieci. Ten proces jest określany mianem kontroli dostępu do sieci.

### Oprogramowanie antywirusowe i ochrona przed złośliwym oprogramowaniem

Określenie „złośliwe oprogramowanie” oznacza między innymi wirusy, robaki, trojany, oprogramowania ransomware oraz spyware. Czasami zdarza się, że złośliwe oprogramowanie zainfekuje sieć, a następnie pozostaje uśpione przez kilka dni czy nawet tygodni. Najlepsze programy chroniące przed złośliwym oprogramowaniem nie tylko skanują ruch przychodzący do sieci pod kątem zagrożeń, lecz także bezustannie monitorują pliki krążące w sieci w poszukiwaniu anomalii, usuwają złośliwe oprogramowanie i naprawiają wyrządzone przez nie szkody.

### Zabezpieczenia aplikacji

Każde oprogramowanie używane w działalności firmy również wymaga zabezpieczeń: stworzonych przez własny dział IT lub zakupionych od producenta. Niestety każda aplikacja może zawierać luki w zabezpieczeniach, wykorzystywane przez cyberprzestępców do infiltracji sieci. Zabezpieczenia aplikacji obejmują sprzęt, oprogramowanie i procesy umożliwiające uszczelnienie tych luk.

### Analizy zachowań

Aby wykryć nietypowe zachowania w sieci, należy najpierw znać typowe zachowania. Narzędzia do analizy zachowań automatycznie rozpoznają działania odbiegające od normy. Dzięki temu zespół ds. bezpieczeństwa może skuteczniej identyfikować sygnały świadczące o naruszeniu zabezpieczeń i potencjalnych problemach oraz szybko wyeliminować zagrożenie.

### Zapobieganie utracie danych

Organizacje muszą mieć pewność, że ich pracownicy nie będą przesyłać informacji wrażliwych poza sieć. Technologie zapobiegania utracie danych umożliwiają zapobieganie pobieraniu, przesyłaniu czy nawet drukowaniu istotnych informacji w sposób niezapewniający ich bezpieczeństwa.

### Zabezpieczenia poczty e-mail

Bramy poczty e-mail są podstawowym wektorem naruszeń bezpieczeństwa. Cyberprzestępcy wykorzystują dane osobowe i socjotechniki do tworzenia wyrafinowanych kampanii wyłudzania informacji, które mają na celu oszukanie odbiorców i przekierowanie ich do witryn rozsyłających złośliwe oprogramowanie. Aplikacja zabezpieczające pocztę e-mail blokują ataki z zewnątrz i kontrolują wiadomości wychodzące w celu zapobieżenia utracie wrażliwych danych.

### Firewalle

Firewalle stanowią zaporę między zaufaną siecią wewnętrzną i niezaufaną siecią zewnętrzną, na przykład Internetem. Używają do tego zbioru zdefiniowanych zasad zezwalających na ruch lub blokujących go. Firewall może mieć postać sprzętu lub oprogramowania bądź stanowić ich połączenie. Firma Cisco oferuje urządzenia do ujednoliconego zarządzania zagrożeniami i ukierunkowane na obronę przed zagrożeniami firewalle nowej generacji.

### Systemy zapobiegania włamaniom

System zapobiegania włamaniom (IPS) skanuje ruch sieciowy, aby aktywnie blokować ataki. Działanie urządzeń IPS nowej generacji (NGIPS) firmy Cisco polega na korelowaniu ogromnych ilości globalnych informacji o zagrożeniach w celu blokowania złośliwych ataków, a także monitorowania zachowania podejrzanych plików i złośliwego oprogramowania w całej sieci, aby uniemożliwić rozprzestrzenianie się ognisk infekcji oraz ponowne zainfekowanie sieci.

# Podstawowe informacje o zabezpieczeniach sieci dla średnich i małych firm

## Zabezpieczenia urządzeń przenośnych

Celem cyberprzestępców coraz częściej stają się urządzenia przenośne i zainstalowane na nich aplikacje. W ciągu najbliższych trzech lat 90% działów IT może obsługiwać aplikacje firmowe na osobistych urządzeniach przenośnych. Naturalnie będzie się to wiązać z koniecznością kontrolowania, które urządzenia mogą uzyskać dostęp do sieci, a także skonfigurowania tych połączeń w sposób zapewniający prywatność ruchu sieciowego.

## Segmentacja sieci

Zdefiniowana programowo segmentacja sieci umożliwia podział ruchu sieciowego na różne klasyfikacje oraz ułatwia egzekwowanie zasad bezpieczeństwa. W idealnej sytuacji takie klasyfikacje są oparte na tożsamości urządzenia końcowego, nie samych adresach IP. Prawa dostępu można przypisywać na podstawie roli, lokalizacji i innych, co umożliwia przypisanie właściwego poziomu dostępu do właściwych osób, a także wyizolowanie i wyeliminowanie podejrzanych urządzeń.

## VPN

Wirtualna sieć prywatna umożliwia szyfrowanie połączenia między punktem końcowym i siecią, realizowane często za pośrednictwem Internetu. Sieć VPN zdalnego dostępu używa zazwyczaj protokołu IPsec lub SSL (Secure Socket Layer) do uwierzytelniania komunikacji między urządzeniem i siecią.

## Zabezpieczenia sieci WWW

Rozwiązania z zakresu bezpieczeństwa sieci WWW pozwalają kontrolować to, jak personel firmy korzysta z sieci WWW, blokować zagrożenia WWW oraz uniemożliwiać dostęp do złośliwych witryn internetowych. Pomogą chronić bramę sieci w siedzibie firmy lub w chmurze. Określenie „zabezpieczenia sieci WWW" odnosi się również do kroków podejmowanych w celu ochrony własnej witryny internetowej firmy.

## Zabezpieczenia sieci bezprzewodowej

Sieci bezprzewodowe nie są równie bezpieczne jak sieci przewodowe. Bez zastosowania skutecznych środków bezpieczeństwa instalację bezprzewodowej sieci LAN można porównać do zainstalowania wszędzie portów Ethernet, nawet na parkingu. Udaremnienie ataku na sieć bezprzewodową wymaga produktów opracowanych specjalnie z myślą o jej ochronie.


**Centrala dla krajów Ameryki Północnej i Południowej**
Cisco Systems, Inc.
San Jose, CA

**Centrala dla krajów Azji i Pacyfiku**
Cisco Systems (USA) Pte. Ltd.
Singapur

**Centrala europejska**
Cisco Systems International BV, Amsterdam, Holandia

Firma Cisco ma ponad 200 biur na całym świecie. Pełną listę adresów, numerów telefonów oraz faksów można znaleźć w witrynie firmy Cisco pod adresem **www.cisco.com/go/offices.**