ARTYKUŁ PRZEGLĄDOWY

PIĘĆ NAJWAŻNIEJSZYCH PROBLEMÓW DOTYCZĄCYCH BEZPIECZEŃSTWA W MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTWACH

Samo broniące się sieci (Self-Defending Network) – oferta dostosowana do potrzeb małych i średnich przedsiębiorstw

STRESZCZENIE

W małych i średnich przedsiębiorstwach Internet oraz aplikacje sieciowe służą do pozyskiwania nowych klientów i wydajniejszego świadczenia usług. Jednocześnie nowe zagrożenia oraz obowiązujące przepisy coraz częściej zmuszają firmy do zapewnienia niezawodności i bezpieczeństwa swoich sieci. Cisco Systems oferuje wszechstronne i niedrogie, zintegrowane systemy zabezpieczeń dostosowane do potrzeb małych i średnich przedsiębiorstw. Rozwiązania te zapewniają utrzymanie ciągłości biznesowej, ochronę poufności i obniżenie kosztów operacyjnych. Dzięki temu firmy mogą spokojnie rozwijać swoją działalność, zamiast koncentrować się na problemach bezpieczeństwa sieciowego.

WYZWANIA BIZNESOWE

We współczesnym, konkurencyjnym środowisku biznesowym, małe i średnie przedsiębiorstwa koncentrują się na rozwijaniu działalności i usprawnianiu obsługi klienta, przy jednoczesnym obniżaniu kosztów. Na szczęście Internet oraz aplikacje sieciowe wyrównują szanse na rynku. Małe i średnie przedsiębiorstwa traktują sieć jako narzędzie, które umożliwia zdobywanie nowych klientów oraz pozwala szybko i tanio komunikować się z klientami i partnerami. Jednak rozwijający się e-biznes jest bronią obusieczną — naraża firmy na niebezpieczeństwo kosztownych włamań. Coraz większego znaczenia nabierają więc takie aspekty, jak niezawodność, bezpieczeństwo i dostępność w posiadanej sieci.

PROBLEMY DOTYCZĄCE BEZPIECZEŃSTWA

Według najnowszych badań, bezpieczeństwo jest największym wyzwaniem dla małych i średnich przedsiębiorstw. Nieustannie zmieniające się zagrożenia, które czają się zarówno wewnątrz sieci firmowych, jak i poza nimi, mogą wywołać wiele szkód, zmniejszając rentowność i zadowolenie klientów. Ponadto, małe i średnie przedsiębiorstwa muszą działać zgodnie z nowymi przepisami i regulacjami, dotyczącymi ochrony danych osobowych i zabezpieczenia informacji elektronicznej.

Problem pierwszy — robaki i wirusy

Robaki i wirusy stanowią najpowszechniejsze zagrożenie: w ciągu ostatniego roku 75% małych i średnich przedsiębiorstw zostało zaatakowanych przez co najmniej jednego wirusa[1]. Robaki i wirusy mogą zaszkodzić ciągłości biznesowej oraz wynikom finansowym firm. Ataki stają się coraz bardziej inteligentne i sieją większe zniszczenia, co więcej, rozprzestrzeniają się coraz szybciej, infekując cały oddział w kilka chwil. Natomiast czyszczenie zaatakowanych komputerów zajmuje coraz więcej czasu. Utracone zamówienia, uszkodzone bazy danych oraz niezadowoleni klienci — to wszystko może prowadzić do katastrofy. Mimo iż firmy starają się instalować najnowsze poprawki systemowe i programy antywirusowe, nowe ataki mogą nastąpić w każdym chwili. Jednocześnie pracownicy nieświadomie otwierają destrukcyjne strony WWW, z których rozprzestrzeniają się wirusy i programy szpiegujące (*spyware*), pobierają pliki z niepewnych źródeł lub otwierają groźne załączniki do wiadomości e-mail. Działania te, inicjowane w sposób niezamierzony wewnątrz przedsiębiorstwa, również mogą wywołać poważne straty finansowe. Systemy zabezpieczające muszą wykrywać i usuwać robaki, wirusy oraz programy szpiegujące w całej sieci.

[1] Źródło: Maritz Research, 2005

Copyright © 1992–2005 Cisco Systems, Inc. Wszelkie prawa zastrzeżone. Ważne informacje oraz oświadczenia o poufności.

Problem drugi — kradzież informacji

Kradzież informacji stała się zorganizowaną działalnością. Hakerzy włamują się do sieci firmowych, aby zarabiać na kradzieży numerów kart kredytowych i innych informacji. Małe i średnie przedsiębiorstwa są tu szczególnie zagrożone, ponieważ złodzieje postrzegają je jako łatwiejszy cel niż wielkie korporacje. Ochrona strefy zdemilitaryzowanej to dobry początek, jednak wciąż za mało. Wiele informacji jest bowiem wykradanych przez zaufanych użytkowników wewnętrznych, na przykład pracowników lub wykonawców zleceń.

Przedsiębiorstwom zależy na zadowoleniu klienta i dobrej renomie, kradzież informacji może być dla nich bardzo kosztowna. Firmy, które nie zapewniają właściwej ochrony informacji, muszą liczyć się z negatywną reklamą, ustawowymi karami, a nawet sprawami sądowymi. Na przykład, zgodnie z nowymi prawami konsumenta w Kalifornii, w przypadku podejrzenia, że niepowołana osoba uzyskała dostęp do danych osobowych jakiegoś klienta, firma musi powiadomić o tym fakcie WSZYSTKICH klientów. Każda strategia bezpieczeństwa musi zapobiegać zarówno zewnętrznym, jak i wewnętrznym kradzieżom poufnych danych w postaci elektronicznej.

Problem trzeci — dostępność

Robaki i wirusy mogą radykalnie osłabić niezawodność zasobów sieciowych. W efekcie firma traci możliwość szybkiego reagowania na żądania klientów. Jednak nie tylko robaki i wirusy zagrażają dostępności. Internetowi terroryści, świadomi kluczowego znaczenia sieci w codziennym funkcjonowaniu przedsiębiorstw, szantażują firmy, grożąc zablokowaniem serwisów WWW i operacji handlu elektronicznego w przypadku niespełnienia ich żądań. Stosują oni ataki typu odmowa usługi (*denial of service — DoS*), polegające na kierowaniu dużych ilości ruchu do krytycznego składnika sieci, który przez to nie może obsłużyć właściwych danych bądź ulega awarii. Skutki są katastrofalne: utracone dane i zamówienia, żądania klienta pozostawione bez odpowiedzi. Jeżeli informacja o takim zdarzeniu przedostanie się do opinii publicznej, wiarygodność firmy zostaje zrujnowana. Rozgłos towarzyszący atakom typu odmowa usługi dotyczy przede wszystkim dużych banków i największych światowych korporacji, jednak zagrożone są również małe i średnie przedsiębiorstwa. Firmy te postrzega się bowiem jako gorzej przygotowane do odparcia ataków, niż wielkie korporacje.

Małe i średnie przedsiębiorstwa mogą się również spotkać z wieloma innymi, mniej poważnymi, lecz bardziej prawdopodobnymi zagrożeniami dostępności. Z każdym z nich wiąże się spadek rentowności i zadowolenia klienta. Przykładem może być włamanie do firmowych zasobów i wykorzystanie ich do nielegalnego rozpowszechniania muzyki, filmów i oprogramowania. Często firmy są nieświadome trwającego naruszenia bezpieczeństwa. Tymczasem komputery i sieć zbyt wolno obsługują klientów, a bezwiedne uczestnictwo w nielegalnym rozpowszechnianiu plików naraża przedsiębiorstwa na pozwy sądowe.

Problem czwarty — nieznane niebezpieczeństwo

Hakerzy wykorzystują do nieuczciwych celów każde nowe osiągnięcie technologii informatycznych i komunikacyjnych. Pojawienie się nowego sprzętu lub oprogramowania stwarza kolejne możliwości oszustwa. Sieci równorzędne i programy do natychmiastowego przesyłania wiadomości były jeszcze stosunkowo nowymi rozwiązaniami, gdy ich użytkownicy zostali zaatakowani destrukcyjnym kodem napisanym specjalnie pod kątem takich aplikacji. Obecnie celem wirusów stały się telefony komórkowe. Nikt nie wie, co będzie dalej — jednak najlepszą obronę stanowią rozwiązania, które można łatwo i bez wielkich kosztów dostosować do zabezpieczenia przed przyszłymi zagrożeniami.
Problem piąty — przepisy dotyczące bezpieczeństwa

Małe i średnie przedsiębiorstwa są zmuszone do zapewnienia poufności i spójności powierzonych im danych nie tylko ze względu na zagrożenia w postaci destrukcyjnego kodu. Obowiązek stosowania takich rozwiązań nakładają nowe ustawy i przepisy. W Unii Europejskiej oraz w wielu innych państwach obowiązujące prawo reguluje kwestie danych osobowych przekazanych instytucjom. W niektórych krajach wprowadzono także dodatkowe ustawy odnoszące się do szczególnych rodzajów danych, na przykład do informacji o stanie zdrowia. W Stanach Zjednoczonych obowiązuje ustawa HIPAA, która na wszystkie instytucje służby zdrowia, w tym również gabinety lekarskie, nakłada obowiązek zainstalowania systemów zabezpieczeń, w celu zapewnienia poufności kartotek i ochrony danych pacjentów przed dostępem nieupoważnionych osób. Firmy mają też obowiązek stosowania się do przepisów i ustaw obowiązujących w ich branży. Niestety, zasoby wielu mniejszych firm są niewystarczające do zapewnienia takiej zgodności z obowiązującymi przepisami. Tymczasem klienci chcą mieć pewność, że informacje powierzone tym firmom nie zostaną ujawnione

© 2005 Cisco Systems, Inc. Wszelkie prawa zastrzeżone.
Ważne informacje, oświadczenia o poufności oraz znaki towarowe Cisco Systems, Inc. znadują się w serwsie cisco.com.

Wszystkie firmy muszą zabezpieczać swoją infrastrukturę. Proste, przystępne i dostosowane do określonych potrzeb rozwiązania oczekiwane są zwłaszcza w małych i średnich przedsiębiorstwach. W Cisco opracowano rozwiązanie przeznaczone specjalnie dla tego segmentu rynku, uwzględniające zasady strategii Self-Defending Network — samodzielnie broniącej się sieci.

CISCO SELF-DEFENDING NETWORK

Cisco Self-Defending Network (samodzielnie broniąca się sieć) jest długoterminową strategią Cisco, której celem jest zabezpieczanie procesów biznesowych poprzez rozpoznawanie zagrożeń zewnętrznych i wewnętrznych, zapobieganie im oraz dostosowywanie się do ochrony przed nimi. Technologie Cisco Self-Defending Network pozwalają chronić firmy obecnie oraz dostosowywać się do przyszłych potrzeb. Dzięki Cisco przedsiębiorstwa chronią nie tylko sieci, lecz także związane z nimi inwestycje. Wynikiem są usprawnione procesy biznesowe oraz znaczne oszczędności.

Strategię Cisco Self-Defending Network można scharakteryzować trzema pojęciami: integracja, współpraca oraz dostosowanie. Przede wszystkim, zabezpieczenia są umieszczane we wszystkich elementach sieci, tak by każdy jej punkt mógł samodzielnie bronić się przed zagrożeniami zewnętrznymi i wewnętrznymi. Po drugie, wszystkie elementy sieci współpracują ze sobą i wymieniają informacje, co zapewnia dodatkową ochronę. Po trzecie, dzięki nowatorskim mechanizmom rozpoznawania zachowania użytkowników sieć dostosowuje się do ochrony przed nowymi zagrożeniami.

Cisco Secure Network Foundation jest prostym i niedrogim, lecz wszechstronnym rozwiązaniem zabezpieczającym dla małych i średnich przedsiębiorstw, umożliwiającym tworzenie niezawodnych, samodzielnie broniących się sieci.

SECURE NETWORK FOUNDATION — PRZEGLĄD

Strategia Cisco Secure Network Foundation pozwala małym i średnim przedsiębiorstwom skoncentrować się na rentowności, zamiast na sprawach sieci. Udostępnia spójne, bezpieczne usługi wszystkim użytkownikom korzystającym zarówno z połączeń przewodowych, jak i bezprzewodowych. Rutery, przełączniki oraz urządzenia zabezpieczające Cisco mają wbudowane zabezpieczenia, co pozwala usprawnić działalność firm i obniżyć koszty.

Cisco Secure Network Foundation skupia w sobie technologie Cisco Self-Defending Network, które chronią sieci obecnie i dostosowują się do przyszłych potrzeb w zakresie bezpieczeństwa. Zapewnia firmom ciągłość biznesową, nawet podczas ataku, oraz zgodność z oczekiwaniami klienta i wymaganiami prawa w zakresie ochrony poufności danych.

Obsługa klienta również podczas ataku

Gdy nadchodzą zagrożenia, firmy i klienci muszą mieć pewność właściwej ochrony przed zakłóceniami, kosztownymi awariami i uszkodzeniem danych. Sprawdzona strategia Cisco Self-Defending Network stanowi wszechstronne podejście do ochrony firm przed destrukcyjnymi działaniami robaków, wirusów, terrorystów internetowych oraz przed innymi atakami.

Wirusy, robaki oraz programy szpiegujące zazwyczaj dostają się do sieci firm przez wiadomości e-mail, aplikacje do natychmiastowego przesyłania wiadomości oraz pliki kopiowane lub pobierane z Internetu. Najbardziej zaawansowane ataki odbywają się za pośrednictwem usług mobilnych lub usług systemów operacyjnych. Oferowane przez Cisco najlepsze w branży systemy zapobiegania włamaniom (Intrusion Prevention Systems, IPS) przeglądają i analizują w czasie rzeczywistym cały ruch przychodzący, poszukując znanych nieprawidłowości zapowiadających atak. W przypadku wykrycia anomalii, urządzenie zabezpieczające Cisco ocenia stopień zagrożenia i przekazuje tę informację do innych części sieci. W ten sposób atak może zostać natychmiast powstrzymany u źródła, zanim rozprzestrzeni się w całej sieci. Ale robaki, wirusy oraz programy szpiegujące to nie jedyne zagrożenia dla firm. Tych samych mechanizmów przeglądania i analizy ruchu urządzenia zabezpieczające Cisco używają również do wykrywania i powstrzymywania ataków typu odmowa usługi, a także innych zagrożeń, którym nie nadano jeszcze nazwy.

Wyposażenie firmy w urządzenia zabezpieczające powstrzymuje znane i nieznane ataki w czasie rzeczywistym. Dzięki komunikacji między elementami sieci rozwiązania te dostosowują się do zmiennych warunków bezpieczeństwa. Dzięki takim warstwowym zabezpieczeniom małe i średnie przedsiębiorstwa mogą utrzymać ciągłość biznesową i obsługiwać klientów nawet podczas ataku.

© 2005 Cisco Systems, Inc. Wszelkie prawa zastrzeżone.
Ważne informacje, oświadczenia o poufności oraz znaki towarowe Cisco Systems, Inc. znadują się w serwsie cisco.com.

Obsługa poufnych danych klienta

Rozwiązanie Cisco Secure Network Foundation zawiera wiele narzędzi, które zapobiegają nieautoryzowanemu dostępowi do danych klienta, bez względu na to, czy następuje on wewnątrz firmy czy spoza niej. Dzięki usługom wirtualnej sieci prywatnej (VPN) małe oddziały i pracownicy będący w podróży mogą komunikować się między sobą oraz z centralą, zachowując całkowitą poufność, nawet gdy do transportu danych jest wykorzystywany publicznie dostępny Internet. Dzięki zastosowaniu wymagających standardów uwierzytelniania użytkowników, dostęp do sieci VPN mają tylko upoważnione do tego osoby. Natomiast dzięki technologii silnego szyfrowania dane przesyłane łączem VPN będą całkowicie niezrozumiałe, gdyby doszło do ich przechwycenia podczas transportu publicznymi łączami.

Zapora oraz systemy zapobiegania włamaniom w każdym punkcie wejścia do sieci pozwalają powstrzymać robaki, programy szpiegujące oraz próby kradzieży firmowych informacji. Zapory służą również do ochrony danych poufnych przed użytkownikami wewnętrznymi. Na przykład reguły zapory mogą uniemożliwiać nieautoryzowanym pracownikom dostęp do komputerów i ruchu sieciowego w dziale finansów, dziale kadr lub w księgowości. Wirtualne sieci lokalne (VLAN) pozwalają na jeszcze większą segmentację komunikacji w firmie. Poufne informacje finansowe lub dane osobowe można umieścić w odrębnej sieci VLAN, do której pracownicy nie mają dostępu.

Rozwiązanie Cisco Secure Network Foundation pozwala także firmom spełnić wymagania prawne związane z bezpieczeństwem i poufnością danych klienta, chroniąc sieć przed naruszeniem bezpieczeństwa oraz nieautoryzowanym dostępem z wnętrza sieci i spoza niej.

Obniżenie kosztów

Rozwiązanie Cisco Secure Network Foundation ułatwia małym i średnim przedsiębiorstwom kontrolowanie kosztów na dwa sposoby. Po pierwsze, pozwala uniknąć zbędnych kosztów związanych z naruszaniem bezpieczeństwa, a po drugie, jest wielofunkcyjnym, niedrogim rozwiązaniem, które można dostosowywać do zmiennych potrzeb firmy. Zintegrowane zabezpieczenia upraszczają zarządzanie siecią, zmniejszają koszty utrzymania oraz całkowity koszt posiadania sieci.

Z naruszeniem bezpieczeństwa sieci wiążą się koszty bezpośrednie oraz koszty ukryte. Wiele incydentów, takich jak stosunkowo niegroźne wirusy, wywołuje niewielkie szkody. W takich przypadkach koszty bezpośrednie obejmują czas i zasoby konieczne do wyczyszczenia zainfekowanych systemów. Koszt rośnie wraz z liczbą zaatakowanych komputerów, zatem ochrona i szybkie wykrywanie przyczyniają się do oszczędności. Mniej oczywisty koszt wiąże się z czasem pracy straconym w trakcie czyszczenia komputerów. Inne przykłady kosztów ukrytych obejmują: utracone możliwości biznesowe, utraconych klientów, pogorszenie reputacji oraz koszty prawne związane z naruszeniem bezpieczeństwa. Koszty te występują rzadziej, mogą jednak osiągać znaczny poziom. W ubiegłym roku przestępstwa internetowe kosztowały brytyjską gospodarkę 2,4 mld GBP[2] . Rozwiązanie Cisco Secure Network Foundation pozwala firmom uniknąć obu rodzajów kosztów, obniżyć ryzyko prowadzenia działalności oraz zwiększyć wiarygodność i zaufanie klienta.

W małych i średnich przedsiębiorstwach często brakuje personelu oraz środków na wdrożenie i utrzymywanie złożonych rozwiązań zabezpieczających. Rozwiązanie Cisco Secure Network Foundation jest narzędziem pewnym, niezawodnym i jednocześnie prostym. Pozwala firmom obniżyć całkowity koszt posiadania sieci i skoncentrować się na prowadzeniu działalności, zamiast na sprawach sieci. Co więcej, rozwiązanie to można łatwo dostosowywać do zmiennych potrzeb i warunków bezpieczeństwa, dzięki czemu poziom kosztów odpowiada rozwojowi firmy.

[2] Źródło: National Hi-Tech Crime Unit (brytyjski krajowy zespół ds. zwalczania przestępstw komputerowych)

© 2005 Cisco Systems, Inc. Wszelkie prawa zastrzeżone.
Ważne informacje, oświadczenia o poufności oraz znaki towarowe Cisco Systems, Inc. znadują się w serwsie cisco.com.

Schamat rozwiązań Cisco Secure Network Foundation

Cisco Secure Network Foundation jest składa się z dwóch głównych grup produktów: routerów z rodziny Cisco ISR oraz urządzeń zabezpieczających z serii Cisco ASA 5500 Adaptive Security Appliance (ASA). Stanowią one podstawowe elementy do budowy samodzielnie broniącej się sieci Cisco dla małych i średnich przedsiębiorstw.

Routery Cisco ISR oferują wiele funkcji w ramach jednej, niezawodnej i niedrogiej platformy, doskonale nadającej się dla jednoosobowego biura bądź małej lub średniej firmy. Cisco ISR jest routerem szerokopasmowego dostępu DSL z wbudowanym nadmiarowym łączem, przełącznikiem sieci LAN, punktem dostępu bezprzewodowego oraz przełącznikiem bezprzewodowej sieci LAN — wszystko to w jednym urządzeniu. Wymienione funkcje można dodawać do routerów Cisco ISR w zależności od potrzeb, co pozwala na łatwe dostosowywanie tych urządzeń do zmiennych wymagań małych i średnich przedsiębiorstw. Routery ISR zawierają również wiele podstawowych zabezpieczeń, między innymi zaporę, systemy zapobiegania włamaniom oraz funkcje VPN.

Seria Cisco ASA 5500 obejmuje wydajne, zintegrowane urządzenia zabezpieczające, oparte na sprawdzonej technologii zabezpieczeń Cisco, które reagują na znane i nieznane zagrożenia oraz potrafią się dostosowywać do obrony przed nimi. Urządzenia z serii Cisco ASA 5500 stanowią połączenie najlepszej w swojej klasie zapory, systemu zapobiegania włamaniom, sieciowego rozwiązania antywirusowego, funkcji analizy aplikacji oraz usług dostępu zdalnego i łączy VPN między lokalizacjami. Cisco ASA 5500 zapewnia najwyższy poziom ochrony przed nieautoryzowanym dostępem, robakami, wirusami, programami szpiegującymi oraz niebezpiecznymi lub destrukcyjnymi aplikacjami. W jednym urządzeniu, zaprojektowanym specjalnie pod kątem sieci w małych i średnich przedsiębiorstwach, zintegrowano sprawdzone technologie zabezpieczeń. Rozwiązanie to jest opłacalne, łatwe do wdrożenia, zarządzania, utrzymania i rozbudowy. W przypadku nowych zagrożeń sieciowych, można dostosować Cisco ASA do bieżących potrzeb za pomocą instalowanych przez użytkownika rozszerzeń i uaktualnień. Seria urządzeń Cisco ASA 5500 to idealny wybór dla centrali firmy lub oddziału wymagającego wszechstronnej ochrony.

Opcjonalnym komponentem rozwiązania Cisco Secure Network Foundation są przełączniki z serii Cisco Catalyst® Express 500. Jest to rodzina prostych, inteligentnych przełączników, przeznaczonych dla małych i średnim przedsiębiorstw. Wszystkie przełączniki Cisco Catalyst są wyposażone w funkcje zabezpieczeń, które wykrywają nieprawidłowości w ruchu sieciowym i nie dopuszczają do ich rozprzestrzenienia na inne punkty sieci lub do zablokowania przełącznika. Przełącznik Cisco Catalyst Express 500 został zoptymalizowany pod kątem transmisji danych i głosu oraz zastosowań bezprzewodowych. Oferuje niezawodność i bezpieczeństwo charakterystyczne dla całej rodziny przełączników Catalyst, a przy tym ma łatwą w obsłudze obudowę, dzięki czemu montaż urządzenia zajmuje zaledwie kilka minut. Do każdego przełącznika Cisco Catalyst Express 500 dołączane jest oprogramowanie Cisco Network Assistant, które rozpoznaje pozostałe składniki sieci i ułatwia skonfigurowanie urządzenia. Kolejny opcjonalny moduł to Cisco Aironet® Access Points — urządzenie zapewniające bezpieczny dostęp bezprzewodowy do sieci LAN w małych i średnich biurach. Produkty Cisco do komunikacji bezprzewodowej charakteryzują się takim samym poziomem bezpieczeństwa, skalowalności i łatwości zarządzania, jaki znany jest z przewodowych sieci LAN. W przypadku zastosowania urządzenia klienckiego firmy Cisco lub zgodnego, Cisco Aironet Access Points zapewnia szybki i bezpieczny roaming, umożliwiając autoryzowanym użytkownikom przełączanie się między poszczególnymi punktami dostępowymi.

Łącząc wszystko razem

Dla długoterminowego powodzenia rozwiązania sieciowego bardzo ważne są doskonałe, wszechstronne usługi. Usługa Cisco SMB Support Assistant została zaprojektowana w celu zaspokojenia potrzeb małych i średnich przedsiębiorstw. Jest to łatwy w użyciu i niedrogi program do obsługi sieci, który pozwala rozwiązać najczęstsze problemy małych i średnich przedsiębiorstw oraz zapewnia dostępność i bezpieczeństwo firmowych sieci. Przedsiębiorstwa mogą korzystać z aktualnych diagnoz i wskazówek dotyczących rozwiązywania problemów, a także z przeprowadzanej z wyprzedzeniem wymiany części. Kluczowym modułem programu jest portal Cisco SMB Support Assistant Portal — bezpieczny zestaw narzędzi dostępnych w trybie online, który umożliwia klientom odtwarzanie haseł, korzystanie z dokumentacji technicznej, badanie stanu systemu, pobieranie poprawek do oprogramowania oraz zapoznanie się z opisami przykładowych czynności serwisowych.

© 2005 Cisco Systems, Inc. Wszelkie prawa zastrzeżone.
Ważne informacje, oświadczenia o poufności oraz znaki towarowe Cisco Systems, Inc. znadują się w serwsie cisco.com.

DLACZEGO CISCO?

Rozwiązanie Cisco Secure Network Foundation dla małych i średnich przedsiębiorstw zapewnia ciągłość biznesową, poufność danych klienta oraz kontrolę kosztów związanych z utrzymaniem dostępnej, bezpiecznej i samodzielnie broniącej się sieci. Wymienione zalety przekładają się na wzrost zaufania klientów, utrzymanie lub wzrost wydajności pracowników, zapewnienie zgodności z przepisami oraz obniżenie całkowitego kosztu posiadania sieci.

Cisco Secure Network Foundation jest jednym z serii inteligentnych rozwiązań Cisco dla małych i średnich przedsiębiorstw (Cisco SMB Class). Rozwiązania te zaprojektowano w taki sposób, by firmy z tego sektora mogły zwiększyć wydajność pracy, zapewnić obsługę nowatorskich usług, podnieść poziom zadowolenia klienta i obniżyć koszty operacyjne. Dzięki zwiększonej funkcjonalności w zakresie transmisji głosowej, bezpieczeństwa, mobilności oraz ochrony inwestycji, rozwiązania Cisco dla małych i średnich przedsiębiorstw spełniają zarówno dzisiejsze, jak i przyszłe potrzeby firm.

Firmie Cisco Systems i jej partnerom handlowym zależy na jak najlepszych relacjach z klientami z sektora małych i średnich przedsiębiorstw. Dzięki oferowanym opcjom finansowania, wyróżnianej obsłudze technicznej oraz spersonalizowanym szkoleniom, firmy te mogą czerpać pełnię korzyści z rozwiązań Cisco dla małych i średnich przedsiębiorstw.

Cisco jest czołowym producentem routerów, przełączników i systemów zabezpieczeń. Oferuje elastyczne rozwiązania, które spełniają dzisiejsze i przyszłe potrzeby oraz umożliwiają firmom rozwój i prężne działanie. Strategia bezpieczeństwa Cisco opiera się na koncepcji samodzielnie broniącej się sieci — Self-Defending Network — w której każdy punkt infrastruktury zawiera wbudowane zabezpieczenia, współpracuje z innymi elementami sieci w celu zapewnienia dodatkowej ochrony oraz dostosowuje się do zmiennych warunków i nowych zagrożeń.

NASTĘPNE KROKI

Więcej informacji na temat rozwiązania Cisco Secure Network Foundation można uzyskać od Partnera Cisco lub w Internecie, pod adresem **http://www.cisco.com/go/smbclass**.
Listę partnerów handlowych Cisco można znaleźć pod adresem **http://www.cisco.com/go/partnerlocator**.

Centrala Cisco Systems
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
Tel: 800 553-NETS (6387)
Fax: 408 526-4100

Centrala na Europę
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Centrala na Amerykę Północną, Południową i Środkową
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Centrala na region Dalekiego Wschodu
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems ma ponad 200 biur w następujących krajach i regionach. Adresy, numery telefonów i numery faksów są dostępne na:
stronie internetowej Cisco.com pod adresem www.cisco.com/go/offices.

Arabia Saudyjska · Argentyna · Australia · Austria · Belgia · Brazylia · Bułgaria · Chile · Chińska Republika Ludowa · Chorwacja · Czechy Dania · Dubaj, Zjednoczone Emiraty Arabskie · Filipiny · Finlandia · Francja · Grecja · Hiszpania · Holandia · Hongkong · Indie · Indonezja Irlandia · Izrael · Japonia · Kanada · Kolumbia · Korea · Kostaryka · Luksemburg · Malezja · Meksyk · Niemcy · Norwegia · Nowa Zelandia Peru · Polska · Portoryko · Portugalia · Republika Południowej Afryki · Rosja · Rumunia · Singapur · Słowacja · Słowenia · Stany Zjednoczone Szkocja · Szwajcaria · Szwecja · Tajlandia · Tajwan · Turcja · Ukraina · Wenezuela · Węgry · Wielka Brytania · Wietnam · Włochy · Zimbabwe

© 2005 Cisco Systems Inc. Wszelkie prawa zastrzeżone. CCIP, CCSP, logo Cisco Arrow, znak Cisco Powered Network, Cisco Unity, Follow Me Browsing, FormShare oraz StackWise są zastrzeżonymi znakami towarowymi Cisco Systems Inc.; Changing the Way We Work, Live, Play, and Learn oraz iQuick Study są znakami usług Cisco Systems Inc.; Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, logo Cisco Certified Internetwork Expert, Cisco IOS, logo Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, logo Cisco Systems, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, logo iQ, iQ Net Readiness Scorecard, LightStream, MGX, MICA, logo Networkers, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath i VCO są zastrzeżonymi znakami towarowymi Cisco Systems Inc. i/lub jego spółek zależnych w Stanach Zjednoczonych oraz niektórych innych krajach.

Wszelkie inne znaki towarowe wymienione w tym dokumencie lub na tej stronie są własnością odpowiednich podmiotów. Użycie słowa „partner" nie oznacza związku partnerskiego między Cisco a inną firmą. (0502R)