Bezpieczeństwo w Twoim Urzędzie — rozwiązanie Cisco Integrated Security dla Jednostek Samorządu Terytorialnego.

W miarę jak administracje publiczne na całym świecie w coraz większym stopniu wykorzystują sieci do świadczenia obywatelom usług na coraz wyższym poziomie oraz zwiększania bezpieczeństwa publicznego, krytycznego znaczenia nabiera bezpieczeństwo sieciowe. Samorządowe zespoły informatyczne muszą opracowywać wielowarstwowe strategie zapobiegania epidemiom wirusów i robaków internetowych, ochrony przed atakami typu DDoS (distributed denial of service — rozproszone blokowanie dostępu do usług internetowych) oraz zapobiegania kradzieży informacji poufnej czy danych personalnych.

ROZWIĄZANIA ZABEZPIECZAJĄCE FIRMY CISCO POZWALAJĄ SAMORZĄDOWYM ZESPOŁOM INFORMATYCZNYM ZAPEWNIĆ CIĄGŁĄ KOMUNIKACJĘ, KONIECZNĄ DO ŚWIADCZENIA USŁUG I UTRZYMANIA BEZPIECZEŃSTWA PUBLICZNEGO

Cisco Systems

Wprowadzenie

Technologie sieciowe, takie jak Cisco IP Communications czy rozwiązania bezprzewodowe Cisco, umożliwiają samorządom podniesienie poziomu świadczonych usług, poprzez modyfikację procesów biznesowych bez zwiększania kosztów operacyjnych. Usługi świadczone przez samorządy wymagają nieprzerwanej komunikacji. Dlatego samorządowe zespoły informatyczne muszą zabezpieczyć swoje sieci przed takimi zagrożeniami, jak epidemie wirusów i robaków czy ataki typu DDoS, które mogłyby zakłócić realizację tych usług. Władze samorządowe muszą również zapobiegać kradzieżom informacji, kontrolując dostęp do danych poufnych, takich jak zapisy dotyczące podatku od nieruchomości, dane osobowe mieszkańców i inne.

Bezpieczeństwo sieciowe ma podstawowe znaczenie dla osiągnięcia przez władze samorządowe najważniejszych celów, omówionych poniżej.

- *Zwiększenie efektywności usług*. Samorządy na całym świecie wykorzystują swoje sieci do świadczenia usług, takich jak scentralizowane centra kontaktowe, bezprzewodowy dostęp do informacji dla pracowników opieki społecznej i innych pracowników mobilnych, czy wypełnianie przez Internet formularzy wniosków o przyznanie pozwolenia na budowę lub licencji. Utrzymanie dostępności tych usług wymaga zapewnienia ich bezpieczeństwa.
- *Poprawa bezpieczeństwa mieszkańców.* Bezpieczeństwo rozpatruje się w dwóch aspektach: ochrony życia i własności oraz ochrony poufności informacji. Technologie zabezpieczające są warunkiem koniecznym osiągnięcia obu tych celów. W celu zwiększenia bezpieczeństwa obywateli władze samorządowe mogą wykorzystać rozwiązanie Cisco IP Communications, które umożliwia błyskawiczne przesyłanie głosu, obrazu wideo i danych o znaczeniu krytycznym do organów bezpieczeństwa publicznego za pośrednictwem telefonów IP firmy Cisco lub urządzeń bezprzewodowych. Dzięki ochronie sieci przed infekcją, atakiem lub włamaniem zwiększa się dostępność tych usług. Z kolei takie mechanizmy jak szyfrowanie poufnych danych w celu ich przesłania wirtualną siecią prywatną (VPN), pozwalają ochronić mieszkańców przed naruszeniem ich prywatności czy kradzieżą tożsamości.
- *Rozwój gospodarczy*. Samorząd, który w efektywny sposób realizuje usługi i chroni bezpieczeństwo obywateli, jest w stanie skuteczniej przyciągać nowych mieszkańców, przedsiębiorców i turystów. Efektywność i bezpieczeństwo usług zależą od dostępności i prywatności sieci.
- *Zgodność z przepisami.* Bezpieczeństwo jest również wymagane na mocy coraz większej liczby przepisów, takich jak raport Turnbull'a dotyczący kontroli wewnętrznej (Turnbull Report on Internal Control), odnoszący się do instytucji publicznych w Wielkiej Brytanii, czy Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r., która określa minimalne standardy bezpieczeństwa danych i aplikacji. W lipcu 2002 r. w państwach członkowskich UE zaczęła obowiązywać dyrektywa o prywatności i łączności elektronicznej (2002/58/EC), będąca częścią ram regulacyjnych w dziedzinie łączności elektronicznej (eCommunications Regulatory Framework). Ta dyrektywa o „e-prywatności" chroni podstawowe prawa i wolności osób fizycznych w zakresie automatycznego przechowywania i przetwarzania ich danych oraz nakłada ścisłe ograniczenia na wykorzystywanie spamu.

Mimo dostępności skutecznych rozwiązań zabezpieczających, wiele samorządów nadal nie zapewnia wystarczającej ochrony swoich infrastruktur sieciowych i danych poufnych. Przyczyną jest fakt, iż do niedawna wirusy były zaledwie niedogodnościami, ledwo zauważanymi przez urzędników samorządowych. Dzisiaj kombinacja samorozprzestrzeniających się zagrożeń, aplikacji wspomagających współpracę i wzajemnie połączonych środowisk sprawiła, że bezpieczeństwo — lub jego brak — stało się tematem nagłówków prasowych. Na przykład w styczniu 2003 r. robak SQL Slammer unieruchomił wiele sieci samorządowych i komercyjnych na całym świecie. W czerwcu 2005 r. władze Wielkiej Brytanii ostrzegły samorządy i przedsiębiorstwa sektora prywatnego przed szeroko rozpowszechnionym koniem trojańskim, wykorzystującym pocztę elektroniczną w celu kradzieży informacji.

Niniejszy artykuł przeglądowy jest przeznaczony dla samorządowych zespołów informatycznych obawiających się o bezpieczeństwo swoich sieci IP. W pierwszym rozdziale opisano strategię Cisco Self-Defending Network (samodzielnie broniących się sieci) oraz sposób, w jaki pozwala ona wyeliminować różne luki w zabezpieczeniach sieci samorządowych. Kolejny rozdział zawiera analizy przypadków. Artykuł kończy się omówieniem unikatowych kwalifikacji firmy Cisco Systems® jako dostawcy rozwiązań do zabezpieczania sieci dla samorządów.

STRATEGIA CISCO SELF-DEFENDING NETWORK DLA ADMINISTRACJI PUBLICZNEJ

Self-Defending Network (samodzielnie broniąca się sieć) to długoterminowa strategia firmy Cisco, której celem jest zabezpieczenie procesów biznesowych organizacji poprzez rozpoznawanie zagrożeń zewnętrznych i wewnętrznych, zapobieganie im oraz dostosowywanie się do ochrony przed nimi. Dzięki takiej ochronie organizacje są w stanie lepiej wykorzystać funkcje inteligentnej analizy zawarte w ich zasobach sieciowych, a tym samym usprawnić procesy biznesowe i obniżyć koszty.

Samodzielnie broniąca się sieć jest oparta na trzech zasadach: integracji zabezpieczeń we wszystkich elementach sieci, wzajemnej współpracy między różnymi systemami zabezpieczeń i elementami sieci oraz adaptacji sieci do nowych zagrożeń. Zdolność adaptacji jest osiągana dzięki zastosowaniu technologii rozpoznawania anomali zachowania, rozróżniania danych z poszczególnych aplikacji oraz kontroli sieci:

- *Zasada integracji.* Każdy element sieci pełni funkcję obronną. Przełączniki, rutery, urządzenia sieciowe i punkty końcowe zawierają wbudowane zabezpieczenia, takie jak zapory, funkcje obsługi sieci VPN czy mechanizmy kontroli zaufania i tożsamości. Integracja odnosi się również do technologii, takich jak Control Plane Policing czy progi wykorzystania procesora i pamięci, które zapewniają bezpieczne działanie tych urządzeń sieciowych.
- *Zasada współpracy.* Różne składniki sieci współpracują ze sobą, tworząc nowe sposoby ochrony. Bezpieczeństwo staje się systemem opartym na współpracy między punktami końcowymi, elementami sieciowymi i mechanizmami egzekwującymi przestrzeganie reguł. Przykładem zasady współpracy jest mechanizm NAC (Network Admission Control). Punkty końcowe uzyskują dostęp do sieci pod warunkiem, że przestrzegają reguł bezpieczeństwa, co kontrolują urządzenia sieciowe takie jak rutery i przełączniki.
- *Zasada adaptacji*. Sieć automatycznie powstrzymuje nowe rodzaje zagrożeń, gdy tylko się pojawią, poprzez identyfikowanie nienormalnego zachowania sieci lub aplikacji oraz stosowanie mechanizmów kontroli sieciowej. Usługi zabezpieczeń i mechanizmy analizy ruchu sieciowego mają wzajemnie „świadomość" swojego istnienia. Pozwala to zwiększyć skuteczność zabezpieczeń, z większym wyprzedzeniem reagować na nowe rodzaje zagrożeń oraz zmniejszyć ryzyko poprzez powstrzymywanie zagrożeń w wielu warstwach sieciowych naraz.

Dzięki połączeniu tych trzech zasad sieci samorządowe zyskują właściwości niezbędne do skutecznego świadczenia usług i zapewnienia bezpieczeństwa publicznego, tj.: dostępność, powszechny dostęp do usług, kontrola dostępu, inteligentna analiza aplikacji, ochrona przed atakami typu „day zero" i powstrzymywanie infekcji.

Dostępność sieci

Podatność na zagrożenia

Sieci samorządowe są podatne na różnego rodzaju ataki, które zagrażają dostępności i ciągłości świadczonych usług:

- Ukierunkowane ataki tzw. botnet'ów, będące nowym wynalazkiem, bywają wykorzystywane do wymuszeń, których ofiarami padają również instytucje administracji publicznej. Stanowią one odmianę ataków DDoS, które przeciążają łącze WAN organizacji, aby uniemożliwić uprawnionym użytkownikom korzystanie z serwisów internetowych i innych zasobów sieciowych.
- Wewnętrzne ataki blokujące sieć (ang.flooding) są częstym skutkiem rozprzestrzenienia się robaków i wirusów. Przeciążają one procesor urządzenia sieciowego i wewnętrzną przepustowość łączy oraz mogą spowolnić lub zatrzymać przetwarzanie zasobów na serwerze.

Rozwiązania zwiększające dostępność

Firma Cisco Systems oferuje następujące rozwiązania chroniące dostępność sieci samorządowych. Ich połączenie pozwala na utworzenie samodzielnie broniącej się sieci.

- *Cisco Guard*. Rozwiązanie Cisco Guard stale monitoruje ruch sieciowy, wykrywając pakiety związane z atakami DDoS. Przepuszcza ruch uprawniony, blokuje ruch destrukcyjny oraz chroni zasoby przed awarią. Samorządy mogą wdrożyć rozwiązanie Cisco Guard na miejscu lub korzystać z niego w ramach usługi zarządzanej, oferowanej przez usługodawcę. Jeśli rozwiązanie Cisco Guard jest wdrożone u usługodawcy, chroni ono zewnętrzne łącza WAN, a także łącza do użytkowników i zasoby.
- *Cisco NetFlow*. Funkcja Cisco NetFlow, wbudowana w rutery i przełączniki Cisco, zapewnia inteligentną analizę aplikacji i widoczność wymaganą do ochrony przed atakami typu „day zero". Samorządowe zespoły informatyczne mogą włączyć tę funkcję, aby otrzymywać wczesne ostrzeżenia przed rozpoczynającymi się przypadkami floodingu.
- *Cisco Intrusion Prevention System (IPS)*. System Cisco IPS rozpoznaje i eliminuje szkodliwe pakiety, które mogą powodować odmowę usługi na systemach docelowych. Wdrażając rozwiązanie Cisco IPS w wielu miejscach sieci, samorządy mogą rozpoznawać ataki jak najbliżej miejsca penetracji, ograniczając ich wpływ na dostępność.
- *Control Plane Policing*. Udostępniana przez rutery Cisco funkcja Control Plane Policing chroni dostęp do ścieżki przesyłania ruchu sterującego, korzystając z reguł dotyczących akceptowalnych typów ruchu sieciowego; reguły te są oparte na takich czynnikach jak nadawca, odbiorca, protokół i inne.
- *Quality of Service (QoS)*. Dzięki zawartym w ruterach i przełącznikach Cisco funkcjom QoS punkty końcowe mogą uniemożliwić generowanie nieakceptowanego natężenia ruchu sieciowego. Mechanizmy QoS pozwalają również zagwarantować, że płaszczyzna komunikacyjna dowodzenia i sterowania (ang. command-and-control communication plane) stale monitoruje sieć i wprowadza do niej dynamiczne zmiany podczas ataku.
- *Cisco Security Agent*. Cisco Security Agent chroni punkty końcowe przed różnorodnymi atakami, w tym polegającymi na przeciążeniu pamięci, interfejsów wejścia-wyjścia i procesora serwera.
- *Cisco Lifecycle Services*. W ramach usług Cisco Lifecycle Services, firma Cisco Systems i jej partnerzy przeprowadzają analizę bezpieczeństwa sieci w celu ustalenia jej bieżącej wydajności oraz kwalifikacji personelu. Eksperci ds. bezpieczeństwa sieciowego z firmy Cisco analizują również sieci i systemy będące przedmiotem ataków, aby określić skuteczność aktualnych zabezpieczeń, zakres luk w zabezpieczeniach na poziomie sieci oraz zdolność organizacji do wykrycia ataku i zareagowania na niego. Klienci z sektora samorządowego otrzymują szczegółowy raport z wykazem luk w zabezpieczeniach sieci oraz zalecanymi działaniami korekcyjnymi, pozwalającymi zmniejszyć ryzyko.

- *Procedury Bezpieczeństwa*. Przestrzeganie stosownych procedur przy konfiguracji pozwala zabezpieczyć rutery i przełączniki przed unieruchomieniem wskutek ataków.

Powszechny dostęp

Podatność na zagrożenia

Metody kontroli dostępu do sieci są często arbitralne. Na przykład, wiele samorządów umożliwia lokalnym użytkownikom korzystającym z połączeń przewodowych nieograniczony dostęp do sieci bez uwierzytelniania użytkownika czy urządzenia, podczas gdy lokalni użytkownicy łączący się bezprzewodowo muszą się uwierzytelnić, a użytkownicy zdalni mogą nawiązać połączenie tylko za pośrednictwem protokołów IPSec lub SSL, często bez dostępu do niektórych aplikacji. Podobnie w wielu organach administracji pracownicy znajdujący się w zdalnych biurach mogą nawiązać połączenie bez uwierzytelnienia, gdy korzystają z innych serwisów w urzędzie. Dostęp nieupoważnionych pracowników do niektórych aplikacji naraża samorząd na ryzyko naruszenia przepisów związanych z bezpieczeństwem oraz prywatności obywateli. Z drugiej strony, jeśli nieelastyczne reguły dostępu uniemożliwiają pracownikom samorządowym korzystanie z aplikacji wtedy, kiedy jest to potrzebne, może to prowadzić do spadku skuteczności.

Rozwiązania Cisco zapewniające powszechny dostęp

Rozwiązania Cisco Self-Defending Network umożliwiają samorządowym zespołom informatycznym bezpieczne udostępnienie dowolnej aplikacji dowolnemu użytkownikowi przy użyciu dowolnej metody dostępu. Stosowane są jednolite zasady uwierzytelniania i autoryzacji, bez względu na metodę dostępu. Informacje poufne są chronione nawet przy dostępie z niezaufanych obszarów lub zasobów wysokiego ryzyka. Do rozwiązań firmy Cisco zapewniających bezpieczny, powszechny dostęp należą:

- *Funkcja Cisco Secure Desktop.* Koncentratory Cisco VPN 3000 pozwalają utworzyć „wirtualny pulpit" na zasobach i w obszarach wysokiego ryzyka. Po zakończeniu sesji SSL (Secure Sockets Layer) użytkownika funkcja ta usuwa wirtualny pulpit oraz wszelkie ślady poufnych danych, w tym pliki cookie, historię przeglądarki i foldery tymczasowe.

- *Szyfrowanie*. Produkty Cisco pozwalają szyfrować każdy rodzaj ruchu, w tym komunikację między biurami, sesje zdalnego dostępu i połączenia bezprzewodowe. W dużych organizacjach samorządowych technologia dynamicznych, wielopunktowych sieci VPN (DMVPN) umożliwia szyfrowanie dużych ilości ruchu bez nieakceptowanych opóźnień.

- *Uwierzytelnianie i autoryzacja dla wszystkich metod dostępu*. Cisco Secure Access Control Server (ACS) tworzy scentralizowaną infrastrukturę sieciową do obsługi tożsamości dla wszystkich urządzeń firmy Cisco i aplikacji do zarządzania bezpieczeństwem, co upraszcza administrowanie. Łącząc uwierzytelnianie, dostęp użytkowników i administratorów oraz kontrolę przestrzegania reguł, serwer Cisco Secure ACS ułatwia zapewnienie dostępu do sieci mobilnym pracownikom i telepracownikom samorządowym, zwiększa bezpieczeństwo i ogranicza obciążenie informatyków pracą.

Kontrola dostępu

Podatność na zagrożenia

W większości sieci uwierzytelnianie dotyczy czasem urządzenia, a czasem użytkownika. Co więcej, zazwyczaj jest ono realizowane tylko w niektórych przypadkach, takich jak dostęp zdalny czy bezprzewodowy. Na przykład częstą sytuacją jest uwierzytelnianie użytkowników korzystających z dostępu zdalnego i sieci WLAN, przy jednoczesnym braku uwierzytelniania użytkowników sieci lokalnej oraz zdalnych użytkowników sieci WAN. Taka sytuacja stwarza możliwość naruszeń prywatności i niezgodności z przepisami, gdyż pracownicy mogliby skorzystać z sieci LAN czy WAN w celu uzyskania dostępu do danych i aplikacji, do których nie mają upoważnienia.

Kolejną słabością tradycyjnych koncepcji kontroli dostępu jest brak prewencyjnej oceny stanu bezpieczeństwa punktów końcowych, w tym bieżących wersji systemów operacyjnych, programów korygujących, oprogramowania antywirusowego i innych zabezpieczeń. Zasób o słabym poziomie zabezpieczeń może zainfekować inne zasoby sieciowe i zakłócić świadczenie usług samorządowych.

Rozwiązania firmy Cisco zapewniające kontrolę dostępu

Rozwiązania Cisco Self-Defending Network do kontroli dostępu zapewniają uwierzytelnianie użytkowników, uwierzytelnianie urządzeń oraz ocenę stanu bezpieczeństwa przy użyciu następujących technologii:

- *Wiele technologii uwierzytelniania.* Rozwiązania Cisco udostępniają różne technologie uwierzytelniania dla każdego typu punktu końcowego czy metody połączenia: dostęp przewodowy przez porty warstwy 2., dostęp bezprzewodowy, połączenia między biurami oraz połączenia dostępu zdalnego. Do udostępnianych technologii należą:
  - Uwierzytelnianie IKE (Internet Key Exchange) na potrzeby dostępu zdalnego za pomocą sieci VPN opartej na protokole IPSec.
  - Protokół EAP (Extensible Authentication Protocol) i uwierzytelnianie 802.1x na potrzeby dostępu bezprzewodowego.
  - Przekrojowe usługi uwierzytelniania na potrzeby dostępu przez zapory i łącza WAN.
- *Cisco Access Control Server.* Serwer Cisco ACS sprawdza, czy żądania dostępu wysyłane przez użytkowników są zgodne z regułami administracyjnymi, korzystając przy tym z usług uwierzytelniania, autoryzacji i rozliczeń (Authentication, Authorisation and Accounting — AAA) opartych na protokole RADIUS.
- *Cisco Network Admission Control (NAC)*. Mechanizm Cisco NAC sprawdza, czy punkty końcowe próbujące nawiązać połączenie z siecią mają odpowiednie oprogramowanie zabezpieczające. Jeśli nie, to punkt końcowy jest łączony z serwisem internetowym, który koryguje ten problem. Samorządy mogą wybrać jedno z dwóch rozwiązań. Cisco NAC Framework wykorzystuje funkcje inteligentnej analizy wbudowane w przełączniki firmy Cisco, natomiast urządzenie Cisco NAC Appliance, wyposażone w program Cisco Control Agent, realizuje tę samą funkcję jako osobne rozwiązanie przeznaczone dla środowisk z mniej intensywnie zarządzanymi punktami końcowymi.

Inteligentna analiza aplikacji

Podatność na zagrożenia

Tradycyjne sieci traktują cały ruch w ten sam sposób, niezależnie od aplikacji, która go wygenerowała. Sieciom tym brakuje „inteligencji" wymaganej do udostępniania usług zabezpieczeń na poziomie aplikacji, takich jak kontrola dostępu do poszczególnych aplikacji biznesowych czy rozróżnianie między usługami korzystającymi z tych samych kanałów komunikacyjnych warstwy 3. lub 4.

W rezultacie większość działów informatycznych w samorządach musi uciekać się do egzekwowania reguł bezpieczeństwa „ponad siecią", zamiast wykorzystywać w tym celu samą sieć. Nie tylko zwiększa to złożoność i koszty infrastruktury, ale także może pogorszyć wydajność sieci.

Rozwiązania firmy Cisco do inteligentnej analizy aplikacji

Samodzielnie broniąca się sieć (Cisco Self-Defending Network) potrafi dopasować pakiety do przepływów generowanych przez aplikacje, takich jak MIME i HTTP, a nie tylko do adresów MAC, adresów IP i portów.

Rozwiązania Cisco do inteligentnej analizy aplikacji obejmują:

- *Rutery Cisco.* Firma Cisco nieustannie wzbogaca swoje rutery o nowe mechanizmy inspekcji aplikacji. Na przykład, mechanizmy inspekcji stanów (ang. stateful inspection) potrafią kontrolować przepływy aplikacyjne przechodzące przez każdy punkt warstwy 3 sieci, uniemożliwiać nieporządane tunelowanie na porcie 80 oraz zapobiegać nieprawidłowemu wykorzystywaniu protokołów poczty elektronicznej. Funkcja NBAR (Network-Based Application Recognition) oprogramowania IOS™ pozwala ruterowi klasyfikować ruch poprzez analizę aplikacji (7. warstwa modelu OSI).
- *Zapory firmy Cisco, w tym Cisco PIX Firewall, Cisco Adaptive Security Appliance (ASA) i Cisco Firewall Security Module (FWSM).* Zapory Cisco stosują różne reguły do różnych typów aplikacji. Samorządowe zespoły informatyczne mogą użyć zapór w celu kontroli komunikacji równorzędnej (ang. peer-to-peer), egzekwowania reguł dotyczących wiadomości (i załączników) przesyłanych za pomocą komunikatorów, ograniczenia dostępu do serwera WWW na podstawie metod i poleceń, filtrowania treści MIME i poczty elektronicznej oraz sprawdzania ruchu zgodnego z protokołami opisanymi w standardach RFC pod kątem anomalii.

Ochrona przed atakami typu „day zero"

Podatność na zagrożenia

Ataki robaków internetowych, wirusów, koni trojańskich i programów szpiegujących (ang. spyware) są coraz częstsze, a reagowanie na nie wymaga od samorządowych zespołów informatycznych poświęcania coraz większej ilości zasobów. Opóźnienia między wykryciem problemu a ręczną reakcją mogą spowodować konieczność instalacji programów korygujących, usunięcia szkodliwego kodu oraz odtworzenia setek bądź tysięcy komputerów biurkowych i serwerów. Jeśli nie uda się zapobiec atakom typu „day zero", to mogą one zakłócić świadczenie kluczowych usług samorządowych.

Na przykład, w czerwcu 2005 r. brytyjskie Narodowe Centrum Koordynacyjne Bezpieczeństwa Infrastruktury (National Infrastructure Security Co-ordination Center) wydało ostrzeżenie o ataku skierowanym na przeszło 300 brytyjskich urzędów i przedsiębiorstw. Atak ten wykorzystuje ponad 75 różnych rodzajów koni trojańskich i ma na celu kradzież informacji. Hakerzy wysyłają wiadomość e-mail do osób, które niedawno uczestniczyły w konferencji lub innym wydarzeniu. Wiadomość wygląda na wysłaną przez organizatorów, a w jej załączniku znajduje się formularz kontaktowy. Po otwarciu formularza komputer użytkownika zostaje zainfekowany koniem trojańskim. Oprogramowanie antywirusowe nie zapewnia ochrony przed tym typem ataku, ponieważ nie zna ono jego sygnatury.

Rozwiązania Cisco do ochrony przed atakami typu „day zero"

Samorządy potrzebują ochrony przed zagrożeniami — zarówno tymi znanymi, jak i nowymi, których sygnatury jeszcze nie są znane, tak jak w przypadku niedawnych ataków koni trojańskich w Wielkiej Brytanii. Cisco Security Agent zaspokaja tę potrzebę za pomocą mechanizmów wykrywania anomalii w zachowaniu aplikacji. Po zainstalowaniu na komputerze biurkowym lub serwerze, Cisco Security Agent nieustannie monitoruje zachowanie aplikacji, porównując je z pewnym stanem odniesienia. W przypadku wykrycia anomalii w zachowaniu aplikacji, Cisco Security Agent zatrzymuje jej działanie do momentu wyraźnego zatwierdzenia takiego zachowania przez człowieka. W ten sposób samorządy mogą ochronić swoje systemy przed nieznanymi programami szpiegującymi, skanowaniem portów, przepełnieniami bufora, końmi trojańskimi, robakami rozprzestrzeniającymi się przez pocztę elektroniczną i innymi niebezpiecznymi atakami.

W przypadku ataków koni trojańskich, jakie wystąpiły w czerwcu 2005 r. w Wielkiej Brytanii, program Cisco Security Agent tworzy skuteczną linię obrony. Na początku wykrywa próbę zainstalowania nowego oprogramowania. Następnie, w zależności od sposobu skonfigurowania przez samorządowy zespół informatyczny, Cisco Security Agent zatrzymuje instalację albo informuje użytkowników o próbie instalacji oprogramowania i czeka na ich zgodę. Jeśli niektóre komputery zostały już spenetrowane, system CiscoSecure MARS (Monitoring, Analysis, and Response System) wykrywa je, umożliwiając działowi informatyki ich naprawienie.

Powstrzymywanie infekcji

Podatność na zagrożenia

Celem systemu bezpieczeństwa opartego o koncepcję samodzielnie broniącej się sieci (Self-Defending Network) jest zapobieganie infekcjom. Jeśli jednak dojdzie do infekcji, samorządy muszą mieć możliwość szybkiej i automatycznej reakcji, aby odizolować infekcję, zanim obejmie kolejne usługi. Obecnie reagowanie na zdarzenia jest w dużej mierze działaniem wykonywanym ręcznie i wymagającym zaangażowania znacznych zasobów.

Rozwiązania firmy Cisco do powstrzymywania infekcji

Strategia Cisco Self-Defending Network udostępnia automatyczne środki przeciwdziałające niewłaściwemu wykorzystywaniu sieci, m.in. izolowanie źródeł infekcji, filtrowanie szkodliwych treści i stosowanie mechanizmów QoS w celu łagodzenia przeciążeń.

- *CiscoSecure MARS.* CiscoSecure MARS rozpoznaje źródła i cele szkodliwej działalności, w tym ich lokalizację w topologii sieciowej. W tym celu narzędzie dokonuje korelacji danych generowanych przez serwery, urządzenia sieciowe, zapory i urządzenia IPS, a następnie nakłada te informacje na dynamicznie aktualizowane mapy topologii warstw 2. i 3. sieci. Narzędzie CiscoSecure MARS może na przykład odczytać tabelę CAM na przełączniku Cisco Catalyst i zgłosić, że komputer o adresie 10.1.1.1 zainfekowany robakiem Sasser jest podłączony na porcie 7 przełącznika switch_pietro_10. Następnie może on zaproponować działania korekcyjne, takie jak izolacja portu czy zastosowanie odpowiednich list kontroli dostępu do ruterów warstwy 3.
- *Rutery Cisco*. Rutery Cisco są wyposażone w mechanizmy klasyfikacyjne IPS odfiltrowujące szkodliwe pakiety. Przetwarzanie sprzętowe gwarantuje, że działania te nie spowodują zakłóceń w świadczeniu usług.
- *Cisco Guard*. Rozwiązanie Cisco Guard nieustannie skanuje ruch w poszukiwaniu nietypowych schematów sygnalizujących możliwość ataku DDoS. Podejrzany ruch jest kierowany do modułu, który przeprowadza dodatkową analizę, po czym usuwa szkodliwy ruch, przesyłając „czyste" pakiety do ich punktu docelowego.

ZALETY SAMODZIELNIE BRONIĄCEJ SIĘ SIECI Z PUNKTU WIDZENIA ADMINISTRACJI PUBLICZNEJ

Rozwiązania Cisco Self-Defending Network chronią komputery osobiste, serwery i urządzenia sieciowe w samorządowych sieciach miejskich, kampusowych, brzegowych oraz w bezprzewodowych sieciach lokalnych, zapewniając wielowarstwową ochronę rozproszonych zasobów informacyjnych. Tabela 1 zawiera podsumowanie obszarów, w których samodzielnie broniące się sieci firmy Cisco zaspokajają potrzeby samorządów.

Analiza przypadku — Urząd Miejski Lizbony

W Portugalii Urząd Miejski Lizbony dąży do poprawy skuteczności usług, zwiększenia produktywności pracowników i ograniczenia kosztów operacyjnych. W 2001 r. rada miasta postanowiła połączyć 25 osobnych działów informatyki w jeden scentralizowany dział, aby usprawnić realizowane procesy i obniżyć koszty.

Tabela 1. Zalety samodzielnie broniącej się sieci z punktu widzenia samorządu

Potrzeba samorządu	Metoda działania Cisco Self-Defending Network
Zapewnienie ciągłości świadczenia usług poprzez ochronę infrastruktury	• Łagodzi ataki robaków • Uniemożliwia nieautoryzowany dostęp • Zapobiega atakom typu DoS i DDoS • Chroni poufne zasoby informacyjne i punkty dostępu do sieci
Zapewnienie ciągłości świadczenia usług poprzez reagowanie na zagrożenia sieciowe	• Zabezpiecza infrastrukturę na wypadek ataku, ograniczając tym samym szkody wywołane przez ataki typu „day zero”, zanim zdążą się rozprzestrzenić • Rozwiązuje problemy z siecią, a w razie potrzeby zmienia jej konfigurację • Udostępnia osobom decyzyjnym miarodajne i istotne informacje o bezpieczeństwie
Przestrzeganie przepisów dotyczących przetwarzania danych	• Przeprowadza audyt sieci samorządowych za pomocą zaawansowanych usług specjalistycznych • Udostępnia produkty i usługi, które pozwalają klientom zachować zgodność z przepisami prawa
Zwiększenie produktywności	• Minimalizuje zakłócenia w pracy użytkowników i przestoje w działaniu sieci • Udostępnia narzędzia internetowe do wykonywania zadań związanych z bezpieczeństwem, takich jak konfigurowanie i monitorowanie sieci VPN, zapór oraz sieciowych i serwerowych systemów IPS, a także rozwiązywanie problemów z ich działaniem • Eliminuje konieczność dodatkowych inwestycji przeznaczonych na odrębne zakupy, kontakty z dostawcami i wiedzę specjalistyczną związaną z bezpieczeństwem • Tworzy infrastrukturę, która będzie w stanie zapewnić ochronę także przyszłych funkcji, takich jak telefonia IP, wideokonferencje i aplikacje do obsługi klientów • Upraszcza bieżącą konserwację, obsługę i administrację siecią
Zapewnienie zdalnym biurom bezpiecznej łączności	• Ułatwia współpracę między urzędami • Zapewnia poufność danych dzięki sieciom VPN z wydajnym szyfrowaniem • Zapewnia zdalnym pracownikom lub agencjom partnerskim dostęp do sieci za pomocą bezpiecznych, szybkich połączeń, co ułatwia pracę zespołową w grupach roboczych, a także umożliwia tworzenie ekstranetów, mobilnych centrów operacyjnych oraz wirtualnych, ogólnoświatowych centrów kontaktowych • Daje gwarancję bezpieczeństwa, dostępności i wysokiej wydajności połączeń sieciowych dzięki gwarantowanemu poziomowi usług (ang. service level agreements – SLA), który jest zawierany z partnerem firmy Cisco

„Wybraliśmy firmę Cisco ze względu na jej światową renomę jako dostawcy doskonałych technicznie rozwiązań, a także ze względu na jej doświadczenie w dziedzinie sieci i komunikacji w sektorze publicznym”

Dr Jorge Baptista, dyrektor ds. informatyki w Urzędzie Miejskim Lizbony

W chwili obecnej we wszystkich 135 budynkach należących do Urzędu Miejskiego Lizbony można korzystać z szybkiego, bezpiecznego dostępu do centralnych aplikacji i danych. Dostęp ten odbywa się za pomocą światłowodów, łączy Frame Relay oraz łączy bezprzewodowych. Bezpieczna sieć IP umożliwia radzie miasta świadczenie takich usług, jak telefonia IP, publicznie dostępne centrum kontaktowe, publiczny serwis WWW zapewniający wygodny dostęp do informacji i formularzy oraz możliwość oglądania na żywo sesji rady.

Ponieważ sieć jest wykorzystywana do świadczenia usług o krytycznym znaczeniu, takich jak telefonia IP, bezpieczeństwo było ważnym kryterium projektowym. Zgodnie z zaleceniem firmy Cisco rada utworzyła dwa centra przetwarzania danych z identycznym, całkowicie nadmiarowym sprzętem. W przypadku awarii jednego centrum przetwarzania danych lub znajdującego się w nim urządzenia, jego funkcje są natychmiast przejmowane przez drugie centrum lub urządzenie, dzięki czemu nigdy nie występują przerwy w usługach informatycznych czy komunikacyjnych.

Trójwarstwowa topologia zabezpieczeń chroni komunikację między budynkami rady, łącza internetowe, dane oraz aplikacje. Pierwsza warstwa zawiera połączenie z Internetem chronione przez rozwiązanie Cisco PIX 515E Firewall Platform z oprogramowaniem do przełączania awaryjnego. Druga warstwa zabezpieczeń znajduje się między zaporą Cisco PIX a modułami Cisco FWSM (Firewall Services Modules), które są zainstalowane w przełącznikach Cisco Catalyst w każdym centrum przetwarzania danych. Warstwa ta chroni wszystkie publicznie dostępne serwery, a także koncentratory z serii Cisco VPN 3000 i urządzenia z serii Cisco 565 Content Engine. Trzecia warstwa, znajdująca się między modułami Cisco FWSM, chroni bazy danych rady miasta, jej serwer intranetowy oraz wszystkie serwery aplikacji przeznaczone do użytku wewnętrznego. Warstwa ta zawiera wiele modułów Cisco IDS, które nieustannie skanują sieć w poszukiwaniu śladów włamań. Oddzielenie systemów wewnętrznych i zewnętrznych pozwala zapobiegać nieautoryzowanemu dostępowi do poufnych danych obywateli i samorządu.

Opracowując politykę bezpieczeństwa dla Urzędu Miejskiego Lizbony, firma Cisco Systems uwzględniła elementy należące do strategii Self-Defending Network. Na przykład, pełna nadmiarowość na każdym poziomie infrastruktury nie tylko chroni sieć przed błędami systemowymi, ale także pozwala zapewnić stałą aktywność i dostępność sieci, nawet w trakcie ataków. Dzięki zastosowaniu koncentratorów Cisco VPN 3000 kierownicy działów oraz informatycy w Urzędzie Miejskim Lizbony mają bezpieczny dostęp do sieci z domu lub innych zdalnych lokalizacji, przy użyciu protokołu IPSec lub SSL (Secure Sockets Layer).

Bezpieczna infrastruktura zapewnia Urzędowi Miejskiemu Lizbony większą elastyczność niż wcześniej. Na przykład, kilka spośród budynków rady miasta jest zbyt małych, by mogły mieć własne połączenia światłowodowe, więc w tych przypadkach zastosowano technologie dostępu bezprzewodowego, jako bardziej ekonomiczną alternatywę. „Rozbudowując sieć, szukamy technologii, które najlepiej odpowiadają naszym celom i zapewnią nam najwyższy zwrot z inwestycji” — mówi Jorge Baptista. „To kwestia wyboru. Infrastruktura informatyczna daje nam ten wybór, znacznie ułatwiając realizację naszego zadania, jakim jest poprawa poziomu usług świadczonych pracownikom i mieszkańcom”.

Analiza przypadku — region Lombardii

Lombardia jest jednym z najbardziej zróżnicowanych regionów we Włoszech; ma 11 prowincji, 15 lokalnych placówek opieki zdrowotnej oraz wiele innych agencji samorządowych. Niektórzy mieszkańcy regionu żyją w małych miejscowościach, liczących zaledwie kilkadziesiąt osób, zaś inni — w aglomeracji Mediolanu skupiającej ponad 1,5 miliona ludzi. Aby poprawić skuteczność usług świadczonych na rzecz agencji w całym regionie, postanowiono utworzyć regionalną sieć telekomunikacyjną łączącą wszystkie agencje, w tym szpitale, posterunki policji, biblioteki, lokalne placówki opieki zdrowotnej i inne organizacje regionalne.

Sieć regionalna musiała być bezpieczna, należało zatem wprowadzić identyfikację użytkowników, która potwierdzałaby ich upoważnienie do skorzystania z żądanej usługi oraz zapewniała poufność komunikacji. Ponieważ przedsięwzięcie zamierzano finansowawać ze środków publicznych, sieć musiała być ekonomicznie zrównoważona, a ponadto konieczne było zapewnienie wykorzystania dotychczasowych inwestycji technologicznych poszczególnych agencji.

„Nie zaczynaliśmy od zera w kwestii technologii” — mówi Antonio Confalonieri, szef działu telekomunikacji i systemów informatycznych w Regionie Lombardii. „W poprzednich latach dokonywano wielu inwestycji na poziomie lokalnym. Władze regionu chciały te inwestycje nie tylko uwzględnić, ale i aktywnie wykorzystać. Wszystkie agencje, niezależnie od ich wielkości, otrzymały połączenie z Internetem. Ten wspólny mianownik odpowiadał naszej potrzebie zbudowania prywatnej sieci, której szkieletem komunikacyjnym byłby Internet”.

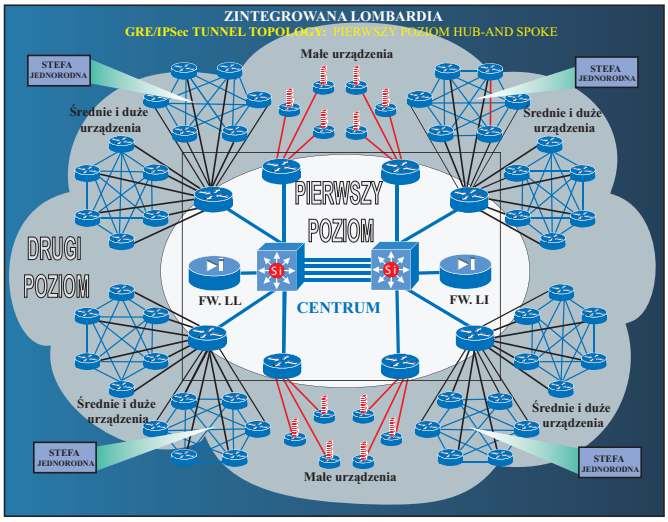
Firma Cisco Systems zaproponowała rozwiązanie VPN, gdyż pozwalało ono spełnić wymagania regionu dotyczące bezpiecznej łączności przy niższym koszcie niż w przypadku linii dzierżawionych. Podstawowym problemem technologicznym byłaby obsługa do 5000 zdalnych lokalizacji, 500 innych małych ośrodków należących do centralnej administracji regionu oraz licznych telepracowników w różnych częściach regionu.

Firma Cisco Systems zaprojektowała hierarchiczną topologię sieci (rys. 1). Pierwszy poziom tworzą zdalne lokalizacje, z których każda jest wyposażona w ruter Cisco z serii 1700, umiejscowiony między siecią lokalną a ruterem ADSL operatora. Użytkownicy łączą się z Internetem za pośrednictwem operatora, a z siecią Regionu Lombardii — przez ruter Cisco 1700, który ustanawia tunel IPSec VPN do rutera wielousługowego Cisco 2600 Multiservice Platform w centralnej lokalizacji.

Kolejnym poziomem hierarchii są rutery wielousługowe Cisco 2600 Multiservice Platform, z których każdy łączy się z wieloma zdalnymi lokalizacjami, a także z dwoma ruterami Cisco 7200 w głównym centrum przetwarzania danych. Rutery te stanowią trzeci poziom hierarchii i tworzą pełną sieć połączeń, która pozwala każdej agencji komunikować się z każdą inną agencją za pośrednictwem sieci IPSec VPN. Pięćset małych ośrodków należących do centralnej administracji regionu łączy się bezpośrednio z podwójnymi koncentratorami Cisco

VPN 3000 w centrum przetwarzania danych. Koncentratory VPN obsługują również zdalny dostęp uzyskiwany przez telepracowników korzystających z oprogramowania Cisco VPN Client.

Rysunek 1. Topologia sieci w rozwiązaniu VPN przygotowanym dla regionu Lombardii



W rozwiązaniu sieciowym dla regionu Lombardii wykorzystano zawarte w strategii Cisco Self-Defending Network wytyczne dotyczące bezpiecznej łączności, zarządzania poziomem zaufania i tożsamością oraz obrony przed zagrożeniami. Na przykład, każde urządzenie w sieci ma klucz, który umożliwia komunikację z innymi urządzeniami i stanowi jego upoważnienie do korzystania z sieci. Pracownicy agencji korzystają z kart procesorowych zawierających certyfikat cyfrowy, który uprawnia do korzystania z poszczególnych usług. Cały ruch jest szyfrowany algorytmem 3DES. W samym rdzeniu sieci dwuwarstwowa zapora i strefy zdemilitaryzowane chronią usługi aplikacyjne oraz bazy danych.

Rozwiązania zabezpieczające firmy Cisco pomagają regionowi Lombardii osiągać nadrzędne cele dotyczące efektywności usług, bezpieczeństwa publicznego i rozwoju gospodarczego. Efektywność usług wzrosła, ponieważ agencje mogą wymieniać dokumenty drogą elektroniczną, zamiast korzystać z procesów opartych na dokumentach papierowych. Agencje mogą również oferować swoje usługi innym agencjom, co pozwala uniknąć dublowania tych samych działań. Bezpieczeństwo publiczne wzrosło dzięki wysokiej dostępności sieci: w razie awarii jednego urządzenia, rutery wielousługowe Cisco 2600 Multiservice Platform są w stanie ponownie ustanowić tunel VPN z użyciem alternatywnej trasy. Korzyści odnosi również gospodarka regionu, gdyż dzięki obsłudze telepracy zwiększają się szanse zatrudnienia w odległych obszarach.

DLACZEGO CISCO?

Firma Cisco dysponuje wyjątkowymi atutami w dziedzinie bezpieczeństwa systemów samorządowych — są to: znakomita wiedza specjalistyczna, najlepsi w branży partnerzy, rozwiązania o dużej zgodności operacyjnej, kompleksowe usługi w zakresie cyklu życia zabezpieczeń sieciowych oraz elastyczne możliwości finansowania.

Znakomita wiedza specjalistyczna

Rozwiązania Cisco Self-Defending Network obejmują najlepsze w branży, zgodne ze standardami oprogramowanie i sprzęt instalowane w całej sieci sieci, dzięki czemu chronią dane i aplikacje od rdzenia sieci po komputer biurkowy. Zaawansowane funkcje zabezpieczające są wbudowane w rutery, przełączniki, urządzenia i punkty końcowe Cisco. Usługi zabezpieczeń są ściśle zintegrowane z usługami sieciowymi. Na przykład sieci VPN współdziałają w przezroczysty sposób z aplikacjami Cisco IP Communications. Dzięki temu organy administracji publicznej dowolnej wielkości mogą bezpieczne wdrażać zaawansowane aplikacje oparte na protokole IP, które zwiększają efektywność usług, poprawiają bezpieczeństwo publiczne i stymulują rozwój gospodarczy.

Firma Cisco oferuje również:

- utrzymywaną od prawie 20 lat pozycję lidera na rynku sieci; jedną z innowacji technicznych firmy było pierwsze urządzenie Cisco Adaptive Security Appliance (ASA), łączące w sobie funkcje zapory, sieci VPN i systemu IPS (wprowadzone w maju 2005 r.);
- zespół światowej klasy certyfikowanych inżynierów sieciowych Cisco mających dogłębną wiedzę o sieciach;
- rozległe doświadczenie w projektowaniu i obsłudze skalowalnych sieci, zarządzaniu nimi oraz świadczeniu pomocy technicznej ich użytkownikom;
- rozległe doświadczenie we wdrażaniu sieci w sektorze publicznym na całym świecie;
- szeroki zespół specjalistów technicznych i inżynierów, którzy rozumieją potrzeby samorządów, standardy i ważne inicjatywy.

Najlepsi w branży partnerzy

Firma Cisco Systems utrzymuje partnerskie relacje z liderami rynku informatycznego. Dzięki tej współpracy partnerskiej może pomagać samorządom we wdrażaniu infrastruktur sieciowych o dużej zdolności adaptacji, a także innowacyjnych aplikacji, które pozwalają uzyskać maksymalne korzyści z poniesionych inwestycji i w jak najlepszy sposób służyć obywatelom.

Rozwiązania o dużej zgodności operacyjnej

Otwarte, zgodne ze standardami rozwiązania sieciowe firmy Cisco zapewniają najwyższą zgodność operacyjną, co umożliwia ochronę i rozszerzanie inwestycji samorządowych.

Kompleksowe usługi w zakresie kompleksowych zabezpieczeń sieciowych

Firma Cisco oferuje usługi analizy bezpieczeństwa, wsparcia przy projektowaniu zabezpieczeń oraz przy ich obsłudze i zarządzaniu nimi, a także usługi poprawiające bezpieczeństwo sieci. Firma Cisco Systems i jej partnerzy zatrudniają konsultantów o ogromnym doświadczeniu w sferze samorządowej. Samorządy mogą więc skorzystać z usług oferowanych przez firmę Cisco w celu osiągnięcia maksymalnego zwrotu z inwestycji w bezpieczeństwo sieciowe. Na przykład, analizy stanu bezpieczeństwa pozwalają organom administracji na prewencyjne wykrywanie punktów sieci podatnych na zagrożenia oraz ocenę braków w zabezpieczeniach wewnętrznych systemów, dzięki czemu możliwie jest powstrzymanie ataków sieciowych, zanim zostaną przeprowadzone.

Do innych usług w zakresie kompleksowych zabezpieczeń sieciowych należą:

- *Przegląd architektury bezpieczeństwa sieciowego (Network Security Architecture Review)*. Firma Cisco i jej partnerzy dokonują przeglądu architektury sieci samorządowej oraz wewnętrznej polityki bezpieczeństwa sieciowego, po czym proponują działania korekcyjne oraz wyjaśniają, w jaki sposób należy zapewnić przestrzeganie stosownych części standardu ISO 17799, najlepszych procedur i wewnętrznych reguł bezpieczeństwa. Rezultatem usługi jest raport zawierający szczegółowe omówienie stanu operacyjnego zarządzania ryzykiem (ang. operational risk management — ORM) w odniesieniu do architektury sieci oraz zalecenie odpowiednich działań.
- *Usługi oceny gotowości na nieporządane zdarzenia (Incident Readiness Assessment Services)*. Korzystając z najlepszej w branży metodyki zarządzania zdarzeniami opracowanej przez Cisco, firma Cisco i jej partnerzy ustalają, na ile skutecznie sieć jest w stanie złagodzić skutki działalności robaków internetowych, epidemii wirusów czy ataków typu DoS. Usługa ta ostrzega samorządowe zespoły informatyczne przed zagrożeniami sieciowymi i operacyjnymi, które mogą utrudniać szybkie i skuteczne reagowanie na włamania.
- *Usługi planistyczno-projektowo-wdrożeniowe (Plan-Design-Implement Services)*. Firma Cisco i jej partnerzy mogą świadczyć usługi planowania, projektowania i wdrażania rozwiązań zabezpieczających, takich jak Cisco Security Agent, Cisco NAC, Cisco Guard i inne.

Projekty Cisco SAFE

W administracji publicznej pierwszym krokiem prowadzącym do zabezpieczenia sieci jest przedstawienie urzędnikom i wyborcom przekonującej argumentacji biznesowej. Potrzebne informacje znajdują się w projektach Cisco SAFE, które można dostosowywać do własnych potrzeb. „Moduły" zabezpieczeń upraszczają projektowanie i wdrażanie zabezpieczeń oraz zarządzanie nimi. Każdy moduł zawiera pewną kombinację zapór, systemów wykrywania włamań i zapobiegania włamaniom, uwierzytelniania urządzeń i użytkowników, technologii antywirusowych, szyfrowania, tunelowania i rozwiązań VPN. Plany rozwoju wskazują samorządowym zespołom informatycznym, w jaki sposób komponenty firmy Cisco dostosowują się do zmiennych wymagań aplikacji i ewoluujących przepisów prawa. Projekty Cisco SAFE zawierają również elastyczne scenariusze wdrożeń, przewidujące lub nie, wsparcie partnerów firmy Cisco.

Dzięki projektom Cisco SAFE dotyczącym bezpiecznych rozwiązań dla e-administracji, samorządy mogą:

- zbudować podstawę umożliwiającą migrację do bezpiecznej, efektywnej kosztowo sieci konwergentnej;
- wdrożyć modułową, skalowalną infrastrukturę zabezpieczeń w ekonomiczny, sposób z podziałem na etapy;
- zapewnić zintegrowaną ochronę sieci opartą na produktach i usługach gwarantujących wysoki poziom bezpieczeństwa.

Finansowanie

Spółka Cisco Systems Capital, w całości należąca do firmy Cisco Systems Inc., specjalizuje się w finansowaniu rozwiązań sieciowych. Oferuje nowatorskie, elastyczne usługi finansowe klientom firmy Cisco i jej partnerom po konkurencyjnych cenach. Oferowane przez nią programy finansowania są dostępne na całym świecie i obejmują szeroki wachlarz kreatywnych, indywidualizowanych opcji, które pomagają klientom z sektora administracji publicznej budować, obsługiwać i modernizować rozwiązania firmy Cisco.

WNIOSKI

Kompleksowe podejście do bezpieczeństwa sieciowego jest warunkiem koniecznym osiągnięcia przez władze regionalne i lokalne postawionych sobie celów — tj. zwiększenia efektywności usług, poprawę bezpieczeństwa mieszkańców i pobudzenia rozwoju gospodarczego. Model zintegrowanych zabezpieczeń Cisco dla samorządów (Cisco Integrated Security for Regional and Local Government) ułatwia ochronę centralnych, regionalnych i lokalnych sieci samorządowych we wszystkich ich częściach — od rdzenia sieci po urządzenia końcowe. Model ten obejmuje zaawansowany sprzęt, oprogramowanie i usługi cyklu życia związane z bezpieczeństwem.

Więcej informacji o modelu zintegrowanych zabezpieczeń Cisco dla samorządów oraz o sposobach budowania samodzielnie broniącej się sieci (Self-Defending Network) można znaleźć pod adresami:

http://www.cisco.com/go/security
http://www.cisco.com/selfdefend
http://www.cisco.com/securitynow

Więcej informacji o rozwiązaniach dla administracji publicznej można znaleźć pod adresem www.cisco.pl/jst
www.cisco.com/go/localgov

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

European Headquarters
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

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
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 has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Cyprus • Czech Republic • Denmark • Dubai • UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India Indonesia • Ireland • Israel ItalyJapan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa Spain • SwedenSwitzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe