

Zagadnienia bezpieczeństwa informacji w branży energetycznej

WEWNĄTRZ

- > Rozrost systemów informatycznych w branży energetycznej
- > Luki w zabezpieczeniach sieci w branży energetycznej
- > Możliwe skutki złamania zabezpieczeń
- > Strategie zaradcze

Spis treści

Streszczenie	3
Rozrost systemów informatycznych w branży energetycznej	4
Systemy tradycyjne.	4
Rozwój elektronicznych form działalności.	5
Nowe dziedziny działalności.	6
Luki w zabezpieczeniach sieci w branży energetycznej.	7
Możliwe skutki złamania zabezpieczeń	8
Strategie zaradcze	9

> Streszczenie

Wprowadzenie konkurencji w branży energetycznej przy rosnącym popycie na energię elektryczną spowodowało, że firmy energetyczne w coraz większym stopniu wykorzystują systemy i sieci informatyczne. Systemy informatyczne stanowią osnowę systemów sterowania i zarządzania przepływem energii w sieciach energetycznych od turbin po liczniki u odbiorców, a firmy energetyczne używają ich również do zarządzania innymi aspektami działalności. Do zarządzania relacjami z klientami, łączności z dostawcami, a nawet do obsługi transakcji kupna i sprzedaży energii innym firmom coraz częściej są używane sieci informatyczne.

Wzrostowi skali zastosowań systemów informatycznych towarzyszy również szybkie obniżenie ich bezpieczeństwa. Wysiłki zmierzające do ułatwienia dostępu do danych eksploatacyjnych oraz informacji o klientach i dostawcach, w połączeniu z geograficznym rozszerzeniem sieci informatycznych w następstwie fuzji i przejęć w branży energetycznej znacznie obniżają bezpieczeństwo sieci komunikacyjnych firm energetycznych. Wskutek tego wpływ ewentualnego złamania zabezpieczeń wykracza daleko poza problemy związane z eksploatacją. Włamanie może mieć niszczące skutki również dla kondycji finansowej firm.

Celem niniejszego artykułu jest opisanie stanu zabezpieczeń informatycznych w branży energetycznej i wskazanie najważniejszych trendów, wskutek których sieci informatyczne stały się czułym punktem firm energetycznych. W artykule opisano kilka najważniejszych luk w zabezpieczeniach informatycznych i ich możliwe skutki. W końcowej części wskazano, jakie kroki mogą podjąć firmy energetyczne w celu opracowania skutecznej strategii bezpieczeństwa danych.

> Rozrost systemów informatycznych w branży energetycznej

Struktura branży energetycznej przechodzi całkowite przeobrażenie. Ponieważ wynika ono z deregulacji tej branży, restrukturyzacja dotyczy nie tylko sposobu prowadzenia działalności, lecz również typów działalności podejmowanej przez firmy z sektora energetycznego. Technologia informatyczna jest zarówno przyczyną jak i metodą restrukturyzacji: firmy energetyczne widzą w Internecie środek do osiągnięcia celu, jakim jest ułatwienie podstawowych działań, związanych z obsługą klientów, zarządzaniem przesyłem energii i zarządzaniem awariami zasilania. Firmy energetyczne stają się coraz bardziej zależne od szybkich, łatwych w rozbudowie i „otwartych” systemów informatycznych.

SYSTEMY TRADYCYJNE

Sieci informatyczne były używane w firmach energetycznych do nadzoru podstawowych działań jeszcze przed deregulacją tej branży. Sieci te umożliwiały centralny nadzór nad systemami zarządzania energią (EMS) i przesyłem prądu od turbin elektrowni aż po odbiorcę końcowego. Systemy EMS spowodowały utworzenie dużej liczby podstacji transmisyjnych i dystrybucyjnych, nierzadko rozrzuconych na dużych obszarach i wymagających centralnego zarządzania. W firmach energetycznych powołano w tym celu do życia systemy SCADA (z ang. supervisory control and data acquisition, czyli systemy nadzoru i pozyskiwania danych), które zapewniały ośrodkom sterowania dane z węzłów rozmieszczonych w całej sieci energetycznej. Systemy SCADA na podstawie gromadzonych danych inicjowały alarmy dotyczące sieci energetycznej, a personel nadzorczy przy użyciu systemów SCADA przekazywał instrukcje postępowania do stacji terenowych.

Ponieważ nowoczesne sieci energetyczne rozciągają się na ogromnych obszarach, systemy SCADA, powszechnie stosowane w branży energetycznej, są niezbędne do skutecznego zarządzania energią. W Ameryce Północnej jest 3200 firm energetycznych. W większości z nich systemy SCADA są podstawowym narzędziem zarządzania wytwarzaniem, przesyłaniem i dystrybucją prądu. Typowy system SCADA gromadzi dane z 30 000 – 50 000 punktów. Centralne zarządzanie danymi sieciowymi stało się czynnikiem decydującym o niezawodności systemu energetycznego i wydajnej pracy służb obsługi.

Doceniając ważną rolę systemów EMS i SCADA, większość firm energetycznych utworzyła te sieci w izolacji od innych systemów przedsiębiorstwa. Pierwsze systemy SCADA były skutecznie „odseparowane” dzięki zastosowaniu nietypowych systemów zasilania, specjalnych procedur postępowania w razie awarii i odrębnych protokołów programowania systemu. Z czasem jednak scalanie sieci firm energetycznych i zapotrzebowanie na dostęp zdalny do systemów nadzorczych doprowadziły do tego, że systemy SCADA stały się dostępne z sieci innych niż dedykowane sieci SCADA.

ROZWÓJ ELEKTRONICZNYCH FORM DZIAŁALNOŚCI I PRZEKSZTAŁCENIA TRADYCYJNEJ ARCHITEKTURY SIECIOWEJ

W ciągu ostatnich pięciu lat rozszerzenie zastosowań technologii internetowych doprowadziło do zmian sposobu prowadzenia działalności w niemal każdej ważniejszej branży w Ameryce Północnej, z energetyką włącznie. Strategie wdrażania technologii elektronicznych przyniosły firmom energetycznym zmniejszenie kosztów, zwiększenie skuteczności komunikacji i rozszerzenie dziedzin działalności. Korzyści te stały się jeszcze ważniejsze, gdy firmy energetyczne wkroczyły na wolny rynek, na którym rządzi zasada konkurencji. Tabela zamieszczona na następnej stronie wskazuje niektóre z najważniejszych dziedzin, w których firmy energetyczne odniosły znaczące korzyści dzięki wdrożeniu strategii wykorzystania Internetu w biznesie.

Korzyści są ewidentne, ale wiele firm dopiero zaczyna zdawać sobie sprawę z niebezpieczeństw, do których nieuchronnie prowadzi zarówno zwiększenie dostępności sieci, jak i wzrost liczby użytkowników. Integrowanie systemów korporacyjnych w celu zapewnienia dostępu klientom, dostawcom i innym osobom z zewnątrz znacznie zmniejsza bezpieczeństwo poufnych informacji firmowych zawartych w tych systemach.

NOWE DZIEDZINY DZIAŁALNOŚCI

Wiele firm energetycznych, starając się utrzymać na rynku, na którym zapanowała zasada konkurencji, poszukuje nowych źródeł przychodów. Firmy te inwestują w dziedziny „nieelektryczne”, którymi dawniej nie interesowały się ze względu na odmienność branży. Dzięki inwestycjom małe spółki w fazie organizacji błyskawicznie przekształcają się w średnie firmy lub wielkie, samodzielne korporacje. Najbardziej interesujące są tu spółki handlujące energią, w ogromnym stopniu zależne od systemów informatycznych. Na przykład jedna z największych platform handlu energią, uruchomiona w roku 1999, w pierwszym półroczu działalności przeprowadziła 130 000 transakcji, a jej obroty sięgały 1,5 miliarda USD dziennie. Ponad połowę tych transakcji przeprowadzono drogą elektroniczną.

Przekształcenia dotychczasowych systemów wspomagających

Klienci	Systemy przetwarzania informacji o klientach (CIS, Customer Information System)	Wiele firm energetycznych zastępuje przestarzałe systemy CIS nowymi, skoncentrowanymi na klientach zewnętrznych i łatwiej dla nich dostępnymi. Ponad połowa stosowanych obecnie systemów CIS ma ponad 10 lat.
Dostawcy	Systemy elektronicznej obsługi dostaw	Firmy energetyczne łączą się, aby uzyskać lepsze warunki dostaw i korzystać z zalet zamawiania ich drogą elektroniczną. Pantellos, obecnie największa niezależna firma dostawcza, powstała wskutek współpracy 21 wielkich firm.
Eksploatacja	Systemy obsługi ruchu i awarii (WMS/OMS, Work/Outage Management System)	Firmy energetyczne w całej Ameryce Północnej, pod naciskiem konkurencji wymuszającej lepszą obsługę klientów i w obliczu zagrożenia „cenami proporcjonalnymi do jakości”, prześcigają się w instalowaniu systemów WMS/OMS. Ścisła integracja systemów WMS/OMS zapewnia krótszy czas reakcji, redukcję zatrudnienia i zwiększenie mocy produkcyjnych.

> **Luki w zabezpieczeniach sieci w branży energetycznej**

Wskutek powszechnego stosowania systemów SCADA do zarządzania siecią korporacyjną, firmy energetyczne stały się nieodporne na wewnętrzne i zewnętrzne ataki sieciowe. Ponieważ sieci korporacyjne i systemy SCADA są często połączone, zabezpieczenia systemu SCADA są tylko tak skuteczne, jak zabezpieczenia sieci korporacyjnej. Wskutek działań wymuszających zmniejszenie poziomu kontroli na rzecz szybkiego wdrożenia funkcji otwartego dostępu podatność sieci korporacyjnych na ataki gwałtownie wzrasta.

LUKI W ZABEZPIECZENIACH ZAGRAŻAJĄ NIE TYLKO SYSTEMOM SCADA

Elektroniczne formy prowadzenia działalności rozwijają się błyskawicznie i znajdują coraz więcej zastosowań. W wielu firmach energetycznych systemy rozliczeniowe i księgowe są scalane z innymi korporacyjnymi systemami informatycznymi. Ponadto fuzje i nowe dziedziny działalności podejmowane w firmach energetycznych wymuszają pospieszne scalanie różnorodnych przestarzałych systemów bez rozważenia wpływu takich operacji na bezpieczeństwo. Wszystko to zwiększa liczbę luk w zabezpieczeniach i wagę płynących stąd zagrożeń. Zagadnienia bezpieczeństwa danych w branży energetycznej w coraz mniejszym stopniu dotyczą eksploatacji, a w coraz większym – elektronicznych łączów komunikacyjnych i internetowych.

Firmy energetyczne zaczynają już sobie zdawać sprawę, że są wystawione nie tylko na zagrożenia bezpieczeństwa systemów informatycznych związane z przesyłem i dostawą prądu. Nowe zagrożenia wiążą się przede wszystkim z rozwojem zaawansowanych systemów obsługi klientów (CIS) i elektronicznych metod obsługi dostaw. Dochodzi do tego podejmowanie nowych rodzajów działalności, wymagające integracji przestarzałych systemów, co wprowadza dodatkowe, całkiem nowe zagrożenia bezpieczeństwa.

> Możliwe skutki złamania zabezpieczeń

Zagrożeniem najczęściej spędzającym sen z powiek prezesów firm energetycznych jest możliwość przerwania ciągłości dostaw energii. Naciski ze strony rządu i odbiorców sprawiły, że firmy energetyczne zainwestowały sporo pieniędzy w metody polepszania niezawodności i ciągłości dostaw energii. Luki w zabezpieczeniach sieci od początku stanowiły zagrożenie dla niezawodności sieci energetycznej. Rozpowszechnienie systemów SCADA, do których można uzyskać dostęp zdalny, wdrożenie elektronicznych metod prowadzenia działalności oraz pospieszna integracja przestarzałych systemów znacząco zwiększyły liczbę możliwych luk w systemie. Zarazem podobnie zwiększyły się potencjalne koszty usuwania skutków złamania zabezpieczeń. Poniższa tabela zawiera zestawienie negatywnych skutków złamania zabezpieczeń w systemach firm energetycznych.

Możliwe skutki złamania zabezpieczeń

Przerwanie dostaw	W branży energetycznej nie ma nic ważniejszego niż niezawodne i ciągłe dostawy prądu do sieci. W firmach tych konieczna jest nieustanna czujność, gdyż złamanie zabezpieczeń systemu nadzorczego sieci energetycznej i systemu SCADA może doprowadzić do przerwania przesyłu energii. Systemy te były niegdyś w dużym stopniu odizolowane od sieci ogólnodostępnych, ale umożliwienie zdalnego dostępu do funkcji zarządzania systemem SCADA w istotny sposób zwiększyło ich podatność na ataki z zewnątrz. Ilustracją mierzonego pieniędzmi kosztu przerw w dostawach prądu niech będzie niedawna 8-godzinna awaria w stanach Delaware, Maryland i Wirginia: tamtejsze firmy poniosły stratę w wysokości 30,8 mln USD.
Zaufanie do firmy	Konkurencja wymusiła większą koncentrację na obsłudze klientów. W związku z tym dane dotyczące nawyków związanych z użytkowaniem, dane rozliczeniowe i demograficzne są niezwykle ważne dla strategii zarządzania relacjami z klientami w firmach energetycznych. Przerwa w ciągłości działania systemów obsługi klientów może spowodować osłabienie troskliwie pielęgnowanych więzi z klientami i poderwanie zaufania klientów w dłuższej perspektywie. W związku z tym firmy energetyczne muszą być w stanie zagwarantować bezpieczeństwo danych klientów, a punkty kontaktu z klientami, takie jak infolinie i witryny internetowe, muszą być odpowiednio zabezpieczone przed atakami DoS (powodującymi odmowę obsługi) i aktami „cyberwandalizmu”. Przykładem ilustrującym koszt w postaci utraty zaufania publicznego wskutek złamania zabezpieczeń niech będzie niedawne włamanie do sieci informatycznej brytyjskiej firmy Powergen. Nieco wcześniej firma Powergen przyznała, że błąd w zabezpieczeniach sieci spowodował publiczne udostępnienie danych rozliczeniowych ponad 7000 jej klientów. Do wszystkich tych klientów firma wysłała zawiadomienia i zaoferowała im odszkodowania w wysokości 50 funtów.
Reputacja firmy	Być może najważniejszym następstwem złamania zabezpieczeń systemów informatycznych w każdej firmie jest utrata reputacji. Wystarczy jedno włamanie, aby bezpowrotnie zniszczyć dobrą reputację i kondycję finansową firmy, zwłaszcza na rynku energetycznym, opartym od niedawna na silnej wolnorynkowej konkurencji. Ponieważ wielu inwestorów z uwagą przygląda się firmom energetycznym, działającym w nowych dla nich warunkach, ocena reputacji ma ogromne znaczenie dla oceny ryzyka inwestycyjnego i pociąga za sobą wahania notowań giełdowych. W ocenach ryzyka inwestycyjnego liczy się nie tylko cena akcji i wiarygodność kredytowa, lecz również to, w jaki sposób inwestorzy postrzegają jakość zarządzania firmą, włączając zdolność firmy do reagowania na działania konkurencji i inne zagrożenia rynkowe.

> Strategie zaradcze

Liczba zagrożeń bezpieczeństwa sieci gwałtownie wzrasta, a koszty naruszeń zabezpieczeń są coraz wyższe, zatem firmy energetyczne muszą opracować niezawodne procedury zabezpieczeń. Właściwe podejście do bezpieczeństwa sieci wymaga przede wszystkim rzetelnej oceny obecnych luk w zabezpieczeniach i oceny samej architektury zabezpieczeń sieciowych. Kierownictwo firm energetycznych musi być przede wszystkim świadome ograniczenia możliwości swojej firmy w dziedzinie bezpieczeństwa sieciowego i w razie potrzeby zasięgnąć konsultacji w firmach wyspecjalizowanych. Kolejne kroki działań zabezpieczających przedstawione na następnych stronach doskonale świadczą o tym, jak ogromne jest zapotrzebowanie na produkty i usługi zabezpieczające w branży energetycznej.

Najskuteczniejsze strategie zabezpieczeń informatycznych dla firm energetycznych to połączenie systematycznych, okresowych analiz stanu zabezpieczeń oraz ciągłej uwagi poświęcanej architekturze zabezpieczeń i monitorowaniu. Na następnych stronach wskazano najważniejsze działania, które powinna podjąć każda firma energetyczna, aby zmniejszyć liczbę i wagę przypadków naruszenia zabezpieczeń.

KROK 1: SYSTEMATYCZNE ANALIZY STANU ZABEZPIECZEŃ

Firmy energetyczne muszą przeprowadzać okresowe oceny stanu zabezpieczeń systemów i sieci informatycznych obsługujących najważniejsze procesy firmowe. Niestety, wiele firm energetycznych nie dokonuje systematycznych, okresowych ocen stanu zabezpieczeń systemów SCADA i EMS. Oprócz oceny zabezpieczeń systemów eksploatacyjnych należy wykonywać dodatkowe analizy stanu bezpieczeństwa sieci korporacyjnych, serwerów sieci WWW i systemów zarządzania relacjami z klientami. Rzetelna analiza może ujawnić nieoczekiwane luki w zabezpieczeniach, nieznane połączenia między sieciami publicznymi i prywatnymi oraz problemy z konfiguracją zapór ogniowych.

KROK 2: FACHOWY PROJEKT ARCHITEKTURY ZABEZPIECZEŃ INFORMATYCZNYCH

Firmy energetyczne mają do wyboru ogromną liczbę technologii zabezpieczeń, urządzeń sieciowych i opcji konfiguracji. Co prawda zapory ogniowe, systemy wykrywania włamań (IDS) i wirtualne sieci prywatne (VPN) są stworzone do ochrony sieci i danych przed atakami, ale nieprawidłowa konfiguracja lub zły dobór środków zabezpieczających wystarczą, by drastycznie zmniejszyć skuteczność zabezpieczeń.

Często zdarza się, że firmy wydają krocie na znakomite zabezpieczenia, które jednak nie zdadzą się na nic – tylko dlatego, że zostały nieprawidłowo zainstalowane i źle skonfigurowane. Aby zmniejszyć zagrożenia związane z niepoprawną architekturą sieci, firmy energetyczne powinny konsultować się ze specjalistami w dziedzinie zabezpieczeń informatycznych. Pozwoli to wykluczyć przypadki obniżenia bezpieczeństwa wskutek wprowadzania zmian w architekturze sieci.

KROK 3: ZARZĄDZANIE ZABEZPIECZENIAMI

Im więcej urządzeń zabezpieczających stosują firmy w swoich sieciach, tym trudniejsze staje się właściwe zarządzanie tymi urządzeniami i ich nadzorowanie. Poniższa tabela ilustruje fakt, że w większości wielkich firm urządzenia zabezpieczające rzadko bywają stosownie zarządzane i monitorowane. Niestety, samo wdrożenie rozwiązań technicznych przy braku ścisłego nadzorowania i zarządzania zapewnia administratorom systemu jedynie ograniczone zabezpieczenia (a nawet zmniejsza skuteczność urządzeń zabezpieczających). Ponieważ zatrudnienie doświadczonych fachowców w dziedzinie zabezpieczeń informatycznych do nadzoru nad urządzeniami zabezpieczającymi i zarządzania nimi jest zbyt kosztowne, wiele organizacji zleca te zadania wysoce wyspecjalizowanym firmom. Usługi zarządzania zabezpieczeniami zapewniają właściwą, aktualną konfigurację wszystkich urządzeń zabezpieczających, a zarazem monitorowanie faktycznej aktywności każdego urządzenia przy użyciu inteligentnych rozwiązań programowych i fachową ocenę podejrzanych działań. Usługi zarządzania zabezpieczeniami pozwalają firmom korzystać z monitorowania bezpieczeństwa w czasie rzeczywistym przy względnie niskim koszcie, a jednocześnie zwiększyć wartość stosowanych urządzeń zabezpieczających dzięki pełnemu wykorzystaniu ich faktycznych możliwości. W tabeli poniżej przedstawiono listę podstawowych korzyści płynących ze zlecenia zarządzania zabezpieczeniami wykwalifikowanym firmom specjalistycznym.

Korzyści ze zlecenia zarządzania zabezpieczeniami

Oplacalność	Zlecenie zarządzania zabezpieczeniami eliminuje konieczność rekrutacji i zatrudniania wykwalifikowanego personelu informatycznego – na co w ostatnich latach przeznaczana jest coraz większa część budżetu działów informatycznych.
Centralne monitorowanie urządzeń	Dużo wielkich i średnich organizacji używa wielu urządzeń zabezpieczających rozmieszczonych w różnych odległych geograficznie regionach. Nieustanne monitorowanie tych urządzeń z jednej lokalizacji jest zazwyczaj trudne lub niemożliwe. Zarządzane produkty zabezpieczające pozwalają organizacjom przekazywać dane z wszystkich urządzeń zabezpieczających do centralnej (obsługiwanej przez usługodawcę) lokalizacji i ich nieustanne monitorowanie i analizowanie w czasie rzeczywistym.
Zarządzanie uaktualnieniami i poprawkami	W wielu organizacjach dochodzi do przeoczenia często udostępnianych przez producentów poprawek i uaktualnień systemowych (poprawek do systemów operacyjnych, uaktualnień reguł zapory ogniowej itd.), wskutek czego mechanizmy zabezpieczające stają się nieodporne na nowe techniki hakerskie. Zarządzane produkty zabezpieczające gwarantują stosowanie wszelkich poprawek i uaktualnień natychmiast po ich udostępnieniu przez producentów.
Reagowanie na incydenty, dane umożliwiające podjęcie czynności prawnych	W wielu organizacjach, nawet po wykryciu destrukcyjnych działań włamywaczy, niezwykle trudno jest odnaleźć niezbędne dane wśród milionów wpisów zdarzeń i alertów. Zarządzane produkty zabezpieczające, normalizując dane generowane przez wszelkie urządzenia zabezpieczające, pozwalają z łatwością uzyskać dane identyfikujące typ i źródło destrukcyjnych działań, umożliwiające zgłoszenie przestępstwa i podjęcie działań prawnych przeciw napastnikom.
Inteligentne wspomaganie decyzji	Zarządzane produkty zabezpieczające przekazują dzienniki urządzeń zabezpieczających, raporty z działań i alerty do specjalnego mechanizmu analizy. Mechanizm ten wykrywa wzorce destrukcyjnych działań, które zostałyby przeoczone (lub zignorowane) przez zarówno niedoświadczony, jak i wykwalifikowany personel ds. zabezpieczeń. Funkcja wspomaganie decyzji nie dostarcza spóźnionych informacji o problemie, który już się zdarzył – pozwala ona organizacjom podejmować bezwzględne działania, które zapobiegają naruszeniu bezpieczeństwa.

FIRMA SYMANTEC – ŚWIATOWY LIDER W DZIEDZINIE TECHNOLOGII ZABEZPIECZEŃ INTERNETOWYCH – OFERUJE SZEROKI ZAKRES OPROGRAMOWANIA ORAZ URZĄDZEŃ ZABEZPIELAJĄCYCH SIĘĆ DLA UŻYTKOWNIKÓW INDYWIDUALNYCH ORAZ FIRM. FIRMA SYMANTEC JEST NAJWIĘKSZYM NA ŚWIECIE DOSTAWCĄ TECHNOLOGII OCHRONY ANTYWIRUSOWEJ, ZAPÓR OGNIOWYCH, WIRTUALNYCH SIECI PRYWATNYCH, ZARZĄDZANIA LUKAMI W ZABEZPIECZENIACH, WYKRYWANIA WŁAMAŃ, FILTROWANIA TREŚCI INTERNETOWYCH I ZAWARTYCH W POCZCIE ELEKTRONICZNEJ, ZDALNEGO ZARZĄDZANIA ORAZ USŁUG ZABEZPIELAJĄCYCH DLA PRZEDSIĘBIORSTW. MARKA NORTON FIRMY SYMANTEC, KTÓRĄ OPATRZONE SĄ DETALICZNE WERSJE PRODUKTÓW ZABEZPIELAJĄCYCH, JEST ŚWIATOWYM LIDEREM POD WZGLĘDEM SPRZEDAŻY DETALICZNEJ ORAZ ZDOBYWCĄ NAJWIĘKSZEJ LICZBY NAGRÓD PRZYZNAWANYCH PROGRAMOM KOMPUTEROWYM. CENTRALA ŚWIATOWA FIRMY ZNAJDUJE SIĘ W CUPERTINO W KALIFORNII, USA, A JEJ FILIE DZIAŁAJĄ W 38 KRAJACH NA CAŁYM ŚWIECIE.

WIĘCEJ INFORMACJI MOŻNA ZNALEZĆ NA STRONIE [HTTP://ENTERPRISESECURITY.SYMANTEC.COM](http://ENTERPRISESECURITY.SYMANTEC.COM)

CENTRALA ŚWIATOWA
20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
+ 1 408 517 8000
+1 800 441 7234

SYMANTEC (POLSKA)
Al. Jana Pawła II 29
00-867 Warszawa
Tel. (22) 586 92 00
Faks (22) 654 69 69
www.symantec.pl

Firma Symantec ma biura w 38 krajach. Informacje o biurach i numery telefonów dla poszczególnych krajów można znaleźć w naszej witrynie internetowej: www.symantec.com

Informacje dotyczące obsługi klientów i pomocy technicznej można znaleźć w naszej witrynie internetowej: www.symantec.com/eusupport