

MAGAZYN INFORMACYJNY FIRMY ASCOMP S.A.

SECURIUSZ

NR 1 (23)

IT SYSTEMS SECURITY

Aktualności firmowe

Podpisane umowy:

- Zakłady Metalowe „MESKO”

dostawa i instalacja oprogramowania zabezpieczającego system informatyczny (węzeł dostępowy do Internetu)

- Zakłady Koksownicze „Przyjaźń”

dostawa i instalacja oprogramowania zabezpieczającego system informatyczny (węzeł dostępowy do Internetu)

- Fabryka Urządzeń Mechanicznych „KAMAX”

dostawa i instalacja oprogramowania zabezpieczającego system informatyczny (węzeł dostępowy do Internetu)

- Inteligo Financial Services

elementy systemu bezpieczeństwa

- Philip Morris Polska

system kontroli dostępu

- Sanofi Synthelabo oddz. Rzeszów

zintegrowany system bezpieczeństwa BMS

- Zelmer

biometryczny system kontroli dostępu dla ośrodka Informatyki

- Zakład Ubezpieczeń Społecznych

wdrożenie systemu filtracji stron www



Szanowni Państwo,

Securiusz to nasz nowy magazyn informacyjny poświęcony tematyce bezpieczeństwa systemów teletransmisyjnych oraz teleinformatycznych.

Na jego stronach postaramy się przedstawić Państwu najnowsze trendy rozwoju bezpiecznych i niezawodnych systemów. Opiszemy rozwiązania proponowane przez producentów specjalizujących się w bezpieczeństwie danych i bezpiecznych systemach.

Na podstawie naszych wieloletnich doświadczeń zaprezentujemy najbardziej optymalne rozwiązania zarówno dla małych jak i dużych przedsiębiorstw.

W pierwszym numerze przedstawiamy m. in. rozwiązania firmy Secure Computing i Internet Security Systems, budowę bezpiecznego dostępu do Internetu, systemy antywirusowe oraz porównanie sprzętowych rozwiązań VPN.

Mam nadzieję, że Securiusz okaże się interesującą lekturą i znajdą Państwo czas na zapoznanie się z treścią kolejnych wydań.

Ponieważ jest to nasza pierwsza edycja bardzo miło nam będzie, jeżeli zechcą Państwo podzielić się swoimi uwagami oraz oczekiwaniami. Informacje proszę przesyłać na adres securiusz@ascomp.com.pl.

Życzę miłej lektury.

Z poważaniem
dr inż. Andrzej Szymowski
Prezes ASCOMP S.A.



Nowa koncepcja bezpiecznej sieci teleinformatycznej **Secure Harbour** firmy Enterasys zaprezentowana na seminarium 8 i 9 grudnia 2001 r. w Myczkowcach.

(więcej informacji na str. 16)



Zbigniew
Grabis,
Cenzor
Naczelny

Kim jest Securiusz?

Po prostu młodszym bratem Fibro-niusza! Tak, tak – nie zastępuje ani też nie odsyła na emeryturę krzepkiego wciąż organu Partii Zaawansowanych Usług Sieciowych (w skrócie PZUS – podobieństwo do innych znanych skrótów jest dziełem najczystsze, jak onegdaj spirytus do czyszczenia przewijaków, przypadku). Co więcej, sama Partia trzyma się dzielnie, usługi zaawansowane w sieciach krzewi, a jej ludziom żyje się coraz dostatniej. WHAT'S UP ?!!!! można by zakrzyknąć cytując naszych przyjaciół Moskali – kto za tym wszystkim stoi ? (to już cytat z innego pamiętnego źródła). Odpowiedź jest równie oczywista jak jej historyczne analogie – stoją za tym Siły Bezpieczeństwa (skrótów wołę tym razem nie przywoływać), które wspierają Partię w działaniu dając jej niezbitą pewność tego, iż na straży jedynie słusznych idei (czytaj: danych) stoją prawdziwi fachowcy. Ci ostatni do tego stopnia powiększyli ostatnio w naszym firmowym państwie swoje wpływy tudzież rozszerzyli zestaw narzędzi oraz metod inwigilacji, że o przymusie bezpośrednim nie wspomnę, iż dało to realne podstawy do wydania niniejszego opatrzonego klauzulą tajne/poufne okólnika. Znając zawziętość autorów oraz podziwu godną nieustrasłość w śledzeniu i tępieniu w zarodku wszelkiej sieciowej nieprawomyślności, mogę z całkowitą pewnością zapewnić Państwa, którym ten egzemplarz Securiusza trafił do ręki, że nie będzie to numer nasz ostatni. Stojąc na straży pryncypiów i nienaruszalności naszych sieciowych granic (już nie na Odrze ale raczej na Sun-ie) chcemy, aby nasz Securiusz był trybuną, z której padać będą najcelniej i najrzetelniej słowa, które sprawią, że Wasza czujność będzie wzmożona, a świadomość określi byt zdolny oprzeć się czyhającym zewsząd zagrożeniom. Hasłem przewodnim naszych specjalistów ds. bezpieczeństwa jest: „Nie ufamy nikomu”, zawołanie Securiusza brzmi: „Nam możesz zaufać”. Możesz, bo musi to na Rusi, a w Polsce ...

**Securiusze wszystkich sieci
łączcie się !!!**

KT



**Początki współpracy
między Secure Computing
i ASCOMP S.A. sięgają roku
1998. W tym momencie
ASCOMP S.A. jako jedyna
firma w Polsce posiada
status Autoryzowanego
Partnera firmy
Secure Computing.**

Secure Computing jest światowym liderem na rynku dostawców produktów bezpieczeństwa dla e-businessu, dostarczając silną kontrolę dostępu, autentykację użytkownika oraz możliwość filtrowania zasobów WWW. Rozwiązania te można w łatwy sposób dostosować do wielkości i potrzeb klienta. Baza klientów Secure Computing zawiera firmy z listy Fortune 50, agencje rządowe oraz dostawców usług internetowych i aplikacji.

Firma Secure Computing zaczęła swoją działalność jako dział bezpieczeństwa firmy Honeywell. Przez lata jej inżynierowie opracowali wiele nowych technologii i standardów podnoszących bezpieczeństwo informacji. W 1995 roku Secure Computing wprowadziła na rynek pierwszy prawdziwie bezpieczny firewall – Sidewinder. Następnie uzupełniła swoją ofertę o rodzinę produktów do silnej autentykacji – SafeWord Family oraz system filtrowania zawartości stron WWW.



SAFEWORD[®]
PREMIERACCESS[®]

Każdy administrator odpowiadający za działanie i bezpieczeństwo korporacyjnej sieci ma nie mały problem do rozwiązania. Musi zdefiniować użytkowników mających uprawnienia do: korzystania z Internetu, dostępu do sieci wewnętrznej poprzez VPN lub dialup, strony WWW dla partnerów, wykorzystywanych w firmie aplikacji oraz oczywiście systemów operacyjnych. Podczas przydzielania tych uprawnień okazuje się, że wiele z tych systemów wykorzystuje bazy użytkowników, które ze sobą nie współpracują. Tak więc zarządzanie na poziomie całej korporacji staje się bardzo uciążliwe, co skutkuje zwiększeniem prawdopodobieństwa popełnienia błędu przez administratora. Problem się pogłębia, oprócz mnogości systemów i aplikacji, w sieci korporacyjnej istnieje kilka sposobów autentykacji takich jak np. hasła dynamiczne, hasła statyczne, certyfikaty cyfrowe. Zarządzanie takim systemem staje się prawdziwym wyzwaniem dla każdego działu IT.

Istnieje jednak rozwiązanie tego problemu – SafeWord PremierAccess firmy Secure Computing. Jest to pierwszy na świecie produkt umożliwiający w pełni zintegrowane zarządzanie kontrolą dostępu.

Wdrożenie systemu SafeWord PremierAccess w sieci korporacyjnej umożliwi:

- zarządzanie wszystkimi punktami dostępu do zasobów za pomocą jednego zintegrowanego narzędzia,
- kontrolowanie kto i gdzie może się udać, wykorzystując elastyczne narzędzie do autoryzacji opartej na przypisanych do każdego użytkownika rolach,
- zabezpieczenie każdego serwera WWW, wraz z zarządzaniem sesjami, personalizacją zawartości oraz Single Sign-On,

Silna autentykacja, autoryzacja oraz zarządzanie uprawnieniami użytkowników na poziomie całej korporacji

- oszczędność czasu administratorów poprzez rozwiązanie User-Self-Enrollment,
- elastyczną rozbudowę od kilkudziesięciu użytkowników do milionów,
- wykorzystanie technologii Authentication Broker aby rozszerzyć możliwości autoryzacji oraz zintegrować z istniejącą infrastrukturą np. ActiveDirectory lub innymi systemami wykorzystującymi tokeny.

Silne uwierzytelnianie – serwer AAA

SafeWord PremierAccess umożliwia silną autentykację i autoryzację. Udostępniając pełną gamę narzędzi do autentykacji daje administratorowi działu IT możliwość dostosowania autentykacji do wymagań polityki bezpieczeństwa firmy. Należy zwrócić uwagę na różnorodność sposobów autentykacji. Istnieje również możliwość łączenia kilku autentykatorów (np. certyfikat cyfrowy i hasło) w celu podniesienia poziomu bezpieczeństwa. Dzięki tej właściwości Oficerowie Bezpieczeństwa lub Administratorzy, mając do dyspozycji szeroką gamę autentykatorów, mogą zdefiniować i sprecyzować jak mocna autentykacja jest potrzebna przy dostępie do poszczególnych zasobów. W ten sposób użytkownikowi logującemu się do systemu wystarczy token, natomiast przy korzystaniu z aplikacji bazodanowej oprócz tokenu musi jeszcze wpisać hasło statyczne. Idąc dalej wszystkie konta administratorów można chronić łącząc token z identyfikacją biometryczną.

Sposoby autentykacji:

- Hasło
- Token
- SofToken –Windows
- SofToken – Palm
- SofToken – Ericsson
- Smart Card
- Certyfikat cyfrowy
- Cechy biometryczne
- Token USB

Zarządzanie – profile użytkowników

Każdy użytkownik znajdujący się w systemie jest przydzielany do pewnych profili – np. Dyrektor działu Sprzedaży ma przypisane profile: pracownika, sprzedawcy i kadry zarządzającej. W ten sposób może korzystać z zasobów i danych, które są dozwolone dla tych trzech profili. Do każdego profilu przypisane są odpowiednie listy praw dostępu (ACL), definiujące uprawnienia użytkowników mających przypisany dany profil. Całość znajduje się w jednej bazie danych. Warto tutaj zaznaczyć, że ACL definiują prawa dostępu do różnego rodzaju zasobów tj. połączenie do sieci poprzez VPN, dostęp do aplikacji, systemów operacyjnych. Tym samym osiągamy centralnie zarządzaną kontrolę dostępu w sieci teleinformatycznej. Administrator musi uaktualniać informacje o użytkowniku tylko w jednej bazie danych.

Współpraca z istniejącymi rozwiązaniami

PremierAccess umożliwia zintegrowanie rozwiązań wielu producentów w jednolite zarządzanie i zabezpieczoną strukturę. Współpracuje z rozwiązaniami VPN firmy Check Point, Cisco, Alcatel, Microsoft, aplikacjami Citrix, Oracle, serwerami WWW, wszystkimi popularnymi systemami operacyjnymi.

Dzięki zastosowaniu nowoczesnych technologii PremierAccess może zintegrować zaimplementowane wcześniej systemy autentykacji i autoryzacji oparte np. na standardzie RADIUS, ActiveDirectory lub ACE/Server. W ten sposób można wyko-

rzystać wcześniej wdrożone systemy w budowie systemu centralnego zarządzania kontrolą dostępu do danych lub zasobów.

Zabezpieczenie dostępu do serwerów WWW

Firma Secure Computing opracowała uniwersalnego agenta dla serwerów WWW. Premier Access umożliwia kontrolę dostępu połączoną z silną autentykacją do umieszczonych na serwerze zasobów, personalizację zawartości oraz zarządzanie sesją. Wszystko to może być dokonane niezależnie od typu serwera WWW.

Self Enrollment

Odwiecznym problemem administratorów IT jest konieczność wprowadzania dużej ilości informacji o użytkownikach do baz danych. PremierAccess posiada zaimplementowane rozwiązanie umożliwiające przeniesienie większości pracy na użytkownika, który chce być wprowadzony do systemu. To rozwiązanie nazywa się Self Enrolment Server i jest częścią systemu PremierAccess. Self Enrollment Server ogranicza pracę administratora do przygotowania rezerwacji miejsca w bazie dla takiego użytkownika. Przeprowadzając rezerwację generuje hasło, dzięki któremu użytkownik będzie mógł wpisać się do systemu i przypisuje użytkownikowi odpowiedni profil. Następnie wysyła do użytkownika np. token wraz z hasłem umożliwiającym zapis. Użytkownik przy pierwszym logowaniu wprowadza wszystkie swoje dane, aktywuje token, a następnie już normalnie może pracować w systemie.

*Krzysztof Tyl
Specjalista ds. Bezpieczeństwa
ASCOMP S.A.*



Budowa bezpiecznego węzła dostępowego do Internetu

W dobie narastających zagrożeń płynących z sieci Internet konieczne wydaje się opracowanie w instytucji pragnącej zabezpieczyć się przed takimi niebezpieczeństwami spójnej koncepcji ochrony sieci lokalnej przed intruzami.

Równie ważne jest, aby dostrzec zagrożenia w sieci wewnętrznej i odpowiednio zabezpieczyć zasoby przed niepowołanym dostępem czy zniszczeniem. Ponieważ luki w poszczególnych zabezpieczeniach są ogólnie znane, dla zdolnego hakera przejście przez niewystarczające zabezpieczenia staje się coraz mniejszym problemem. Dlatego też najlepszym wyjściem jest podejście kompleksowe, ujmujące bezpieczeństwo w ramy spójnego systemu, obejmującego kilka rodzajów zabezpieczeń. W tym artykule przedstawię, w jaki sposób można uzyskać naprawdę wysoki poziom bezpieczeństwa stosując wiele różnych rozwiązań z tej dziedziny. Jednak w praktyce możliwe jest dochodzenie do takiego stanu bezpieczeństwa stopniowo, etapami rozbudowując swoją infrastrukturę. Za takim postępowaniem mogą przemawiać zarówno względy organizacyjne, jak i ekonomiczne.

Spróbujmy najpierw rozważyć aspekt sprawy związany z zabezpieczeniami przed zagrożeniami zewnętrznymi. Zaliczyć należy do nich nie tylko nieautoryzowany dostęp do danych czy ich modyfikacja, ale również szkody mogące wystąpić w przypadku zainfekowania naszej sieci wirusem. W przypadku konieczności

zapewnienia zdalnego dostępu do naszej sieci z zewnątrz, czy to przez pracowników, czy partnerów, konieczne jest zastosowanie technologii wirtualnych sieci prywatnych (VPN). Ponieważ w ten sposób niejako otwieramy furtkę dostępu do naszej sieci, należy zadbać o właściwą autentykację i autoryzację użytkowników uprawnionych do takiej drogi dostępu do sieci wewnętrznej. W Internecie znaleźć można dziesiątki stron z informacjami o lukach w poszczególnych systemach bezpieczeństwa, łącznie z lukami firewalli. Dobrze zabezpieczona sieć powinna więc być zaopatrzona w dwa firewalle, spełniające różne funkcje, co wiele firm stosuje z doskonałym skutkiem. Zasada dublowania rozwiązań bezpieczeństwa sprawdza się także w przypadku kontroli antywirusowej – stosuje się dwa oddzielne produkty do kontroli antywirusowej, jedno do ochrony komputerów stacjonarnych czy serwerów, inne do kontroli ruchu sieciowego. Innym poważnym problemem, szczególnie ważnym w przypadku sieci wymagających stałego dostępu jest zapewnienie stałej i bezawaryjnej pracy posiadanych zabezpieczeń. Pomagać nam tu będą klastry serwerów, firewalli, czy redundantne elementy sieci.

Z drugiej strony nie należy lekceważyć zagrożeń płynących z wnętrza organizacji, od jej pracowników oraz innych osób mających dostęp do zasobów sieci. Dlatego też w bezpiecznej infrastrukturze zadbać należy o wykorzystanie systemów automatycznego wykrywania włamań i nadużyć, lokalnych skanerów antywirusowych oraz sprawnego systemu autoryzacji i autentykacji użytkowników w całej organizacji.

Postaram się przybliżyć Państwu sposób logicznej rozbudowy systemu zabezpieczeń w oparciu o produkty

będące w sprzedaży w firmie ASCOMP S.A. Nasza firma dąży do tego aby mieć w ofercie możliwie najpełniejszy zakres produktów z dziedziny bezpieczeństwa, dbając równocześnie o to, by w możliwie najlepszy sposób współpracowały one ze sobą.

Etap Pierwszy – początek

W pierwszym etapie budowy systemu informatycznego zwrócić należy uwagę na właściwe rozpoznanie potrzeb i wymagań naszej organizacji. Wiele rozwiązań bezpieczeństwa, zawartych w popularnych produktach jest niewykorzystywane, gdyż nie ma takiej potrzeby. Tak więc najważniejsze wydaje się właściwe zaplanowanie i stworzenie koncepcji sposobu ochrony naszej sieci. Należy przemyśleć gdzie w całej strukturze umieszczone zostaną najważniejsze informacje czy serwery, które należy szczególnie chronić. Należy przemyśleć pod kątem przyszłych potrzeb organizacji zastosowanie rozwiązań VPN. Zwrócić należy uwagę na ilość potrzebnych interfejsów firewalla, które będą konieczne do wykorzystania obecnie i w przyszłości, tak by kupując odpowiednią platformę mieć możliwość rozbudowy. Kiedy już taka koncepcja powstanie można przystąpić do implementacji rozwiązań mających wcielić naszą koncepcję w życie.

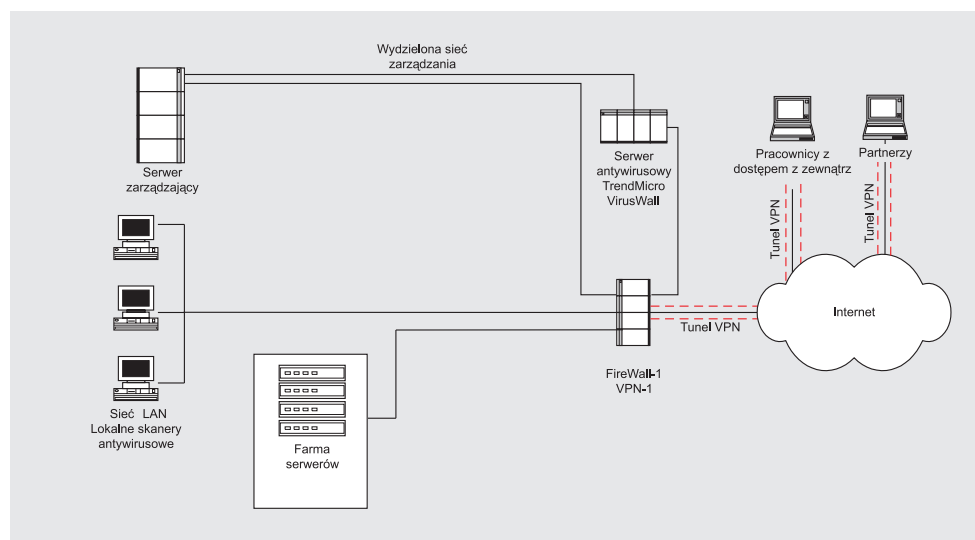
Podstawowym elementem systemu zabezpieczeń jest firewall, który może jednocześnie pełnić funkcję szyfratora VPN. Ważne jest, by już na tym etapie zdecydować się, czy ta funkcjonalność jest nam potrzebna, czy też nie, gdyż można w ten sposób zaoszczędzić sobie zbędnych wydat-

Etap Drugi – rozbudowa

Organizacje posiadające już zbudowany system bezpieczeństwa oparty na firewallu i kontroli antywirusowej często poszukują rozwiązań, które dodatkowo wzmocnią posiadane przez nich zabezpieczenia. W tej sytuacji logicznym uzupełnieniem systemu jest zaimplementowanie w miejscu styku sieci wewnętrznej z Internetem systemu automatycznego wykrywania włamań i nadużyć – IDS

np. ISS Real Secure. System ten, posiadając pewną bazę wzorców ataków, dokonuje sprawdzenia całego ruchu sieciowego pod kątem zgodności z sygnaturami ataków i nadużyć, po czym po wykryciu takich wykonuje akcje zdefiniowane przez administratora systemu. Sensory tego systemu instaluje się we wrażliwych miejscach sieci oraz na serwerach narażonych na ataki.

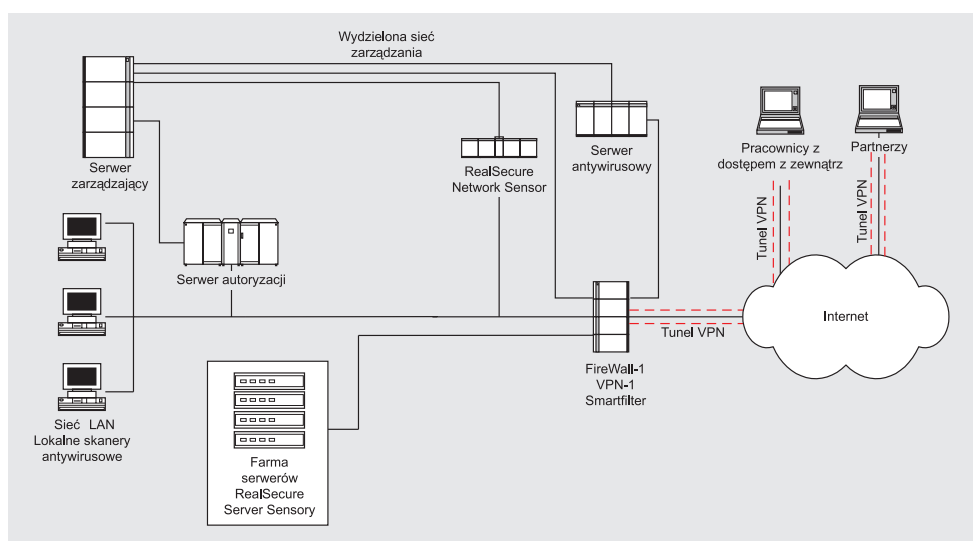
Innym rozwiązaniem, mającym zdecydowanie pozytywny wpływ na bezpieczeństwo systemu teleinformatycznego jest zastosowanie systemu jednorazowych haseł, najlepiej połączonego ze zintegrowanym systemem przydzielania uprawnień, oraz rozliczania użytkowników z ich działań (postępków) w sieci. Systemem takim jest SafeWord firmy SecureComputing. Jego działanie polega (w du-



ków w przyszłości. Pamiętać należy również, iż generowanie tuneli VPN jest zajęciem bardzo obciążającym firewall, dlatego w przypadku planowania wykorzystania tego rozwiązania rozważyć należy zakupienie mocniejszej platformy sprzętowej pod software firewalla. Innym rozwiązaniem jest zainstalowanie specjalnej karty akcelerującej szyfrację, lub zastosowanie w tym celu odrębnych szyfratorów.

W naszym przykładzie zastosowaliśmy jako firewall rozwiązanie firmy Check Point – FireWall-1/VPN-1. Na poszczególnych interfejsach jego platformy stworzone zostały strefy o różnym poziomie bezpieczeństwa – sieć wewnętrzna, farma serwerów i sieć zarządzania. Dodatkowo, na osobnym interfejsie podłączony został serwer antywirusowy, w naszym przypadku TrendMicro VirusWall, którego zadaniem jest badanie ruchu http, ftp i poczty pod kątem mogących w nim wystąpić wirusów, koni trojańskich, złośliwych elementów ActiveX, itp. Na stacjach roboczych zainstalowane zostało oprogramowanie antywirusowe innego producenta (np. Symantec Norton Antivirus Corporate Edition). Sieć zarządzania tworzy zamknięty obieg, poprzez który możliwe staje się administrowanie wszystkimi elementami systemu bezpieczeństwa, przy czym

została ona fizycznie oddzielona od sieci wewnętrznej, dla uzyskania lepszej ochrony przed zagrożeniami. W naszym przypadku występuje tylko jeden serwer zarządzający, jednak może być to oczywiście grupa serwerów w zależności od potrzeb. Dzięki zastosowaniu rozwiązania CheckPoint VPN-1 możliwe jest ustanowienie tuneli VPN pomiędzy komputerami pracowników mających prawa do zdalnego dostępu oraz przez partnerów firmy do udostępnionych danych wewnątrz strefy serwerów (de facto DMZ). Taka konfiguracja systemów bezpieczeństwa tworzy nam standardowe rozwiązanie bezpieczeństwa, które do czasu uzyskania funduszy może wystarczyć do skutecznej ochrony sieci.

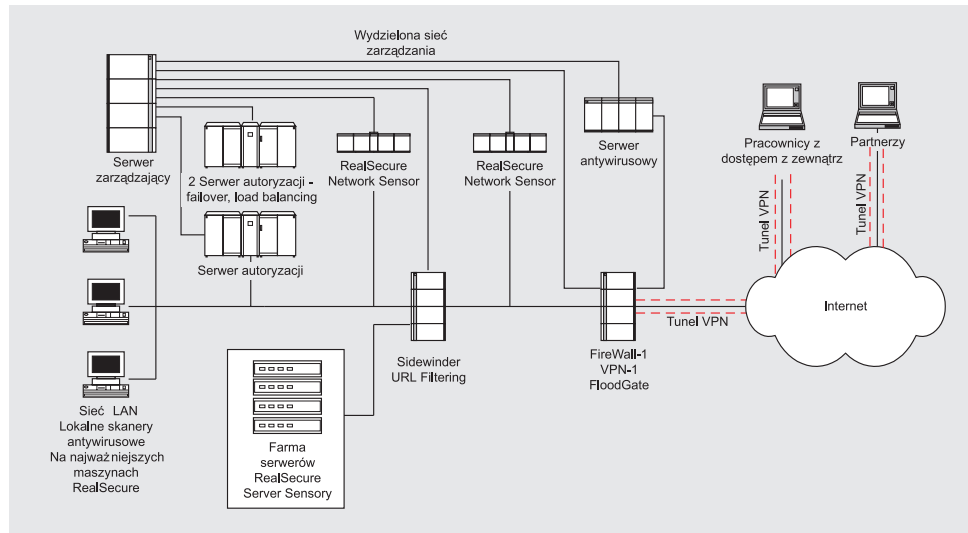


zym skrócie) na zintegrowaniu wszystkich uprawnień do poszczególnych elementów sieci w jednej wspólnej bazie a następnie, w oparciu o nią, przydzielaniu praw do usług po spełnieniu określonych warunków. Możliwe jest oczywiście przydzielanie poszczególnym użytkownikom różnych uprawnień, zależnie od ich pozycji w firmie, a także określanie dla nich wymaganego poziomu bezpieczeństwa. Niektórzy autoryzować muszą

godzinnych wycieczek po sieci w poszukiwaniu treści często nie całkiem związanych z wykonywaną przez nich pracą. Oprogramowanie Smartfilter posiada szeroką, na bieżąco uaktualnianą bazę stron zawierającą strony skategoryzowane w wiele grup związanych z różnymi dziedzinami, np. samochody, sex, internet banking. Nad aktualizacją tych stron pracuje zespół ludzi, również polskojęzycznych, którzy zajmują się przeszukiwaniem Internetu.

stwach ISO/OSI, taki jak Sidewinder firmy Secure Computing. Strefy o różnym stopniu zaufania przenosimy na drugi firewall, przez co dodatkowo odciążamy nasz podstawowy element systemu bezpieczeństwa.

Drugim rozwiązaniem mogącym usprawnić system teleinformatyczny jest zainstalowanie modułu sterowania pasmem na pierwszym firewallu. W przypadku CheckPointa jest to moduł FloodGate. Po jego zainstalowaniu zna-



cząc wzrasta stopień wykorzystania dostępnego pasma transmisji. Można także zastanowić się nad zastosowaniem mechanizmów load balancing'u – czy to z wykorzystaniem oprogramowania CheckPoint, czy też za pomocą stworzonego do tego celu programowania lub specjalizowanych maszyn. Zasadne jest również przewidzenie konfiguracji dwóch firewalli tego samego producenta, umożliwiające w razie awarii przełączenie na działającą maszynę całego ruchu – failover. W przypadku posiadania dostępu poprzez VPN zasadne może być również zainstalowanie specjalnej karty szyfrującej/desyfrującej ruch VPN, co znacznie odciąża sam firewall.

się jedynie hasłem, inni tokenem, jeszcze inni za pomocą innych metod, np. biometrycznych. Jednocześnie system zapisuje w logu działania użytkowników, które miały miejsce w sieci. Ponieważ w przypadku zastosowania takiego rozwiązania wszystkie elementy sieci są niejako uzależnione od działania tego serwera, silnie zalecane jest zastosowanie mechanizmu fail-over dostępnego w tym produkcie w celu zapobieżenia nieprzewidzianym trudnościom w razie awarii serwera autoryzującego. Przy naprawdę dużej ilości użytkowników możliwa jest również konfiguracja load balancing, w której serwery pracujące równolegle rozdzielają między siebie równe części autoryzowanego ruchu. Takie rozwiązania można jednak zastosować już po wdrożeniu drugiego etapu.

Innym produktem przydatnym w tworzeniu zintegrowanego systemu bezpieczeństwa jest Smartfilter firmy Secure Computing. Jest to oprogramowanie wymuszające pewną kulturę pracy z Internetem. Zmora wielu firm są pracownicy dokonujący wielo-

Po zaimplementowaniu tych produktów nasza sieć jest zabezpieczona w sposób stojący na wysokim, światowym poziomie. Właściwie pozostało nam już tylko dokonanie kilku niezbędnych szlifów.

Etap Trzeci – ostatnie starcie (końcowa rozbudowa)

Przy poziomie zabezpieczeń, jaki uzyskaliśmy po zaimplementowaniu rozwiązań opisanych w poprzednich dwóch rozdziałach pozostaje nam już tylko dokonanie kilku usprawnień by mieć system bliski ideałowi. Jedną z takich rzeczy jest zaimplementowanie drugiego firewalla, najlepiej innego producenta niż pierwszy, tak by mieć podwójne zabezpieczenie przed zdolnymi hackerami. Jednocześnie dzięki takiemu rozwiązaniu można nieco odciążać firewall poprzez przeniesienie np. Smartfiltera na drugą maszynę. Można tu zastosować firewall działający na wszystkich war-

Aby zabezpieczyć nie tylko serwery dostępne z wnętrza sieci, ale także ważniejsze stacje robocze zalecane jest zainstalowanie na nich oprogramowania firmy ISS do ochrony desktopów. Gromadzone przez nie dane trafiają do wspólnego systemu z Network Sensorami oraz Server Sensorami zainstalowanymi na serwerach i tworzą spójny obraz nieuprawnionych działań podejmowanych w sieci wewnętrznej.

Po zaimplementowaniu takich rozwiązań, jakie opisałem w tym artykule stajemy się dumnymi posiadaczami znakomicie zabezpieczonej sieci i możemy śmiało pograć się w lekturze najnowszej prasy informatycznej, nie obawiając się o bezpieczeństwo danych (lub obawiając się umiarkowanie) oddanych pod naszą opiekę.

Milosz Franaszek
Specjalista ds. Bezpieczeństwa
ASCAMP S.A.



Koncepcja

Secure

Harbour

– nowe

spojrzenie firmy

**Enterasys
Networks**

na bezpieczeństwo sieci



Firma Enterasys Network, (firma ASCOMP posiada tytuł Enterasys Networks Elite Partner) opublikowała nową koncepcję podejścia do zagadnień bezpieczeństwa, którą pragnie zaimplementować w swoich produktach. Elementem tej koncepcji jest oprogramowanie typu Intrusion Detection System – Enterasys Dragon. Jest to system składający się z trzech elementów – serwera, sondy host-based, oraz network-based. Sonda typu network-based o nazwie Dragon Sensor posiada kilka funkcji, które dla użytkowników są nie do przecenienia. Zapewnia wydajność znacznie przekraczającą 100Mbps, analizuje ruch sieciowy na dwa sposoby – wykrywając anomalie, a także porównując go z przechowywaną bazą wzorców ataków. Dzięki temu potrafi wykryć szeroką gamę ataków, od skanowania portów aż po działanie koni trojańskich. Drugim elementem systemu IDS jest Dragon Squire, sonda typu host-based. Działa ona poprzez analizowanie logów systemowych pod kątem nadużyć lub nieuprawnionego dostępu. Sprawdza także kluczowe pliki systemu, alarmując w momencie ich modyfikacji lub zniszczenia. Współpracuje z większością firewallei, działając na samym firewallu, lub analizując jego logi. Dzięki niewielkim wymaganiom zużywa znikomą część pracy procesora maszyny na której jest zainstalowany. Pracuje na wielu popularnych systemach operacyjnych, min. WinNT/2000, Solarisie, HP-UX, Linuxie, OpenBSD i FreeBSD.

PC

REALSECURE SITEPROTECTOR

nowa

wizja

bezpieczeństwa

firmy ISS

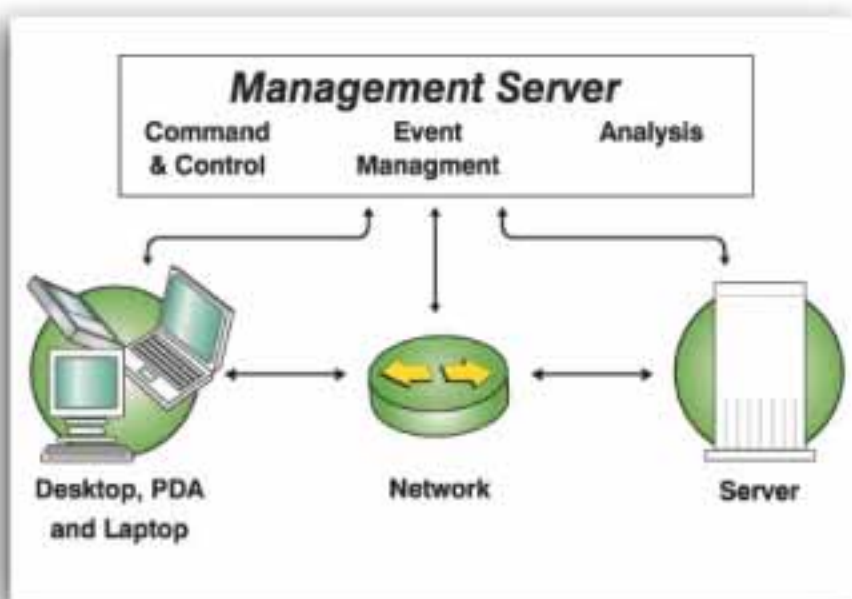


**INTERNET
SECURITY
SYSTEMS**

Firma ISS przedstawiła ostatnio nowy produkt mający poszerzyć możliwości pakietu RealSecure, pod nazwą SiteProtector. Jego funkcją jest gromadzenie informacji ze wszystkich dostępnych źródeł i korelowaniu ich ze sobą. Korelacja może odbywać się w czasie rzeczywistym lub w zadanych okresach czasu. Produkt umożliwia zarządzanie wszystkimi elementami systemu RealSecure ze wspólnej konsoli i przeznaczony jest do zastosowań w połączeniu z resztą komponentów systemu. Równocześnie z wprowadzeniem tego produktu firma ISS zmienia podejście do ochrony zasobów sieci przedsiębiorstwa. Produkty podzielone zostają na kategorie Network, Server oraz Desktop Protection. Z konsoli SiteProtectora można zarządzać wszystkimi produktami, łącznie z dokonywaniem

ich instalacji, konfiguracji i uaktualnienia. Korelacje zdarzeń w czasie rzeczywistym, dokonywane przez engine bazy MS SQL Server2000 mają pomóc oficerom bezpieczeństwa w dokonywaniu oceny bezpieczeństwa oraz w sytuacjach kryzysowych, wymagających natychmiastowych reakcji. Informacje gromadzone w systemie pochodzić mogą zarówno z systemu RealSecure, jak i ze źródeł zewnętrznych, jak np. logi routerów, firewallei, systemów operacyjnych. Zaimplementowanie w nowym produkcie największej dostępnej bazy danych wzorców ataków i nadużyć pozwala mieć nadzieję na uzyskanie przez niego popularności równej reszcie oprogramowania RealSecure.

MF



Bezpieczeństwo sieci w usłudze **Voice over IP**

*Obecnie
coraz większą
popularność
zyskuje usługa
przenoszenia głosu
poprzez sieć IP,
zwana VoIP.*

W skrócie polega ona na kodowaniu głosu i zamianie go na krótkie pakiety IP, które następnie przesyłane są poprzez standardową sieć IP. Aby możliwe było działanie całego systemu poprawnie muszą działać dwa jego podstawowe elementy. Pierwszym z nich jest centralny system sterowania, zwany GateKeeper, który zajmuje się utrzymywaniem ruchu poprzez kierowanie pakietów pomiędzy GateWay'ami, stanowiącymi drugi element systemu. Ich działanie polega na kodowaniu głosu i przesyłaniu go poprzez sieć IP do analogicznego urządzenia w żądanym miejscu przeznaczenia pakietów. Usługa ta jest jednak ze swej natury narażona na wiele niebezpieczeństw. Podstawowym problemem jest zabezpieczenie centralnego systemu sterowania usługą, gdyż jego bezproblemowe działanie jest warunkiem poprawnego funkcjonowania usługi. W przypadku jego awarii niemożliwe staje się przesyłanie pakietów pomiędzy GateWay'ami, co mogłoby spowodować upadek całego systemu, którego podstawowym działaniem jest przecież realizowanie natychmiastowych połączeń między tymi urządzeniami. Dlatego też dla ochrony GateKeepera wykorzystać należy wszystkie dostępne sposoby

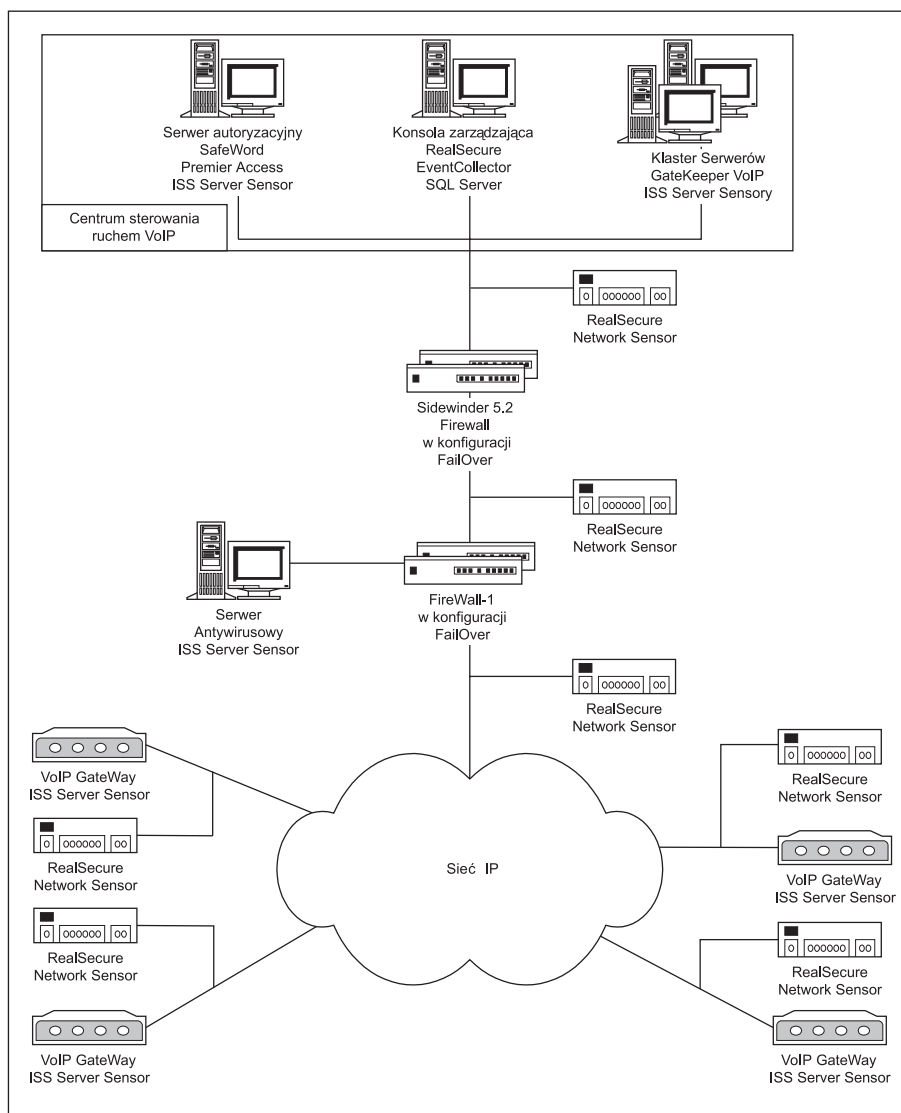
ochrony. Jeżeli zaś chodzi o bramki – GateWay'e, podstawową sprawą jest zapewnienie jak najkrótszego czasu propagacji dla pakietu przemierzającego naszą sieć. Dlatego też niemożliwe jest zastosowanie jakichkolwiek rozwiązań wprowadzających opóźnienie na drodze pakietów. Powoduje to, że niemożliwe jest przesiewanie ruchu dochodzącego do bramki w celu wyeliminowania niepożądanych zachowań użytkowników sieci. Co za tym idzie te właśnie maszyny są najbardziej podatnym na uszkodzenia elementem usługi VoIP. Na szczęście uszkodzenie pojedynczego GateWay'a nie powoduje zniszczenia całego systemu i jest ryzykiem możliwym do zaakceptowania. Oczywiście należy zastosować rozwiązania pomagające dostrzegać problem powstały w konkretnym punkcie systemu i umożliwiające jego wyeliminowanie. Nie można również zapominać o bardziej przyziemnym aspekcie ochrony – same urządzenia są kosztowne i łatwo poddają się uszkodzeniom fizycznym. W tym artykule postaram się przybliżyć Państwu projekt zabezpieczenia sieci VoIP, którego autorem jest firma ASCOMP, a który doskonale spełnia wszystkie przedstawione wyżej warunki.

Jako że najważniejszą sprawą jest zapewnienie bezpieczeństwa centralnemu systemowi zarządzania usługą VoIP, zacznijmy opis od zabezpieczeń tego właśnie elementu. Sam system został posadowiony na klastrze serwerów, z których każdy zaopatrzony jest w redundantne zasilacze i dyski w konfiguracji RAID. Ponieważ wraz ze wzrostem popularności tej usługi liczba jej użytkowników będzie się stopniowo powiększała przewidziane jest zastosowanie dodatkowo zew-

trnych macierzy dyskowych zapewniających wymaganą pojemność dyskową dla powiększającej się bazy danych użytkowników systemu. Podobne rozwiązanie przewidziane jest dla serwera autoryzacji znajdującego się w tym samym segmencie sieci, w centrum zarządzania ruchem VoIP. Jego zadaniem jest przechowywanie danych o uprawnieniach administracyjnych i operatorskich do systemu GateKeepera i bramek VoIP. W przypadku projektu firmy ASCOMP tą funkcję realizuje serwer SafeWord Premier Accesss firmy SecureComputing. Pozwala to na wykorzystanie różnych metod autentykacji – od zwykłych haseł, poprzez tokeny i SmartCard aż po techniki biometryczne. Dodatkowo, w celu zachowania bezpieczeństwa na wszystkich serwerach pracujących w sieci zainstalowano Server Sensory systemu RealSecure firmy ISS. Ich zadaniem jest monitorowanie ruchu sieciowego na interfejsach serwerów, oraz badanie zawartości logów systemowych i plików rejestru w poszukiwaniu śladów agresywnych zachowań mogących stanowić zagrożenie dla całego systemu i poszczególnych jego elementów. W bardzo niewielkim stopniu obciążają one procesor maszyny, na której są zainstalowane, jednocześnie znacząco zwiększając poziom bezpieczeństwa. Konsola zarządzająca tymi sensorami również znajduje się w centrum kierowania ruchem VoIP, które stanowi serce systemu. Pomiędzy centrum zarządzania a resztą sieci znajduje się zespół firewall'i dwóch różnych producentów – CheckPoint FireWall-1 sprawdzający ruch na niższym poziomie i zapewniający w połączeniu z serwerem antywirusową ochronę przed wirusami oraz SecureComputing Side-

winder Firewall dokonujący sprawdzenia ruchu przez niego przechodzącego aż do 7 warstwy modelu ISO/OSI. Dzięki temu zminimalizowane zostaje ryzyko przeniknięcia do centrum intruza z zewnątrz. Aby dodatkowo upewnić się co do posiadanych zabezpieczeń na wszystkich interfejsach firewalli zainstalowane są Network Sensory systemu RealSecure, zarządzane z tej samej konsoli co Server Sensory. Ich działanie polega na analizie ruchu przechodzącego przez chroniony fragment sieci i reakcji w razie wykrycia ataku lub nadużycia. Możliwe jest takie skonfigurowanie systemu, by automatycznie przerywane były podejrzane sesje lub na firewallu dokonywana była blokada jakichkolwiek połączeń z adresu budzącego podejrzenia. Dzięki takiej konfiguracji systemu bezpieczeństwa centrum kierowania ruchem VoIP staje się bastionem niezwykle trudnym do sforsowania. Nie należy również zapominać o zastosowaniu redundancji i konfiguracji fail-over routerów zapewniających nieprzerwane połączenie z siecią zewnętrzną. Jeżeli dodatkowo umiejscowione ono zostanie w miejscu zapewniającym fizyczne bezpieczeństwo cały system VoIP ma zapewnione działanie.

Jeżeli chodzi o zabezpieczenia zastosowane w celu wyeliminowania zagrożeń dla bramek VoIP, to pamiętając o zasadzie nie wnoszenia opóźnień do ruchu IP, możliwe jest jedynie zastosowanie metod biernego oczekiwania na atak i reakcji na niego, bez działań prewencyjnych, realizowanych za pomocą firewalla. Oczywiście jeżeli w infrastrukturze sieciowej istnieją firewalle, mogą one zostać wykorzystane do ochrony nowych jej elementów w postaci bramek VoIP. Nie jest jednak przewidziane dokładanie nowych zapór ogniowych. W zamian za to na wszystkich elementach systemu przewidziane jest zastosowanie Server Sensorów systemu RealSecure. Ich cechy pozwalają na uzyskanie częściowego działania firewalla – blokowania niektórych połączeń i zrywania sesji uznanych za niepożądane, oraz dokonywanie wpisów w logach lokalnych



oraz centralnej konsoli zarządzającej. W razie wykrycia ataku możliwe jest zastosowanie innych jeszcze dodatkowych czynności, które w założeniu mają umożliwić przywrócenie poprawnej pracy systemu. Dodatkowo, na interfejsach GateWay'ów prowadzących do sieci IP zainstalowane zostaną RealSecure Network Sensory, które monitorować będą wszystkie ramki przechodzące przez ten segment sieciowy i reagować na sytuacje zdefiniowane w ich polityce bezpieczeństwa w celu ograniczenia skutków ataku i ewentualnego wykrycia sprawcy nadużyć. Takie rozwiązanie pozwoli na zachowanie maksymalnego bezpieczeństwa przy równoczesnym zachowaniu szybkości przesyłania pakietów w sieci. Ważnym elementem systemu bezpieczeństwa jest również sam system

zarządzania usługami VoIP, którego działanie pozwala na zmiany konfiguracji bez potrzeby wyłączania całego systemu.

Opisany tutaj system bezpieczeństwa usługi VoIP odpowiada na potrzebę zapewnienia zabezpieczenia dla ruchu sieciowego o specyficznych właściwościach i jest stworzony specjalnie do tego celu. Jego autorem jest w całości firma ASCOMP S.A. W chwili obecnej gwarantuje on możliwie największy poziom zabezpieczeń.

Miłosz Franaszek
Specjalista ds. Bezpieczeństwa
ASCOMP S.A.

Grzegorz Cebula
Kierownik Zespołu Sprzedaży
Systemów Telekomunikacyjnych
ASCOMP S.A.

Sprzętowe rozwiązanie VPN

s z y f r a t o r y

Dla firm posiadających oddziały zamiejscowe, które nie są połączone z centralą za pomocą dedykowanych łącz, pragnących zachować poufność przekazywanych danych nieocenionym narzędziem są szyfrotory sprzętowe.

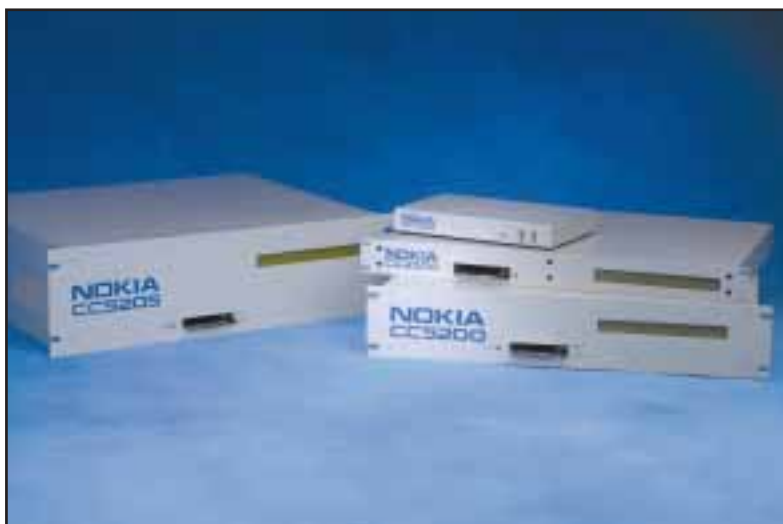
Dzięki takim urządzeniom bez specjalizowanego oprogramowania firewall możliwe jest stworzenie tuneli VPN pomiędzy centralą firmy a wysuniętymi placówkami, czy też pracownikami pracującymi na przenośnych komputerach. Kilku producentów sprzętu sieciowego posiada w swoim portfolio maszyny realizujące taką szyfrację. W ofercie firmy ASCOMP znajdują Państwo szyfrotory NOKIA CryptoCluster oraz Enterasys Aureoan.

Wszystkie maszyny NOKIA CC posiadają zintegrowane zdalne zarządzanie – darmowy software CryptoConsole (Windows NT/95/98, Solaris) z wbudowanym Certification Authority. Darmowy jest również klient VPN dla pojedynczych, mobil-

nych użytkowników - SafeNet (Windows 95, 98 and NT 4.0). NOKIA CC są w pełni zgodne ze standardami IPSec, PPTP i L2TP. Prócz tego obsługują translację adresów i portów NAT. Urządzenia posiadają dwa interfejsy Ethernet 10/100 (do sieci wewnętrznej, chronionej oraz do sieci zewnętrznej). Dodanie funkcjonalności VPN dla sieci polega więc po prostu na włączeniu urządzenia w istniejącą infrastrukturę. Naturalnym sposobem działania tych routerów jest klastr – z automatycznym przejęciem wszystkich aktywnych sesji i aplikacji w przypadku awarii któregoś z urządzeń (Active Session Failover), dynamicznym podziałem obciążenia (Dynamic Load Balan-

cing) i możliwością skalowania wydajności klastra przez dodawanie kolejnych urządzeń. Obie te możliwości nie wymagają specjalnych ustawień, są wpisane w działanie urządzeń. Dlatego też wszelkie parametry ustawia się dla klastra niezależnie od ilości urządzeń go tworzących. Na tych samych platformach z innym oprogramowaniem można zrealizować sprzętową akcelerację SSL.

Nokia CC500 to urządzenie przeznaczone do stosowania w małych i średnich firmach, oddziałach i zdal-



NOKIA

CONNECTING PEOPLE

nych biurach. Wydajność pojedynczego routera wynosi 6 MB/s ciągłego ruchu szyfrowanego 3DES z SNA-1, terminuje około 250 tuneli. Dodanie drugiego urządzenia do klastra podnosi wydajność do 12 MB/s. CC500 jest w pełni zgodny ze standardami IPSec, PPTP i L2TP. W przypadku modelu CC2500 wydajność szyfrowania wynosi 52 MB/s ciągłego ruchu 3DES z SNA-1, obsługuje około 1000 tuneli. Dodanie drugiego urządzenia do klastra podnosi wydajność do 87 MB/s. Jest to więc urządzenie mogące stanowić ciekawą propozycję dla średnich i dużych firm, banków ISP, (Internet Service Provider). CC5200 to urządzenia przeznaczone do stosowania w dużych firmach, centrach danych, centralach korporacji, bankach, ISP – wydajność pojedynczego routera wynosi 180 MB/s ciągłego ruchu szyfrowanego 3DES z SNA-1, obsługuje około 30 000 tuneli. Dodanie drugiego urządzenia do klastra podnosi wydajność do 360 MB/s. Dla tego samego grona klientów przeznaczony jest model CC5205 – jedyną różnicą w budowie tych modeli jest posiadanie przez ten ostatni 2 portów Gigabit Ethernet SX. W tym przypadku wydajność pojedynczego routera wynosi 220 MB/s ciągłego ruchu szyfrowanego 3DES z SNA-1, obsługuje około 30000 tuneli. Dodanie drugiego urządzenia do klastra podnosi wydajność do 440MB/s. Przy wybieraniu odpowie-

dniego do potrzeb szyfratora należy brać pod uwagę ilość przewidywanych zaszyfrowanych połączeń, oraz przewidywanego ruchu przez nie przechodzącego.

ENTERASYS NETWORKS™

Drugim producentem mającym w ofercie szyfratory sprzętowe jest **Enterasys Networks**. Jego rozwiązanie opiera się na dwóch rodzajach szyfratorów, w założeniu przeznaczonych dla małych lub dużych sieci czy klientów. Maszyną przeznaczoną na rynek SOHO jest seria Aureoran ANG-11xx. W jej skład wchodzi szyfratory ANG1102 oraz ANG1105, różnica między nimi polega na dołożeniu do modelu ANG1105 4-portowego huba 10/100 Ethernet oraz karty przyspieszającej szyfrowanie. Są one zarządzalne i konfigurowalne poprzez interfejs przeglądarki WWW, jednak ich instalacja jest niezwykle łatwa i nieskomplikowana. Maszyny te oferują przepustowość rzędu 3 Mb/s. Dla klientów wymagających nieco większych przepustowości przeznaczony jest produkt Aureoran ANG3000. Jego budowa pozwala na uzyskanie przepustowości rzędu 30 Mb/s. Dla otrzymania szyfrowania większego pasma niezbędne jest zastosowanie maszyny ANG7050, dzięki której możliwe jest przetworzenie 100Mb/s. Obydwa urządzenia zaopatrzone są w trzy porty Ethernet – zewnętrzny, wewnętrzny i zarządzający. Dodatkowym składnikiem

pakietu umożliwiającego tworzenie tuneli VPN jest serwer zarządzający Aureoran Policy Server 7000 lub 3000. Jego rolą jest centralne zarządzanie prawami dostępu do sieci, systemem ustawień bezpieczeństwa dla całego systemu VPN i poszczególnych jego elementów oraz kontrola profili użytkowników i grup. Aureoran Policy zarządza polityką bezpieczeństwa dla wszystkich klientów VPN i wymusza ich realizację przy każdorazowym logowaniu się do sieci. Posiada rozbudowany system raportowania, jego zarządzanie może odbywać się z poziomu przeglądarki WWW. Wszystkie maszyny Aureoran są zgodne ze standardami IPSec, PPTP z kodowaniem MPPE, ARCFour, DES, 3DES oraz autentykacją SHA1 lub MD5, wspierają Internet Key Exchange (IKE). Mogą współpracować z każdym standardowym systemem autentykującym RADIUS, wspierają dwuskładnikową autentykację (np. za pomocą tokenów).

Dla firmy pragnącej zbudować sieć VPN sprzętowe rozwiązania szyfrowane są dobrze ocenianą propozycją. Jako że wymagania firm rosną wraz z jej rozwojem należy przy projektowaniu takiej sieci wziąć pod uwagę przyszłe zapotrzebowanie na szyfrowane pasmo.

*Krzysztof Tyl
Specjalista ds. Bezpieczeństwa
ASCOMP S.A.*

Parametry	ANG1102 ANG1105	CC500	ANG3000	CC2500	ANG7050	CC5200	CC5205
Przepustowość dla pojedynczej maszyny	3 Mb/s	6Mb/s	30Mb/s	52 Mb/s	100 Mb/s	180 Mb/s	220 Mb/s
Przepustowość dla klastra dwóch szyfratorów	-	12 Mb/s	-	87 Mb/s	-	360 Mb/s	440 Mb/s
Liczba tuneli	-	250	500	1000	5000	1000 - - 30000	1000 - - 30000
Cena 1 urządzenia	750\$/870\$	1645\$	9800\$	10995\$	15000\$	84330\$	9166\$

S Y S T E M Y ANTYWIRUSOWE

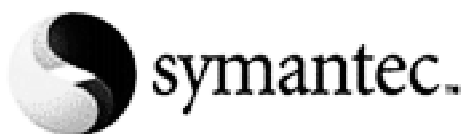
P O T R Z E B Y I R O Z W I A Z A N I A

Coraz częściej słyszymy o wirusach atakujących sieci największych światowych firm. W dobie Internetu szczególne znaczenie dla eGospodarki ma więc zapewnienie organizacjom możliwie najlepszej ochrony antywirusowej.

Ponieważ na rynku produktów antywirusowych znaleźć można wiele różnych rozwiązań każda firma planując zaimplementowanie skutecznej ochrony przed wirusami staje przed niełatwym zadaniem wyboru najwłaściwszego z nich. Jako że ochrona przed wirusami jest zadaniem szczególnie ważnym, gdyż skuteczny atak wirusa może unieruchomić całą organizację na długi czas, należy ze szczególną ostrożnością podchodzić do tego zagadnienia. W tym artykule postaram się przybliżyć dwa rodzaje ochrony antywirusowej – ochronę lokalną, serwerów oraz ochronę ruchu sieciowego.

Jeżeli rozmawiamy o ochronie lokalnej stacji roboczych istnieje kilka elementów, które powodują,

że niektóre produkty uzyskują przewagę nad innymi. Podstawową sprawą jest oczywiście baza wzorców wirusów, oraz sposób korelacji zawartości plików z jej zawartością. Inną bardzo ważną cechą jest sposób zarządzania. Jeżeli zaś chodzi o kontrolę antywirusową ruchu sieciowego to najważniejszym parametrem obok bazy wirusów jest zakres skanowanych protokołów sieciowych, oraz bezproblemowa współpraca z serwerami pełniącymi funkcję firewallei, czy proxy. Z doświadczeń integratorskich firmy ASCOMP wynika, iż najlepszym produktem do ochrony stacji lokalnych i serwerów dostępnym na polskim rynku jest Symantec Norton Antivirus, natomiast najlepszym rozwiązaniem do ochrony ruchu sieciowego jest produkt VirusWall firmy Trend Micro.



Firma **Symantec** jest światowym liderem na rynku zabezpieczeń antywirusowych dla komputerów stacjonarnych. Najnowszym produktem tej firmy jest Norton AntiVirus Enterprise Edition 7.6 – najnowocześniejsze zabezpieczenie tej firmy przed wirusami. Zapewnia automatyczne, bezobsługowe wykrywanie, analizę i usuwanie

makrowirusów, dzięki czemu czas reakcji na szybko rozprzestrzeniające się zagrożenia jest znacznie krótszy, a sprawność systemu – znacznie lepsza. Umożliwia centralne zarządzanie wirusami przez skierowanie wszystkich nienaprawialnych, zainfekowanych wirusami plików w bezpieczny obszar serwera centralnego w celu dalszej kontroli. Automatycznie wykrywa i usuwa wirusy znajdujące się w skompresowanych plikach, także zagnieżdżonych. Obsługuje wszystkie najczęściej spotykane formaty plików skompresowanych. NAV automatycznie odszukuje nowe i nieznanne wirusy, wykorzystując przełomową technologię heurystyczną – Bloodhound™. NAV automatycznie przeszukuje załączniki przychodzących wiadomości poczty elektronicznej w większości popularnych programów pocztowych. Zapewnia niezawodne zabezpieczenie przed wirusami dla serwerów połączonych w klastry – coraz popularniejszej technologii. Po założeniu kwarantanny na nowy, nienaprawialny plik zainfekowany wirusem można w prosty i szybki sposób wysłać pocztą elektroniczną do Symantec Security Response plik podlegający kwarantannie. Wtedy Symantec AntiVirus Research Automation (SARA) automatycznie przeanalizuje wirus, opracuje szczepionkę oraz wyśle poprawkę (definicję wirusa) z powrotem do firmy, i to

zwykle w ciągu dwóch do ośmiu godzin. Można wysłać nową definicję do pojedynczego zainfekowanego klienta lub całej firmy. W tym samym czasie Symantec Security Response opracuje nową definicję wirusa i udostępni ją wszystkim użytkownikom oprogramowania Norton AntiVirus na całym świecie. Codziennie odkrywanych jest około kilkunastu nowych wirusów, pobieranie pakietów typu delta (różnicowych) za pomocą LiveUpdate powoduje oszczędności związane z pracą w trybie online oraz redukuje obciążenie pasma niezbędnego do transmisji przez sieć. Możliwe jest ponowne uruchomienie niewykonanych zadań, aby stacje klienckie zawsze miały aktualne definicje nawet wtedy, gdy w zaplanowanym czasie aktualizacji nie było to możliwe.



Firma **TrendMicro** jest produującym producentem oprogramowania analizującego zawartość transmisji internetowych, chroniąc przepływ informacji na stacjach roboczych, serwerach plików i pomostach do Internetu za pomocą kompletnego, centralnie zarządzanego oraz sterowanego systemu typu VirusWall (zaporę anty-wirusową). Odpowiednia architektura gwarantuje bezproblemowe wdrożenie systemu analizującego zawartość listów elektronicznych czy transmisji Web pod kątem wirusów i innych złośliwych aplikacji, dla dowolnie dużych sieci korporacyjnych. Możliwość odległej administracji wszystkich produktów Trend Micro za pośrednictwem przeglądarki WWW oraz automatyczne uaktualnianie bazy wiedzy

(wzorców) znacznie ułatwia pracę administratora. Trend Micro specjalizuje się w centralnie zarządzanych rozwiązaniach serwerowych przeznaczonych do ochrony całych sieci i usług internetowych. Produkty TrendMicro mogą współpracować z produktami innych producentów, takimi jak systemy zaporowe czy serwery pocztowe. InterScan VirusWall jest systemem ochraniającym sieć lokalną przed wirusami i innymi niebezpiecznymi modułami przechodzącymi przez pomost do Internetu. Produkt posiada certyfikat OPSEC.

Zadaniem InterScan VirusWall jest wykrywanie i usuwanie wirusów oraz blokowanie niebezpiecznego kodu przedostającego się wraz ze strumieniem danych przepływającym z (lub do) Internetu. Zestaw składa się z trzech zintegrowanych modułów, które mogą być zainstalowane i zarządzane niezależnie lub wspólnie.

- E-Mail VirusWall wykrywa i usuwa wirusy z plików załączonych do przesyłek listowych (SMTP)
- Web VirusWall wykrywa niebezpieczne kontrolki ActiveX i applety Java
- FTP VirusWall wykrywa i usuwa wirusy "ukryte" w transferach za pośrednictwem protokołu FTP.

W przypadku wykrycia wirusa jest on izolowany na serwerze, a decyzja o przyszłości pliku jest odłożona na później. W przypadku listu informacja o wykryciu wirusa wysyłana jest do nadawcy, odbiorcy i administratora. Jeżeli list zawiera treść i zainfekowany załącznik, sama treść jest przekazywana odbiorcy. VirusWall obsługuje także większość formatów kompresujących i analizuje pliki zawarte w skompresowanych archiwach. Dodatkowo, wyposażony jest w

motor MacroTraps, który wykrywa i usuwa znane i nieznanne wirusy makr (np. w plikach MS-Word), obsługuje Content Vectoring Protocol (CVP) API, co umożliwia bardzo prostą integrację z FireWall-1. Konfiguracja do współpracy z FireWall-1 jest bardzo prosta i sprowadza się do określenia nazwy maszyny z zainstalowanym InterScan VirusWall. InterScan VirusWall może być skonfigurowany na kilka sposobów w odniesieniu do sposobu reagowania na wykryte, niebezpieczne zdarzenia, np.:

- Wysyłanie alertów do administratora
- Blokowanie niebezpiecznych ActiveX i appletów Java
- Kasowanie zainfekowanych plików
- Udzielenie zezwolenia na skopiowanie pliku przy spełnieniu wielu warunków bezpieczeństwa.

InterScan VirusWall może być zarządzany za pośrednictwem graficznego interfejsu Windows GUI z dowolnego punktu sieci lokalnej jak i z poziomu przeglądarki WWW z sieci rozległej. Podstawowe cechy tego produktu to przede wszystkim 100%-owa zgodność ze specyfikacją CVP, gwarantująca pełną współpracę z Check Point FireWall-1, skanowanie przychodzących i wychodzących listów SMTP i ich załączników w czasie rzeczywistym, skanowanie ruchu HTTP i FTP w czasie rzeczywistym, wykrywanie niebezpiecznych kontrolek ActiveX i appletów Java, wykrywanie i usuwanie znanych i nieznanych wirusów makr „w locie”. Zawiera on graficzny interfejs GUI i interfejs ISAPI/GDI do konfiguracji za pośrednictwem przeglądarki WWW.

*Miłosz Franaszek
Specjalista ds. Bezpieczeństwa
ASCOMP S.A.*





czyli jak wprowadzić

kultu

PRACY Z INTERNETEM

Internet może rozwijać horyzonty każdej organizacji, oferując dostęp do globalnego rynku, zwiększając możliwości sprzedaży i rozszerzając architekturę sieci. Podczas gdy umożliwienie dostępu Internetu każdemu pracownikowi jest często kluczowe dla sukcesu i rozwoju, to jednak niepożądane i bezproduktywne „serfowanie” po Internecie zmniejsza produktywność oraz przepustowość sieci.

Według badań wykonanych przez Departament Pracy Stanów Zjednoczonych, Voultreports.com, Gallup, MSNBC, większa część pracowników (w niektórych przypadkach ponad 60%), spędza 20 minut do jednej godziny dziennie przeglądając strony nie związane z ich pracą, włączając w to strony z grami on-line, aukcjami, pornografią, sportem i po-

dróżami. Niektóre raporty szacują, że organizacje tracą 3 biliony USD rocznie w związku z opisanym wyżej zjawiskiem. Sieci są blokowane przez filmy, gry interaktywne itp.

SmartFilter firmy Secure Computing pomaga firmom zaimplementować i wyegzekwować odpowiednie użytkowanie stron WWW, poprawiając efektywność dostępu do Internetu. SmartFilter to nowy wymiar w zarządzaniu kontrolą dla serwerów proxy, firewalli. Poprzez filtrowanie niepotrzebnych i niechcianych treści Internetowych SmartFilter jest efektywnym narzędziem do implementacji i egzekwowania polityki korzystania z Internetu. SmartFilter zarządza dostępem do Internetu dla pracowników, udostępnia pasmo, które by-

łoby zajęte przez nieautoryzowany przeglądanie stron WWW.

Łatwo dostosowujące się do potrzeb klientów oraz przezroczyste dla końcowego użytkownika SmartFilter dostarcza właściwych możliwości dla każdego systemu operacyjnego, serwera proxy i firewalla udostępniając efektywne opcje dla odpowiedniego kształtowania dostępu do zasobów Internetu. Jako najlepsze narzędzie do monitorowania i kontroli dostępu do WWW udowodnił swoją wartość i skuteczność w sieciach firm z listy Fortune 500. SmartFilter Control List jest ciągle uaktualniana oraz ściśle integrowana z firewallami, serwerami proxy.

*Krzysztof Tyl
Specjalista ds. Bezpieczeństwa
ASCOMP S.A.*



Właściwości

Cechy	Zalety
Filtrowanie/Blokowanie	Pozwala administratorom zdefiniować typy URL, które chcą filtrować z listy 27 kategorii zawartych w SmartFilter Control List
Ostrzeżenie	Umożliwia administratorom konfigurację, w której predefiniowane wiadomości lub ostrzeżenia są wyświetlane użytkownikowi. Informacje, że strona została zidentyfikowana jako zabroniona i dostęp do niej jest możliwy na własne ryzyko użytkownika
Grupy	Umożliwia administratorom zdefiniować dostęp do zasobów odpowiedni dla każdej z grup (np. inżynierowie, zarząd, studenci itd.)
De-priorytetyzacja	Umożliwia administratorom spowolnić ściąganie stron niedozwolonych. Poprzez tę funkcję można zniechęcić użytkowników do korzystania z takich zasobów
Auto FTP download	Administrator może skonfigurować SmartFilter w taki sposób, że uaktualnia SmartFilter Control List automatycznie co tydzień, lub ręcznie
Ograniczenia na wyszczególnionych stacjach roboczych	Umożliwia administratorowi umiejscowić ograniczenia w stosunku do jednego szczególnego klienta w sieci, nie wpływając na całą organizację
Dostosowanie ostrzeżeń do potrzeb klienta	Administrator może zdefiniować odpowiednie ostrzeżenia pojawiające się podczas dostępu do stron znajdujących się na SF Control List

ZELMER S.A. – system kontroli dostępu

Zaprojektowany i zainstalowany przez naszą firmę biometryczny system kontroli dostępu zabezpiecza pomieszczenia Ośrodka Informatyki ZELMER S.A. System identyfikuje osoby uprawnione do wejścia na chroniony teren na podstawie obrazu ich linii papilarnych. Drzwi otwierane są automatycznie tylko w przypadku pozytywnej weryfikacji tożsamości osoby, która zamierza przedostać się do strefy chronionej. W przeciwnym przypadku osoba taka może zostać wpuszczona do wewnątrz jedynie przez uprawnionego pracownika Ośrodka.

Głównym elementem systemu jest zintegrowany czytnik linii papilarnych iGuard FPS110 firmy iGuard Security System. Urządzenie to jest zamontowane przy drzwiach

wejściowych i połączone bezpośrednio z układem elektromechanicznym otwierającym drzwi oraz z zakładową siecią komputerową. Dzięki temu możliwy jest bezpośredni dostęp do danych i ustawień pamiętanych przez urządzenie z uprawnionych stacji roboczych wyposażonych w tym celu jedynie w zwykłe przeglądarki stron www.

Podstawowe cechy urządzenia iGuard FPS110:

- klawiatura alfanumeryczna 12-klawiszowa (0-9, A-B)
- kody PIN o długościach od 1 do 10 znaków
- podświetlany wyświetlacz LCD 2 x 16 znaków
- wizualna i akustyczna sygnalizacja wyniku odczytu

- gniazdo RJ-45 do sieci Ethernet
- wbudowany serwer web
- stopa błędu odczytu linii papilarnych < 0,01 %
- możliwość pamiętania dwóch wzorców linii papilarnych dla każdego użytkownika
- niewielkie gabaryty i zwarta konstrukcja.

Dostęp do danych gromadzonych przez system, które dotyczą ruchu osób (nazwiska, godziny wejścia i wyjścia) jest uzyskiwany z poziomu przeglądarki internetowej.

Proces przejścia do strefy chronionej przez osobę uprawnioną z wykorzystaniem czytnika i Guard FPS110 składa się z następujących trzech etapów:



Etap 1:
Osoba podaje swój PIN ...



Etap 2:
... umieszcza palec na czytniku ...



Etap 3:
... może otworzyć drzwi.

The screenshot shows the 'iGuard Security System' web interface. The main content is an 'Attendance Report' table. The table has columns for 'No.', 'ID', 'Name', 'Date', and 'In/Out' times. The data is organized by employee ID and name, showing their check-in and check-out times for a specific date.

No.	ID	Name	Date	In	Out	In	Out	In	Out	More
1.	A1002	Wang, Cai Chang	07/12/1999	08:00	08:15
2.			07/13/1999	08:08	08:24
3.			07/14/1999	08:08
4.	A1007	Tsui, Ping Pak	07/12/1999	08:07	08:34
5.			07/13/1999	08:01	08:33
6.			07/14/1999	08:02
7.	A1015	Chu, Chai Cheng	07/12/1999	08:27	08:18
8.			07/13/1999	08:29	08:08
9.			07/14/1999	08:29
10.	A1019	Chan, Chuen Heung	07/12/1999	08:19	08:16
11.			07/13/1999	08:08	08:19
12.			07/14/1999	08:13
13.	A1050	Chan, KC	07/12/1999	08:47	08:39
14.			07/13/1999	08:52	08:32
15.			07/14/1999	08:52
16.	A1154	Chow, Man Heung	07/12/1999	09:04	08:30
17.			07/13/1999	09:04	08:30
18.			07/14/1999	09:05
19.	A1155	Shui, Ying Tsun	07/12/1999	09:31	08:30
20.			07/13/1999	09:31	08:29
21.			07/14/1999	09:35
22.	B1004	Ng, Lee Fong	07/12/1999	08:48	08:50
23.			07/13/1999	08:47	08:13
24.			07/14/1999	09:07

Możliwy jest również eksport tych danych w formacie arkusza kalkulacyjnego Excel lub pliku tekstowego. Dane te można następnie wykorzystać np. do przygotowania listy płac lub w celu potwierdzenia bądź zaprzeczenia czyjeś obecności w chronionej strefie w określonym czasie. Użyteczność oferowanych przez system kontroli dostępu funkcji została potwierdzona w praktyce, a dzięki jego rozproszonej architekturze przewidywana jest dalsza ekspansja na terenie przedsiębiorstwa ZELMER S.A.

Zbigniew Grabis
Dyrektor ds. Sprzedaży
ASCOMP S.A. □

Mikołajki

Informacyjne

Myczkowce 2001

W dniach 8 i 9 grudnia 2001 r. w Myczkowcach w hotelu Energetyk zorganizowaliśmy dla naszych Klientów seminarium połączone z Mikołajkową Biesiadą.

Seminarium poświęcone było prezentacji nowych produktów firmy Enterasys (dawniej Cabletron Systems). Prelegentami byli Zbigniew Grabis – Dyrektor ds. Sprzedaży firmy ASCOMP, który mówił o tym dokąd zmierza integracja systemów IT,



oraz Krzysztof Tyl – Specjalista ds. Bezpieczeństwa, który przedstawił opracowaną przez inżynierów z firmy Enterasys nową koncepcję bezpiecznej sieci teleinformatycznej – Secure Harbour.

Szczegółowo zostały omówione elementy tej koncepcji:
– rodzina szyfratorów Enterasys Aurean do zarządzania i tworzenia wirtualnych sieci prywatnych VPN

– system automatycznego wykrywania włamań (intrusion detection system – ids) – Enterasys

Dragon do detekcji i reakcji na włamania i niebezpieczne zachowania w sieci – systemy autoryzacji i zarządzania użytkownikami – Enterasys NetSight Policy Manager.

Prezentowane rozwiązania spotkały się z dużym zainteresowaniem. Na zakończenie odbyło się „Forum wymiany doświadczeń, czyli poszukiwanie optymalnych rozwiązań”. Dyskusja dotyczyła omawianych produktów oraz możliwości ich zastosowania. Uczestnicy wyrażali swoje opinie, a także dzielili się posiadanym doświadczeniem oraz spostrzeżeniami na temat zagrożeń związanych z włamaniami do sieci.



Wieczorową porą zaprosiliśmy naszych gości na Mikołajkową Biesiadę: po kilkunastominutowym spacerze pod osłoną gwieździstego nieba i przy towarzystwie siarczystego mrozu (-12°C) dotarliśmy do ogniska. Tam jedliśmy pieczoną kiełbasę, a grzaniec spowodował, że mróz nie był już taki siarczysty. Największą atrakcją tego wieczoru był kulig – dwie pary koni ciągnęły sanki (najlepiej było siedzieć na końcu),

okazało się że dla niektórych naszych uczestników był to pierwszy kulig w życiu.

Następnego dnia udaliśmy się na zwiedzanie zapory w Solinie. Zapoznaliśmy się z wnętrzem zapory, oraz poznaliśmy jej historię.

Na zakończenie spacer po grzbiecie zapory, wspólne zdjęcie i powrót do hotelu, gdzie po obiedzie rozstaliśmy się.

Uczestnicy byli zadowoleni z tego, że postanowili skorzystać z naszego zaproszenia, aby więc nie zawieść naszych Klientów planujemy oczywiście podobne spotkania.

Monika Kubuśka, Specjalista ds. Marketingu, ASCOMP S.A. □

ZAPROSZENIE

Serdecznie zapraszamy na seminarium

„Bezpieczne systemy teleinformatyczne”,

maj 2002 r., Warszawa. Szczegóły: www.ascomp.com.pl.

Bezpieczny system teleinformatyczny

rozwiązania firmy
Secure Computing
Seminarium

5 lutego w sali konferencyjnej firmy ASCOMP S.A. odbyło się seminarium poświęcone bezpiecznym systemom teleinformatycznym w oparciu o rozwiązania firmy Secure Computing.

Na spotkaniu zaprezentowano:

- SafeWord Premier Access – system silnej autentykacji, autoryzacji i kontroli dostępu
- Sidewinder – bezpieczny aplikacyjny firewall
- SmartFilter – system wprowadzający politykę pracy z Internetem.



Seminarium prowadzone było przez Pana Franka Koelmela – Dyrektora ds. Sprzedaży Secure Computing na Europę Centralną i Wschodnią.

Zainteresowanie prezentowanymi rozwiązaniami i produktami było bardzo duże. Wysoka frekwencja zaproszonych gości wskazywała na ogromne zainteresowanie problemem bezpieczeństwa sieci teleinformatycznych.

Na zakończenie wywiązała się burzliwa dyskusja podczas której analizowano zalety poszczególnych produktów oraz możliwości zastosowań prezentowanych rozwiązań.

MK □

WYDAWCA: **ASCOMP S.A.**
ul. Walerego Sławka 3, 30-653 Kraków
Tel. (+48 12) 254 62 61 do 65
Fax (+48 12) 254 62 72
Red. Nacz.: Zbigniew Grabis
e-mail: z.grabis@ascomp.com.pl
Dział Bezpieczeństwa: wew. 105, 120
e-mail: securiusz@ascomp.com.pl
www.ascomp.com.pl