BIBLIOTEKA INFOTELA

Cena 15 zł (w tym 0 % VAT)
ISBN 83-921962-8-7

SYSTEMY MONITORINGU I KONTROLI DOSTĘPU

sponsor veracomp

- BEZPIECZEŃSTWO INFORMATYCZNE
- ZAPORY OGNIOWE
- SZYFRATORY DANYCH
- BLOKOWANIE WŁAMAŃ DO SIECI KOMPUTEROWYCH
- CYFROWY MONITORING WIDEO IP

Targi z rekomendacją Polskiej Korporacji Targowej

INTERTELECOM

XVII Międzynarodowe Targi Łączności

22-24.03.2006

Łódź

Najważniejsza w Polsce impreza branży IT

Organizator:

MTŁ

Międzynarodowe Targi Łódzkie Sp. z o.o.
90-531 Łódź, ul. Wólczańska 199
tel: 42 637 29 34, 637 29 36
fax: 42 637 29 35
www.mtl.lodz.pl/targi/intertelecom

Patroni honorowi:

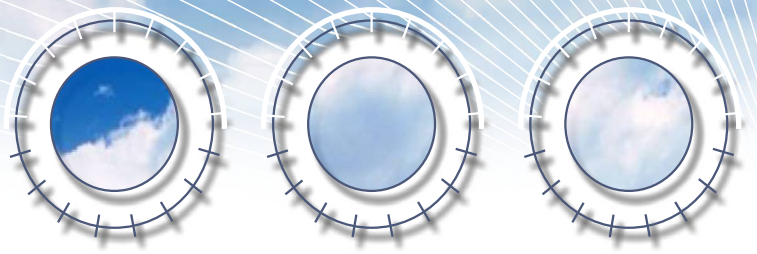
KIGEiT PIIT

Patroni medialni:

Puls Biznesu
INFOTEL
TV BIZNES
Radio 101,3 FM złote przeboje

Veracomp SA

specjalizowany
dystrybutor
rozwiązań
teleinformatycznych



Bezpieczeństwo

Blue Coat Systems

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

FORTINET
REAL TIME NETWORK PROTECTION

f5 NETWORKS

INTERNET SECURITY SYSTEMS™

RSA SECURITY®

SONY

SECURE COMPUTING

SurfControl®

utimaco® safeware

Zabezpieczenia sieci
- Zapory ogniowe
- Systemy IDS / IPS

Kontrola treści
- Kontrola zawartości poczty
- Filtrowanie ruchu www
- Ochrona antywirusowa

Bezpieczny zdalny dostęp do zasobów
- Bramki VPN IPsec
- Systemy zdalnego dostępu przez protokół SSL
- Identyfikacja, uwierzytelnianie i autoryzacja

Systemy monitoringu wizyjnego IP

veracomp

Veracomp SA prowadzi sprzedaż produktów i usług wyłącznie za pośrednictwem Partnerów Handlowych.

Podczas trwania targów
INTERTELECOM 2006 w Łodzi (22–24 marca 2006 r.)

zapraszamy na:

KONFERENCJĘ

„Komunikacja elektroniczna – konwergencja sieci: biznes, technologie, regulacje"

(22 marca 2006 r. w sali S2, hala nr 1 o godz. 12.30)

dla pierwszych 50. uczestników KONFERENCJI redakcja INFOTELA przygotowała miłą niespodziankę!

TEMAT:

Rozwiązania NNGN
czyli
Netia
New Generation Network

Organizator

MSG MEDIA

tel. (52) 325 83 10; fax (52) 373 52 43
e-mail: office@msgmedia.pl
www.msgmedia.pl

Sponsor

netia

Patronat branżowy

KIGEiT

Patronat medialny

INFOTEL 1997

TECHBOX.PL

ISBN 83-921962-8-7
Cena 15 zł (w tym 0% VAT)
Nakład: 7000 egz.

Wydawca:

MSG – Media s.c.
ul. Stawowa 110
85-323 Bydgoszcz
tel. (52) 325 83 10
fax (52) 373 52 43
office@msgmedia.pl
www.techbox.pl

Sponsor wydania

Redakcja
Marek Kantowicz
Grzegorz Kantowicz

DTP
Czesław Winiecki

Marketing
Janusz Fornalik
Arkadiusz Damrath

Korekta
Ewa Winiecka

Druk
Drukarnia ABEDIK
Sp. z o.o.
85-861 Bydgoszcz
ul. Glinki 84
tel./fax (52) 370 07 10
info@abedik.pl
www.abedik.pl

SPIS TREŚCI

Wstęp
Jerzy Trzepla – kierownik działu rozwiązań bezpieczeństwa w Veracomp 4–5

Błażej Marciniak
Telewizja przemysłowa CCTV czy cyfrowy minitoring IP? 6–8

Mariusz Rzepka
Bezpieczeństwo biur terenowych: krok naprzód czy wstecz? 9–11

Łukasz Światek
Trusted Computing sposobem na zabezpieczenie notebooków 12–13

Michał Kułakowski
Techniki obrony przed atakami przez przepełnienie bufora 14–6

Sony: nowa zewnętrzna obudowa do kamery SNC 18–19

System do zarządzania czasem pracy X/TIME 21

Grzegorz Kantowicz
Kryptograficzne elementy bezpieczeństwa i kontroli dostępu 22–37

Grzegorz Kantowicz
Biometryczne systemy zabezpieczeń 38–45

Arkadiusz Rabiega
Bezpieczniej już nie będzie 46–48

Jerzy Trzepla
kierownik działu rozwiązań bezpieczeństwa
w Veracomp

Konieczność zapewnienia bezpieczeństwa to jeden z obowiązków każdego menedżera, wynikający nie tylko z wymagań biznesowych, ale również z regulacji prawnych. Obecnie co najmniej 60 ustaw nakłada obowiązek zapewnienia ochrony i bezpieczeństwa informacji wewnątrz organizacji. Wymaga to z kolei podjęcia całego szeregu działań: decyzji organizacyjnych, szkoleń, wdrożenia pewnych rozwiązań technologicznych i, co najważniejsze, musi być to ciągły proces, a nie jednorazowa akcja.

Systemy informatyczne instytucji i przedsiębiorstw są obecnie, bardziej niż kiedykolwiek wcześniej, narażone na różnorodne niebezpieczeństwa. Wynika to z faktu upowszechnienia internetu jako środka komunikacji biznesowej. Jednocześnie internet jako środowisko globalne, w którym odległości, granice, strefy czasowe nie mają praktycznego znaczenia, a jednocześnie względnie łatwo można zachować anonimowość, stał się obszarem szczególnego zainteresowania dla grup przestępczych. Obecnie określenie cyberprzestępczość jest w pełni uzasadnione, ataki nie są już przeprowadzane przez nieprzystosowanych społecznie maniaków czy zbuntowanych nastolatków, ale przez dobrze zorganizowane, międzynarodowe grupy przestępcze.

System zabezpieczeń jest jak mur obronny biegnący wokół średniowiecznego miasta, gwarantuje tak dobrą ochronę, jak mocny jest w najsłabszym miejscu. Skuteczne zablokowanie lub utrudnienie ataku w jednym miejscu, powoduje natychmiastowe przeniesienie ataku w miejsca słabiej chronione. Można więc ze 100-proc. prawdopodobieństwem przyjąć, że atak będzie przeprowadzony w najsłabszym, najmniej chronionym miejscu. Wynika stąd konieczność budowy zrównoważonych systemów ochronnych, dostosowanych do przewidywanych dróg i metod ataku.

W filmach sensacyjnych można niejednokrotnie zobaczyć hakera komputerowego włamującego się do systemu, łamiącego hasła itp. Jest to jeden z mitów nie znajdujących pokrycia w rzeczywistości – stosowane obecnie mechanizmy ochronne w postaci systemów firewall stanowią wystarczająco skuteczne zabezpieczenie. Obecnie ataki są znacznie bardziej wyrafinowane i wykorzystują luki bezpieczeństwa istniejące w aplikacjach, np. takich jak edytory tekstów czy przeglądarki plików graficznych. Wynika stąd konieczność wykorzystywania zaawansowanych systemów blokowania włamań.

Techniczne mechanizmy kontroli połączeń sieciowych oraz użytkowników mogą być nieskuteczne, jeżeli atak będzie oparty na metodach socjotechnicznych. Jak dowodzi Kevin Mitnick w swojej książce, mechanizmy techniczne są trudne do przełamania, ale ludzie łatwo dają się podejść i oszukać. Nie oznacza to wcale, że jesteśmy wobec takich ataków bezbronni. Istnieją mechanizmy silnego uwierzytelniania, których wdrożenie przeciwdziała takim naruszeniom polityki bezpieczeństwa. Jednocześnie automatycznie zanika obyczaj zapisywania haseł na kartkach przyklejonych do klawiatury.

Innym poważnym zagrożeniem spotykanym obecnie jest tzw. spam czyli niechciana korespondencja, którą każdego dnia znajdujemy w swojej poczcie elektronicznej. Wraz z interesującymi lub nieinteresującymi ofertami handlowymi możemy otrzymać i przypadkiem uruchomić program, który zacznie bez naszej wiedzy i zgody wykorzystywać nasz komputer w celu realizacji zadań zleconych przez hakera. Może to być np.

wysłanie zawartości książki adresowej albo również innych bardziej istotnych poufnych danych. Ale istnieje w tym przypadku drugie dno. Nasz komputer może w takiej sytuacji zostać tzw. zombie, komputerem służącym do dalszego rozsyłania spamu lub innego złośliwego kodu. Poważnym zagrożeniem w takiej sytuacji nie jest to, że ktoś wykorzystuje nasz komputer, ale przede wszystkim to, że może za jego pomocą rozpowszechniać treści zakazane, np. wzywające do przemocy czy dziecięcą pornografię. Udowodnienie własnej niewinności może być zadaniem trudnym lub niewykonalnym.

Kolejnym zagrożeniem, często bagatelizowanym, jest utrata przechowywanych danych. Powszechnie korzystamy z przenośnych urządzeń (komputery, palmtopy, zaawansowane telefony), które mogą zostać skradzione lub zgubione. Strata materialna, jaka się z tym wiąże, może być znikomo mała w porównaniu z konsekwencjami pozyskania zapisanych w urządzeniu danych przez osoby nieupoważnione. Grozi nam ujawnienie danych stanowiących tajemnicę przedsiębiorstwa lub nawet takich, których ochrona wynika z obowiązującego prawa.

Powyższy spis nie wyczerpuje, oczywiście, katalogu, możliwych zagrożeń i scenariuszy ataku, dlatego systemy ochrony stosowane dotychczas muszą być stale i na bieżąco unowocześniane i uzupełniane, tak aby nie pozostawiać miejsc nie chronionych lub osłabionych. Z tego powodu budowę systemu należy rozpocząć od zdefiniowania zasobów oraz ich znaczenia dla firmy, określić rodzaje oraz poziom ryzyka, na jakie są wystawione i na tej podstawie zdefiniować wymagania wobec mechanizmów ochronnych. Opracowany projekt pozwala na skuteczną implementację systemu zabezpieczeń, którego praca podlega stałemu monitorowaniu. Monitorowanie systemu jest szczególnie istotne, gdyż w ten sposób możemy zgromadzić informacje o stwierdzonych incydentach zagrożenia bezpieczeństwa, które po analizie mogą stanowić ewentualny dowód w sprawie lub być podstawą do modyfikacji systemu bezpieczeństwa.

Jak widać, proces przygotowania, wdrożenia i zarządzania jest złożony i wymaga specjalistycznych rozwiązań oraz stosownych służb po stronie ich użytkownika. Duże instytucje i przedsiębiorstwa są w stanie uruchomić oraz utrzymać tego typu systemy oraz liczne zespoły specjalistów realizujących na bieżąco procesy bezpieczeństwa. Nie oznacza to bynajmniej, że małe firmy nie mogą wdrożyć skutecznych zabezpieczeń. Producenci rozwiązań ochronnych rozumiejąc specyfikę małych firm zmodyfikowali swoja ofertę, tak aby odpowiedzieć na potrzeby małych firm.

Systemy wielofunkcyjne nazywane UTM (*Unified Thread Management*) przeznaczone są właśnie dla tego segmentu rynku. Cechą charakterystyczną rozwiązań UTM jest połączenie w jednym urządzeniu wielu mechanizmów ochronnych: firewall, IPS, ochrona antywirusowa, filtrowanie treści, ochrona przed spamem oraz oprogramowaniem szpiegowskim itp. Jednocześnie zarządzanie tymi rozwiązaniami jest znacznie uproszczone, tak aby skutecznie mógł je wdrożyć inżynier nie mający dużej wiedzy z zakresu bezpieczeństwa sieciowego.

Veracomp SA, jako dystrybutor specjalizujący się w systemach zabezpieczeń, oferuje szeroki wachlarz różnorodnych systemów zabezpieczających przeznaczonych dla odbiorców różnej wielkości, z różnych segmentów rynku, o specyficznych wymaganiach. Ale naszą rolę rozumiemy znacznie szerzej, gdyż system bezpieczeństwa to nie tylko zestaw rozwiązań technologicznych. Bezpieczeństwo to przede wszystkim świadomość użytkowników, stąd krzewimy wiedzę o zagrożeniach i metodach przeciwdziałania w ramach własnej inicjatywy FORT – Forum Ochrony Rozwiązań Teleinformatycznych oraz na konferencjach powszechnych lub branżowych.

Dla firm oraz instytucji zainteresowanych wybranymi aspektami bezpieczeństwa organizujemy warsztaty, gdzie można się bardziej szczegółowo zapoznać z konkretnymi realizacjami technicznymi. W centrum edukacyjnym Compendium prowadzone są na bieżąco szkolenia z tematyki bezpieczeństwa.

Veracomp SA współpracuje z uznanymi producentami, liderami rynku w zakresie rozwiązań bezpieczeństwa, gdyż tylko taki dobór partnerów gwarantuje odpowiednio wysoki poziom oferowanych zabezpieczeń. Jednym z podstawowych partnerów Veracomp SA jest firma CheckPoint Software Technologies, oferująca od kilkunastu lat stosowane powszechnie rozwiązania Firewall-1. Powszechność stosowania technologii CheckPoint potwierdza fakt, że wszystkie 100 firm wchodzących w skład Fortune 100 korzysta z systemów CheckPoint.

Ponadto oferta Veracomp SA obejmuje produkty firm: Internet Security Systems, Nokia Enterprise Solutions, RSA Security, Secure Computing, Fortinet Inc., Surf Control, Utimaco Safeware AG, BlueCoat.

Szczegółowe informacje
można odszukać na stronach:
www.veracomp.pl,
a w przypadku pytań zachęcamy do kontaktu pod adresem:
bezpieczenstwo@veracomp.pl.

Telewizja przemysłowa CCTV czy cyfrowy monitoring IP?

Wybierając system do monitorowania wizyjnego należy sobie zadać pytanie: Potrzebuję prostego rejestrowania obrazów z kamer czy też systemu monitoringu cyfrowego?

Różnica jest podstawowa. **Nadzór wideo CCTV** to przede wszystkim analogowy, prosty i tani system rejestrowania obrazów z kamer. Transmisja z kamer jest przesyłana kablami koncentrycznymi do centralnego rejestratora, gdzie jest zapisywana przeważnie na magnetowidzie VHS lub za pośrednictwem urządzeń konwertujących sygnał do postaci cyfrowej, zapis jest dokonywany na twardym dysku. Analogowe systemy CCTV oferują bardzo niewielkie możliwości konfiguracyjne. Dodawanie nowych kamer oznacza zawsze konieczność montażu dodatkowego okablowania, osobnego do transmisji i do zasilania, niekiedy także do sterowania kamerą ruchomą. Dodatkowo są bardzo ograniczone możliwości konfiguracji parametrów pracy samej kamery. Jeśli po zamontowaniu w trudno dostępnym miejscu okaże się, że Zle została ustawiona np. przysłona lub ostrość obrazu, pozostaje do wyboru albo się do kamery dostać, albo ją ściągnąć na dół. Także inne ograniczenia CCTV uwidoczniają się przy pewnej skali. Przy archiwizacji na taśmach VHS zawsze istnieje ryzyko, że właściwa taśma się zgubi, zostanie nadpisana, niepoprawnie opisana lub niemożliwa do odnalezienia w krótkim czasie. Wyszukiwanie konkretnego zdarzenia oznacza konieczność ręcznego przeglądnięcia na szybkim podglądzie niekiedy dziesiątek godzin nagrań, co jest żmudne i czasochłonne. Do prostych zastosowań analogowe rozwiązania CCTV są wystarczające, zwłaszcza jeśli nie jest planowana ich rozbudowa.

Pośrednim etapem w migracji do technologii wideo IP są rozwiązania hybrydowe, które w dalszym ciągu wykorzystują analogowe kamery CCTV oraz transmisję, jednakże przed zapisem materiał jest konwertowany na rejestratorze do postaci cyfrowej. Rozwiązuje to część problemów związanych z archiwizacją danych, jednakże w dalszym ciągu pozostawia ograniczenia kamer analogowych.

Cyfrowy monitoring wideo IP jest systemem znacznie wykraczającym poza zwykłą rejestrację obrazów otoczenia. Dzięki wbudowanej inteligencji potrafi także poddać obraz analizie i zaprezentować administratorowi nie tyle obraz z kamer, co obraz sytuacji. Koszty kamer IP są nieco wyższe od tradycyjnych analogowych kamer, lecz posiadają nieporównywalnie większą kompleksowość. Wykorzystują zaawansowane techniki przetwarzania obrazu oraz „wbudowaną inteligencję". Kamera w takim systemie jest czymś znacznie więcej niż obiektywem z przetwornikiem AC. Znaczna część analizy obrazu i alarmów jest wykonywana już na kamerze, odciążając system zarządzający i przyspieszając czas reakcji. Pomimo wyższego początkowego kosztu instalacji, system IP bardzo szybko staje się tańszy w utrzymaniu i rozbudowie od swojego analogowego odpowiednika.

- ✔ Dzięki wykorzystaniu protokołu transmisji IP nie potrzebuje dedykowanego okablowania, które determinuje jego zasięg. Sieć komputerową można bardzo łatwo i tanio rozbudować, zwłaszcza wykorzystując powszechnie dostępne technologie transmisji bezprzewodowej WLAN. Sygnały sterujące ruchomymi kamerami PTZ są przesyłane tą samą drogą transmisji. Zbędne są dodatkowe kable przenoszące sygnały kontrolne.
- ✔ Zastosowanie nowoczesnych standardów konwersji sygnału wideo (MJPEG, MPEG4) umożliwia otrzymanie lepszych jakościowo obrazów obiektów w ruchu, przy mniejszym zapotrzebowaniu na pasmo. Można także stosować różne standardy konwersji do różnych celów: np. kompresję MPEG4 do podglądu, MJPEG do archiwizacji danych. Dzięki cyfrowej formie zapisu wyszukiwanie konkretnego zapisu obrazu jest niemal błyskawiczne: jako kryteria wyszukiwania można użyć dat, czasu lub nazwy kamery, która zarejestrowała zdarzenie.
- ✔ Skalowalność systemu IP jest niemal nieograniczona: rozbudowa systemu o dodatkowe kamery sprowadza się tylko do doprowadzenia do wybranego miejsca transmisji Ethernet (kablem lub bezprzewodowo). Doprowadzenie osobnego kabla zasilającego kamerę może nie być konieczne. Większość kamer

IP potrafi pobierać zasilanie z kabla Ethernet. Dzieje się to dzięki obsłudze standardu zasilania Power over Ethernet (PoE) 803.2af. Dzięki temu system monitoringu składający się z kilku kamer można rozbudować nawet do 100 i więcej kamer.

- ✔ Rozbudowa systemu rejestracji oraz archiwizacji oznacza tylko zwiększenie pojemności pamięci dyskowej na firmowych serwerach lub macierzy dysków. Nie oznacza konieczności zakupu dedykowanych urządzeń archiwizujących, wymagających obsługi oraz zarządzania. Cały system jest zarządzany jak infrastruktura sieciowa. Eliminuje to konieczność zatrudniania i szkolenia dodatkowego personelu. Dzięki wbudowanej w system inteligencji nie jest konieczne śledzenie na bieżąco obrazów na kamerach. Operator jest tylko powiadamiany o wydarzeniach należących do wcześniej zakwalifikowanych klas alarmów. Także wtedy nie musi to oznaczać konieczności wykazywania się refleksem. System zareaguje we wcześniej zaplanowany sposób, np. zamykając elektroniczne zamki, powiadamiając odpowiednie służby.
- ✔ Bezpieczeństwo danych łatwiej zapewnić w systemie IP, ponieważ mogą być one archiwizowane w zupełnie innej lokalizacji niż kamera, więc zniszczenie lokalnego repozytorium danych niczego przestępcom nie da. Dzięki zastosowaniu profesjonalnych systemów zabezpieczeń danych można zapewnić ich integralność nawet w wypadku awarii sprzętu.
- ✔ Jedno Centrum Monitoringu może świadczyć usługi monitoringu wielu klientom zabezpieczając wiele obiektów jednocześnie, dzięki przesyłaniu danych poza zabezpieczany obiekt dodatkowo podnosząc ich poziom bezpieczeństwa.
- ✔ W odróżnieniu od systemów analogowych, systemy IP można niewielkim kosztem dobrze zabezpieczyć przed nieautoryzowanym dostępem. Bezpieczeństwo sieci komputerowych jest na bardzo wysokim poziomie, większość urządzeń stosowanych w sieciach przesyłowych potrafi szyfrować transmisję. Nic nie stoi na przeszkodzie, aby wykorzystywać kilka metod zabezpieczeń jednocześnie, wprost przeciwnie – jest to zalecana polityka. Dostęp do samego systemu także można autoryzować, przyznając adekwatne do obowiązków prawa każdemu upoważnionemu użytkownikowi. Zdalny dostęp poprzez internet można zrealizować bez kompromisu na rzecz bezpieczeństwa. Upoważniona osoba może w bezpieczny sposób zdalnie zarządzać systemem.
- ✔ Zastosowanie kamer IP umożliwia korzystanie z aktualizacji ich oprogramowania. W ten sposób podnosi niezawodność oraz pozwala na optymalne wykorzystanie sprzętu, dzięki najnowszym technologiom przetwarzania obrazu. Podobnie aktualizacje oprogramowania zarządzającego systemem mogą udostępnić zupełnie nowe funkcjonalności bez ponoszenia dużych nakładów inwestycyjnych.

W kontraście z analogowymi kamerami wideo, które są zasadniczo „jednostronnymi" urządzeniami przesyłającymi obraz, kamery IP pozwalają także na przesyłanie dZwięku, i to dwukierunkowo. Po podłączeniu mikrofonu monitoring można rozszerzyć o sygnały akustyczne, które mogą być Zródłem alarmu. Zarejestrowany materiał wideo może posiadać wówczas ścieżkę dZwiękową, także operator systemu może poprzez dołączone do kamery IP głośniki przekazywać komunikaty lub ostrzeżenia. Większość kamer posiada własny tzw. *bufor pre-alarm*, gdzie są składowane klatki z kilku-kilkunastu sekund wstecz. W sytuacji alarmowej są one przesyłane do systemu rejestracji, dzięki czemu operator ma zapis nie tylko samego zdarzenia, ale także jak do niego doszło. Wykorzystanie wbudowanych w kamery IP mechanizmów wykrywania ruchu może znacznie poprawić efektywność nawet niewielkiego systemu monitoringu. Poziom czułości ruchu oraz jego zakres można konfigurować bezpośrednio na kamerze. Dzięki temu kamera zignoruje poruszający się obiekt wielkości np. kota lub psa, ale zostanie wszczęty alarm przy pojawieniu się obiektu wielkości człowieka. Nie całe pole widzenia kamery musi być monitorowane na okoliczność ruchu, można to pole zawęzić do interesującego obszaru, np. wejście do budynku, drzwi lub

okna. Kamery IP posiadają także złącza niskoprądowe I/O (wejścia/wyjścia), które można wykorzystać do sterowania innymi urządzeniami lub do przyjmowania sygnałów z tychże. Dzięki temu wykryty ruch na terenie monitorowanym kamerą może spowodować np. włączenie oświetlenia lub syreny alarmowej. Kamery IP mogą zmieniać samodzielnie parametry swojej pracy. Dzięki automatycznemu przełączaniu się z trybu „dziennego" na „nocny" zawsze otrzymujemy obrazy najwyższej jakości.

Czy tylko monitoring wideo?

Poza oczywistymi korzyściami wynikającymi z faktu, że administrator bezpieczeństwa sieci może być także administratorem systemu monitoringu wideo, weZmy pod uwagę szerszy aspekt: zapewnienia bezpieczeństwa ludziom w sytuacjach kryzysowych. Wobec stale wzrastającego ruchu ludzi – drogowego, pasażerskiego na dworcach lotniczych lub kolejowych, komercyjnego w centrach handlowych – niezwykłego znaczenia nabiera zarządzanie ruchem tłumu (*crowd management*). Zle ustawiona tablica informacyjna na lotnisku lub dworcu może powodować gromadzenie się ludzi. W tłumie jest się bardziej narażonym na kradzież lub incydent. W wypadku zagrożenia ewakuowanie takiej liczby ludzi nie będzie możliwe do przeprowadzenia w krótkim czasie, a wybuch paniki może być groZniejszy w skutkach od pożaru. Systemy zarządzające monitoringiem IP można wyposażyć w oprogramowanie pozwalające śledzić i analizować ruch ludzi, dzięki czemu takie „wąskie gardła" można w porę zlokalizować i rozładować, np. tylko przestawiając tablicę informacyjną w przestronniejsze miejsce. Centralne oprogramowanie analizujące jest zdolne do samodzielnego sterowania kamerami. Może także śledzić wskazanego przez operatora człowieka, w sposób ciągły monitorując jego położenie poprzez przekazywanie śledzenia z kamery do kamery. Poza aspektem zapewnienia bezpieczeństwa ludziom mamy też do czynienia z aspektem komercyjnym monitoringu IP. Jeśli można policzyć, ile osób przewija się dziennie przez określony obszar, reklama sprzedana w takim miejscu ma też zupełnie inną wartość. System monitoringu IP można także wykorzystać do zbierania statystyk o liczbie np. ludzi odwiedzających supermarkety w określonym czasie (święta). Pozwoli to na lepsze przygotowanie dostępności towaru oraz liczby ludzi do obsługi. Wraz z postępem technologii analizy obrazu będzie można (oprócz liczby) określać płeć i wiek klientów. Takie informacje będą niezwykle cenne dla kadry zarządzającej centrum handlowym.

Dzięki monitorowaniu i bieżącej analizie ruchu ulicznego można poznać liczbę pojazdów przejeżdżających dziennie przez np. most i oszacować czas jego zużycia i konieczność remontu. Można także zareagować np. na awarię sygnalizacji świetlnej i (dzięki powiadomieniu policji) zapobiec lub ograniczyć skutki powstałego korka. Monitoring parkingów i osiedli mieszkaniowych

pozwala na ograniczenie kradzieży i znacznie podnosi poziom poczucia bezpieczeństwa mieszkańców. W przyszłości zintegrowanie systemów monitoringu z biometrycznymi systemami rozpoznawania twarzy będzie umożliwiało zidentyfikowanie twarzy znanego policji przestępcy w tłumie i śledzenie jego poczynań.

Udział kamer IP w ogólnej liczbie montowanych kamer monitoringu jest obecnie rzędu kilkunastu procent. Liczba systemów budowanych rocznie wyłącznie w oparciu o IP wzrasta niezwykle dynamicznie. Przykładem może tu być projekt monitoringu stadionu sportowego klubu Porto Football w Portugalii. Obiekt na 52 000 miejsc jest monitorowany przez 139 ruchomych kamer IP Sony, którymi zarządza oraz rejestruje obrazy dedykowane oprogramowanie *RealShot Manager Sony.* Kamery w wodoszczelnych i wandaloodpornych obudowach zapewniają bieżący podgląd sytuacji na trybunach, parkingach, w kasach biletowych oraz bramkach wejściowych dla kibiców. Odpowiednia optyka zastosowana w kamerach zapewnia wysoką jakość obrazów w zmiennych warunkach oświetlenia słonecznego. Pozwala też rejestrować zbliżenia wystarczające na odróżnienie rysów twarzy osoby będącej po drugiej stronie stadionu. Operatorzy systemu monitoringu mają bieżący podgląd sytuacji na 42-calowych ekranach dzięki zastosowaniu „warstw" interfejsu zarządzającego oprogramowania Sony. Wystarczy wybrać interesujący operatora obiekt, aby obejrzeć jego otoczenie, a także wnętrze, przechodząc na odpowiednie „warstwy": budynek z zewnątrz, konkretne piętro, następnie pokój. Dzięki możliwości wprowadzenia do oprogramowania *RealShot Manager* dwuwymiarowych map terenu, obsługa systemu jest bardzo intuicyjna.

Migracja systemów monitoringu w stronę środowiska IP jest nieunikniona i już postępuje od strony centrum zarządzania przesuwając się w stronę kamer. Z pewnością warto przed podjęciem decyzji dokładniej przeanalizować oczekiwania wobec systemu monitoringu nie tylko dziś, lecz także i jutro.

Błażej Marciniak
menedżer produktu w Veracomp SA

Bezpieczeństwo biur terenowych: krok naprzód czy wstecz?

Biura terenowe są obecnie fundamentalną częścią każdego rozwijającego się przedsiębiorstwa. Jeśli warunki rynkowe są odpowiednie, biura terenowe mogą udostępnić przedsiębiorstwu nawet cały nowy region. Systemy bezpieczeństwa IT nowej generacji są czynnikiem umożliwiającym wzrost.

Przedsiębiorstwa o skali międzynarodowej w większym stopniu koncentrują się na działalności marketingowej zorientowanej na rynek lokalny, zaś tradycyjna struktura takiego przedsiębiorstwa ulega daleko idącym zmianom: w miejsce centralnego biura sterującego powstaje sieć równorzędnych oddziałów przedsiębiorstwa. Wśród tych kształtujących handel makrotrendów warto zwrócić uwagę na jedną ze strategii wzrostu, która odgrywa decydującą rolę w powodzeniu przedsiębiorstwa: otwieranie biur terenowych. Biura terenowe umożliwiają firmom wejście na nowy rynek poprzez wybranie lokalizacji w pobliżu klienta, czego celem jest poprawa cyklu sprzedaży.

Dlaczego jednak biura terenowe są obecnie tak atrakcyjną propozycją? W końcu kwestia wzrostu międzynarodowego nie jest sprawą nową. Decydujący wpływ na podjęcie decyzji ma stwierdzenie, czy warunki rynkowe są odpowiednie, lecz taką decyzję łatwiej podjąć dzięki wchodzącej technologii, która zwiększa wydajność biura terenowego. Nowe technologie, takie jak VPN, tworzą fundamenty, a wchodzące technologie, takie jak VoIP, zapewniają zaawansowane kanały komunikacyjne z innymi biurami.

Biorąc pod uwagę kluczową rolę IT w osiągnięciu zyskowności przez nowe biura terenowe oraz potrzebę szybkiego odzyskania kosztów związanych z rozpoczęciem działalności niezbędne jest, żeby systemy bezpieczeństwa IT gwarantowały zwrot z inwestycji. Jakikolwiek spadek wydajności może opóZnić firmę o wiele miesięcy przy próbie wchodzenia na nowy rynek. W przypadku każdej firmy jest to najgorszy typ opóZnienia, ponieważ świeże rynki praktycznie gwarantują sprzedaż. Ostatnie badania europejskie wykazały, że 70 proc. z 3000[1] administratorów systemów IT oświadczyło, że uaktualniali oni szczepionki oprogramowania antywirusowego w biurach terenowych i zdalnych komputerach raz na tydzień, a nawet rzadziej. Zarządzanie bezpieczeństwem w biurach terenowych jest problemem, który nie zniknie z kilku powodów.

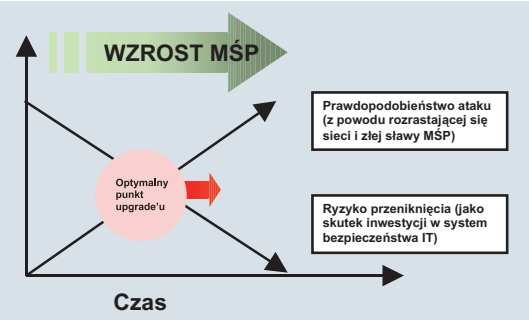
Po pierwsze, liczba ataków internetowych rośnie z powodu robaków, takich jak Sasser czy szkodliwego oprogramowania, jak np. Code Red. Po drugie, przeważnie zabezpieczenia w biurach terenowych nie są tak dobre, jak w głównej siedzibie firmy. Po trzecie, w biurach terenowych nie zawsze uzasadnione jest zatrudnienie administratora IT, w związku z czym całościowe zarządzanie bezpieczeństwem firmy może być utrudnione.

Zabezpieczenie najsłabszego elementu

Stare porzekadło *„Jesteś tak silny, jak twój najsłabszy punkt”* jest oczywiście prawdziwe także w systemach bezpieczeństwa IT. Z powyższych przyczyn wspólną troską managerów IT są biura terenowe. Rozwiązania bezpieczeństwa punktowego następnej generacji, takie jak Proventia M10 firmy Internet Security Systems są właściwym wyborem.

Takie urządzenia wykorzystują środki bezpieczeństwa, które do niedawna były dostępne wyłącznie na poziomie korporacji. Co więcej, umożliwiają one scentralizowane zarządzanie systemem, który posiada pojedynczy interfejs zarządzania bezpieczeństwem, obsługujący dwie bardzo istotne funkcje. Po pierwsze, pozwala on zmniejszyć obciążenie związane z zarządzaniem bezpieczeństwa, po drugie – pozwala administratorom na monitorowanie i pracę z systemem bezpieczeństwa jako całością, w przeciwieństwie do konieczności zajmowania się kilkoma systemami z osobna.

Dodatkowo, administratorzy IT w korporacjach muszą być świadomi potencjalnego skalowania systemów bezpieczeństwa pod kątem przyszłych technologii VoIP. Aby to zrobić, dostępna dziś nowa generacja rozwiązań powinna zapewniać ochronę inwestycji, oferując dołączenie środków bezpieczeństwa specyficznych dla przyszłych zastosowań, jak np. ochrona VoIP. Ten typ technologii zastosowany do ochrony punktu dostępowego może w przyszłości umożliwić managerom IT wprowadzenie zwiększających produktywność technologii, takich jak VoIP, w biurach międzynarodowych. Ważne jest też, że mogą one być dołączone do parasola bezpieczeństwa całej firmy.



Rys. 1

Co więcej, możliwość zmniejszenia prawdopodobieństwa ataku przez działania prewencyjne odsuwa konieczność uaktualnień systemów bezpieczeństwa, przez co jednocześnie redukuje konieczność kolejnych inwestycji w dłuższym terminie (patrz rys. 1).

Interesujące przykłady przedsiębiorstw wykorzystujących takie strategie zabezpieczenia prewencyjnego obejmują firmę Basis Technologies[2] – specjalistę w produkcji oprogramowania uzupełniającego rozwiązania firmy SAP. Zamiast zdecydować się na proste punktowe rozwiązanie, które wymagałoby uaktualniania co kilka miesięcy, Basis zdecydował się na wdrożenie w swoim biurze w Londynie systemu Proventia M10. Ponieważ to rozwiązanie zawiera zabezpieczenia tak zaawansowane, że były one do niedawna dostępne wyłącznie na poziomie centrali, prawdopodobieństwo, że firma Basis będzie musiała inwestować w kolejne rozwiązania zabezpieczające, jest bardzo znikome. Dzięki temu Basis może przeznaczyć swoje zasoby na szybkie zdobywanie rynku. Przykład ten pokazuje, że poprzez długoterminowe planowanie biura terenowe mogą zapewnić sobie długoterminowe oszczędności.

Zapobiegawcze zabezpieczenia

Mimo że systemy bezpieczeństwa IT przeważnie wdrażają strategie zabezpieczeń po zaistnieniu zagrożenia, to jednak kluczem do zabezpieczenia wydajności jest zapobieganie atakom. Zamiast kupować środki do szybkiego zwiększenia wydajności po ataku, przedsiębiorstwa zwracają się w stronę filozofii inwestowania w zabezpieczenia zapobiegające atakom. Gartner przewiduje, że przed końcem roku 2005[3] wydatki na nowe wdrożenia dedykowanych systemów zapobiegania włamaniom przekroczą wydatki przeznaczone na wdrożenia podobnych systemów do wykrywania włamań.

Zabezpieczanie jest połączeniem technik zarówno wykrywania, jak i zapobiegania, które bazują na pochodzących z grup badawczych informacjach na temat aktualnych i potencjalnych zagrożeń. Z powodu stale rosnącej liczby nowych i zmodyfikowanych zagrożeń, systemy bezpieczeństwa są jedynie tak dobre, jak najświeższe informacje wywiadowcze. Inwestując w rozwiązania bezpieczeństwa manager IT musi podjąć decyzję o wielkości zasobów dedykowanych do danego zagrożenia oraz o tym, jakie rozwiązanie zapobiegawcze powinno być użyte. Na przykład, laboratoria badawcze, takie jak X-Force firmy ISS, oferują różne poziomy analizy zagrożeń pogrupowane jako AlertCon 1-4, przekazujące informacje o słabych punktach, propozycjach działań i prognozach zagrożeń. Usługi takie, jak te z gwarancją bezpieczeństwa, są oferowane firmom z listy Global 500 oraz rządom różnych krajów świata, zapewniając subskrybentom spokojne funkcjonowanie.

Scentralizowane zarządzanie

Managerowie IT muszą dodatkowo rozważyć fakt, że mimo iż informacje wywiadowcze dla systemów zabezpieczających są najświeższe i najpełniejsze z możliwych, to sposób, w jaki te informacje są rozpowszechniane, jest równie istotny, jak one same. Nic nie da identyfikująca i analizująca zagrożenia grupa badawcza, taka jak X-Force, jeśli sieć zabezpieczeń nie jest na bieżąco uaktualniana.

Przeważnie personel IT ręcznie uaktualnia każde urządzenie, ale wskaZnik koszt/korzyść dla zapewnienia kompletnej platformy zabezpieczeń przed zagrożeniami w biurze terenowym jest przeważnie zbyt wysoki. Rozwiązaniem tego problemu jest wybór zabezpieczenia, które oferuje centralne zarządzanie. W rzeczywistości znaczy to, że każde z biur terenowych może odnosić korzyści z milionów dolarów zainwestowanych w badania bezpieczeństwa przez takie grupy, jak X-Force.

Dodatkowo, scentralizowane zarządzanie oznacza, że biura terenowe mogą otrzymywać informacje o najnowszych zagrożeniach bezpieczeństwa przez synchronizację z resztą sieci uruchomioną z centralnego punktu administracyjnego. Równie ważne jest to, że ataki na biura terenowe mogą być monitorowane i eliminowane z jednego punktu. Funkcja taka zapewnia wyższy poziom integralności w obrębie sieci i ogranicza koszty wsparcia IT w biurach terenowych.

Ewolucja sieci

W momencie, gdy nowe rozwiązania zabezpieczeń punktowych zostają zintegrowane z siecią biur terenowych, kluczowym punktem rozważań staje się ewolucja sieci. Przeważnie osoba podejmująca decyzje dotyczące działki IT uzasadnia wydatki poprzez zwrot z inwestycji. Jest on połączony z produktywnością, która jednocześnie jest zależna od zabezpieczeń.

Problem, z którym stykają się architekci systemów IT, zwłaszcza tych, w których występują biura terenowe

jest taki, że przeważnie klasyczne systemy są tworzone na zasadach inwestycji typu „czekaj i patrz". Oznacza to, że w momencie, gdy pojawią się problemy z bezpieczeństwem, nowa technologia jest kupowana, żeby je rozwiązać. Prowadzi to do bezładnego zestawienia różnorakich narzędzi bezpieczeństwa, które nie potrafią efektywnie współpracować ze sobą czyniąc cały system koszmarnym w zarządzaniu.

Poza tym filozofia taka w żaden sposób nie wpływa na skrócenie czasu pomiędzy odkryciem słabych punktów a atakiem. Ponieważ ataki stają się coraz bardziej zaawansowane, czekając z zabezpieczeniami na moment, kiedy atak zostanie przeprowadzony, sieć narażona jest na poważne awarie.

Następny etap tworzenia sieci odsuwa na bok te powszechne problemy dzięki wdrożeniu powszechnie stosowanych urządzeń zabezpieczających o wysokim stopniu bezpieczeństwa, dzięki czemu punkty monitorowania mogą być zdecentralizowane, co oferuje dużą elastyczność rozwiązania. Te punkty monitorowania mogą dostarczać cenne informacje do centralnego systemu zarządzającego.

Systemy zarządzające, takie jak SiteProtector firmy ISS, umożliwiają centralne zarządzanie zaporami ogniowymi, ochroną antywirusową, badanie treści www oraz poczty elektronicznej czy ochronę przed atakami typu *hacking* czy *Brute Forcing*, umożliwiając szybkie wykrycie potencjalnych zagrożeń przez agregacje i korelacje wykrytych zdarzeń.

Już teraz przedsiębiorstwa zamierzają stosować taką metodologię. Przykładem może być firma Heidelberger Sand und Kies[4], która produkuje wysokiej klasy materiały budowlane w Niemczech. Używa ona rozwiązania Proventia M10 jako podstawy do przyszłego scentralizowanego zarządzania.

Poza odpieraniem ataków systemy bezpieczeństwa nie mogą pomijać przyszłych technologii. Oferowanie urządzenia zabezpieczającego, które zasadniczo stosuje po kolei różne filtry zabezpieczające, mija się z celem, ponieważ wpływa to na opóZnienie sygnału. Często systemy przyśpieszają inspekcję na poziomie pakietu dzięki dużej przepustowości, ale tak naprawdę opóZnienia są najbardziej istotne dla aplikacji pracujących w sieci. Na przykład VoIP nie może funkcjonować przy opóZnieniach sieciowych większych niż 150 milisekund. Jeśli środki bezpieczeństwa zwiększają opóZnienia ponad tę wartość, istotne dla przedsiębiorstwa technologie, takie jak VoIP, odmawiają posłuszeństwa. Takie ograniczenia mogą oznaczać, że produktywność i rentowność biura terenowego maleje. Przedsiębiorstwa, które myślą o szybkiej ekspansji, muszą pomyśleć o tym wcześniej czy póZniej, w przeciwnym razie ryzykują porażkę na nowych rynkach.

Zabezpieczenia następnej generacji

Przy zastosowaniu technologii, takich jak ADSL, WLAN czy Wi-Max – pomagających zwiększyć rentowność biur terenowych – bezpieczeństwo tych biur staje się tematem, który będzie w centrum uwagi w 2006 roku. Fakt, że liczba nowych i modyfikowanych zagrożeń stale rośnie, a dodatkowo czas pomiędzy wykryciem słabych punktów a atakiem maleje, oznacza, że kolejna era w zarządzaniu systemami IT narodzi się w najbliższych latach.

Przedsiębiorstwa nie będą już usatysfakcjonowane łataniem dziur po przeprowadzeniu ataku, ale wymagane będzie przygotowanie na zagrożenie, zanim się ono pojawi. Co więcej, zabezpieczenia muszą sprostać przyszłym strategiom IT przedsiębiorstwa. Jeśli środki bezpieczeństwa nie pozwalają firmie na maksymalizację wykorzystania zwiększających produktywność aplikacji, to znaczy, że nie są warte inwestowania w nie.

Jeśli przedsiębiorstwa chcą czerpać korzyści z nowych rynków, to biura terenowe są właściwym sposobem na to, by być blisko klientów. Niemniej logistyczne przygotowanie sposobu, w jaki biuro to będzie współpracowało z resztą organizacji, jest równie istotne, jak decyzja związana z wejściem na ten rynek.

Bez właściwego wsparcia systemów IT i ich zabezpieczenia biura terenowe mogą stać się ciężarem, jednak jeśli otrzymają odpowiednie zasoby, mogą być przepustką do całkiem nowej ligi wzrostu.

Mariusz Rzepka
menedżer produktu w Veracomp

Przypisy

[1] Dane zaczerpnięte z badań Sophos, dostępne na stronie internetowej Sophos w dziale biura prasowego. Zamieszczony poniżej adres strony www przekieruje przeglądarkę na ogłoszenie prasowe odnoszące się do badań. Pełny adres strony jest następujący:
http://www.sophos.com/pressoffice/pressrel/uk/20030429survey.html.

[2] Pełne studium przypadku firmy Basis Technologies dostępne jest na stronie internetowej ISS (niestety, studium przypadku firmy Basis nie było ostatnio dostępne, dlatego adres internetowy zawarty jest w odnośniku. Pełny adres strony to:
www.iss.net).

[3] Dane z raportu Gartnera na 2005 rok „Bezpieczeństwo w kierunku zapobieganiu atakom". Badania z 29 paZdziernika 2004 r. Dot. G00123633.

[4] Pełne studium przypadku firmy Heidelberger Sand und Kies dostępne jest na stronie internetowej ISS. Zamieszczony odnośnik przekieruje przeglądarkę bezpośrednio do części strony ISS zawierającej informacje dla klienta. Pełny adres strony internetowej to:
http://www.iss.net/about/testimonials/heidelberger.php.

Trusted Computing sposobem na zabezpieczenie notebooków?

Technologia Trusted Computing jest w stanie przeciwdziałać zagrożeniom i problemom, które nękają dzisiejsze przedsiębiorstwa w zakresie IT. Pomaga także zwiększyć kontrolę nad sieciami korporacyjnymi oraz poprawić mobilność i produktywność w firmach. Tworzenie realnego bezpieczeństwa informatycznego wymaga przejrzystych koncepcji, dobrej technologii, infrastruktury i ludzi, którzy rozwijają, komunikują i używają produktów bezpieczeństwa.

O co chodzi w Trusted Computing?

Technologia Trusted Computing (TC), podobnie jak standardy tworzone przez Trusted Computing Group, są wysoko kompleksowymi zagadnieniami. Nie ma jednak oczywistej definicji TC. Najbliższa mojemu poglądowi mówi, że Trusted Computing jest środowiskiem IT lub obszarem w jego wnętrzu, w którym użytkownik, administrator IT lub partner biznesowy może mieć „zaufanie", z tym, że termin „zaufanie" zawiera w sobie inne terminy, takie jak „integralność systemów", „niezawodność" i „przewidywalność". Proste, prawda? I o to chodzi. Nie komplikujmy tymczasem tej prostoty definicjami pojęć, wprowadzaniem skrótów i szczegółów technologii. Tekst ten ma dawać ogólne pojęcie o zagadnieniu. Zacznę od klasyfikacji dwóch podstawowych założeń Trusted Computing.

Założenie 1

Użycie dodatkowych komponentów sprzętowych istotnie zwiększa bezpieczeństwo. Mówimy tu o tokenach, kartach chipowych oraz TPM (*Trusted Platform Module*).

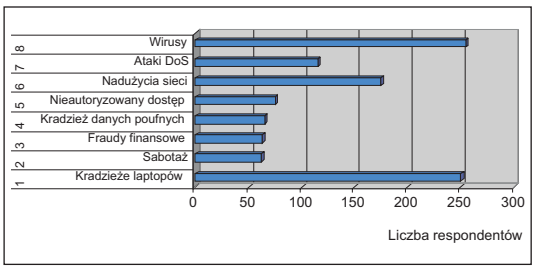
Założenie 2

Ostateczną ochronę danych gwarantuje tylko szyfrowanie. Klucze szyfrujące muszą być przechowywane w zgodzie z założeniem 1.

A teraz komentarz. O ile tokeny i karty chipowe są nam znane i powszechnie stosowane, to TPM może stanowić zagadkę – a jest to istotna część idei Trusted Computing. *Trusted Platform Module*, w jednym zdaniu, służy do zapewnienia integralności oprogramowania używanego w systemie, w tym rozwiązań bezpieczeństwa. TPM nie jest tylko ideą, ale rzeczywistością. W 2004 roku Microsoft ogłosił, że zaimplementuje TPM w nowym systemie operacyjnym, nazwanym roboczo *Longhorn*. Komponent systemu odpowiedzialny za TPM będzie nazywał się NGSCB (*Next Generation Secure Computing Base*). Nowy system Microsoftu jest wciąż w przygotowaniu, ale już dziś można kupić notebooki i desktopy wyposażone w TPM. Oczywiście, dostępne są rozwiązania szyfrujące współpracujące z TPM. A więc realizacja idei Trusted Computing przez użytkowników komputerów osobistych jest już teraz całkowicie możliwa. Popatrzmy zatem, gdzie i jak stosuje się Trusted Computing.

Jak to wygląda w praktyce?

Notebooki są aktualnie preferowanym narzędziem pracy w firmach. Zwykle zawierają one dużą liczbę ważnych i wartościowych danych. Możemy sobie łatwo wyobrazić liczbę zagrożeń, jakim podlegają mając kontakt z siecią globalną.



Zródło: CSI/FBI: Przestępstwa komputerowe i badanie bezpieczeństwa 2003

Komputery przenośne są zagrożone wieloma typami identyfikowalnych ataków, w tym także „niesieciowych". Jak wynika z wykresu, pierwszym typem są ataki wirusowe, takie same jakie zagrażają tradycyjnym komputerom PC. Konieczne jest zatem wyposażenie zsieciowanych notebooków w dobre oprogramowanie antywirusowe. Ale co zrobić z drugim co do ważności zagrożeniem – kradzieżą? Kradzież oznacza, że tracimy kontrolę nad naszą (firmową) własnością. Przytoczę to, co Microsoft mówi na ten temat w *„Dziesięciu niezmiennych prawach bezpieczeństwa"*. Prawo numer 3 brzmi: *Jeżeli „zły człowiek" dostaje fizyczny, nieograniczony dostęp do twojego komputera, ten komputer po prostu przestaje być TWÓJ*. Ale Microsoft tworzy systemy operacyjne, a my mamy problem ze sprzętem. Czy powinniśmy zatem pogodzić się z przykrą świadomością, że posiadanie notebooka stanowi zagrożenie samo w so-

bie dla naszych danych i nas samych? Otóż niekoniecznie. Jeżeli przesuniemy spojrzenie poza oprogramowanie operacyjne, znajdziemy odpowiedZ.

Sklasyfikujmy komputery przenośne w dwóch roboczych kategoriach. Jedną z nich jest stan, w którym notebook jest „wyłączony". To zwykle stan, w którym komputer dostaje się w ręce złodzieja. Przyjrzyjmy się zatem problemowi zabezpieczenia „włączenia zasilania".

WyobraZmy sobie, że notebook zostaje skradziony lub po prostu pozostawiony w taksówce. I tu okazuje się, że pomimo utraty sprzętu ten wciąż może być chroniony przed nieautoryzowanym odczytem danych! Metoda ochrony w takich przypadkach nazywa się *Bulk Encryption*. *Bulk Encryption* oznacza, że każdy sektor na dysku twojego byłego notebooka jest zaszyfrowany. Dotychczas można było przynajmniej teoretycznie zapewnić szyfrowanie danych na notebookach, ale wyłącznie na poziomie oprogramowania systemowego lub aplikacji. Takie indywidualne szyfrowanie plików i folderów wymagało jednak specyficznej polityki bezpieczeństwa i zdyscyplinowanych użytkowników. Zdyscyplinowany użytkownik to z kolei taki, który chce, ma czas i dba o bezpieczeństwo swoich plików, usuwa te, których już nie potrzebuje itd. Użytkownik musiałby stosować pewnego typu politykę bezpieczeństwa, choćby własną. Ale takie zachowania użytkowników zwykle nie funkcjonują w realnym świecie. Kto administruje sieciami, ten wie, że tacy użytkownicy są jak mityczny Graal – to legenda. Rozwiązanie stanowi tutaj metoda *Bulk Encryption*. Uwalnia bowiem użytkowników od zadań administratora sieci, czyni ich bardziej produktywnymi i bezpiecznymi. Po prostu szyfrowanie *Bulk Encryption* działa w tle, bez żadnych interakcji z użytkownikiem i jest od niego zupełnie niezależne. *Bulk Encryption* oznacza zatem pełną ochronę notebooka w trybie „wyłączony". Zabezpiecza zarówno system plików, jak i bazę danych SAM (*Security Account Manager*), w której składowane są hasła. Ochrona SAM jest konieczna, gdyż złodziej mógłby próbować podmienić bazę SAM. *Bulk Encryption* zabezpiecza system operacyjny, aplikacje, dane – po prostu zabezpiecza wszystko, co jest na dysku. Wygodne, prawda? Powstrzymuje złodzieja nawet przed odczytaniem plików, które pozostały otwarte na pulpicie, kiedy komputer przeszedł w stan hibernacji.

Bulk Encryption jest technologią aktualnie wykorzystywaną na milionach stacji roboczych na całym świecie. Te zabezpieczenia nigdy, w ciągu 10 lat istnienia i rozwoju, nie zostały złamane. Jednak zagadnienia bezpieczeństwa nie są statyczne – zagrożenia i scenariusze obrony wciąż ewoluują. Z tego powodu każdy producent powinien wychodzić poza istniejące dzisiaj zagrożenia i sposoby przeciwdziałania. Takim wyjściem „poza" jest – dla przykładu – praktyczne wdrożenie ochrony sprzętowej z kluczami szyfrującymi. Innym zagadnieniem, które można wziąć pod uwagę, jest problem ataków słownikowych. Takie ataki wykazują dużą skuteczność w zastosowaniu przeciwko rozwiązaniom w pełni programowym, ale stają się nieskuteczne w zderzeniu ze strukturami sprzętowymi. To jest właśnie miejsce do zastosowania wspomnianego TPM (*Trusted Platform Module*). Praktycznym, czysto sprzętowym, zastosowaniem TPM jest na przykład sytuacja, w której ktoś próbuje podłączyć skradziony dysk do innego systemu. Jeżeli nawet zna lub złamie hasła dostępu, to odczytanie danych będzie niemożliwe – taka akcja wymaga autoryzacji „swojego" TPM. To tak zwany *Machine Binding*, czyli „przywiązanie" danych do platformy sprzętowej.

Oczywiście, dla złodzieja problemem nierozwiązywalnym, poza TPM, pozostanie wciąż zaszyfrowanie danych na nośniku.

Funkcja *Bulk Encryption* i koncepcje Trusted Computing są realizowane aktualnie przez unikatowe oprogramowanie szyfrujące SafeGuard Easy firmy Utimaco. Oprogramowanie to razem z TPM i IBM ESS (*Embeded Security Subsystem*) zostało – dla przykładu – zastosowane w kilkunastu instytucjach finansowych w Europie. Instytucje te używają zwykle notebooków jako rozbudowanych stacji klienckich – są wyposażone w oprogramowanie pozwalające świadczyć usługi konsultingowe klientom końcowym. Gdyby takie oprogramowanie z danymi klientów dostało się w niepowołane ręce – mogłoby dojść do spadku konkurencyjności rynkowej tych firm. Łatwo sobie wyobrazić także dużo dotkliwsze konsekwencje.

Zaczęliśmy od teorii Trusted Computing. Potem były wzmianki o TPM, opisy *Bulk Encryption* i kilku koncepcji oraz pomysłów na rozwój zabezpieczeń w informatyce. Kończę ten wstęp do Trusted Computing praktycznymi przykładami wziętymi z naszej dzisiejszej rzeczywistości biznesowej. Istnieją już gotowe i sprawdzone produkty, będące urzeczywistnieniem założeń przyjętych przez Trusted Computing Group. Zaleceń TCG używają do budowy komponentów najwięksi producenci, tacy jak Microsoft, IBM, ale działają też firmy specjalizowane, jak Utimaco, dostarczające całej gamy produktów szyfrujących dane lokalnie i w transmisji sieciowej.

Wiemy, że bezpieczeństwo IT nie jest procesem statycznym, ale postępującym. Ta krótka lektura pokazuje, że idea i treść Trusted Computing stanowi istotną podstawę do tworzenia silnych produktów bezpieczeństwa, których stosowanie wzmacnia bezpieczeństwo IT w firmach, a przez to – ich konkurencyjność i pozycję rynkową. Trusted Computing nie jest zatem jedną z tysięcy bezużytecznych koncepcji naukowych, choć jej bezpośrednia przydatność do użytku końcowego jest nikła. Producenci IT od lat jednak wdrażają Trusted Computing. Biorąc do ręki płytę z takim produktem, jak SafeGuard Easy warto wiedzieć, że stanowi ona inkarnację wielu lat prac naukowych, konsultacji branżowych i testów. Zawarte na niej oprogramowanie naprawdę będzie chronić nasze dane – nawet jeżeli nasz notebook jest już naszym BYŁYM notebookiem. Czego, oczywiście, ani sobie, ani Wam nie życzę.

Łukasz Światek
menedżer produktów w Veracomp SA

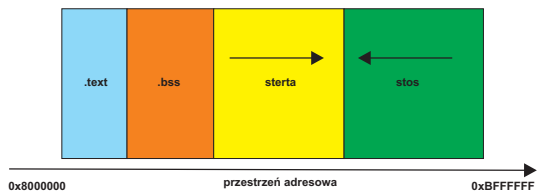
Techniki obrony przed atakami przez przepełnienie bufora

Pośród nagłówków list dyskusyjnych raportujących podatności w aplikacjach często zobaczyć można pojęcie przepełnienia bufora (ang. buffer overflow). Na ogół występuje ono w kontekście możliwości zdalnego wykonania dowolnego kodu albo przynajmniej ataku typu DoS, czyli unieruchomienia podatnej aplikacji. Eksperci przewidują dalszy wzrost wykrywanej liczby takich podatności zwłaszcza w dużych systemach informatycznych o niedostępnym kodzie źródłowym. Narażone są systemy operacyjne, motory baz danych, serwery web. W niniejszym artykule chciałbym przybliżyć czytelnikowi mechanizmy przepełnienia bufora, pokazać, skąd się biorą podatności tego typu i jak można się przed nimi bronić.

Przyczyny

Przepełnienie jest efektem błędu programisty, który nie kontroluje długości i formatu danych przetwarzanych przez aplikację. Jest to najczęściej przypadłość aplikacji napisanych w C i C++, ponieważ w tych językach najczęściej stosowana jako bufor danych tablica jest jedynie wskaźnikiem do pamięci i nie przechowuje informacji o swojej długości. Konstrukcja taka, kiedyś podyktowana względami wydajnościowymi, dzisiaj odbija się czkawką. Jakie są konsekwencje wpisania do tablicy większej liczby danych niż jest ona w stanie pomieścić? Żeby się o tym przekonać, należy zrozumieć podstawy zarządzania pamięcią.

Współczesne systemy operacyjne stosują technikę tzw. pamięci wirtualnej. Oznacza ona, że proces nie ma dostępu do bezpośredniej adresacji pamięci fizycznej, ale jest wyposażony we własną przestrzeń adresową. Niemal zawsze (z wyjątkiem kilku systemów mainframe'owych) jest to pełna, 32-bitowa przestrzeń dynamicznie mapowana przez jądro do rzeczywistych zasobów komputera: pamięci operacyjnej i pliku bądź partycji wymiany. Mapowanie to następuje w jednostkach zwanych stronami. Ma ono wiele zalet. Obok wygody związanej z zarządzaniem pamięcią i programami nie „wpadającymi" na siebie na skutek błędu programisty, istnieje też możliwość wprowadzenia praw dostępu dla określonej strony pamięci operacyjnej. Rodzaje tych praw zależą od systemu operacyjnego i architektury (całość operacji mapowania jest wspomagana sprzętowo przez procesor), ale zwykle funkcjonuje przynajmniej rozróżnienie pomiędzy stroną RO (ang. *Read Only*) a RW (ang. *Read/Write*). Przyjrzyjmy się teraz, jak wygląda wykorzystanie pamięci przez proces. Uruchomienie pliku wykonywalnego powoduje start tzw. loadera, czyli struktury odpowiedzialnej za prawidłowe umieszczenie programu w pamięci. Loader relokuje (zmienia adresy używane w kodzie, tak by pasowały do aktualnej mapy pamięci) i ładuje do pamięci poszczególne segmenty programu. Trzy najważniejsze z nich to .text, .bss i .data. Segment .text zawiera kod programu. Strony pamięci go zawierające mają z reguły ustawioną flagę RO. .data i .bss to dane programu, odpowiednio zainicjowane i nie. Obie te przestrzenie nie wyczerpują jednak zasobów potrzebnych procesowi do składowania danych, istnieją bowiem sytuacje, w których programista nie jest w stanie przewidzieć liczby pamięci, której używać będzie program. Jedną z nich jest uruchomienie funkcji. Na etapie pisania programu nie da sie powiedzieć, ile razy funkcja będzie wywołana, czy to z poziomu samej siebie, czy innych funkcji. Nie wiadomo zatem, ile kopii danych lokalnych będzie potrzebnych jednocześnie. Rozwiązaniem tego problemu jest stos. Stos jest strukturą danych implementującą model LIFO (ang. *Last In First Out*), przypominającą rzeczywisty stos papieru albo talię kart. Dane są zdejmowane z wierzchołka stosu i odkładane na wierzchołek. Struktura taka nadaje się idealnie do przechowywania danych lokalnych funkcji, ponieważ zmienne można na niej odkładać w kolejności, w której funkcje te są wywoływane. Drugim przypadkiem szczególnym są dane alokowane dynamicznie, którym pamięć przydzielana jest z tzw. sterty. Przepełnienia stosu (*stack overflow*) i sterty (*heap overflow*) stanowią trzon najpopularniejszych podatności wynikających z możliwości nieuprawnionego manipulowania pamięcią.



Rys. 1. Przestrzeń adresowa procesu. Linux x86.

Przyjrzyjmy się bliżej samemu mechanizmowi ataku. Po załadowaniu programu do pamięci mógłby on wyglądać na przykład tak, jak na rys. 1.

Przykład ten dotyczy systemu Linux na platformie x86, ale jego konsekwencje są ogólne i w równym stopniu dotyczą innych systemów.

Przeanalizujmy, co dokładnie dzieje się, kiedy wołana jest nowa funkcja, jak w poniższym przykładzie (1):

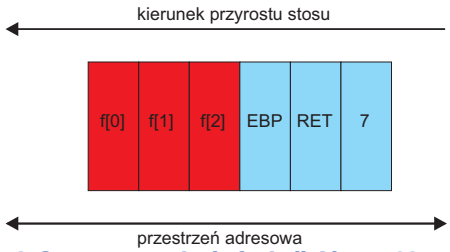
```
function a(int k) {
int f[3];
f[0] = k;        <-----------------------------------(2)
}

void main(){
a(7);            <-----------------------------------(1)
}
```

Kolejno:

1. Na stos odkładane są argumenty funkcji (w odwrotnej kolejności), w tym przypadku liczba 7;
2. Na stos odkładany jest adres powrotu funkcji (rejestr IP);
3. Na stos odkładany jest tzw. wskaźnik ramki (rejestr EBP);
4. Następuje skok do nowego adresu;
5. Na stosie rezerwowane jest miejsce na wszystkie zmienne lokalne funkcji (w tym przypadku 10-elementową tablicę f).

W punkcie (2) stos wygląda jak na rys. 2. Jak łatwo zauważyć, wobec braku kontroli granic tablicy, nadpisanie nieistniejącego f[5] skończy się modyfikacją adresu powrotu funkcji, co oznacza dla atakującego przejęcie kontroli nad wykonaniem programu.



Rys. 2. Stos po wywołaniu funkcji. Linux x86.

Konsekwencje

Współczesne procesory nie rozróżniają kodu od danych. Mając do dyspozycji aplikację podatną na przepełnienie bufora, atakujący może zapisać na stosie kod i przenieść do niego sterowanie. Jest to najczęstsza i najbardziej powszechna forma przepełnienia stosu, jako że na 32-bitowych procesorach z rodziny x86 nie ma osobnej flagi dającej prawo wykonania pamięci, a więc znajdujący się na stosie kod można wykonywać tak samo jak segment .text. Jednak nawet gdyby stos nie był wykonywalny, nie oznacza to jeszcze całkowitego zablokowania ataków z przepełnieniem bufora. Atakujący może bowiem odłożyć na stosie parametry wywołania systemowego bądź funkcji zawartej w którejś z bibliotek dzielonych i (zakładając, że uda mu się poznać adres tego wywołania) skoczyć do kodu zdefiniowanego gdzie indziej z własnymi parametrami.

Tę klasę ataków określa się zwyczajowo jako *'return-to-libc'*, od nazwy biblioteki standardowej języka C. Ograniczeniem jest jedynie ilość miejsca na stosie, którą dysponuje atakujący i uprawnienia atakowanego procesu.

Problem nie dotyczy jedynie aplikacji serwerowych, przyjmujących dane z internetu. Podatna może być na przykład biblioteka obsługująca pliki graficzne. W ten sposób specjalnie spreparowany obrazek będzie mógł być użyty do wykonania dowolnej operacji z prawami użytkownika go otwierającego. Co więcej, podatność biblioteki może implikować podatność wielu aplikacji używających jej do obróbki obrazu.

Ważne, żeby uświadomić sobie, że maszyna, na którą przypuszczono atak umożliwiający wykonanie dowolnej operacji w systemie, musi zostać przeinstalowana, ażeby znowu można ją było traktować jako platformę zaufaną. Przy odpowiednich środkach i determinacji atakujący, który uzyskał najwyższy poziom uprawnień w zaatakowanym systemie, może tak zamaskować swoją obecność, że jego działania przestaną być widoczne dla administratora systemu. Co więcej, nie mając pewności kiedy doszło do krytycznego zdarzenia, nie można ufać kopii zapasowej systemu, może ona bowiem zawierać zarówno tzw. *rootkit*, czyli aplikację ukrywającą napastnika w systemie i zapewniającą mu uprzywilejowany dostęp, jak i zwyczajnie zmodyfikowane dane, które nie będą już dłużej wiarygodne.

Remedia

Co można zatem zrobić, aby poradzić sobie z problemem przepełnień bufora? Z całą pewnością uważniej pisać aplikacje. Nawoływanie do rozwagi w tym zakresie trwa już prawie 10 lat (pierwszy głośny artykuł[1] na temat tej techniki włamań ukazał się w listopadzie '96), a zgłaszanych podatności jest ciągle coraz więcej, co więcej – liderami statystyk pozostają te same firmy.

Nie wynika to z braku odpowiednich metod zarządzania jakością. Istnieją wyspecjalizowane firmy zajmujące się tzw. audytem kodu źródłowego. Za pomocą dedykowanych narzędzi i eksperckiej wiedzy weryfikują kod źródłowy pod kątem występowania w nim niebezpiecznych konstrukcji. Pozwala to nie tylko zmniejszyć ryzy-

ko włamania, ale i ograniczyć odpowiedzialność cywilną firmy piszącej oprogramowanie. Podpisując umowę o stworzenie aplikacji warto zawsze sprawdzić, czy dostawca wykonuje niezależny audyt kodu (niezależny, czyli wykonywany przez zewnętrzną firmę gwarantującą jego jakość swoją renomą), czy też zapisuje w umowie licencyjnej *„dostawca nigdy i pod żadnym pozorem nie ponosi żadnej odpowiedzialności za straty wywołane użytkowaniem...”*.

Naturalnie, ogromna większość używanych aplikacji jest oprogramowaniem generalnego przeznaczenia, co bardzo ogranicza możliwość wpływania na jego producenta. Co wtedy? Większość popularnych systemów operacyjnych implementuje obecnie zabezpieczenia przed przepełnieniem stosu. Microsoft w Windows 2003 SP1 i Windows XP SP2 implementuje technologię zwaną DEP[2]. Używa ona mechanizmów sprzętowych (głównie na procesorach 64-bitowych) i programowych do zapobieżenia wykonania kodu na stosie.

Podobny mechanizm, nazwany PaX[3], już od dawna istnieje dla systemów Linux. Programowa wersja obu mechanizmów sprowadza się do odkładania na stosie dodatkowej, losowej wartości zwanej canary, której integralność jest później sprawdzana.

Aplikacja, która stwierdzi atak na samą siebie, może w ten sposób dobrowolnie zakończyć swoje działanie zanim zostanie wykorzystana jako nośnik kodu napastnika. Podejście takie ma jeden mankament – wymaga rekompilacji aplikacji. Nie jest to duży kłopot dla użytkowników aplikacji o dostępnym kodzie źródłowym, wiele z nich posiada już skompilowane wersje zgodne z opisanymi technikami zabezpieczeń.

Nieco inaczej wygląda sytuacja w obszarze zabezpieczeń przed atakami typu *‘return-to-libc’*. W ramach pakietu PaX otrzymujemy implementację techniki ASLR (ang. *Address Space Layout Randomization*), poważnie utrudniającą atakującemu odgadnięcie adresu zadanej funkcji w pamięci. Systemy operacyjne Microsoft’u jak dotąd nie posiadają takiego zabezpieczenia, tym niemniej jest ono możliwe do zrealizowania przez oprogramowanie stron trzecich[4].

Co jednak zrobić, jeśli chroniona aplikacja jest jednocześnie niemożliwa do zmodyfikowania, a z drugiej strony – zbyt krytyczna, żeby ingerować w system zewnętrznym oprogramowaniem? Na tym etapie pozostaje inspekcja danych wysyłanych do i z aplikacji na poziomie sieciowym. Trzeba powiedzieć, że w ogólnym przypadku znalezienie kodu mogącego przepełnić bufor jest dość trudne. Oparte na sygnaturach systemy ochronne, nawet często uaktualniane, są pomyślane raczej jako zabezpieczenie przed znanymi i powszechnymi robakami niż przed twórczym umysłem człowieka.

System, który miałby chronić przed przepełnieniami bufora na poziomie ogólnym, powinien:

- ✔ zrozumieć i zdekodować protokół, którym posługuje się aplikacja;
- ✔ zidentyfikować i wyizolować parametry podejrzewane o to, że zawierają kod binarny;
- ✔ zdekodować i zdeasemblować kod binarny oraz przeprowadzić jego analizę;
- ✔ wobec stwierdzenia cech charakterystycznych dla ataku, zablokować komunikację.

Przykładem takiego systemu dla aplikacji webowych może być Web Intelligence[5] firmy Check Point, zawierający moduł Malicious Code Protector, który potrafi zablokować każdą komunikację Web zawierającą kod wykonywalny.

Rozwój w dziedzinie systemów chroniących przed całą klasą ataków, jaką są przepełnienia bufora, jest obecnie niezwykle dynamiczny zwłaszcza w grupie systemów analizujących ruch przed dotarciem do docelowego systemu.

W nadchodzącym czasie należy spodziewać się zarówno nowych premier, jak i intensywnego wzrostu możliwości istniejących systemów ochronnych. To ważna wiadomość, bowiem w sytuacji, kiedy czas pomiędzy publikacją informacji o podatności a jej masowym wykorzystaniem ciągle maleje, stosowanie systemów chroniących przed całą klasą ataków staje się koniecznością.

Michał Kułakowski
inżynier bezpieczeństwa IT w Veracomp SA

Przypisy

[1] Aleph1 „Smashing The Stack For Fun And Profit”, Phrack#49.

[2] http://support.microsoft.com/kb/875352.

[3] http://www.grsecurity.net/.

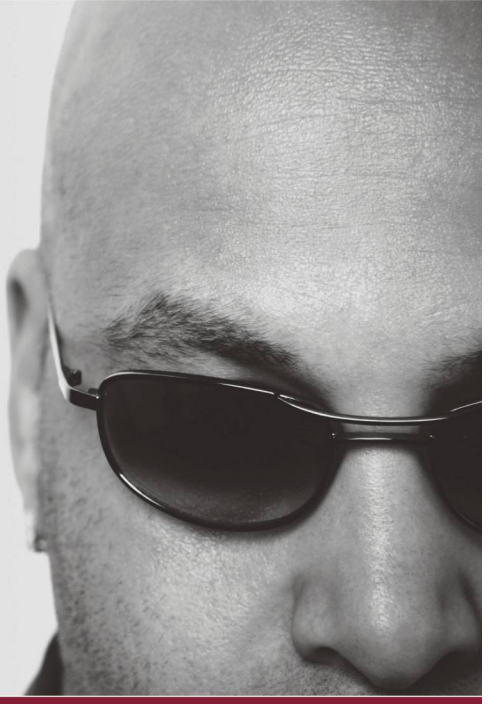
[4] np. produkt WehnTrust firmy Wehnus (http://www.wehnus.com).

[5] http://www.checkpoint.com/products/web_intelligence/index.html.

O autorze

Michał Kułakowski
jest inżynierem bezpieczeństwa IT
w Dziale Systemów Sieciowych
firmy Veracomp SA.
W branży od czterech lat.
Z autorem można skontaktować się
pisząc na adres:
michal.kulakowski@veracomp.pl.

Chciałbyś, żeby ktoś taki
myszkował po Twoich danych?



CheckPoint Integrity zabezpiecza Twoje dane przed oprogramowaniem szpiegowskim

CheckPoint Integrity™, niekwestionowany lider ochrony stanowisk roboczych, chroni przed stratami finansowymi powodowanymi przez cyberprzestępców korzystających z oprogramowania szpiegowskiego czy koni trojańskich w celu kradzieży istotnych danych lub bezprawnego korzystania z infrastruktury informatycznej przedsiębiorstwa.

Poza neutralizacją oprogramowania szpiegowskiego Integrity zapewnia kompleksową, pewną, sprawdzoną ochronę stanowisk roboczych oraz wykorzystywanych sieci przed robakami internetowymi, atakami hybrydowymi czy innymi wyrafinowanymi metodami współczesnych ataków. Techniki ochrony oferowane przez Integrity obejmują: osobisty firewall, blokowanie ruchu wychodzącego, przeciwdziałanie włamaniom, usuwanie oprogramowania szpiegowskiego oraz gwarancję dostępu do sieci tylko dla sprawdzonych i bezpiecznych komputerów. Integrity zapewnia niezrównaną łatwość wdrożenia i zarządzania.
Integrity współpracuje z urządzeniami sieciowymi wielu producentów, realizując ideę Total Access Protection, w celu zagwarantowania dostępu do sieci tylko dla komputerów spełniających założenia przyjętej polityki bezpieczeństwa.

W celu uzyskania więcej informacji
zapraszamy do kontaktu pod adresem:
bezpieczenstwo@veracomp.pl

Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

veracomp

Veracomp SA jest Autoryzowanym Dystrybutorem
rozwiązań Check Point Software Technologies.
Prowadzi sprzedaż wyłącznie za pośrednictwem Partnerów Handlowych.

www.veracomp.pl

Sony: nowa zewnętrzna obudowa do kamery SNC

Na rynku polskim pojawiły się nowe, zewnętrzne obudowy Sony do kamery SNC RZ25P. Hermetyczna obudowa i rozmaite uchwyty pozwalają na zamontowanie kamery na masztach i ścianach na zewnątrz budynków.

Nowa obudowa zewnętrzna do kamery Sony SNC-RZ25P wyposażona została w wodoszczelną i odporną na uszkodzenia przeszkloną kopułę. Opcjonalnie do obudowy można dodać specjalne uchwyty montażowe, które umożliwią zainstalowanie kamery na maszcie lub przy ścianie. Aby zainstalować kamerę na maszcie lub na rogu budynku trzeba wykorzystać dwa uchwyty. Najpierw konieczne jest zastosowanie uchwytu naściennego (SONIP-SNCA-WM20G). Następnie do obudowy z uchwytem naściennym można zamontować uchwyt montażowy do masztu (SONIP-SNCA-PM3) lub uchwyt montażowy narożny (SONIP-SNCA-CA2).

Uniwersalna ruchoma kamera IP

SNC RZ25P to najnowsza ruchoma kamera IP Sony. Obsługuje standardy kompresji MPEG-4 oraz JPEG. Można ją podłączyć bezpośrednio do sieci LAN lub do sieci bezprzewodowej poprzez złącze FE 10/100 Mbps (RJ45). Wbudowany serwer www umożliwia konfiguracji i natychmiastowy podgląd obrazu w standardowej graficznej przeglądarce www. Poziomy zasięg wynosi maksymalnie 340 stopni, pionowy do 120 stopni, co w połączeniu z 18-krotnym przybliżeniem optycznym daje kamerze możliwość objęcia nadzorem nawet dużego magazynu czy parkingu.

Podgląd typu „panorama" oraz bezpośredni i funkcja „dzień/ noc"

Kamera umożliwia przełączanie czułości, przystosowując się automatycznie do zmieniających się warunków oświetlenia. W ciągu dnia kamera generuje kolorowy obraz do poziomu oświetlenia 0,7 luksów, w nocy przełącza się na tryb czarno-biały, dając obraz nawet przy oświetleniu 0,01 luksa. Przełączanie może być ustawione na 3 sposoby: automatyczne, manualne lub czasowe (zegar). SNC RZ25P może w cyfrowy sposób połączyć obrazy z poszczególnych sfer i wygenerować w ten sposób nieruchomą

panoramę monitorowanego obiektu. Wskazanie punktu podglądu następuje poprzez kliknięcie wybranego punktu na panoramie. Kamera ma także możliwość zaprogramowania pozycji (kombinacja położenia poziomego, pionowego oraz zbliżenia).

Obraz wysokiej rozdzielczości

Dzięki wbudowanemu przetwornikowi 1/4 Exwave HAD CCD kamera SNC RZ25P przekazuje bardzo ostre i wyraźne obrazy w maksymalnej rozdzielczości 640x480 pikseli, zarówno w kompresji MPEG-4, jak i M-JPEG. Maksymalna wydajność kamery w klatkach na sekundę (fps):

- ✔ standard JPEG: 25 fps (320x240), 18 fps (640x480);
- ✔ standard MPEG-4: 25 fps (320x240), 15 fps (640x480).

Kamera posiada także analogowe wyjście wideo, dzięki któremu sygnał wideo może być przekazywany do analogowego monitora lub urządzenia rejestrującego (złącze BNC).

Dwukierunkowa transmisja sygnału audio

Kamera SNC RZ25P obsługuje standardy kodowania audio: ITU-T G.711 oraz G.726. Dzięki temu kamera wyposażona w złącze wejściowe na mikrofon może monitorować obiekt także akustycznie, wykryty sygnał audio traktując jako alarm. Kamera posiada także wyjście audio na głośniki aktywne. Pozwala to operatorowi przekazywać do monitorowanego obiektu komunikaty głosowe, ostrzeżenia itp.

Funkcje alarmu

Kamera SNC RZ25P posiada wbudowaną funkcję detekcji ruchu, a przy podłączonym mikrofonie także dźwięków. Funkcja ta umożliwia przekazywanie informacji o alarmie na zewnętrzne złącze niskoprądowe. Kamera może także przyjmować takie sygnały na wejściowy obwód niskoprądowy (czujnik w drzwiach, itp.). Pamięć Pre-/Post-Alarm umożliwia zarejestrowanie kilku, kilkunastu sekund podglądu sprzed zdarzenia, które wywołało alarm. Pojemność bufora (definiowana w menu) wynosi:

- ✔ kompresja MPEG-4: ok 30 sekund (pre-/post-15 sek.); przy 320x240, 25 fps i 512 kbps;
- ✔ kompresja JPEG: ok. 10 sekund (pre-/post-5 sec), przy 320x240, 15 fps i jakości obrazu na poziomie 3.

Dane rejestrowane są przesyłane na serwer FTP lub do aplikacji zarządzającej RealShotTM Manager Sony. Nieruchome obrazy mogą być wysyłane także na zdefiniowany adres e-mail (3 obrazy w formacie JPEG).

Funkcje sieciowe

W celu kontrolowania QoS (Quality of Service) kamera SNC RZ25P stosuje adaptacyjną kontrolę generowanych klatek na sekundę. W ten sposób dostosowuje się do wydajności sieci, zapobiegając zrywaniu strumienia wideo i audio. Kamera zapewnia jednoczesny dostęp dwudziestu użytkownikom w trybie JPEG oraz dziesięciu w MPEG-4. Dzięki obsłudze standardu multicast kamera może transmitować strumień wideo i audio do większej liczby użytkowników. Dzieje się to we współpracy z multicastowym routerem lub przełącznikiem warstwy 3. Filtrowanie adresów IP pozwala ograniczyć dostępu do kamery. Można stworzyć maksymalnie 10 grup adresów IP uprawnionych do łączenia się z kamerą. Możliwe jest także tworzenie do 4 grup użytkowników o zróżnicowanych uprawnieniach.

Współpraca z systemem monitoringu RealShot Manager

Wykorzystując aplikację RealShotTM Manager można zbudować profesjonalne centrum monitoringu, zapewniające całkowitą kontrolę nad kamerami i serwerami kamer Sony. Przechowywane archiwa mogą być przeszukiwane po znacznikach daty, alarmach oraz dodanych komentarzach. Intuicyjny interfejs zapewnia szybki dostęp do kamery/ archiwum. Dzięki możliwości podłożenia przestrzennej mapy monitorowanego obiektu jako tła aplikacji łatwo się zorientować w lokalizacji każdej z kamer. Do zbudowania rozległej infrastruktury transportowej można wykorzystać szybkie sieci bezprzewodowe np. system Tsunami MP.11a firmy Proxim, będący w ofercie firmy Veracomp.

Autoryzowanym dystrybutorem
rozwiązań
Sony networld Video
na rynku polskim
jest Veracomp SA.
Więcej informacji
można znaleźć na stronie

www.veracomp.pl

extranet
internet creator

Platforma NetAdmin
nowoczesne rozwiązania dla biznesu

W związku z tym, iż serwisy internetowe wymagają dość częstej aktualizacji to w przypadku standardowych rozwiązań (przekazywanie materiałów, poprawek, informacji do specjalizowanej firmy) nie zawsze docierają one na czas do odwiedzających serwis. W wyniku powstałych opóźnień odwiedzający stronę z trudem znajdują właściwe informacje, rośnie liczba wiadomości nieaktualnych lub powtarzających się, nie ma spójności w wyglądzie graficznym witryny i w nawigacji, na głównej stronie brakuje informacji o najważniejszych nowościach w serwisie, piętrzą się trudności z zarządzaniem dużą liczbą plików.

W takich przypadkach naturalną rzeczą jest przeniesienie obowiązku aktualizacji serwisu na osoby tworzące jego treść i nadanie im uprawnień do samodzielnej modyfikacji witryny. Takie właśnie możliwości daje stworzony przez nas System Zarządzania Serwisem Internetowym **NetAdmin** Ze względu na łatwość jego obsługi jest on idealnym narzędziem nawet dla osób z minimalną wiedzą informatyczną.

www.extranet.pl | tel.623-23-54, fax.657-29-57 | email: biuro@extranet.pl

System do zarządzania czasem pracy X/TIME

LST

System X/TIME to rozwiązanie do elektronicznego zarządzania czasem pracy, wykorzystywane w przedsiębiorstwach różnej wielkości, różnych branż. Dzięki swej elastyczności system posiada referencje w branży przemysłowej, w handlu, bankowości, w sektorze ubezpieczeniowym, jak i w administracji publicznej.

Wszystkie obszary funkcjonalne objęte działaniem systemu X/TIME, takie jak rejestracja czasu pracy, kontrola dostępu, rejestracja danych stołówki czy planowanie zmian są obsługiwane za pomocą jednej karty dostępu, przez jeden system o jednolitej bazie danych i platformie obsługi. Wszystkie dane w ramach systemu są dostępne w czasie rzeczywistym, co umożliwia korzystanie z takich funkcji systemu, jak monitorowanie obecności pracowników online czy monitorowanie działania terminali kontroli dostępu i rejestracji czasu pracy.

System X/TIME umożliwia korzystanie z nowoczesnych technologii, takich jak obsługa aplikacji przez internet czy rejestracja czasu pracy z wykorzystaniem telefonów komórkowych. Jest systemem otwartym, umożliwia wymianę danych z narzędziami Microsoft oraz Lotus Notes. System operacyjny Unix lub Windows, na którym bazuje X/TIME oraz wykorzystanie zaawansowanych baz danych, zapewnia szybkie przetwarzanie danych zarówno przy rejestracji pracownika na terminalu, podczas codziennej pracy działu kadr, jak i przy przetwarzaniu danych masowych, np. przy przenoszeniu danych do płac.

Zalety systemu:

- ✔ kompleksowe i zintegrowane rozwiązanie;
- ✔ system otwarty – umożliwia wykorzystanie narzędzi programowych innych firm;
- ✔ budowa modułowa systemu – dobór tylko tych jego elementów, które odpowiadają wymaganiom Klienta;
- ✔ praca w środowisku graficznym Windows – serwerem bazy danych jest MS-SQL Server lub Oracle;
- ✔ pracujący w systemie operacyjnym Windows NT, zapewniający niezawodność oraz bezpieczeństwo danych;
- ✔ możliwość współpracy (wymiana danych) z innymi produktami firmy Microsoft (głównie Word, Excel);
- ✔ praca wielostanowiskowa w sieciach obsługiwanych przez środowisko Windows;
- ✔ zapewnienie dostępu do informacji oraz możliwości zmiany informacji tylko dla osób uprawnionych;
- ✔ system oferuje możliwość stopniowego rozszerzania jego funkcjonalności do systemów zbierania danych zakładowych, rejestracji danych maszyn czy kontroli jakości produkcji;

Zakres funkcjonalny X/TIME:

- rejestrowanie wejścia/wyjścia pracownika;
- rejestrowanie wyjść prywatnych i służbowych oraz delegacji;
- rejestrację na czytnikach lub bezpośrednio w systemie innych rodzajów nieobecności;
- rejestrację innych odchyleń od harmonogramów czasu pracy: zamian zmian, nadgodzin itp.;
- rozliczenie czasu pracy; przygotowanie eksportu danych;
- przekazywanie komunikatów pracownikom;
- planowanie zatrudnienia;
- kontrolę pracy portierów i strażników;
- kontrolę dostępu do urządzeń, pomieszczeń i zakładów;
- bezgotówkową obsługę sprzedaży wewnętrznej;
- obsługę stołówki;
- obsługę tankowania paliw.

- ✔ jedna instalacja obsługuje wiele lokalizacji i jednostek gospodarczych;
- ✔ interfejsy do wielu systemów kadrowo-płacowych.

Karty identyfikacyjne

Każdy pracownik wyposażony jest w indywidualną kartę identyfikacyjną. Oferowane czytniki współpracują z następującymi rodzajami kart:

- ✔ Karta magnetyczna – informacja o numerze karty zakodowana jest na pasku magnetyczny;
- ✔ Karta z kodem kreskowym na podczerwień – informacja o numerze karty zakodowana jest w kodzie kreskowym zabezpieczonym czarnym paskiem, tak aby kod nie był widoczny gołym okiem;
- ✔ Karta chipowa – informacja o numerze zakodowana jest w układzie scalonym wtopionym w kartę;
- ✔ Karta zbliżeniowa – pozwala na bezkontaktowy odczyt karty przez czytnik z odległości od 10 do 40 centymetrów, co pozwala np. na noszenie karty w portfelu bez konieczności jej wyjmowania.

Na wszystkich rodzajach kart można nadrukować logo firmy, adres, zdjęcie pracownika lub inne dane pracownika.

Nasi Klienci, wykorzystujący rozwiązanie X/TIME: Ferrero, Grupa Żywiec, Hochland Polska, WAGO Elwag.

LST Sp. z o.o.
ul. Grunwaldzka 45A
81-754 Sopot
tel. (+48 58) 55 00 263
http://www.LST.com.pl

Kryptograficzne elementy bezpieczeństwa i kontroli dostępu

Optymalny dobór sposobu rozwiązywania problemów i osiągania celów z zakresu ochrony informacji wymaga bardzo specjalistycznej wiedzy, znajomości rynku rozwiązań przeznaczonych dla takich zastosowań oraz dużego doświadczenia w praktycznym wykorzystywaniu dostępnych strategii, metod, narzędzi i produktów. W zależności od stopnia złożoności: od małych rozwiązań dla użytkowników indywidualnych po skomplikowane systemy, wspierane bardzo rozbudowaną infrastrukturą organizacyjną (polityki i procedury), należy zawsze zdefiniować poprawnie problem, wyspecyfikować wymagania, zanalizować potrzeby, przepisy prawa, cele organizacyjne, standardy technologiczne, zaprojektować model operacyjny, niezbędne polityki i procedury funkcjonowania, przygotować harmonogram realizacji, określić strategie i specyfikacje testów funkcjonalnych, systemowych, akceptacyjnych, przygotować plany implementacji, integracji, wdrożenia pilotowego, wdrożenia produkcyjnego, strategie i plany zarządzania oraz migracji systemu i inne. W każdym ze szczegółowych opisów działań, stanowić one będą pewien kompromis między możliwościami ekonomicznymi a zakresem ochrony.

Poza ogólnymi obszarami typowymi dla budowy systemów ochrony informacji, szczególną rolę odgrywają zagadnienia związane z ogólnie rozumianą kryptografią.

W dalszej części artykułu omówione zostaną następujące zagadnienia:

- ✔ podpis elektroniczny (zagadnienia bezpiecznego podpisu elektronicznego),
- ✔ systemy kart elektronicznych,
- ✔ technologie i standardy ochrony informacji,
- ✔ organizacyjne aspekty systemów Zaufanej Trzeciej Strony (polityki, procedury),
- ✔ sprzętowe środki ochrony informacji (sprzętowe moduły kryptograficzne),
- ✔ system tachografu cyfrowego wg wymagań EU,
- ✔ infrastruktura i aplikacje PKI w środowisku Microsoft Windows.

Przy dużych projektach jednym z ważniejszych elementów jest analiza ryzyka i wdrażania systemów zarządzania bezpieczeństwem informacji. Jest to szczególnie ważne przy powiązaniu wyżej wymienionych zagadnień z zagadnieniami bezpieczeństwa sieci, systemów antywirusowych, ciągłości zasilania, zarządzania kopiami zapasowymi danych i innych obszarów związanych z bezpieczeństwem funkcjonowania systemów informatycznych.

Objaśnienia skrótów:

PKI – Public Key Infrastructure – zbiór powiązanych ze sobą technologii bezpieczeństwa, opartych na obiegu certyfikatów klucza publicznego. Celem PKI jest zapewnienie efektywnego i bezpiecznego zarządzania kluczami publicznymi. Rezultatem prawidłowo funkcjonujących reguł PKI jest system, w którym użytkownik uzyskuje uwierzytelniony dostęp do danych i aplikacji, zaś przesyłanym treściom nadawane są atrybuty poufności i niezaprzeczalności. W skład PKI wchodzą rozmaite instytucje (urzędy) oraz rozwiązania sprzętowe i programowe, których obiektem operacji są certyfikaty oparte na szyfrowaniu asymetrycznym.

FIPS – Federal Information Processing Standard – zbiór norm stworzony przez amerykański Narodowy Instytut Standardów i Technologii (NIST), definiujący wymagania i standardy w zakresie tworzenia bezpiecznych systemów komputerowych, z założenia na użytek rządu USA, później wykorzystywany również jako standard w instytucjach komercyjnych oraz przez producentów sprzętu kryptograficznego.

CA – Certificate Authority – ośrodek wydawania certyfikatów klucza publicznego, działający na zasadzie zaufanej strony trzeciej i stanowiący jeden z podstawowych składników PKI. Urzędy certyfikacji zorganizowane są na zasadzie hierarchii, w której zaufanie do pewnego CA wynika ze zweryfikowania go przez inny CA. Na szczycie struktury mieści się tzw. źródłowy Urząd Certyfikacji (root CA), który przedstawia się własnoręcznie wydanym certyfikatem.

ACCE – Advanced Configurable Crypto Environment – opracowane przez firmę AEP środowisko sprzętowo-programistyczne do bezpiecznego przechowywania i zarządzania kluczami kryptograficznymi. Charakteryzuje się odpornością na manipulacje zgodną ze standardami zabezpieczeń FIPS 140-1 level 4 oraz ITSEC E3. W zakresie zarządzania kluczami oferuje bezpieczne składowanie ponad 1000 kluczy wraz z możliwościami ich eksportowania i przesyłania. ACCE jest podstawą wysokiej klasy modułów sprzętowych z serii AEP SureWare. Standardowe algorytmy szyfrujące (3-DES, RSA, DSA, Diffie-Hellman. MD5, SHA-1) mogą zostać wzbogacone o nowe mechanizmy, zaś każdy moduł podlega zdalnej konfiguracji.

PKCS – Public Key Cryptography Standards – jeden ze standardów PKCS. Definiuje niezależny interfejs programistyczny dla urządzeń kryptograficznych, takich jak karty elektroniczne.

CSP – Cryptographic Service Provider – producent lub dostawca bibliotek programowych zawierających funkcje związane z obsługą operacji kryptograficznych.

Infrastruktura Klucza Publicznego

Zaprojektowanie i wdrożenie właściwej dla danej organizacji Infrastruktury Klucza Publicznego może ustanowić szkielet większości usług ochrony informacji, jakie będą definiowane, projektowane i wdrażane w następnych miesiącach i latach. Technologie używane do budowy PKI są już dość rozpowszechnione, oferowane przez wielu producentów, w dużym zakresie spotykane już w podstawowej formie w ramach popularnych systemów operacyjnych i pakietów biurowych. Jednak właściwa analiza potrzeb, wymagań prawnych, standardów i technologii zapewniających kompatybilność, niezawodność i bezpieczeństwo realizacji tych odpowiedzialnych usług ciągle wymagają unikatowej wiedzy i doświadczenia.

PKI to nie tylko technologia i kryptografia. To również, a raczej przede wszystkim, bardzo precyzyjnie zaprojektowany model działania, role i odpowiedzialności uczestników tej infrastruktury, sposób pełnienia tych ról przez strony wymiany informacji, jasne i przejrzyste procedury funkcjonowania, bezpieczeństwo i ciągłość świadczenia usług, wyczerpująco określone środowisko prawne mapujące technologię, bity i bajty na znane nam z realnego świata pojęcia odpowiedzialności, woli, dowodu, poufności, identyfikacji, niepodważalności itp.

Osiągnięcie tych celów wykracza dużo dalej niż instalacja wybranego oprogramowania i uruchomienie technicznych interfejsów pozwalających wygenerować certyfikaty. To co dla demonstracji modelu PKI stanowi koniec, nawet trudno nazwać wstępem prawdziwej, mającej oparcie w prawie, zgodnej z potrzebami i wymaganiami organizacyjnymi Infrastrukturze Klucza Publicznego.

W ramach przygotowań i samego wdrożenia PKI należy zdefiniować, zaprojektować i wdrożyć tę, stanowiącą w zasadzie istotę infrastruktury, fundamentalną część odpowiedzialnego modelu PKI: polityki, procedury, kodeksy postępowania, umowy, plany działań, role uczestników itd. itp. Bez odpowiedniej dla danej organizacji (być może bardzo ograniczonej, ale niemożliwej do pominięcia!) specyfikacji i dokumentacji organizacyjnej części PKI zbudowany i wdrożony system informatyczny jest tylko tym, czym jest fizycznie: zbiorem serwerów, aplikacji, urządzeń przetwarzających ciągi bitów i bajtów, a pomiędzy nim a tak pożądanymi pojęciami jak podpis elektroniczny, identyfikacja, niezaprzeczalność, autentyczność, poufność itd. pozostanie ogromna przepaść niedookreślonych i przypadkowych domysłów, twierdzeń, zaprzeczeń, unikania odpowiedzialności itd.

Podpis elektroniczny

Od chwili ogłoszenia zamiaru opracowania ustawy o podpisie elektronicznym ogromne rzesze użytkowników i dostawców rozwiązań, którzy w jakimś zakresie wcześniej zetknęli się z tym pojęciem, odetchnęły z ulgą licząc na oczekiwane od dawna doprecyzowanie jednolitych i obowiązujących z mocy prawa wymagań i konsekwencji stosowania podpisu elektronicznego, którego olbrzymią rolę w gospodarce elektronicznej trudno przecenić. Niestety, rzeczywistość okazała się bardziej skomplikowana niż zamierzenia i plany zarówno ustawodawców w kraju, Europie i na świecie, jak i twórców technologii i standardów dotyczących podpisu elektronicznego lub z nim związanych.

Zagadnienia te nie są intuicyjne, łatwe i oczywiste, zwłaszcza gdy wątpliwości wykraczają poza modelowe, kryptograficzne pojęcie „podpisu cyfrowego". Należą do nich:

- ✔ zagadnienia prawne dotyczące podpisu zwykłego i kwalifikowanego (w tym szczególnie ustawa i rozporządzenia w Polsce oraz przepisy i zalecenia europejskie),
- ✔ technologie i standardy podpisów, dokumentów podpisanych, protokołów używanych w ramach podpisywania i weryfikacji,
- ✔ procesy i model podpisywania oraz weryfikacji podpisu (w tym również walidacja certyfikatów),
- ✔ zagadnienia organizacyjne,

3-DES – Triple Data Encryption Standard – algorytm szyfrowania oparty na DES, lecz oferujący większą przestrzeń klucza (keyspace) i odporność na ataki metodą brute-force.

DES – Data Encryption Standard – algorytm szyfrujący, powstały w latach 70. z inicjatywy rządu USA. DES oferuje 64-bitowe szyfrowanie oparte na kluczu 56-bit. Parametry te nie gwarantują obecnie bezpieczeństwa, dlatego zalecane jest stosowanie jego silniejszej odmiany (3DES) lub nowego algorytmu AES.

RSA – twórcy: Rivest, Shamir, Adleman – algorytm szyfrowania asymetrycznego, wynaleziony w 1978 r. przez trzech kryptografów. Ma wszechstronne zastosowanie jako mechanizm szyfrowania, podpisywania i wymiany kluczy symetrycznych.

DSA – Digital Signature Algorithm – algorytm szyfrujący, opublikowany w 1994 r. przez NIST (National Institute of Standards and Technology) w Stanach Zjednoczonych. Jest odmianą algorytmu El-Gamal, stosowaną szczególnie do ustanawiania podpisu cyfrowego.

Diffie-Hellman – Diffie Hellman – protokół wymiany wspólnie utworzonego klucza symetrycznego z wykorzystaniem szyfrowania asymetrycznego. Technologia ta wystawiona jest na atak typu „man-in-the-middle". Utworzona w 1976 r., później opatentowana, od roku 1997 może być używana bez naruszenia prawa patentowego.

SHA – Secure Hash Algorithm – algorytm z rodziny funkcji mieszających (hash functions). Służy do generowania 160-bitowego skrótu dokumentu elektronicznego, stosowanego do potwierdzania integralności przekazu. Wielkość skrótu SHA-1 sprawia, że jest bardziej odporny na atak metodą paradoksu urodzeniowego (Birthday Attack) niż podobny algorytm MD5, który tworzy skrót 128-bitowy.

- ✔ aplikacje i standardy programistycznych API związanych z używaniem podpisu elektronicznego,
- ✔ zakres, sposób, standardy i metody korzystania z usług Zaufanej Trzeciej Strony (w tym usług certyfikacyjnych, oznaczania czasem, walidacji, notaryzacji, itd.).

Systemy kart elektronicznych

Karty elektroniczne znalazły bardzo szerokie zastosowania w ramach systemów bezpieczeństwa informacji zarówno w roli osobistego tokenu zwiększającego bezpieczeństwo procesów identyfikacji i silnego uwierzytelniania, jak i jako nośnik kluczy w ramach infrastruktury PKI i ściśle z nią związanej instytucji podpisu elektronicznego. W skład systemu kart elektronicznych wchodzą m.in. karty pamięciowe, procesorowe, kryptograficzne, zarówno stykowe jak i zbliżeniowe oraz wszelkie technologie i rozwiązania dotyczące kart – czytniki i terminale, protokoły, aplikacje, narzędzia, interfejsy programistyczne API itp.

Technologie i standardy

Współczesne systemy informatyczne wysoko cenią sobie otwartość i standardowość użytych rozwiązań, dających ich właścicielom znaczny poziom niezależności w doborze składników swoich systemów, ułatwiających migrację oraz zapewniających pewien poziom przejrzystości co do bezpieczeństwa stosowanych metod, środków i protokołów komunikacyjnych. W przypadku systemów ochrony informacji występuje szczególnie dużo standardów, zaleceń, formatów, protokołów, dobrych praktyk itd. dotyczących stosowanych w ramach tych systemów technologii lub opisujących zasady ich używania, model organizacyjny, role i odpowiedzialność poszczególnych modułów i podsystemów. Można tu wymienić m.in. skróty typu: SSL, PKI, RSA, CRL, CRT, CDP, TSP, DES, AES, RC4, SGS, SCS, SCA, SIM, USIM, WIM, S/WIM X.509, LDAP, OCSP, SSCD, CN, SN.

Systemy tachografu cyfrowego

Na podstawie rozporządzenia Rady Europy 2135/98 powołana została do życia koncepcja systemu tachografu cyfrowego (STC, ang. *Digital Tachograph System*) jako nowoczesnej drogi do rozwiązania problemu rejestracji czasu pracy kierowców samochodów ciężarowych i kontroli parametrów tej pracy. W Polsce regulacje tego rozporządzenia wprowadziła ustawa z dnia 29 lipca 2005 r. „O systemie tachografów cyfrowych". Jednym ze współautorów koncepcji i realizacji tego systemu w Polsce jest firma Crypto Tech z Krakowa. Ponieważ techniczna realizacja koncepcji bezpieczeństwa obiegu informacji w tym systemie bazuje na użyciu kryptograficznych kart procesorowych, specjalizowanego modelu PKI, certyfikatów cyfrowych, podpisu cyfrowego, naturalnym stało się zaangażowanie firmy w prace standaryzacyjne, legislacyjne i wdrożeniowe.

W zakresie zastosowania kryptografii w systemach bezpieczeństwa i kontroli dostępu możemy wyróżnić kilka grup rozwiązań:

- rozwiązania dla korporacji,
- podpis elektroniczny,
- systemy PKI,
- ochrona e-commerce,
- kontrola dostępu i uprawnień,
- bezpieczeństwo sieci.

Rozwiązania dla korporacji

Uwierzytelnienie użytkownika

Jedną z funkcji współczesnej karty kryptograficznej jest uwierzytelnienie, czyli bezpieczna weryfikacja tożsamości użytkownika. Karty takie często wspierają zarówno proste systemy zbliżeniowe, jak i rozwiązania wymagające zaawansowanego uwierzytelnienia z użyciem kodu PIN. Najczęściej działają z wieloma rozpowszechnionymi na rynku czytnikami kart takich producentów, jak Gemplus, SCM Microsystems i Omnikey.

Kontrola dostępu i logowania

Karta korporacyjna umożliwia przydzielenie użytkownikowi dostępu do obiektów fizycznych (budynek lub pomieszczenie) oraz zasobów informatycznych, takich jak aplikacja, system operacyjny czy sieć korporacyjna. Rozwiązanie takie często zawiera możliwość integracji z istniejącą infrastrukturą sprzętowo-programową, czego rezultatem jest wygodne i bezpieczne „jednokrotne uwierzytelnienie" (SSO – *Single Sign-On*).

Bezpieczny nośnik klucza

Karty zapewniają kluczom kryptograficznym trwałość, bezpieczeństwo i odporność na próby nieautoryzowanego dostępu. Wyspecjalizowany system operacyjny wraz ze sprzętowymi zabezpieczeniami tworzą jedno z najbezpieczniejszych środowisk dla przechowywania kluczy prywatnych i wykonywania na nich operacji kryptograficznych. Klucz nie jest udostępniany na zewnątrz urządzenia, tak jak w przypadku tradycyjnych, mniej bezpiecznych nośników, np. dysku twardego, tokenu USB, dyskietki.

Kwalifikowany podpis elektroniczny

Karta powinna posiadać certyfikat bezpieczeństwa ITSEC na poziomie E3 high, co umożliwia jej zastosowanie do składania podpisu elektronicznego opartego na kwalifikowanych certyfikatach klucza publicznego (kwalifikowany podpis elektroniczny). Stosowane rozwiązania powinny być zgodne z ustawą „O podpisie

elektronicznym" i realizować zalecenia legislacyjne Unii Europejskiej.

Szyfrowanie danych

Stosowanie kart wieloaplikacyjnych umożliwia wykonywanie wielu operacji związanych z szyfrowaniem. Oprócz bezpiecznego przenoszenia i składowania kluczy prywatnych, karta taka wyposażona jest w zaawanasowane oprogramowanie umożliwiające uruchamianie kryptograficznych operacji wewnątrz zabezpieczonego układu scalonego. W ramach obsługiwanych działań znajduje się szyfrowanie i deszyfrowanie DES, 3-DES i RSA, generowanie kluczy RSA oraz generowanie i weryfikacja podpisu RSA.

Integracja z PKI

Stosowanie sprawdzonych rozwiązań i standardów umożliwia m.in. funkcjonowanie w ramach Infrastruktury Klucza Publicznego (PKI). Oprogramowanie kart często jest oparte na sprawdzonym systemie operacyjnym, np. SetCOS i aplikacjach kryptograficznych, opartych na standardach PKCS#11, PKCS#15, PC/S.C.

Podpis elektroniczny

Obecne techniki funkcjonowania współczesnych przedsiębiorstw coraz częściej wymuszają na nich przejście z tradycyjnego obiegu dokumentów na ich odpowiednik elektroniczny. Aby był on w pełni funkcjonalny, konieczne są narzędzia, takie jak podpis elektroniczny. Zapewnia on następujące funkcje:

- ✔ autentyczność – zapewnia, iż nadawca jest tym, za kogo się podaje,
- ✔ integralność – zapewnia, że wiadomość nie została zmodyfikowana w drodze do odbiorcy,
- ✔ niezaprzeczalność – zapewnia, że wiadomość została podpisana przez konkretną osobę.

Bezpieczna poczta

Zagrożenia

Przesyłanie e-maili poprzez publiczne, pozbawione zabezpieczeń sieci stało się ryzykowną operacją. Wśród wielu zagrożeń, na jakie jest narażona elektroniczna przesyłka, znajdują się poważne naruszenia prywatności odbiorcy i nadawcy, a nawet niebezpieczeństwo ingerencji w ich systemy komputerowe. Niezabezpieczony e-mail może zostać odczytany, zmieniony lub skasowany bez upoważnienia i wiedzy zainteresowanych stron.

Możliwości obrony

Stosowane szeroko zabezpieczenie transmisji poprzez kodowanie SSL nie daje pełnej gwarancji bezpieczeństwa. Istnieje zatem potrzeba silnej ochrony przesyłki na każdym etapie jej obiegu. Światowym standardem bezpieczeństwa poczty elektronicznej stało się rozwiązanie polegające na szyfrowaniu wiadomości kluczem kryptograficznym i opatrywaniu jej podpisem cyfrowym.

Obecnie oferowane systemy ochrony poczty elektronicznej, oparte na silnym szyfrowaniu wiadomości i załączników, podpisywaniu cyfrowym za pomocą kluczy do 2048 bitów, obsługą schematu bezpośredniego zaufania i systemu Zaufanej Strony Trzeciej (TTP) współpracują także z kartami elektronicznymi.

Zaufanie i bezpieczeństwo

Pojęcie bezpieczeństwa przeszło w ostatnich latach poważną ewolucję, w wyniku której wykształciła się grupa czterech cech określających warunki konieczne do uznania usługi za bezpieczną.

Bezpieczna poczta zapewnia spełnienie wszystkich wymagań bezpieczeństwa, określonych następującymi właściwościami:

- ✔ uwierzytelnienie,
- ✔ integralność,
- ✔ poufność,
- ✔ niezaprzeczalność.

Systemy VPN

Obecnie coraz częściej systemy tworzenia sieci VPN stanowią uzupełnienie instalacji typu „ściana ognia" i budowane są w oparciu o infrastrukturę klucza publicznego (PKI). Podstawą ochrony Wirtualnej Sieci Prywatnej jest uwierzytelnianie użytkowników poprzez bezpieczną weryfikację certyfikatów.

Zbudowanie bezpiecznej sieci w oparciu o takie rozwiązanie przynosi następujące korzyści:

- ✔ bezpieczeństwo w sieci,
- ✔ uniwersalne uwierzytelnienie,
- ✔ skalowalność.

Bezpieczna witryna

Bezpieczeństwo w przeglądarce www

Istniejący obecnie model zabezpieczenia komunikacji pomiędzy przeglądarką a serwerem www uwzględnia standardowe modele bezpieczeństwa, oparte na szyfrowaniu SSL. Szybki rozwój opartych na www systemów elektronicznego handlu i bankowości wymaga coraz częściej rozwiązań dostosowanych do rosnących potrzeb klientów. Silne szyfrowanie jest konieczne przy takich procesach, jak logowanie na witrynę www i wysyłanie formularza z poufnymi danymi.

Integracja z PKI

Stosowane obecnie systemy zabezpieczania witryny www umożliwiają bezpieczeństwo oparte z jednej strony na certyfikacie klienta, a z drugiej – na zaufanym źródle potwierdzającym wiarygodność transakcji. W ten sposób realizowane zostają zasady budowy infra-

struktury klucza publicznego, zapewniające poufność, obustronne uwierzytelnienie oraz integralność danych.

Systemy PKI

Zaufanie i bezpieczeństwo

Celem PKI jest zapewnienie najwyższego poziomu bezpieczeństwa w systemach opartych na kryptografii klucza publicznego. Pojęcie bezpieczeństwa przeszło w ostatnich latach ewolucję, w wyniku której wykształciła się grupa czterech własności określających warunki konieczne do uznania usługi za bezpieczną:

- uwierzytelnienie,
- integralność,
- poufność,
- niezaprzeczalność.

PKI gwarantuje spełnienie wymogów bezpieczeństwa wyznaczonych powyższymi cechami.

Elementy środowiska PKI

PKI obsługuje wszelkie zdarzenia związane z obiegiem certyfikatów klucza publicznego poprzez zorganizowaną strukturę obiektów, operacji i zasad postępowania. Podstawowe obiekty PKI to urzędy rejestracji (RA) i certyfikacji (CA), a także rozmaite składnice kluczy i certyfikatów oraz listy unieważnionych certyfikatów (CRL). Obiektom tym towarzyszą operacje, takie jak rejestracja użytkownika, wydawanie certyfikatów, generowanie par kluczy kryptograficznych, przedłużanie ważności certyfikatu, unieważnianie certyfikatów, odzyskiwanie certyfikatu z bezpiecznego repozytorium i wiele innych. Nad całością czuwa zbiór zasad regulujących reguły postępowania w środowisku PKI i określanych jako polityki bezpieczeństwa.

Karta elektroniczna a PKI

Środowisko PKI wymaga obecności bezpiecznego nośnika poufnej informacji, która służy do identyfikacji posiadacza i uwierzytelniania jego działań. Karta elektroniczna jest obecnie najbardziej rozpowszechnionym urządzeniem tej kategorii. Budowane systemy infrastruktury klucza publicznego współpracują z zaawansowanymi kartami typu multiSIGN, które służą jako bezpieczne narzędzie pracy z danymi i uprawnieniami chronionymi certyfikatami klucza publicznego.

Ochrona e-commerce

Profesjonalne systemy ochrony e-commerce oferują największy stopień zabezpieczenia dla aplikacji korzystających z formularzy HTTP, obsługujących płatności elektroniczne i transfery bankowe. Zgodność ze standardami umożliwia dostosowanie rozwiązania do każdego zbioru urządzeń uwierzytelniających użytkownika, takich jak systemy kart elektronicznych lub tokenów USB. Dodatkowym atutem jest wsparcie dla infrastruktury klucza publicznego (PKI), ułatwiające stosowanie certyfikatu użytkownika w procesie zawierania bezpiecznych transakcji.

Istota ochrony handlu elektronicznego

Proces zawierania transakcji handlowych i bankowych poprzez sieć jest jedną z najbardziej wrażliwych i podatnych na zagrożenia operacji przeprowadzanych w internecie. Z tego powodu istotne jest bezpieczeństwo typu *end-to-end*, które chroni transakcję na każdym etapie jej przeprowadzania.

Rola standardów

Zróżnicowanie współczesnego rynku IT powoduje konieczność oferowania otwartych propozycji, które nie wykluczają integracji z dowolnym z wielu szeroko rozpowszechnionych systemów e-commerce.

Kontrola dostępu i uprawnień

Do kontroli dostępu i uprawnień stosowane są obecnie wysoko specjalizowane terminale i czytniki kontroli dostępu do obiektów bazujące na technologiach kart elektronicznych i metodach biometrycznych. Są to m.in. systemy ochrony informacji i kontroli dostępu do zasobów informatycznych (wspólna karta), np. w ramach infrastruktury klucza publicznego, karty bezstykowe lub stykowe oraz skanery linii papilarnych.

Metody biometrycznej identyfikacji i weryfikacji tożsamości ludzi przenoszą do cyfrowego świata proces rozpoznawania osoby na podstawie jej fizycznych lub behawioralnych cech unikatowych tylko dla danej osoby. Takie automatyczne metody biometryczne przewyższają obecnie szeroko stosowane metody zastępczej identyfikacji polegające na prezentowaniu PIN-u, hasła lub posiadaniu specjalnego urządzenia identyfikacyjnego, jednak umiejętnie zintegrowane z innymi technologiami mogą połączyć zalety obu rozwiązań.

Bezpieczeństwo sieci

Powszechnie stosowane rozwiązania sprzętowe i programowe obejmują:

- ✔ IDS/IPS – systemy detekcji/prewencji intruzów,
- ✔ Firewall – rozbudowane systemy ścian ogniowych filtrujące ruch wejściowy/wyjściowy,
- ✔ Proxy – usługa pośrednicząca pomiędzy klientem a usługą, z którą klient chce nawiązać połączenie. Może posiadać funkcje buforujące oraz filtrujące,
- ✔ VPN – bramki umożliwiające bezpieczne podłączenie się do wewnętrznych zasobów firmy z dowolnego miejsca na świecie,
- ✔ SSL Gateway – usługa terminująca połączenia (sesje) SSL przed wejściem do sieci firmowej. Dzięki nim można zredukować obciążenie serwerów usługowych.

Przykłady rozwiązań

Karty i tokeny

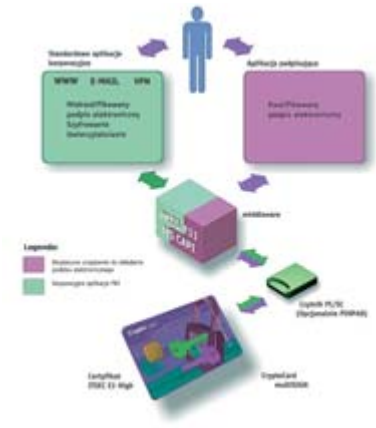
Na rynku dostępne są karty i tokeny elektroniczne o różnych parametrach użytkowych i różnym stopniu zabezpieczenia. Wiele aplikacji i systemów specjalizowanych, jak i ogólnie dostępnych na rynku może być wspieranych przez takie urządzenia, znakomicie podnosząc ich poziom bezpieczeństwa.

Karty elektroniczne

Karty elektroniczne zawierają specjalizowany mikroprocesor z własną pamięcią o rozbudowanej kontroli dostępu. Stosowane są w wielu dziedzinach bezpieczeństwa, od składania podpisu elektronicznego poprzez logowanie oparte na bezpiecznym protokole SSL, do szyfrowania danych. Poniżej kilka przykładów kart oferowanych przez firmę Crypto Tech.

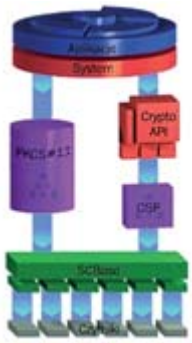
CryptoCard multiSIGN – zaawansowana karta zgodna z ustawą o podpisie elektronicznym.

CryptoCard multiSIGN jest specjalizowaną kryptograficzną kartą mikroprocesorową przeznaczoną do realizacji kwalifikowanego i niekwalifikowanego podpisu elektronicznego oraz funkcji identyfikacji i silnego uwierzytelniania użytkowników. Karta ta, uzupełniona o oprogramowanie podpisujące i uwierzytelniające, stanowi doskonałe narzędzie wspierające szeroką gamę rozwiązań pracujących w ramach Infrastruktury Klucza Publicznego (PKI). Wsparcie dla dominujących na rynku standardów pozwala na użycie karty w typowych zastosowaniach wewnątrz organizacji (takich jak dostęp do komputerów, sieci i innych zasobów) oraz pełną realizację idei oraz w pełni realizować ideę podpisu cyfrowego. CryptoCard multiSIGN może zawierać aplikację niekwalifikowanego podpisu elektronicznego lub certyfikowaną aplikację podpisu kwalifikowanego. W tym drugim przypadku karta stanowi komponent techniczny zgodny z wymaganiami polskiego prawa stawianymi dla bezpiecznych urządzeń do składania kwalifikowanego podpisu elektronicznego. Oferujemy również unikatową wersję karty realizującą jednocześnie obie wersje podpisu elektronicznego, łącząc zalety obu zastosowań.



CryptoCard PKI – uniwersalna karta elektroniczna dla systemów bezpieczeństwa.

CryptoCard PKI jest kryptograficzną kartą mikroprocesorową o wszechstronnym zastosowaniu. Wraz z oprogramowaniem stanowi doskonałe narzędzie wspierające szeroką gamę rozwiązań pracujących w ramach Infrastruktury Klucza Publicznego (PKI). Wsparcie dla dominujących na rynku standardów pozwala na użycie karty w typowych zastosowaniach wewnątrz organizacji, jak dostęp do komputerów, sieci i innych zasobów informatycznych, oraz w pełni realizować założenia podpisu cyfrowego. Odpowiednio duża ilość pamięci pozwala przechowywać wiele informacji, umożliwiając realizację różnych funkcji, np. zestawianie bezpiecznego połączenia z serwerem www, podpisywanie i szyfrowanie poczty elektronicznej, logowanie do domeny Windows 2000/XP i wiele innych.



Mechanizmy zarządzania kluczami i szyfrowania są zlokalizowane na karcie. Karta zarówno generuje klucze, przechowuje je w pamięci, jak również przy ich użyciu szyfruje informacje na zlecenie zewnętrznych aplikacji po weryfikacji kodu PIN użytkownika. Wysoki poziom bezpieczeństwa karty potwierdzony jest odpowiednimi certyfikatami. System operacyjny karty bazuje na systemie certyfikowanym do poziomu ITSEC E3 HIGH lub FIPS 140-1 Level 2, a obecnie jest w trakcie certyfikacji wg standardu Common Criteria EAL4+.

Oprogramowanie CryptoCard PKI realizuje standardy PKCS#11 i PKCS#15 oraz zawiera certyfikowany przez firmę Microsoft moduł CSP do pracy w ramach CryptoAPI. Ponieważ interfejsy te wykorzystują standard PC/SC, możliwe jest używanie szerokiej gamy czytników w środowisku Windows. Karta spełnia również wymagania European Digital Signature Law i polskiej ustawy o podpisie elektronicznym.

Pakiet CryptoCard PKI łatwo integruje się z popularnymi aplikacjami bezpiecznej poczty, uwierzytelniania w przeglądarkach i generowania podpisów cyfrowych.

CryptoCard PKI współpracuje z oprogramowaniem liderów rynku PKI: Entrust, RSA Security, CheckPoint, Netscape, Microsoft, SecGo i innych.

Tokeny USB

Jako alternatywę dla zestawu karta elektroniczna + czytnik kart bardzo często stosuje się tokeny USB podłączane wprost do wolnego portu USB w komputerze, hubie, monitorze, itp. Jest to rozwiązanie szczególnie wygodne dla posiadaczy notebooków. Przykładem takiego urządzenia jest iKey 1000, przeznaczony do silnego uwierzytelniania w oparciu o model challenge-response („zapytanie-odpowiedź") oraz do przechowywania haseł i kluczy chronionych osobistymi kodami użytkownika (PIN), bez sprzętowej kryptografii asymetrycznej RSA. IKey 2032 jest z kolei funkcjonalnym odpowiednikiem kart kryptograficznych i przechowuje klucze kryptograficzne oraz wykonuje na nich operacje wewnątrz tokenu.

iKey 1000 oferuje bezpieczeństwo uwierzytelniania użytkownika w systemach sieciowych, obsługuje standard *plug and play* pod Windows 2000. Dodatkowo iKey 1000 może pracować w systemie Windows 2000 jako urządzenie uwierzytelniające podczas dostępu do systemu – „smart token login" oraz podczas szyfrowania plików. Łatwo integruje się z programami Outlook, Outlook Express i Internet Explorer. Posiada wbudowany algorytm liczenia skrótu MD5 oraz generator liczb pseudolosowych. Zbudowany jest na bazie struktury plików dla kart elektronicznych zgodnie z normą ISO 7816-4, posiada trzy tryby dostępu do systemu plików: dostęp nieograniczony, dostęp tylko dla użytkownika, dostęp tylko dla administratora. Umożliwia to elastyczną konfigurację pamięci, dając możliwość pełnego zabezpieczenia danych przed niepowołanym odczytem lub modyfikacją. Duża liczba wewnętrznej pamięci EEPROM – 8 KB (z możliwością rozszerzenia do 32 KB) potrafi sprostać większości wymagań konfiguracyjnych użytkowników. Dostępny jest też bogaty zestaw narzędzi typu SDK, umożliwiający integrację z dowolnym oprogramowaniem.

Produkowany przez SafeNet Inc. iKey 2032 jest pierwszym w swojej klasie przenośnym urządzeniem uwierzytelniającym zdolnym do przechowywania kluczy prywatnych, cyfrowych certyfikatów i wykonywania operacji podpisu elektronicznego – jest prawdziwym tokenem PKI. iKey 2032 zapewnia wszystkie aspekty bezpieczeństwa wymagane przez systemy PKI, w tym wykonywanie operacji deszyfrowania i podpisywania wewnątrz tokenu. Dostarcza niezbędnych funkcji kryptograficznych dla przeglądarek Netscape i Internet Explorer oraz dla klientów poczty elektronicznej, tj. Outlook, Outlook Express i Netscape Communicator, a także innych aplikacji PKI takich producentów, jak: Betrusted, Entrust, Xcert, Verisign, CheckPoint, KyberPASS i innych. Do iKey 2032 oferujemy też bogaty zestaw narzędzi SDK, umożliwiający integrację z dowolnym oprogramowaniem. Duża liczba wewnętrznej pamięci EEPROM – od 8 KB do 32 KB – potrafi sprostać większości wymagań konfiguracyjnych użytkowników.

Karty elektroniczne mogą być również dostarczone w formie klucza/tokena USB. Taka wygodna dla wybranych zastosowań postać jest również dość atrakcyjna cenowo, a funkcjonalnie zbudowana jest na bazie „anonimowego" małego czytnika kart elektronicznych w formie klucza USB i karty w formacie ID-000 (SIM). Łącznie stanowią one rozwiązania tokenów/kluczy USB spotykane na rynku firm Rainbow/SafeNet, Alladin, ARX itp.

Tokeny haseł jednorazowych

RSA SecurID – dwuskładnikowe, bezpieczne uwierzytelnienie.

Rozwiązanie firmy RSA realizujące funkcje uwierzytelniania użytkowników w szeroko pojętym dostępie do sieci korporacyjnej jest zbudowane w oparciu o strategię dwuczęściowej weryfikacji tożsamości danego użytkownika. Typowym „analogowym" przykładem takiego rozwiązania jest sposób korzystania z karty bankomatowej, gdzie do poprawnego zautoryzowania się w systemie konieczne są dwa komponenty – ważna karta („coś-co-masz") i numer identyfikacyjny PIN („coś-co-wiesz"). W przypadku rozwiązania elektronicznego konieczny jest PIN oraz dodatkowy numer, generowany automatycznie co minutę przez niewielkie urządzenie zwane tokenem.

RSA SecurID SD600

Aby się zalogować w systemie, należy podać niezmienny PIN oraz zgodny z nim numer, wyświetlony na ekraniku tokena – w systemie obliczana jest kombinacja obydwu numerów i na podstawie rezultatu podejmowana jest decyzja dotycząca zaufania dla użytkownika. System jest zaimplementowany dla długiej listy systemów operacyjnych (m. in. systemów Microsoft, systemu Linux i innych systemów Unix), może współpracować z wieloma pośredniczącymi sposobami uwierzytelniania (Novell NMAS, Microsoft Windows, Linux PAM i in.). Dla poszczególnych rodzajów zasobów (grupy lub pojedynczne aplikacje/strony web, zasoby sieciowe VPN, zasoby dyskowe i in.) dostępne są moduły RSA Authentication Agents, współpracujące z central-

BlackBerry z programowym tokenem RSA SecurID

RSA SecurID SID700 **RSA SecurID SD200**

nym komponentem systemu o nazwie RSA Authentication Manager.

Czytniki kart elektronicznych

Na rynku znajduje się bogata oferta czytników kart elektronicznych do stosowania w systemach ochrony informacji oraz systemach kontroli dostępu do zasobów i obiektów. Modele dla różnych środowisk i interfejsów (szeregowych, równoległych, USB, PS/2, itd.). Zgodne ze standardami: ISO7816, EMV, PC/SC, PKCS#11, itp. Dostępne są także modele zintegrowane ze skanerem linii papilarnych.

SCR531 – dualny czytnik dla USB i portu szeregowego.

Czytnik SCR531 obsługuje komunikację poprzez port szeregowy i USB. Funkcjonalność tego modelu odpowiada możliwościom dwóch innych czytników SCM Microsystems – SCR131 i SCR331. Urządzenie jest wyposażone w wymienny kabel odpowiadający obsługiwanym standardom połączenia z komputerem.

SCR243 – czytnik PCMCIA dla notebooków.

Czytnik SCR243 zaprojektowany specjalnie dla użytkowników mobilnych. Model SCR243 jest zgodny ze standardowym slotem PCMCIA Type II w notebookach. Oprogramowanie firmowe czytnika może być sprawnie aktualizowane dzięki wbudowanej pamięci flash. SCR243 jest zgodny ze standardami EMV I oraz PC/SC i współpracuje ze wszystkimi ważniejszymi modelami kart elektronicznych.

SPR532 – bezpieczne wprowadzanie PIN.

Czytniki z serii SPRx32 umożliwiają ochronę kodu PIN podczas przesyłania go do karty elektronicznej. SPR532 to najbardziej uniwersalny model, wspierający komunikację z komputerem poprzez dwa podstawowe interfejsy – USB i port szeregowy. Czytnik znajduje zastosowanie w rozwiązaniach wymagających poufnego dostępu, takich jak logowanie do zaufanej sieci czy bankowość internetowa.

CardMan 6121 Dongle – najmniejszy na świecie czytnik USB.

CardMan Dongle jest przenośnym miniczytnikiem wyposażonym we wtyczkę USB i gniazdo SIM dla karty procesorowej. Niewielki rozmiar i zwarta konstrukcja sprawiają, że urządzenie to znajduje szerokie zastosowanie na stale rosnącym rynku kart elektronicznych. Zgodność ze specyfikacją GSM 11.11 umożliwia ściąganie danych z sieci wprost na kartę. Produkt należy do szerokiej rodziny czytników CardMan Desktop i jest zgodny ze standardowymi interfejsami.

Czytnik jest dostarczany ze sterownikami dla systemów Windows 98/Me/NT/2000/XP/CE, Linux, Mac OS X.

CardMan Trust 3821 – czytnik dla e-commerce.

CardMan Trust 3821 jest wyspecjalizowanym czytnikiem kart elektronicznych, dedykowanym dla handlu elektronicznego i zdalnej bankowości. Jest wyposażony w wyświetlacz (2 linie x 16 znaków) oraz klawiaturę do wprowadzania kodów PIN. Produkt jest przedstawicielem rodziny czytników CardMan Trust, charakteryzujących się dodatkowym zabezpieczeniem procesów wprowadzania i modyfikacji kodu PIN oraz zgodnością ze standardem EMV, tworzącym podwaliny bezpiecznego środowiska e-commerce.

Kontrola dostępu do zasobów IT

Oferowane na rynku rozwiązania integrują zazwyczaj technologie uwierzytelniania z szerokim wachlarzem aplikacji i usług. Produkty te realizują kontrolę dostępu w stopniu znacznie wykraczającym poza standardową funkcjonalność danej aplikacji. Wysoki stopień zabezpieczenia uzyskiwany jest dzięki stosowaniu zaawansowanych kart elektronicznych, pełnym uwierzytelnieniu stron wymiany danych, często dodatkowej integracji z metodami biometrycznymi. Dostępne rozwiązania mogą uzupełniać systemy kontroli dostępu do pomieszczeń poprzez stosowanie dualnych kart elektronicznych, których część bezstykowa odpowiedzialna jest za dostęp do pomieszczeń, a układ z procesorem kryptograficznym zintegrowany jest z np. Infrastrukturą Klucza Publicznego (PKI).

CryptoCard Logon – zestaw do logowania z wykorzystaniem karty CryptoCard.

CryptoCard Logon jest nowoczesnym rozwiązaniem firmy Crypto Tech, pozwalającym wykorzystywać karty procesorowe z rodziny CryptoCard do logowania w systemie Windows. Rozwiązanie to uzupełnia standardowe elementy systemu Windows, dodając możliwość wykorzystania karty do zabezpieczenia komputera nie będącego elementem domeny. Informacje służące do logowania (nazwa użytkownika, statyczne hasło) są zapisane w pamięci karty procesorowej i zabezpieczone kodem PIN. Dzięki temu posiadacz karty nie musi pamiętać hasła. Hasło tym lepiej chroni komputer, im jest dłuższe i trudniejsze do zgadnięcia. Hasło zapisane na karcie może być odpowiednio długie i skomplikowane, ponieważ nie trzeba go pamiętać.

CryptoCard Logon jest elementem rozwiązania pozwalającego na bazie karty elektronicznej zbudować system dostępu do zasobów. Ta sama karta może równocześnie pełnić wiele funkcji. Może być fizycznym identyfikatorem ze zdjęciem i elementami uniemożliwiającymi sfałszowanie karty. Może, w przypadku tzw. kart hybrydowych, dzięki wbudowanemu układowi zbliżeniowemu służyć do kontroli dostępu fizycznego do pomieszczeń. Może przechowywać klucze i certyfikaty służące do uzyskiwania dostępu do systemów teleinformatycznych. Pozwala także na składanie podpisu elektronicznego i szyfrowanie danych.

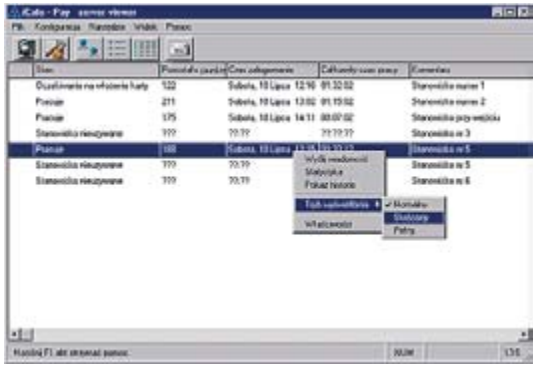
Dodatkowym zabezpieczeniem jest możliwość blokowania komputera oraz wygaszenie ekranu poprzez wyciągnięcie karty z czytnika. Powoduje to pojawienie się ekranu z informacją o zablokowaniu stacji, a jedynymi dostępnymi metodami jej odblokowania są ponowne włożenie karty i podanie kodu PIN (możliwość ręcznego wpisania nazwy użytkownika i hasła jest ustalana przez administratora).

RSA ClearTrust – zarządzanie dostępem do serwisów www.

W miarę wzrostu znaczenia wizerunku firmy w internecie, rośnie zapotrzebowanie na narzędzia zarządzania użytkownikami i uprawnieniami w dostępie do witryn internetowych. Ten zakres oprogramowania określany jest nazwą Infrastruktury Zarządzania Uprawnieniami (*Priviledge Management Infrastructure*/PMI). Produkt ClearTrust firmy RSA Security został stworzony, aby realizować tę właśnie funkcjonalność. Jego wykorzystanie możliwe jest w sieciach intranetowych, extranetowych, portalach informacyjnych, systemach wymiany informacji. We wszystkich zastosowaniach używany jest mechanizm jednorazowego logowania (*Single Sign-On*). Graficzny interfejs do zarządzania uprawnieniami opartymi na przydziale ról zdefiniowanych w strukturze LDAP, pełna integracja z architekturą klucza publicznego oraz implementacja SAML są najważniejszymi zaletami ClearTrust jako produktu o uznanej marce i wysokim poziomie jakości.

iCafe-Pay – przykładowy system płatności za korzystanie ze stanowisk kawiarni internetowej.

System iCafe-Pay został zaprojektowany jako sposób zautomatyzowania problemu rozliczania czasu spędzonego przy komputerach popularnych kawiarni internetowych. Produkt realizuje kontrolę dostępu do stanowisk



oraz umożliwia korzystanie z nich wyłącznie na podstawie odpowiedniej karty elektronicznej zawierającej wcześniej wykupione punkty. Karta taka pełni rolę karnetu, za pomocą którego można odblokować stację użytkownika wyłącznie na czas, za który została pobrana opłata z karty elektronicznej. Karta może również służyć do płacenia za wszelkie usługi oferowane w kawiarni, a także zawierać inne aplikacje, np. Digital ID, czyli certyfikat klucza publicznego.

System składa się z oprogramowania klienta iCafe-Pay Client, serwera operacji kryptograficznych iCafe-Pay Server wraz z programem wizualizacji aktywności wszystkich stacji klientów oraz aplikacji iCafe-Pay Supervisor, służącej do personalizacji i wydawania kart, sprzedaży punktów na kartach, konfiguracji systemu. W skład systemu wchodzą czytniki kart elektronicznych i elektroniczne karty procesorowe.

Ochrona danych

Bezpieczeństwo pojedynczej stacji roboczej, równie ważne jak bezpieczeństwo sieci, wymaga dedykowanych rozwiązań sprzętowo-programowych chroniących wszelkie możliwe aspekty pracy użytkownika. Poniżej

przedstawiam kilka rozwiązań firmy **Utimaco Safeware AG i WinMagic Inc**.

SafeGuard Advanced Security – wszechstronna kontrola dostępu.

SafeGuard Advanced Security zapewnia użytkownikom różnorodnych środowisk sieciowych bezpieczeństwo procesu logowania i ochronę danych poprzez wszechstronną kontrolę dostępu. Z jednej strony zapewnia zaawansowaną definicję przywilejów i łatwość zarządzania, z drugiej strony – pozwala na praktyczne zastosowanie wysokich wymagań istniejących polityk bezpieczeństwa w firmie. Oprogramowanie to wykorzystywane jest w ochronie intranetu przed świadomymi i nieświadomymi atakami ze strony wewnętrznego personelu. SafeGuard Advanced Security oferuje również możliwości bezpiecznego uwierzytelnienia poprzez zastosowanie procedury trzech sposobów wezwanie/odpowiedź. Tylko użytkownik posiadający kartę elektroniczną i znający jej kod PIN może zalogować się do systemu. SGAS weryfikuje klucz prywatny użytkownika bezpośrednio na karcie elektronicznej, co uniemożliwia przechwycenie hasła podczas procesu logowania.

SafeGuard Easy – zabezpieczenie danych na dysku twardym.

SafeGuard Easy jest programem, który zapewnia użytkownikowi ochronę ważnych danych na komputerach przenośnych i pojedynczych stacjach roboczych. Ochrona systemu podczas ładowania, konieczność uwierzytelnienia przed bootowaniem systemu (PBA) i kodowanie dysku przy użyciu mocnych algorytmów powoduje, że osoba nieuprawniona nie ma dostępu do stacji roboczej. Dane chronione w ten sposób są bezpieczne przy próbie ich rozkodowania z wykorzystaniem zaawansowanych narzędzi, nawet wtedy gdy dysk twardy zostanie wyjęty z komputera lub skopiowany. Do najważniejszych zalet SG Easy należą łatwość instalacji i konfiguracji oraz działanie w sposób przezroczysty dla użytkownika.

SafeGuard LAN Crypt – bezpieczna administracja sieci.

SafeGuard LAN Crypt dostarcza maksimum bezpieczeństwa poprzez ochronę poufnych danych. Kodowanie danych odbywa się przez wykorzystanie powszechnie akceptowalnych mocnych algorytmów, takich jak np. 128 bit IDEA. Zgodnie z EDC (*Enterprise Distribution Concept)*, system realizuje oddzielenie administracji sieci od zarządzania bezpieczeństwem. Tylko administrator ma możliwość przypisywania kluczy do plików i katalogów. Nawet administrator sieci bez specjalnych uprawnień nie może przeczytać plików z danymi zakodowanymi poprzez SafeGuard LAN Crypt. Dane i ich bezpieczeństwo kontrolowane są poprzez centralne przypisanie kluczy.

SafeGuard PrivateCrypto – bezpieczna wymiana danych.

SafeGuard PrivateCrypto jest programem, który umożliwia zabezpieczenie poufnych danych i plików za pomocą algorytmu AES o długości klucza 128 bitów oraz hasła bez względu na to, czy nasze poufne dane znajdują się na lokalnym komputerze, czy też są przesyłane przez internet. Integracja z systemem Windows oraz z oprogramowaniem do czytania poczty elektronicznej sprawia, że dane są przesyłane w sposób bezpieczny i prosty. Dostępna także wersja SafeGuard PrivateCrypto dla Pocket PC daje możliwość ochrony danych na urządzeniach przenośnych.

SafeGuard PrivateDisk – elektroniczny sejf dla plików.

SafeGuard PrivateDisk jest rozwiązaniem zabezpieczającym poufne pliki przed nieautoryzowanym dostępem. Bez różnicy jest, czy ważne pliki są przechowywane na pojedynczej stacji, czy też w sieci – dostęp do nich jest w skuteczny sposób chroniony przed nieupoważnionymi osobami. Technologia *Secure Virtual Disk* oferowana przez Utimaco Safeware jest idealnym rozwiązaniem tego problemu: oprogramowanie automatycznie zabezpiecza ważne i cenne pliki zachowując je w „elektronicznym sejfie". Elektroniczny sejf może być tworzony przez PrivateDisk na dyskach lokalnych lub przenośnych nośnikach danych (stacja dyskietek, napęd ZIP lub dysk magnetooptyczny, CD-ROM, DVD, karta pamięci flash itd.).

WinMagic SecureDoc – kompleksowe szyfrowanie dysków i partycji.

SecureDoc firmy WinMagic Inc. jest nowoczesnym programem przeznaczonym do szyfrowania całych dysków oraz wybranych partycji. Program szyfrując dysk lub partycję szyfruje praktycznie każdy jego sektor, dzięki czemu wszystkie informacje przechowywane są na nim wyłącznie w formie zaszyfrowanej, łącznie z samym systemem operacyjnym, wszystkimi danymi, plikami tymczasowymi, plikami wymiany (*swap file*), plikami znajdującymi się w koszu oraz tymi, które zostały z kosza usunięte. Gwarantuje to, że żadne poufne informacje nigdy nie znajdą się na dysku w formie niezaszyfrowanej, a tym samym – nie zostaną odczytane przez osoby niepowołane. Szyfrowanie całego dysku i wszystkich przechowywanych na nim informacji jest jedyną metodą dającą użytkownikowi 100 proc. bezpieczeństwa.

WinMagic SecureDoc Enterprise Server

SecureDoc Enterprise Server korzystając z sieci LAN/WAN umożliwia łatwą i bezpieczną instalację programu SecureDoc na wszystkich stacjach roboczych w sieci. Program współpracuje z Active Directory, PKI, tokenami USB (kartami kryptograficznymi), co pozwala na duże oszczędności finansów, ponieważ można wykorzystać istniejącą już w przedsiębiorstwie strukturę. SecureDoc Enterprise Server umożliwia administratorom stworzenie prostej paczki instalacyjnej, która następnie może zostać przesłana na stacje robocze poprzez sieć LAN/WAN. Ponadto program korzysta z usługi LDAP, dzięki czemu administrator ma możliwość łatwego zaimportowania istaniejących profili użytkownika z Active Directory lub z serwerów PKI. SecureDoc Enterprise Server umożliwia również importowanie danych z innych baz wykorzystując plik MS Excel CSV. Koncepcja organizowania grup użytkowników

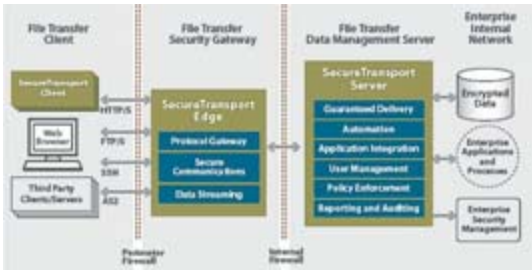
znacznie ułatwia zarządzanie kluczami szyfrującymi, ich zbiorami (*KeyFile*) jak również profilami użytkowników, które w łatwy sposób mogą być przenoszone pomiędzy różnymi grupami. Administrator ma pełną kontrolę nad projektem i może dowolnie zmieniać profile użytkowników z jednego miejsca w sieci. Dzięki wykorzystaniu bazy MS SQL Server lub MS Access administrator ma możliwość dowolnego zwiększania liczby użytkowników korzystających z SecureDoc Disk Encryption.

Ochrona sieci

Nowoczesny model bezpieczeństwa wymaga wzbogacenia popularnych aplikacji o możliwości współpracy ze standardami bezpieczeństwa. Istotną rolę odgrywa tutaj oprogramowanie dedykowane do celów bezpiecznej komunikacji. Oto kilka zaawansowanych systemów ochrony komunikacji i przesyłania danych czołowych producentów rynku e-security.

SecureTransport – bezpieczny system wymiany dokumentów.

Firma Tumbleweed jest jednym z wiodących na świecie dostawców rozwiązań w zakresie bezpieczeństwa sieci komputerowych i ochrony danych w systemach elektronicznego obiegu dokumentów (*Electronic Dokument Interchange/EDI*). Jednym z trzech podstawowych produktów tej firmy jest oprogramowanie SecureTransport – rozwiązanie zapewniające korporacjom dostosowany do ich wymagań, wieloplatformowy i wielostronny system wymiany dokumentów w większości najważniejszych formatów (łącznie ponad 100), jakie są obecnie stosowane w środowisku e-commerce. Możliwości współpracy z szerokim wachlarzem systemów operacyjnych, relacyjnych baz danych, systemów ERP, serwerów aplikacyjnych i nowoczesnych technologii szyfrujących to najważniejsze zalety SecureTransport jako niezawodnego i bezpiecznego narzędzia do transferu danych pomiędzy jego użytkownikami. Unikatowymi cechami rozwiązania Secure Transport jako całości są integracja z infrastrukturą informatyczną o praktycznie nieograniczonej rozpiętości geograficznej i niepodważalność metod potwierdzających dostarczenie danych do użytkownika końcowego.



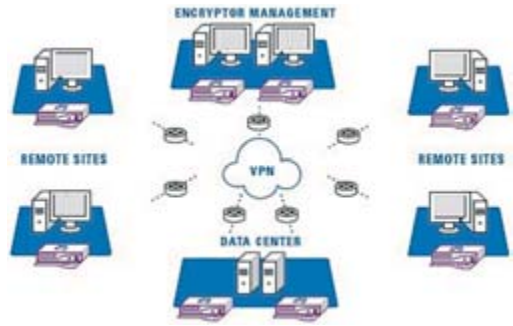
Elementy systemu SecureTransport

SureWare Net – ochrona trasmisji w sieciach.

AEP SureWare NET jest produktem zapewniającym wysoki poziom bezpieczeństwa i szybkość przesyłania w ochronie transmisji danych w sieciach IP. Pozwala uzyskać zarówno niepodważalną poufność danych, jak i uwierzytelnianie tożsamości użytkowników. Poprzez wykorzystanie natywnego oprogramowania VPN oraz architektury klucza publicznego Unicert, w usługach uwierzytelniania i certyfikacji, dostarcza użytkownikom maksymalnej ochrony danych przed próbami ich przechwycenia czy modyfikacji, jaką zapewnia istniejąca obecnie technologia. Produkt może zostać włączony jako brama bezpieczeństwa IP pomiędzy wybranymi interfejsami sieciowymi lub przyłączony do dowolnej stacji roboczej jako wsparcie transmisji end-to-end pomiędzy punktami, których oddzielenie od reszty sieci ma istotne znaczenie. AEP SureWare NET dostępny jest w trzech wersjach (ED20M, EC20M, CD20M), zależnych od wsparcia dla poszczególnych algorytmów szyfrowania oraz konfiguracji systemu w związku ze współpracą z określonymi urzędami certyfikacji w architekturze PKI.

Cechy systemu:

- ✔ wykorzystanie protokołu IPSEC (szyfrowanie na warstwie IP),
- ✔ możliwość opcjonalnego podłączenia sprzętowego modułu szyfrującego AEP SureWare NET Keyper HSM,
- ✔ możliwość korzystania z podpisanych cyfrowo certyfikatów przechowywanych na kartach mikroprocesorowych,
- ✔ zintegrowany czytnik kart, wyświetlacz i klawiatura w obudowie 19",
- ✔ możliwości audytu i rejestracji działań.



AEP Netilla Security Platform – zarządzanie VPN przez www.

AEP Netilla Security Platform to nowatorskie urządzenie pełniące funkcję uniwersalnej, bezpiecznej bramki łączącej chronione wewnętrzne zasoby firmy z szeregiem aplikacji klienckich. Pozwala to na dużą swobodę nawiązywania połączeń z firmowym intranetem z dowolnie zlokalizowanej maszyny wyposażonej w standardową

przeglądarkę www. Dużą zaletą rozwiązania jest niezależność od stosowanej w firmie platformy, umożliwiająca szybką komunikację pomiędzy wieloma rozmaitymi urządzeniami w różnych lokalizacjach. Od strony administracyjnej oferuje skoncentrowane zarządzanie jednym urządzeniem, dostępnym w bezpieczny sposób poprzez interfejs www, zestaw poleceń linii komend oraz port szeregowy.

Platforma:

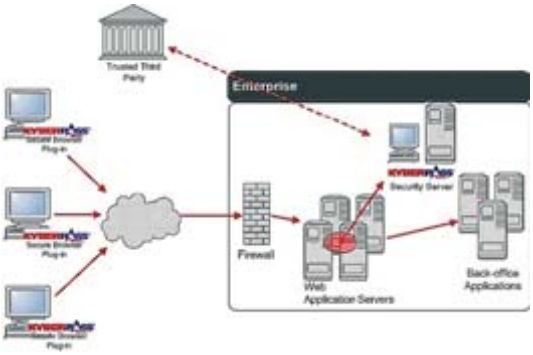
- ✔ umożliwia pracownikom bezpieczny zdalny dostęp do zasobów firmy,
- ✔ zapewnia bezpieczeństwo komunikacji w sposób przeźroczysty dla systemu użytkownika,
- ✔ jest niezależna od istniejącej platformy aplikacyjnej.

KyberPass TrustPlatform – zintegrowana platforma bezpiecznego e-biznesu.

TrustPlatform firmy KyberPass jest w pełni zintegrowanym wewnętrznie rozwiązaniem, umożliwiającym przeniesienie obecnych form działalności w środowisko e-biznesu firmie w każdej skali i w dowolnym punkcie rozwoju. Niezależnie od rodzaju i liczby wykorzystywanych aplikacji, TrustPlatform oferuje bezproblemowe wdrożenie i krótki okres pomiędzy jego ukończeniem a pojawieniem się oferty firmy na rynku elektronicznym. Poprzez wykorzystanie takiej platformy firma zyskuje większą kontrolę nad wydatkami i wydajnością prowadzonych interesów i zarządzaniem liniami projektowymi w zgodzie z założeniami strategii ROI (*Return On Investment*). Rozwiązanie zbudowano z trzech ściśle współpracujących ze sobą komponentów – TP Security Server, TP Desktop Plug-ins i TP Developer Toolkit – serwera usług związanych z kontrolą bezpieczeństwa i integralności danych, aplikacji klienckiej obsługującej integrację zewnętrznych aplikacji z systemem bezpieczeństwa i szeroko udokumentowanego zestawu bibliotek programistycznych, umożliwiającego dostosowanie specyficznych cech rozwiązania do oczekiwań użytkownika. W wersji oferowanej w sprzedaży pełny pakiet zawiera moduły obsługi intra- i extranetu (*Common Services, Extranet Services, VPN support*), sterowniki i translatory obsługi formatu XML (B2B Integration Services, Secure XML Web Services), komponenty umożliwiające współpracę z architekturą PKI (*PKI Validation Services*) oraz rozszerzenia Marketplace Extensions dla konkretnych rodzajów działalności biznesowej. Jako gotowe komponenty składnika Desktop Plug-ins dostępne są Extranet Plug-in, Signing Plug-in i Email Plug-in, dzięki którym firma natychmiast po ukończeniu wdrożenia może w 100 proc. wykorzystać elektroniczny obieg dokumentów, równolegle lub zamiennie z użyciem rozwiązań analogowych.

Sprzętowe moduły kryptograficzne

Są to urządzenia zwiększające efektywność i szybkość pracy protokołów kryptograficznych do bezpiecznej wymiany informacji. Dzięki zastosowaniu unikatowych rozwiązań umożliwiają osiągnięcie najwyższego poziomu bezpieczeństwa dla kluczy kryptograficznych w systemach PKI. Realizują również zaawansowany system zarządzania kluczami kryptograficznymi.



Schemat funkcjonalny platformy KyberPass TrustPlatform

W ramach sprzętowych modułów kryptograficznych (HSM) istnieją dwie rodziny produktów. Pierwsza to akceleratory SSL, które rozwiązują problem szybkiego przetwarzania autoryzacji na serwerach www. Druga rodzina to moduły zarządzające kluczami kryptograficznymi – odgrywają one kluczową rolę w zabezpieczaniu wrażliwych danych (np. klucze urzędów certyfikacji) elementów Infrastruktury Klucza Publicznego (PKI).

Moduły HSM

Są to sprzętowe moduły przeznaczone do przechowywania, ochrony i zarządzania kluczami kryptograficznymi w Infrastrukturze Klucza Publicznego (PKI).

SureWare Keyper – centrum zarządzania kluczami kryptograficznymi.

AEP SureWare Keyper to sprzętowy moduł kryptograficzny, zapewniający najwyższy stopień bezpieczeństwa. Moduł oferuje szybkie generowanie i bezpieczne przechowywanie kluczy kryptograficznych w środowisku odpornym na manipulacje. Złącze Ethernet umożliwia współdzielenie urządzenia w sieci TCP/IP. SureWare Keyper Professional posiada zintegrowany wyświetlacz, klawiaturę, czytnik kart oraz przełącznik sprzętowy do uruchamiania operacji tworzenia kopii zapasowych kluczy, zmiany ustawień i aktywowania serwisów kryptograficznych. Urządzenie jest jednym z nielicznych modeli HSM posiadających najwyższy certyfikat bezpieczeństwa FIPS 140-1 Level 4. Przeznaczone jest dla najbardziej wymagających obiektów środowiska PKI, takich jak urzędy certyfikacji, do przeprowadzania najistotniejszych operacji kryptograficznych, takich jak generowanie kluczy urzędów. Urządzenie jest dostępne również w postaci karty PCI, wyposażonej dodatkowo w zewnętrzny czytnik kart z klawiaturą i wyświetlaczem, podłączanym poprzez SureWare OmniPort.

Private Server/EMV – wysoko wydajny, elastyczny i skalowalny HSM.

Private Server to moduł HSM podłączany przez sieć. Zapewnia on bezpieczne środowisko dla wykonywania operacji kryptograficznych, przechowywania kluczy oraz zarządzania nimi.

netHSM – zaawansowany sieciowy HSM.

HSM firmy nCipher reprezentuje nową generację sprzętu kryptograficznego, zdolną do zastąpienia rozbudowanych i kosztownych rozwiązań serwerowych. Moduł został zaprojektowany do współdzielenia swojej funkcjonalności w sieciach wymagających bezpiecznego transferu i silnego uwierzytelniania. Wydajność kryptograficzna netHSM sięga 1600 podpisów 1024-bitowych na sekundę. Ponadto moduł umożliwia bezpieczne składowanie nieograniczonej ilości kluczy i współpracę z maksymalnie 20 serwerami. Zgodność ze środowiskiem nCipher Security World otwiera szerokie możliwości dostosowania netHSM do polityki bezpieczeństwa w firmie.

nShield – zaawansowana ochrona i zarządzanie kluczami kryptograficznymi.

Moduł nShield to nie tylko wysokiej klasy produkt zapewniający bezpieczne przechowywanie kluczy kryptograficznych. To także unikatowe, oparte na zabezpieczeniach sprzętowych i programowych, bezpieczne środowisko nCipher Security World – kompletne rozwiązanie do zarządzania kluczami kryptograficznymi. Do modułu dołączony jest pakiet oprogramowania, w skład którego wchodzi m.in. aplikacja KeySafe, która z wykorzystaniem graficznego interfejsu pozwala na sprawne zarządzanie środowiskiem. Środowisko nCipher Security World sprawnie integruje się z istniejącymi systemami PKI, a dodatkowe narzędzia programistyczne umożliwiają tworzenie własnych aplikacji wykorzystujących zalety modułu nShield. Mechanizmy zarządzania kluczami uzupełniono funk-cjami akceleracji operacji kryptograficznych. Ze względu na uniwersalny charakter i zgodność ze standardami Infrastruktury Klucza Publicznego nShield znajduje zastosowanie w wielu związanych z bezpieczeństwem sektorach branży IT, od złożonych środowisk PKI poprzez systemy bezpiecznego dostępu do baz danych do rozwiązań przeznaczonych do szybkiego przetwarzania operacji SSL. Najnowszy model **nShield 800** jest najmocniejszym urządzeniem z serii, jest on zdolny do wykonania 800 podpisów (1024-bitowych). Dodatkowo została poprawiona wydajność pozostałych funkcji urządzenia.

nForce – bezpieczeństwo PKI i maksymalna wydajność SSL.

Moduły sprzętowe nForce zapewniają znaczące zwiększenie szybkości operacji SSL. Najnowsza generacja tych urządzeń pozwala na osiągnięcie przepustowości 1600 nowych połączeń SSL na sekundę, co redukuje zapotrzebowanie na moc obliczeniową serwerów. Rozwiązania korzystające z nForce są szybsze i tańsze niż tradycyjne implementacje SSL, pozbawione sprzętowej akceleracji.

Podstawą bezpieczeństwa większości usług sieciowych jest ochrona kluczy prywatnych wykorzystywanych przez sesje SSL. Urządzenie nForce posiada certyfikat FIPS 140-2 Level 2, co oznacza najwyższy poziom bezpieczeństwa kluczy, których składowanie i przetwarzanie odbywa się w ramach odpornego na manipulacje modułu kryptograficznego.

Wszystkie moduły nCipher funkcjonują w ramach środowiska Security World, które odpowiada za bezpieczeństwo zarządzania dostępem, skalowalność rozwiązań budowanych na ich podstawie oraz dystrybucję kluczy kryptograficznych. Osadzenie sprzętu w tak zdyscyplinowanej strukturze umożliwia dowolne łączenie modułów w celu dopasowania rozwiązań kryptograficznych do zróżnicowanych potrzeb usług z zakresu bezpieczeństwa.

W module nForce funkcjom przyspieszającym operacje SSL towarzyszy bezpieczna obsługa kluczy kryptograficznych w odpornym na manipulacje środowisku. Urządzenie wypełnia zapotrzebowanie na wielofunkcyjny moduł bezpieczeństwa, dostosowany zarówno do pracy z serwerem SSL, jak i Infrastrukturą Klucza Publicznego. nForce dostępny jest w formie karty PCI lub zewnętrznego modułu SCSI. Modułowi towarzyszy oprogramowanie KeySafe oraz technologia nCipher Remote Operator do zdalnego zarządzania kluczami.

nForce Ultra jest kontynuacją udanej serii akceleratorów nForce. Najnowszy model oferuje niespotykaną na rynku wydajność 10.000 operacji na sekundę. Jest on również pierwszym urządzeniem przetwarzającym w całość sesje SSL/TLS na karcie. Dodatkowo wysoką jakość urządzenia gwarantuje certyfikat FIPS 140-2 Level 3.

Akceleratory SSL

Są to urządzenia zewnętrzne i karty PCI pozwalające na przeniesienie ciężaru operacji kryptograficznych (np. obsługa sesji SSL) z procesora serwera na wysoko wydajny akcelerator.

SureWare Runner – rozwiązanie dla obciążonych serwerów SSL.

Akceleratory AEP to rodzina rozwiązań zwiększających wydajność operacji SSL na serwerach www. Modele SureWare Runner 1000 i SureWare Runner 2000 umożliwiają przeprowadzanie odpowiednio 1000 i 2000

1024-bitowych transakcji SSL na sekundę. Przeniesienie obliczeń kryptograficznych do akceleratora AEP pozwala ponadto na znaczne zredukowanie obciążenia procesora na serwerze www, co prowadzi do podniesienia wydajności całego rozwiązania opartego na SSL. Badania laboratoryjne wykazały nawet 12-krotne przyspieszenie operacji SSL w procesach stosujących AEP SSL Accelerator. Model S1000 oferuje ponadto funkcje zarządzania kluczami kryptograficznymi.

nFast Ultra – maksymalna wydajność operacji SSL.

Najnowszy akcelerator firmy nCipher oferuje najwyższą wydajność przetwarzania SSL i umożliwia całkowite przejęcie wykonywania operacji SSL oraz odciążenie procesorów serwera, w którym zainstalowana jest karta nFast Ultra. Działanie modułu oparte jest na całkowitym przejęciu obsługi sesji SSL i przekazywaniu do docelowej aplikacji czystego (zdeszyfrowanego) strumienia danych. W ten sposób nFast Ultra staje się niezależny od zewnętrznych interfejsów sieciowych i nie wymaga zainstalowania na macierzystym serwerze aplikacji wspierających SSL.

Wydajność nFast Ultra wynosi do 10,000 połączeń na sekundę dla kluczy 1024-bitowych, maksymalna wielkość obsługiwanych kluczy to 4096 bitów, zaś przepustowość sięga 300 Mbps. Moduł w pełni wspiera protokół SSL, łącznie z szyfrowaniem symetrycznym i asymetrycznym. Firma nCipher zapowiada na pierwszy kwartał 2006 r. dodanie do nFast Ultra możliwości zarządzania kluczami kryptograficznymi i certyfikowanie urządzenia do standardu FIPS.

Urządzenia specjalizowane

Istnieją również sprzętowe moduły kryptograficzne o specjalnym przeznaczeniu. Poza standardową funkcjonalnością zostały one wyposażone przez producenta w dodatkowe funkcje, które umożliwiają wykorzystanie ich dla specyficznych zastosowań.

CoSign – centralny moduł przechowujący klucze użytkowników.

CoSign firmy Algorithmic Research oferuje kompletne środowisko do składania podpisu elektronicznego. Zaletą CosSgn jest przeniesienie administracji na zewnętrzny system obsługi użytkowników typu Microsoft Active Directory lub LDAP. Urządzenie korzysta również z repozytoriów certyfikatów klucza publicznego, współpracując z czołowymi urzędami certyfikatów. CoSign posiada certyfikat FIPS 140-2 Level 3, co sytuuje urządzenie w klasie rozwiązań korporacyjnych wymagających wysokiego poziomu bezpieczeństwa. Produkt jest stale rozwijany, a jego najnowsza wersja obsługuje kolejny system katalogowy Novell/NDS i umożliwia grupom użytkowników współdzielenie kluczy podpisujących.

Dzięki wydajnej architekturze i prostej administracji CoSign jest idealnym rozwiązaniem dla bezpiecznego podpisywania dokumentów funkcjonujących w złożonych systemach obiegu informacji elektronicznej.

Z rodziny CoSign pochodzi również mniej rozbudowany Signlet, certyfikowany do poziomu bezpieczeństwa FIPS 140-2 Level 1. Urządzenie obsługuje podpisywanie dokumentów i poczty elek-tronicznej z poziomu popularnych aplikacji biurowych: MS Word, MS Excel, MS Outlook oraz Adobe Acrobat. Signlet przeznaczony jest dla małych i średnich firm, które poszukują efektywnego rozwiązania do silnego zabezpieczenia dokumentów elektronicznych.

Unikatową cechą CoSign i Signlet jest ręczne składanie tradycyjnego pisemnego podpisu, który następnie jest konwertowany do pliku graficznego i funkcjonuje jako bezpieczny ekwiwalent podpisu elektronicznego.

payShield – czołowy HSM dla e-commerce.

Znaczenie modułu kryptograficznego payShield wynika z rygorystycznego przestrzegania zasad bezpieczeństwa transakcji internetowych. Urządzenie spełnia kryptograficzne wymagania standardów Visa 3-D Secure oraz MasterCard SPA i znajduje zastosowanie w procesach e-commerce. Certyfikacja do poziomu FIPS 140-2 Level 3 sprawia, że payShield może stanowić podstawę bezpiecznej, odpornej na manipulacje infrastruktury płatności elektronicznych. Zaimplementowane funkcje kryptograficzne wraz z szeroką gamą wspieranych algorytmów szyfrujących zapewniają dużą szybkość wykonywania wszechstronnych operacji kryptograficznych. Moduł payShield jest osadzony w uznanym modelu Security World, stworzonym przez firmę nCipher w celu zapewnienia bezpiecznego zarządzania kluczami kryptograficznymi.

Właściwości payShield:

- ✔ w pełni zgodny ze ścisłymi wymaganiami standardu 3-D Secure,
- ✔ wspiera inne standardy i aplikacje, takie jak MasterCard SecureCode, EMV SmartCards, EFTPOS, przetwarzanie ATM PIN,
- ✔ jest kompletnym środowiskiem zarządzania kluczami symetrycznymi i asymetrycznymi,
- ✔ przyspiesza przetwarzanie kryptograficzne, eliminując „wąskie gardła" i umożliwiając uwierzytelnienie transakcji w czasie rzeczywistym,
- ✔ wspiera dedykowane API, które pozwalają na dostosowanie do potrzeb użytkownika operacji szyfrowania, deszyfrowania i podpisywania.

Elementy infrastruktury PKI

Są to systemy i aplikacje do obsługi najbardziej rozpowszechnionego modelu obiegu i zarządzania certyfikatami. Do dyspozycji mamy zarówno kompletne środowiska, jak i pojedyncze, wyspecjalizowane produkty.

Certification Authority

Urząd certyfikacji wydaje elektroniczne certyfikaty tożsamości dla innych osób czy instytucji. Jest przykładem Zaufanej Trzeciej Strony. Urzędem certyfikacji może być zewnętrzna firma, która za pewną opłatą wydaje certyfikat na podstawie, którego można poświadczyć tożsamość właściciela klucza. Istnieje również możliwość ustanowienia urzędu certyfikacji wewnątrz firmy, dzięki czemu uniezależnimy się od zewnętrznych instytucji.

RSA Keon Certificate Authority – weryfikacja certyfikatów w czasie rzeczywistym.

Moduł ten zaspokaja rosnące zapotrzebowanie na instrument do wydawania, zarządzania i weryfikacji certyfikatów klucza publicznego. Został zbudowany na otwartych standardach w celu współpracy z szeroką gamą programów zgodnych z Infrastrukturą Klucza Publicznego (PKI). Potwierdzona niezależnymi testami skalowalność umożliwia budowanie systemów zdolnych do obsługi ponad 8 milionów użytkowników. Certificate Authority posiada unikatową możliwość weryfikacji certyfikatów w czasie rzeczywistym poprzez Online Certificate Status Protocol (OCSP). Moduł wspiera również standard Certificate Revocation List (CRL), w którym weryfikacja odbywa się w ustalonych odstępach czasu.

RSA Keon Root Signing Service – zgodność certyfikatów z wielu źródeł.

Root Signing Service zapewnia zgodność używanych certyfikatów z oprogramowaniem komunikacyjnym i rozszerza funkcjonalność wewnątrzfirmowego rozwiązania Certificate Authority poza ramy organizacji, w której jest stosowany. W ten sposób można utworzyć bezpieczne relacje z wieloma partnerami, dostawcami i klientami. Moduł ten tworzy pomost pomiędzy globalnie uznawanymi certyfikatami w programach klienckich a certyfikatami wydawanymi w ramach niezależnej struktury urzędów certyfikatów. Zapobiega to odrzuceniu nierozpowszechnianego certyfikatu przez przeglądarkę www lub innego klienta. Operacja ta nie zmienia statusu certyfikatu z firmowego na uznawany przez RSA.

RSA Keon Web PassPort – integracja autoryzacji SSL, S/MIME, VPN.

Web PassPort integruje się z oprogramowaniem komunikacyjnym zdolnym do współpracy z kluczem publicznym (przeglądarka, klient poczty) w celu uproszczenia procesu autoryzacji w systemach opartych na SSL, S/MIME lub VPN. Moduł działa w oparciu o logowanie na serwer Web PassPort, pobieranie danych użytkownika z katalogu zgodnego z LDAP oraz przekazywanie certyfikatu poprzez plug-in Web PassPort zainstalowany w oprogramowaniu użytkownika. Centrum systemu stanowi wirtualna karta zawierająca certyfikaty i klucze publiczne użytkownika, zabezpieczone symetrycznym 256-bitowym kluczem RC5 oraz dodatkowo 112-bitowym algorytmem 3DES. System umożliwia korzystanie z wielu takich wirtualnych kart, przez co użytkownik może autoryzować się w różnych środowiskach, które nie współpracują ze sobą. Web PassPort automatycznie aktualizuje Microsoft Trusted Certificate Authority List, co pozwala na integrację certyfikatów z programami Microsoftu.

RSA Keon Web Server SSL – serwer SSL z dystrybucją certyfikatów.

Web Server SSL Solution jest przeznaczony dla średnich i dużych firm, które potrzebują bezpiecznego serwera www oraz własnego systemu autoryzacji. Utworzone certyfikaty są następnie współzatwierdzane przez firmę RSA Security, co umożliwia ich powszechne rozpoznawanie. Pakiet ten może efektywnie zastąpić zewnętrzne rozwiązania SSL, a w integracji z innymi modułami RSA Keon – znacznie wzbogacić i rozwinąć zarządzanie certyfikatami.

UniCERT – modułowy, skalowalny i elastyczny system obsługi urzędów certyfikatów.

Pozostający w czołówce światowej najważniejszy element środowiska architektury klucza publicznego, stworzony dla zapewnienia bezpieczeństwa wszelkim operacjom z zakresu e-biznesu. Jako system wydawania i zarządzania certyfikatami spełnia wymagania istniejące w tradycyjnym środowisku prowadzenia działalności komercyjnej (prywatności, integralności, niepodważalności i określenia tożsamości).

- Security Policy – polityka bezpieczeństwa – moduł definiujący podstawową strukturę dystrybucji zaufanej informacji. Polityka bezpieczeństwa zwykle zawiera wytyczne obsługi kluczy elektronicznych i chronionej przez nie informacji oraz określa poziom kontroli w oparciu o poziom zagrożenia poszczególnych stref całej infrastruktury.
- Certificate Practice Statement (CPS) – praktyczne założenia certyfikacji – to moduł szczegółowo określający procedury operacyjne wdrażanej polityki bezpieczeństwa. Definiuje budowę i zasady działania centrum certyfikacji (jednego lub więcej), sposoby wydawania i unieważniania certyfikatów, sposoby generowania i certyfikowania kluczy oraz zasady ich przechowywania i udostępniania użytkownikom.
- Certificate Authority (CA) – centrum certyfikacji – podstawowy komponent architektury klucza publicznego odpowiedzialny za zarządzanie certyfikatami przez cały cykl ich ważności, odpowiedzialny za wydawanie certyfikatów w oparciu o informacje określające tożsamość użytkownika zawarte w wygenerowanych kluczach elektronicznych, definiowanie okresów ważności wydawanych certyfikatów oraz publikowanie list certyfikatów unieważnionych (*Certificate Revocation List* – CRL).
- Registration Authority (RA) – centrum rejestracji użytkowników – element pośredniczący pomiędzy centrum certyfikacji a użytkownikami kluczy, obsługujący żądania wygenerowania certyfikatów na podstawie informacji o użytkownikach. Poziom jakości usług centrum rejestracji określa stopień zaufania dla wydanych certyfikatów.

- Certificate Distribution System (CDS) – system dystrybucji certyfikatów – mechanizm obsługujący otrzymywanie kluczy przez użytkowników końcowych. Zwykle jest to katalog korporacyjny (serwer LDAP) funcjonujący jako repozytorium certyfikatów i serwer udostępniający informacje o statusie danego certyfikatu przy użyciu protokołu określania statusu (*Online Certificate Status Protocol* – OCSP).

OmniRoot – uzupełnienie systemu wydawania certyfikatów w ramach UniCERT.

OmniRoot jest opcjonalną usługą dla systemu architektury klucza publicznego, która daje użytkownikom unikatową możliwość w zakresie definiowania własnej architektury PKI. Jedynie producent UniCERT oferuje swoim klientom opcję stworzenia własnej hierarchii wydawania certyfikatów (hierarchii urzędów certyfikacji) lub integracji architektury klucza publicznego wdrażanej u użytkownika z architekturą PKI istniejącą u producenta. Oznacza to, że OmniRoot daje użytkownikom licencje na wydawanie certyfikatów kwalifikowanych i weryfikowanych w hierarchii CA producenta, co w efekcie umożliwia natychmiastowe rozpoznawanie certyfikatów w popularnych przeglądarkach internetowych.

Validation Authority

Głównym komponentem Infrastruktury Klucza publicznego są certyfikaty. Są to wirtualne identyfikatory wystawione przez niezależne urzędy certyfikacji (CA), zapewniające możliwość potwierdzenia tożsamości osoby, organizacji, komputera itp. Tak samo jak przy fizycznych dokumentach tj. dowód osobisty, prawo jazdy, informacje te mogą wygasnąć, zostać unieważnione lub zawieszone. Dlatego aby zapewnić integralność i prawidłową pracę całego systemu niezbędne są mechanizmy sprawdzające poprawność oraz ważność certyfikatów.

Tumbleweed Validation Authority – czołowy system walidacji certyfikatów.

Kompletny, skalowalny system weryfikacji certyfikatów w czasie rzeczywistym, z szerokim wsparciem dla standardów bezpieczeństwa i kluczowych produktów e-security. Produkty firmy Tumbleweed stanowią niezbędne uzupełnienie modelu PKI o usługi sprawdzania statusu ważności certyfikatów klucza publicznego. Są funkcjonalnym odpowiednikiem usługi potwierdzania ważności karty kredytowej dla akceptującego transakcję płatniczą wykonywaną tą kartą oraz światowym standardem realizującym zadania weryfikacji statusu certyfikatu. Współpracują z wszystkimi urzędami certyfikacji. Pozwalają na budowę serwerów realizujących wszystkie znane protokoły badania statusu certyfikatów (CRL, CRL Distribution Points, OCSP i własny standard firmy: CRT). Zawierają uzupełnienia dla najpopularniejszych aplikacji PKI (programów pocztowych, serwerów i przeglądarek www). Dostępne są też narzędzia programistyczne (toolkity) ułatwiające dodawanie funkcjonalności badania statusu certyfikatów do własnych aplikacji.

Certyfikaty elektroniczne umożliwiają firmom i osobom prywatnym dokonywanie transakcji finansowych i urzędowych operacji w świecie elektronicznym. Niemniej, podobnie jak dowody tożsamości i karty kredytowe, posiadają określony czas ważności oraz mogą zostać zagubione lub skradzione, lub po prostu odebrane przez instytucję, która nadaje prawa do ich używania. Podobnie jak w przypadku zwykłej transakcji, również w świecie elektronicznym kontrahent dokonuje sprawdzenia/potwierdzenia ważności przedstawionego dokumentu – firmy wykorzystujące elektroniczny obrót dokumentami i środkami finansowymi muszą mieć możliwość weryfikacji prezentowanego przez klienta certyfikatu. Tę funkcjonalność w czasie rzeczywistym, w sposób stabilny i kompleksowy oferuje Validation Authority. Dostępne jako produkt lub zarządzalna usługa oprogramowanie Tumbleweed VA, niezależnie od marki używanej architektury PKI, przy współpracy z urzędami certyfikacji i serwerami usługi LDAP (katalog korporacyjny) dokonuje niepodważalnej weryfikacji certyfikatów przedstawianych przez strony biorące udział w transakcji.

Time-Stamping Authority

Time-Stamping Authority jest Zaufaną Trzecią Stroną (TTP), tworzącą znaczniki czasowe, które mogą zostać wykorzystane w celu wykazania, iż pewna informacja istniała w konkretnej chwili. Znacznik czasowy (*time-stamp*) jest niezaprzeczalnym dowodem, że dane nie zostały sfałszowane oraz nie została zmodyfikowana data ich utworzenia. Są one generowane na podstawie skrótu kryptograficznego wiadomości.

DSE 200 – sprzętowe zabezpieczanie dokumentów.

Document Sealing Engine 200 służy do zaopatrywania dokumentów elektronicznych w podpis cyfrowy i stempel czasowy. Urządzenie posiada certyfikat FIPS 140-2 Level 3 i może zostać łatwo włączone w istniejącą infrastrukturę bezpieczeństwa. Dołączone narzędzia dla programistów pozwalają na zintegrowanie obsługi sprzętu z aplikacjami Java lub C, pracującymi pod kontrolą systemów Linux, Solaris i Windows.

Narzędzia programistyczne

Uzupełnieniem wyżej opisnych przykładów systemów i urządzeń są narzędzia do implementacji kryptograficznych metod ochrony informacji w systemach informatycznych. Należą do nich m.in. kompletne środowiska do szerokiego spektrum języków programowania i systemów, w celu przystosowania posiadanych aplikacji do korzystania ze standardów bezpieczeństwa oraz wyspecjalizowanych modułów sprzętowych. Pakiety programistyczne autorstwa najlepszych firm na rynku e-security umożliwiają zastosowanie standardów bezpieczeństwa, jak i specyficznych funkcji obsługujących sprzętowe moduły kryptograficzne (HSM). Należą do nich m.in. biblioteki wspomagające moduły sprzętowe, systemy do bezpiecznego wykonywania kodu Java lub C/C++ oraz biblioteki programistyczne dla obsługi certyfikatów.

Grzegorz Kantowicz

opracowano na podstawie materiałów firm CryptoTech, nCipher, RSA Security, Unicard, Tumbleweed, SafeNet

Biometryczne systemy zabezpieczeń

Biometria może być zdefiniowana jako sposób rozpoznawania i identyfikacji osobistej opartej na cechach fizycznych i behawioralnych. Są to między innymi: linie papilarne, kształt twarzy czy dłoni, charakterystyczne cechy tęczówki oka, pisma ręcznego, jak również mowa, sposób uderzania w klawisze, a nawet układ żył nadgarstka. Biometria może być wykorzystana do uniemożliwiania nieautoryzowanych prób dostępu do bankomatów, komputerów osobistych, sieci komputerowych, telefonów komórkowych, domowych systemów alarmowych, zamków drzwiowych, kart procesorowych... – lista jest nieograniczona.

Identyfikacja biometryczna jest lepsza od obecnie stosowanych metod korzystających z kart dostępu, numerów PIN i haseł z wielu przyczyn. Najistotniejsze jest to, że obecnie stosowane metody identyfikują numer, kartę czy hasło, a nie osobę. Autoryzacja w takim przypadku nie jest w żaden sposób związana z osobą – jest związana wyłącznie z urządzeniem. Prawdziwa, biometryczna identyfikacja zastępuje potrzebę pamiętania hasła całkowicie. Biometryczne metody identyfikacji mogą być stosowane zarówno niezależnie, jak i w połączeniu z dotychczas stosowanymi rozwiązaniami.

Dzięki zastosowaniu dodatkowych systemów ochrony takich jak zapisywanie jedynie matematycznego wzorca cech charakterystycznych czy szyfrowanie transmisji, informacje są chronione zarówno przed przypadkowym jak i celowym działaniem intruzów.

Systemy biometryczne zapewniają wysoki poziom bezpieczeństwa oraz wygody. Osoby podlegające autoryzacji nie muszą nosić z sobą żadnych specjalnych kart, pamiętać skomplikowanych haseł itd. Z drugiej strony techniki te nadają się do zabezpieczania zarówno pilnie strzeżonych zasobów, jak i pojedynczych komputerów PC. Spadające ceny sprawiły, że biometria trafiła pod strzechy.

Techniki biometryczne są obecnie jednym z najbardziej dynamicznie rozwijających się działów teleinformatyki. Rosnąca ilość przetwarzanych informacji powoduje, że ważnym problemem staje się zapewnienie najwyższej jakości kontroli dostępu. Mowa tu zarówno o kontroli dostępu do pomieszczeń, jak i autoryzacji użytkowników korzystających z określonych danych lub programów. Tradycyjne techniki oparte na kartach magnetycznych, mikroprocesorowych czy też na systemach haseł mają zbyt wiele wad, by podołać obecnym wymaganiom użytkowników. Przede wszystkim kartę magnetyczną czy mikroprocesorową można po prostu ukraść, hasło można podejrzeć lub je po prostu wymyślić (zdecydowana większość użytkowników stosuje trywialne hasła, jak imię, data urodzin czy numer rejestracyjny samochodu).

Problemy te nie występują w przypadku kontroli biometrycznej, jest ona bowiem oparta na specyficznych cechach organizmu, charakterystycznych dla każdego człowieka. Warto podkreślić, że również z punktu widzenia kosztów systemy oparte na kartach nie są najbardziej korzystne: wszak oprócz czytnika trzeba jeszcze zakupić, często niebagatelną, liczbę kart. Co gorsza, w przypadku kart magnetycznych konieczna jest ich okresowa wymiana! A przecież w odciski palców nikogo nie musimy wyposażać. Dzięki powstaniu rozwiązań, w których weryfikacja jest przeprowadzona przez komputer, czytnik nie musi już być tak wyładowany elektroniką. W praktyce oznacza to, że profesjonalne urządzenia, np. do identyfikacji na podstawie linii papilarnych, można już kupić za około 1000 PLN netto.

W chwili obecnej najpopularniejsze techniki biometryczne można podzielić na następujące podgrupy:

- ✔ systemy oparte na rozpoznawaniu geometrii twarzy;
- ✔ systemy oparte na rozpoznawaniu linii papilarnych;
- ✔ systemy oparte na rozpoznawaniu geometrii dłoni;
- ✔ systemy oparte na rozpoznawaniu cech charakterystycznych tęczówki oka.

Powyższa lista nie wyczerpuje wszystkich możliwości, tym niemniej są to obecnie najpopularniejsze i najpowszechniej stosowane systemy.

Geometria twarzy

Metoda weryfikacji geometrii twarzy należy (obok weryfikacji tęczówki oka) do najmniej inwazyjnych. Nie jest wymagany absolutnie żaden kontakt fizyczny z urządzeniem. Wykorzystuje się fakt, że twarze dwóch różnych osób nigdy nie będą identyczne. W procesie weryfikacji budowany jest matematyczny wzorzec twarzy, który jest następnie porównywany ze wzorcem zapisanym w trakcie rejestracji. Jeżeli obydwa wzorce do siebie pasują, oznacza to pozytywną weryfikację i udzielane są odpowiednie prawa dostępu. Nie stanowią przeszkody okulary, zarost, makijaż czy zmiana uczesania. Często stosowany jest układ dwóch kamer jednocześnie w celu zwiększenia wiarygodności odczytu.

Geometria dłoni

Weryfikacja geometrii dłoni jest bardzo wygodną i wiarygodną metodą – dzięki temu znajduje zastosowanie w systemach kontroli dostępu i rejestracji czasu pracy. Zalety tego rodzaju weryfikacji zostały uznane i doce-

nione między innymi przez wiele amerykańskich instytucji rządowych i wojskowych. Zasada działania jest prosta. Po umieszczeniu dłoni w komorze urządzenia mierzony jest rozmiar i kształt dłoni – długość, szerokość i grubość czterech palców oraz obszar pomiędzy kostkami palców (kciuk nie jest wykorzystywany). Odbywa się to poprzez oświetlenie dłoni promieniami podczerwonymi i odczytanie obrazu macierzą CCD – tworzony jest trójwymiarowy obraz kształtu dłoni (kilka różnych położeń). Z wyników pomiarów tworzony jest 9-bajtowy (maksimum) wzorzec, który zapisywany jest w pamięci razem z kodem ID osoby. Proces weryfikacji użytkownika polega na wprowadzeniu kodu ID oraz porównaniu wzorca dłoni aktualnie analizowanego ze wzorcem umieszczonym w pamięci. Jeżeli wynik porównania jest pozytywny (osoba próbująca dostać się do pomieszczenia jest osobą uprawnioną), efektem jest np. otwarcie drzwi. Dostępna jest także wersja czytnika wymagająca autoryzcji dwóch osób jednocześnie w celu otwarcia drzwi do np. skarbca. System potrafi także dostosować się do zmian geometrii dłoni postępujących na skutek np. starzenia lub tycia.

Wiele osób na pewno zastanawia się, co będzie, jeśli ręka zostanie obcięta i użyta w celu fałszywej weryfikacji. Odpowiedź jest prosta – nic z tego. Już po kilku sekundach od amputacji dłoń traci swoje właściwości, co jest spowodowane głównie odpływem krwi. W niedługim czasie następuje także stężenie pośmiertne, co uniemożliwia jej prawidłowe ułożenie na skanerze.

Linie papilarne

Wbrew pozorom, **linie papilarne** nie są wynalazkiem XX wieku. Już w starożytności wykorzystywano odcisk palca na parafinowej pieczęci do identyfikacji nadawcy listu i nienaruszalności jego treści, tym niemniej rzeczywiście daktyloskopia zrobiła nieprawdopodobną furorę w wieku XX. Poczyniono badania, dzięki którym udowodniono, że linie papilarne praktycznie jednoznacznie identyfikują człowieka. Nasze palce pokryte są misterną siatką „wzgórz i dolin". Jak łatwo zauważyć, „doliny" czasami się rozdwajają, łączą lub kończą ślepym zaułkiem. To właśnie układ tych punktów (*minutii*) stanowi podstawę identyfikacji odcisków placów.

Podstawą identyfikacji daktyloskopijnej są właściwości linii papilarnych, które charakteryzuje: niezmienność, niezniszczalność (nieusuwalność), indywidualność (niepowtarzalność).

- ✔ **Niezmienność** oznacza, że wzór linii (tworzący się już w okresie płodowym) pozostaje taki sam przez całe życie człowieka – aż do gnilnego rozkładu ciała.
- ✔ **Niezniszczalność** oznacza, że rysunek ten nie ulega zniszczeniu przez całe życie człowieka. Uszkodzenie naskórka powoduje przejściowe zakłócenia wzoru i zostaje on przywrócony po zagojeniu się rany. Jedynie głębokie rany powodują trwałe zmiany w wyglądzie linii papilarnych. Powstałe wówczas blizny są dodatkowymi cechami charakterystycznymi.
- ✔ **Indywidualność** oznacza, że każdy rysunek wzoru linii papilarnych jest niepowtarzalny. Według obliczeń matematycznych, przypadek identyczności dwóch wzorów może się zdarzyć dopiero w masie 64 miliardów ludzi, a więc istnienie osób o identycznych wzorach linii papilarnych jest mało prawdopodobne, jeżeli weźmiemy pod uwagę obecne zaludnienie kuli ziemskej. Obliczenia te potwierdza codzienna praca registratur daktyloskopijnych na całym świecie. Do dnia dzisiejszego nie stwierdzono, aby u dwóch osób wystąpiły identyczne wzory.

Metoda identyfikacji bazująca na badaniu właściwości linii papilarnych, dotychczas dostępna jedynie dla wyspecjalizowanych laboratoriów, dzięki błyskawicznemu postępowi technologicznemu może już być powszechnie stosowana w domu czy biurze. Nie bez znaczenia jest też stosunkowo niewielki rozmiar skanerów linii papilarnych, co znacznie ułatwia zarówno ich instalację, jak i użytkowanie.

Wzór tęczówki oka

Tęczówka każdego oka jest absolutnie wyjątkowa. W całej populacji ludzkiej nie ma dwóch tęczówek, których szczegółowy opis matematyczny byłby identyczny, nawet w przypadku identycznych (jednojajowych) bliźniąt czy trojaczków.

W systemach biometrycznych jednym z kluczowych problemów jest zapewnienie unikatowości odpowiedniej cechy. Problemem nie jest więc np. zbadanie wymiarów dłoni, ale przeprowadzenie badań stwierdzających, jakie cechy dłoni i w jakiej kombinacji są odpowiednio unikatowe. Z prowadzonych badań płynie jeden wniosek: jednym z najbardziej unikatowych identyfikatorów jest **tęczówka oka**.

Tęczówka oka kształtuje się w ciągu dwóch pierwszych lat naszego życia i nie zmienia się aż do śmierci. Ulega zniszczeniu natomiast w bardzo krótkim czasie po śmierci, maksymalnie 5 sekund po zgonie. Co ważne: powyższe informacje dotyczą charakterystycznych (identyfikujących) cech tęczówki. Są one niezmienne (poza mechanicznym uszkodzeniem i przypadkiem raka nie zanotowano odstępstw od tej reguły), co zaś najważniejsze – punktów charakterystycznych jest aż 266. Jest to parokrotnie więcej niż punktów charakterystycznych odcisku palca. Możliwa jest więc ogromna liczba kombinacji i, przyznać trzeba, natura korzysta z tego bardzo skwapliwie. Wystarczy powiedzieć, że nawet u jednej i tej samej osoby tęczówka lewego różni się od tęczówki prawego oka.

Przed środowiskiem zewnętrznym tęczówkę chroni rogówka i ciałko szkliste. W odróżnieniu od siatkówki, tęczówka jest wyraźnie widoczna z pewnej odległości. Rejestrowanie obrazów w celu rozpoznania i zaakceptowania określonej osoby jest łatwe w realizacji i nieinwazyjne.

Żadna inna technologia biometryczna nie może równać się z matematyczną pewnością i nieinwazyjnym działaniem metody rozpoznawania tęczówki.

Proces rozpoznawania tęczówki

Przypadkowe wzory tęczówki stanowią odpowiednik skomplikowanego „ludzkiego kodu paskowego", zbudowanego z poplątanej siateczki tkanki łącznej oraz innych, widzialnych elementów. Olbrzymia różnorodność obrazów tęczówki, jej stabilność w okresie życia człowieka oraz odporność na zmiany, spowodowane wykonywaną pracą lub innymi czynnikami, to istotne zalety z punktu widzenia zautomatyzowanych pomiarów biometrycznych. Proces rozpoznawania tęczówki został opracowany przez firmę Iridian[1].

Proces rozpoznawania tęczówki rozpoczyna się od uchwycenia jej obrazu za pomocą urządzeń wideo, lokalizujących oko i tęczówkę. Następnie określone zostają granice źrenicy i zewnętrzna granica tęczówki. Następnie specjalna kamera wykonuje zdjęcie tęczówki o bardzo wysokiej rozdzielczości. Systemy radzą już sobie z przypadkowymi i celowymi ruchami głowy, mrugnięciem czy przymknięciem powieki. Nie stanowią problemu okulary czy szkła kontaktowe. Następnie system ze zrobionego zdjęcia przygotowuje kod, zawierający skrócony opis punktów charakterystycznych.

W systemach zaawansowanych taki kod jest następnie szyfrowany (z zastosowaniem szyfrów jednokierunkowych) i porównywany z zaszyfrowanym kodem oryginału – zapisanym w bazie danych. W tego typu systemach nawet po wykradzeniu zaszyfrowanego kodu nie jest możliwe odtworzenie na jego podstawie zarysu tęczówki. Istniejące rozwiązania zapewniają poziom błędów rzędu 10^{-10} a nawet 10^{-20}. Nic więc dziwnego, że tego typu systemy zdobywają rosnącą popularność w szczególnie wymagających instalacjach.

Wzór tęczówki jest przetwarzany i zakodowany w postaci rekordu IrisCode™, który jest następnie przechowywany i używany do rozpoznawania przy każdej transakcji, podczas której żywa tęczówka jest przedstawiana do porównania.

Identyfikacja trwa zwykle około dwóch sekund.

Ważnym wyróżnikiem technologii rozpoznawania tęczówki jest możliwość pełnego przeszukania bazy danych, bez żadnych ograniczeń liczby zawartych w niej rekordów IrisCode™.

Najlepsza metoda identyfikacji

Matematyczno-naukowe podstawy procesu rozpoznawania tęczówki IriScan w jasny sposób dowodzą, że jest to najlepsza technika biometryczna. Obiektywne testy, przeprowadzone przez instytucje rządowe i przedsiębiorstwa, potwierdziły, że tak niskiej stopy błędów nie udaje się osiągnąć w żadnej innej metodzie biometrycznej. Rozpoznawanie tęczówki zapewnia poziom pewności statystycznej o wiele rzędów wielkości wyższy od możliwości innych metod biometrycznych.

Porównując rozpoznawanie tęczówki z innymi metodami biometrycznymi, warto zadać kilka trudnych pytań:

- ✔ Czy określona technika wykorzystuje naprawdę unikatowe cechy ciała ludzkiego i jaka jest naukowa podstawa twierdzenia o wyjątkowości tych cech?
- ✔ Jaka jest statystyczna podstawa niepowtarzalności (charakterystyki biometrycznej) w obrębie populacji?
- ✔ Ile niezależnych zmiennych (stopni swobody) jest mierzonych przy zastosowaniu danej techniki?
- ✔ Jaka jest stopa błędów krzyżowych i czy została obliczona w sposób obiektywny?
- ✔ Ile wynosi współczynnik rozstrzygalności d-prim (d')?
- ✔ Czy technika umożliwia wyczerpujące przeszukanie w czasie rzeczywistym bazy danych o dowolnych rozmiarach?
- ✔ Czy uzyskany kod może być wykorzystany do współpracy z różnymi bazami danych, a nawet z różnymi produktami do rozpoznawania tożsamości?

Najważniejsze cechy identyfikatora biometrycznego

Najważniejsze cechy każdego identyfikatora biometrycznego to:

- ✔ poziom niezależnego zróżnicowania wybranego wskaźnika w całej populacji ludzkiej, ponieważ od niego zależy wyjątkowość identyfikatora (na przykład tęczówki);
- ✔ niezmienność identyfikatora w czasie i odporność na wpływy zewnętrzne;
- ✔ możliwości komputeryzacji procesów wydajnego kodowania i niezawodnego rozpoznawania wzorca identyfikującego.

We wszystkich tych kryteriach żaden inny identyfikator biometryczny nie dorównuje tęczówce.

Kolejne cechy zwiększające przydatność tęczówki do automatycznej identyfikacji osób to:

- ✔ jej naturalne odseparowanie od środowiska zewnętrznego i zabezpieczenie przed jego wpływami, wynikające z faktu, że jest to wewnętrzny organ oka. Przy tym możliwe jest zapisanie i zakodowanie jego obrazu przy użyciu kamery wideo umieszczonej w odpowiedniej odległości;
- ✔ jej fizjologiczna reakcja na światło i naturalne ruchy źrenic, uniemożliwiające zastąpienie żywej tkanki fotografią lub jakimś innym odwzorowaniem;
- ✔ ograniczona zależność od kodu genetycznego osoby, zapewniająca, że nawet identyczne (jednojajowe) bliźniaki i trojaczki mają wzory tęczówek tak samo różne pod względem szczegółów matematycznych, jak osoby niespokrewnione.

Przykłady rozwiązań

Ze względu na różnorodność oferty tego typu urządzeń na rynku światowym, wybrałem tylko kilka przykładów oferowanych czytników.

Linie papilarne

W przypadku kontroli dostępu weryfikacja musi się odbywać bardzo szybko i z dużą dokładnością. Służą do tego specjalne czytniki **linii papilarnych**. Urządzenia takie wyposażone są w okienko, do którego należy przyłożyć opuszkę palca. System sprawdza nasze linie papilarne, bada układ punktów charakterystycznych i innych cech identyfikujących, wreszcie porównuje te dane z zapamiętanym wzorcem. Stosowane mogą tu być dwa rozwiązania: albo identyfikacja jest dokonywana w samym czytniku (jest to wtedy urządzenie dość złożone), albo w połączonym z nim komputerze PC. W tym drugim przypadku czytnik jest tak naprawdę wysokiej jakości „skanerem" i nie musi być wyposażony w szczególnie skomplikowane oprogramowanie. Właśnie to umożliwiło zdecydowane obniżenie cen na te urządzenia.

Możliwości weryfikacyjne urządzenia opierają się na możliwościach oprogramowania umieszczonego w komputerze. Jedną z metod sprawdzenia linii papilarnych jest stworzenie obrazu palca przy pomocy czujnika pojemnościowego. Czujnik ten rejestruje różnice w pojemności naszej skóry w danym punkcie. Dzięki temu zarys naszych linii papilarnych pochodzi de facto z głębi skóry. To z kolei oznacza niewrażliwość na proste uszkodzenia opuszki palca.

Skoro w tego typu urządzeniach punkt ciężkości został przeniesiony na komputer PC, to ważna staje się jakość tego oprogramowania. Na całe szczęście, do podanych urządzeń dostępne są wysokiej klasy gotowe rozwiązania zapewniające najbardziej rygorystyczne poziomy autoryzacji. Co więcej, dostępne są też specjalne pakiety programistyczne pozwalające na samodzielne tworzenie złożonych rozwiązań przy zastosowaniu opisanych urządzeń.

Identix BioTouch PCMCIA

Czytnik odcisków palców BioTouch PC Card jest przełomem w dziedzinie bezpieczeństwa i wygody użytkowników komputerów przenośnych. Czytnik ten wykonano w formie karty PC-Card Type II, da się go więc zastosować w niemal dowolnym notebooku. Wystarczy nacisnąć bok karty, a wysunie się specjalna podkładka z polem odczytu. Całość skonstruowana jest z wielką dbałością o ergonomię i łatwość używania. Czytnik BioTouch dostarczany jest wraz z oprogramowaniem Biologon Client for Windows, które umożliwia kontrolę dostępu do systemu operacyjnego.

Jeśli istnieje potrzeba zabezpieczenia całej sieci, oprogramowanie Biologon może być w bardzo łatwy sposób skonfigurowane w celu logowania do dowolnej domeny Windows NT przy pomocy serwera Biologon for Windows (dostępnego osobno) – w takim przypadku wzorce odcisków palców mogą być przechowywane centralnie. Oprogramowanie Biologon zastępuje klasyczne okienko logowania się do systemu MS Windows. Dzięki temu logowanie zostaje uproszczone do granic możliwości – wystarczy przytknąć palec do pola odczytu. Nawet naciśnięcie klawisza ENTER nie jest potrzebne.

Specyfikacja techniczna

Sprzęt: karta Type II PCMCIA; certyfikaty FCC/B/CE. Czytnik biometryczny: czytnik optyczny Identix DFR-300 Fingerprint Reader.

Wymagania:

- ✔ Pentium 100 MHz lub szybszy;
- ✔ minimum 32 MB RAM;
- ✔ 10 MB wolnego miejsca na dysku twardym;
- ✔ wolny slot Type II PC Card (PCMCIA);
- ✔ system operacyjny: Microsoft Windows 95/98/NT/2000/ME/XP.

Proste działanie: umieść PC Card w slocie, wysuń czytnik linii papilarnych, umieść palec na czytniku.

Identix BioTouch USB

BioTouch USB to optyczny czytnik liniii papilarnych chroniący dostęp zarówno do pojedynczych komputerów jak i całych sieci. Jest autonomicznym urządzeniem typu plug-and-play wyposażonym w interfejs USB. Ochrona dostępu do komputera za pomocą linii papilarnych jest niewątpliwie niezwykle pewnym i wygodnym sposobem zabezpieczenia danych firmy. Klasyczne hasła mogą być przecież zapomniane, podejrzane przez niepowołane osoby, itd.

Wykorzystanie zaawansowanej technologii CMOS firmy Motorola gwarantuje wysoką dokładność odczytu. Urządzenie posiada zintegrowany system kontroli reagujący na takie czynniki, jak: ułożenie palca, jakość odcisku palca, siła nacisku, itp. System ten zdecydowanie poprawia jakość odczytu, a co za tym idzie, umożliwia jeszcze bardziej precyzyjną weryfikację tożsamości. Czytnik przechwytuje i zapamiętuje rozkład minutii palca. Większość obrazu odcisku palca użytkownika jest usuwana, co redukuje ryzyko wykorzystania przechowywanych danych w celu podrobienia odcisku palca. Co więcej – dane przechowywane są w znacznie mniejszej objętości, to zaś umożliwia przyspieszenie procesu weryfikacji tożsamości.

Specyfikacja techniczna

Wymiary: 96 mm x 31 mm x 60 mm (dł. x wys. x szer.).

Waga: 150 gramów.

Czytnik biometryczny:

- ✔ czytnik optyczny DFR-200;
- ✔ powierzchnia odczytu 17x17 mm;
- ✔ rozdzielczość pozioma 530dpi;
- ✔ rozdzielczość pionowa 380dpi;
- ✔ czytnik CMOS;
- ✔ odczyt odcisku palca w zakresie 360 stopni.

Interfejs: USB i kabel 1,8 m.

Zasilanie: napięcie stałe 4,4-5,25V z portu USB; pobór prądu w stanie czuwania 8 mA.

Inne: temperatura pracy od 0 do +55 stopni; certyfikaty FCC/CE/VCCI/Ctick.

Oprogramowanie: Biologon for Windows Desktop Client/Server.

System operacyjny:
Microsoft Windows 95/98/NT/2K/ME/XP.

IMM Skan 200

IMMSkan 200 jest przeznaczony do zastosowań w systemach kontroli dostępu i w systemach rejestracji czasu pracy. Terminal może pracować autonomicznie lub z komputerem poprzez kanał komunikacyjny RS-485 lub RS-232.

Cechy charakterystyczne to:

- ✔ niepodważalna weryfikacja na podstawie linii papilarnych;
- ✔ odporność na fałszerstwa;
- ✔ eliminacja kart, żetonów, tajnych haseł;
- ✔ zapewnienie prywatności; zapamiętany wzorzec linii papilarnych nie może być wykorzystany do innych celów;
- ✔ prosta i szybka obsługa;
- ✔ bezpośrednie sterowanie ryglem i linią alarmową;
- ✔ możliwość pracy autonomicznej lub z komputerem;
- ✔ wyrób polski z głowicą sensorową linii papilarnych.

Urządzenie jest pierwszym krajowym biometrycznym terminalem linii papilarnych z głowicą sensorową, zapewniającym wiarygodną weryfikację użytkowników.

Terminal ma szeroko rozbudowane możliwości funkcjonalne. Umożliwia rejestrację wzorców linii papilarnych użytkowników, weryfikację osób, rejestrację zdarzeń w ruchu osób wchodzących i wychodzących, nadawanie i cofanie uprawnień poszczególnym użytkownikom, zmianę parametrów konfiguracyjnych. Porównuje wprowadzony obraz linii papilarnych z przechowywanym wzorcem. Po pozytywnej weryfikacji terminal zapisuje zdarzenie do pamięci i w systemach kontroli dostępu wysyła sygnał do rygla, odblokowującego zamek drzwi. Rozpoznawanie użytkowników odbywa się w terminalu, co znacznie obniża czas oczekiwania na weryfikację i otwarcie drzwi oraz uniezależnia terminal od awarii lokalnej sieci.

IMMSkan 200 zapewnia najwyższy stopień bezpiecznego rozpoznawania, wykorzystując wprowadzony kod osobisty, numer karty zbliżeniowej i obraz linii papilarnych, dzięki wyposażeniu terminalu:

- ✔ w sensorową głowicę linii papilarnych, będącą najnowszym osiągnięciem technologii światowej;
- ✔ w głowicę kart zbliżeniowych;
- ✔ w klawiaturę, umożliwiającą wprowadzanie kodu osobistego.

Oprogramowanie

Terminal IMMSkan 200 pracuje pod kontrolą opracowanego w Instytucie Maszyn Matematycznych oprogramowania XChronos realizującego funkcje kontroli dostępu i rejestracji czasu pracy.

Współpraca

Terminal współpracuje z systemami firm: Andover Controls, CERBERUS, COTAG, Honeywell, JOHNSON CONTROLS i innymi z wykorzystaniem interfejsu typu Wiegand.

Wykonanie

Terminal jest dostępny w wersji zintegrowanej oraz modułowej.

Rozpoznawanie geometrii dłoni

Niestety, identyfikacja za pomocą linii papilarnych ma swoje wady: głębsze uszkodzenia powierzchni skóry mogą mieć wpływ na odczyt, a więc i na identyfikację danej osoby. Biorąc to pod uwagę warto rozważyć identyfikację przy pomocy geometrii dłoni. Przykładem takiego urządzenia jest HandKey II. Czytnik ten wykonuje trójwymiarowe zdjęcie naszej dłoni, rejestrując długość, szerokość, grubość czterech palców oraz wielkość obszarów pomiędzy kostkami. Łącznie wykonywanych jest ponad 90 pomiarów różnych cech charakterystycznych dłoni. Wynik tych pomiarów jest przechowywany w pamięci urządzenia w formie (maksimum) 9-bajtowego wzorca.

Identyfikator ten jest praktycznie unikatowy dla każdego człowieka. Specjalny system kontrolujący ułożenie dłoni zapewnia, że wykonany wzorzec będzie dokładnie pasował do zaprezentowanej dłoni. A jak wygląda sam proces autoryzacji? Wystarczy podejść do urządzenia i na jego klawiaturze podać swój numer. Dzięki temu urządzenie wie, z jakim wzorcem porównywać naszą dłoń. Potem wystarczy umieścić dłoń na charakterystycznej tabliczce w dolnej części urządzenia. To wszystko! Na wyświetlaczu pojawi się odpowiedni komunikat o dopuszczeniu lub odrzuceniu próby dostępu. Samo urządzenie może też wysłać sygnał otwierający bramę czy zezwalający programowi na pokazanie odpowiednich informacji.

Jak widać, HandKey II jest reprezentantem urządzeń „inteligentnych", bo wyposażonych w pamięć wzorców, a co za tym idzie, w możliwość autoryzacji osób. W bardziej złożonych instalacjach urządzenia takie można łączyć w całe sieci – wspólnie zarządzane i administrowane. Co więcej, tego typu urządzenia (skoro autoryzacja jest dokonywana „wewnątrz") można tak skonfigurować, by „udawały" np. czytnik kodów kreskowych czy czytnik kart magnetycznych. W efekcie nic nie trzeba zmieniać w istniejącym oprogramowaniu zabezpieczającym dostęp. Wyobraźmy sobie kontrolę dostępu do pewnego pomieszczenia bankowego. Do tej pory otwarcie drzwi było wyzwalane odczytaniem odpowiedniej karty magnetycznej w czytniku połączonym z zamkiem. Dodatkowo czytnik przesyłał numer karty oraz go-

dzinę wejścia do pomieszczenia do komputera klasy PC.

Na komputerze tym działał specjalizowany system odczytujący te dane i pozwalający na ich odpowiednie raportowanie. Otóż w takiej sytuacji wystarczy czytnik kart magnetycznych zamienić na „inteligentne" urządzenie biometryczne. Nie trzeba wymieniać oprogramowania na komputerze! Oprogramowanie to będzie przekonane, że cały czas ma do czynienia z czytnikiem kart magnetycznych. Dzięki systemom geometrii dłoni nie musimy się martwić nawet bardzo głębokim skaleczeniem naszego palca. Warto przy tym podkreślić, że tego typu rozwiązania w realnych instalacjach można dodatkowo wzbogacać o odczyt linii papilarnych.

HandKey II

Czytnik geometrii dłoni HandKey II firmy Recognition Systems Inc. bazując na sprawdzonej technologii rejestruje i weryfikuje kształt dłoni w czasie krótszym od 1 sekundy.

Konstrukcja i zasada działania

Konstrukcja HandKey II zapewnia najwyższy stopień niezawodności. Każde urządzenie stanowi kompletny system kontroli dostępu zawierający sterownik rygla, obsługę wyjścia i monitorowanie alarmu. Wszystkie informacje włącznie z danymi oraz modułem decyzyjnym znajdują się wewnątrz urządzenia. Zabezpiecza to system przed problemami z siecią komputerową i zapewnia nieprzerwane działanie i bezpieczeństwo, nawet gdy połączenie z głównym komputerem sterującym zostanie przerwane. Po umieszczeniu dłoni w komorze urządzenia mierzony jest jej rozmiar i kształt: długość, szerokość i grubość czterech palców oraz obszar pomiędzy kostkami (kciuk nie jest wykorzystywany).

Wynikiem pomiaru jest trójwymiarowy obraz kształtu dłoni, który zamieniany jest na 9-bajtowy wzorzec, zapisywany łącznie z kodem ID osoby badanej. Proces weryfikacji polega na wprowadzeniu kodu ID i porównaniu przypisanego doń wzorca z aktualnie badaną dłonią. Jeśli wynik jest pozytywny, tzn. osoba badana jest osobą uprawnioną, efektem będzie np. otwarcie drzwi. Do zarządzania i kontroli nad czytnikami HandKey II służy oprogramowanie HandNet for Windows umożliwiające współpracę czytników w sieci.

Cechy HandKey II

- ✔ obsługa i monitorowanie drzwi;
- ✔ wejście dla czytników kart magnetycznych;
- ✔ obsługa wyjścia;
- ✔ wyłącznik alarmowy, pamięć dla 512 użytkowników (z możliwością rozbudowy do 32512);
- ✔ wyjście drukarkowe RS-232;
- ✔ praca jednostanowiskowa lub w sieci;
- ✔ emulacja czytników kart;
- ✔ zintegrowana budowa;
- ✔ 62 definiowalne strefy czasowe;
- ✔ dostępna wersja zewnętrzna odporna na warunki atmosferyczne;
- ✔ bogaty wybór opcji komunikacyjnych (modem, sieć Ethernet).

Dane techniczne

- ✔ czas weryfikacji: poniżej 1 sekundy;
- ✔ zasilanie: 12-24 V DC;
- ✔ podtrzymanie pamięci: do 5 lat przy standardowej baterii litowej;
- ✔ długość kodu PIN: od 1 do 10 cyfr z klawiatury lub czytnika kart;
- ✔ pamięć zdarzeń: 5187 zdarzeń;
- ✔ komunikacja: RS-485 (4 wire and 2 wire), RS-232 Serial Printer Support, sieć lokalna;
- ✔ wejścia: Proximity, Wiegant, czytniki kart magnetycznych lub kodów kreskowych;
- ✔ kontrola drzwi: wyjście zasilania rygla, monitorowanie: czujnik otwarcia pokrywy i otwarcia drzwi, 2 wejścia dodatkowe, 3 wyjścia dodatkowe, Request for Exit;
- ✔ pojemność pamięci: 512 użytkowników, rozszerzana do 32512;
- ✔ kod alarmowy: jednocyfrowy, definiowany przez użytkownika;
- ✔ strefy czasowe: 62 strefy, nielimitowane definiowanie dni wolnych;
- ✔ wymiary: 21,7 cm dł. x 22,3 cm szer. x 29,6 cm wys.;
- ✔ masa: 2,7 kg.

Wzór tęczówki oka

Prywatność danych osobistych w dzisiejszym skomplikowanym społeczeństwie jest iluzoryczna. Gdy jedyną metodą identyfikacji i ochrony są hasła, numery identyfikacyjne lub numery statystyczne obywateli, każdy jest narażony na naruszenie poufności swoich danych osobistych lub bezpieczeństwa. Tradycyjne metody identyfikacji nie zapewniają wysokiego poziomu zabezpieczenia przed dostępem osób niepowołanych i każdy może skorzystać z tych informacji w celu symulowania tożsamości innej osoby.

Za pomocą wykorzystania takiej fałszywej tożsamości możliwe jest uzyskanie dostępu do ważnych informacji osobistych i firmowych, a nawet dokonanie przestępstwa. Rozpoznawanie tęczówki pozwala na praktyczne wyeliminowanie przypadków oszustw podczas uwierzytelniania oraz podszywania się pod czyjąś tożsamość, a także umożliwia bezpieczne kontrolowanie dostępu do rejonów, materiałów lub danych, dozwolonego wyłącznie dla określonych, upoważnionych osób. Oprócz ochrony prywatności, rozpoznawanie tęczówki

może być wykorzystane do niezliczonych innych zastosowań, zapewniając ochronę i bezpieczeństwo.

Handel elektroniczny
– transakcje online
– zaopatrzenie przedsiębiorstw

Dla skutecznego wykorzystania potencjału handlu elektronicznego konieczne jest stosowanie niezwykle solidnych i niezawodnych zabezpieczeń. Krytyczne znaczenie ma absolutnie pewna identyfikacja osób po obu stronach transakcji zawieranej za pośrednictwem sieci komputerowej. Dla maksymalnego bezpieczeństwa technologia szyfrowania danych musi być uzupełniona o proces identyfikacji, taki jak rozpoznawanie tęczówki, pozwalający na bezpośrednie powiązanie transakcji z osobą upoważnioną, a nie elektronicznym identyfikatorem lub hasłem, do którego dostęp mogą uzyskać inne osoby.

Dane medyczne oraz inne informacje osobiste

Oznaczenie dokumentacji medycznej lub innych ważnych informacji osobistych nazwiskiem osoby, jej numerem lub kodem identyfikacyjnym nie zapewnia bezpieczeństwa, ani dokładności danych przy dostarczaniu lekarstw. Informacje stanowiące własność przedsiębiorstwa lub dane osobiste mogą zostać zapieczętowane przy użyciu zapisu IrisCode™, zapewniając, że tożsamość pacjenta lub dawcy pozostaje utajona. Jedynie uprawniony „właściciel" danych lub wyników może uzyskać do nich dostęp lub upoważnić do tego innego użytkownika, co zapewnia ochronę poufności i zabezpieczenie danych osobistych.

Identyfikacja dla celów bezpieczeństwa
– kontrola dostępu
– weryfikacja tożsamości

Stopień bezpieczeństwa budynków przedsiębiorstw, skarbców, rejonów z ograniczonym dostępem oraz ich zawartości zależy od dokładności i niezawodności systemów kontroli dostępu. Numery PIN, kody, hasła, plakietki identyfikacyjne, klucze oraz inne identyfikatory mogą łatwo zostać sfałszowane, podrobione lub przejęte w nielegalny sposób. Żaden z tych podatnych na sfałszowanie identyfikatorów nie może zagwarantować ani potwierdzić z absolutną pewnością tożsamości osoby, która je przedstawia. Rozpoznawanie tęczówki daje absolutną pewność, że osoba uzyskująca dostęp do ważnych środków, materiałów lub rejonów jest właśnie tą osobą, która ma prawo do takiego dostępu.

Ochrona sieci komputerowych
– kontrola tożsamości użytkowników
– bezpieczeństwo komputerów

Rozpoznawanie tęczówki zwiększa bezpieczeństwo komputerów i sieci komputerowych oraz przechowywanych, udostępnianych i przetwarzanych danych, poprzez pewną identyfikację uprawnionego użytkownika, a nie hasła, którego można łatwo się nauczyć lub zapisać je w formie elektronicznej. Dzięki rozpoznawaniu tęczówki osoby zagrażające systemom komputerowym oraz intruzi, tacy jak „hakerzy", napotykają potężną barierę chroniącą dostęp do ważnych baz danych.

Bankomaty
– handel detaliczny
– podróże i zakup biletów

Technologia rozpoznawania tęczówki zapewnia znaczne korzyści i udogodnienia w transporcie publicznym i imprezach masowych. Pasażerowie i osoby dojeżdżające do pracy mogą uniknąć niedogodności związanych z zakupem biletów, dokumentów uprawniających do przejazdu i koniecznością posiadania drobnych sum w bilonie. Wydawanie biletów w oparciu o rozpoznawanie tęczówki dałoby wygodę użytkownikom oraz usprawnienie księgowości, przepływu środków pieniężnych i redukcję kosztów firmom świadczącym usługi transportowe.

Egzekwowanie prawa
– wojsko
– instytucje administracji państwowej

Stacjonarne oraz mobilne platformy rozpoznawania tęczówki przyspieszają lokalną identyfikację i rejestrację, przetwarzanie danych osób przybywających z zagranicy oraz kontrolę tożsamości pracowników. Systemy tego typu umożliwiają pewną identyfikację pracowników, osób odwiedzających oraz przebywających w zakładach karnych, mogą uprościć kontrolę administracyjną w instytucjach administracji państwowej oraz zapewniają automatyczną i natychmiastową weryfikację tożsamości w każdym środowisku pracy, w którym konieczne jest efektywne połączenie wysokiego stopnia kontroli oraz wygody użytkowania systemu.

Emerytury,
renty, świadczenia socjalne,
świadczenie usług

Najważniejszą zaletą technologii rozpoznawania tęczówki jest zdolność do realizacji w czasie rzeczywistym lub w trybie offline wyczerpujących wyszukiwań w bazach danych zawierających rekordy IrisCode™ o prawie nieograniczonych rozmiarach. Ta możliwość ma szczególne znaczenie dla obsługi dużych programów dotyczących uprawnień do świadczeń lub usług,

w otoczeniu zapewniającym ochronę przed oszustwem. Wielokrotne rejestracje pod fałszywymi numerami identyfikacyjnymi zostają praktycznie wyeliminowane dzięki zastosowaniu systemu, który nie powoduje jednocześnie stygmatyzacji osób z przeszłością kryminalną i nie jest podatny na nadużycia dla celów politycznych, tak jak inne procedury identyfikacji.

Kamery fotografujące dwoje oczu

Oki IrisPass WG

Panasonic BM-ET 300

Zastosowania:
- ✔ dostęp do budynków;
- ✔ praca służb imigracyjnych/zabezpieczenia lotnisk;
- ✔ centra informacyjne;
- ✔ zakłady i elektrownie;
- ✔ przyjęcia i zwolnienia więźniów w zakładach karnych;
- ✔ kontrola czasu pracy i obecności pracowników.

Cechy charakterystyczne:
- ✔ kamera dwuoczna;
- ✔ Auto Focus, regulacja rozciągania i nachylenia obrazu;
- ✔ polecenia głosowe;
- ✔ zasięg 45-75 cm;
- ✔ minimalny zakres współpracy ze strony użytkownika.

Kontrola dostępu do komputera

Kamery fotografujące jedno oko Oki IrisPass-h

Zastosowania:
- ✔ logowanie do sieci lokalnej;
- ✔ logowanie do domeny;
- ✔ dostęp jednorazowy;
- ✔ zarządzanie siecią lokalną;
- ✔ zabezpieczenia komputerów osobistych SAFLink SAF2000T.

Cechy charakterystyczne:
- ✔ dioda czerwona i zielona;
- ✔ zasięg od 3 do 10 cm.

Panasonic BM-100/120

Zastosowania:
- ✔ logowanie do sieci lokalnej;
- ✔ logowanie do domeny;
- ✔ dostęp jednorazowy;
- ✔ zarządzanie siecią lokalną;
- ✔ zabezpieczenia komputerów osobistych.

Cechy charakterystyczne:
- ✔ oprogramowanie IO Software SecureSuiteT;
- ✔ dioda czerwona i zielona;
- ✔ zasięg 40-60 cm;
- ✔ niewielki rozmiar.

Opracował Grzegorz Kantowicz
na podstawie materiałów firm
AutoID Polska, Iridian Technologies, OKI oraz Panasonic

Przypisy

[1] Firma Iridian jest wyłącznym właścicielem i twórcą innowacyjnej techniki identyfikacji biometrycznej, opartej na rozpoznawaniu niepowtarzalnych wzorów widocznych na tęczówce ludzkiego oka – kolorowym pierścieniu otaczającym źrenicę. Proces rozpoznawania tęczówki został przez firmę opatentowany na całym świecie. Założona w 1990 r. (jako Delaware Corporation) firma IriScan rozpoczęła działalność w 1993 r., teraz występuje pod marką IRIDIAN stosując swoją unikatową technologię w produktach komercyjnych, przeznaczonych początkowo do kontroli dostępu, zastosowań penitencjarnych oraz identyfikacji osób dla celów bezpieczeństwa.

Bezpieczniej już nie będzie

Większość producentów rozwiązań antywirusowych od dawna przestała się ograniczać tylko do ochrony komputerów przed wirusami, robakami i koniami trojańskimi. Dlatego zamiast „systemy antywirusowe" powinniśmy zacząć korzystać z określenia „systemy antimalware". Słowo „malware" pochodzi od angielskiego „malicious software" (złośliwe programy). Pod tą nazwą kryją się programy działające na szkodę użytkownika, komputera lub sieci komputerowej.

Na co więc powinien zwrócić uwagę użytkownik oraz w jaki system wyposażyć swój PC, aby ochronić się przed coraz nowszymi formami zagrożeń?

Hakerzy i twórcy wirusów wymyślają coraz to nowsze, trudniejsze do wykrycia sposoby, aby wykraść poufne dane użytkownikom i osiągnąć korzyści finansowe. Każdego dnia pojawiają się nowe zagrożenia, które są w stanie nawet w ciągu kilku godzin zainfekować tysiące komputerów na całym świecie.

Dużą rolę odgrywają programy szpiegujące (*spyware*), narzędzia hakerskie, kreatory wirusów, dialery, fałszywe alarmy wirusowe, rozsyłane za pomocą poczty elektronicznej i komunikatorów (*hoaxy*) czy programy symulujące infekcje (*jokes*). Dość groźnym ostatnio zjawiskiem jest phishing, który polega m.in. na fałszowaniu wiadomości e-mail, które przekierowują na strony www do złudzenia przypominające oryginalne witryny banków czy instytucji finansowych. Phishing wykorzystuje również luki w programach, takich jak Outlook Express czy Internet Explorer. Inny rodzaj zagrożeń stwarzają luki bezpieczeństwa (*vulnerability*). Są to cechy systemu informatycznego, które często wykorzystują twórcy wirusów, żeby przejąć kontrolę nad komputerem. Luki systemowe można podzielić na: wynikające z błędnego lub niedopracowanego kodu oprogramowania, np. systemu operacyjnego, luki wprowadzone do systemu przez administratora poprzez błędną konfigurację zabezpieczeń oraz luki wprowadzane przez użytkowników stacji roboczych, np. wyłączenie ochrony permanentnej w oprogramowaniu antywirusowym.

Wraz ze wzrostem liczby zagrożeń rośnie też liczba dostępnych rozwiązań programowych i sprzętowych zabezpieczających nasze komputery przed zagrożeniami.

Biorąc pod uwagę to, że każdego dnia jesteśmy narażeni na niebezpieczeństwo ze strony nowych złośliwych kodów, powinniśmy korzystać z innowacyjnych systemów bezpieczeństwa, które ochronią nas nawet przed nieznanymi jeszcze zagrożeniami. Pamiętajmy, że stale zwiększa się nie tylko liczba wirusów, ale również poziom ich technologicznego zaawansowania. Proste, typowe systemy zabezpieczeń, niestety, nie mają już racji bytu. Niezaktualizowane w odpowiednim czasie nie potrafią zidentyfikować najnowszych wirusów, gdyż nie posiadają ich sygnatur.

Zanim powstanie szczepionka, wirus może rozprzestrzenić się na dużą skalę. Na rynku pojawiły się już technologie, które blokują wirusy nieznanego rodzaju, nawet gdy oprogramowanie nie zostanie jeszcze zaktualizowane. Zabezpieczają również przed próbami włamań oraz wirusami sieciowymi, stanowiąc drugą warstwę zabezpieczenia i uzupełniając system antywirusowy. Jest to dobry sposób na przewidywanie zagrożenia, czyli działanie prewencyjne. Cały proces jest w pełni zoptymalizowany. Najpierw oprogramowanie antywirusowe filtruje znane zagrożenia, a następnie skupia się na pozostałych, nieznanych wirusach, analizując, czy je zablokować. Jako przykład można tu wymienić technologię TruPrevent zaimplementowane w produktach Panda Software. Okazuje się, że cały proces jest w pełni skuteczny i nie powoduje fałszywych alarmów. Identyfikowane są tylko te złośliwe kody, które stanowią potencjalne zagrożenie w zabezpieczonym komputerze. Dzięki zastosowaniu ochrony plików i procesów systemy takie same potrafią się obronić przed próbą zaburzenia ciągłości ochrony. Sieć komputerowa nie pozostaje wtedy bez ochrony nawet na sekundę.

Technologie TruPrevent potrafią przeanalizować zachowanie nieznanego zagrożenia, sprawdzając, czy nie podejmuje żadnych niebezpiecznych działań w systemie.

Połączenie tradycyjnego systemu antywirusowego z mechanizmem do walki z nierozpoznanym, najnowszym i najbardziej niebezpiecznym kodem stało się nowym wyznacznikiem jakości bezpieczeństwa systemów komputerowych.

Bardzo istotnym elementem w systemach antywirusowych jest korzystanie z aktualnej wersji oprogramowania. Użytkownicy mniej zaawansowanych rozwiązań muszą sami zadbać o to, aby regularnie pobierać nowe wersje i aktualizować bazy sygnatur wirusów minimum raz dziennie. Uaktualnienie takie udostępniane jest użytkownikom danego programu zaraz po pojawieniu się nowych szczepionek. Lepszym, wygodniejszym i bezpieczniejszym rozwiązaniem są aktualizacje automatyczne – użytkownik nie musi ingerować w pracę danej aplikacji.

Program antywirusowy musi wykrywać nie tylko różnego rodzaju wirusy, ale również zabezpieczać komputer przed włamaniami. Firewall jest podstawowym elementem, w który powinien być wyposażony system. Często pomocne okazuje się również zabezpieczenie połączeń

bezprzewodowych Wi-Fi, z których korzysta coraz większe grono użytkowników. Istotna jest również funkcja do walki z programami szpiegującymi i phishingiem, w celu ochrony poufnych danych. Niektóre programy zapewniają mechanizm informowania o wynikach autodiagnozy oraz informują o zagrożeniu wirusowym obecnym na całym świecie. Powyższe podstawowe wymagania dotyczą pojedynczego użytkownika. Kwestia systemu antywirusowego w przypadku sieci komputerowych wymaga szerszego wyjaśnienia.

Dobrym zabezpieczeniem sieci, niezależnie od ich wielkości, jest stosowanie warstwowej strategii ochrony. Jak wiadomo, głównym źródłem zagrożenia jest internet, a nie dyskietki i płyty CD, jak miało to miejsce jeszcze nie tak dawno. Dlatego warto zabezpieczyć sieć lokalną już na styku z internetem, tak aby zagrożenia typu *malware* przedostające się z internetu były od razu blokowane. Stosowanie strategii warstwowej zwiększa efektywność ochrony antywirusowej, dlatego warto inwestować w tego typu rozwiązania. Ochrona *antimalware* może być zastosowana w trzech różnych warstwach: na każdej stacji roboczej (ochrona komputera, na którym instaluje się oprogramowanie antywirusowe), na serwerze (ochrona serwera plików lub poczty w wewnętrznej sieci korporacyjnej) oraz w miejscu połączenia sieci lokalnej z internetem (ochrona strefy brzegowej, gdzie *malware* jest rozpoznawany przy wejściu). Trzecią warstwę najczęściej stanowią rozwiązania sprzętowe, które z bardzo dużą przepustowością skanują cały ruch przychodzący i wychodzący. Rozwiązaniem takim zazwyczaj zarządza się zdalnie z konsoli administracyjnej, z którą administrator łączy się poprzez szyfrowane połączenie HTTPS. Często urządzenia takie są wyposażone w dodatkowe moduły ochrony, w zależności od potrzeb firmy. Podstawową funkcję pełni moduł *antimalware*, w którym dostęp do konsoli musi być szybki, łatwy, ale przede wszystkim bezpieczny. Sama konsola powinna być prosta w użyciu, intuicyjna tak, aby nawet mniej zaawansowany administrator potrafił skonfigurować odpowiednio urządzenie, nie pozostawiając luk w zabezpieczeniach, które haker mógłby wykorzystać do przeprowadzenia ataku. Ważną rzeczą jest także śledzenie i obserwacja tego, co dzieje się w sieci. Dlatego tak istotna jest funkcja umożliwiająca przeglądanie raportów o zdarzeniach (np. wykrycie wirusa) w czasie rzeczywistym. Administrator może sprawdzić, który z komputerów w sieci próbuje, przykładowo, ściągnąć zainfekowany plik, jakich rodzajów zagrożeń jest najwięcej itp. Moduł *antimalware* powinien charakteryzować się dużą skutecznością, łatwością w konfiguracji, ale również dużą szybkością działania (np. urządzenie *Panda GateDefender* firmy Panda Software potrafi obsłużyć ruch od 5 Mbps do 30 Mbps).

Spam obniża wydajność przedsiębiorstwa

Oprócz opisywanego modułu *antimalware*, który jest odpowiedzialny za ochronę przed wszelkimi zagrożeniami z internetu, istotne są również funkcja antyspamowa oraz filtry stron internetowych (*Web Filter)*. Według statystyk Panda Software w ciągu jednego dnia wysyłanych jest 31 miliardów wiadomości e-mail, z czego 40 proc. uznawane jest za spam, czyli w ciągu jednego dnia wysyła się 12,4 miliarda niechcianych wiadomości. Średnio jedna osoba w ciągu jednego roku otrzymuje 2200 wiadomości-śmieci. Czas potrzebny do usunięcia jednej niechcianej wiadomości wynosi około 4-5 sekund[1]. Prosta kalkulacja pokazuje, że na samo usuwanie niechcianych e-maili tracimy średnio 3 godziny w roku. Na tym jednak nie koniec. Niepożądanymi skutkami obecności spamu są także koszt zajmowanego przez nie miejsca na serwerze oraz czasu procesora potrzebnego na ich obsługę, zmarnotrawiona na ich przesyłanie przepustowość łącza internetowego itd. Dlatego tak ważny jest dobry filtr antyspamowy, który sam usunie niechciane wiadomości, zanim dostaną się do sieci. Dość znana w tej dziedzinie jest firma MailShell, która specjalizuje się w systemach antyspamowych i posiada rozwiniętą bazę sygnatur. Użytkownicy nie muszą na własną rękę usuwać irytujących e-maili, a serwery pocztowe nie są zbędnie zapychane. Koszty zarządzania spamem można obniżyć w takim przypadku do minimum. Aplikacje antyspamowe umożliwiają wybór poszczególnych opcji, jak postępować w przypadku, kiedy jakaś wiadomość zostaje uznana jako spam. Do opcji tych należy między innymi usunięcie wiadomości, przekierowanie wiadomości na adres e-mail wskazany przez administratora lub dodanie do tematu wiadomości wyrazu „spam". Tę ostatnią opcję można wykorzystać dalej, konfigurując reguły w kliencie pocztowym w taki sposób, aby wiadomości zawierające wyraz SPAM w temacie były automatycznie przenoszone do folderu nazwanego np. Spam. Filtry antyspamowe powinny być oparte na kilku silnikach skanujących automatycznie pocztę i posiadać jednocześnie zdolność samodzielnego uczenia się, tak aby tysiące wiadomości nie trafiało na nasze skrzynki, a jednocześnie te ważne nie były kasowane. Pierwszy silnik porównuje zawartość wiadomości z zawartością z wewnętrznej listy wiadomości śmieci, zapisanej w postaci bazy sygnatur, która jest automatycznie aktualizowana. Mechanizm ten sprawdza również, czy dana wiadomość była wysyłana „hurtowo", czyli do wielu adresatów w tym samym czasie. Drugi silnik powinien odpowiadać za sprawdzenie reputacji nadawcy – czy ten nie jest przypadkiem na wewnętrznej liście spamerów, zapisanej

w bazie sygnatur, która jest również automatycznie aktualizowana. Trzeci mechanizm, zaimplementowany w urządzeniu, powinien odpowiadać za zawartość wiadomości – styl, przeznaczenie, język oraz słowa kluczowe sugerujące, że jest to spam (np. v-i-a-g-r-a itp.). Filtr antyspamowy powinien się wyróżniać również możliwością skanowania wiadomości pod względem trików technicznych, zwykle używanych przez spamerów. Zastosowanie kilku różnych poziomów skanowania pozwala określić prawdopodobieństwo, czy dana wiadomość jest spamem i podjąć odpowiednie działania. Na przykład, przy prawdopodobieństwie na poziomie 99 proc. wiadomość zostaje uznana jako spam i skasowana. Jeżeli będzie poniżej ustawionej wartości, zostanie uznana jako „Prawdopodobnie spam" i zapisana w odpowiednim folderze lub zostanie przepuszczona, jeśli zostanie uznana za pożądaną.

Jak wiadomo, internet jest w obecnych czasach najczęściej używanym źródłem informacji. Według statystyk, co trzecia zatrudniona osoba ma dostęp do internetu, 30-40 proc. czasu spędzonego w internecie nie jest związane z pracą. Statystyki mówią także, że ponad 60 proc. zatrudnionych używa internetu w celach prywatnych, a 70 proc. wszystkich odwiedzin stron pornograficznych jest dokonywane w godzinach pracy[2]. Strata czasu pracy i zachowania nieetyczne to nie jedyne zagrożenia. Odwiedzając witryny pornograficzne, hakerskie, itp., można narazić komputer na infekcję wirusem, dialerem czy programem szpiegującym, co może doprowadzić do zniszczenia i utraty danych. Na rynku dostępnych jest wiele filtrów URL, które sprawdzają strony internetowe i wyszukują określone słowa kluczowe. Jeżeli w tekście na stronie internetowej znajdą wyraz „seks", administrator może w dość prosty sposób zablokować taką stronę. Co zrobić jednak, jeżeli strona nie zawiera treści pornograficznych, tylko jest to, przykładowo, serwis wiadomości i w jednym z artykułów, np. o wirusie HIV, pojawia się wyraz „seks"? Niestety, proste filtry w tego typu przypadkach nie sprawdzają się – potrzebne są inteligentniejsze rozwiązania.

Pozostaje zatem pytanie, jak walczyć z tym zjawiskiem, które coraz bardziej się pogłębia? Jest wiele sposobów rozwiązania tego problemu. Można przecież zablokować dostęp do internetu wszystkim pracownikom, ale bez internetu trudno się pracuje, jest to bowiem wciąż główne źródło aktualnych informacji. Nie jest to dobre rozwiązanie. Istnieje, oczywiście, możliwość kontrolowania stacji roboczych poszczególnych osób, które korzystają z internetu. Ale powiedzmy szczerze, zajęłoby to zbyt dużo czasu i zasobów, więc w średnich firmach ta opcja nie jest raczej możliwa. Pozostaje jeszcze wprowadzenie kontrolowanego dostępu do internetu przez serwer proxy lub ograniczanie dostępu do witryn tylko niektórym pracownikom itd. Rozwiązań jest wiele, jednak nie wszystkie wszędzie się sprawdzają. Najlepszym wyjściem jest dobry filtr URL, którego listy są bardzo często aktualizowane i wzbogacane o nowe adresy. Firma Cobion jest specjalistą w katalogowaniu stron internetowych. Mając specjalne mechanizmy, automatycznie wyszukuje w internecie witryny o określonych kategoriach tematycznych. Posiada jedną z najdłuższych i najczęściej aktualizowanych list filtrów URL na świecie. Zawiera ponad 20 milionów adresów WEB, zanalizowano już ponad 2600 milionów stron internetowych. Każdego dnia lista ta zostaje zwiększona o więcej niż 100 000 nowych adresów. W przypadku filtrów URL istotna jest możliwość wyboru kategorii tematycznej, którą chcemy zablokować pracownikom. Oprócz tego administrator musi mieć sposobność skonfigurowania białej i czarnej listy adresów stron www, domen oraz adresów IP. Jeśli natomiast prezes firmy ma wszechstronne zainteresowania, administrator musi mieć możliwość skonfigurowania listy VIP, tzn. wskazać komputery, których użytkownicy będą mieli dostęp do wszystkich stron internetowych.

Kluczową korzyścią, jaka wynika z zastosowania sprzętowego rozwiązania antywirusowego, jest m.in. bardzo szybka instalacja takiego rozwiązania, nawet w sieciach komputerowych o bardzo skomplikowanej typologii i dowolnych systemach operacyjnych. Inną dość istotną zaletą jest zmniejszenie obciążenia sieci. Instalacja na brzegach sieci powoduje, oprócz zwiększenia bezpieczeństwa, zmniejszenie niepotrzebnego wewnętrznego ruchu sieciowego, w wyniku blokowania spamu czy niepożądanych stron www. Dodatkowo zostają odciążone serwery pocztowe. Optymalna wydajność przy znikomym wpływie na ruch w sieci czyni urządzenie całkowicie niewidocznym dla użytkowników.

Połączenie sprzętu i oprogramowania w jednym urządzeniu umożliwia osiągnięcie najwyższej wydajności w skanowaniu i zwalczaniu niebezpiecznego kodu.

Należy pamiętać, że tak naprawdę nie istnieją metody zabezpieczenia, programy antywirusowe, które dają 100-proc. gwarancję bezpieczeństwa, miarą jakości rozwiązania jest jednak zbliżenie się do tego ideału. Istotna jest również możliwość dostosowania się do indywidualnych potrzeb i wymagań użytkowników. Jedno jest pewne – w obliczu rosnącej liczby zagrożeń i zwiększonego ryzyka infekcji nie wolno zapomnieć o bezpieczeństwie naszych komputerów. Należy chronić je, korzystając z najnowszych technologii. Wyścig zbrojeń trwa – bezpieczniej już nie będzie.

Arkadiusz Rabiega
autor jest pracownikiem firmy Panda Software Polska

Przypisy

[1] Spam Filter Review (hhtp://www.spamfilterreview.com/spam-statistics.html).

[2] Cobion.

Narażony jesteś
na te same zagrożenia,
co największe
międzynarodowe
korporacje!

Bądź tak samo zabezpieczony!
Korzystaj z Check Point Express CI !

NGX

CheckPoint Express™ jest zintegrowaną bramą bezpieczeństwa przeznaczoną dla średnich przedsiębiorstw. Express oferuje te same mechanizmy zabezpieczeń i taki sam poziom ochrony, jaki jest stosowany przez wszystkie firmy Fortune 100.

Zintegrowane rozwiązanie CheckPoint Express CI zapewnia wszystkie mechanizmy bezpieczeństwa wymagane do ochrony sieci oraz zdalnego dostępu dla pracowników mobilnych. Aby zagwarantować wysoki poziom zabezpieczeń w miejscu styku z siecią zewnętrzną CheckPoint Express łączy zalety sprawdzonego rozwiązania Firewall-1 z mechanizmami przeciwdziałania włamaniom SmartDefense, aby uniemożliwić przeprowadzenie wyrafinowanych ataków. Dzięki temu firmowe dane pozostają bezpieczne.

W celu uzyskania więcej informacji zapraszamy do kontaktu pod adresem:
bezpieczenstwo@veracomp.pl

Pracownicy mobilni mogą bez przeszkód nawiązywać bezpieczną łączność z firmą korzystając z mechanizmów sieci prywatnych (VPN) gwarantujących poufność przesyłanych danych. Wygoda rozwiązania polega na tym, ze można korzystać z mechanizmów IPSec oraz SSL, zależnie od potrzeb i własnych preferencji.
Dodatkowo ochrona antywirusowa wbudowana w Express CI, blokuje różnorodne złośliwe próby ataku których celem mogą być serwery oraz komputery robocze.
Wszystkie funkcje zabezpieczeń zarządzane są z jednego miejsca, korzystając z efektywnych i wygodnych narzędzi SmartCenter.

Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

veracomp

Veracomp SA jest Autoryzowanym Dystrybutorem
rozwiązań Check Point Software Technologies.
Prowadzi sprzedaż wyłącznie za pośrednictwem Partnerów Handlowych.

www.veracomp.pl

V Kongres INFOTELA

Komunikacja elektroniczna drog¹ do zwiêkszenia konkurencyjnoœci w Unii Europejskiej

Kudowa Zdrój „Kongres Centrum” 24–27 maja 2006 r.

Tematy Kongresu:

Sesje tematyczne – regulacje

- Regulacje w komunikacji elektronicznej;
- Dostêp do informacji elektronicznej w Polsce;
- Finansowanie rozwoju komunikacji elektronicznej;
- Bezpieczeństwo komunikacji elektronicznej.

Sesje tematyczne – biznes

- Œwiatowe trendy w komunikacji elektronicznej, kierunki rozwoju i ich wp³yw na biznes oraz budowanie spo³eczeństwa informacyjnego w Polsce;
- Modele biznesowe w komunikacji elektronicznej;
- Narzêdzia wzrostu budowy infrastruktury dostêpowej w Polsce;
- Prezentacje Sponsorów i Partnerów.

Sesje tematyczne – technologie

- Nowoczesne us³ugi mobilne;
- Rynek us³ug szerokopasmowych w dobie globalizacji;
- Przysz³oœæ technologii UMTS i WiMAX w Polsce i Europie;
- Telefonia IP;
- Potrójna us³uga – Triple-play;
- Us³ugi dostêpu do internetu (mobile internet, internet szerokopasmowy, internet satelitarny);
- Telewizja cyfrowa.

Sponsorzy:

Partnerzy:

Imprezy towarzyszące:

- Rozstrzygnięcie VIII edycji ogólnopolskiego konkursu o Laur INFOTELA
- Uroczysta Gala telekomunikacji
- Biesiada „Przy Górskim Strumyku”
- Wyjazd do Pragi
- Konkurs w rzucie komórką

Patronat medialny:

Organizator:

MSG MEDIA
ul. Stawowa 110, 85-323 Bydgoszcz
tel. (52) 325 83 10, fax (52) 373 52 43, www.msgmedia.pl