MSG MEDIA

ISSN 1429-0200

INFO TEL

1/2009

INDEKS 345237

Cena 15 zł
(w tym 0% VAT)

kwartalnik – STYCZEŃ/MARZEC

NOWOCZESNA KOMUNIKACJA ELEKTRONICZNA

TELEKOMUNIKACJA • INFORMATYKA • TELEWIZJA

czytaj strona 34-35

KONFERENCJA z cyklu

„Przyszłość komunikacji elektronicznej w Polsce"

17 marca 2009 r.

podczas trwania targów INTERTELECOM 2009 w Łodzi (17–19 marca 2009 r.)

sponsor konferencji:

ksi.pl
KOMPLEKSOWE SYSTEMY INFORMACYJNE

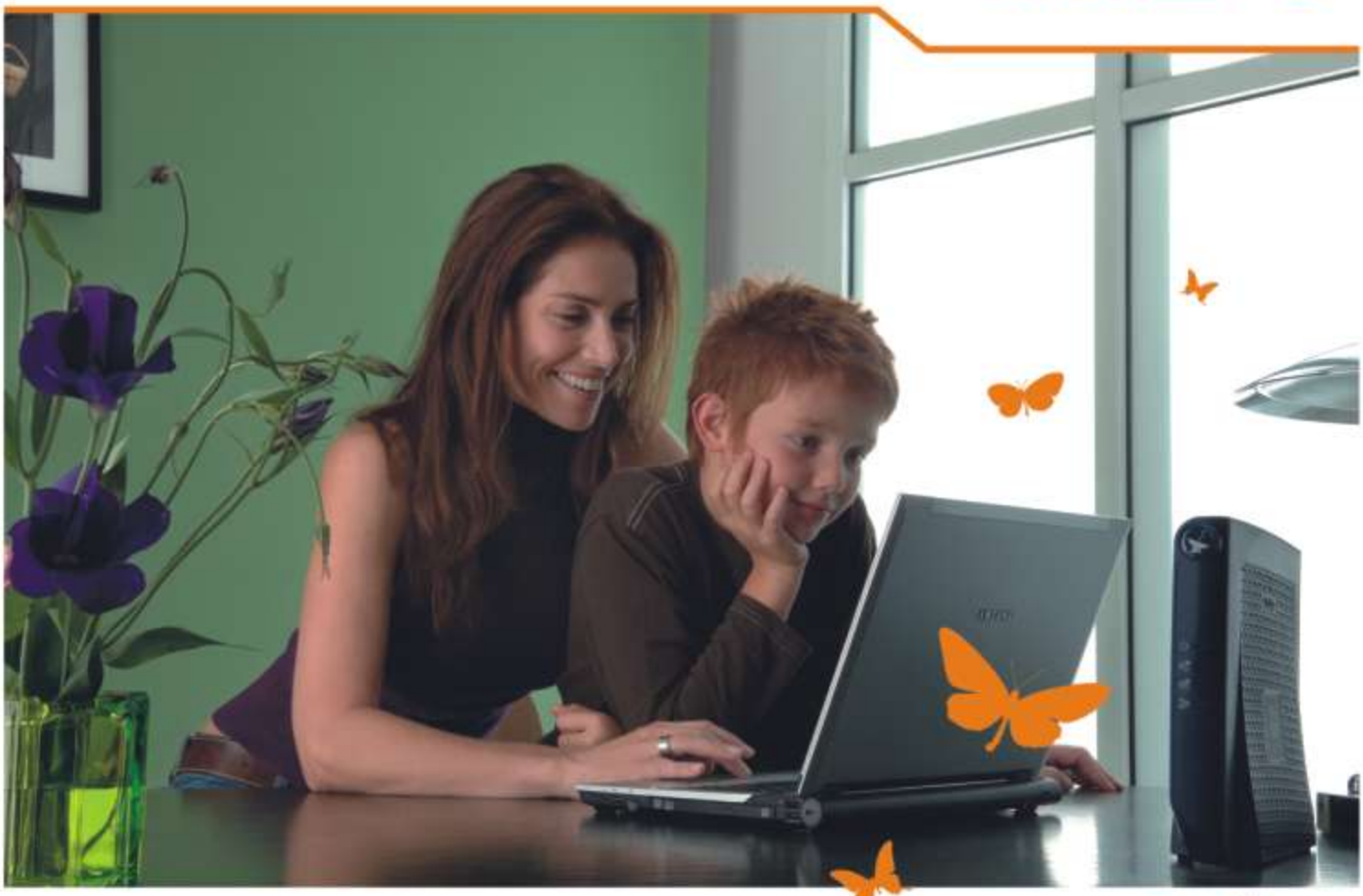
Konferencja będzie kolejnym spotkaniem specjalistów z dziedziny komunikacji elektronicznej, a także pracowników firm telekomunikacyjnych, izb branżowych, naukowców zainteresowanych rozwojem branży w Polsce. W konferencji wezmą udział przedstawiciele Urzędu Komunikacji Elektronicznej oraz sejmowej podkomisji 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.

Organizator:
MSG MEDIA

tooway™
The new way to broadband



Internet bez granic

Tooway™ – szerokopasmowy Internet satelitarny dla odbiorców indywidualnych

Usługa Tooway™ to wysokiej jakości łącze internetowe nowej generacji dla odbiorców indywidualnych na terenie całej Polski. Tooway™ to alternatywa dla połączeń typu „dial-up" o niskiej przepustowości. Koszt niezbędnych urządzeń i instalacji jest znacznie niższy niż cena profesjonalnych satelitarnych systemów szerokopasmowych. Do uruchomienia usługi Tooway™ wystarczy modem i antena satelitarna o niewielkich wymiarach. Dodatkowe oprogramowanie nie jest wymagane.

Rozwiązanie Tooway™ zapewnia nieograniczony dostęp do szybkiego Internetu niezależnie od istniejącej infrastruktury naziemnej.

eutelsat
COMMUNICATIONS

Sprzęt do Tooway™

KLIKASZ – rozmawiasz

bez opłat

bez konta

bez logowania

bezpiecznie

VOICELINK

czytaj strona: 26-27

INFOTEL 1997

INDEKS 345237
numer 1 (101), rok dziesiąty
styczeń/marzec 2009
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

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; kom. 728 496 599
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

RYNEK

Prezes Netii „Graczem Roku 2009" wg „Forbes"

Mirosław Godlewski, Prezes Zarządu firmy Netia SA, zajął pierwsze miejsce w rankingu „Gracze Roku 2009" miesięcznika „Forbes" w kategorii: media, telekomunikacja, IT.

W tegorocznej edycji rankingu „Gracze Roku" miesięcznika „Forbes", jurorzy – doradcy biznesowi oraz menedżerowie funduszy private equtiy – wybrali sześciu przedsiębiorców, których uznano za potencjalnych liderów w swoich branżach w 2009 roku. Prezes Netii został uhonorowany pierwszym miejscem w kategorii: media, telekomunikacja, IT.

BEZPIECZEŃSTWO

UKE chce wyróżniać rzetelnych operatorów

UKE ogłosił program certyfikacji usług telekomunikacyjnych mający na celu dopingowanie działań operatorów telekomunikacyjnych związanych z bezpieczeństwem użytkowników usług telekomunikacyjnych.

Program zakłada promocję działań operatorów telekomunikacyjnych mających na celu podniesienie jakości świadczonych usług, a także świadomości użytkowników usług telekomunikacyjnych, a przede wszystkim ochronę dzieci i młodzieży.

Do programu „Bezpieczny internet", „Bezpieczny telefon" „Uczciwy transfer" mogą przystąpić wszyscy operatorzy spełniający określone przez UKE warunki. Udział w programie jest dobrowolny, przystąpienie do któregokolwiek programu nie powoduje konieczności zmiany regulaminu świadczenia usług telekomunikacyjnych.

TELEKOMUNIKACJA

Molex ogłasza wprowadzenie na rynek Pionowego organizatora kablowego (VRM)

Firma Molex Premise Networks poinformowała o wprowadzeniu na rynek Pionowego organizatora kablowego (ang. Vertical Cable Rack Manager, VRM). Pionowy organizator kablowy w połączeniu z 19-calową stojącą ramą montażową 42U firmy Molex umożliwia skuteczne porządkowanie kabli.

Współczesne technologie sieciowe wymagają coraz większej gęstości kabli, a jednocześnie dostępu do nich i możliwości skutecznego porządkowania. Pionowy organizator kablowy nadaje się idealnie do stosowania w środowiskach o dużej gęstości kabli, takich jak centra danych czy serwerownie. Pionowy organizator kablowy umożliwia skuteczne porządkowanie kabli. Zapewnia niezbędne wsparcie dla wiązek kabli krosowych, przenosząc ich ciężar z paneli na ramę przy konsekwentnym zachowaniu promienia gięcia. Kable można prowadzić elastycznie, a także szybko zmieniać ich bieg dzięki szpulkom Quick Fit.

Montowane na zatrzask prowadnice kabli umożliwiają elastyczne prowadzenie kabli oraz nieograniczoną rozbudowę.

Pionowy organizator kablowy jest dostępny w wersji 8- i 12-calowej. Drzwi otwierają się na lewo lub na prawo i dają łatwy dostęp do kabli. Szpulki i elementy podtrzymujące poziome przebiegi kablowe można ponadto łatwo mocować i demontować.

Więcej informacji o tym nowym rozwiązaniu udzieli Kierownik Wsparcia Technicznego – Michał Muszalski mmuszalski@molex.com.

Wirtualne telemuzeum

Z inicjatywy Prezesa Urzędu Komunikacji Elektronicznej powstała strona internetowa o niezwykłych ludziach telekomunikacji, którzy część swojego życia poświęcili pasji kolekcjonowania historycznych już urządzeń służących do zapewnienia łączności.

„Chcemy przedstawić ich trud i starania, by zachować dla kolejnych generacji przekaz o początkach komunikowania się ludzi za pomocą urządzeń elektrycznych i elektronicznych, jak następowała ich miniaturyzacja, rozwój techniczny i standaryzacja, aż do postaci takiej, z jakiej obecnie na co dzień korzystamy" – czytamy w komunikacie UKE. Zachęcamy także do współpracy osoby, które chciałyby podzielić się z gośćmi strony internetowej telemuzeum.uke.gov.pl również swoimi kolekcjami.

Zmiana numeracji

Na mocy Rozporządzenia Ministra Infrastruktury zmienia się numeracja strefowa Abonenckich Usług Specjalnych i numerów skróconych tp. Od 15 lutego 2009 r. przed 4-cyfrowymi numerami telefonicznymi rozpoczynającymi się cyfrą 9 będziemy dodatkowo wybierać cyfrę 1. Dotyczy to m.in. numerów błękitnej linii tp 9393 (nowy numer: 19393) oraz błękitnej linii tp biznes 9330 (19330).

Zmiany obejmują wszystkie 4-cyfrowe numery rozpoczynające się od 9 z wyjątkiem tych, w których po cyfrze 9 następuje 8 lub 9. Przykładowo, przed takimi numerami jak 9393 (błękitna linia tp), 9491 (informacja miejska tp) czy też numerami radio taxi lub pogotowia drogowego będziemy dodatkowo wybierać cyfrę 1.

HOT BIRD™ 10 na orbicie

Spółka Eutelsat Communications umieściła na orbicie okołoziemskiej nowego satelitę HOT BIRD™ 10.

Przed włączeniem do konstelacji HOT BIRD™ na pozycji 13°E HOT BIRD™ 10 zostanie umieszczony początkowo na 7°W, kluczowej pozycji orbitalnej dla obszaru Bliskiego Wschodu. Eutelsat rozpoczął przekaz z 7°W w roku 2006 z wykorzystaniem satelity ATLANTIC BIRD™ 4 kolokowanego z dwoma satelitami egipskiego operatora Nilesat. Zastąpienie ATLANTIC BIRD™ 4 przez HOT BIRD™ 10 spowoduje znaczne zwiększenie zasobów orbitalnych Eutelsat dostępnych na tej pozycji.

Alcatel-Lucent dla sieci LTE

Firma Alcatel-Lucent wprowadziła moduł oprogramowania, który umożliwia operatorom sieci bezprzewodowych szybkie wdrożenie technologii LTE (ang. *Long Term Evolution*). Moduł ten jest kluczowym elementem udoskonalonego rozwiązania eNodeB i stanowi ważny krok w realizacji strategii firmy, mającej na celu wspomaganie wdrażania bezprzewodowych usług nowej generacji na całym świecie.

Moduł oprogramowania LTE jest już w eksploatacji próbnej u największych usługodawców na całym świecie i zostanie ogólnie udostępniony w połowie roku 2009.

42 Mbps w nowej technologii multi-carrier

Ericsson podczas Mobile World Congress w Barcelonie zaprezentował po raz pierwszy nową technologię multi-carrier HSPA ze szczytową prędkością pobierania danych wynoszącą 42 Mbps. Technologia multi-carrier jest kolejnym krokiem w ewolucji HSPA i umożliwia konsumentom otrzymywanie danych jednocześnie na dwóch częstotliwościach kanałów. Podwaja to prędkość transmisji danych w obszarze objętym siecią HSPA i na skraju zasięgu, gdzie zazwyczaj klienci doświadczają wolniejszej prędkości transmisji danych. W rezultacie szczytowa prędkość pobierania danych zwiększy się z dzisiaj dostępnej najszybszej prędkości wynoszącej 21 Mbps do 42 Mbps. Dzięki temu doświadczenia klientów związane z usługami online dotyczącymi treści wysokiej jakości w znaczny sposób się poprawią. Technologia multi-carrier HSPA firmy Ericsson będzie gotowa do zastosowania komercyjnego pod koniec 2009 r.

INFORMATYKA

Polski avatar w amerykańskiej firmie

Notowana na rynku NewConnect spółka informatyczna InteliWISE SA zawarła nową umowę z amerykańską korporacją Kraft Foods Global Inc, jedną z wiodących firm w branży dóbr szybko zbywalnych na świecie.

Umowa dotyczy nowego projektu – przygotowania i wdrożenia systemu „Wirtualny Doradca" dla potrzeb globalnego serwisu Kraft Foods Global, wspierającego działania IT. Wartość kontraktu wynosi ponad 1 mln zł.

Firma jako pierwsza w Europie wdrożyła tego typu rozwiązanie informatyczne, które zostało zainstalowane między innymi na stronie www.lot.com.

TELEWIZJA

Pierwsze próby DVB-SH

Firmy RAI, 3 Italia, Alcatel-Lucent i Eutelsat przeprowadzają próbę DVB-SH – mobilnej telewizji satelitarnej i naziemnej.

Pierwsza próba DVB-SH, przeprowadzona w Turynie przez włoską telewizję RAI, operatora sieci komórkowej 3 Italia, Alcatel-Lucent oraz Eutelsat, przyniosła znakomite rezultaty. Wstępne wyniki wskazują na dobrą jakość odbioru telewizji przy użyciu tej nowej technologii przez komercyjnie dostępne terminale mobilne. Po pełnym wdrożeniu rozwiązanie umożliwi odbiór telewizji z satelitów i sieci naziemnych.

Próba była nadzorowana przez Centrum Badań i Innowacji Departamentu Strategii Technologicznych RAI oraz przez operatora 3 Italia, który jako pierwszy na świecie oferuje usługi telewizji mobilnej opartej na technologii DVB-H. Alcatel-Lucent dostarczył wyposażenie nadawcze DVB-SH oraz integrację sieci i niezbędną pomoc techniczną. Eutelsat zapewnił satelitarną dystrybucję treści oraz łącza uplink.

Próba w Turynie potwierdziła zalety sieci naziemnych, obejmujących sieć komórkową z nadajnikami niskiej mocy i sieć nadawczą z nadajnikami średniej mocy.

PRAWO

Wyrok ETS w sprawie definicji abonenta

Komisja Europejska w skardze do Trybunału wniosła o stwierdzenie, że nie dokonując prawidłowo transpozycji dyrektywy Parlamentu Europejskiego dotyczącej definicji „abonenta", Rzeczpospolita Polska uchybiła zobowiązaniom, które na niej ciążą na mocy tej dyrektywy.

Zdaniem Komisji, polskie przepisy – w zakresie, w jakim przewidują, że „abonentem" w rozumieniu dyrektywy ramowej może zostać tylko osoba, która zawarła umowę „w formie pisemnej" – wykraczają poza wymogi tej dyrektywy i pozbawiają osoby, które nie zawarły umowy w takiej formie, określonych uprawnień przyznanych im przez dyrektywy o łączności elektronicznej, np. uprawnienia do umieszczenia swoich danych w spisie abonentów.

Obecnie procedowany w Sejmie projekt ustawy o zmianie ustawy *Prawo telekomunikacyjne* nie zawiera zmian w zakresie definicji „abonenta".

MULTIMEDIA

Technologie 3G Femtocell w Barcelonie

Podczas GSMA Mobile World Congress firma NETGEAR® zademonstrowała bramkę Femtocell Voice Gateway (DVG834GH) umożliwiającą konwergencję usług sieciowych.

Była to pierwsza publiczna prezentacja w pełni funkcjonalnej bramki do zastosowań domowych, łączącej modem ADSL2+, router, Ethernet LAN, punkt dostępu Wi-Fi, telefonię Voice-over-IP (VoIP) oraz miniaturową stację bazową 3G w technologii femtocell. Demonstracja obejmowała nawiązywanie połączeń głosowych 3G i ściąganie treści multimedialnych protokołem High-Speed Packet Access (HSPA) z internetu i sieci domowej do urządzenia przenośnego. NETGEAR prezentuje produkty na targach Mobile World Congress na stoisku partnera – Ubiquisys, wiodącego producenta technologii 3G femtocell.

REGULACJE

Powstaje Krajowe Forum Szerokopasmowe

Powołanie Krajowego Forum Szerokopasmowego to nowa inicjatywa Prezesa UKE, realizowana w ramach programu „Polska Cyfrowa". Została powołana grupa inicjatywna, w skład której wchodzą: Fundacja Wspomagania Wsi, Stowarzyszenie Budowniczych Telekomunikacji oraz Fundacja Telefony Polskie.

Z założenia Forum ma być miejscem integracji wokół wspólnego celu, jakim jest rozwój rynku telekomunikacyjnego. Forma, w jakiej pracuje Forum, jest otwarta dla organów rządowych, podmiotów rynkowych, organizacji pozarządowych, instytutów naukowych, inwestorów, jednostek samorządu terytorialnego i organizacji konsumenckich. Według UKE, Forum powinno stać się miejscem wymiany modeli biznesowych w aspekcie budowy sieci nowej generacji, dobrych praktyk techniczno-organizacyjnych oraz efektywnego wykorzystania pieniędzy europejskich. W trakcie uruchomienia jest Portal Forum, na którym będzie można korzystać z bazy wiedzy: gdzie szukać fachowców, jak pisać SIWZ, wypełniać formularze, pozyskiwać fundusze, rozmawiać z wykonawcami itp. Taka forma współpracy umożliwi szybką wymianę informacji i wdrażanie najbardziej efektywnych rozwiązań, budowę standardów uczciwego doradztwa.

Założenia do ustawy o rozwoju sieci

Urząd Komunikacji Elektronicznej przedstawił dokumenty przygotowane przez Prezesa UKE w ramach prac w Zespole Polska Cyfrowa. Pierwszy z nich to analiza zasadności i zakresu interwencji publicznej na rynku usług szerokopasmowych, mająca na celu uzasadnić szczególne narzędzia zmierzające do promowania rozwoju usług szerokopasmowych. Drugi z nich to wstępne założenia do zapowiadanego przez Prezesa Urzędu Komunikacji Elektronicznej projektu ustawy o modernizacji i rozwoju sieci telekomunikacyjnych.

Dokumenty znajdują się na stronie internetowej UKE
http://www.uke.gov.pl/uke/index.jsp?place=Lead07&news_cat_id=168&news_id=3799&layout=3&page=text.

Przewodnik o dostępie do infrastruktury

Dostęp telekomunikacyjny w zakresie wykorzystania budynków oraz istniejących masztów i wież jako elementów wsporczych do montażu anten. Przewodnik o dostępie do infrastruktury zawiera: wykaz przepisów prawa mających zastosowanie przy realizacji dostępu telekomunikacyjnego w zakresie objętym przewodnikiem, określenie obszaru, zakresu i sposobu realizacji obowiązku zapewnienia dostępu telekomunikacyjnego wraz ze wskazaniem przepisów prawa obejmujących te zagadnienia, możliwy do wykorzystania obszar działania, procedurę postępowania dla pozyskania obszaru działania i jego eksploatacji, zakres rzeczowy umowy na dostęp do infrastruktury – zwanej dalej „Umową", sugestie co do ustalania wysokości opłat tytułem dostępu, opis problemów i propozycje zmian legislacyjnych.

Więcej informacji na stronie UKE.

Translation

Rozwiązanie PowerCat™ 6A

W świetle obecnych wymagań dotyczących przepustowości oraz szybko powstających nowych trendów technologicznych, znaczenie szybkich rozwiązań sieciowych wzrosło niepomiernie. Opracowany na potrzeby sieci 10 Gigabit Ethernet (10 GBase-T) system kategorii 6A jest zoptymalizowanym pod kątem szybkości rozwiązaniem z zakresu okablowania strukturalnego, zapewniającym najwyższe parametry szybkości, niezawodności, gotowości na przyszłe potrzeby oraz długoterminowej eksploatacji. Dzięki temu staje się preferowanym systemem w centrach danych, instytucjach finansowych oraz przedsiębiorstwach, którym do pracy niezbędna jest najwyższa jakość działania.

Nieekranowane rozwiązania kablowe były tradycyjnie preferowane na wielu rynkach. Jednak wskutek dziesięciokrotnego wzrostu wymagań związanych z transmisją danych w instalacjach 10 GBase-T, realizacja systemów okablowania kategorii 6A jest znacznie bardziej złożona niż poprzednio, a ponadto wymaga rozwiązywania pewnych problemów związanych z układem, projektowaniem i prowadzeniem kabli oraz przesłuchem obcym. Jedynym sposobem przezwyciężenia tych trudności przy zachowaniu szybkiej transmisji danych jest ekranowane rozwiązanie kategorii 6A.

Rozwiązanie PowerCat™ kategorii 6A firmy Molex zostało opracowane z myślą o najwyższych parametrach. Biorąc pod uwagę lepszą transmisję danych przy wyższych częstotliwościach oraz lepsze tłumienie szumu, nie warto iść na kompromis. Nasze rozwiązanie zostało starannie opracowane, dzięki czemu zapewnia najbardziej zaawansowane tłumienie przesłuchu obcego oraz poziom strat na złączu nieosiągalny dla wszelkich systemów nieekranowanych.

Technologia

Zastosowanie rozwiązania ekranowanego kategorii 6A znacznie redukuje typowe problemy związane z użytkowaniem produktów nieekranowanych, takie jak przesłuch obcy, koszty miejsca oraz systemów prowadzenia kabli, a także projekt infrastruktury budynku. Rozwiązania ekranowane zapewniają wyjątkową niezawodność przy ekstremalnych szybkościach, większym paśmie oraz zapasie wydajności. Czas zakańczania produktów ekranowanych, które kiedyś uważano za zajęcie uciążliwe, został znacząco skrócony – głównie dzięki zmniejszeniu średnicy kabla, lepszemu uporządkowaniu kabli, narzędziom oraz technologiom złączy.

Rozwiązanie kategorii 6A firmy Molex

Naszą rodzinę produktów ekranowanych opracowaliśmy z myślą o rozwiązaniu sieciowym zapewniającym najwyższe parametry działania. Rozwiązanie ekranowane kategorii 6A firmy Molex jest przeznaczone specjalnie do szybkiego przesyłu danych przy małym marginesie błędu, wyjątkowo skutecznym tłumieniu przesłuchu obcego, doskonałym poziomie strat na złączu oraz ochronie przed zakłóceniami elektromagnetycznymi (EMI).

Złącze DataGate™ odlewane pod ciśnieniem z przesłoną

Odlewane pod ciśnieniem ekranowane złącze PowerCat 6A RJ45 jest podstawą systemu PowerCat 6A oraz zapewnia doskonały poziom ochrony przed przesłuchem obcym oraz strat na złączu. Przesłona z mechanizmem sprężynowym chroni złącze przed kurzem i zabrudzeniami, a także odrzuca nieprawidłowo wpięte lub uszkodzone kable krosowe.

Panele krosowe

Solidne 24- i 48-portowe panele z równie solidnymi tacami, które jednolicie porządkują przebiegi kablowe oraz chronią je przed uszkodzeniami mechanicznymi. Kątowa konstrukcja panelu zwiększa dostępność portów i minimalizuje promień gięcia kabli krosowych, a jednocześnie eliminuje konieczność stosowania poziomych systemów porządkowania kabli. Dzięki temu osiąga się większą gęstość portów w szafach, co idealnie zaspokaja potrzeby centrów danych.

Kabel U/FTP

Ten wysokiej jakości kabel, przeznaczony specjalnie do sieci 10 Gigabit Ethernet (10 GBase-T), minimalizuje przesłuch obcy (między kablami) oraz zapewnia doskonałą izolację sygnału, eliminując jednocześnie wpływ zakłóceń elektromagnetycznych.

Kable krosowe

Ekranowane kable krosowe PowerCat 6A wykonane z wysokiej jakości czteroparowej ekranowanej linki 26 AWG i dostępne w różnych kolorach oraz długościach są fabrycznie zakończone ekranowanymi wtykami RJ45 oraz zawierają wzmocnione osłony wtyków.

Wybrane zalety rozwiązania Molex PowerCat kategorii 6A

Połączenie ekranowane na 360° dzięki odlewanemu pod ciśnieniem złączu DataGate.

Ochrona – wyjątkowa przesłona sprężynowa złącza DataGate nie tylko chroni przed kurzem i zabrudzeniami, ale też odrzuca nieprawidłowo wpięte bądź uszkodzone kable krosowe.

Niezawodność – funkcje porządkowania przebiegów kablowych zmniejszają naprężenie kabli i zapewniają spójną jakość działania, a złącze DataGate zmniejsza poziom szkód i przyspiesza instalację.

Doskonałe parametry – rozwiązanie ekranowane end-to-end spełniające wymagania kategorii 6A.

Ekranowany kabel skutecznie zmniejsza efekt przesłuchu obcego.

Co robimy

Od ponad 30 lat Molex produkuje wszechstronne systemy okablowania miedzianego oraz światłowodowego do transmisji głosu, danych i sygnałów wizyjnych.

Gwarancja spokoju
System PowerCat 6A jest objęty 25-letnią Globalną Gwarancją na Produkty, System i Aplikacje.

Zgodność ze standardami
C6 A TIA/EIS-568-B.2-10; ISO/IEC 11801

Nasza sieć instalatorów gwarantuje **bezproblemowe wdrożenia**

Niezależnie od skali trudności instalacji czy wdrożenia zawsze dążymy do tego, by przebiegały one jak najsprawniej. Ściśle współpracujemy z naszymi partnerami instalującymi systemy, aby zapewnić spójną, wysoką jakość, niezależnie od złożoności czy prostoty projektu.

Naszą dbałość o wysoką jakość profesjonalnych instalacji odzwierciedla globalna sieć Certyfikowanych Instalatorów, inwestycje w szkolenia oraz pomoc techniczna okazywana z zaangażowaniem klientom na całym świecie.

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

www.molexpn.com.pl

molex
one company › a world of innovation

Rynek komunikacji elektronicznej będzie impulsem dla pozostałej części gospodarki

Nie będzie złagodzenia regulacji

Z prezes Urzędu Komunikacji Elektronicznej – ANNĄ STREŻYŃSKĄ – rozmawiał Grzegorz Kantowicz.

– W listopadzie ubiegłego roku ukazał się „Raport o stanie infrastruktury telekomunikacyjnej w Polsce" sporządzony przez KPMG Advisory i MDI. Zdaniem autorów, obecne regulacje sprzyjają jedynie obniżaniu cen usług telekomunikacyjnych, natomiast rynek komunikacji elektronicznej oczekuje od regulatora regulacji bardziej ukierunkowanych na promocję inwestycji w infrastrukturę. Czy nie czas na zmianę strategii regulacyjnej UKE?

– Nie, mimo opłaconych przez zainteresowanych kreowaniem określonej rzeczywistości raportów, promocja infrastruktury to rola rządu. UKE realizuje zadania w zakresie infrastruktury poprzez umożliwianie budowy kolejnych infrastruktur radiowych, stacjonarnych oraz mobilnych i to jedyna nasza rola. Wobec dotychczasowej bierności odpowiedzialnego ministra w tym zakresie, podejmowaliśmy się także innych proinfrastrukturalnych inicjatyw (stanowisko w sprawie barier inwestycyjnych czy współpraca z samorządami, a ostatnio inicjatywa ustawodawcza w sprawie modernizacji i rozwoju infrastruktury telekomunikacyjnej), jednak to musi być priorytet rządu i koordynacja wielu resortów, inaczej działania UKE nie są w stanie skutecznie wpływać na budowę infrastruktury. Zmiana na stanowisku wiceministra napawa nas nadzieją.

– Podział Telekomunikacji Polskiej to temat budzący wiele kontrowersji. Co Pani sądzi o ostatniej transakcji sprzedaży i leasingu zwrotnego części infrastruktury TP swej spółce zależnej TP Invest? Czy transakcja ta może krępować próby regulatora związane z ewentualnym podziałem spółki?

– Może to być taka próba, jednak dopiero przyszłość pokaże prawdziwe intencje TP i kolejne kroki. Obecnie, jak zapewnia TP i z czym się zgadzamy, w związku z zapisami dyrektywy dotychczasowe obowiązki nadal spoczywają na TP, tym razem jako dysponencie, a nie właścicielu. Zastanawiamy się, czy nie jest to próba autoseparacji – jeśli tak, to bardzo interesująca, i czas pokaże, czy będziemy w stanie tę autoseparację kontrolować z pożytkiem dla rynku.

– W styczniu odbyło się pierwsze spotkanie Międzyresortowego Zespołu ds. Realizacji Programu „Polska Cyfrowa" – ciała doradczego Prezesa Rady Ministrów. Do końca marca zespół ten ma przedstawić harmonogram działań dla realizacji programu. Co, z punktu widzenia regulatora, wymaga najpilniejszych działań?

– Najpilniejsze działania to zapewnienie sprawnego wydatkowania środków UE w programach szerokopasmowych i teleinformatycznych, a także zapewnienie otoczenia prawnego i regulacyjnego sprzyjającego inwestycjom oraz dostępowi klientów do budowanej infrastruktury. UKE przygotowuje raport o stanie rynku oraz zasadności i zakresie interwencji państwa, założenia do ustawy oraz samą ustawę. Oby nie utopiła się ona w zabiegach lobbystów i oby rewolucja nie skończyła się na dobrych chęciach.

– Z inicjatywy UKE powstał pomysł utworzenia Fundacji „Cyfrowa Polska" mającej na celu wspieranie procesu cyfryzacji w Polsce. Jakie są obecnie losy tej inicjatywy?

– Propozycja została przekazana do MI, jako organu kierującego zespołem międzyresortowym ds. cyfryzacji. Czekamy na stanowisko ministra. Wdrożenie tej inicjatywy wymaga stanowczości i odwagi, gdyż koszty cyfryzacji obarczają jej beneficjentów, czyli nadawców i operatorów multipleksów.

– Wszyscy zdajemy sobie sprawę z tego, że działania regulatora muszą być wsparte odpowiednimi działaniami zaplecza Rządu. Czy ostatnia zmiana na stanowisku wiceministra ds. telekomunikacji w Ministerstwie Infrastruktury rokuje nadzieje na sprawniejszą współpracę UKE z zapleczem legislacyjnym w Rządzie?

– Oczywiście tak, pani minister Gaj to osoba niezwykle kompetentna i przy tym niezależna w swoich poglądach. Jako radca prawny przywykła do ponoszenia odpowiedzialności za swoje działania, więc nie podejmuje decyzji pochopnie ani pod wpływem jakichkolwiek innych czynników niż wiedza, o czym wielokrotnie mogłam się przekonać, gdy sama musiałam się pogodzić z tym, że nie uzyskam jej zgody (wówczas dyrektora dep. prawnego w UKE) na różne moje zbyt oderwane od rzeczywistości prawnej pomysły. Jestem spokojna, że prace w MI będą odtąd na wysokim poziomie i szybkie, a współpraca z UKE nie tylko sprawniejsza, ale i oparta na wymianie merytorycznych argumentów.

– Wszystko wskazuje na to, że zbliżają się trudne czasy dla naszej gospodarki. Czy przewiduje Pani na tę okoliczność jakieś szczególne działania w kwestiach regulacyjnych rynku komunikacji elektronicznej?

– Jeśli pytanie dotyczy złagodzenia regulacji, to nie, nie przewiduję, przeciwnie – to rynek komunikacji elektronicznej będzie impulsem dla pozostałej części gospodarki i nadal pozytywną pozycją na listach wydatków obywateli. Jeśli zaś chodzi o dodatkowe impulsy regulacyjne, to są one potrzebne w zakresie NGA; bierzemy udział w europejskiej debacie i na pewno nie będziemy ostatnimi, którzy podejmą odpowiednie kroki. Wielu małych operatorów buduje światłowody o wysokich przepływnościach do samego klienta, jednak ich sieci nie znajdują odpowiednio taniej oferty z rynku pozwalającej na wyjście na świat. To i wiele innych problemów z NGA stanowi nasze główne zadania na kryzys.

– Dziękuję za rozmowę.

XX Targi INTERTELECOM

Targi zmieniły swoją funkcję

Z prezesem zarządu Międzynarodowych Targów Łódzkich – PAWŁEM FENDLEREM oraz dyrektorem MIROSŁAWEM PIETRUCHĄ – rozmawiał Grzegorz Kantowicz.

Prezes zarządu MTŁ – Paweł Fendler

– Tegoroczne XX Targi INTERTELECOM zbiegają się z dwudziestą rocznicą działalności Międzynarodowych Targów Łódzkich. Jak Pan ocenia z perspektywy tych lat obecny rynek targowy?

– Spółka Międzynarodowe Targi Łódzkie ma rzeczywiście duże doświadczenie w działalności na polskim rynku usług targowych. Należymy do grupy dziesięciu wiodących organizatorów w tej branży. Na przestrzeni 20 lat organizowaliśmy różnorodne projekty promujące najważniejsze dziedziny życia gospodarczego. Kalendarz wystawienniczy Spółki zmieniał się wraz z przemianami ekonomicznymi w Polsce. Dlatego pewne projekty należą już do przeszłości, ale ich miejsce zajmują inne, związane z nowymi obszarami biznesu. Jednak w dalszym ciągu kilka imprez stanowi wizytówkę i znak rozpoznawczy Międzynarodowych Targów Łódzkich. Można tu wymienić FILM VIDEO FOTO; Łódzkie Targi Edukacyjne; INTERTELECOM – Międzynarodowe Targi Komunikacji Elektronicznej oraz PET FAIR – Międzynarodowe Targi Zoologiczne. Równocześnie proponujemy udział w nowych imprezach – w 2009 roku będą to m.in.: MOTOMANIA – Salon Motoryzacyjny; URODA i ESTETYKA; NATURA FOOD – Dni Naturalnej Żywności.

Nie jesteśmy, oczywiście, odosobnieni w dążeniu do modernizowania naszej oferty, bo tak postępują wszyscy organizatorzy targów w Polsce. Rynek targowy musi przecież elastycznie reagować na impulsy płynące z gospodarki i uwzględniać oczekiwania firm planujących promocję poprzez udział w targach. W tym kontekście nie powinniśmy lekceważyć negatywnego wpływu kryzysu gospodarczego na rozwój rodzimego rynku targowego. W najbliższym okresie możemy mieć do czynienia z „obroną" osiągniętego *status quo*, ale i zaostrzeniem konkurencji w naszym sektorze; pół biedy, jeżeli będzie to konkurencja uczciwa.

– INTERTELECOM zawsze był sztandarową imprezą organizowaną przez MTŁ. Jak obecnie ocenia Pan te targi poprzez pryzmat branży komunikacji elektronicznej?

– Targi INTERTELECOM były zawsze i są w dalszym ciągu odzwierciedleniem kondycji branży komunikacji elektronicznej w Polsce. Gdy dwadzieścia lat temu Spółka organizowała pierwszy raz tę imprezę, branża łączności uznawana była za priorytetową z punktu widzenia dalszego rozwoju gospodarczego. Zasadnicza modernizacja systemu łączności stała się możliwa dzięki wejściu na polski rynek zagranicznych koncernów, nowych operatorów telefonii kablowej i rewolucji związanej z telefonią komórkową oraz internetem. Wszystkie te zmiany znajdowały odzwierciedlenie w ofercie wystawców łódzkiej imprezy. To tutaj miały miejsce debiuty firm i całych kolekcji nowych wyrobów oraz usług, a targi stanowiły priorytetowy element strategii wizerunkowej firm działających w branży. W chwili obecnej, mimo że obserwujemy stabilizację rynku oraz ograniczenie nowych inwestycji, targi INTERTELECOM są w dalszym ciągu znaczącą formą kontaktów środowisk profesjonalnie związanych z branżą komunikacji elektronicznej.

– Często słychać głosy, że targi nie są już miejscem do zawierania kontraktów i obserwacji rynku, ponieważ większość informacji biznesowych można pozyskać z internetu. Co Pan o tym sądzi?

– Zgadzam się z opinią, że w dobie niezwykłej dostępności do informacji i elektronicznych technik błyskawicznego porozumiewania się targi zmieniły swoją funkcję. Stały się nie tyle okazją do finalizowania kontraktów handlowych, ile miejscem integracji branży. Targi zapewniają wystawcom niezwykłą intensywność kontaktów B2B i B2C. Okazuje się, że w dalszym ciągu obecność na targach ma na celu promocję marki firmy i prezentację nowych produktów. Spotkania ze zwiedzającymi służą poszerzaniu bazy potencjalnych klientów oraz poznawaniu ich opinii o prezentowanej ofercie. Nie bez znaczenia jest także możliwość udziału w branżowych debatach i konferencjach, gdzie spotykają się producenci, naukowcy oraz przedstawiciele instytucji centralnych, struktur samorządowych i mediów.

Z tych właśnie względów nie jestem zwolennikiem poglądu o marginalizacji funkcji targów. W biznesie, a zwłaszcza jego warstwie negocjacyjnej, bezpośrednie kontakty międzyludzkie są nie do zastąpienia; zdobycze komunikacji elektronicznej należy traktować, moim zdaniem, jako istotne ułatwienie w pozyskiwaniu i przepływie informacji.

– Co będzie motywem przewodnim w tym roku na INTERTELECOMIE? Czego mogą się spodziewać uczestnicy i wystawcy tegorocznej edycji targów?

– Jak zawsze, specjalną uwagę przykładamy do skonstruowania interesującego dla uczestników targów programu konferencyjno-seminaryjnego. W tym roku, obok cyklicznych debat przygotowanych przez naszych partnerów, odbędzie się cykl prezentacji pod wspólnym tytułem **„Technologie teleinformatyczne a infrastruktura na EURO 2012 i na innych imprezach masowych"**. Pragnę polecić również organizowaną przez

ITTI prezentację nowych interdyscyplinarnych projektów pod wspólnym tytułem **„Bezpieczeństwo w teleinformatyce”**.

Po raz pierwszy podejmiemy ważną problematykę **ochrony własności intelektualnej w kontekście nowych technologii**. Z pewnością warto rekomendować zwiedzającym premierę **DIALOGmedia (Domowa Platforma Multimedialna)**. To nowy produkt Telefonii Dialog, zapewniający pakiet usług: internet, telefon, telewizja i wypożyczalnia filmów.

Nowością będą, przygotowane przez firmę Interlab, otwarte warsztaty z pomiarów **sieci PON (*Passive Optical Networks* – Pasywne Sieci Optyczne)**. Podane przeze mnie przykłady potwierdzają, że program seminaryjny jest tradycyjnie ważnym czynnikiem wzbogacającym łódzką imprezę.

– Obecnie MTŁ przygotowują się do realizacji dużej inwestycji w infrastrukturę. Czy może Pan powiedzieć kilka zdań o celu tego przedsięwzięcia?

– Z dumą mogę powiedzieć, że finalizujemy prace projektowe związane z budową nowego obiektu targowego w Łodzi. Istniejące hale, a zwłaszcza ich infrastruktura nie spełniają już oczekiwań Spółki, innych organizatorów imprez oraz wystawców. W ostatnim okresie odnotowaliśmy bolesne zjawisko „exportu” realizowanych od wielu lat w Łodzi imprez do innych ośrodków targowych. To duża strata dla naszego miasta i wizerunku Łodzi jako liczącego się centrum targowego.

Decyzja o budowie w Łodzi nowoczesnego, odpowiadającego europejskim standardom centrum wystawienniczo-konferencyjnego była koniecznością, aby w dalszym ciągu można tu było zapraszać firmy z całego świata i oferować warunki odpowiadające oczekiwaniom tak wystawców, jak i zwiedzających.

* * *

– Trwają przygotowania do realizacji nowego Centrum Targowego w Łodzi. Proszę o przybliżenie naszym Czytelnikom, na jakim etapie są prace realizacyjne?

Mirosław Pietrucha – zastępca Dyrektora Generalnego Międzynarodowych Targów Łódzkich

– Najważniejszym momentem było podjęcie decyzji i opracowanie projektu architektonicznego. Obecnie trwają ostatnie ustalenia dotyczące zewnętrznego wyglądu i funkcjonalności nowego obiektu. Będzie on budowany na działce przy ul. Stefanowskiego 17, dlatego nie oferujemy już powierzchni wystawienniczej w Hali Expo Bis, dotychczas stojącej na tej działce.

– Co będzie wchodziło w skład Centrum Targowego?

– Po zakończeniu pierwszego etapu inwestycji Centrum Targowe pozostające w dyspozycji Spółki składać się będzie z dwóch obiektów: Hali Expo (4,4 tys. m^2 powierzchni) i nowej hali (7 tys. m^2 powierzchni wystawienniczej). Docelowo nowy obiekt będzie miał ok. 12 tys. m^2.

Wybudowana hala będzie spełniała wiele funkcji. Powierzchnia ekspozycyjna zostanie wyposażona w taki system podziału, który umożliwi realizację w tym samym czasie nawet czterech niezależnych imprez.

W nowej hali powstaną także nowoczesne sale konferencyjne, w tym jedna dla kilkuset osób. Ponadto w obiekcie znajdzie się część administracyjna z wydzieloną powierzchnią magazynową.

Warto podkreślić, że kubatura i wyposażenie techniczne hali pozwolą na organizowanie nie tylko targów, ale i imprez kulturalnych dla kilku tysięcy osób.

Istotne jest również i to, że hala spełniać będzie obowiązujące standardy; zadbano w niej o wygodę osób niepełnosprawnych, pomieszczenia dla matki i dziecka oraz funkcjonalną infrastrukturę (parkingi, dojazdy, gastronomia, łączność).

– Czy oprócz nowej infrastruktury fizycznej i nowoczesnego zaplecza przewidujecie nową ofertę dla wystawców i uczestników na miarę współczesnych wymagań biznesowych?

– Projekt nowego obiektu zakłada możliwość zintegrowania nie tylko z halą Expo, ale i z halą Miejskiego Ośrodka Sportu i Rekreacji. To z pewnością otworzy perspektywę rozwoju dla nowych projektów. Mamy wiele pomysłów i będziemy je sukcesywnie przedstawiać.

Jesteśmy w trakcie przygotowywania nowej koncepcji naprawdę nowatorskiej formy funkcjonowania targów, ale na konkrety jest jeszcze za wcześnie. Nowy projekt na pewno zmieni podejście do formuły targów. Jestem pewny, że wystawcy w pełni wykorzystają tę nową propozycję dla własnych interesów.

– W jakim kierunku będzie zmierzał INTERTELECOM w następnych latach po realizacji inwestycji?

– Uważam, że nadszedł czas, by firmy w Polsce zdecydowały, czy chcą mieć swoją imprezę branżową. Dla nas bardzo ważne są płynące z firm sygnały, że zaangażowanie w obecność na targach INTERTELECOM jest dla nich w dalszym ciągu istotnym elementem wizerunku i funkcjonowania na polskim rynku.

Nasza Spółka, jako firma w gruncie rzeczy usługowa, będzie robiła wszystko, by branża komunikacji elektronicznej mogła się przekonać, że targi to miejsce gdzie naprawdę można robić „biznes”.

Dla targów INTERTELECOM niezwykle ważny będzie fakt, że oddanie do użytku nowej hali pozwoli na dysponowanie nowoczesnymi salami konferencyjnymi. Będziemy wtedy mogli powrócić do pomysłu zorganizowania przy tych targach dużej ogólnopolskiej lub międzynarodowej konferencji. Będziemy mogli również zaproponować wystawcom przygotowywanie towarzyszących targom eventów promocyjnych dla indywidualnych klientów.

Generalnie chciałbym podkreślić, że sytuowanie imprez targowych w nowej hali wpłynie na standard obsługi wystawców i zwiedzających oraz wizerunek wszystkich imprez organizowanych przez Międzynarodowe Targi Łódzkie.

– Dziękuję Panom za rozmowę.

Raport F-Secure

Bezpieczeństwo internetu

Walka z cyberprzestępczością jest coraz trudniejsza, a ostatnie wyroki sądowe oraz brak koordynacji działań prewencyjnych w skali międzynarodowej jeszcze bardziej ją utrudniają. Oto kilka przykładów z raportu firmy F-Secure.

Phisher zarabia na kryzysie bankowym

Międzynarodowy kryzys bankowy wstrząsnął światową gospodarką. Konsumenci nie mają pewności, który bank utrzymuje w danym tygodniu ich oszczędności lub kredyt hipoteczny. Sytuację tę wykorzystują phisherzy do pozyskania poufnych danych, takich jak numery kont czy kart kredytowych. – *Za przynętę służyły np. e-maile mówiące o sprzedaży Wachovia Corporation do Citibanku. Oszuści próbowali nakłonić odbiorców, żeby pobrali nowy „certyfikat" z podrobionej strony Wachovii. Napastnicy nie tylko gromadzą informacje, ale w ramach ataku instalują także bankowego konia trojańskiego* – wyjaśnia **Sean Sullivan**, doradca ds. bezpieczeństwa w firmie F-Secure.

Amerykańska Federalna Komisja Handlu wydała oświadczenie, nakłaniając użytkowników internetu, aby byli bardzo ostrożni w stosunku do wiadomości e-mail wyglądających jakby wysłała je instytucja finansowa, która niedawno nabyła bank konsumencki, hipoteczny bądź towarzystwo oszczędnościowo-pożyczkowe.

Zbrodnia i brak kary

W ciągu ostatniego kwartału odbyło się kilka interesujących rozpraw dotyczących przestępczości internetowej, które pokazały trudności, jakie wiążą się z wymierzeniem kary cyberprzestępcom. Jednym z przykładów jest sprawa przeciwko spamerowi, zakończona niedawno w Stanach Zjednoczonych. Jeremy Jaynes był pierwszą osobą osądzoną i skazaną na podstawie prawa przeciwko spamowi uchwalonego w 2003 r. Ostatnio odwołał się od wyroku. W trakcie apelacji Sąd Najwyższy w Wirginii uznał, że stanowe prawo antyspamowe naruszało pierwszą poprawkę do amerykańskiej konstytucji, dotyczącą prawa do swobodnej i anonimowej wypowiedzi, następnie we wrześniu uchylił wyrok skazujący spamera na wiele lat więzienia.

Akta procesu pokazują, że nie było wątpliwości co do winy Jaynes'a. Wykorzystał kilka komputerów, routerów i serwerów, żeby przy trzech różnych okazjach wysłać w ciągu 24 godzin ponad 10 tys. wiadomości do abonentów America Online (AOL). Celowo też sfałszował nagłówki informacji oraz domenę nadawcy. Przeszukując dom Jaynes'a, policja odkryła płyty CD zawierające ponad 176 milionów adresów e-mail oraz 1,3 miliarda nazwisk użytkowników poczty elektronicznej. Skonfiskowała także płyty z prywatnymi informacjami dotyczącymi kont milionów abonentów AOL. Informacje o użytkownikach AOL zostały skradzione przez byłego pracownika tej firmy i znalazły się w posiadaniu Jaynes'a.

Zaledwie sześć miesięcy wcześniej ten sam sąd potwierdził ważność przepisów antyspamowych i uznał, że prawa gwarantowane przez pierwszą poprawkę nie dotyczą spamu. Ostatnia zmiana sprowokowała wiele pytań ze strony komentatorów zajmujących się bezpieczeństwem internetowym.

Nastoletni „władca zombie" z Nowej Zelandii

Owen Thor Walker (18 l.) z Nowej Zelandii, znany w internecie pod pseudonimem „AKILL", a przez międzynarodowe media ochrzczony mianem „Nowozelandzkiego władcy zombie", uniknął w lipcu ubiegłego roku kary więzienia, choć wcześniej przyznał się do tworzenia bankowych koni trojańskich, dzięki którym grupa przestępcza zarobiła około 15,4 miliona dolarów. Sąd nakazał nastolatkowi zapłatę odszkodowania i kosztów procesu w wysokości 10 800 USD. Sędzia opisał go jako młodego człowieka mającego przed sobą „potencjalnie świetlaną przyszłość" po tym, jak Walker pomógł policji w prowadzeniu postępowania. Sędzia stwierdził również, że Walker, cierpiący na syndrom Aspergera, czyli łagodną postać autyzmu, hakował z ciekawości, a nie z pobudek przestępczych. Walker został aresztowany po trwającym 18 miesięcy śledztwie, prowadzonym przez nowozelandzkie, holenderskie i amerykańskie władze. Z informacji przekazanych opinii publicznej wynika, że Walker współpracował z amerykańskim studentem, doprowadzając do zainfekowania 1,3 mln komputerów, co naraziło ofiary na koszty w wysokości 20 mln dolarów. Według ostatnich informacji, o Walkera zabiegają teraz duże zagraniczne firmy IT. Lokalna policja także przyznała, że zdolności nastolatka mogą okazać się przydatne.

Scareware i Microsoft

Biuro Prokuratora Generalnego w Waszyngtonie (USA) oraz firma Microsoft niedawno ogłosiły, że składają nowe pozwy skierowane przeciwko twórcom scareware, czyli straszącego oprogramowania. Jego działanie polega na wyświetlaniu niepokojących, a zarazem nieprawdziwych komunikatów, np. o występowaniu błędów. Oskarżonym w jednej z takich spraw jest James Reed McCreary IV. Zarzuca mu się, że wysyłał do użytkowników aplikację generującą wyskakujące okienka, przypominające ostrze-

żenia systemowe. Wyświetlały one komunikat: „WYSTĄPIŁ KRYTYCZNY BŁĄD! – REJESTR ZNISZCZONY I USZKODZONY", a następnie kierowały użytkowników na wskazaną stronę internetową, skąd pobrać można było aplikację Registry Cleaner XP.

– Osobom trafiającym na stronę proponowano darmowe skanowanie sprawdzające ich komputer. Haczyk polegał na tym, że program wykrywał „krytyczne" błędy za każdym razem – powiedziała **Paula Selis**, kierująca działem zaawansowanych technologii w Prokuraturze Generalnej. *– Następnie użytkownicy otrzymywali informację, że mają zapłacić 39,95 USD, żeby naprawić te wątpliwe problemy.* Microsoft twierdzi, że 50 procent wszystkich telefonów do działu pomocy technicznej, związanych z awariami komputerów, można powiązać z oprogramowaniem typu scareware.

Eksperci z Laboratorium F-Secure uważają, że Registry Cleaner XP to tylko jedna z coraz liczniejszej grupy podstępnych, pozornie zabezpieczających aplikacji, obejmujących także takie nazwy, jak Antivirus 2009, Malwarecore, WinDefender, WinSpywareProtect i XPDefender.

Internetpol – pomysł na międzynarodową policję i prokuraturę internetową

Mikko Hypponen, dyrektor ds. badań w F-Secure, uważa, że powinna istnieć międzynarodowa agencja z uprawnieniami do egzekwowania prawa, która stanowczo rozprawiłaby się ze zorganizowaną przestępczością w Sieci.

– Internet nie ma granic, a popełniane w nim przestępstwa niemal zawsze mają charakter międzynarodowy. Tymczasem lokalne oddziały policji często dysponują jedynie ograniczonymi zasobami, które mogą przeznaczyć na prowadzenie śledztw. Nawet jeżeli uda się odszukać sieciowych przestępców, dochodzenia rzadko kiedy odkrywają pełen zakres prowadzonych przez nich działań. Ofiary, policja, prokuratorzy i sędziowie nie mają kompletnego obrazu i dlatego nie są w stanie poznać prawdziwych kosztów tych przestępstw – mówi Hypponen.

– Firmy tworzące systemy antywirusowe i zabezpieczające nie są i nie powinny być stróżami prawa. Zajmują się ochroną komputerów swoich klientów, ale jako organizacje niezwiązane z rządem mogą bardzo niewiele jeżeli chodzi o zwalczanie przestępczości zorganizowanej lub dopiero się organizującej. Powinniśmy rozważyć utworzenie sieciowej wersji Interpolu – „Internetpolu" – którego głównym zadaniem byłoby wykrywanie i dochodzenie aż do samego wierzchołka światka przestępczego – twierdzi Hypponen.

Hypponen zdaje sobie sprawę, że tego typu organizacja na pewno napotkałaby szereg problemów natury prawnej, na przykład złośliwe oprogramowanie jest często tworzone w krajach, w których nie jest to zabronione ani ścigane. *– Jeżeli jednak nie podejmiemy działań zwalczających źródło cyberprzestępczości, to będzie ona rosła w siłę i zagrozi zniszczeniem obecnego modelu internetowej przedsiębiorczości, bankowości i handlu* – podkreśla Mikko Hypponen.

Spam w kampanii prezydenckiej USA

W miarę jak kampania wyborcza w Stanach Zjednoczonych zbliżała się do kulminacyjnego momentu, spamerzy coraz częściej wymyślali sensacyjne nagłówki związane z kandydatami, które miały przekonać ludzi do otworzenia niebezpiecznych wiadomości. Ostatnia odsłona tej kampanii to fałszywa obietnica ujawnienia seksskandalu z udziałem senatora Baracka Obamy, kandydata Demokratów. E-mail z nieprawdziwą wiadomością zawierał załącznik, który prowadził do pornograficznego filmu wideo. Prawdziwy cel tej wiadomości to zainfekowanie komputera trojanem wyszukującym informacje o transakcjach bankowych. Cyberprzestępcy, aby ukryć ten motyw i uniemożliwić użytkownikowi odpowiednio szybką reakcję, spowodowali, że wideo zaczynało się odtwarzać w czasie, gdy trwało pobieranie i uruchamianie złośliwego pliku. W efekcie za każdym razem, gdy użytkownik uruchamiał przeglądarkę Internet Explorer i łączył się z określonymi stronami banków, zwłaszcza dobrze znanymi bankami niemieckimi, trojan zbierał informacje i publikował je na stronie fikcyjnego Hotelu Medved w Finlandii. Układ tej strony wyglądał przekonująco dla nieświadomych użytkowników, ponieważ został ukradziony ze strony prawdziwego fińskiego hotelu.

Powrót niebezpiecznych załączników

W trzecim kwartale 2008 r. Laboratoria F-Secure odnotowały gwałtowne zwiększenie liczby złośliwych aplikacji dostarczanych jako załączniki do poczty elektronicznej. To zaskakujące, ponieważ tego typu załączniki rzadko kiedy trafiają do odbiorców, gdyż są automatycznie usuwane przez dostawców internetu bądź programy pocztowe. W efekcie autorzy złośliwych aplikacji porzucili to podejście i przestawili się na wysyłanie odnośników w e-mailach lub automatyczne pobieranie plików ze stron internetowych z wykorzystaniem luk w zabezpieczeniach.

Ostatnio niebezpieczne załączniki znajdowały się w archiwach, zwykle plikach ZIP, które niestety nie są filtrowane przez większość rozwiązań zabezpieczających. Niektóre z nich wymagały nawet hasła, przez co systemy antywirusowe miały problemy z ich skanowaniem. Nadawcy wiadomości próbują różnych sztuczek, żeby nakłonić użytkowników do uruchomienia takich plików. Udają one m.in. rachunki lub potwierdzenia zapłaty od wielu różnych firm, takich jak JetBlue czy UPS, a także elektroniczne kartki pocztowe. To podejście pod pewnymi względami przypomina oszustwa phishingowe, gdzie wykorzystuje się strach przed utratą pieniędzy, żeby przekonać użytkownika do uruchomienia pliku, który powoduje infekcję. ■

Dla uczniów telefon jest taką samą „zabawką", jak komputer

„Komórkowe" pokolenie

Nowe pokolenie zupełnie inaczej postrzega telefon komórkowy, ale nadal potrzebuje starych dobrych zasad.

Uczeń: U mnie w klasie dwie osoby nie mają komórki.

Rodzic: Mamy kontrolę nad tym, gdzie dziecko pójdzie.

To fragmenty wypowiedzi, które pojawiły się w trakcie pionierskich badań fokusowych, przeprowadzonych przez Instytut Badawczy Millward Brown SMG/KRC oraz CenterNet wśród dzieci w wieku około 10 lat oraz ich rodziców.

Największym motywatorem, decydującym o wyposażeniu dziecka w telefon komórkowy, jest planowana dłuższa rozłąka, np. z powodu wyjazdu na kolonie lub zieloną szkołę. Jednocześnie rodzice coraz rzadziej spotykają się z krytyką takiej decyzji wśród najbliższych – bardzo często chrzestni czy dziadkowie, po konsultacji z rodzicami, wybierają taki prezent.

Z punktu widzenia rodziców, telefon umożliwia dziecku nawiązanie z nimi kontaktu w dowolnym momencie, choć tak naprawdę to dziecko decyduje kiedy rodzic może zadzwonić – dostosowując się np. do godzin zajęć. Jak wynika z badań, bardzo rzadko zdarza się, że dzieci celowo wyłączają aparat, by uniemożliwić rodzicom kontakt, o wiele częściej postępują w ten sposób z natarczywymi kolegami i koleżankami.

Rozmawiać przez telefon – nuda

Jednocześnie, dla uczniów telefon jest taką samą „zabawką" jak komputer czy play-station – im więcej multimedialnych możliwości, tym lepiej. Używanie telefonu w taki sposób, w jaki robią to dorośli, wydaje im się nudne i monotonne. Rodzice również zwrócili uwagę na korzyści płynące z multimedialności telefonów, którymi posługują się ich pociechy, jednak w zupełnie innym aspekcie. Uznali, że mają one wartości poznawcze, które pozwalają dziecku oswoić się z nowinkami technologicznymi i rozwijać pasje, np. fotografowanie.

Rodzice kupują, szkoła uczy

Najczęściej pojawiającym się słowem w ustach rodziców jest „bezpieczeństwo". Jednak mało który ojciec czy matka edukuje dziecko w zakresie posługiwania się telefonem w razie niebezpieczeństwa. Zazwyczaj ograniczają się do wpojenia zasady „jeżeli dzieje się coś złego, zadzwoń do mamy lub taty". Niewielu opiekunów decyduje się na rozmowę z dzieckiem na temat korzystania z numeru 112. Rodzice nie dopuszczają myśli o wypadkach losowych, które mogą spotkać ich dziecko lub uważają, że jest ono za małe, by zrozumieć czym jest numer alarmowy i do czego służy.

Tymczasem dzieci mówią wprost, że oczekują informacji na temat postępowania w sytuacjach zagrożenia, ponieważ chcą czuć się pewnie.

Obowiązek edukacji przejmowany jest więc przez szkołę. Temat bezpiecznego i kulturalnego korzystania z telefonu komórkowego coraz częściej poruszany jest na lekcjach wychowawczych. Towarzyszą im pogadanki z policjantami i strażnikami miejskimi. Dzieci uczą się, że telefon to nie tylko zabawka, ale narzędzie, które w groźnych sytuacjach może uratować komuś życie.

Dziecko nie ma tajemnic

Podczas badań, szeroko omawianą kwestią była cyberprzemoc oraz kontrola zawartości telefonu dziecka. Rodzice przyznają, że mają poczucie dyskomfortu podczas przeglądania zawartości skrzynki odbiorczej lub sprawdzania listy połączeń, ale w większości przypadków dzieci o tym wiedzą, bo takie zasady zostały ustalone wcześniej. Bardzo często zdarza się tak, że dziecko samo przybiega pochwalić się, co właśnie otrzymało od kolegi z klasy, nawet jeżeli jest to coś niestosownego. Jak podkreślają rodzice, w wieku wczesnoszkolnym ich pociechy nie mają jeszcze tajemnic.

Postęp technologiczny sprawił, że dzieci zupełnie inaczej patrzą na elektroniczne urządzenia. Są to dla nich rzeczy naturalnie dostępne. I tylko od nas zależy czy za „naturalnością" użytkowania, będzie stało również bezpieczeństwo.

Okazuje się również, że korzystanie z telefonu komórkowego może być znakomitym pretekstem do dialogu między pokoleniem młodych i starszych użytkowników. Młodzi ludzie potrzebują starych dobrych zasad, natomiast rodzice chętnie skorzystają z wiedzy dzieci na temat możliwości wykorzystania nieznanych im funkcji telefonów komórkowych.

Badanie z grudnia 2008 roku, jest pierwszym tego typu publikowanym w Polsce. Zostało przeprowadzone na potrzeby akcji firmy CenterNet – Moja Pierwsza Komórka, której celem jest rozpropagowanie zasad bezpiecznego i racjonalnego korzystania z telefonu komórkowego przez dzieci. Trwa ona od września 2008 roku i jak zapowiada organizator będzie kontynuowana również w roku 2009. ■

Konsumenci na rynku telefonii ruchomej

Preferencje użytkowników komórek

Analiza Urzędu Komunikacji Elektronicznej dotycząca preferencji konsumentów korzystających z usług dostępnych na rynku telefonii ruchomej w Polsce.

Przeprowadzone w latach 2006-2007 na zlecenie Urzędu Komunikacji Elektronicznej badania opinii publicznej wykazały wysoki stopień rozpoznawalności marek operatorów telefonii ruchomej w Polsce (Era – 90,2 proc., Plus – 88 proc., Orange – 87,1 proc., Play – 54 proc., w 2007 roku). Tak wysoki stopień świadomości konsumenckiej wiąże się ze znacznymi nakładami operatorów telefonii ruchomej na marketing, w tym na reklamę (16 proc. udziału branży telekomunikacyjnej i 13 proc. samego segmentu telefonii ruchomej, w całkowitej wielkości sprzedaży branży reklamy zewnętrznej w Polsce w pierwszym kwartale 2008 roku). Wystarczy dodać, iż trzej najlepiej rozpoznawalni operatorzy telefonii ruchomej znaleźli się w lipcu 2008 roku w pierwszej piątce marek o największych wydatkach na reklamę w telewizji. Działania operatorów są tym bardziej uzasadnione, iż zdecydowana większość (aż 83,3 proc. w 2007 roku) Polaków czerpie informacje o ofertach operatorów właśnie z radia i telewizji.

Walka o klienta sieci podyktowana jest wysokim stopniem nasycenia rynku po stronie popytu (penetracja na poziomie 108,6 proc. na koniec 2007 roku), gdzie w dalszym ciągu wyraźnie widoczna jest ilościowa dysproporcja w profilach użytkowników sieci. Według badania konsumenckiego, respondenci w zbliżonym stopniu wykorzystywali w 2007 roku usługi abonamentowe – 51,9 proc. i przedpłacone – 43,4 proc., jednak wyniki te nie odzwierciedlały rzeczywistej struktury baz abonenckich operatorów, w których dość wyraźnie przeważali użytkownicy telefonów na kartę – 26,7 miliona wobec 14,8 miliona klientów abonamentowych w 2007 roku.

Przyczyny tej dysproporcji wynikają z działań zarówno operatorów, jak i konsumentów. Operatorzy ostatnimi laty koncentrowali się na pozyskiwaniu i utrzymywaniu w sieci głównie mniej lojalnych – z racji braku długoterminowej umowy – klientów usług przedpłaconych. Dodatkowo konsumenci (zarówno pre-paid jak i post-paid) nie wykazywali skłonności do zmiany dostawcy, co potwierdzało 83,5 proc. ankietowanych, którzy nie rozważali w 2007 roku rezygnacji z usług własnego operatora, oraz 87,5 proc., którzy nie planowali zakupu lub dokupienia telefonu. Według prognoz, omawiana dysproporcja może utrzymać się nawet do 2012 roku, o ile operatorzy nie rozpoczną aktywnej walki o utrzymanie w sieci klientów abonamentowych.

Warto dodać, iż w latach 2006-2007 blisko 3-krotnie wzrosła liczba przeniesionych numerów i, chociaż nadal mniej niż 1 proc. użytkowników decyduje się na tę usługę, dynamiczny wzrost zainteresowania nią, dodatkowo przy planowanym przez UKE skróceniu czasu jej trwania, może w przyszłości skutkować większą skłonnością konsumentów do zmiany sieci. To wymusi jeszcze aktywniejszą rywalizację rynku po stronie podaży, również o klientów abonamentowych, którzy, choć mniej liczni, wydają miesięcznie na usługi telefonii ruchomej zdecydowanie więcej niż klienci usług przedpłaconych (90,7 PLN wobec 50,6 PLN w 2007 roku).

Decydującym kryterium wyboru oferty operatora w dalszym ciągu pozostaje koszt korzystania z telefonu (w 2007 roku 67,5 proc. ankietowanych wskazało cenę jako bardzo ważną przy wyborze oferty, a 63,5 proc. badanych atrakcyjność promocji i rabatów). Stąd też głównym narzędziem omawianej powyżej rywalizacji operatorów o klientów sieci z pewnością będzie cena najpopularniejszych usług, a więc połączeń głosowych (73,3 proc. respondentów wskazało jako najczęściej wykorzystywane w 2007 roku) oraz wiadomości SMS (29,6 proc.), które chociażby w ofertach roamingowych operatorów Unii Europejskiej i Europejskiego Obszaru Gospodarczego pozostawały w kwartale br. na zdecydowanie wyższym poziomie aniżeli oczekiwania respondentów w 2007 roku.

Walka cenowa może też w pewnym stopniu objąć swym zasięgiem usługi niszowe, jak wiadomości MMS (tylko 0,2 mld MMS-ów wysłanych w 2007 roku wobec 38,8 mld SMS-ów) oraz WAP/Internet (tylko 0,3 proc. ankietowanych w 2007 roku wskazało usługę jako najczęściej wykorzystywaną). W zakresie konkurencji cenowej operatorów w dalszym ciągu jest więc o co grać, zwłaszcza iż, wg prognoz, miesięczne wydatki aktywnych klientów sieci będą rosły z ok. 43 PLN w 2007 roku do blisko 48 PLN w roku 2012, a wydatki detaliczne wszystkich klientów sieci na usługi telefonii ruchomej z ok. 19 mld PLN do ok. 26 mld PLN.

W najbliższym czasie nie można również wykluczyć zorientowania ofert operatorów na zmniejszający się, ale wciąż istniejący segment konsumentów nie korzystających z telefonu komórkowego. Chociaż znaczna część, bo 45 proc., respondentów w 2007 roku nie posiadających telefonu komórkowego deklarowała, iż wystarcza im telefon stacjonarny, a 32,1 proc. deklarowało rzadkie korzystanie z usług telefonicznych, to 26,3 proc. badanych za główny powód braku komórki podawało zbyt wysokie koszty. Z pewnością ta właśnie grupa może w pierwszej kolejności zmienić zdanie wskutek dalszych obniżek cen usług przez operatorów, zwłaszcza iż większość społeczeństwa – 54,7 proc. ankietowanych w 2007 roku – uznaje posiadanie telefonu komórkowego za bardzo istotne, co świadczy o powszechnej akceptacji usług telefonii ruchomej i częściowo o postępującym rozwoju społeczeństwa informacyjnego w Polsce.

Pełna treść analizy preferencji konsumentów jest dostępna na stronie internetowej UKE. ■

Nowe technologie w naszych domach

Grzegorz Kantowicz

Wi-Fi oraz laptopy na topie

W ciągu minionego roku liczba notebooków w polskich domach niemal się podwoiła – wynika z badania D-Link Technology Trend (DTT), przeprowadzonego na zlecenie firmy D-Link przez Millward Brown SMG/KRC. Obecnie notebookami dysponuje 11 procent gospodarstw domowych, a w co szóstym domu z dostępem do internetu funkcjonuje sieć bezprzewodowa.

Więcej laptopów, więcej Wi-Fi

Wśród nowoczesnych urządzeń technologicznych w ciągu minionego roku zdecydowanie wzrosła liczba posiadanych przez Polaków notebooków (z 6 do 11 proc. w porównaniu z badaniem z czerwca 2007 roku), telewizorów HD lub HD ready (również z 6 do 11 proc.) oraz odtwarzaczy multimedialnych, m.in. DVD (z 20 do 30 proc.). Natomiast po raz pierwszy zanotowano niewielki spadek liczby komputerów stacjonarnych (z 45 do 44 proc.), będący efektem bardziej przystępnych cen komputerów przenośnych.

Mariusz Piaseczny,
PR Manager firmy D-Link w Europie Wschodniej

Na tak szybko rosnącą popularność sprzętu hi-tech mają wpływ przede wszystkim czynniki finansowe: spadek cen urządzeń połączony z umocnieniem kursu złotego i wzrostem zarobków Polaków. Jeszcze dwa lata temu komputer przenośny był poza zasięgiem przeciętnej rodziny. Dziś, gdy przyzwoitej klasy notebook kosztuje poniżej 2 tysięcy złotych, czyli mniej więcej tyle, ile komputer klasy PC, naturalny jest spadek popularności „blaszaków", które w domu są kolejnym meblem. Kupując laptopa Polacy wybierają urządzenie zajmujące zdecydowanie mniej miejsca, mobilne i równie wydajne co komputer stacjonarny.

Z tego trendu korzystają nie tylko dostawcy notebooków, ale też producenci urządzeń do budowy domowych sieci bezprzewodowych. Sięgając po mobilnego notebooka Polacy chcą mieć dostęp do internetu nie tylko przy domowym biurku, ale też w salonie czy w kuchni. Jak na razie, swoją szansę nie do końca wykorzystują operatorzy telefonii komórkowej, oferujący dostęp do internetu w technologii 3G. To efekt dość słabej jakości tych usług, a przede wszystkim bardzo ograniczonego zasięgu szybkiej transmisji i stosunkowo wysokich cen.

Wzrostowi popularności notebooków sprzyja także rozwój domowych sieci Wi-Fi. Obecnie sieci bezprzewodowe znajdują się w 15 proc. gospodarstw domowych z dostępem do internetu. To 6-procentowy wzrost w stosunku do 2007 roku. W kolejnych 43 proc. domów znajduje się sieć przewodowa. Według deklaracji ankietowanych, liczba wszystkich sieci domowych wzrosła w ciągu roku o 14 proc. (z 44 do 58 proc.).

Gry nie tylko dla młodzieży

W badaniu D-Link Technology Trend zadano także pytania dotyczące rozrywki elektronicznej. Do grania na komputerze przyznaje się 13 proc. wszystkich Polaków, czyli co czwarty posiadacz komputera (26 proc.). Ponad połowa graczy (51 proc.) nie skończyła jeszcze 25 roku życia, ale co ósmy (13 proc.) ma powyżej 40 lat.

Podobnie wygląda struktura wiekowa wśród osób prowadzących rozgrywkę w sieci, czyli z innymi graczami, za pośrednictwem internetu (2 proc. wszystkich Polaków). Tu również przoduje młodzież (66 proc. to gracze poniżej 25 lat), ale i tutaj co ósmy gracz ma więcej niż 40 lat. Z kolei grę na konsolach do gier deklaruje obecnie 3 procent Polaków, wśród tej grupy nie ma czterdziestolatków.

Operatorzy kablowi gonią ADSL

Według badań, 38 proc. gospodarstw domowych posiada dostęp do internetu. Najpopularniejsze w Polsce są wciąż łącza ADSL dostarczane przez operatorów telekomunikacyjnych (m.in. TP, Netia, Tele2). Z takiego połączenia korzysta ponad 1/3 gospodarstw (37 proc. zarówno w 2007 roku, jak i obecnie), a jego popularność jest odwrotnie proporcjonalna do wielkości miejscowo-

ści. Na terenach wiejskich łącza ADSL stanowią 56 proc., w małych miastach (do 100 tys. mieszkańców) – 44 proc., a w aglomeracjach miejskich (pow. 500 tys. mieszkańców) już tylko 17 proc. wszystkich łączy internetowych.

Największy przyrost zanotowali operatorzy telewizji kablowych – z 22 proc. w 2007 roku do 25 proc. obecnie. Internet z kablówki jest najbardziej popularny w największych miastach (pow. 500 tys. mieszkańców) – 51 proc oraz w miastach od 100 do 500 tys. mieszkańców – 36 proc.

Dość popularne są wciąż łącza operatorów osiedlowych (15 proc. wszystkich łączy internetowych), szczególnie w średnich miastach (100-500 tys. mieszkańców), gdzie co czwarte łącze (24 proc.) pochodzi właśnie od dostawcy osiedlowego. Na rynku dostawców szerokopasmowego dostępu do internetu wzrósł także udział operatorów komórkowych – z 3 proc. w 2007 roku do 5 proc. obecnie – spada zaś popularność modemów (z 11 do 7 proc.) oraz dostawców internetu bezprzewodowego (z 8 do 5 proc.).

Badanie D-Link Technology Trend na temat posiadanych urządzeń elektronicznych oraz dostępu do sieci przeprowadzono w dniach 17-23 lipca 2008 r. na reprezentatywnej grupie 998 osób w wieku 15-75 lat. ■

Kuba Antoszewski
MillwardBrown SMG/KRC

Wygląda na to, że Polacy postanowili skorzystać z umacniania się złotego i spadku cen w Europie i USA. Elektronika wydaje się najlepszym „łupem". Zakup, również za pośrednictwem internetu, jest prosty, zwłaszcza jeśli sprowadza się towar z zagranicy. Jest to proces podobny do tego, który już od ok. dwóch lat obserwujemy na rynku samochodów. Większe zainteresowanie sprzętem komputerowym tłumaczy z pewnością znaczący wzrost od początku 2008 roku liczby internautów w Polsce, w porównaniu z rokiem 2007. Prócz tego jednak wydaje się, że obecnie mobilność staje się czynnikiem dominującym w zakupach Polaków w obszarze informatyki. Widać to zarówno po znaczącym wzroście liczby posiadanych przez Polaków notebooków, jak i spadku liczby komputerów stacjonarnych. Co za tym idzie – rośnie też liczba urządzeń do rozsyłania internetu bezprzewodowo. Biorąc pod uwagę rosnącą popularność internetu i ciągłe umacnianie się polskiej waluty, należy się spodziewać utrzymania tego trendu. To dobrze, bo wydaje się, że obecnie w Polsce podstawową barierą dla szybszego rozwoju internetu są pieniądze. Należałoby oczekiwać, aby za korzystnymi cenami internetowej elektroniki szła również polityka providerów dalszego obniżania cen dostępu do internetu.

Nowe technologie szerokopasmowe

Mieczysław Borkowski

Dla polskiej telekomunikacji

W październiku ubiegłego roku Nokia Siemens Networks zaprezentowała w Warszawie kilka swoich wysoce zaawansowanych technologicznie rozwiązań. Między innymi była to platforma Long Term Evolution (LTE) oraz Telewizja Przyszłości. Oba te rozwiązania wyznaczają najnowsze trendy w dziedzinie telekomunikacji.

Do 2015 roku ponad 5 miliardów ludzi będzie połączonych w sieci umożliwiającej swobodną komunikację. Około 4 miliardów osób będzie dysponowało szerokopasmowym dostępem do internetu, gdzie znajdą olbrzymią liczbę aplikacji. Spowoduje to stukrotny wzrost wolumenu transmisji danych.

Taka wizja przyświeca firmie współpracującej z dostawcami usług telekomunikacyjnych oraz przedstawicielami władz, starając się wspólnie opracować innowacyjne, oszczędne i przyjazne dla środowiska rozwiązania.

Sektory informatyki i telekomunikacji przechodzą szybką transformację. Rośnie wolumen transferu danych, co dla dostawców oznacza wymóg modernizacji sieci, natomiast konsumenci żądają niższych opłat za lepszej jakości usługi. Dostawca staje wobec wyzwania rozwijania zakresu usług przy jednoczesnym kontrolowaniu kosztów. Jedynie nowe źródła przychodów mogą pomóc w rozwiązaniu tego dylematu.

LTE – lider technologiczny

Dzięki współpracy z dostawcami usług telekomunikacyjnych na całym świecie, w tym z czołowymi polskimi operatorami, Nokia Siemens Networks jest gotowa do wprowadzenia Long Term Evolution. Po kolejnych instalacjach testowo-pilotażowych w 2009 roku możliwe będą pierwsze komercyjne podłączenia u operatorów mobilnych, pragnących przeprowadzić migrację do płaskiej sieci opartej w całości na protokole internetowym (IP). Taka architektura sieci, łatwo skalowalna i bardziej ekonomiczna, pozwala na szerokopasmowe mobilne usługi multimedialne, z wysoką prędkością przesyłu danych. Przygotowana jest właśnie na prognozowany stukrotny wzrost wolumenu transferu.

Firma zainaugurowała też w lutym 2008 roku całościowe rozwiązanie LTE oparte na Flexi Multimode Base Station, małej stacji bazowej stworzonej na platformie Flexi BTS.

LTE pomaga użytkownikom w korzystaniu z różnych aplikacji w sieci komórkowej, zapewniając szybki czas reakcji, wysoką przepustowość sieci, a także prędkości do 173/58 Mbps (downlink/uplink). Pozwala na mobilny dostęp szerokopasmowy do aplikacji: przeglądanie internetu, e-mail, wymiana plików wideo, pobieranie plików muzycznych itp. Usługi te mogą być dostarczone przez operatora. Dostępne są również w internecie.

Szczególnymi adresatami tego rozwiązania są operatorzy modernizujący swoje sieci GSM/WCDMA/ HSPA oraz CDMA, potrzebujący szybkich usług internetowych w ramach mobilnego dostępu szerokopasmowego. Flexi Base Station może być stosowane w ramach sieci WCDMA/HSPA, a później dostosowane do technologii LTE za pomocą odpowiedniego oprogramowania.

Światowa łączność staje się obciążeniem dla gospodarki i środowiska, a to za sprawą rosnącego poboru energii elektrycznej i związanej z tym emisji CO_2. Około 86 proc. energii pobieranej przez operatora zużywa sieć. Nokia Siemens Networks pracuje nad minimalizacją tego zjawiska dzięki nowoczesnym stacjom bazowym. Flexi Base Station automatycznie przechodzi w stan oszczędnościowy poza godzinami szczytu, co zmniejsza koszty operatora i pośrednio oszczędza środowisko. Dalsze zmniejszenie zużycia energii daje ograniczenie temperatury pracy stacji do 40°C. Oszczędności energetyczne tej stacji sięgają 70 proc. Firma używa też materiałów bezpiecznych dla środowiska.

Telewizja przyszłości

Połączenie telewizji mobilnej w standardzie DVB-H oraz IPTV tworzy interaktywną telewizję przyszłości. Szacunkowa wielkość światowego rynku telewizji mobilnej i usług wideo sięga 7 miliardów euro. Konieczne jest kompletne, oszczędne rozwiązanie w tym zakresie. Telewizja mobilna jest jedną z najbardziej ekscytujących nowych usług. Pojawiła się w wyniku szybkiego rozwoju technologii. Prostota działania, a jednocześnie wrażenie wywierane na użytkownikach dają operatorom możliwości zdobycia nowych źródeł przychodów. Według prognoz branżowych, już w 2011 roku około pół miliarda ludzi będzie oglądało transmisje w telefonach komórkowych.

Aktualnie ponad 30 operatorów korzysta z technologii telewizji mobilnej w systemie Unicast, dostarczonej przez Nokia Siemens Networks. Standard DVB-H używany jest komercyjnie przez operatorów w Finlandii, Indiach, Malezji, Szwajcarii oraz Holandii, zaś instalacje pilotażowe działają u ponad 20 operatorów i zapewniają dostęp do programów o każdej porze i w każdym miejscu. Dają też możliwość interaktywnej reklamy. ■

3Com zwiększa wsparcie dla energooszczędnego IT

Grzegorz Kantowicz

Środowiska sieciowe a zużycie energii

W dzisiejszym, pełnym wyzwań, środowisku ekonomicznym konieczne jest wielopłaszczyznowe, holistyczne podejście do wdrażania rozwiązań sieciowych. Aby wspomóc menedżerów IT, firma 3com, członek organizacji Green Grid, przygotowała klika wskazówek służących do skierowania organizacji na drogę zrównoważonego ekologicznie rozwoju.

Według najnowszego raportu firmy badawczej IDC, to infrastruktura sieciowa w firmach może być głównym czynnikiem przyjaznego środowisku IT i to na każdym etapie działalności – od zarządzania dostawami, poprzez komunikację, a na indywidualnych pracownikach kończąc. Właśnie zmiany i inwestycje w tej dziedzinie dają również widoki na zmniejszenie gigantycznej sumy sześciu miliardów dolarów, jaką pochłonęło zasilanie centrów danych w samej tylko Europie w 2007 roku.

Robert Kogut z 3Com wymienia kilka sposobów na korzystne dla firmy i środowiska wdrożenie energooszczędnej infrastruktury sieciowej:

- Przejście na Voice over IP, co czyni możliwym wykorzystanie w pełni potencjału telekonferencji. Badanie wykonane przez IDC pokazuje, że dopiero 32 proc. firm wdrożyło VoIP i tylko 15 proc. korzysta z niego do wirtualnych spotkań i telekonferencji. Z powyższych danych wynika olbrzymi potencjał oszczędności na kosztach podróży w przypadku skutecznego wdrożenia komunikacji IP.
- Wdrożenie technologii takich, jak Power over Ethernet, które pozwalają przykładowo wyłączyć zasilanie telefonów IP, gdy nie są one w użyciu.
- Zaplanowanie już dziś pełnego wykorzystania energooszczędnego Ethernetu, żeby móc w pełni wykorzystać jego potencjał w momencie ratyfikacji tego standardu w 2010 roku.
- Wybór dostawcy sprzętu sieciowego, który oferuje energooszczędne udoskonalenia na poziomie procesorów, pamięci i zasilania urządzeń. Ponieważ z każdą generacją produktów oszczędności w przypadku sprzętu sieciowego są większe niż w przypadku samych komputerów, również ich przełożenie na budżet jest bardziej odczuwalne.
- Uczynienie usług i aplikacji sieciowych, takich jak optymalizacja WAN, częścią infrastruktury sieciowej dzięki rozwiązaniom zintegrowanych sieci.
- Unowocześnienie infrastruktury sieciowej. Przykładowo – wymiana switchów starszej generacji, takich jak m.in. switch 3Com 4924 na 3Com 4200G, w typowej firmowej sieci LAN na 100 switchów ethernetowych 2000 węzłów sieci może dać oszczędności roczne rzędu 77890 kilowatogodzin, czyli tyle energii, ile potrzeba do zasilania 62 domostw przez cały rok.

Firma 3Com stoi na stanowisku, że większość firm nie może dziś czerpać pełnych korzyści z przyjaznego środowisku IT, ponieważ ich podejście do „zielonych" technologii jest jedynie wycinkowe. Dopiero podejście holistyczne, którego motorem będzie IT, może przełożyć się na oszczędność energii i pieniędzy oraz na spełnienie celów ekologicznych, jakie stawiają sobie rządy i ustawodawcy.

– *Firmy powinny w przypadku przyjaznego środowisku IT postarać się unikać podejścia opartego na „odhaczaniu" kolejnych punktów* – stwierdza **David Law**, przewodniczący Grupy Roboczej Ethernet w IEEE 802.3, a także przedstawiciel 3Com w Green Grid. – *Proekologiczne ustawy są bez wątpienia czynnikiem zmian w wielu firmach, ale skupienie się na nich i powolne dostosowywanie do nich pozbawia organizacje szansy na pełne skorzystanie z oszczędności, które mogłyby zaistnieć już dziś.*

– *Głównym zmartwieniem menedżerów IT w dużych firmach jest dzisiaj energia elektryczna – jej dostarczanie, zarządzanie i oszczędzanie* – mówi Law. – *Znaczenie tego zagadnienia będzie z pewnością coraz większe z każdym rokiem. Menedżerowie IT muszą śledzić zużycie energii dzisiaj, ale także analizować zapotrzebowanie na nią, które w ich firmie wystąpi jutro. W większości wypadków przyjdzie im brać pod uwagę czynniki finansowe, a także coraz częściej te dotyczące ochrony środowiska.* Infrastruktura sieciowa jest kluczem do zmniejszenia zużycia energii elektrycznej i zjawiska jej marnotrawstwa, ponieważ umożliwia bardziej efektywną komunikację. Możemy oczekiwać, że w przyszłości nowoczesne sieci pozwolą na zastąpienie na dużą skalę podróży komunikacją cyfrową, a także udostępnią pracownikom pracującym na odległość optymalizację WAN, wideokonferencje i dostęp do skonsolidowanych centrów danych.

Więcej na temat Green Grid

Green Grid to globalne konsorcjum firm zaangażowanych w promowanie energooszczędnych centrów danych i komputerowych ekosystemów. Green Grid nie preferuje rozwiązań ani produktów konkretnych firm, stara się natomiast wyszukiwać i rekomendować najlepsze praktyki i technologie, które poprawią efektywność centrów danych. Członkostwo jest dostępne dla wszystkich firm zainteresowanych operacyjną efektywnością centrów danych i może występować na poziomie Członka Generalnego lub Kontrybuującego. Członkowie Generalni biorą udział w spotkaniach Green Grid, w ocenie propozycji i specyfikacji, mają też dostęp do specyfikacji dla celów testowych, wytycznych projektowych i licencjonowania IP. Dodatkowe przywileje Członków Kontrybuujących obejmują udział i prawo głosu w komitetach i grupach roboczych. Więcej informacji pod adresem www.thegreengrid.org. ■

Usługi finansowe operatorów i płatności mobilne

Mieczysław Borkowski

Karta kredytowa sposobem na lojalność

W dzisiejszych czasach proces indywidualizacji towarzyszy nam niemal na każdym kroku i w każdej dziedzinie życia. Klienci, bez względu na to czy chodzi o kupno pakietu telewizji kablowej, zmianę abonamentu w telefonie, czy założenie konta bankowego, oczekują spersonalizowanego traktowania i „uszytej na miarę" oferty uwzględniającej ich konkretne potrzeby. Z biznesowego punktu widzenia, takie oczekiwania konsumenckie stwarzają konkretny obszar do współpracy firm z sektora finansowego z operatorami komunikacji elektronicznej.

W przypadku Polski stale mówi się o stosunkowo młodym rynku finansowym, ale – co ważne – jest to rynek bardzo otwarty na innowacje i niestandardowe rozwiązania. W najbliższym czasie, w ramach takich nieszablonowych rozwiązań, na naszym rynku powinny pojawić się pierwsze karty kredytowe wydawane przez trzech partnerów – sieć kablową, instytucję finansową (bank) oraz system płatniczy. Czy i komu może się takie „karciane" przedsięwzięcie opłacać?

Dostrzec potrzeby konsumenta

Karta płatnicza, a właściwie wyciąg z konta karty, może być kopalnią dogłębnej wiedzy o zachowaniach i preferencjach klientów. Nikogo już chyba nie trzeba przekonywać do tego, że aby zbudować lojalność klientów, trzeba nie tylko odpowiadać, ale wręcz kreować ich potrzeby. Czasy budowania strategii w oparciu o dane demograficzne są już definitywnie historią. W dzisiejszych czasach, aby pozyskać klienta na dłużej i sprawić, by stał się nie tylko jednorazowym użytkownikiem, ale ambasadorem marki, trzeba umieć wejść w jego skórę, tzn. zacząć myśleć jak on i mówić do niego zrozumiałym językiem, a więc takim, jakim sam się posługuje. Gdzie szukać informacji o stylu życia potencjalnego konsumenta? Na przykład w jego portfelu, a precyzyjniej, na wyciągu z rachunku jego karty płatniczej. Interesującą z punktu widzenia dostępności danych metodę wykorzystuje aplikacja Customer Insight firmy 5ne z grupy LaSer. W ramach tzw. *customer knowledge* wspólna agenda dla działów zarządzania kategoriami marketingu i dostawców pozwala firmie na dostosowanie kwestionariusza danych pozyskiwanych od klientów (użytkowników kart płatniczych) do priorytetów biznesowych firmy. W kwestionariuszach klientów, oprócz podstawowych danych demograficznych, mogą się także pojawić rozmaite informacje dodatkowe, dotyczące m.in. zwyczajów zakupowych, responsywności na akcje promocyjne, reakcji na oferty itp.

Większe możliwości

Jak taki system może zadziałać w odniesieniu do sektora telewizyjnego? Dysponując danymi pochodzącymi z karty płatniczej, możemy m.in. sprawdzić i porównać poziom wydatków obecnego abonenta w dłuższej perspektywie, jak i to, czy swoje zobowiązania spłaca terminowo. Wyciąg z konta karty może nam także wiele powiedzieć o jego preferencjach zakupowych, ułatwić określenie całościowego „modus vivendi" widza. Na podstawie historii płatności kartą możemy zbadać nie tylko to, gdzie i za jakie dobra dana osoba płaci regularnie swoją kartą, czy z jakich usług korzysta, ale również to, czy nasz klient podróżuje, a jeśli tak, to czym.

Dzięki precyzyjnym danym pochodzącym z wyciągu z karty płatniczej jesteśmy także w stanie wywnioskować, czy nasz widz, robiąc zakupy, kieruje się jakąś konkretną filozofią (np. wybiera produkty ekologiczne, dobra z konkretnych regionów świata lub usługi świadczone przez konkretne grupy zawodowe). Zbiór takich informacji to istna kopalnia wiedzy i inspiracji służąca do tego, aby na ich bazie przygotować zindywidualizowaną ofertę uwzględniającą potrzeby konkretnych segmentów klientów. W jej skład mogą wejść np. specjalne akcje promocyjne z lokalnymi sieciami handlowymi. Wystarczy tu tylko prześledzić wyciągi pod kątem zakupów konkretnych produktów czy marek, aby potem skierować do ich nabywców taką „uszytą na miarę" akcję. Czy jednak potencjalni użytkownicy takich kart będą chcieli powierzyć objęte dotąd tajemnicą bankową dane operatorom? Jeśli tak, to karta kredytowa może być, z powodzeniem, paszportem nawet do najbardziej rozbudowanego programu lojalnościowego. Przykładem jest karta Real MasterCard wydawana przez Sygma Bank Polska, część grupy LaSer. Dzięki zastosowaniu podwójnej identyfikacji klientów, paska magnetycznego oraz kodu kreskowego jest ona typowym środkiem płatniczym, jak również kartą lojalnościową pozwalającą klientowi zbierać punkty w programie Dziesiątka Real. Również dzięki zastosowaniu technologii chipowej podstawowe cechy płatnicze kart mogą zostać z łatwością uzupełnione o dowolny dodatkowy program lojalnościowy. Tak funkcjonują karty wspólnych marek, tzw. *karty co-branded*.

Z biznesowego punktu widzenia, taki sprofilowany na potrzeby telewidzów program lojalnościowy z kartą kredytową może zwiększyć sprzedaż usług oraz pozwolić na uzyskanie większej interakcji z odbiorcami. Multifunkcjonalność karty jako cecha, która daje widzowi dostęp do wielu usług w jednym prostym narzędziu, to także gwarancja większej satysfakcji użytkownika. Z kartą tą może on, przykładowo, płacić za różnego rodzaju zakupy, regulować płatności za abonament, zbierać punkty, czy też korzystać z rabatów na określone programy nawet bez wychodzenia z domu.

MasterCard Sky Card – doświadczenia brytyjskie

Ciekawym przedsięwzięciem z pogranicza finansów i mediów, z biznesowego punktu widzenia, jest karta Sky Card. Karta została wprowadzona przez trzech partnerów: Sky TV, Barclay Bank i MasterCard. Jest to karta kredytowa z programem lojalnościowym umożliwiającym gromadzenie punktów, tzw. SkyPoints. Dla Sky TV wydawnictwo własnej karty płatniczej było przede wszystkim szansą na zwiększenie lojalności i przychodów w przypadku posiadanych klientów oraz zdobycie, dzięki innowacyjnej technologii, nowych abonentów.

W krótkim czasie okazało się, że interaktywna karta z bogatym programem lojalnościowym bardzo spodobała się widzom Sky TV, a jednocześnie pomogła zdobywać nowych abonentów. Sky TV zyskała m.in. 1,5 milionów nowych użytkowników/kont oraz średnie saldo na aktywnej karcie na poziomie 1600 funtów.

Aby rozpocząć ich gromadzenie, użytkownik karty musi po prostu za codzienne zakupy płacić kartą Sky Card. Za każdy 1 funt wydany na zakupy przy użyciu karty Sky Card otrzymuje on 1 punkt – tzw. SkyPoint. Zgromadzone punkty można następnie wymienić na 4 kategorie nagród, takich jak m.in. rabat na abonament za Sky TV, filmy dostępne w ramach Sky Box Office Movies, miesięczny dostęp do wybranych kanałów TV. Zebrane punkty można nawet wymienić na kilka wariantów imprez dostarczających bezcennych emocji, takich jak wycieczka do Paryża na turniej tenisowy ATP Masters czy uczestnictwo w BRIT Awards w strefie VIP.

Szybkość i wygoda płatności bezstykowych PayPass

Karty płatnicze, choćby takie jak karta Sky, to również szybkie płatności za codzienne zakupy, rachunki czy inne zobowiązania. W czasie gdy wszystko można załatwić za pomocą internetu lub telefonu, zwykłe zakupy robimy w biegu, ciągłe kolejki w sklepach odstraszają przecież wielu klientów. Dlatego także w usługach finansowych następuje ewolucja w stronę rozwiązań jak najmniej czasochłonnych i najbardziej wygodnych.

W celu ułatwienia płatności kartą za drobne codzienne zakupy MasterCard wprowadził technologię płatności zbliżeniowych PayPass. Korzystając z takiej karty użytkownik może płacić za drobne zakupy (do 50 zł) bez konieczności szukania drobnych, podawania kodu PIN, czy składania podpisu na papierowym potwierdzeniu transakcji.

Do wykonania płatności wystarczy tylko zbliżenie karty do specjalnego czytnika PayPass. To rozwiązanie pozwala na szybkie, łatwe i bezpieczne płatności. Taka forma zakupów zajmuje znacznie mniej czasu niż zapłata gotówką, a w czasie transakcji właściciel nawet nie wypuszcza swojej karty z ręki.

W Polsce kartę w technologii zbliżeniowej MasterCard PayPass wprowadzono w 2007 roku, była to pierwsza taka karta wydana w Europie Środkowo-wschodniej.

Zbliżeniowa karta Maestro® PayPass™ jest kartą przedpłaconą, którą można otrzymać bez otwierania konta. Aby nią płacić, należy ją zasilić gotówką bądź przelewem na bankowy numer dołączony do karty. Jej obsługa jest na tyle prosta, że nie odstraszy nawet największego przeciwnika nowinek technicznych. Jednocześnie tego typu płatności są bardzo bezpieczne, ponieważ karty są dodatkowo wyposażone w chip posiadający specjalne zabezpieczenia przed kopiowaniem danych z karty.

Karta Maestro PayPass pozwala dokonywać płatności za drobne zakupy (do 50 zł) w sposób bezstykowy – bez podawania kodu PIN ani podpisywania paragonów – w około 2,5 tys. punktów akceptacji. Do punktów akceptujących kartę należą restauracje McDonald's, apteki sieci Euro-Apteki, kawiarnie Mercers, coffeeheaven oraz saloniki prasowe Ruch, a także sklepy sieci Żabka i księgarnie Empik. Karta była również oficjalnym środkiem płatniczym na dwóch organizowanych w Polsce festiwalach muzycznych Heineken Open'er Festiwal w Gdyni oraz Coke Live Music Festiwal w Krakowie.

Ze względu na fakt, że karty z technologią PayPass zachowują wszystkie cechy klasycznej karty płatniczej, można nimi płacić nie tylko w punktach akceptujących tę technologię, ale we wszystkich punktach akceptujących karty ze znakiem Maestro i MasterCard oraz używać ich do wypłaty gotówki z bankomatów.

Specjalny chip wykorzystywany do płatności bezstykowych nie musi się znajdować na klasycznej plastikowej karcie płatniczej. Można go umieścić w zegarku, breloczku, bransoletce bądź w telefonie komórkowym i zamienić te urządzenia w instrumenty płatnicze.

W Europie technologia płatności zbliżeniowych rozwija się niezwykle dynamicznie. Kolejnym etapem ewolucji płatności *contactless* jest technologia NFC (*Near Field Communication*), która jest podstawą płatności mobilnych. Dzięki tej technologii telefon komórkowy, który dziś ma już wiele funkcji, można dodatkowo zamienić w kartę płatniczą i za bilety czy parking płacić przy pomocy telefonu. Nad wprowadzeniem mobilnych płatności zbliżeniowych w Polsce pracują wraz z organizacją płatniczą MasterCard operatorzy komórkowi. Planują oni wprowadzenie do oferty specjalnej naklejki z wykorzystaniem technologii bezkontaktowej, a następnie zamierzają zaoferować klientom telefony komórkowe z usługą płatności mobilnych.

Według ostatnich danych, podawanych przez organizację MasterCard, na koniec września 2008 roku w obiegu było blisko 44 mln kart i urządzeń wyposażonych w technologię PayPass, akceptowanych w 135 tys. punktów akceptacji na całym świecie. 25 krajów, w których miały miejsce wdrożenia lub testy PayPass, to Australia, Kanada, Chiny, Czechy, Francja, Niemcy, Indonezja, Włochy, Japonia, Korea, Liban, Malezja, Meksyk, Mongolia, Filipiny, Polska, Rosja, Hiszpania, Szwajcaria, Tajwan, Tajlandia, Turcja, Emiraty Arabskie, Wielka Brytania i USA.

Tekst został przygotowany w oparciu o materiały prasowe grupy LaSer

„Jestem zawsze w internecie”

Rewolucja mobilnego internetu

Mobilny internet doskonale uzupełnia, a często nawet zastępuje internet stacjonarny. Rewolucja, jaką wywołał kilkanaście lat temu w Polsce intensywny rozwój telefonii komórkowej, czeka nas zapewne również w przypadku mobilnego internetu. O zjawisku tym dyskutowali uczestnicy konferencji Polskiej Izby Informatyki i Telekomunikacji, poświęconej bezprzewodowemu internetowi, która odbyła się 21 stycznia br. w Warszawie.

Z testów przeprowadzonych w grudniu 2008 r. przez Audytel SA w 22 polskich miastach wynika jednoznacznie: komfort użytkowania dostępu do internetu poprzez sieć GSM/UMTS jest porównywalny do dostępu poprzez stałe łącze. Mobilny internet jest bardzo atrakcyjną konkurencją dla stacjonarnego zwłaszcza w przypadku łatwości dostępu i zasięgu, a coraz bardziej również w przypadku prędkości i cen połączeń.

Na bazie przeszło 2,5 tys. pomiarów w 107 lokalizacjach, dokonanych w 4 sieciach GSM/UMTS (P4, Polkomtel, PTC, PTK Centertel), najwyższą ocenę uzyskał Polkomtel. Jak podkreślono w raporcie, usługi Polkomtela cechowały się największą stabilnością pracy oraz maksymalnymi zanotowanymi osiągami prędkości pobierania przekraczającymi 5,5 Mbit/s. Temu operatorowi ustępuje inny, dość wysoko oceniany – PTK Centertel. Satysfakcjonujące wyniki odnotowały także w niektórych lokalizacjach PTC i P4.

– *Główną wartością badania było określenie, jaki jest stan usług mobilnego internetu dla końcowego użytkownika. Badano nie tyle rozmieszczenie masztów czy parametry infrastruktury, ale mierzono rzeczywiste wartości połączeń w typowych lokalizacjach. Za punkt przełomowy dla rozwoju mobilnego internetu można uznać stwierdzenie autorów raportu, że usługi mobilne są wystarczające do korzystania z serwisów multimedialnych typu YouTube. To rzeczywiście rewolucja mobilnego internetu* – powiedział **Krzysztof Król**, wiceprezes Polskiej Izby Informatyki i Telekomunikacji.

Ocena końcowa, przyznawana każdemu operatorowi, była sumą ocen punktowych dla kategorii prędkości pobierania i wysyłania danych, opóźnień oraz stabilności połączenia (maksimum to 100 pkt). Najlepszy okazał się Polkomtel (95,7 pkt), nieznacznie zwyciężając z PTK Centertel (93,7 pkt). Niżej uplasowało się dwóch pozostałych operatorów – PTC (76,3 pkt) i P4 (72,4 pkt). Polkomtel uzyskał maksymalną punktację za prędkość pobierania danych i za stabilność połączenia. Z kolei PTK Centertel został oceniony najwyżej w kategorii „opóźnienie przesyłania danych”; był też bardzo blisko maksimum punktowego jeśli chodzi o prędkość pobierania danych. Maksymalna punktacja za prędkość wysyłania przypadła operatorowi P4.

Średnia zmierzona prędkość pobierania danych dla wszystkich operatorów wyniosła nieco ponad 700 kbit/s. Pierwsze miejsce zajął Polkomtel (822 kbit/s) przed PTK Centertel (803 kbit/s); poniżej średniej mierzonej dla wszystkich operatorów znalazły się PTC (645 kbit/s) i P4 (553 kbit/s).

Z kolei w przypadku średniej zmierzonej prędkości wysyłania danych liderem okazał się P4 (251 kbit/s). Za nim uplasowali się: PTK Centertel (230 kbit/s), PTC (207 kbit/s) i, na ostatniej pozycji, Polkomtel (165 kbit/s). Pod względem opóźnienia przesyłania danych u badanych operatorów najmniejsze opóźnienie zanotował PTK Centertel (256 ms). Zaraz za nim znalazł się Polkomtel (282 ms), a na dalszych miejscach – P4 (380 ms) i PTC (390 ms).

Liderem, jeśli chodzi o średnią stabilność przesyłania danych, okazał się Polkomtel z 76-proc. stabilnością. Pozostali operatorzy zanotowali niemal wyrównane wyniki – PTK Centertel (61 proc.), P4 (58 proc.), PTC (55 proc.).

Autorzy opracowania porównali poszczególne kategorie także ze względu na wielkość miast, w których prowadzono badania. Najlepszą średnią prędkość przesyłania danych w miastach do 50 tys. mieszkańców odnotował PTK Centertel (729 kbit/s), ale w większych miastach wygrywa Polkomtel (766 kbit/s w miastach 50-250 tys. mieszk., 898 kbit/s w miastach zamieszkiwanych przez ponad 250 tys. osób). Z kolei najlepszą średnią prędkością pobierania danych na zewnątrz pomieszczeń może pochwalić się PTK Centertel (792 kbit/s), a wewnątrz – Polkomtel (890 kbit/s).

W opracowaniu znalazło się zestawienie 20 badanych miejsc w Polsce, gdzie odnotowano największe szybkości pobierania danych – z nich 18 przypada na Warszawę. Pierwsza ósemka to miejsca, gdzie najszybszy okazał się Polkomtel, m.in. gmach główny Politechniki Warszawskiej (2 lokalizacje, ze średnią prędkością 5 644 i 5 580 kbit/s) i biurowiec przy ul. Wspólnej (3 790 kbit/s).

We wnioskach z przeprowadzonych badań znalazło się stwierdzenie, że codzienne korzystanie z mobilnego internetu właściwie nie wykazuje różnic z dostępem stacjonarnym. – *Strony www oraz pliki multimedialne pobierają się w zasadzie równie szybko, niekiedy tylko można odczuć nieco większe opóźnienia przy przeglądaniu skomplikowanych stron www. Omawianych opóźnień nie odczuwa się natomiast w znaczącym stopniu w aplikacjach VoIP typu Skype* – czytamy w raporcie.

– *Kilkadziesiąt lat temu, przekazując informację o możliwościach skontaktowania się z daną osobą, zostawiano wiadomość: „Jestem w domu”, później pojawiły się stwierdzenia: „Jestem pod telefonem”, potem (choć bardzo krótko w Polsce): „Jestem pod pagerem”. W ostatnich 10 latach karierę zrobił komunikat „Jestem pod komórką”. Rewolucja mobilnego internetu wywoła pewnie stwierdzenie typu: „Jestem zawsze w internecie”* – powiedział prowadzący konferencję Krzysztof Król. ■

Jako Partner Technologiczny zapraszamy na
XX Międzynarodowe Targi Komunikacji Elektronicznej INTERTELECOM 2009
17-19 Marca 2009, Stoisko nr 26 w hali nr 1

ksi.pl
KOMPLEKSOWE SYSTEMY INFORMACYJNE

ROZWIĄZANIA MOBILNE

Od kilku lat obserwujemy gwałtowny rozwój technologii bezprzewodowych powiązany z systematycznym spadkiem cen urządzeń. Dla nikogo dziś nie jest zaskoczeniem bezprzewodowa sieć, bezprzewodowy laptop, bezprzewodowy telefon oraz zminiaturyzowane czy zintegrowane wersje tych koncepcji - palmtop, smartfon, netbook. Zacierające się granice zarówno w nazewnictwie, jak i klasyfikacji kolejnych produktów prowadzą do jednego wniosku - nowoczesna technologia nie lubi kabli. Chcemy bezprzewodowo się komunikować, gromadzić, przetwarzać i wyświetlać dane na użytecznych, poręcznych, mobilnych urządzeniach - coraz bardziej funkcjonalnych i coraz tańszych.

Wychodząc z tych założeń chcielibyśmy zaprezentować Państwu platformę mobilną NOTOS, wykorzystywaną do gromadzenia i prezentacji danych na szeregu urządzeń bezprzewodowych. Autorskie rozwiązanie firmy ksi.pl znajdzie zastosowanie wszędzie tam gdzie użytkownicy muszą rejestrować i otrzymywać informacje pozostają równocześnie w pełni mobilnymi.

BLUETOOTH MARKETING

Wszechobecne ulotki i broszury, zapełniają śmietniki, fruwają po ulicach miast i zalegają w kątach, stając się coraz bardziej natrętną i coraz mniej efektywną formą reklamy.

Rozwiązaniem odpowiadającym potrzebie wprowadzenia nowoczesnej, atrakcyjnej formy przekazu informacji marketingowych, jest system BlueSend, pozwalający w sposób wygodny i tani docierać do urządzeń mobilnych potencjalnych klientów. Bramka systemu BlueSend wyszukuje, a następnie przesyła za pomocą protokołu Bluetooth wybrane treści marketingowe na urządzenia mobilne znajdujące się w pobliżu. Umożliwia to wysyłanie nie tylko obrazów i muzyki, ale również bardziej rozbudowanych, interaktywnych aplikacji (np. katalogu produktów, czy mapy punktów sprzedaży).

Co istotne, reklama, bądź informacje dostarczane w ten sposób nie zmuszają odbiorcy do zapoznania się z nimi – to odbiorca decyduje czy ściągnie na swój telefon zaproponowany przez system, darmowy plik. Tak podana informacja pobudza ciekawość i receptywność, ale nie ingeruje niepotrzebnie w naszą przestrzeń osobistą.

Zastosowanie nowoczesnych narzędzi, takich jak Bluetooth Marketing ściśle wiąże markę z takimi przymiotami jak innowacyjność, czy skuteczność.

Technologie i kryzys

Co czeka branżę IT?

Jakie będą najważniejsze kwestie w branży IT w roku 2009 i dlaczego – prognozuje ROBERT KOGUT, dyrektor zarządzający regionu Europy Wschodniej 3Com Poland.

Zrobić więcej przy zredukowanym budżecie

– Całkowicie zrozumiałe jest, że najważniejszą kwestią w 2009 roku będą rozmiary, prędkość oraz intensywność spadku koniunktury w światowej gospodarce. Niektórzy sprzedawcy z branży technologicznej przetrwają kryzys w lepszej kondycji niż inni.

Analitycy prognozują zmniejszenie wydatków w branży technologicznej w Stanach Zjednoczonych i Europie, jednak w przypadku rynków azjatyckich oczekują niewielkiego trendu wzrostowego. Firmy technologiczne, które koncentrują swoją działalność głównie na rynku amerykańskim i europejskim, mają duże powody do obaw. Nagle bardzo pilnym zadaniem dla nich stało się zwiększenie sprzedaży w Azji i na innych wschodzących rynkach, a także ponowne zweryfikowanie własnego łańcucha wartości. Akurat 3Com jest aktualnie w dobrym, niejako uprzywilejowanym położeniu, ponieważ ponad połowa przychodów firmy pochodzi obecnie z Chin oraz rejonu Azji i Pacyfiku.

Ponadto posiadamy rozwiązania sieciowe oferujące zbliżoną lub nawet lepszą wydajność i funkcjonalność niż rozwiązania konkurencji, ale po mniejszych kosztach. Przedsiębiorstwa zdają sobie dziś sprawę, że nie muszą ponosić dodatkowych kosztów za oczekiwaną wydajność. Rok 2009 będzie rokiem zredukowanych budżetów w branży IT oraz wyjątkową okazją dla sprzedawców sprzętu komputerowego, ponieważ w obszarze konkurencyjności zaczyna liczyć się przede wszystkim wartość.

Zielony – kolor z wyboru

– W kategoriach rozlokowania technologii coraz więcej firm będzie podejmować działania w celu zmniejszania poboru energii we własnych centrach przetwarzania danych i sieciach.

Projekt energooszczędnego Ethernetu IEEE P802.3az, będący kluczowym elementem „zielonej technologii", skupia się obecnie na dopracowaniu i wdrożeniu rozwiązania noszącego nazwę *low power idle*. Z racji że energia stanowi moc zużywaną w określonym przedziale czasu, najbardziej energooszczędnym podejściem jest transfer pakietów danych w Ethernecie z możliwie największą prędkością przesyłu, a tym samym w jak najkrótszym czasie. Kolejnym krokiem jest to, by urządzenia pobierały jak najmniejszą ilość energii w czasie pomiędzy przesyłem kolejnych pakietów, co określane jest mianem *low power idle*.

Myślę, że główną zaletą *low power idle* jest zapewnienie sygnału uśpienia i wybudzenia, kiedy połączenie wchodzi w stan *low power idle* lub z niego wychodzi. To umożliwia także innym urządzeniom przyłączonym do sieci wejście w stan niskiego poboru mocy bądź uśpienia, a przy odebraniu sygnału wybudzenia natychmiastowe wyjście z trybu energooszczędnego, by kontynuować transfer pakietów.

Wierzę, że ta funkcjonalność pozwoli zapewnić znaczące oszczędności energii ponad te oszczędności, które są uzyskiwane zwyczajnie przez zwiększenie energooszczędności fizycznej warstwy Ethernetu.

Zarządzanie wirtualizacją sieci

– W 2008 roku w całym regionie duże zainteresowanie budziła technologia wirtualizacyjna. Tematyka ta będzie obecna również w roku 2009 aż do momentu, kiedy firmy wykonają kolejne kroki po uprzednim zwirtualizowaniu swoich serwerów, przestrzeni do przechowywania danych oraz samej sieci.

Przełączniki wyposażone w technologię XRN (*eXpandable Resilient Networking*) potrafią zwirtualizować różnorodne przełączniki brzegowe w logiczny przełącznik wirtualny, podczas gdy technologia wirtualizacji rdzeniowej pozwala połączyć wiele przełączników rdzeniowych w jeden megaswitch. To podejście pozwala usprawnić łatwość zarządzania, dostępność oraz skalowalność. Oprócz tego kluczową kwestię stanowić będzie zdolność zarządzania w zintegrowany sposób zwirtualizowanymi serwerami, sieciami oraz klientelą. Narzędzia potrzebne ku temu już się pojawiają, a w następnym roku zostaną rozwinięte i dopracowane.

Usługi sieciowe – infrastruktura sprzętowa vs. oprogramowanie

– W okresie kilku ostatnich miesięcy, gdy gospodarka zauważalnie zwolniła, firmy zaczęły powtórnie rozważać słuszność swoich wyborów w kwestii zakupów infrastruktury sieciowej. Kiedy coraz więcej firm cierpi na brak pieniędzy, oczekujemy, że zaczną one korzystać z platform usługowych do rozwijania usług sieciowych, gdy jest im to potrzebne, zamiast przyłączać do sieci kolejny fizyczny serwer lub inne urządzenie. Poza istotną oszczędnością kosztów wspomniane podejście daje firmom lepszą kontrolę nad ich przedsięwzięciami i umożliwia im szybsze rozmieszczenie nowych usług.

Szybsze dostarczanie usług multimedialnych na życzenie

– Koszty dostarczenia usług multimedialnych do biur i miejsc zamieszkania były wysokie. Kiedy w 2008 roku klienci dopytywali się o usługę wideo na życzenie (*video-on-demand*, *VoD*), a firmy pragnęły usług multimedialnych, wideokonferencji, to wiele spośród tych usług było niedostępnych lub ich koszty nie były atrakcyjne dla znacznej grupy użytkowników końcowych.

Ta sytuacja będzie się teraz zmieniać równocześnie z dojrzewaniem technologii pasywnych sieci optycznych EPON (*Ethernet Passive Optical Network*). EPON zacznie być atrakcyjną możliwością, by rozwijać sieci WAN nawet dla kampusów i przedsiębiorców budowlanych, co wcześniej zarezerwowane było jedynie dla firm telekomunikacyjnych oraz instytucji rządowych.

3Com zdążył już przetestować swoją technologię EPON m.in. we własnym systemie dystrybucji treści multimedialnych MCDS (*Multimedia Content Delivery Solutions*), zastosowanym w systemie nadzoru i monitoringu ulicznego, jaki został użyty podczas Igrzysk Olimpijskich w Pekinie.

To rozwiązanie zostanie poparte ratyfikacją we wrześniu 2009 r. projektu EEE P802.3av 10 Gb/s EPON, który ma zapewnić zwiększoną przepustowość przez infrastrukturę PON. Projekt IEEE P802.3av zapewnia szybkości pobierania i wysyłania danych równe 10 Gb/s.

Podobnie rzecz ma się w przypadku transferu przez infrastrukturę sieci PON (*Passive Optical Network*), stosowaną na pierwszej mili (*first mile*) pomiędzy dostawcą usług internetowych lub firmą telekomunikacyjną, a abonentem i jego biurem.

Ta zwiększona przepustowość będzie wspierać większą zdolność do zapewnienia takich usług, jak IPTV oraz wideo na życzenie (*video-on-demand*, *VoD*). ■

Nowatorski sposób komunikacji głosowej przez stronę internetową

Grzegorz Kantowicz

VoiceLink – kliknij i rozmawiaj

Usługa VoiceLink umożliwia natychmiastowy kontakt głosowy odwiedzającego witrynę internetową z pracownikiem/konsultantem firmy lub urzędu. Jest to doskonały kanał komunikacji z klientem. Łatwość implementacji i użytkowania daje szansę uzyskania przewagi konkurencyjnej nad innymi graczami na rynku zwłaszcza teraz, gdy z badań wynika, iż zaledwie kilka minut decyduje o tym, czy kupującego zainteresuje towar oraz czy spróbuje skontaktować się ze sprzedającym.

Umożliwienie po kliknięciu na stronie internetowej bezpłatnego bezpośredniego kontaktu głosowego z konsultantem w urzędzie przyspiesza i ułatwia interesantowi załatwienie sprawy czy wypełnienie formularza. Buduje przy okazji wizerunek przyjaznego urzędu.

Każdy dział w firmie czy wydział w urzędzie, a nawet każda osoba może mieć zaimplementowaną usługę VoiceLink do kontaktu z klientami i partnerami biznesowymi.

Aby wykonać darmowe połączenie, odwiedzający witrynę internetową nie musi posiadać żadnego dodatkowego sprzętu z wyjątkiem komputera wyposażonego w mikrofon i głośniki lub słuchawki. W zależności od konfiguracji oprogramowania na komputerze może się okazać, że konieczne jest doinstalowanie maszyny Java firmy SUN niezbędnej przy oglądaniu wielu stron internetowych. O tym fakcie powiadomi użytkownika przeglądarka i system przeprowadzi go przez proces instalacji.

Firma lub urząd, które chcą umożliwić to swoim odwiedzającym, musi wyposażyć się w minimum pakiet startowy. Platforma umożliwiająca komunikowanie się internautów z konsultantami Klienta jest dostarczana i obsługiwana przez Operatora Usługi VoiceLink.

Użytkownik nie musi:

- rejestrować się jako użytkownik usługi u operatora;
- uzyskiwać indywidualnego numeru;
- uzyskiwać spersonalizowanego identyfikatora.

Jej uruchomienie jest bardzo proste i następuje po kliknięciu w dedykowaną ikonę odwiedzanej witryny.

Pakiet startowy

W ramach pakietu startowego usługi Klient abonując jeden VoiceLink otrzymuje możliwość obsługi do 3 konsultantów skojarzonych z określoną ikoną na jego stronie www. Liczbę konsultantów można zwiększyć. System dba o rozłożenie ruchu pomiędzy wszystkich pracowników, kolejkując przychodzące zgłoszenia w przypadku zajętości wszystkich końcówek. Internauta w takim przypadku widzi, który jest w kolejce i jaki orientacyjnie jest czas oczekiwania.

Operator dostarcza wzór ikony oraz oprogramowanie niezbędne do zaimplementowania w ramach witryny internetowej Klienta. Rolą Klienta jest jedynie umieszczenie na swojej stronie otrzymanej ikony oraz linku do programu wykonawczego. Program realizujący usługę VoiceLink znajduje się na serwerze operatora i jest pobierany do komputera użytkownika/internauty wraz z otwieraną stroną www.

Każdy Klient dla swojego VoiceLinka otrzymuje indywidualny kod skojarzony z daną ikoną. W przypadku większej liczby VoiceLinków na stronach Klienta, każdy VoiceLink ma swój identyfikator. Identyfikator jest przekazywany do programu wykonawczego przy aktywacji połączenia jako parametr identyfikujący Klienta.

W trakcie nawiązywania połączenia użytkownik/internauta widzi na ekranie komunikaty odpowiadające stanowi, w jakim znajduje się system. Operator w tym miejscu daje Klientowi możliwość zdefiniowania treści wyświetlanych komunikatów. Przykładowo, jeżeli Klient do obsługi VoiceLinka ma 3 konsultantów, to może zdecydować, że w trakcie połączenia użytkownik ma uzyskać informację, z kim rozmawia.

Dodatkowe wypisy i komunikaty do użytkownika/internauty mogą dotyczyć przykładowo:

- czasowej nieobecności konsultanta „Konsultanci chwilowo nieobecni";
- stałej nieobecności konsultanta „Przepraszamy. Konsultanci nieobecni";
- przykładowych godzin obsługi VoiceLinka w godzinach gdy brak konsultantów „Zapraszamy: pn. – pt. od 8.00 do 16.00".

Maksymalna długość tekstu to 40 znaków wraz ze spacjami. Klient może skorzystać z predefiniowanych przez operatora komunikatów lub w momencie abonowania usługi podać swoje wersje komunikatów dla poszczególnych stanów połączenia. W przypadku koniecznej aktualizacji można zlecić operatorowi zmianę wypisów.

W przypadku wykorzystywania telefonów IP oferowanych przez operatora konsultanci mogą w pewnym zakresie sterować pracą węzła. Wykorzystując klawiaturę alfanumeryczną telefonu mogą zrealizować funkcje dodatkowe, takie jak:

- blokada czasowa połączeń przychodzących – ruch przychodzący będzie kierowany na pozostałych konsultantów; jeśli nie ma więcej stanowisk, na ekranach internautów próbujących nawiązać połączenie pojawi się komunikat o czasowej nieobecności konsultanta lub inny zadeklarowany przez Klienta; blokada czasowa trwa 15 minut;

- blokada połączeń przychodzących – konsultant wyłączony z pracy do momentu odwołania blokady z jego aparatu; wypisy jak powyżej;
- blokada połączeń złośliwych – w trakcie wywołania lub bezpośrednio po nim konsultant ma możliwość czasowego zablokowania adresu IP, z którego pochodziło ostatnie połączenie; blokada czasowa – 30 minut.

Niezbędny sprzęt

Nakłady na wyposażenie sprzętowe konsultantów są bardzo małe, a wręcz można je zredukować do zera. W celu obsługi zgłoszeń przychodzących ze stron www do konsultantów Klient musi wyposażyć swoich pracowników w dedykowane telefony IP pozwalające na prowadzenie rozmów w technologii VoIP. Telefony mogą być wpięte w sieć LAN Klienta albo można dla nich stworzyć dedykowaną podsieć. Jest też możliwe zastosowanie konwerterów ATA i wykorzystanie istniejących telefonów analogowych lub wręcz zaimplementowanie na komputerach konsultantów tzw. softphonów, czyli aplikacji komputerowych do obsługi połączeń telefonicznych w technologii VoIP.

Podłączenie telefonu dla obsługi zgłoszeń

Odbieranie wywołań telefonicznych generowanych z internetu poprzez łącza VoiceLink możliwe jest na trzy sposoby:

- z telefonu internetowego (VoIP) podłączonego bezpośrednio do sieci internet (konfiguracja 1);
- z telefonu analogowego dołączonego do abonenckiej centrali wewnętrznej (konfiguracja 2);
- z telefonu analogowego dołączonego do sieci internet poprzez bramkę VoIP (konfiguracja 3).

Konfiguracja 1

Wykorzystuje się dostarczany przez operatora telefon VoIP, na który będą przychodziły wywołania bezpośrednio z internetu.

Zalety:

- pełna współpraca telefonu z systemem VoiceLink, w tym realizowanie przy pomocy klawiatury telefonu usług specjalnych, np. usługi czasowej blokady wywołań;
- w przypadku telefonu obsługującego kilka kont możliwość wykorzystywania telefonu do obsługi innych połączeń VoIP;
- możliwość rozbudowy systemu w kierunku telefonii VoIP.

Konfiguracja 2

Wykorzystanie istniejącej centrali wewnętrznej i dołączenie internetu poprzez dostarczoną bramkę VoiceLink do wejścia przeznaczonego dla linii miejskiej. Połączenia internetowe VoiceLink są odbierane przez wyposażenie centralki, tak jak połączenia miejskie.

Zalety:

- możliwość skierowania przychodzących połączeń na dowolny telefon końcowy centrali (w centrali należy ustawić przekierowanie na stałe);
- możliwość wykorzystania istniejących telefonów;
- kierowanie wywołań VoiceLink na już istniejący telefon.

Wykorzystanie wszystkich możliwości systemu VoiceLink jest uzależnione od parametrów posiadanej centrali wewnętrznej. Operator gwarantuje pełną współpracę z systemem w przypadku wykorzystywania centrali systemowej VDmaster.

Konfiguracja 3

Zwykły telefon analogowy dołącza się poprzez bramkę VoiceLink dostarczoną przez operatora w momencie zawarcia umowy na świadczenie usługi VoiceLink. Telefon przeznaczony do odbierania rozmów zostaje umieszczony na stanowisku konsultanta.

Zalety:

- możliwość wykorzystania posiadanego analogowego aparatu telefonicznego;
- niskie koszty rozwiązania;
- możliwość zastosowania bramki obsługującej jednocześnie analogową linię miejską i łącze VoiceLink na jednym telefonie analogowym.

Wady:

- możliwości funkcjonalne ograniczone do możliwości posiadanego aparatu.

Należy zwrócić uwagę, że wykorzystanie oferowanych telefonów IP rozszerza paletę dostępnych usług dla konsultantów.

Statystyki i funkcje dodatkowe

W celu optymalnego zarządzania liczbą i pracą konsultantów, Klient otrzymuje od operatora usługi raporty dotyczące ruchu w ramach posiadanych przez niego VoiceLinków. Statystyki pokazują:

- łączną liczbę połączeń;
- średni czas połączenia;
- średnią długość kolejki do konsultanta lub grupy konsultantów;
- liczbę wywołań nieobsłużonych;
- rozkład wywołań w czasie.

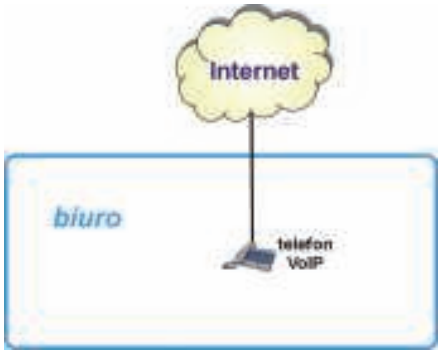
Trwają prace nad wdrożeniem kolejnych raportów.

Zasady korzystania z usługi

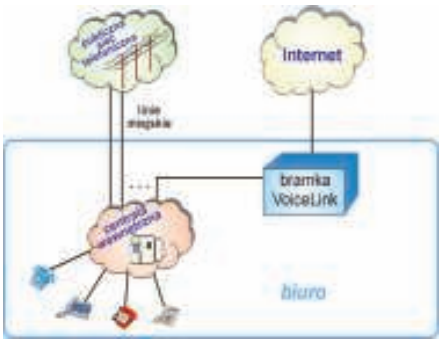
Usługa VoiceLink jest usługą abonamentową i wymaga podpisania umowy pomiędzy Klientem i Operatorem. Klientem jest firma lub urząd posiadające własną witrynę www i chcące umożliwić swoim odwiedzającym szybki bezpłatny kontakt z pracownikami.

Usługa VoiceLink jest aktywowana po podpisaniu umowy na abonament i wpłacie pierwszej opłaty abonamentowej. Opłaty abonamentowe można uiszczać miesięcznie lub zapłacić za rok góry. Po stronie Klienta leży implementacja dostarczonego przez Operatora oprogramowania na własnych stronach www oraz instalacja telefonów IP. Telefony IP są dostarczane już skonfigurowane dla konkretnej usługi i wymagane jest jedynie dołączenie ich do własnej sieci LAN przez Klienta.

Usługę można zamówić na stronie www.voicelink.pl. ■



Konfiguracja 1. Bezpośrednie dołączenie do internetu



Konfiguracja 2. Podłączenie przez bramkę VoiceLink z wykorzystaniem centrali wewnętrznej

Konfiguracja 3 Dołączenie z wykorzystaniem telefonu analogowego

Nadążyć z wydajnością

Grzegorz Kantowicz

TX Matrix Plus dla sieci szkieletowych

Firma Juniper Networks wprowadza na rynek TX Matrix Plus, rutery IP do sieci szkieletowych pracujące w architekturze wielostojakowej, pozwalające operatorom na dostarczanie nowatorskich usług z maksymalną rentownością i ochroną już poczynionych inwestycji. Sprzęgający ze sobą wiele ruterów szkieletowych T1600 system TX Matrix Plus współpracuje z systemem sterowania Juniper Control System (JCS) 1200, co umożliwia wirtualizację ruterów IP, sieci i usług – wprowadzając nowy wymiar swobody skalowalności sieci szkieletowych.

System TX Matrix Plus wykorzystuje doskonałe rozwiązania techniczne zastosowane w jednostojakowych ruterach szkieletowych T1600, cechujących się największą na rynku pojemnością i energooszczędnością. TG1600 i TX Matrix Plus obniżają całkowity koszt posiadania poprzez zapewnienie do 25 procent większej przepustowości kierowania ruchem przy o połowę mniejszych gabarytach urządzeń i do 40 procent mniejszym poborze energii niż rozwiązania konkurencyjne.

Architekturę systemu zaprojektowano do obsługi przepustowości do 25 Tb/s, ponieważ pozwala na sprzężenie ze sobą maksymalnie 16 ruterów T1600 w jeden wielostojakowy węzeł kierowania ruchu. Takim ruterem zespolonym można zarządzać jak pojedynczym dużym ruterem bądź w połączeniu z JCS 1200 można zrealizować wirtualizację ruterów szkieletowych – co prowadzi do oszczędności płynących z możliwości konsolidacji sieci, usług i funkcjonalności

Wirtualizacja w sieciach szkieletowych

Ze względu na zapewniany przez wirtualizację wzrost efektywności i ograniczenie kosztów płynące z konsolidowania i współużytkowania zasobów, szybko zaczęła ona być wprowadzana do ośrodków przetwarzania danych. Wprowadzenie wirtualizacji dotąd odrębnych sieci i usług w sieciach szkieletowych było trudniejsze ze względu na szereg kwestii związanych z wymogami prawnymi, operacyjnymi, organizacyjnymi i bezpieczeństwem sieci. TX Matrix Plus i JCS 1200 rozwiązuje te kwestie poprzez możliwość zapewnienia sprzętowej wirtualizacji wysoce skalowalnych elastycznych ruterów szkieletowych. Rutery szkieletowe firmy Juniper można dzielić na partycje – z dokładnością do gniazda – czyli na liczne rutery wirtualne, z których każdy może stanowić usługę lub rodzaj elementu sieciowego i może korzystać wspólnie z zasobów takich, jak łącza pośredniczące czy międzywęzłowe. Dzięki tej funkcji operatorzy mogą utrzymać wymagany poziom rozdziału administracyjnego i usługowego oraz zarządzania i zabezpieczeń, jednocześnie w dalszym ciągu uzyskując znaczący wzrost sprawności i ograniczenie kosztów niesione przez wirtualizację.

Operatorzy, którzy wykorzystają TX Matrix Plus w połączeniu z innymi rozwiązaniami firmy Juniper, by zwirtualizować swe sieci szkieletowe, będą mogli szybko wdrażać w istniejącej infrastrukturze nowe usługi, w dalszym ciągu indywidualnie zarządzając każdą siecią i usługą. Ta możliwość ogromnie przyspiesza wprowadzanie nowych usług i otwiera możliwości stosowania nowych modeli biznesowych oraz rodzajów współpracy, takich jak możliwość świadczenia usług niewymagających uwierzytelniania (*Open Garden*), powstawania wirtualnych operatorów sieci, zapewniania sieci jako usługi (*NaaS*) i współdzielenia sieci.

Skalowanie wirtualizowanej sieci szkieletowej

Aby umożliwić klientom pełne wykorzystanie możliwości stwarzanych przez wirtualizację i zaspokojenie rosnącego zapotrzebowania na pojemność, firma zapewnia szereg pomocniczych rozwiązań technicznych przeznaczonych zarówno dla jednostojakowych, jak i wielostojakowych ruterów T1600s. Jako jedyny na rynku ruter szkieletowy o przepusto-

Kilka przykładów dla zobrazowania wydajności nowych rozwiązań:

- 25 Tb/s = 25.000.000.000.000 bitów na sekundę!
- Jest to przepływność wystarczająca do obsługi 8 milionów szerokopasmowych łączy abonenckich ADSL o przepływności 3 Mb/s każde.
- Jednym w pełni wyposażonym węzłem TX Plus Matrix można by obsłużyć wszystkich użytkowników szerokopasmowego dostępu do internetu w Hiszpanii!
- Cała ludność świata licząca 7 miliardów osób mogłaby realizować jednoczesne rozmowy VoIP poprzez jeden w pełni wyposażony węzeł TX Plus Matrix (przyjmując transmisję 15 kb/s na rozmowę).
- 100 milionów ludzi mogłoby jednocześnie rozgrywać sieciowy mecz piłki nożnej (zakładając 250 kb/s na sesję gracza), czyli cała Hiszpania (40 milionów obywateli) mogłaby jednocześnie grać przeciwko całym Włochom (60 milionów obywateli).
- 4 miliony gospodarstw domowych mogłoby jednocześnie oglądać na żywo transmisję telewizyjną przez tylko jeden w pełni wyposażony węzeł TX Plus Matrix (zakładając 6 Mb/s na kanał telewizyjny).
- Jednocześnie 250 milionów ludzi mogłoby słuchać strumieniowego przekazu muzycznego z przepływnością 100 kb/s.
- Każdy z 200 krajów świata mógłby do TX Plus Matrix podłączyć się strumieniem 125 Gb/s, co odpowiada prowadzeniu w każdym kraju 25.000 jednoczesnych wideokonferencji, z których każda zajmuje pasmo 5 Mb/s.
- Szacuje się, że serwis YouTube zawiera 1,06 petabajta danych [http://beerpla.net/2008/08/14/how-to-find-out-the-number-of-videos-on-youtube]. To odpowiada 12,8 petabitom. Zawartość tę można by przesłać ruterem o przepływności 25,6 Tb/s w około 500 sekund, czyli 8,3 minut.

wości 100 Gigabitów na gniazdo, T1600 jest optymalny do obsługi łączy o ultrawysokiej pojemności potrzebnych dla wirtualizowanych ruterów szkieletowych.

Ponadto firma Juniper w dalszym ciągu rozwija możliwości integracji po stronie optycznej, dodając nowe zintegrowane interfejsy do optycznej sieci transportowej G.709 (OTN) oraz funkcjonalność GMPLS. Dzięki wbudowanej obsłudze łączy światłowodowych nie trzeba stosować wolno stojących transponderów optycznych, co oszczędza dużo miejsca i energii elektrycznej.

Zmniejszając liczbę warstw sieciowych i konsolidując interfejsy sieciowe, wirtualizacja i interfejsy OTN mogą zmniejszyć koszt przesyłu usług sieciowych wyrażany na bit – co zwiększy rentowność, pozwalając dostawcom usług maksymalnie wykorzystywać możliwości sieci.

– *Wirtualizacja stała się faktycznym modelem działania ośrodków przetwarzania danych, ponieważ przynoszone przez nią oszczędności finansowe i zalety operacyjne są bezdyskusyjne* – powiedział **Opher Kahane**, wiceprezes i dyrektor generalny High-End Systems Business Unit w Juniper Networks. – *TX Matrix Plus zapewnia takie same zalety wirtualizacji w sieciach szkieletowych jako najelastyczniejszy na rynku system sterowania ruterami IP w układzie wielostojakowym. Dzięki temu przełomowi spada całkowity koszt posiadania, przez co nasi klienci mogą budować sieci skalowalne i niezawodne, pozwalające na świadczenie nowatorskich usług przy najwyższej ich dochodowości i ochronie dotychczasowych inwestycji.*

Skalowalność w trzech wymiarach

Platformy firmy Juniper z serii T pozwalają klientom na wymiarowanie sieci w trzech płaszczyznach: przekazywania, sterowania i usług. Klienci użytkujący urządzenia T640 mogą rozbudować wymiar przekazywania przechodząc na T1600, TX Matrix i obecnie TX Matrix Plus – co można realizować bez zaburzania pracy sieci i w maksymalnie elastyczny sposób.

JCS 1200 jest jedyną w branży platformą pozwalającą na rozbudowanie płaszczyzny sterowania, umożliwiającą rozbudowę pojemności tej płaszczyzny bez zaburzania wydajności płaszczyzny przekazywania ruchu – a jest to możliwość krytyczna dla wirtualizacji sieci szkieletowych i usług.

Wszystkie powyższe platformy pracują pod kontrolą oprogramowania JUNOS, pojedynczego systemu operacyjnego do systemów kierowania, komutacji i ochrony ruchu – produkcji Juniper Networks. Umożliwiając klientom i partnerom opracowywanie aplikacji pod system JUNOS w ramach Platformy Rozwijania Rozwiązań przez Partnerów (*Partner Solution Development Platform – PSDP*) Juniper jest także jedyną firmą w branży umożliwiającą klientom rozbudowywanie płaszczyzny usług o usługi indywidualnie tworzone i modyfikowane (wiąże się to z dodatkowymi opłatami). Klienci i partnerzy mogą w oparciu o PSDP opracowywać i wdrażać nowatorskie usługi dodane zapewniające większą wydajność i dochodowość ich sieci.

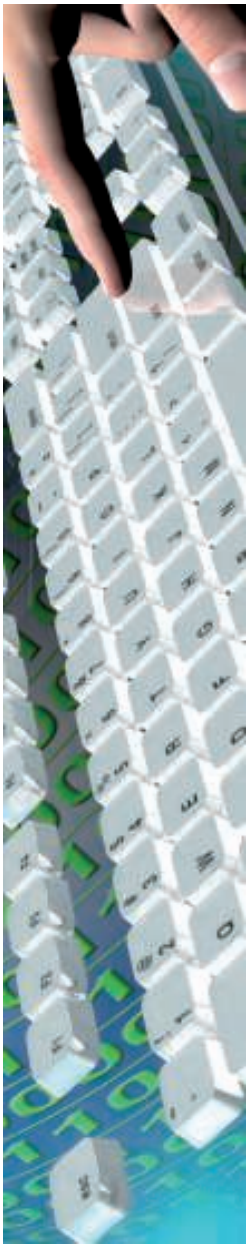
TX Matrix Plus będzie dostępny w trzecim kwartale 2009 roku. Interfejsy OTN będą dostępne w bieżącym kwartale. ■

MPLS aż do węzłów dostępowych

David Noguer Bau, Jean-Marc Uzé

Niech sieci miejskie zaczną zarabiać!

Najrealniejsze szanse na zwiększenie zarobków kryją się w sieciach metropolitalnych, a nie w szkieletowych: pakiety multiplay dla użytkowników domowych, usługi zarządzane dla przedsiębiorstw, nowa generacja łączności ruchomej, oprogramowanie jako usługa, itd. Operatorzy – dostawcy usług – powinni dokładniej się przyjrzeć budowanym przez siebie sieciom metropolitalnym i ocenić stopień ich zoptymalizowania oraz możliwości rozwijania ich w tempie wzrostu popytu na nowe usługi.



Od kilku lat dostawcy usług znaczną część swoich budżetów przeznaczali na sieci dostępowe i metropolitalne. Przyczyną tych inwestycji była konwergencja usług na protokół IP, niestety, często owocowało to budową oddzielnych sieci specjalizowanych pod kątem poszczególnych usług i oprogramowania – paradoksalnie w czasach konwergencji, czyli zbieżności, powstało wiele oddzielnych sieci, przez co świat sieciowy zrobił się de facto rozbieżny.

Nadszedł czas, by te sieci doprowadzić do prawdziwej zbieżności, co pozwoli zmniejszyć koszty i uprościć infrastrukturę, a – co ważniejsze – w przyszłości móc na nich lepiej zarabiać.

Poszukiwanie wzorca sieci szkieletowych

Kilka lat temu projektanci architektury sieci szkieletowych stanęli przed podobnym dylematem: przy spadającym zapotrzebowaniu na usługi TDM (zwielokrotnienie z podziałem czasowym) i przyjmowaniem się Ethernetu jako standardowego interfejsu, żeby zapewnić pełną konwergencję, trzeba było zdecydowanie przebudować sieci szkieletowe. Zadanie polegało wtedy na stworzeniu sieci bez niepotrzebnych warstw, by umożliwić sprawną koegzystencję transmisji pakietowej z komutacją łączy. Pomysł na ich uwarstwienie i rozdzielenie „usług" od „infrastruktury" był uzasadniony tym, że pozwalał na tworzenie sieci bardzo stabilnych, w których każdą usługą można było zarządzać niezależnie od pozostałych. Dlatego awaria jednej usługi nie wpływała na pozostałe usługi. Jednakże współcześnie, przy coraz powszechniej stosowanej warstwie wielousługowej opartej na IP/MPLS wdrażanej przez piony do spraw usług IP, bardzo niewiele usług posadawia się bezpośrednio na warstwie transportowej.

Ponieważ operatorzy większość przychodów osiągają z wyższych warstw sieci, w szkielecie sieci postawili na bardziej pragmatyczne rozwiązanie: łączą ze sobą piony transportu i IP w jeden, by lepiej ogarniać wszystkie warstwy niezbędne do zbudowania sprawnej sieci, a także by uprościć eksploatację. Pojawiły się nowe techniki, takie jak PBB-TE czy MPLS-TP, obiecujące dalszą integrację z elementami transmisyjnymi i docelowo mające zapewnić zoptymalizowany model usług warstw L0 do L2. Jednakże owe przekształcane sieci są budowane w protokole IP-MPLS przesyłanym po DWDM, co zapewnia możliwość lepszego wykorzystania atutów obydwu środowisk i zapewnia elastyczność i sprawność niezbędną dla usług dających przychody, obchodząc jednocześnie ograniczenia występujące przy wyłącznie komutacji łączy lub transmisji czysto pakietowej. Ponadto dzięki temu podejściu można stosować w sieciach metropolitalnych ten sam model, architekturę i procesy operacyjne, jakie w ciągu ostatnich 10 lat stosowano w sieciach szkieletowych.

Ujednolicanie sieci metropolitalnych

Współczesne sieci metropolitalne już są ethernetowe i większość z nich może obsługiwać ruch IP, jednakże bardzo wielu operatorów w dalszym ciągu utrzymuje odrębne sieci dla użytkowników biznesowych, mieszkaniowych i dla dostępu ruchomego. A przez tę odrębność operatorzy tracą cenne możliwości wykorzystania synergii występujących między tymi sieciami.

Głównymi celami stawianymi konwergencji jest zapewnienie uproszczenia, obniżenia kosztów operacyjnych i zwiększenie elastyczności. Aby osiągnąć prawdziwą konwergencję, każdy z dostawców usług musi przeanalizować specyficzne wymagania stawiane przez każdą usługę czy aplikację, bo dopiero wtedy będzie je w stanie optymalnie zintegrować. Równie istotne jest zapewnienie tym posunięciem większej odporności wszystkich usług i aplikacji na uszkodzenia i większej ich skalowalności. Wygląda na to, że MPLS ma wszystkie cechy do tego potrzebne.

Budowa sieci miejskich MPLS nie jest nowością, jednakże ze względu na brak możliwości rozbudowy niektórych wczesnych implementacji, wielu operatorów decydowało się na podzielenie sieci metropolitalnych na wiele odrębnych sieci, które obecnie eksploatują. W tej chwili MPLS już umożliwia operatorom osiąganie wymaganej skalowalności, istnieją narzędzia do obsługi konwergentnych sieci metropolitalnych, a firma Juniper Networks może je zaoferować na ekonomicznych warunkach: współpraca międzysieciowa LDP/BGP MPLS, LSP punkt-wielopunkt, niedoścignione tablice adresów MAC, integracja warstw L2 i L.

Inteligentne brzegowe usługowe zakończenia sieci zwiększą jej dochodowość

Sieci budowane pod specjalizowane zastosowania można było uruchamiać szybciej, zgodnie z wymogami umów o jakości usług SLA, ale doprowadziło to do powstania drogich, monolitycznych i nieelastycznych infrastruktur niezdolnych do ewolucji wraz z nowymi usługami i potrzebami. W konwergentnych sieciach metropolitalnych pojawia się ryzyko ponownego brnięcia w budowę specjalizowanych

brzegowych punktów dostarczania usług – powodujących liczne problemy już znane z przeszłości. Specjalizowany usługowy element brzegowy sieci nie jest w stanie ewoluować z nowymi aplikacjami i narzuca model „uniwersalnego kombajnu", który nie sprawdzi się przy wszystkich usługach.

Dostawcy usług coraz bardziej doceniają korzyści z bardziej rozproszonego ich uruchamiania, na przykład jako serwisy uwzględniające lokalizację użytkownika, wstawianie ogłoszeń lokalnych, utrzymywanie rozproszonych kopii usług intensywnie wykorzystywanych (wideo, P2P, itp.), ale w dalszym ciągu niektóre usługi powinny pozostać scentralizowane. W miarę ewoluowania usług rozlokowanie punktów ich świadczenia może się przeogromnie zmieniać w funkcji popytu na nie ze strony użytkowników i w funkcji wymogów optymalizacji kosztów eksploatacyjnych.

Rozwiązanie w tym zakresie powinno być oparte na dodaniu inteligentnej płaszczyzny usługowej, pozwalającej węzłom sieci metropolitalnych na obsługę szerokiej gamy usług. Dostawca usług musi mieć możliwość decydowania, jakie usługi chce zapewniać i gdzie je musi uruchamiać, by architektura pozwalała na świadczenie każdej z nich. W tym modelu praktycznie każdy węzeł sieci metropolitalnej zostaje przekształcony we w pełni „Inteligentny Usługowy Punkt Brzegowy" (*Intelligent Services Edge*). W tym modelu usługę można świadczyć praktycznie w każdym miejscu, co daje wymaganą elastyczność i ostatecznie przekłada się na oczekiwaną elastyczność i szybkość wdrażania usług, pozwalającą na wprowadzanie nowych kreatywnych usług, utrzymywanie dotychczasowych abonentów i pozyskiwanie nowych.

Konwergentna sieć metropolitalna MPLS z wbudowanymi mechanizmami elastycznego wdrażania usług zapewni dostawcy usług przewagę konkurencyjną dzięki najbogatszemu dostępnemu zestawowi narzędzi: VPNy w warstwie L2, VPNy IP, wykrywanie i zapobieganie włamaniom (IDP), zarządzanie abonentami szerokopasmowymi, Session Border Control (SBC), a firma Juniper przyjęła politykę otwarcia swoich platform, by mogły także wykonywać aplikacje opracowane przez firmy zewnętrzne.

MPLS aż do dostępów: ostatni krok!

Zobaczyliśmy, jak jednolita infrastruktura MPLS zapewnia gładką ciągłość między siecią szkieletową i metropolitalną, co pozwala na lokowanie usług tam, gdzie jest to najskuteczniejsze. Jeżeli sieci dostępowa, metropolitalna i szkieletowa działają w różnych technologiach, przenoszenie między nimi usług jest zdecydowanie trudne, może też wymuszać przesuwanie granic między sieciami lub przeprojektowywanie architektury całej sieci.

Dostawcy usług dążą do zapewnienia powszechnego dostępu do swoich usług niezależnie od wykorzystywanych technik dostępowych (xDSL, FTTx, 2G, 3G, 4G), a to wymaga dysponowania skalowalną i odporną na usterki siecią. Forum łączności szerokopasmowej (*Broadband Forum* – BBF) już prowadzi rozważania nad „MPLS aż do węzłów dostępowych" do właśnie takich zastosowań.

W rozwiązaniach z obsługą MPLS „od końca do końca", od chwili gdy pakiet klienta wchodzi do sieci, nie przechodzi już przez punkty nieciągłości, niezależnie od tego, czy pochodzi od klienta mieszkaniowego czy biznesowego, stacjonarnego czy ruchomego, podłączonego tanim łączem dostępowym czy usługowym w warstwie 2, 3 czy nawet 7. Wdrożenie MPLS aż do poziomu węzłów dostępowych zapewnia konwergencję, ponieważ sieć jest jednolita.

Ponadto zapewnia prawdziwą elastyczność usługową pozwalającą na uruchamianie usług tam i wtedy, gdzie i kiedy są potrzebne, jako że typowo LSP dostępowe staje się wirtualnym łączem dostępowym do danej instancji usługi, posadowionej w najstosowniejszym dla niej inteligentnym usługowym węźle brzegowym. Pozwala także na szybkie i łatwe wprowadzanie nowych usług i przenoszenie ich zgodnie ze zmieniającymi się potrzebami.

Wymagania na budowę jednolitej sieci MPLS opisanej powyżej wiążą się z koniecznością zapewnienia wielkiej skalowalności – od poniżej 1000 węzłów dziś, do od 10 do 100 tysięcy węzłów w jednej sieci MPLS obejmującej wszystko, poczynając od dostępów, przez sieć metropolitalną, aż do sieci szkieletowej. Wymaga to także solidnych protokołów, urządzeń oraz systemu eksploatacji i utrzymania (OAM), małych opóźnień i odporności na uszkodzenia zapewniającej przywrócenie usług w 50 milisekund. Architektura sieci spełniającej powyższe wymagania nie może w żaden sposób ograniczać usług.

Technika MPLS wykorzystuje podejście hierarchiczne i sygnalizację międzydomenową (BGP) pozwalające na utworzenie skalowalnego modelu obejmującego wszystko. Architektura realizująca powyższe będzie dzieliła sieć na „regiony" i zapewniała wymaganą w nich łączność. Prostotę zapewni jednolita łączność IP w płaszczyźnie sterującej oraz łączność MPLS dla pakietów wszystkich klientów.

Podsumowanie

Istnieją już sieci umożliwiające świadczenie usług, ale niestety zbyt często architektura takich sieci decyduje o tym, jakie usługi można przez nie oferować. A to usługi powinny dyktować układy połączeń oraz parametry jakościowe i niezawodnościowe.

Budowa konwergentnych sieci metropolitalnych i dodanie do nich swobody świadczenia usług stwarza znaczącą przewagę konkurencyjną dostawców usług, którzy zajmują się wysoko wydajnymi infrastrukturami sieciowymi. Rozszerzenie protokołu MPLS z sieci szkieletowej na metropolitalne i być może nawet na węzły dostępowe zapewni gładką ciągłość usług z większymi możliwościami wpływu na jakość postrzeganą przez klientów, co ostatecznie przyniesie pożądany wzrost dochodowości sieci.

Inteligentne usługowe rozwiązania brzegowe (*Intelligent Service Edge*) w połączeniu z zastosowaniem protokołu MPLS w obszarze dostępowym ostatecznie umożliwią dostawcom usług świadczenie dowolnych usług na właściwą skalę, przy jednoczesnej minimalizacji kosztów zarządzania nimi. Ponadto usługodawcy będą mogli tworzyć dalsze nowatorskie usługi, co ostatecznie pozwoli na działanie metodą prób i nieszkodliwych błędów, która jak dotąd zaowocowała powstaniem najbardziej dochodowych serwisów dostępnych w internecie.

Bo jedynym powodem korzystania przez abonentów z Państwa sieci są oferowane przez nie usługi.

Autorzy są pracownikami firmy Juniper Networks

Sieć digital signage interaktywna i w HD

Grzegorz Kantowicz

Sieciowe projekcje multimedialne

Veracomp SA – specjalizowany dystrybutor rozwiązań teleinformatycznych – wprowadził na polski rynek nowe odtwarzacze do dystrybucji multimedialnych treści na cyfrowych ekranach i zarządzania nimi w ramach sieci digital signage – Cayin SMP-WEBPLUS i SMP-WEBPLUS-T.

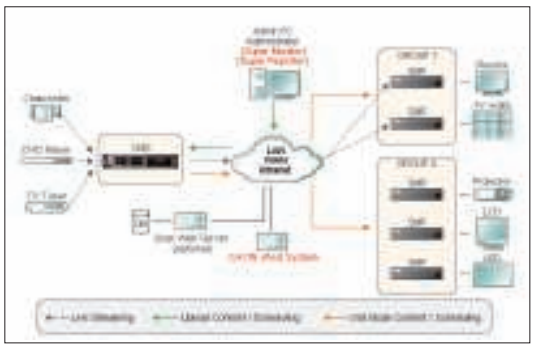
Odtwarzacze umożliwiają zbudowanie interaktywnej i obsługującej rozdzielczość High Definition sieci digital signage (systemu dystrybucji multimedialnej treści połączonych w sieć, centralnie i zdalnie zarządzanych wyświetlaczy), złożonej z nawet tysięcy cyfrowych ekranów. Działający w oparciu o SMP-WEBPLUS i SMP-WEBPLUS-T firmy Cayin Technology system jest centralnie i zdalnie zarządzany i oferuje duże możliwości konfiguracji multimedialnej zawartości.

Dzięki nowym odtwarzaczom digital signage można równocześnie, na wszystkich podpiętych cyfrowych ekranach, zaprezentować pliki HD, animacje Flash, HTML, zdjęcia JPG, tekst i streaming plików wideo (dwóch jednocześnie). Co istotne, w przypadku urządzeń działających bez przerwy w nieprzychylnej sprzętowi IT przestrzeni publicznej, posiadają funkcję odzyskiwania systemu oraz rozwiązania automatyzujące ich pracę. Odtwarzacze same wyświetlają treści według wcześniej zaprogramowanego schematu, automatycznie wykrywają sieci, dokonują zmiany zawartości po jej uaktualnieniu na serwerze i zdalnie aktualizują oprogramowanie.

Za pomocą Cayin SMP-WEBPLUS-T można stworzyć interaktywne środowisko, nakładając na podłączony do odtwarzacza ekran panel dotykowy. Urządzenie współpracuje z większością paneli dotykowych dostępnych na rynku producentów (m.in. Tyco Electronics, Lumio, NextWindow). Z kolei Cayin SMP-WEBPLUS (o oznaczeniu LB500) różni się od modelu „T" i poprzednika (LB300) mniejszymi, kompaktowymi rozmiarami, które ułatwiają jego montaż. Urządzenie wyposażone jest w wejście DVI-D, dzięki czemu materiały wideo czy zdjęcia dostarczane z odtwarzacza wyświetlają się na wielu ekranach błyskawicznie i bez straty jakości. Co więcej, nowy Cayin obsługuje sieć bezprzewodową (802.11b/g), umożliwiając zdalne zarządzanie jego zawartością za pośrednictwem WiFi.

– Interaktywność zwiększa zainteresowanie klientów cyfrowymi ekranami, angażuje przechodnia i pobudza go do działania, co przekłada się na większą skuteczność przekazu – powiedział **Michał Rędziak**, kierownik ds. systemów audiowizualnych w Veracomp SA. *– Nowe odtwarzacze zostały zaprojektowane ze względu na rosnące zainteresowanie systemami digital signage ze strony reklamodawców i oczekiwaniem przez klientów większej interaktywności. Jak pokazują najnowsze badania, w 2009 r. przychody z reklamy za pomocą nośników DS będą stanowiły 0,5 proc. całego rynku reklamy, a w 2012 roku udział ten przekroczy 2 proc.*

Odtwarzacze z serii SMP-WEBPLUS, dzięki obsłudze wszystkich popularnych języków programistycznych (np. Flash, DHTML, CSS, etc.), gwarantują dużą swobodę w tworzeniu multimedialnych treści. Urządzenia przeznaczone są do prezentowania zaawansowanych multimediów oraz interaktywnych aplikacji. Odtwarzacze mają otwartą strukturę i tworzą skalowalną platformę do łatwej integracji. Mogą pracować zarówno pojedynczo, połączone w sieć i zarządzane poprzez internet, jak i podłączone do serwera w istniejącej infrastrukturze sieciowej przedsiębiorstwa.



Digital signage to sieć cyfrowych ekranów centralnie i zdalnie zarządzanych. Za ich pomocą można rozpowszechniać równocześnie treści promocyjne, rozrywkowe i informacyjne, by przykuć uwagę klientów. W Veracomp dostępne są wszystkie niezbędne elementy systemu: ekrany LCD (public display NEC i SHARP, LCD MAG), projektory (Optoma, SHARP) lub cylindryczne ekrany LED 360 stopni (DynaScan), ponadto dedykowane do digital signage odtwarzacze i serwery wraz z oprogramowaniem do zarządzania treścią (Cayin Technology) oraz niezbędne akcesoria (jak np. splittery, przełączniki i matriksy ATEN). Funkcjonalność DS mogą wzbogacić systemy montażowe (Edbak, Ergotron), urządzenia do przetwarzania i dystrybucji przekazów multimedialnych (Kramer Electronics), głośniki emitujące dźwięk kierunkowy (Panphonics) oraz folia do tylnej projekcji Vikuiti (3M). ■

Rozwiązanie dla producentów telewizyjnych i filmowych

Grzegorz Kantowicz

Zarządzanie pamięcią w produkcji materiałów HD

Avid Technology zaprezentował kolejną wersję systemu Avid Unity™ ISIS® 2.0, przeznaczonego do przechowywania i zarządzania dużą ilością materiałów cyfrowych. Dzięki ISIS® 2.0 producenci telewizyjni i filmowi mogą ograniczyć koszty związane z utrzymaniem kilku systemów pamięci oraz przyśpieszyć edycję materiałów cyfrowych.

Nowe narzędzie oferuje większą pamięć (384 TB), skalowanie w czasie rzeczywistym do 330 klientów równocześnie i wysoki poziom zabezpieczeń przechowywanych danych. Umożliwia też zaangażowanie w proces produkcji wszystkich osób zaangażowanych w projekt, w tym również spoza zespołu.

Avid Unity ISIS to podsystem pamięci oparty na inteligentnej architekturze komputerowej, tzw. *blade-based*. Co charakterystyczne, pamięć wbudowana jest bezpośrednio w bibliotekę. Jej wyposażenie obejmuje m.in. elementy inteligentnej pamięci typu dual-drive, zintegrowane przełączanie Ethernet oraz nadmiarowe zasilanie i chłodzenie. W przeciwieństwie do sieci pamięci masowej (SAN), autorównoważąca architektura Avid Unity ISIS dystrybuuje dane i metadane tak, aby każdy element pamięci mógł podejmować natychmiastowe decyzje. Dzięki temu wydajność systemu pozostaje cały czas zoptymalizowana. Ponadto w sytuacji awarii lub wymiany elementu system automatycznie adaptuje się, zapewniając nieprzerwaną dostępność.

Następującą opinię na temat pracy z systemem Avid Unity ISIS wyraził **Ian Burling**, szef działu pomocy technicznej w firmie Films@59 LTD: – *Wydajność 10 GB połączenia klienckiego w systemie Avid Unity ISIS znacząco przyśpieszyła produkcję. Mogliśmy połączyć kilka systemów Avid Symphony™ pracujących z nieskompresowanym materiałem HD o różnej liczbie klatek na sekundę, a każdy z systemów obsługiwał kilka strumieni jednocześnie. Mimo to, nie byliśmy w stanie w pełni wykorzystać szerokości oferowanego przez system pasma. Avid Unity ISIS 2.0 jest również bardzo pomocny podczas szeregowania pakietów do edycji online. Wcześniej, aby móc wydajnie pracować z nieskompresowanym materiałem HD, musieliśmy korzystać z pamięci SCSI, co ograniczało swobodę przenoszenia projektów pomiędzy stanowiskami. Dla firmy, która zajmuje się edycją materiałów HD, szeregowanie stanowi nieodłączną i – niestety – bardzo żmudną część naszej pracy. Dlatego też obsługa wysokiej rozdzielczości jest dla nas olbrzymim atutem, gdyż znacząco przyśpiesza produkcję.*

Udoskonalenia Avid Unity ISIS 2.0 obejmują:

- wysoko wydajną infrastrukturę, która umożliwia natychmiastowy i jednoczesny dostęp do materiałów wielu użytkownikom – pozwala oszczędzić czas dzięki połączeniu cykli produkcji offline i online w jednym systemie;
- dostęp do klienta Ethernetu 10 GB/s obsługującego nieskompresowane materiały HD i 2K, dzięki wydajności każdego z silników ISIS wynoszącej do 400 MB/s i skalowaniu w 12 silnikach o maksymalnej wydajności wynoszącej 4,8 GB/s, 32 strumienie nieskompresowanego materiału HD albo 240 strumieni skompresowanego materiału HD;
- większą elastyczność umożliwiającą szybkie zmiany priorytetu i linii czasowej. System eliminuje koszty związane z posiadaniem kilku stacji przetwarzających, urządzeń wyjściowych i podobnych narzędzi. Pozwala przyłączyć klientów spoza zespołu montażowego – zarówno rejestratorzy materiału, dziennikarze, jak i producenci mogą pracować jednocześnie;
- zwiększoną całkowitą pojemność pamięci systemu do 384 TB (pojemność maksymalna) lub do 196 TB (przy pełnej symetrii), z monitorowaniem całego systemu. W trybie lustrzanym opcja ta umożliwia klientom przechowywanie do 300 godzin nieskompresowanego materiału HD lub do 6300 godzin skompresowanego materiału HD 50 MB/s;
- wirtualizację umożliwiającą elastyczne i dokładne przydzielanie zasobów pamięci w określonych warunkach, z opcją uwzględniającą dzienne, godzinne i minutowe zmiany szeregowania bez przestojów;
- siedem poziomów zabezpieczeń systemu zapewniających kopię zapasową materiałów HD – inaczej niż w tradycyjnych systemach RAID, które w przypadku wystąpienia błędu mogą wymagać natychmiastowej interwencji użytkownika, a podczas procesu przywracania mogą zużywać 50 proc. lub więcej wydajności systemu. System pozwala zaoszczędzić czas i koszty związane z przestojami, jakie mogą mieć miejsce w innych systemach. ■

Beta tester systemu Avid Unity ISIS 2.0

Telewizja cyfrowa najnowszej generacji dla partnerów

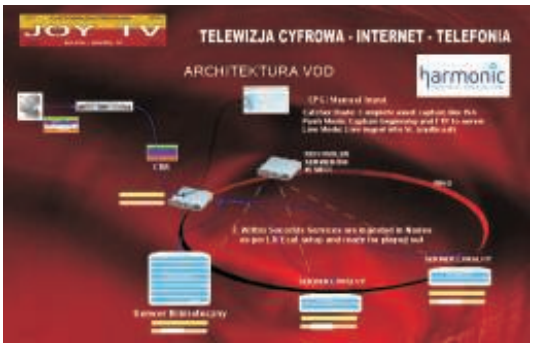
Kablowa cyfrowa interaktywna platforma multimedialna JOY TV INTERACTIVE

W związku zrozwojem usług cyfrowych w Polsce, pragniemy Państwu zaprezentować najnowszą wersję naszej platformy cyfrowej JOY TV przeznaczoną dla firm internetowych IPTV i kablowych DVB-C na terenie naszego kraju.

dla partnerów:

Platforma **JOY TV** oparta jest całkowicie na urządzeniach firmy **HARMONIC INC USA** – zarówno system multipleksacji, transkodowania i szyfrowania, jak i serwery **VoD (Video on Demand)**. Platforma JOY TV przygotowana jest do współpracy z urządzeniami przystosowanymi do pracy w sieciach **IP**, jak i **DVB-C**. W sieciach DVB-C możliwe jest zastosowanie **interaktywności** poprzez wprowadzenie urządzeń hybrydowych (STB-ów odbiorników cyfrowych DVB przystosowanych do komunikacji zwrotnej) odbywającej się np. za pomocą modemu kablowego. Obecnie system jest zintegrowany z urządzeniami firmy Motorola.

Poniżej schemat kompletnego systemu **VoD** (jednego z najbardziej złożonych elementów systemu), na którym bazuje nasza platforma.



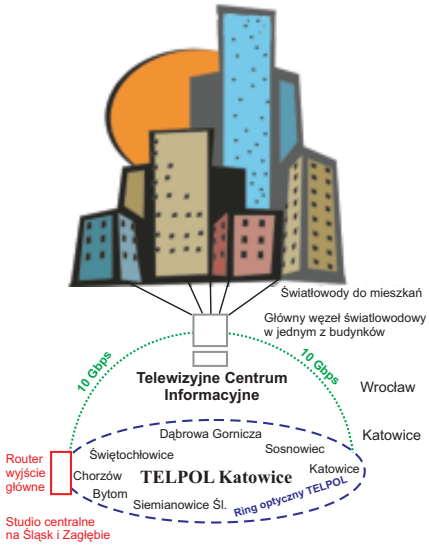
Dla sieci IPTV posiadamy przygotowany midleware, system do wyświetlania programów TV zintegrowany z usługami WIDEO. System ten zawiera typowe funkcje telewizyjne dostępne w STB DVB-C oraz dodatkowe usługi interaktywne zawarte w serwisie **e-dom.**

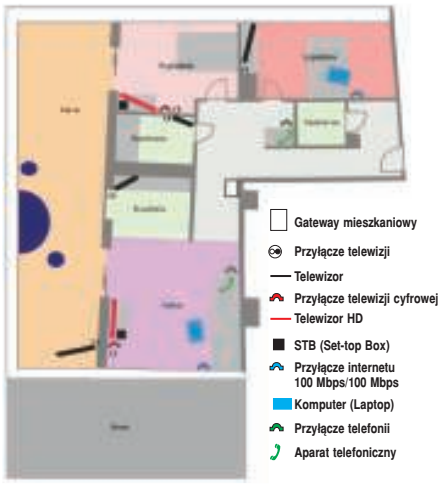
Niebagatelną rolę przy tworzeniu naszej platformy odegrało przygotowanie oferty dla największych obiektów mieszkalnych w kraju.

To nowatorskie rozwiązanie spotkało się z dużym zainteresowaniem i firmy te być może zdecydują się na jego wdrożenie.

Wszystkie elementy rozwiązania pracują w naszych sieciach interaktywnej telewizji cyfrowej i oprócz części mieszkalnej są zintegrowane z obiektami rekreacyjnymi, handlowymi i innymi. Wszystkie informacje są przekazywane mieszkańcom na ekrany telewizorów (nawet w każdym pomieszczeniu).

Poniżej pokazujemy Państwu kilka elementów rozwiązania.





Przykładowy schemat rozmieszczenia przyłączy (apartament)

Fragment portalu TV dla mieszkańców

Nasza Platforma JOY TV

Obsługa kanałów TV:

- bardzo rozbudowane EPG (elektroniczny przewodnik programowy), niespotykane funkcje na innych platformach
  - wyszukiwanie programów;
  - wyszukiwanie audycji;
- nasze informacje o najciekawszych programach, audycjach sportowych, filmach i innych;
- wyszukiwanie audycji programu z podglądem dowolnego kanału;
- radio;
- mail;
- chat;
- zarządzanie odbiornikiem TV, szybkie ustawienia (język, napisy), listy ulubionych programów, kontrola rodzicielska.

Serwis **e-dom – interaktywna usługa zawierająca najbardziej przydatne i użyteczne informacje i usługi interaktywne (cieszący się dużą oglądalnością).**

Po ostatniej modyfikacji (15.02.2009 r.) bardziej przypomina portal internetowy niż telewizję cyfrową.

Na serwis **e-dom** składa się **portal e-dom i niektóre pozycje menu głównego**:

- dostęp do internetu – ulubione;
- data, kalendarz;
- kilka ważnych, bieżących informacji on-line;
- oferta firmy TELPOL lub współpracującej
  - telewizja,
  - telefonia,
  - internet;
- serwis news on-line;
- serwis pogodowy on-line;
- kanały telewizji internetowej;
- wiele, wiele innych ciekawych informacji;
- możliwość integracji reklamy lub informacji o swoich usługach w portalu **e-dom** w kilku pozycjach;
- dla wsparcia funkcji opisowych dostępna jest klawiaturka bezprzewodowa.

Serwis e-dom będzie ciągle rozwijany! Być może przy współpracy z Waszą firmą

Obecnie Platforma **JOY TV** jest przystosowana do pracy w sieciach kablowych ze wszystkimi STB pracującymi w systemie CONAX z wbudowanym dyskiem twardym, STB z PVR dostępne są również dla platform IPTV. Dodatkowo istnieje możliwość wprowadzenia STB interaktywnych dla sieci DVB, są one całkowicie przystosowane do współpracy z systemami **WIDEO na żądanie** (VoD) i zawierają wszystkie funkcje dostępne dla sieci IPTV.

Oprócz ciekawych i ciągle rozwijanych funkcji i możliwości w naszej platformie posiadamy bogaty content telewizyjny podzielony na różne pakiety. Warto zwrócić uwagę na to, iż na dzień dzisiejszy mamy w naszej ofercie dziewięć kanałów HD. Dla Partnerów przewidujemy możliwość dodania dowolnej funkcji w serwisie **e-dom** oraz dowolnego kanału nie będącego w naszej ofercie. A dla firm współpracujących wysokie prowizje!

Ostatnią nowością w naszych sieciach jest wsparcie naszej Platformy **JOY TV** przez pakiety internetowe **Bronze Interactive 6+3/1,5**, **Silver Interactive 8+3/3** oraz **Gold Interactive 25+3/5 Mbps** już w technologii **Docsis 3.0**.

Niebagatelną rolę odgrywa nasz serwis i monitoring, który zapewniają nam firmy zachodnie oraz firma KLONEX z Opola.

Czytaj więcej na naszej stronie internetowej www.telpol.net.pl

Internet na domowych ekranach telewizyjnych

Grzegorz Kantowicz

Przystawki internetowe

Podczas targów CES NETGEAR zaprezentował dwa nowe produkty umożliwiające korzystanie z internetowego wideo, telewizji, muzyki, zdjęć, mediów HD i innych treści na ekranie telewizora HDTV. NETGEAR Internet TV Player (ITV2000) i NETGEAR Digital Entertainer Elite (EVA9150) zaprojektowano z myślą o wzbogaceniu cyfrowej rozrywki.

Internet TV Player (ITV2000)

NETGEAR Internet TV Player (ITV2000) to kompaktowa, łatwa w użyciu i automatycznie konfigurująca internetowa przystawka do telewizora z prostym pilotem, umożliwiająca oglądanie internetowego wideo w miejscu, w którym wcześniej nie było to możliwe – na ekranie telewizora w salonie. Zamiast oglądać filmy na komputerach PC w oddzielnych pokojach, rodziny mogą teraz wspólnie oglądać wideo z różnych internetowych źródeł na ekranie telewizora, korzystając z wygód salonu czy pokoju telewizyjnego.

Internet TV Player zwiększa zakres zastosowań nowych telewizorów HDTV, a także starszych telewizorów analogowych. To idealne urządzenie dla rodzin aktywnie korzystających z internetowych treści wideo, a także dla tych, którzy znajdują się poza krajem czy regionem, w którym nadawane są ich ulubione programy telewizyjne, na przykład międzynarodowe wydarzenia sportowe czy filmowe produkcje. Urządzenie strumieniowo przesyła treści z popularnych witryn, takich jak BBC.com, CNN.com, ESPN.com, EuroSport.com, NBC.com, PGATour i TMZ.com, a także z repozytoriów nagrań wideo, takich jak YouTube, Google Videos™, Yahoo Videos™ i MetaCafe™. NETGEAR Internet TV Player obsługuje strumieniowe przesyłanie transmisji TV na żywo z różnych witryn internetowych na świecie, płatnych filmów na żądanie z witryn takich, jak CinemaNow.com, a także filmów ściąganych z serwisów takich, jak BitTorrent®. Zaawansowana funkcja wyszukiwania VTap™ umożliwia inteligentne przeszukiwanie internetowych zasobów wideo, w tym wybieranie witryn wideo według kraju, tematyki, nazwisk osób czy popularnych witryn. Użytkownicy mogą również odtwarzać wideo, muzykę i zdjęcia z lokalnych pamięci flash USB lub serwerów mediów z rodziny NETGEAR ReadyNAS®.

Kompaktowy Internet TV Player jest niewiele większy niż talia kart. Urządzenie łączy się z domową siecią i internetem poprzez adapter USB Ethernet lub adapter sieci bezprzewodowej. Nie wymaga komputera PC do odtwarzania internetowego wideo; nie wymaga również instalowania żadnego oprogramowania na komputerze PC ani konfigurowania ustawień współdzielenia plików czy zezwoleń w zaporze. NETGEAR Internet TV Player (ITV2000) dostępny będzie w sprzedaży na początku lata 2009 roku.

Digital Entertainer Elite (EVA9150)

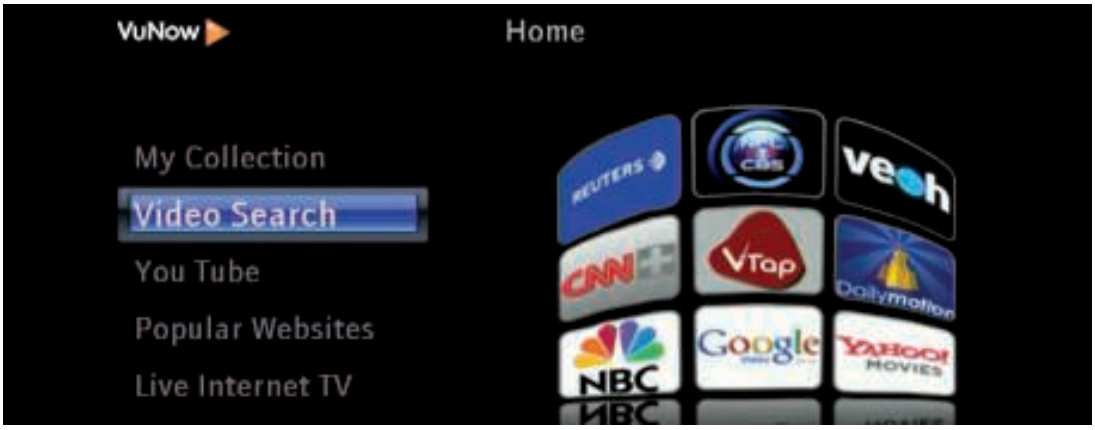
NETGEAR Digital Entertainer Elite (EVA9150) to idealne rozwiązanie dla zaawansowanych entuzjastów mediów. To najwydajniejszy i najbardziej elastyczny odtwarzacz mediów cyfrowych na rynku, obsługujący najnowsze technologie wideo, audio oraz sieci bezprzewodowe.

Urządzenie ze zintegrowanym twardym dyskiem o pojemności 500 GB można łatwo rozbudować o większą pojemność. Użytkownicy mogą odtwarzać na ekranie telewizora filmy cyfrowe o jakości Blu-Ray (do 1080p), oglądać zdjęcia cyfrowe w wysokiej rozdzielczości, odtwarzać pliki MP3 i programy telewizyjne nagrane na komputerze PC lub przechowywane w lokalnej sieci. Urządzenie daje również dostęp do treści z internetu, takich jak YouTube, internetowe radio, Flickr™, kanały RSS i materiały wideo z popularnych witryn internetowych.

Digital Entertainer Elite automatycznie wynajduje wszystkie pliki z cyfrowymi mediami w sieci domowej i organizuje je w łatwo dostępną bibliotekę. Digital Entertainer Elite jest rozwiązaniem wyjątkowym, ponieważ współpracuje jednocześnie z komputerami Windows®, Mac® i Linux, a także z serwerami NAS, takimi jak seria NETGEAR.

Urządzenie obsługuje niezrównanie obszerną listę formatów plików, w tym:

- **formaty wideo:** AVI, DivX, Xvid WMV, MOV, M4V, MP4, VOB, MPG, MP1, MP2, P4, ISO, IFO, MKV, TS i M2TS;
- **formaty audio:** MP1, MP2, MP3, WMA, WMA-Pro, AAC, FLAC, AIFF, WAV, LPCM, Dolby AC3 5.1 stereo downmix, Dolby AC3 5.1 passthrough, DTS 5.1 passthrough, Dolby TrueHD Downmix, Dolby+ Passthrough i DTS-HD Master Audio passthrough;
- **formaty napisów:** SUB, SRT, SMI, SAMI, TXT i DVD Subpicture oraz,
- **kodeki wideo:** MP1, MP2, MP4, Xvid, VC-1/WMV-9, H.264 i OpenDivX.



Digital Entertainer Elite ma dwa porty USB umożliwiające błyskawiczny dostęp do treści w przenośnych pamięciach flash USB, aparatach cyfrowych, odtwarzaczach iPod® lub innych magazynach danych ze złączem USB. Dzięki trzem wewnętrznym metamateriałowym antenom NETGEAR RangeMax™ i dwuzakresowej sieci bezprzewodowej 802.11n, Digital Entertainer Elite zapewnia najwyższą wydajność pracy bezprzewodowej spośród wszystkich odtwarzaczy mediów cyfrowych na rynku. Dwuzakresowa sieć bezprzewodowa umożliwia korzystanie nie tylko z trzech kanałów 2,4 GHz, w których pracuje już bardzo wiele urządzeń 802.11g, lecz także z 20 rzadziej wykorzystywanych kanałów w paśmie 5 GHz. Ponadto układ Sigma Designs 8635 zapewnia najwydajniejszą i najbardziej elastyczną wydajność przetwarzania danych audio i wideo.

W domu może pracować jednocześnie wiele urządzeń NETGEAR Digital Entertainer Elite. Korzystając z funkcji „Follow Me" użytkownik może zatrzymać odtwarzane wideo i kontynuować oglądanie w innym pomieszczeniu. W trybie „Party" możliwa jest synchronizacja odtwarzania muzyki w całym domu.

Digital Entertainer Elite wyposażono również w wielokrotnie nagradzaną funkcję NETGEAR Push 'N' Connect, która łatwo i bezpiecznie łączy bezprzewodowe urządzenia klienckie w systemie Wi-Fi Protected Set-up (WPS), eliminując konieczność pamiętania i wprowadzania haseł.

Ponadto NETGEAR Digital Entertainer Elite jest przyjazny środowisku i wyróżnia się energooszczędnością oraz funkcją automatycznego przechodzenia w stan uśpienia. ■

Jak zunifikować interakcję?

Grzegorz Kantowicz

Interactive Media Manager – element telewizji przyszłości

Obserwując rynek telewizyjny w ostatnich latach można zauważyć kolejne etapy jego rozwoju. Początkowo walka o klienta rozpoczęła się od oferowania większej liczby kanałów, następnie jakości cyfrowej, a obecnie rozdzielczości HD. A co czeka nas w niedalekiej przyszłości? Telewizja mobilna? Telewizja interaktywna? Docelowo będzie to interaktywna telewizja 3-ekranowa, czyli telewizja na telewizorze, komputerze oraz telefonie komórkowym, w której przełączanie programów pilotem zostanie zastąpione interakcją z programem i dostarczaniem treści zgodnie z preferencjami widza.

Personalizacja medium pociąga za sobą jednak konieczność szybkiego tworzenia dużej liczby serwisów, tak jak to ma miejsce w modelu internetowym, a do tego potrzebne są dedykowane narzędzia edytorskie (WYSIWYG). Nie da się również przygotowywać interaktywnych serwisów telewizyjnych na masową skalę rysując je pixel po pixelu, dlatego np. w Wielkiej Brytanii – wiodącym w Europie rynku telewizji interaktywnej – 80 proc. usług interaktywnych przygotowuje się przy pomocy szablonów.

Rozwiązanie takie proponuje m.in. firma Alcatel-Lucent pod nazwą *Interactive Media Manager* (*IMM*). Umożliwia ono budowanie całych serwisów jako sekwencji pojedynczych szablonów (*screen-flow*), na które nakłada się szatę graficzną. Takie podejście umożliwia między innymi zmianę szaty graficznej w zależności od pory dnia przy zachowaniu tej samej struktury serwisu – prosty zabieg, a znacznie poprawia wrażenie dynamizmu. Dla każdego medium telewizyjnego (satelita, IPTV, MobileTV) tworzy się specyficzne szablony, dzięki czemu usługi dostarczane na ekrany o różnych możliwościach nie muszą być sprowadzane do najmniejszego wspólnego mianownika.

Alcatel-Lucent dostarcza gotowe biblioteki szablonów m.in. do interaktywnych reklam, programów sponsorowanych, quizów, konkursów, badań opinii publicznej, portali telewizyjnych. Szczególnym powodzeniem cieszą się interaktywne reklamy, które pozwalają na pogodzenie różnych oczekiwań. Wielu widzów (w Polsce około 45 proc.) traktuje reklamę jak intruza i chciałoby mieć możliwość jej przewijania, co jest w oczywisty sposób sprzeczne z interesem reklamodawców.

Dla odmiany reklama interaktywna ma dla użytkowników większą wartość informacyjną, a nawet rozrywkową, natomiast dla reklamodawców marketingową. Wystarczy sobie wyobrazić możliwość obejrzenia samochodu z różnej perspektywy (wnętrze, karoseria, silnik), zamówienia broszury informacyjnej na konto e-mail czy możliwość wygrania jazdy testowej. System umożliwia również integrację z zewnętrznymi źródłami danych, dzięki czemu widz na życzenie może obejrzeć najnowsze wiadomości, prognozę pogody, listę przebojów filmowych czy inne informacje związane z oglądanym programem. Można również zostać współrealizatorem transmisji sportowej – np. po naciśnięciu czerwonego przycisku na pilocie obejrzeć aktualne statystyki z meczu piłkarskiego, tabele ligowe, historię klubu, profile ulubionych zawodników czy kupić klubową koszulkę lub zapisać się do fan-klubu.

Rozwiązanie *Interactive Media Manager* firmy Alcatel-Lucent obsługuje wszelkie modele interaktywności (pilot, klawiatura, SMS, MMS, e-mail) i jest wykorzystywane przez największe firmy medialne, którym rokrocznie przynosi krociowe zyski z interaktywnych reklam, programów sponsorowanych, głosowań oraz konkursów. ■

Ericsson stawia na rozwiązania multimedialne

Grzegorz Kantowicz

IPTV dla małych osiedli i telewizja mobilna dla wszystkich

Ericsson Consumer Lab ogłosił wyniki badań przeprowadzonych w latach 2007/2008 na wybranych rynkach europejskich i w USA. Wyniki potwierdzają zainteresowanie użytkowników końcowych rozwiązaniami mobilnej telewizji i IPTV. W domach użytkowników internetu na podłączenie do sieci oczekuje średnio siedem ekranów – są to ekrany komputerowe, telewizyjne, wyświetlacze odtwarzaczy MP3 czy ekrany telefonów komórkowych.

Rozwiązanie firmy Ericsson ukryte w skrzynce o rozmiarach 50x50 zapewnia dostęp do sieci szerokopasmowej oraz dostarczenie szeregu atrakcyjnych usług, m.in. IPTV dla 12-24 odbiorców w jednej lokalizacji. Ericsson EDA 1200 jest małą szafką, którą operator telekomunikacyjny może zamontować w budynku. Produkt ten jest częścią kompleksowego rozwiązania *IPTV Network Infrastructure*.

Przepustowość łącza realizowana przez to rozwiązanie pozwala na równoczesne korzystanie z wielu usług i urządzeń. W tym samym czasie przeciętna rodzina może korzystać z pojedynczego łącza bez straty na jakości usług, które są uruchomione. Dla przykładu, podczas gdy dzieci używają aplikacji i gier on-line, mama może jednocześnie sprawdzać nowe przepisy kucharskie w internecie i rozmawiać z przyjaciółką, a tata korzystając z łącza może w tym samym czasie oglądać ulubiony program telewizyjny i nagrywać film, który jest dostępny na innym kanale, również w systemie *video on demand*.

Z punktu widzenia operatora telekomunikacyjnego, instalowanie węzłów dostępowych bliżej użytkowników końcowych oznacza wzrost liczby punktów dostępowych VDSL2, co ułatwia rozbudowę sieci i oferowanie nowych usług, np. telewizji wysokiej rozdzielczości. Jest to rozwiązanie w pełni skalowalne, umożliwiające dostarczenie szerokopasmowego łącza (dziesiątki Mb/s) zarówno do mieszkańców małego osiedla, jak i dużych grup użytkowników.

Ericsson EDA 1200 – EDA RSC24c spełnia wymagania dla sprzętu instalowanego w lokalizacjach niezabezpieczonych przed wpływem warunków atmosferycznych. Obudowa sprzętu zapewnia niskie kosztowo, wysoce elastyczne i bardzo skalowalne rozwiązanie. Ponadto EDA RSC24c używa bezpośredniego chłodzenia powietrzem zamiast tradycyjnej jednostki wymieniającej powietrze. Oznacza to całkowity brak uciążliwego szumu, oszczędności kosztowe sięgające 35 proc. w porównaniu do tradycyjnych rozwiązań oraz łatwiejsze utrzymanie sprzętu. Szafka może być montowana zarówno na ścianie, jak i na podłożu.

Jednocześnie Ericsson Consumer Lab twierdzi, że telewizja mobilna będzie najpopularniejszym serwisem multimedialnym. Mobile TV, aplikacja najbardziej pożądana przez użytkowników, to telewizja i wideo na żądanie oraz nagrywanie filmów.

W Polsce Ericsson wdraża u operatorów rozwiązania pozwalające na pełną usługę telewizji mobilnej, jednakże dotychczas dostępne są jedynie usługi tradycyjnej telewizji w komórce. Telewizja na żądanie oraz podcast są znane odbiorcom w USA, aż 22 proc. użytkowników amerykańskich zaznajomionych z tą technologią chciałoby korzystać z niej w większym stopniu.

EDA RSC24c

Szacuje się, że obecnie 3 proc. posiadaczy telefonów komórkowych w badanych krajach korzysta z aplikacji Mobile TV. Procent zainteresowanych Mobile TV sięga 30 proc. na rynkach brytyjskim i szwedzkim. Mobile TV to znacznie więcej niż tradycyjna telewizja dostosowana do małego ekranu. Aplikacja jest spersonalizowana, interaktywna i można dzięki niej oglądać cokolwiek się zapragnie, bez względu na czas, miejsce czy urządzenie. Te cechy – uzupełnione o łatwość obsługi, szybkie przełączanie programów i reklamę skierowaną do konkretnego odbiorcy – powodują, że usługa zwiększa lojalność użytkownika do usługi i do operatora. Mobile TV to także portfolio, które wychodzi ponad standardowe usługi głosowe. Zawiera usługi takie, jak wideo na żądanie czy przeglądanie stron internetowych. Respondenci, których zapytano o zainteresowanie korzystaniem z szerokopasmowego mobilnego internetu, skorzystaliby z niego w domu (80 proc.), w miejscach publicznych (65 proc.) czy w czasie podróży (63 proc.).

Już ponad 170 operatorów na świecie uruchomiło komercyjnie usługi mobilnej telewizji i wideo. Do końca 2011 roku telewizję za pośrednictwem komórki będzie oglądać niemal pół miliarda osób na całym świecie. Z badań przeprowadzonych przez firmę Ericsson wynika, że klienci spodziewają się od Mobile TV znacznie więcej niż przeniesienia oferty za pośrednictwem komórki. Są skłonni płacić od 10 do 15 euro miesięcznie. To ogromna szansa dla operatorów i nadawców, którzy mogą dodatkowo zwielokrotnić przychody z mobilnej telewizji wprowadzając opłaty za kontent, reklamę tradycyjnej telewizji na mały ekran, za korzystanie z nowych możliwości, za konkursy i głosowania, a nawet wirtualne zakupy. ■

Portale społecznościowe na celowniku hakerów

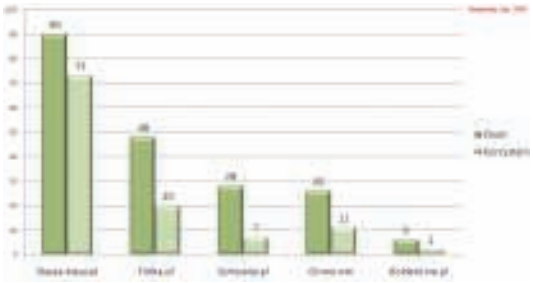
Maciej Ziarek

Pokaż swoje konto, a powiem Ci kim jesteś...

Bez wątpienia serwisy społecznościowe przeżywają teraz w Polsce swoje pięć minut. Nie ma w tym nic dziwnego – w końcu pozwalają nam na łatwe i szybkie nawiązywanie nowych znajomości, odnajdywanie starych znajomych, których nie widzieliśmy od wielu lat, a czasami nawet na znalezienie miłości naszego życia. Pod tym względem serwisy społecznościowe są o wiele efektywniejsze od forów internetowych czy komunikatorów. Ich popularność cały czas rośnie, przybywa użytkowników, a w związku z tym – także i danych osobowych...

W artykule skupiłem się przede wszystkim na najpopularniejszych serwisach w Polsce. Należą do nich Nasza-klasa.pl, Grono.net, Sympatia.pl, Fotka.pl oraz GoldenLine.pl.

Wchodząc po raz pierwszy na te portale, widzimy ambitne hasła o odnalezieniu starych znajomych czy poznaniu wielkiej społeczności internetowej. Tego typu slogany z pewnością zachęcają do rejestracji i dzielenia się swoimi danymi. O tym, jak bardzo popularne są obecnie portale społecznościowe, możemy się przekonać, patrząc na wyniki sondy (http://www.smgkrc.pl/hotnews5pl.html) wykonanej przez Instytut MillwardBrown SMG/KRC na zlecenie D-Link Technology Trend. Wykres przedstawia, ile procent internautów zna i korzysta z portali społecznościowych.



Rys. 1. Znajomość serwisów społecznościowych wśród polskich internautów

Z tego samego badania dowiadujemy się, że o istnieniu takich serwisów wie 53 proc. Polaków, a korzysta z nich 31 proc. Daje to niebagatelną liczbę kilku milionów użytkowników.

Tyle danych osobowych to z kolei pokaźna liczba informacji, które mogłyby być potencjalnie wykorzystane, dlatego należy je odpowiednio zabezpieczyć. Na forach internetowych najczęściej podajemy tylko adres e-mail, ewentualnie nr komunikatora. Portale społecznościowe natomiast, po uzupełnieniu profilu, mogą przechowywać:

- imię i nazwisko;
- datę urodzenia/wiek;
- numery komunikatorów;
- numer telefonu komórkowego;
- zdjęcia, filmy;
- adres e-mail;
- miejsca nauki/pracy;
- wykształcenie;
- listę znajomych/rodzinę;
- CV.

Informacje te mogą być w niektórych przypadkach dostępne za pomocą jednego kliknięcia!

Do czego można wykorzystać dane osobowe? Scenariuszy jest wiele, a wachlarz metod użycia tych informacji jest ograniczony jedynie pomysłowością osoby, która je zbiera. Ktoś może podawać się za nas na forach lub listach dyskusyjnych i oczerniać nasze imię czy reputację. Im więcej danych zdobędzie, tym lepiej będzie mógł wypełnić profil, uwiarygodniając w ten sposób swoje wypowiedzi. Upubliczniając nasz adres e-mail lub numer komunikatora, możemy stać się ofiarami spamu i spimu (spam rozsyłany poprzez komunikatory internetowe). Dojść może także do większych nadużyć, jak próba fałszowania czyjejś tożsamości.

Nigdy też nie wiadomo, z kim tak naprawdę mamy do czynienia w sieci, wypowiadając się na forum czy rozmawiając z nieznajomym przez komunikator. Mało kto podałby świeżo poznanej osobie takie informacje, jak numer telefonu komórkowego czy własne zdjęcia. A jednak niektórzy udostępniają takie dane w serwisach społecznościowych, umożliwiając wgląd do nich każdemu zarejestrowanemu. Nie jest problemem (zadając odpowiednie pytanie np. w Google) odszukanie informacji o kimś po szczątkowych danych, jak np. numer komunikatora. Głównie dzięki portalom społecznościowym.

Należy także pamiętać, że w Sieci nic nigdy nie ginie. Jeżeli ktoś doda do swojego konta zdjęcia na pograniczu dobrego smaku lub wręcz kompromitujące fotografie, musi liczyć się z tym, że za 10 lat zdjęcia te nadal będzie można odnaleźć w Sieci, nawet jeżeli wcześniej zostały wykasowane. Można by rzec, że internet nie wybacza błędów młodości...

Ze względu na olbrzymią ilość przechowywanych danych osobowych, portale społecznościowe muszą dostosować się do obowiązującego na terenie Polski prawa, zwłaszcza do ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 roku. W myśl tej ustawy, na straży ochrony danych osobowych stoi GIODO (Generalny Inspektor Ochrony Danych Osobowych). W ustawie tej znajdują się od-

powiednie artykuły, w myśl których instytucje oraz serwisy zbierające i przetwarzające dane osobowe winny w należyty sposób je zabezpieczyć:

„Art. 36. Administrator danych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem. (Dz. U. z dnia 29 października 1997 r.)".

Przyjrzyjmy się zatem regulaminom wybranych serwisów społecznościowych:

Nasza-klasa.pl:

„Nasza Klasa, spółka z ograniczoną odpowiedzialnością z siedzibą we Wrocławiu, zapewnia wszystkim zarejestrowanym użytkownikom realizację uprawnień wynikających z ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. nr 133, pozycja 883), w szczególności prawo wglądu do własnych danych, prawo żądania aktualizacji i usunięcia danych oraz prawo wniesienia sprzeciwu w przypadkach określonych w przepisach tej ustawy. Baza danych osobowych prowadzona przez Serwis została zgłoszona do Generalnego Inspektora Ochrony Danych Osobowych".

Fotka.pl:

„Dokonując rejestracji w serwisie internetowym Fotka.pl, Użytkownik wyraża zgodę na przetwarzanie swoich danych osobowych zgodnie z Polityką Ochrony Prywatności przedstawioną w dalszej części Regulaminu oraz zgodnie z ustawą z dnia 29 sierpnia 1997 r. o Ochronie Danych Osobowych oraz ustawą z dnia 18 lipca 2002 roku o świadczeniu Usług Drogą Elektroniczną z późniejszym zmianami".

Sympatia.pl:

„Grupa Onet.pl SA, jako administrator danych osobowych serwisu Sympatia, dba o najwyższe bezpieczeństwo udostępnionych naszej firmie danych. Są one szczególnie chronione i zabezpieczone przed dostępem osób nieupoważnionych (...) Zbiór danych osobowych serwisu Sympatia został zgłoszony do Generalnego Inspektora Danych Osobowych".

Grono.net:

„Wraz z rejestracją użytkownik wyraża zgodę na gromadzenie, przetwarzanie oraz wykorzystywanie przekazanych przez siebie danych osobowych przez serwis Grono.net w celach statystycznych i marketingowych (...) Gromadzone przez serwis dane nie będą udostępniane innym podmiotom, chyba że po uzyskaniu uprzedniej zgody użytkownika".

GoldenLine.pl:

„GoldenLine powierzył przetwarzanie danych osobowych Użytkownika OVH Sp. z o.o. z siedzibą we Wrocławiu, przy ul. Powstańców Śląskich 16/18, w zakresie niezbędnym do prawidłowego wykonania czynności związanych z hostingiem portalu internetowego www.goldenline.pl na podstawie pisemnej umowy zawartej zgodnie z art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.)".

Z regulaminów tych jasno wynika, że wszystkie wyżej wymienione serwisy zobowiązują się do należytego przechowywania danych osobowych i ochrony ich przed dostępem osób trzecich.

16 stycznia 2008 r. w biurze GIODO odbyła się konferencja prasowa „Czy nasze dane osobowe są bezpieczne na portalu nasza-klasa.pl?". W związku z bardzo szybko rosnącą popularnością tego portalu, Generalny Inspektor Ochrony Danych Osobowych postanowił przyjrzeć się bliżej serwisowi, a konkretnie sprawdzić, czy wywiązuje się on z przepisów i obowiązków, jakie narzuca na niego ustawa o ochronie danych osobowych.

4 lutego w biurze GIODO odbyła się kolejna konferencja prasowa „Co się stało z Naszą-klasą?". Przedstawiono na niej wyniki kontroli. Chociaż były pewne zastrzeżenia (m.in. do szyfrowania podczas logowania do serwisu, a właściwie jego braku), to generalnie serwis wypadł pozytywnie. GIODO Michał Serzycki powiedział na konferencji m.in.:

„Na tyle, na ile pozwala internet, użytkownicy Naszej-klasy są zabezpieczeni dobrze, ale trzeba mieć świadomość tego, że internet nie jest miejscem bezpiecznym, w związku z tym zawsze może dojść do wycieku informacji, zawsze może się znaleźć genialny hacker, który złamie te zabezpieczenia, tak jak zawsze się znajdzie doskonały złodziej, który otworzy najlepiej nawet zabezpieczony samochód. A druga kwestia, zawsze na końcu jest człowiek, człowiek, który może skusić się chęcią zarobku i po prostu zgrać te dane i wynieść".

Po kontroli serwisu nasza-klasa.pl przez GIODO i orzeknięciu, że dane są chronione i przechowywane w sposób prawidłowy, stosunkowo szybko pojawił się kontrowersyjny i niepokojący artykuł w serwisie Hacking.pl. Jego autor stwierdził, że:

„Dane 7 mln (prawie 8 mln) użytkowników, niestety – każdy może sobie pobrać na swój własny komputer przy pomocy np. VPS za 5 $. Dane – takie jak imię, nazwisko (często również rodowe), ukończona szkoła, zdjęcia, czasem numer telefonu i gg – nie są ukryte".

Pojawiła się groźba wycieku danych osobowych milionów użytkowników. Autor pokazał nawet sposób, w jaki pobrał powyższe informacje o kontach i zapisał je w postaci tabeli w Excelu. Sposób ten polegał na użyciu programu cURL. Jest to aplikacja, która pozwala nam wysłać lub pobrać z serwerów treść formularzy. Działa z wiersza poleceń i obsługuje ta-

Rys. 2. Arkusz Excela zawierający dane osobowe z serwisu nasza-klasa.pl

kie protokoły, jak FTP, FTPS, HTTP, HTTPS, SCP, SFTP, TFTP i inne. Nie wdając się w szczegóły techniczne sposobu, w jaki wszedł w posiadanie danych osobowych, autor zaprezentował na łamach serwisu Hacking.pl zrzut ekranu przedstawiający tabelkę Excela.

Na pierwszy rzut oka mogłoby się wydawać, że rzeczywiście miało tu miejsce duże niedociągnięcie ze strony GIODO, skoro udało się wyciągnąć tyle informacji. Sytuacja staje się jednak bardziej klarowna, kiedy przyjrzymy się sposobowi, w jaki działa program cURL, oraz uzyskanym przy jego pomocy danym. Jak wcześniej wspomniałem, program pozwala przy użyciu odpowiedniej składni wysłać lub pobrać formularz z serwera. Oznacza to, że atakujący wszedł w posiadanie jedynie informacji, które są w portalu nasza-klasa.pl ogólnodostępne z poziomu zwykłego użytkownika. Jeżeli ktoś podał jedynie imię i nazwisko i żadnych dodatkowych informacji, to tylko to znalazłoby się w tej tabeli Excela. Fakt ten potwierdzony jest także przez zespół naszej-klasy.pl.

W poniższym fragmencie oficjalnego komentarza możemy przeczytać:

„Autor artykułu z hacking.pl zasymulował na komputerze osobę, która „chodząc" po profilach użytkowników używa opcji „Zapisz stronę jako...;". Dostępne są więc dla niej tylko te informacje, które dany użytkownik zdecydował się ujawnić. Takie spisywanie można by także praktykować w sposób tradycyjny, używając długopisu i kartki – komputer wykona to oczywiście zdecydowanie szybciej. Zespół naszej-klasy.pl posługuje się wieloma mechanizmami, które pozwalają zweryfikować, czy po serwisie porusza się prawdziwy człowiek, czy maszyna, co pozwala nam skutecznie walczyć z takimi nadużyciami".

Zatem w tym przypadku nie można mówić o wycieku danych osobowych sensu stricte. Nikt nie wejdzie w posiadanie naszego maila, jeśli nie jest upubliczniony, czy ukrytych danych kontaktowych, jak numer komunikatora czy telefonu komórkowego. Jednak reakcja mediów była błyskawiczna, a prostowanie tego doniesienia najczęściej ograniczało się do dopisywania komentarzy pod newsami przez bardziej świadomych sytuacji użytkowników.

Podobna sytuacja miała miejsce już wcześniej (styczeń 2007), lecz dotyczyła serwisu Grono.net. Sprawa dotyczyła danych osobowych, które zostały zindeksowane przez Google, a tym samym stały się dostępne dla każdego, nawet niezarejestrowanego na portalu Grono.net internauty. Zaczęło się od publikacji artykułu w serwisie wiadomości24, w którym autor po wpisaniu frazy Grono.net do wyszukiwarki Google otrzymał dane osobowe użytkowników, nazwiska, telefony, adresy e-mail itd. Nie da się zaprzeczyć, że takie dane dostępne z poziomu wyszukiwarki stanowią niekontrolowany wyciek, a więc błąd. Jakby było tego mało, pojawiły się informacje, że za pomocą Google można się także dostać do skrzynek wiadomości serwisu. Grono.net sprawę potraktowało poważnie. W końcu ustalono przyczynę takiego stanu rzeczy. We fragmencie oświadczenia zarządu Grono.net możemy przeczytać:

Co się stało?

„W wyszukiwarce Google w wyniku błędu skryptu indeksującego znalazły się informacje o użytkownikach grono.net, które normalnie dostępne są dla innych użytkowników grono.net, a nie dla wszystkich internautów. Są to informacje, które użytkownicy sami zdecydowali się uczynić publicznymi dla innych członków grono.net. Ani ich charakter, ani zakres nie powodował żadnego zagrożenia – np. uzyskania dostępu do poczty czy przejęcia konta użytkownika. Przyczyna usterki została przez grono.net usunięta. Zwróciliśmy się także do Google o usunięcie w trybie ekspresowym z wyszukiwarki wszystkich informacji pochodzących z grono.net.".

Jakie dane znalazły się w Google?

„Skrypt indeksujący Google Bot był zarejestrowany w serwisie grono.net jako zwykły użytkownik i miał dostęp wyłącznie do widocznych publicznie danych – tych samych, do jakich dostęp mają wszyscy użytkownicy grono.net. Dostępne były więc dane, które sam użytkownik zdecydował się ujawnić innym uczestnikom grono.net. Nie znalazły się w Google zastrzeżone dane konta użytkownika, hasła itd. Nie zostały także ujawnione dane, które użytkownik uczynił dostępnymi np. wyłącznie znajomym. Google Bot nie indeksował także ukrytych gron, ani żadnych innych informacji, których członkowie społeczności grono.net nie chcieli ujawnić. Zindeksowane zostały więc wyłącznie informacje widoczne dla każdego z miliona użytkowników serwisu. W okresie współpracy reklamowej z systemem Google skrypt zindeksował jedynie ok. 15 proc. profili użytkowników grono.net.".

Innym zagrożeniem, które często przemilcza się, a na które narażony jest każdy użytkownik większych serwisów czy portali, nie tylko społecznościowych, jest phishing. Jest to wyrafinowana metoda wyciągania wszelkich informacji z komputera ofiary. Atakujący wysyła do ofiary maila z linkiem do zainfekowanej strony, gdzie użytkownik podaje dane dotyczące np. konta w banku lub proszony jest o pobranie pliku, który okazuje się trojanem. Z pozoru metoda wydaje się prosta i pozbawiona sensu (bo kto podałby takie dane na życzenie nieznajomego), jednak sprawa staje się jasna, gdy przyjrzymy się takiemu mailowi:

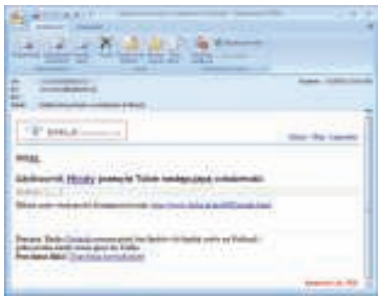
Rys. 3. Przykład wiadomości phishingowej

Z założenia wiadomość ma być łudząco podobna do maila, jaki mógłby zostać wysłany przez bank. Przynajmniej tak ma myśleć ofiara. W treści najczęściej proszeni jesteśmy o podanie nowego hasła lub autoryzację transakcji na konkretnej stronie. Jed-

nak strona ta nie jest prawdziwą stroną banku, lecz witryną spreparowaną przez cyberprzestępcę (adres tej strony to w powyższym przypadku http://host217-36-231-196.in-addr.btopenworld.com/aspnet_client/system_web/1_1_4322/XXXXXX.htm i nie trzeba być ekspertem, aby zauważyć, że nie jest to adres banku), by przechwycić podawane na niej informacje.

Ten sam mechanizm może zostać zastosowany w odniesieniu do serwisów społecznościowych. Użytkownicy mogą otrzymywać maile informujące, że w związku ze zmianami na portalu proszeni są o kontrolne zalogowanie się. Klikając link podany w liście, przechodzą na stronę łudząco podobną do prawdziwej. Dalej scenariusz powtarza się tak samo, jak w przypadku banku.

Na taki problem ostatnio natrafiły dwa serwisy społecznościowe: nasza-klasa.pl oraz fotka.pl. Scenariusz działania był jednak trochę inny niż ten przedstawiony wyżej. Na konta mailowe masowo rozsyłano informację, że jakiś użytkownik napisał do nas wiadomość lub chce pokazać swoje zdjęcia. Autentyczności tej wiadomości miała dodać treść od użytkownika wraz z odnośnikiem do strony przypominającej oryginalną.



Rys. 4. Sfałszowana wiadomość serwisu fotka.pl

Po przejściu na stronę podaną w liście na ekranie pojawiał się komunikat, że nie można wyświetlić treści strony z powodu braku odpowiedniej wersji programu Flash Player.

Rys. 5. Sfałszowana i zainfekowana strona, do której prowadzi odsyłacz z przedstawionego powyżej maila

Proponowano przy tym pobranie pliku o nazwie get_new_flashplayer.exe, który to miał zainstalować na naszej maszynie najnowszą wersję oprogramowania. Oczywiście nie był to Flash Player, tylko backdoor: Backdoor.Win32.Agent.cri.

Jak wcześniej pisałem, podobny problem napotkał serwis nasza-klasa.pl.

Rys. 6. Szkodliwy program wykryty przez oprogramowanie firmy Kaspersky Lab

Rys. 7. Sfałszowana wiadomość serwisu nasza-klasa.pl

Rys. 8. Prośba o pobranie i instalację odpowiedniego oprogramowania

Kilka szczegółów pozwalało odróżnić te wiadomości od prawdziwych:

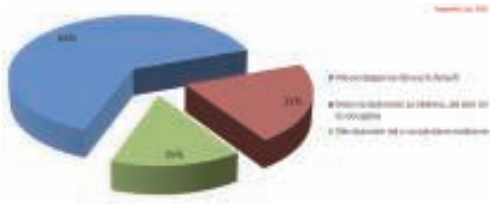
- w temacie wiadomości zabrakło polskiego znaku (uzytkownik, zamiast użytkownik);
- w większości maili rozsyłanych do internautów widniały obcojęzycznie brzmiące nazwy użytkowników, a początek wiadomości często pisany był w innym języku;
- link widniejący w wiadomości nie pokrywał się z adresem ładowanej strony;
- prawie wszystkie odnośniki na zainfekowanej stronie rozpoczynały pobieranie zainfekowanego pliku;
- w linkach występowały domeny inne niż polskie (pl).

Serwisy traktujące o bezpieczeństwie zareagowały błyskawicznie, informując o podejrzanych wiadomościach. Także same portale fotka.pl i nasza-klasa.pl umieściły stosowne informacje na swoich łamach.

Dlaczego fałszerze wybrali właśnie te portale? Aby odpowiedzieć na to pytanie, wystarczy odwołać się do statystyk popularności, które zamieściłem na początku artykułu. Zarówno nasza-klasa.pl, jak i fotka.pl są najbardziej znanymi i odwiedzanymi polskimi serwisami społecznościowymi, a ponieważ atakujący rozsyłali wiadomości do przypadkowych osób, szansa trafienia w użytkowników tych portali była bardzo duża (zwłaszcza w przypadku naszej-klasy.pl). Dodatkowo wchodził w grę element socjotechniczny. Nie od dzisiaj wiadomo, że człowiek

z natury jest ciekawski. W mailach tych widać tylko krótki fragment wiadomości, zatem istniało bardzo duże prawdopodobieństwo, że zaintrygowany użytkownik kliknie link. Nie możemy jednak popadać w przesadę – rejestracja w serwisach społecznościowych sama w sobie nie niesie zagrożenia, niemniej zwiększa ryzyko, że przypadkowo zostaniemy oszukani – jeżeli ktoś nigdy nie rejestrował się w takim portalu i nagle dostaje informacje o czekającym na niego zaproszeniu do grona znajomych, stosunkowo szybko powinien zdać sobie sprawę, że jest to mail fałszywy.

Na zakończenie ponownie odwołam się do sondy wykonanej przez Instytut MillwardBrown SMG/KRC na zlecenie D-Link Technology Trend. Tym razem chcę zwrócić uwagę na świadomość użytkowników w zakresie ryzyka związanego z podawaniem danych osobowych w internecie.



Rys. 9. Świadomość ryzyka związanego z podawaniem danych osobowych

28 stycznia 2008 roku w *Życiu Warszawy* ukazała się rozmowa Karoliny Woźniak z GIODO Michałem Serzyckim. Oto jak odpowiedział na pytanie dotyczące bezpieczeństwa danych osobowych w sieci:

Czy internet jest rzeczywiście tak niebezpieczny?

„Niestety tak, użytkownicy powinni sobie zdawać sprawę z tego, że nasze dane nie zawsze są najlepiej chronione, a wirtualna rzeczywistość to kopalnia wiedzy na nasz temat. Można tu wykraść nie tylko nasz adres czy numer telefonu, ale też dowiedzieć się, jakie mamy preferencje, zainteresowania, sprawdzić, po jakich stronach surfujemy. Dlatego tak ważne jest zachowanie ostrożności. Hackerzy zawsze znajdą bowiem sposób na złamanie nawet najlepszych zabezpieczeń".

Biorąc pod uwagę fragment powyższej rozmowy oraz wspomnianą już sondę, z pewnością cieszy fakt, że prawie 2/3 użytkowników serwisów społecznościowych zdaje sobie sprawę z ryzyka, o jakim mówił GIODO, i nie umieszcza ważniejszych informacji o sobie. Z drugiej strony, pozostaje 1/3 użytkowników, którzy albo wcale nie przejmują się bezpieczeństwem swoich danych osobowych, albo mając świadomość ryzyka – podejmują je. Ceńmy swoje dane, własną prywatność oraz tożsamość. Czy wszyscy muszą znać Twój numer komunikatora oraz telefonu? Czy koniecznie w profilu musisz mieć 30 różnych zdjęć, będących przekrojem Twojego życia, a nawet życia Twoich bliskich i znajomych? Jeżeli jest taka możliwość, ukrywaj dane dla osób niezarejestrowanych i takich, które nie należą do grona Twoich znajomych. Pamiętaj, że jeżeli ktoś bardzo będzie chciał się z Tobą skontaktować, zrobi to chociażby przez wysłanie zwykłego e-maila.

Autor jest niezależnym analitykiem współpracującym z Kaspersky Lab Polska

17-19.03.2009

Łódź

20 lat

INTERTELECOM

XX Międzynarodowe Targi Komunikacji Elektronicznej

Tereny targowe: Łódź, ul. Stefanowskiego / Skorupki

www.intertelecom.info

Patroni Medialni:

Patronat Branżowy:

Organizator:

Bezpieczeństwo danych w urządzeniach przenośnych

Grzegorz Kantowicz

Rosnąca świadomość i brak działań

Firma Symantec opublikowała wyniki badań na temat ochrony przed utratą danych (Data Loss Prevention). Badania te wykazały, że ponad połowa firm jest świadoma niebezpieczeństwa utraty kluczowych i poufnych danych. Ponad 70 proc. respondentów określa własność intelektualną jako ważną lub bardzo ważną dla finansowego powodzenia prowadzonego biznesu. Mimo to wciąż występują rozbieżności pomiędzy wdrażanymi przez firmy standardami ochrony danych a rzeczywistością – dotyczy to przede wszystkim urządzeń przenośnych.

Badanie zostało przeprowadzone wśród 105 respondentów z polskich firm różnej wielkości i prowadzących zróżnicowaną działalność – od zakładów przemysłowych po doradztwo finansowe. Wyniki pokazują, że chociaż większość respondentów (ponad 73 proc.) posiada podstawowe strategie zapobiegania utracie danych, to ponad połowa nie widzi konieczności wprowadzania środków zabezpieczających przed utratą danych przechowywanych na urządzeniach przenośnych. Ponadto 41 proc. polskich przedsiębiorstw zezwala pracownikom na korzystanie z urządzeń przenośnych bez żadnych ograniczeń. Najbardziej restrykcyjną politykę w tym względzie mają Anglicy – tylko 23 proc. pracowników ma nieograniczony dostęp do urządzeń mobilnych, natomiast w Holandii aż 65 proc.

Pozytywnym wnioskiem z badania jest fakt, że rośnie świadomość tego, jak łatwym celem mogą stać się informacje poufne. Ponad 55 proc. badanych przedsiębiorstw potwierdziło, że obawia się utraty danych, a ponad jedna trzecia respondentów utraciła dane przynajmniej raz. Firmy wśród najczęstszych i najpoważniejszych konsekwencji utraty danych wymieniają straty finansowe (27 proc.), utratę klientów (prawie 25 proc.) oraz utratę dobrego wizerunku (17 proc.). W związku z wysokim zagrożeniem oraz rosnącą świadomością istniejącego niebezpieczeństwa, nie zaskakuje fakt, że prawie trzy czwarte przedsiębiorstw posiada strategię ochrony danych. Najczęściej stosowane narzędzia w ramach takiej strategii obejmują kontrolę dostępu do sieci (80 proc.), szyfrowanie (44 proc.) i kontrolę urządzeń (57 proc.) oraz rozwiązania umożliwiające zapobieganie utracie danych (55 proc.).

– *Cieszy nas fakt, że coraz więcej polskich firm dostrzega, jak ważne jest zabezpieczenie poufnych informacji – zarówno zasobów wewnętrznych, jak i danych klientów czy partnerów. Przyrost informacji, ich dostępność oraz łatwość rozpowszechniania, wraz z coraz większą mobilnością pracowników, znacznie utrudnia organizacjom to zadanie* – powiedział **Piotr Chrobot**, Country Manager polskiego oddziału firmy Symantec. – *Aby zmniejszyć ryzyko i skutki utraty danych, przedsiębiorstwa muszą najpierw odpowiedzieć na trzy najważniejsze pytania: Gdzie przechowywane są ich poufne informacje, w jaki sposób dane te są wykorzystywane oraz jak najlepiej zapobiec ich utracie?*

Mobilność a bezpieczeństwo danych

Dane zawierające własność intelektualną są coraz bardziej mobilne: chociaż tylko 13 proc. polskich firm udostępnia pracownikom urządzenia smartphone i organizery (PDA), to już ponad 75 proc. respondentów wyposaża swoich pracowników w komputery przenośne. Średnia europejska wynosi 70 proc. w przypadku komputerów przenośnych oraz 37 proc. w przypadku urządzeń smartphone i PDA. Firmy powinny pamiętać, że dane przechowywane na urządzeniach mobilnych są najbardziej narażone na kradzież lub niekontrolowany wyciek.

W Polsce prawie 46 proc. badanych firm posiada ścisłe wytyczne regulujące wykorzystanie urządzeń przenośnych, w tym takich nośników, jak pamięć USB. Zaskakujące jest to, że 41 proc. przedsiębiorstw zezwala na nieograniczone użycie wszystkich przenośnych nośników pamięci, co zwiększa zagrożenie wycieku danych. W razie utraty takiego urządzenia można podjąć działania zapobiegające

użyciu przechowywanych danych przez osoby niepowołane. Takie rozwiązania są wykorzystywane przez ponad 45 proc. respondentów z polskich firm. W większości przypadków polegają one na kontroli dostępu do sieci, zarządzaniu urządzeniami przenośnymi oraz szyfrowaniu danych zapisanych na tych nośnikach.

– *Pracownicy często wolą używać w pracy własnych urządzeń, takich jak elektroniczne kalendarze, zacierając tym samym granice pomiędzy danymi prywatnymi a firmowymi. Utrudnia to kierownictwu działu IT zabezpieczenie danych oraz zarządzanie nimi. Wymaga to wdrażania wytycznych, szkolenia pracowników oraz szyfrowania i kontroli dostępu do danych, aby zapewnić wiedzę na temat położenia i sposobów wykorzystania danych w dowolnym momencie* – powiedział Piotr Chrobot z firmy Symantec.

Uwaga! Strzeż się szpiegów

Dane przedsiębiorstw, także te przechowywane na urządzeniach przenośnych, stają się coraz cenniejszym towarem. Motywy przechwytywania danych mogą obejmować osobistą korzyść materialną (np. dane bankowe), jak i systematyczne szpiegostwo przemysłowe. W Polsce tylko jedna czwarta respondentów (24 proc.) obawia się strat będących rezultatem szpiegostwa przemysłowego i postrzega je jako wysokie lub bardzo wysokie zagrożenie dla działania swojej firmy. W Turcji obawy takie ma aż połowa badanych. Najmniej zagrożone czują się firmy z Austrii i Anglii (14 proc.). Większość firm, które doświadczyły takiego ataku, potwierdziła, że miały one ujemny wpływ na konkurencyjność przedsiębiorstwa.

W przeszłości szpiegostwo przemysłowe zakładało wykorzystanie miniaturowych aparatów fotograficznych, natomiast obecnie przybiera formę ataków na bazy danych. Mimo to, mniej niż jedna trzecia przedsiębiorstw posiadających strategię obrony przed szpiegostwem przemysłowym wdrożyła zabezpieczenia będące połączeniem rozwiązań fizycznych oraz informatycznych. Ponad połowa respondentów (51 proc.) nie posiada szczegółowej strategii ochrony lub nie ma pewności, czy takową posiada.

– *Badanie pokazało, że większość polskich przedsiębiorstw jest świadoma zagrożeń związanych z utratą danych* – powiedział Piotr Chrobot z firmy Symantec. – *Podejmowane środki bezpieczeństwa wymagają jednak optymalizacji. Dotyczy to szczególnie bezpieczeństwa urządzeń przenośnych. Wprowadzenie odpowiedniej strategii i kontroli w celu zapobiegania utracie poufnych informacji jest konieczne, ponieważ klienci, partnerzy i pracownicy oczekują wymiany informacji na coraz większą skalę. Skuteczne zapobieganie utracie danych wymaga kompleksowego podejścia. Ten problem nie zostanie bowiem rozwiązany za pomocą samej technologii. Strategia zapobiegania utracie danych powinna być, kompletna i spójna oraz przewidywać zagrożenia we wszystkich częściach organizacji.*

Najważniejsze zalecenia

Aby odpowiednio zabezpieczyć dane i zminimalizować ryzyko ich utraty, firmy powinny określić poziom ryzyka dla wszystkich krytycznych informacji. Organizacje powinny aktywnie rozwijać politykę ochrony danych oraz wdrażać odpowiednie technologie, które integrują aplikacje i procesy biznesowe przy jednoczesnym zachowaniu zgodności z wymogami bezpieczeństwa oraz odpowiednimi przepisami i regulacjami.

Trzeba pamiętać, że techniczne zabezpieczenia nie zapewniają całkowitej ochrony. W wielu przypadkach największym zagrożeniem jest sam użytkownik. Wszyscy pracownicy powinni znać zasady polityki bezpieczeństwa oraz przejść odpowiednie szkolenia. ■

Z czym należy się liczyć

Denis Maslennikov, Boris Yampolsky

Zagrożenia związane z komunikatorami internetowymi

Dla wielu osób komunikacja online stanowi integralną część ich codziennego życia. Internet oferuje wiele możliwości komunikowania się z innymi osobami – pocztę elektroniczną, czaty, fora, blogi itd. Jedną z popularnych opcji są komunikatory internetowe (ang. Instant Messenger – IM), które pozwalają użytkownikom rozmawiać ze sobą w czasie rzeczywistym w dowolnym miejscu na świecie.

Klienty IM

Aby móc korzystać z komunikatora internetowego, użytkownik potrzebuje łącza internetowego i aplikacji klienckiej zainstalowanej na swoim komputerze. Istnieje duży wybór aplikacji IM i prawie wszystkie obsługują te same podstawowe funkcje, umożliwiając szukanie innych użytkowników o podobnych zainteresowaniach, dostęp do profili osobowych, wybór trybów itd. Wiele klientów IM oferuje również dodatkowe funkcje.

Najpopularniejszym klientem IM w Rosji jest bez wątpienia ICQ – żartobliwy skrót frazy „I seek you". Każdy użytkownik ICQ posiada unikatowy numer, lub UIN (*Unified Identification Number*), przy pomocy którego loguje się. Każdy UIN jest zabezpieczony hasłem ustawionym przez użytkownika. Wiadomości są wysyłane za pośrednictwem protokołu TCP/IP przy pomocy formatu specjalnie stworzonego przez twórcę tego komunikatora, firmę Mirabilis. Z reguły jedna wiadomość składa się z jednego pakietu TCP. Kilka innych klientów wykorzystuje zmodyfikowane wersje tego protokołu w celu wysyłania wiadomości, np. QIP (*Quiet Internet Pager*) oraz Miranda.

MSN Messenger (lub *Windows Live Messenger*) firmy Microsoft to kolejny klient IM, który jest popularny wśród użytkowników z Zachodu. MSN Messenger wykorzystuje *Microsoft Notification Protocol* (MSNP, znany również jako *Mobile Status Notification Protocol*). Protokół MSNP2 jest publicznie dostępny, natomiast inne wersje nie są. Najnowsza wersja komunikatora MSN Messenger wykorzystuje wersję MSNP14.

W Chinach bardzo popularny jest QQ, komunikator podobny do ICQ.

Skype, oprócz standardowych funkcji komunikatora internetowego, oferuje również komunikację głosową. Ten popularny na całym świecie program umożliwia użytkownikom darmowe komunikowanie się za pomocą głosu. Aby móc skorzystać z tych funkcji, użytkownik musi posiadać słuchawki z mikrofonem (lub zewnętrzny mikrofon podłączony do komputera), samą aplikację oraz łącze internetowe. Przy pomocy Skype'a można również wykonać rozmowę telefoniczną z dowolnym numerem, jednak usługa ta nie jest darmowa.

Szkodliwe działania

Niestety, świat wirtualny jest otwarty na nadużycia, podatne są na nie również komunikatory internetowe. Komunikatory internetowe często są celem następujących szkodliwych działań:

- kradzież haseł do kont komunikatorów internetowych przy pomocy ataku „brute force" lub socjotechniki;
- rozprzestrzenianie szkodliwego oprogramowania – można tego dokonać na dwa sposoby:
  - wysyłanie wiadomości zawierających odsyłacze – po kliknięciu przez użytkownika na odsyłacz jego komputer PC pobierze plik szkodliwego programu (w celu nakłonienia użytkownika do otwarcia pliku wykorzystuje się socjotechnikę),
  - wysyłanie wiadomości zawierających odsyłacze do zainfekowanych stron internetowych;
- spam.

Wszystkie komunikatory internetowe są podatne na pewne rodzaje zagrożeń. Weźmy na przykład popularny chiński komunikator QQ. Rozpowszechniony w Chinach Trojan-PSW.Win32.QQPass i podobny do niego Worm.Win32.QQPass zostały specjalnie stworzone w celu kradzieży haseł do klienta QQ. Worm.Win32.QQPass rozprzestrzenia się poprzez kopiowanie siebie na nośniki przenośne wraz z plikiem autorun.inf (przez co zapewnia sobie uruchomienie na niezainfekowanym komputerze, pod warunkiem że jest włączona funkcja Autorun).

Również Skype nie umknął uwagi twórców wirusów. Worm.Win32.Skipi rozprzestrzenia się za pośrednictwem Skype'a poprzez wysyłanie odsyłacza do swojego pliku wykonywalnego do wszystkich kontaktów Skype'a na zaatakowanej maszynie. Robak rozprzestrzenia się również poprzez kopiowanie się na nośniki przenośne wraz z plikiem o nazwie „autorun.inf". Ponadto, poprzez edytowanie pliku hosts, uniemożliwia aktualizację rozwiązań antywirusowych i systemu Windows oraz próbuje zakończyć procesy związane z aplikacjami bezpieczeństwa. Oczywiście, obraz nie byłby kompletny bez trojana: Trojan-PSW.Win32.Skyper został stworzony w celu kradzieży haseł do kont Skype'a.

MSN Messenger firmy Microsoft jest aktywnie wykorzystywany do rozprzestrzeniania botów IRC. Wiele z nich potrafi rozprzestrzeniać się za pośrednictwem komunikatora internetowego po otrzymaniu polecenia od zdalnego użytkownika za pośrednictwem backdoora. Na przykład, jeżeli cyberprzestępca posiada niewielki botnet, który chce rozszerzyć, wysyła polecenie do backdoorów na zainfekowanych maszynach. Polecenie to „instruuje" maszyny, aby wysłały wiadomość z odsyłaczem, takim jak

http://www.***.com/www.funnypics.com, do wszystkich kontaktów komunikatora MSN Messenger na tych maszynach. Później wszystko zależy już od osoby, która otrzyma taką wiadomość. Jeżeli zdecyduje się obejrzeć „śmieszne zdjęcia", może to oznaczać, że kolejny komputer zostanie dodany do sieci zombie – poprzez kliknięcie na odsyłacz użytkownik pobiera backdoora na swoją maszynę.

Szkodliwi użytkownicy wykorzystują komunikator MSN Messenger, ponieważ wchodzi on w skład pakietu instalacyjnego systemu Windows. To oznacza, że wszyscy użytkownicy tego systemu automatycznie posiadają klienta MSN na swoich maszynach. Popularność MSN na całym świecie czyni go jeszcze bardziej atrakcyjnym dla cyberprzestępców, którzy chcą zwiększyć liczbę zainfekowanych komputerów w swoich botnetach.

Rysunek 1. Fragment Backdoor.Win32.SdBot.clg. Podkreślone sekcje pokazują polecenia wykorzystywane do rozprzestrzeniania trojana.

Zagrożenia związane z ICQ

Sekcja ta zawiera przegląd najpowszechniejszych metod ataków na klienty IM na przykładzie ICQ.

Kradzież haseł

Jak już wspominaliśmy wcześniej, wszyscy użytkownicy ICQ posiadają niepowtarzalny numer identyfikacyjny lub UIN. Obecnie najpowszechniejsze są numery dziewięciocyfrowe, jednak wielu użytkowników chciałoby, aby ich UIN był taki sam jak ich numer telefonu komórkowego, aby był to liczbowy palindrom lub składał się z tych samych cyfr. Takie numery są łatwe do zapamiętania, a dla niektórych posiadanie takiego numeru jest sprawą prestiżu. Pięcio-, sześcio- lub siedmiocyfrowe numery ICQ, które składają się z dwóch różnych liczb, są uważane za szczególnie cenne.

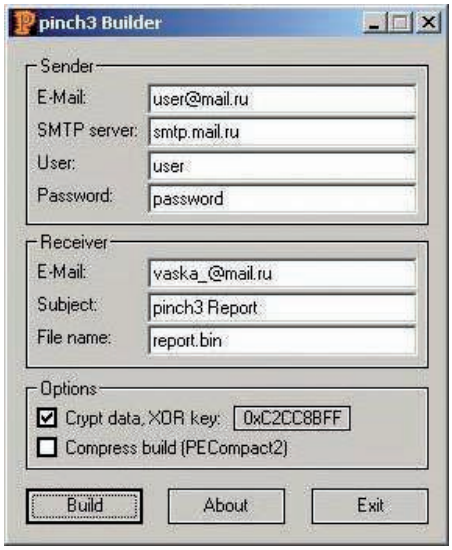
„Atrakcyjne" numery UIN są sprzedawane, często nawet po wysokich cenach. Wiele stron posiada również serwis, za pomocą którego można zamówić numer, i obiecuje „uzyskanie" pożądanego przez klienta numeru. Ponadto osobom zainteresowanym wysyłaniem masowych wiadomości oferowane są niewyróżniające się numery dziewięciocyfrowe. Wykorzystywanie wielu różnych numerów do dystrybuowania spamu pomaga uniknąć czarnych list antyspamowych wykorzystywanych przez zirytowanych użytkowników w celu ignorowania określonych numerów.

Sprzedawcy takich „prestiżowych" numerów rzadko wspominają, w jaki sposób zostały one uzyskane. Strony e-handlu zapewniają, że numery UIN są sprzedawane legalnie, jednak w większości przypadków sprzedawca uzyskał numery ICQ w sposób nielegalny.

Do kradzieży numerów UIN wykorzystuje się wiele metod. Wiele sklepów internetowych sprzedających atrakcyjne numery UIN często bierze udział w poszukiwaniu haseł na skalę przemysłową i kradzieży kont. Inną metodą jest kradzież hasła do poczty elektronicznej użytkownika ICQ, a następnie wykorzystanie go do zmiany oryginalnego hasła UIN bez wiedzy użytkownika. Poniżej szczegółowo opisaliśmy, w jaki sposób to działa.

Pomoc techniczna dla ICQ oferuje usługę dla użytkowników, którzy zapomnieli swoich haseł UIN. Proces przywracania hasła został kilkakrotnie zmodyfikowany i obecnie jest dość wyrafinowany. Stanowi teraz całkiem dobre zabezpieczenie przed kradzieżą haseł. Użytkownicy muszą odpowiedzieć na pytanie, które sami zadali. Jeżeli nie pamiętają odpowiedzi, pytanie może zostać zmienione przy pomocy adresu e-mail podanego w informacjach kontaktowych podczas rejestracji. Proces jest dość bezpieczny, jeżeli jednak osoba trzecia w jakiś sposób uzyska dostęp do poczty elektronicznej, bez trudu zdobędzie też UIN. Po uzyskaniu hasła do poczty elektronicznej szkodliwy użytkownik może skontaktować się z ICQ, podszywając się pod właściciela konta, który zapomniał swojego hasła UIN. Szkodliwy użytkownik może w ten sposób uniemożliwić pierwotnemu właścicielowi uzyskanie dostępu nie tylko do jego własnego konta ICQ, ale również do pierwotnego konta poczty elektronicznej, zmieniając jedynie stare hasło. Kradzież tego typu nie jest łatwa – uzyskanie haseł do kont e-mail połączonych z numerami ICQ wymaga potężnego komputera, a nawet sieci.

Jednak najpopularniejszą metodą kradzieży numerów ICQ jest wykorzystanie szkodliwych programów, w szczególności trojana Trojan-PSW.Win32.LdPinch. W ciągu kilku minionych lat ta rodzina trojanów zaczęła stanowić zagrożenie dla użytkowników. LdPinch nie tylko kradnie hasła do ICQ i innych klientów IM, takich jak Miranda, ale również do kont poczty elektronicznej, różnych programów FTP, gier online itd. Istnieją wyspecjalizowane konstruktory programów do tworzenia określonych typów szkodliwych trojanów. Takie programy umożliwiają ustawienie parametrów określających, które hasła użytkownika zostaną ukradzione przez szkodliwy program po zainstalowaniu się na maszynie. Po skonfigurowaniu programu szkodliwy użytkownik musi tylko podać adres e-mail, na który zostaną wysłane poufne informacje. Łatwość, z jaką można stworzyć ta-



Rysunek 2. Konstruktor wykorzystany do stworzenia trojana Trojan-PSW.Win32.LdPinch

kie szkodliwe programy, powoduje, że są rozpowszechnione nie tylko w ruchu pocztowym, ale również w ruchu IM.

Rozprzestrzenianie szkodliwych programów

Ruch poczty e-mail zawiera szereg różnych rodzin szkodliwych programów, które rozprzestrzeniają własne kopie lub są wysyłane za pośrednictwem spamu. ICQ jest głównie wykorzystywany do rozprzestrzeniania trzech rodzajów szkodliwych programów:

- robaków IM – szkodniki te wykorzystują klienta IM w celu samodzielnego rozprzestrzeniania się;
- trojanów przeznaczonych do kradzieży haseł, łącznie z hasłami do klientów ICQ (w większości przypadków jest to Trojan-PSW.Win32.LdPinch);
- szkodliwych programów sklasyfikowanych przez firmę Kaspersky Lab jako Hoax.Win32.*.* (szkodliwe oprogramowanie stworzone w celu wyłudzania od użytkowników pieniędzy).

W jaki sposób wykorzystuje się ICQ do rozprzestrzeniania szkodliwego oprogramowania?

Robaki IM wymagają niewielkiej interakcji w celu rozprzestrzeniania się. Po uruchomieniu wiele robaków IM wstawia swój kod do kontaktów IM zapisanych na zaatakowanej maszynie. Robaki te posiadają szereg funkcji: mogą kraść hasła, tworzyć botnety, czasem ich funkcja jest czysto destrukcyjna (np. usuwanie wszystkich plików .mp3 z zaatakowanej maszyny). Szkodliwe programy, takie jak Email-Worm.Win32.Warezov oraz Email-Worm.Win32.Zhelatin (Storm Worm), w celu aktywnego rozprzestrzeniania się wykorzystywały ICQ. Jednak w większości przypadków, aby atak mógł się powieść, niezbędne jest działanie ze strony użytkownika. Aby nakłonić potencjalną ofiarę do kliknięcia na odsyłacz i otwarcia pliku pobranego z odsyłacza, stosuje się szereg sztuczek socjotechnicznych.

Oto przykład ataku, którego celem jest pobieranie szkodliwego oprogramowania na maszynę użytkownika. Najpierw szkodliwy użytkownik tworzy kilka kont użytkownika zawierających nęcące informacje w profilu (np. „ładna dziewczyna, 22 lata, szuka chłopaka"). Następnie z numerem tego profilu łączone są boty (niewielkie programy o prymitywnej inteligencji, które potrafią obsługiwać podstawową konwersację). Pierwszą rzeczą, jaką użytkownik chce zobaczyć, jest zwykle zdjęcie owej „ładnej dziewczyny" – bot odpowiada na takie żądania wysyłając odsyłacz. Nie trzeba mówić, że odsyłacz ten nie prowadzi do zdjęcia, ale do szkodliwego programu.

Odmianą tej metody jest przypadek, gdy odsyłacz do szkodliwego programu jest zawarty w danych osobowych „dziewczyny". Tego typu atak wymaga większego wysiłku niż poprzednia metoda. Na przykład, należy wypełnić przynajmniej niektóre z głównych pól dla informacji osobowych i wybrać potencjalne ofiary. Później należy zacząć rozmowę, tak aby przekonać użytkownika do kliknięcia na odsyłacz prowadzący do „fajnych zdjęć z wybrzeża Pacyfiku" w danych osobowych „dziewczyny".

Sztuczki socjotechniczne stosowane są również podczas rozprzestrzeniania szkodliwych programów za pośrednictwem spamu ICQ. Mówiąc ściśle, to nie szkodliwe oprogramowanie jest rozprzestrzeniane – użytkownicy otrzymują odsyłacze do szkodliwego oprogramowania. Odsyłacze w spamie mogą też prowadzić do stron (zarówno tych legalnych, które padły ofiarą włamania hakerów, jak i specjalnie stworzonych w tym celu) zawierających trojany downloadery. Trojany te instalują następnie szkodliwe oprogramowanie na zaatakowanej maszynie. Poniżej znajduje się szczegółowy opis takich ataków.

Luki w przeglądarkach internetowych (zwłaszcza te w Internet Explorer) są często wykorzystywane do pobierania szkodliwego oprogramowania za pomocą szkodliwego kodu, który został wcześniej zamieszczony na stronie internetowej. Najpierw atakowana jest popularna legalna witryna internetowa, na której umieszcza się kod (np. ramka lub zaszyfrowany JavaScript). Kod ten pobiera z kolei szkodliwy program na komputery osób odwiedzających stronę. Inną techniką jest stworzenie prostej strony na tanim lub bezpłatnym serwerze www, która zawiera podobny kod downloadera. Strona taka będzie następnie reklamowana przy pomocy masowej wysyłki za pośrednictwem komunikatorów internetowych. Jeżeli użytkownik kliknie na prowadzący do niej odsyłacz, szkodliwe oprogramowanie zostanie ukradkiem pobrane na maszynę. Użytkownik może nawet nie podejrzewać, że strona, którą odwiedził, została zaatakowana lub jest fałszywa. W tym czasie LdPinch lub IRCBot uruchomią się na zainfekowanym komputerze.

Luki wykorzystywane do przeprowadzania takich ataków mogą być obecne w samych komunikatorach internetowych. W wielu przypadkach luka może powodować przepełnienie buforu i wykonanie losowo wybranego kodu w systemie lub zapewnić zdalny dostęp do komputera bez wiedzy czy zgody użytkownika.

Jeżeli szkodliwy kod, który został uruchomiony w systemie na skutek przepełnienia bufora, jest zdolny do samodzielnego rozprzestrzeniania się, wtedy przy pomocy tej samej luki w zabezpieczeniach aplikacji znajdującej się na innych maszynach program może przeniknąć do komputerów dużej liczby użytkowników, wywołując epidemię. Wykorzystywanie luk w zabezpieczeniach wymaga dużych umiejętności technicznych, co w pewnym stopniu ogranicza opcje dostępne dla cyberprzestępców.

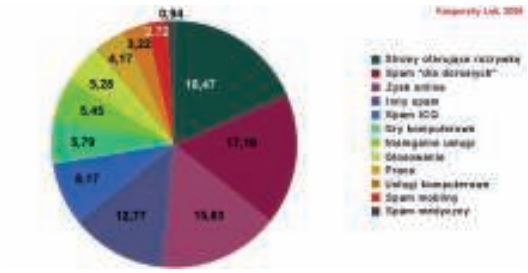
Ostatnio spam ICQ wykorzystywany był do rozprzestrzeniania fałszywych programów, które rzekomo generują PIN-y do kart, przy pomocy których można płacić za różne usługi telefonii komórkowej. Firma Kaspersky Lab wykrywa takie programy jako not-virus.Hoax.Win32.GSMgen. W rzeczywistości takie oprogramowanie generuje nieskończoną ilość losowo wygenerowanych numerów, które rzekomo stanowią kody PIN do kart służących do doładowywania kont telefonów komórkowych. Numery wygenerowane przez program są szyfrowane i aby je odszyfrować, należy uzyskać klucz od autora, za który trzeba naturalnie zapłacić. Kwota jest zwykle niewielka – około 10-15 dolarów – co czyni ofertę jeszcze bardziej atrakcyjną. Ludzie zwykle myślą tak: „Raz zapłacę 15 dolarów i przez resztę życia będę używał telefonu komórkowego za darmo!" Fakt, że otrzymany po zapłaceniu numer nie doładowuje konta, czyni z tego przypadku zwykłą kradzież. Należy zauważyć, że gdyby program rzeczywiście generował kody PIN wykorzystywane do płacenia za usługi telefonii komórkowej, cena byłaby znacznie wyższa, a autorzy staraliby się działać bardziej z ukrycia, tak aby nie zwrócić na siebie uwagi operatorów telefonii komórkowej i organów ścigania.

Spam ICQ

W przeciwieństwie do spamu rozsyłanego za pośrednictwem poczty elektronicznej, spam ICQ nie został dokładnie zbadany. Poniżej przedstawiamy wyniki badania przeprowadzonego w dniach od 23 lutego do 23 marca 2008 roku. Badanie polegało na kategoryzacji tematów niechcianych wiadomości wysłanych do użytkowników ICQ i wykonaniu analizy porównawczej spamu ICQ oraz spamu rozsyłanego za pośrednictwem poczty elektronicznej.

Popularne tematy w spamie ICQ

Tematy wiadomości spamowych ICQ są dość zróżnicowane i mogą zawierać reklamy nowych stron internetowych lub serwerów gier, prośby o głosowanie na określonego uczestnika konkursu, oferty zakupu drogich telefonów komórkowych po obniżonych cenach lub wiadomości zawierające adresy URL prowadzące do szkodliwych programów. Odsyłacz w spamie może prowadzić do strony internetowej zawierającej exploita wykorzystującego luki w zabezpieczeniach przeglądarki Internet Explorer lub innych popularnych przeglądarek (dla celów tego badania wiadomości zawierające zainfekowane odsyłacze nie zostały sklasyfikowane jako oddzielna kategoria).



Rysunek 3. Rozkład spamu ICQ według tematu

Na pierwszym miejscu znalazła się reklama stron oferujących rozrywkę (18,47 proc.). Kategoria ta prawdopodobnie nadal będzie prowadziła w statystykach dotyczących spamu ICQ. Głównym powodem popularności tego rodzaju spamu jest jego skuteczność. Weźmy typową sytuację, gdy osoba pracująca na komputerze od dłuższego czasu otrzymuje wiadomość ICQ o nowej stronie zawierającej mnóstwo zabawnych zdjęć/historyjek/filmów wideo itd. Istnieje duże prawdopodobieństwo, że znużony użytkownik kliknie na odsyłacz, aby na chwilę oderwać się od pracy.

Na drugim miejscu uplasowała się kategoria *Spam dla dorosłych* (17,19 proc.) zawierająca wiadomości przypominające spam rozsyłany za pośrednictwem poczty elektronicznej, który reklamuje strony randkowe, zasoby pornograficzne, prywatne strony zawierające materiały erotyczne itd.

Kategoria *Zysk online* (15,83 proc.) obejmuje wiadomości, które obiecują zarobienie pieniędzy w zamian za klikanie na banery, odwiedzanie określonych stron internetowych i oglądanie reklam. Należą do niej również oferty marketingu sieciowego.

Kategoria *Inny spam* (12,77 proc.) obejmuje wiadomości o różnych tematach. Każdy z nich odpowiada za stosunkowo niski odsetek ruchu spamowego, dlatego nie można sklasyfikować ich do oddzielnych kategorii. Niektórzy z autorów wiadomości z tej kategorii wykazują się dużą wyobraźnią. Wysyłają na przykład łańcuszki, reklamy pasty do zębów, przewidywania arcybiskupów dotyczące faszystowskiej dyktatury w Rosji itd. Wśród reklamowanych artykułów dominują filmy DVD i części samochodowe. Do kategorii *Inny spam* należą również wiadomości phishingowe ICQ, które zostaną omówione w dalszej części artykułu.

Na piątym miejscu znalazły się wiadomości związane z ICQ (8,17 proc.). Interesującym zjawiskiem są „łańcuszki ICQ", z których większość zawiera następujący tekst (przetłumaczony z języka rosyjskiego):

„UWAGA!!! Od 01.12 ICQ będzie usługą płatną. Możesz zapobiec temu wysyłając tę wiadomość do 20 osób z twojej listy kontaktów. To nie jest żart (źródło www.icq.com). Jeżeli wyślesz tę wiadomość 20 razy, otrzymasz e-maila i twój kwiatek zrobi się niebieski. To znaczy, że będziesz wśród tych, którzy są przeciwko. W przypadku przegłosowania ICQ pozostanie darmowy".

Jedyną rzeczą, która się zmienia, jest data i liczba osób, do których należy wysłać tę wiadomość. Interesujące jest to, że niektóre wiadomości zawierają wielopoziomowe cytowanie, co oznacza, że wielu użytkowników naprawdę wierzy, że pewnego dnia „ich kwiatek zrobi się niebieski" i ICQ pozostanie darmowy na zawsze.

Regularnie wysyłane są również wiadomości w różnych językach nakłaniające użytkowników do aktualizacji klienta ICQ do nowej, VI wersji. Na początku nie było wiadomo, dlaczego wiadomości tego typu są tak popularne wśród spamerów. Pojawiła się niepotwierdzona informacja, że ICQ 6.x zawiera lukę w zabezpieczeniach, która prowadzi do błędów podczas przetwarzania wiadomości utworzonych w pewien sposób. 28 lutego 2008 r. informacja ta została potwierdzona: według http://bugtraq.ru, „...wysłanie stworzonej w określony sposób... wiadomości (najprostszym przypadkiem jest „%020000000s") użytkownikowi z zainstalowanym ICQ 6.x spowoduje błąd podczas generowania kodu HTML w celu wyświetlenia wiadomości w osadzonym komponencie Internet Explorera. Błąd ten może prowadzić do wykonania dowolnego kodu w zdalnym systemie". Luka ta nie dotyczy najnowszej wersji klienta ICQ.

Wiadomości z kategorii *Gry komputerowe* (5,79 proc.) można podzielić na dwie duże grupy. Wiadomości z pierwszej grupy reklamują różne gry online oparte na przeglądarce, wiadomości z drugiej grupy – serwery gier, głównie dla Lineage II oraz Counter-Strike.

Oferty *Nielegalnych usług* (5,45 proc.) znajdują się tylko o jedną trzecią punktu procentowego za reklamami gier komputerowych. Oferują one użytkownikom możliwość uzyskania hasła do określonej skrzynki pocztowej, przeprowadzenie ataku DoS, wykonanie fałszywych dokumentów (zarówno rosyjskich i nierosyjskich) oraz kursy łamania kart kredytowych lub możliwość uzyskania informacji niezbędnej do osiągnięcia tego – wszystko za odpowiednią cenę.

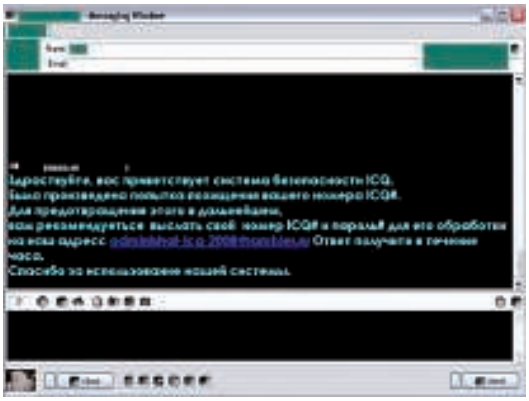
Na ósmej pozycji (5,28 proc.) znalazła się kategoria zawierająca wiadomości proszące odbiorców o głosowanie na określonych uczestników różnych konkursów internetowych.

Na dziewiątym miejscu uplasowały się oferty pracy i wspólnego biznesu (4,17 proc.), na dziesiątym natomiast oferty usług komputerowych, łącznie z hostingiem (3,22 proc.).

Znajdująca się na samym dole rankingu kategoria *Mobilny spam* (2,72 proc.) składa się z dwóch typów wiadomości. Pierwszy typ obejmuje wiadomości reklamujące strony internetowe, na których sprzedawane są telefony komórkowe. Ceny popularnych modeli na takich stronach często są znacznie niższe od cen rynkowych, wzbudzając podejrzenia odnośnie do pochodzenia i legalności takich telefonów. Drugi typ obejmuje wiadomości reklamujące strony zawierające różne treści przygotowane z myślą o telefonach komórkowych.

W okresie od 23 lutego do 23 marca 2008 roku tylko 1 proc. wiadomości w spamie ICQ reklamowało lekarstwa lub usługi zdrowotne.

Od czasu do czasu do użytkowników ICQ wysyłane są wiadomości phishingowe. Wiadomości te nie zostały zaklasyfikowane do oddzielnej grupy, ponieważ występują stosunkowo rzadko. Cyberprzestępcy wykorzystują socjotechnikę, aby uzyskać hasła do numerów UIN użytkowników. Powodzenie lub klęska takich ataków w dużym stopniu zależy od tego, jak dobrze poinformowany jest użytkownik. Jeżeli istnieją rzeczywiste problemy, oficjalny dział pomocy technicznej ICQ poinformuje o nich użytkowników, nigdy jednak nie poprosi ich, aby wysłali swoje hasła za pośrednictwem poczty elektronicznej lub podali je w formularzu na stronie internetowej.



Rysunek 4. Wiadomość phishingowa wysłana w celu uzyskania hasła do konta ICQ
(Tłumaczenie wiadomości: Witam, ta wiadomość została wysłana przez system bezpieczeństwa ICQ. Próbowano ukraść twój numer ICQ. Aby już nigdy podobny przypadek nie miał miejsca, zalecamy, abyś wysłał swój numer ICQ oraz hasło w celu przetworzenia na nasz adres administrat-icqo2008@rambler.ru. Otrzymasz odpowiedź w przeciągu godziny. Dziękujemy za korzystanie z naszego systemu.)

Popularne tematy w spamie ICQ

W przeciwieństwie do poczty elektronicznej, ICQ umożliwia szukanie osób na podstawie ich zainteresowań podanych w informacjach kontaktowych. Dzięki temu cyberprzestępcy mogą kierować spam do określonych osób.

Spamerzy mogą bez trudu uzyskać odpowiednie dane (w większości przypadków jest to wiek oraz zainteresowania użytkowników) i wykorzystać je w celu przyciągnięcia uwagi odbiorców spamu.

Praktycznie wszystkie wiadomości spamowe pochodzą z numerów UIN, których nie ma na liście kontaktów użytkownika. Liczba niechcianych wiadomości otrzymywanych przez użytkownika w danym czasie zależy od numeru UIN. Użytkownicy posiadający sześciocyfrowe numery UIN otrzymują średnio od 15 do 20 niechcianych wiadomości w każdej godzinie, z których wiele zawiera odsyłacze do Trojan-PSW.Win32.LdPinch. Użytkownicy posiadający niczym niewyróżniające się numery dziewięciocyfrowe otrzymują każdego dnia średnio 10-14 takich wiadomości, podczas gdy właściciele „atrakcyjnych" numerów dostają od 2 do 2,5 raza więcej spamu.

Pod względem tematów wiadomości, spam ICQ znacznie różni się od spamu rozsyłanego za pośrednictwem poczty elektronicznej. Podczas gdy około 90 proc. spamu rozsyłanego za pośrednictwem poczty elektronicznej reklamuje różne towary i usługi, odsetek takich reklam w spamie ICQ wynosi niecałe 13 proc. (całkowity udział kategorii *Nielegalne usługi, Usługi komputerowe, Spam mobilny*), z czego *Nielegalne usługi* (5,45 proc.) stanowią największą z wszystkich kategorii oferujących usługi.

Ogólnie w spamie ICQ dominują tematy związane z rozrywką. Wynika to z tego, że ICQ jest rzadko wykorzystywany do komunikacji biznesowej, a większość użytkowników to ludzie młodzi. Spamerzy uwzględniają zainteresowania swoich grup docelowych: w spamie ICQ dominują zaproszenia do odwiedzenia stron oferujących rozrywkę oraz reklamy „dla dorosłych". Spam w kategorii *Gry komputerowe, Głosowanie* oraz *Mobilny spam* również wysyłany jest do młodych ludzi. Ogólnie młodzi ludzie stanowią cel około 50 proc. wszystkich wiadomości spamowych.

Niewielki udział spamu „medycznego" (tradycyjnie wiodąca kategoria w spamie rozsyłanym za pośrednictwem poczty elektronicznej) jest również zdeterminowany przez odbiorców docelowych. W spamie ICQ udział tej kategorii wynosi poniżej 1 proc. Najwidoczniej użytkownicy ICQ nie reagują w sposób zgodny z oczekiwaniami na reklamy towarów i usług medycznych.

Cechy wyróżniające spam ICQ:

- jego celem są młodzi ludzie;
- zorientowany na rozrywkę;
- praktycznie nie reklamuje produktów konsumenckich – wyjątkiem są oferty telefonów komórkowych i produktów farmaceutycznych, jak również niewielka liczba wiadomości należących do kategorii *Inny spam*;
- stosunkowo duży odsetek wiadomości związanych z samym ICQ (8,17 proc.);
- znaczny udział (5,45 proc.) wiadomości oferujących nielegalne usługi. Najbardziej popularne oferty dotyczą włamań do poczty elektronicznej i ICQ, fałszywych dokumentów, łamania kart kredytowych.

Scenariusz ataków

Użytkownik uruchamia plik pobrany za pomocą odsyłacza otrzymanego za pośrednictwem ICQ, jednak obiecane przez spamera zdjęcia nie pojawiają się na ekranie. Użytkownik czeka minutę lub dwie, a w tym czasie trojan przeszukuje jego komputer w celu znalezienia przechowywanych na nim haseł. Niektóre hasła są zaszyfrowane, jednak cyberprzestępcy potrafią je bez trudu odszyfrować. Następnie

trojan zbiera wszystkie hasła znalezione w komputerze i tworzy wiadomość e-mail zawierającą zebrane poufne informacje. Wiadomość zostaje wysłana na adres e-mail cyberprzestępcy, który został utworzony kilka dni przed atakiem. Aby uniemożliwić systemowi Windows ostrzeżenie użytkownika o zagrożeniu, trojan wyłącza zaporę sieciową poprzez zmodyfikowanie odpowiedniego klucza rejestru. Trojan wykonuje podobne działanie w stosunku do innych programów, które mogłyby uniemożliwić mu kradzież haseł i innych istotnych informacji użytkownika. Na koniec szkodliwy program tworzy plik .bat, który usuwa zarówno samego siebie, jak i trojana, niszcząc tym samym ślady szkodliwej aktywności.

Zanim użytkownik zacznie coś podejrzewać, haker przetworzy dziesiątki lub setki wiadomości (w zależności od rozmiaru wysyłki) z hasłami przesłanymi przez trojana. Nawiasem mówiąc, wielu użytkowników w ogóle nie zdaje sobie sprawy, że miała miejsce jakakolwiek szkodliwa aktywność. Jedynym dowodem, jaki posiada użytkownik, jest odsyłacz do nieistniejącego zdjęcia, dlatego szanse na wyśledzenie cyberprzestępcy są bardzo niewielkie.

Użytkownicy często pocieszają się tym, że i tak nie mieli niczego ważnego na swoich komputerach. Jednak haker lub cyberprzestępca jest zupełnie innego zdania: znalazł się w posiadaniu imponującej listy haseł do kont e-mail, klientów FTP i gier online, jak również konta bankowego użytkownika i oczywiście samego konta ICQ.

Ktoś mógłby zapytać, do czego hakerowi potrzebny jest jeszcze jeden dziewięciocyfrowy numer, którego nikt nie zna. Oto dlaczego: haker wprowadzi hasło do klienta ICQ i uzyska dostęp do listy kontaktów użytkownika. Do wszystkich użytkowników na liście kontaktów zostanie wysłana wiadomość z prośbą o pożyczenie 50 e-dolarów i obietnicą zwrócenia ich następnego dnia. Reszta będzie zależała od hojności odbiorców wiadomości i ich relacji z użytkownikiem, którego konto zostało skradzione. Przekonanie do tego zwykle nie jest trudne. W tym samym czasie haker będzie rozmawiał z innymi osobami z listy kontaktów, aby ich również nakłonić do pożyczenia mu pieniędzy. Nawet jeśli tylko jedna osoba z listy kontaktów każdej ofiary zgodzi się zapłacić hakerowi wirtualne pieniądze, zbierze on całkiem sporą sumkę w porównaniu z dziennym zarobkiem dobrego programisty – i to tylko za godzinę czatowania.

A co z kontem FTP? Co będzie, jeżeli na serwerze FTP, do którego cyberprzestępca uzyskał dostęp przy pomocy skradzionego hasła, przechowywane są strony www wystarczająco popularnej witryny internetowej? Cyberprzestępca będzie mógł dodać prostą ramkę lub zaszyfrowany kod JavaScript na koniec każdej strony, który będzie ukradkiem pobierał i uruchamiał szkodliwy program na wszystkich komputerach, z których dana strona będzie oglądana.

Wszystkie opisane wyżej działania można łatwo zautomatyzować. Na różnych serwisach randkowych i forach cyberprzestępca łatwo może znaleźć numery UIN ICQ, na które wyśle spam. Mówiąc ściśle, dokona tego specjalny program wykonujący wszystkie rutynowe działania, łącznie z odfiltrowywaniem dublujących się numerów i sprawdzaniem listy spamowej w celu znalezienia nieaktywnych numerów. Następnie haker „wrzuci" trojana na stronę zarejestrowaną w darmowej usłudze hostingowej i będzie wysyłał odsyłacz do tej strony z pomocą listy spamowej stworzonej przez oprogramowanie hakera. Następnie inny program posortuje ogromne ilości wiadomości wysłanych przez trojany uruchomione na zaatakowanych komputerach i skategoryzuje otrzymane hasła. Lista nowych numerów ICQ otrzymanych od trojana zostanie przekształcona na nową listę spamową. Jeżeli numer zainfekowanego użytkownika ICQ jest atrakcyjny (np. łatwy do zapamiętania), może zostać później sprzedany za sporą sumę pieniędzy. Ostatnim etapem jest wysyłanie wiadomości z przekonującymi prośbami o pożyczenie niewielkiej kwoty pieniędzy. Po otrzymaniu odpowiedzi na takie żądanie wkracza haker, który wykorzystuje swoją wiedzę psychologiczną i socjotechniczną. Następnie „porwane" numery mogą zostać sprzedane hurtowo spamerom. Opisany wyżej proces może wydawać się fikcją, w rzeczywistości jednak takie oszustwa są dość częste.

W podsumowaniu przedstawiamy listę powodów, dla których cyberprzestępcy przeprowadzają ataki na klienty IM:

- sprzedawanie skradzionych numerów ICQ (dziewięciocyfrowe numery sprzedawane są hurtowo, natomiast „atrakcyjne" numery sprzedawane są indywidualnie za znaczną kwotę pieniędzy);
- tworzenie list spamowych przeznaczonych do sprzedaży spamerom lub w celu masowej dystrybucji szkodliwych programów;
- wykorzystywanie list kontaktów zaatakowanych użytkowników jako zaufanych źródeł, od których można „pożyczyć" pieniądze;
- pobieranie szkodliwych programów przy użyciu luk w zabezpieczeniach oprogramowania;
- zmiana stron www legalnych witryn internetowych (przy użyciu haseł do serwera FTP) w celu pobrania szkodliwego oprogramowania na komputery osób odwiedzających strony;
- tworzenie botnetów lub rozszerzanie istniejących sieci zombie;
- inna szkodliwa aktywność.

Odpieranie ataków na systemy IM

W jaki sposób użytkownicy mogą przeciwstawić się wyrafinowanym lub nieustannym atakom? Naturalnie, muszą bronić się przed nimi! Poniżej przedstawiamy kilka wskazówek, w jaki sposób użytkownicy mogą zabezpieczyć się przed zagrożeniami rozprzestrzeniającymi się za pośrednictwem klientów IM.

Przede wszystkim nie należy bezmyślnie klikać na odsyłacze zawarte w otrzymywanych wiadomościach. Poniżej przedstawiamy kilka typów wiadomości, które użytkownicy powinni przeglądać z największą ostrożnością:

- wiadomości otrzymywane od nieznanych użytkowników z dziwnymi nikami (takimi jak SbawpathzsoipbuO);
- wiadomości od użytkowników z własnej listy kontaktów, którzy proszą o obejrzenie zdjęć z rozszerzeniem pliku .exe;
- wiadomości zawierające rzekomo sensacje na temat romansu między dwiema sławnymi osobami wraz ze „sprawozdaniem z miejsca". „Sprawozdanie" stanowi w takim przypadku odsyłacz do pliku: http://www.******.com/movie.avi.exe. Istnie-

je duże prawdopodobieństwo, że odsyłacz ten będzie prowadził do Trojan-PSW.Win32.LdPinch;

- wiadomości sugerujące użytkownikowi pobranie programu, który zapewni mu nowe możliwości, np. „NOWY BŁĄD w ICQ umożliwiający stworzenie dowolnego numeru, który nie istnieje". Odsyłacz w wiadomości bez wątpienia będzie prowadził do programu, jednak program będzie kradł numer UIN użytkownika zamiast tworzyć nowy numer konta.

Takie wiadomości należy po prostu ignorować.

Jeżeli wiadomość pochodzi od użytkownika, którego znamy, należy ustalić, czy rzeczywiście został przez niego wysłany. Nie pobieramy i nie uruchamiamy pliku z rozszerzeniem .exe. Nawet jeżeli rozszerzenie pliku nie jest określone w odsyłaczu, można zostać przekierowanym na inną stronę zawierającą szkodliwy program.

Jak zawsze, użytkownicy powinni przestrzegać podstawowych zasad „higieny komputerowej": na komputerze należy zainstalować produkt antywirusowy z aktualną bazą danych oraz zaporą sieciową, która blokuje nieautoryzowane połączenia sieciowe. Dobrze byłoby, gdyby produkt antywirusowy zawierał ochronę proaktywną, która wykrywa szkodliwe programy na podstawie ich zachowania i/lub mechanizm analizy heurystycznej.

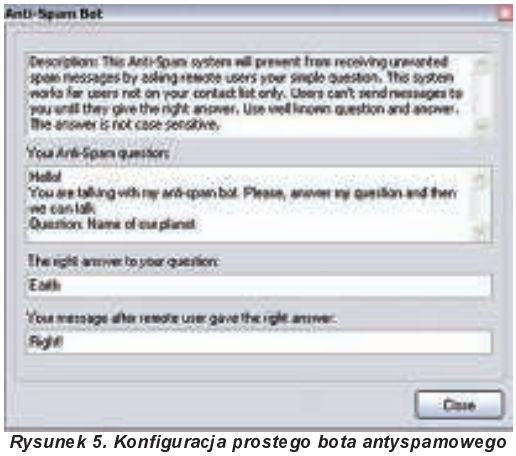
Użytkownicy często nie są świadomi, że na ich komputerze został uruchomiony szkodliwy program. Przyjaciele lub kontakty mogą pomóc w zidentyfikowaniu infekcji komputera PC.

Przykładem może być pytanie przyjaciela: „Dlaczego podczas wczorajszej rozmowy przez ICQ poprosiłeś mnie, abym pożyczył ci 50 jednostek WebMoney?", gdy w rzeczywistości prawdziwy właściciel konta ICQ nie prosił o żadną pożyczkę. Inną, jeszcze bardziej oczywistą wskazówką infekcji jest bezowocna próba wykorzystania loginu lub hasła do usługi: nieudane próby autoryzacji oznaczają, że hasło zostało zmienione. Pytanie: Przez kogo? Przez oficjalnego dostawcę usług lub przez cyberprzestępcę. W pierwszym przypadku użytkownik otrzyma nowe hasło lub zawiadomienie o zmianie hasła zostanie wysłane za pośrednictwem poczty elektronicznej lub w inny sposób. Jeżeli sprawcą jest cyberprzestępca, coś takiego nie będzie miało miejsca.

Co należy zrobić w sytuacji, gdy trojan dostarczył swoją szkodliwą funkcję, a następnie usunął się z komputera? Po pierwsze należy sprawdzić, czy komputer jest naprawdę czysty, wykonując skanowanie za pomocą programu antywirusowego. Następnie, jeśli jest to możliwe, należy zmienić wszelkie hasła, jakie mógł skraść trojan. W tym celu trzeba przypomnieć sobie, które programy wymagają hasła i spróbować wprowadzić te hasła. Jeżeli taka próba zakończy się powodzeniem, należy natychmiast zmienić hasło. Najrozsądniej byłoby również ostrzec wszystkich użytkowników na liście swoich kontaktów i poprosić ich, aby nie odpowiadali na prośby o pożyczenie pieniędzy wysyłane z waszego konta IM oraz nie próbowali oglądać zdjęć przez klikanie na odsyłacze w wiadomościach wysyłanych za pośrednictwem komunikatora internetowego.

Zainstalowanie najnowszej wersji ICQ pobranej z oficjalnej strony ICQ może pomóc zapobiec wykonaniu losowo wybranego kodu w systemie, które jest możliwe dzięki luce w zabezpieczeniach ICQ 6.x związanej z przetwarzaniem kodu HTML.

Ponieważ spamerzy mogą sprawdzić status ICQ użytkownika przy pomocy strony internetowej, rozsądnie jest zablokować tę funkcję w kliencie ICQ. Wiadomości spamowe zwykle wysyłane są do osób, które aktywnie rozmawiają za pomocą ICQ lub przynajmniej są ciągle online. Z tego powodu najlepiej pozostać w trybie niewidocznym, jeśli tylko jest to możliwe. Jednak niektóre programy mogą „powiedzieć" innym użytkownikom, czy rzeczywiście jesteśmy offline, czy jedynie w trybie niewidocznym. W takiej sytuacji można użyć botu antyspamowego – prostego modułu obsługiwanego przez niektóre klienty IM (takie jak QIP). Poniższy zrzut ekranu pokazuje konfigurację prostego bota antyspamowego.



Rysunek 5. Konfiguracja prostego bota antyspamowego

W jaki sposób działa bot antyspamowy? Jeżeli użytkownik, który nie znajduje się na naszej liście kontaktów, chce z nami czatować, będzie musiał najpierw odpowiedzieć na pytanie. Nie będzie mógł wysłać nam żadnej wiadomości, dopóki nie odpowie na to pytanie. Dobrym rozwiązaniem jest stosowanie pytań, na które każdy zna odpowiedź, np. „Ile jest 2+2x2?" lub „Jak się nazywa nasza planeta?". Jeżeli użytkownik odpowie „6" lub "Ziemia" i wyśle wiadomość, będzie mógł wysyłać nam dalsze wiadomości. Taka ochrona jest stosunkowo skuteczna w blokowaniu wielu różnych botów, które wysyłają spam, mimo że niektóre z tych botów mogą być wystarczająco inteligentne, aby odpowiedzieć na większość popularnych pytań, np. na domyślne pytania wykorzystywane w modułach ochrony.

Wniosek

Komunikatory internetowe są bardzo atrakcyjne dla wszelkiej maści szkodliwych użytkowników i z tego względu problem rozprzestrzeniania szkodliwych programów za pośrednictwem klientów IM jest poważny. Nowe wersje klientów IM zawierają nieznane jeszcze luki w zabezpieczeniach, które mogą zostać wykryte najpierw przez hakerów, a następnie przez programistów. Takie sytuacje mogą łatwo prowadzić do masowych epidemii. Niektórzy użytkownicy są zmęczeni otrzymywaniem niechcianych wiadomości (IM spam).

Obecnie nie istnieją żadne metody czy rozwiązania przeznaczone do ochrony klientów IM. Przestrzeganie prostych zasad „higieny komputerowej" oraz wykorzystywanie dobrze skonfigurowanego bota antyspamowego w połączeniu z niewielką dawką zdrowego rozsądku może pomóc użytkownikom bez obaw czatować za pośrednictwem internetu. ■

Systemics Poland doradza

Inwestycje w bezpieczeństwo i ciągłość biznesu to po prostu oszczędność

Przedsiębiorstwa nadal lekceważą działania związane z bezpieczeństwem i ciągłością pracy firmowych systemów IT – wynika z badań ISACA. Systemics Poland – jedna z głównych firm świadczących usługi IT na polskim rynku – przekonuje swoich klientów, że lepiej zainwestować w działania prewencyjne, niż potem ponosić znacznie większe koszty niespodziewanych awarii i przerw w pracy.

W tym roku stowarzyszenie ISACA (*Information Systems Audit and Control Association*) przeprowadziło badanie dotyczące problemów biznesowych spowodowanych wykorzystaniem technologii.

Wynika z niego, że ponad 80 proc. menadżerów w firmach nie ma świadomości i odpowiedniej wiedzy o zagrożeniach, które mogą zagrozić bezpieczeństwu przechowywanych danych w systemach IT przedsiębiorstw. Taki sam procent respondentów nie jest świadom szkód wywołanych przerwami w działalności firmy.

– *Podstawową przeszkodą w mówieniu o tych kwestiach jest postrzeganie bezpieczeństwa informacji jako problemu tylko działu IT, a nie całej firmy. Często menadżerowie uważają, iż doświadczeni pracownicy zapewniają im bezpieczeństwo działalności firmy. Liczą na to, że w razie czego wszystko da się odtworzyć, a praktyka pokazuje, że nie jest to takie proste i tanie* – wyjaśnia **Roman Gradek**, Prezes Zarządu Systemics Poland. – *Naszym klientom zalecamy zawsze prewencję jako działanie zdecydowanie tańsze niż naprawa awarii i odzyskiwanie danych*.

Inwestycje w bezpieczeństwo i ciągłość systemów są traktowane jako „zło konieczne", ponieważ – według zarządów firm – nie przynoszą zysku i nie wspierają wzrostu wartości firmy, a dodatkowo wprowadzone procedury bezpieczeństwa „utrudniają" codzienną pracę. To są znikome niedogodności w porównaniu do strat, jakie każda firma może ponieść, jeżeli nie będzie dbała o swój system IT.

Utrata kluczowych danych lub zastój prac w firmie może doprowadzić nawet do jej bankructwa, a na pewno, w krótkiej perspektywie, negatywnie wpływa na jej finanse.

– *Podstawowym jest pytanie: Po co w ten obszar inwestować? Co nam to da? Rzeczywiście, działania na rzecz ciągłości i bezpieczeństwa nie przynoszą zysku, ale są jak ubezpieczenie, czyli łagodzą lub eliminują konsekwencje wystąpienia awarii* – mówi Prezes Zarządu Systemics Poland.

Korzyści z działań prewencyjnych jest wiele. Przedsiębiorstwo dbające o swoje dane i infrastrukturę IT jest przygotowane na wystąpienia awarii i zabezpieczone na wypadek jej konsekwencji.

Wdrożone procedury pozwalają uniknąć uszkodzenia sprzętu czy utraty kluczowych informacji lub umożliwiają szybką naprawę infrastruktury. Poza tym działania prewencyjne pozwalają firmie zachować obecną jej wartość, dając szanse na prowadzenie normalnej działalności przynoszącej zyski.

Decyzja, czy zabezpieczać się, czy nie, należy do każdego przedsiębiorstwa, ale koszty ewentualnej awarii mogą być nieporównywalnie większe niż koszty działań prewencyjnych lub niewygody związanej z zastosowaniem procedur. ■

Systemics Poland Sp. z o.o.
jest firmą świadczącą usługi IT
od 2003 roku.
Spółka specjalizuje się
w zaawansowanych
usługach teleinformatycznych
zarówno dla dużych korporacji
z branży telekomunikacyjnej,
jak i firm średniej wielkości.

Edu 4 tworzy szkołę przyszłości

Grzegorz Kantowicz

Nowe technologie w służbie edukacji

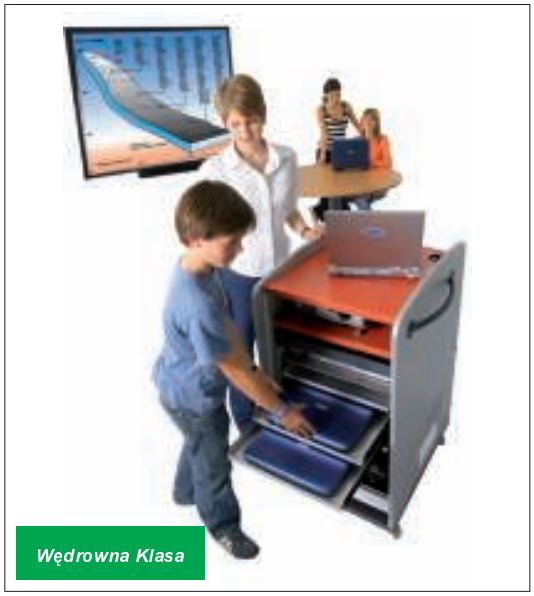
W dniach od 29 do 31 października ubiegłego roku, podczas międzynarodowych targów Worlddidac, francuska firma Edu 4 prezentowała swoje hardware'owe i software'owe rozwiązania przeznaczone dla szkolnictwa. W celu sprostania rosnącym potrzebom związanym z mobilnością nauczycieli, firma opracowała kompleksową ofertę związaną z wejściem na ten rynek laptopów i minilaptopów.

ValiTICE jest niedużą walizką, łatwą do przenoszenia i zawierającą do 10 minipecetów. Umożliwia szybkie utworzenie bezprzewodowej sieci dla potrzeb pedagogicznych. Minipecety ważą mniej niż 1 kg. Wyposażone w pełniącą funkcję twardego dysku pamięć flash są solidnymi urządzeniami, dostosowanymi do intensywnego użytkowania przez uczniów. W razie problemu, ich początkowa konfiguracja może zostać przywrócona w ciągu kilku minut przy użyciu dołączonej pamięci USB.

Walizka zawiera urządzenie zasilające oraz kabel elektryczny do ładowania wszystkich minipecetów, a także łącze Wi-Fi typu infrastrukturalnego. Jest dostarczana wraz ze słuchawkami nagłownymi oraz pakietem informatycznych narzędzi biurowych i multimedialnych, oprogramowaniem dydaktycznym do nauk przyrodniczych, matematyki, czytania, geografii czy muzyki. ValiTICE jest zestawem gotowym do użytku. Oprogramowanie do prowadzenia zajęć lekcyjnych eeVision dostarczane jest na CD-romie, gotowym do zainstalowania na komputerze nauczyciela.

Zestaw *Classe Nomade* (Wędrowna Klasa) obejmuje 16 komputerów przenośnych umieszczonych w niedużym meblu na kółkach z centralnie zamykanym zamkiem. Ułożone w nim na płasko komputery są dobrze chronione i zabezpieczone, a ich ładowanie odbywa się dzięki centralnemu zasilaniu.

ValiTICE



Wędrowna Klasa

Poza łączem Wi-Fi zapewniającym połączenie w sieć wszystkich stanowisk pracy danej klasy, zestaw *Classe Nomade* wyposażony jest w rozmaite zoptymalizowane urządzenia, jak na przykład rzutnik multimedialny z centralnym nagłośnieniem.

Firma Edu 4 opracowała specjalne oprogramowanie Multilab, które jest jednocześnie rozwiązaniem do nadzorowania i prowadzenia zajęć, ale dysponuje również funkcjami związanymi z administrowaniem przenośnymi pecetami. Zoptymalizowane dla potrzeb korzystania z technologii Wi-Fi, posiada ono wielojęzyczny, prosty w użyciu i intuicyjny interfejs użytkownika (w 7 językach), skalowalny plan klasy, multimodalną wizualizację stanowisk pracy uczniów i zaawansowane funkcje umożliwiające śledzenie ich postępów oraz nadzorowanie pracy grupowej.

Wszystkie oferowane rozwiązania są tak skonfigurowane, by były gotowe do użytku na terenie szkoły. Edu 4 oferuje pakiet oprogramowania dostosowanego do wszelkich zastosowań pedagogicznych, na wszystkich poziomach nauczania.

Założona w roku 1987 francuska firma Edu 4 projektuje, opracowuje i produkuje kompleksowe rozwiązania multimedialne, stacjonarne lub przenośne, do nauczania wielu przedmiotów, do nauki języków, dla potrzeb szkolenia na odległość i nauczania nauk ścisłych. Firma przeznacza 10 proc. swoich obrotów na działalność badawczo-rozwojową. Edu 4 obecna jest na rynkach zagranicznych i dysponuje siecią 19 przedstawicielstw we wszystkich zakątkach globu. Z rozwiązań firmy Edu 4 korzysta ponad 1 500 placówek oświatowych we Francji i 4 500 na całym świecie. ■

Efekty cyberslackingu

Grzegorz Kantowicz

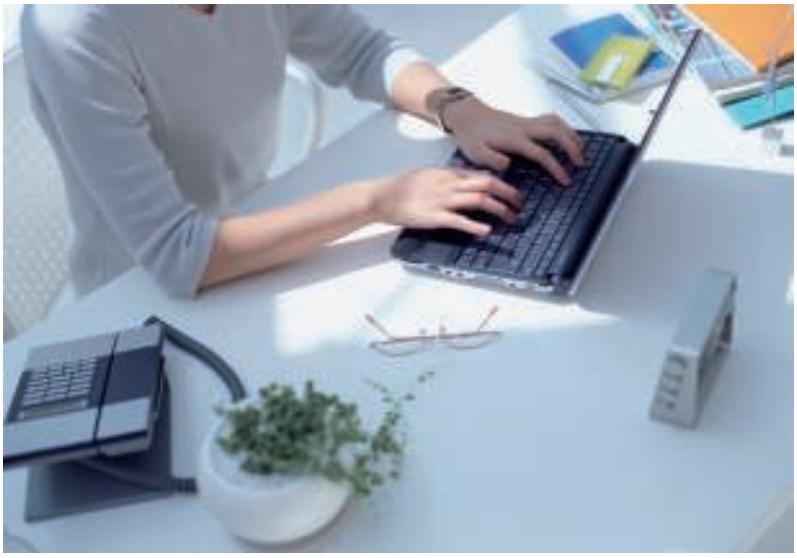
Powszechny internet i popularne blokady

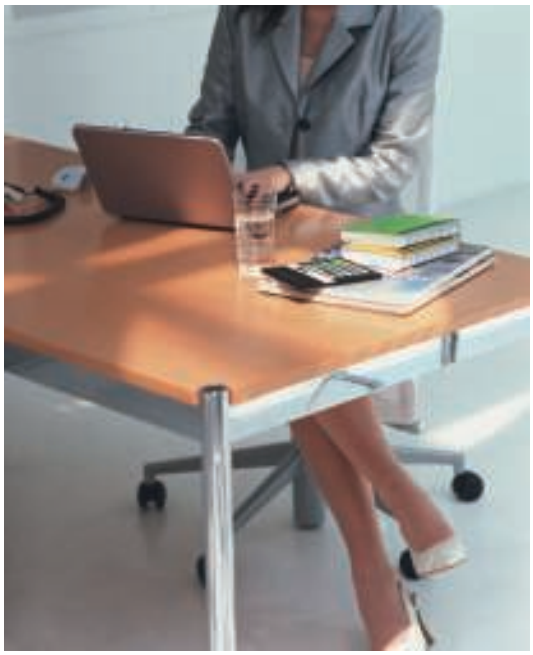
Coraz trudniej znaleźć w Polsce firmę, która nie miałaby jeszcze dostępu do internetu. Według badań D-Link Technology Trend, przeprowadzonych na zlecenie firmy D-Link przez International Data Group, wśród przedsiębiorstw sektora MŚP takich firm w ogóle nie ma. Firmy sektora MŚP powszechnie korzystają także z poczty e-mail i komunikatorów internetowych. Jednak w celu zwiększenia efektywności pracy, 80 procent firm blokuje pracownikom dostęp do niektórych zasobów sieci, w szczególności do serwisów P2P oraz określonych stron www.

W kolejnym badaniu D-Link Technology Trend sprawdzono poziom informatyzacji polskich przedsiębiorstw sektora MŚP pod kątem dostępu do internetu i wykorzystania zasobów sieci. Jak się okazało, wśród polskich firm sektora MŚP nie ma obecnie ani jednej, która nie posiadałaby łącza internetowego. Jednak biorąc pod uwagę, że firmy te zatrudniają od 50 do 250 osób, przepustowości wykorzystywanych łączy są stosunkowo niskie. Tylko co czwarte przedsiębiorstwo dysponuje łączem szybszym niż 6 Mb/s, a 11 proc. firm wciąż pracuje na łączach do 1 Mb/s.

Wraz z popularyzacją usług dostępowych zmienił się także styl komunikacji polskich firm. Obecnie wszystkie firmy MŚP wykorzystują w korespondencji biznesowej pocztę e-mail, prawie 70 proc. używa komunikatorów internetowych, co trzecia firma korzysta z usług *Voice over IP*, a co szósta prowadzi wideokonferencje.

Polskie firmy zdają sobie sprawę z ogromnych możliwości internetu jako narzędzia pracy. W większości także chcą, by pracownicy nie korzystali z internetu w celach prywatnych lub rozrywkowych. Z badań wynika, że przeróżne ograniczenia w korzystaniu z internetu stosuje 80 proc. firm. Najbardziej popularne są tu blokady komunikacji Peer-2-Peer (65 proc.) oraz konkretnych stron www (55 proc.) i portów do gier (50 proc.). Rzadziej pracodawcy blokują komunikatory internetowe (35 proc.), streaming mediów (27 proc.) i prywatną korespondencję e-mail (18 proc.). Co dziesiąta firma całkowicie blokuje pracownikom dostęp do przeglądarek internetowych.





– *Ograniczanie dostępu do zasobów internetu przez pracodawców będzie coraz częstsze* – prognozuje **Mariusz Piaseczny** z firmy D-Link. – *To efekt tzw. cyberslackingu, czyli wykorzystywania internetu w pracy do celów prywatnych. W Stanach Zjednoczonych, gdzie to zjawisko dokładnie przebadano, na prywatne sprawy załatwiane przez internet pracownik przeznacza dziennie ok. 1,5 godziny. Trudno więc się dziwić, że blokady dostępu do pewnych zasobów internetu pracodawcy traktują jako swoje naturalne prawo. Z naszych badań wynika, że już teraz polskie firmy powszechnie z tego prawa korzystają.* ■

Jak to robią inni

Grzegorz Kantowicz

SIGAP – Informatyczny System Zaawansowanego Zarządzania Procedurami

Według sporządzonego przez firmę 40-30 opracowania na temat 2000 niezgodności związanych bezpośrednio lub pośrednio z działaniem procesowym, ponad 90 proc. spośród setek niezgodności, jakie każdego roku generuje każde przedsiębiorstwo, ma swoje źródło w zawodnych procedurach lub w braku ich respektowania. By zaradzić tym zakłóceniom, firma 40-30 opracowała pierwszą wersję systemu SIGAP, który obecnie poddaje testom w swoim zakładzie w Grenoble, specjalizującym się w utrzymaniu i konserwacji aparatury do implantacji jonów, wykorzystywanej przy produkcji półprzewodników.

Od ponad roku system SIGAP zarządza tam około stu procedurami, z których niektóre obejmują ponad setkę interfejsów, uzyskując rezultaty znacznie przewyższające oczekiwania: zerowa liczba błędów przypadająca na ponad 1200 interwencji, poprawa wydajności, wydłużenie średniego czasu międzyawaryjnego (MTBF – *Mean Time Between Failures*), a także – co jest najważniejszym wnioskiem z tego eksperymentu w skali rzeczywistej – doskonałe opanowanie procedur, które definitywnie eliminuje nadmierne przekroczenia kosztów.

Wersja nr 2 systemu SIGAP, obejmująca wybór języków, zostanie wprowadzona na rynek w czerwcu 2009 roku, a wersja 3, wykorzystująca techniki wideo, jest w trakcie opracowywania.

Ten eksperyment prowadzony jest obecnie w pięciu francuskich placówkach firmy 40-30 zajmujących się techniką próżniową, ultraczystymi technologiami, a także działalnością z zakresu elektroniki, zaworów, częstotliwości radiowych itp. oraz na terenie zakładu w Singapurze. Wszystkie one połączone są z głównym serwerem systemu SIGAP.

Blisko 50 terminali jest obecnie podłączonych za pośrednictwem internetu do centralnej bazy danych procedur, w ramach której zespół około dziesięciu osób opracowuje nowe procedury i pracuje nad wersją nr 2 systemu SIGAP, która ma się ukazać w czerwcu 2009 r.

Prowadzący działalność badawczo-rozwojową zespół firmy 40-30 pracuje również nad zakładową wersją programu, dla której referencyjnym ośrodkiem alfa jest liniowy implantator jonów Laboratorium LETI w Grenoble.

SIGAP jest również efektywnym narzędziem szkoleniowym i służącym do transferu kompetencji, które można wykorzystywać dla potrzeb utrzymania ruchu lub produkcji we wszelkich dziedzinach przemysłu. Niezależnie od kraju wykorzystania, SIGAP V2 oferuje wybór języka, począwszy od angielskiego poprzez mandaryński czy arabski aż po rosyjski. Rozróżnia również operatora praworęcznego od leworęcznego (bowiem każdy z nich posługuje się narzędziem w inny sposób). Zastosowanie systemu umożli-

wia skrócenie czasu szkolenia i zapewnienie jego właściwego poziomu. W przeszłości opanowanie utrzymania podzespołów implantatorów wymagało sześciomiesięcznego szkolenia doświadczonego technika, a obecnie taki operator uzyskuje niezbędne kompetencje w ciągu miesiąca. Wersja 3 systemu, wykorzystująca techniki wideo, jest w opracowaniu i powinna ukazać się z początkiem roku 2010.

Celem, jaki firma 40-30 wytyczyła sobie na przyszły rok obrachunkowy, jest osiągnięcie dla systemu SIGAP i produktów pochodnych obrotów w wysokości 2 milionów euro. Rozwojowi systemu SIGAP swojego wsparcia udziela OSEO (francuska agencja wspierania innowacji).

Firma 40-30, założona w roku 1986, ma swą siedzibę we Francji, w Grenoble. Poprzez usługi z zakresu działalności badawczo-rozwojowej rozwija własne koncepcje konserwacji i utrzymania ruchu. Obecnie przedsiębiorstwom pragnącym uzyskać poprawę wydajności produkcji oferuje 5 nowych kierunków rozwoju, na które składają się:

- inżynieria utrzymania ruchu: audyty i doradztwo, plany redukcji kosztów, prowadzenie i wspieranie działań QSE, opracowywanie i redagowanie procedur, konstruowanie i opracowywanie narzędzi i stanowisk badawczych, wyszukiwanie i analiza problemów, reengineering;
- narzędzia do monitoringu i aplikacje komputerowe: SIGAP (Informatyczny System Zaawansowanego Zarządzania Procedurami), ISM (*Industrial Service Management*), RC (*Repair Center*);
- transfery kompetencji: warsztaty utrzymania ruchu, zaplecze w postaci rezerwy awaryjnej;
- system szkolenia: ultraczyste technologie, techniki próżniowe, uprawnienia COFREND (badania nieniszczące);
- oferta z zakres sourcingu: dostawa części zamiennych, kupno i sprzedaż przez internet, prowadzenie gospodarki magazynowej, selekcja podwykonawców. ■

Metody cyberprzestępców

Grzegorz Kantowicz

Aleja wirusów 2008

Od McDonalds, przez policję, po cukiernictwo... Pomysłowość cyberprzestępców nie zna granic. Chwytają się każdego sposobu, by uśpić czujność internautów i uzyskać dostęp do ich komputerów.

Panda Security przygotowała listę zawierającą wybrane złośliwe kody, które – choć nie spowodowały epidemii na szeroką skalę – były szczególnie zauważalne w drugiej połowie ubiegłego roku.

P2PShared.U – robak w hamburgerze

Ten złośliwy kod rozpowszechniany był w wiadomościach e-mail o temacie „McDonalds wishes you Merry Christmas!/McDonalds życzy Wesołych Świąt". W treści listu zawarto obietnicę otrzymania kuponu umożliwiającego uzyskanie bezpłatnego posiłku w restauracjach sieci. W rzeczywistości kupon zawierał robaka. Bez dobrego systemu zabezpieczającego jedyną rzeczą, jaką użytkownicy otrzymywali gratis, była... niestrawność.

Agent.JEN – fałszywy posłaniec

Wyobraźmy sobie posłańca dzwoniącego do drzwi z informacją o paczce dla nas. Tymczasem po ich otwarciu do domu wdziera się banda przestępców! W podobny sposób Agent.JEN traktował nasz komputer. Otrzymywaliśmy wiadomość e-mail z pozoru pochodzącą od firmy UPS, jednakże po otwarciu załącznika uruchomiony trojan natychmiast rozpoczynał kopiowanie na nasz komputer innego złośliwego oprogramowania.

Banbra.FXT – nakaz sądowy

Robak ten informował odbiorców – za pomocą wiadomości pochodzącej rzekomo od brazylijskiego sądu – że prowadzone jest w ich sprawie dochodzenie. Nadawca oferował raport zawierający szczegółowe informacje na temat zarzutów, jakie zostały postawione zainteresowanym. Raport był jednak tylko kopią trojana. Po zainstalowaniu na komputerze wykradał hasła bankowe, dane kont itp.

Banker.LGC – nie wierz we wszystko, co przeczytasz

Czy kierowca Formuły 1 – Fernando Alonso rzeczywiście miał wypadek? Nie. To jedynie historia zmyślona przez twórcę trojana, mająca zachęcić użytkowników do obejrzenia załączonego materiału wideo. Po pobraniu i otwarciu pliku system był infekowany innym trojanem stworzonym w celu kradzieży danych bankowych.

Sinowal.VTJ – wirus, który skarży się na... wirusy

To zapewne jeden z dziwniejszych złośliwych kodów, jakie pojawiły się w drugiej połowie 2008 roku. Jego rozpowszechnianie odbywało się za pośrednictwem wiadomości e-mail pochodzącej od anonimowej osoby, utrzymującej, że odbiorca przesłał jej wirusy. Wiadomość zawierała także groźbę doniesienia o całej sprawie policji. W treści listu znajdowała się zachęta do otwarcia i wydrukowania załącznika, który miał zawierać dowód przesłania zainfekowanych wiadomości. W rzeczywistości załącznik zawierał kopię trojana Sinowal.VTJ.

BatGen.D – hiszpański szef kuchni

Ten szkodliwy kod specjalizował się w przyrządzaniu wszelkiego rodzaju złośliwego oprogramowania. Zagrożenie było rozpowszechniane za pośrednictwem pliku pod smakowitą nazwą „personalcake.bat". Jest to narzędzie do tworzenia złośliwego oprogramowania, które w oczekiwaniu, że sam użytkownik nada mu nazwę, stawiało przed nim takie oto pytanie: „Selecciona el nombre del pastel" („Wybierz nazwę ciastka").

Aidreden.A – makabryczny wróżbita

Czy to nie dziwne, że złośliwy kod miałby przepowiadać przyszłość użytkowników? A co by było, gdyby informował ich o zbliżającej się śmierci? Tymczasem tak właśnie działał ten kod. Po zainfekowaniu komputera wyświetlał komunikat: „You will dead (sic) next month!" („Umrzesz w przyszłym miesiącu"). Okno dialogowe zawierało także opcję „OK" z prośbą o akceptację. I choć trudno w to uwierzyć, wiele osób wybrało tę opcję.

Banker.LLN – prezydent elekt

Trojan przedostawał się do komputerów w pliku pod nazwą „barackobama.exe" z ikoną w postaci flagi Stanów Zjednoczonych. Jak można się było spodziewać, ten złośliwy kod nie miał nic wspólnego z prezydentem elektem. Był to jedynie kolejny trojan stworzony w celu kradzieży danych bankowych.

Banbra.GDB – brazylijska policja

Gdy do naszych drzwi zapuka policja, zwykle lepiej otworzyć. No, chyba że chodzi o trojana, który tylko się pod nią podszywa. Banbra.GDB przedostawał się do komputerów w wiadomości e-mail, której nadawcą była rzekomo brazylijska policja. W treści wiadomości zawarto informację, że komputer nadawcy jest wykorzystywany do nielegalnej działalności, a także zaproszenie do pobrania raportu, który miałby zawierać stosowne dowody. Uruchomienie załącznika skutkowało zainfekowaniem komputera trojanem bankowym.

Spammer.AKE – niebezpieczny przyjaciel

Robak rozprzestrzeniał się w wiadomościach e-mail zawierających przeróżne treści związane z przyjaźnią i miłością. Ale uwaga! To nie był żaden przyjaciel, skoro po zainfekowaniu naszego komputera wykorzystywał go do rozsyłania spamu. ■

KOMUNIKACJA ELEKTRONICZNA 2010

z wersją na CD

Zapraszamy do kolejnej edycji!
materiały przyjmujemy do 30.06.2009 r.

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

extranet
internet creator

Platforma NetAdmin®
nowoczesne rozwiązania dla biznesu

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

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

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

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

XI edycja konkursu o LAUR INFOTELA

„Złoty Laur Czytelników INFOTELA" w kategoriach:

operator telefonii i internetu mobilnego .....
(nazwa operatora)

operator telefonii i szerokopasmowego internetu stacjonarnego .....
(nazwa operatora)

operator satelitarny .....
(nazwa operatora)

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

nadawca i dystrybutor 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 na VIII Kongresu INFOTELA

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
17.04.2009 r.

ORGANIZATOR:
ul. Stawowa 110, 85-323 Bydgoszcz, tel. (052) 325 83 10, fax (052) 373 52 43
e-mail: office@msgmedia.pl, www.msgmedia.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 i internetu mobilnego;
- operator telefonii i szerokopasmowego internetu stacjonarnego;
- operator satelitarny;
- operator telewizji kablowej;
- nadawca i dystrybutor telewizyjny;
- telewizyjny kanał tematyczny;
- witryna internetowa

XI edycja konkursu o
LAUR INFOTELA

INFOTEL 1997 MSG MEDIA

Patronat honorowy:

Ministerstwo Infrastruktury
Urząd Komunikacji Elektronicznej
Krajowa Rada Radiofonii i Telewizji

Uroczyste rozstrzygnięcie i wręczenie LAURÓW INFOTELA nastąpi podczas VIII Kongresu INFOTELA na uroczystej Gali Komunikacji Elektronicznej

Zgłoszenia do udziału w konkursie przyjmujemy do:

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

17.04.2009 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.msgmedia.pl

VIII Kongres INFOTELA

3-6 czerwca 2009 r.

Hotel ASTOR Jastrzębia Góra

Komunikacja elektroniczna

– technologie i usługi: mobilność, cyfryzacja, kontent, multimedia

Patronat honorowy:

MINISTERSTWO INFRASTRUKTURY

KRRiT | KRAJOWA RADA RADIOFONII I TELEWIZJI

Anna Streżyńska
Prezes Urzędu
Komunikacji Elektronicznej

Patronat branżowy:

PIIT PIKE KIGEiT

Sponsorzy i Partnerzy:

emitel inea netia DIALOG telecom ZPAS GROUP Activis POLSKA

Imprezy towarzyszące:

- Rozstrzygnięcie XI edycji ogólnopolskiego konkursu o LAUR INFOTELA;
- Uroczysta Gala Komunikacji Elektronicznej;
- Grillowanie na polanie;
- Turniej o Puchar INFOTELA w bowlingu;
- Ogólnopolski konkurs w rzucie komórką na odległość.

Organizator:

MSG MEDIA

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