MSG MEDIA

ISSN 1429-0200

INFOTEL

3/2009

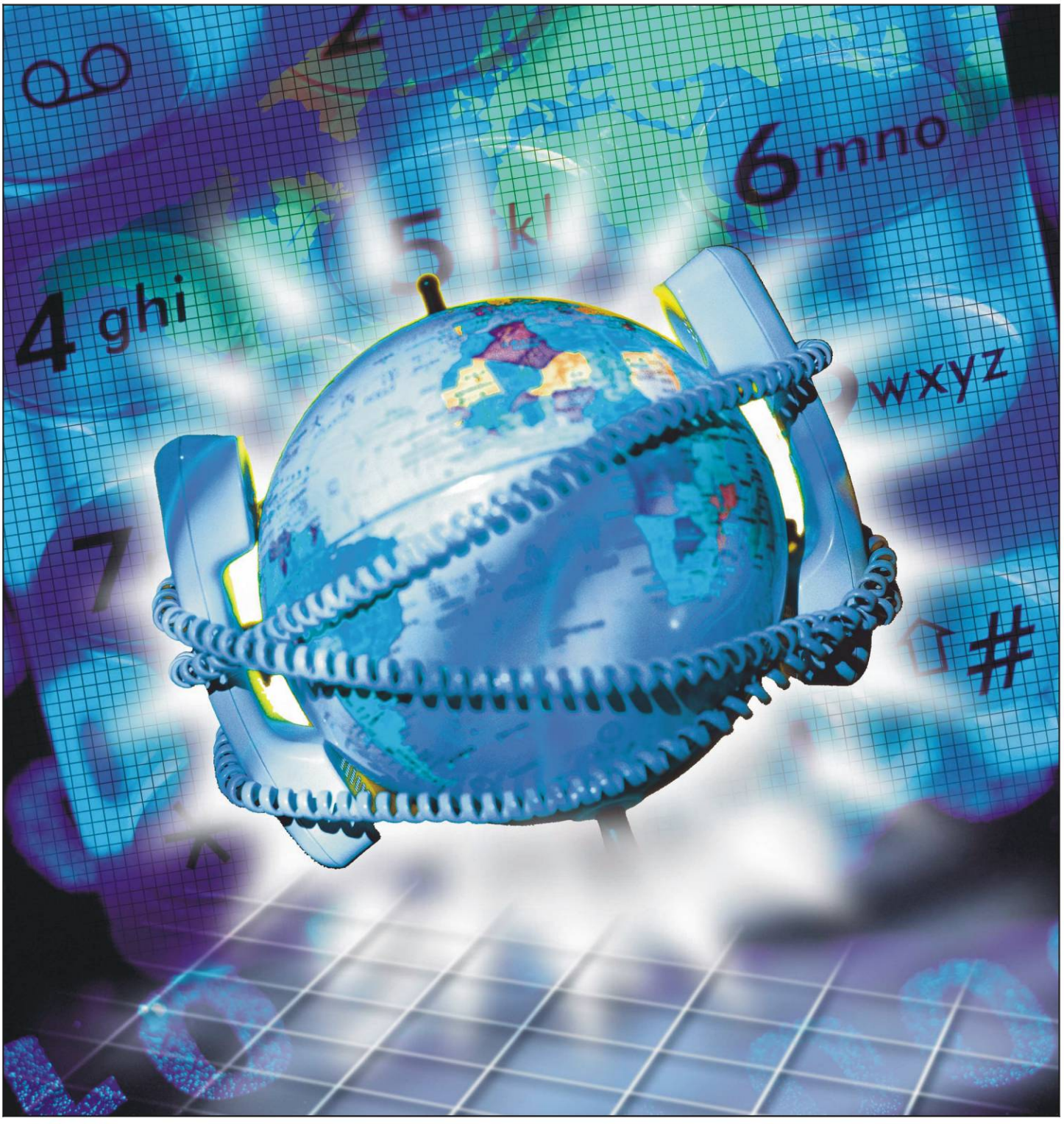
INDEKS 345237

Cena 15 zł
(w tym 0% VAT)

kwartalnik – LIPIEC/WRZESIEŃ

NOWOCZESNA KOMUNIKACJA ELEKTRONICZNA

TELEKOMUNIKACJA • INFORMATYKA • TELEWIZJA



Pozwól klientom na szybki i bezpłatny kontakt z Twoją firmą!

VoiceLink
to innowacyjna forma kontaktu głosowego klientów
z Twojej strony internetowej

Klient skontaktuje się z Tobą:

- bez opłat
- bez konta
- bez logowania
- bez ryzyka

VOICELINK KLIKASZ – rozmawiasz

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

Spotkanie biznesowe firm
z województwa kujawsko-pomorskiego

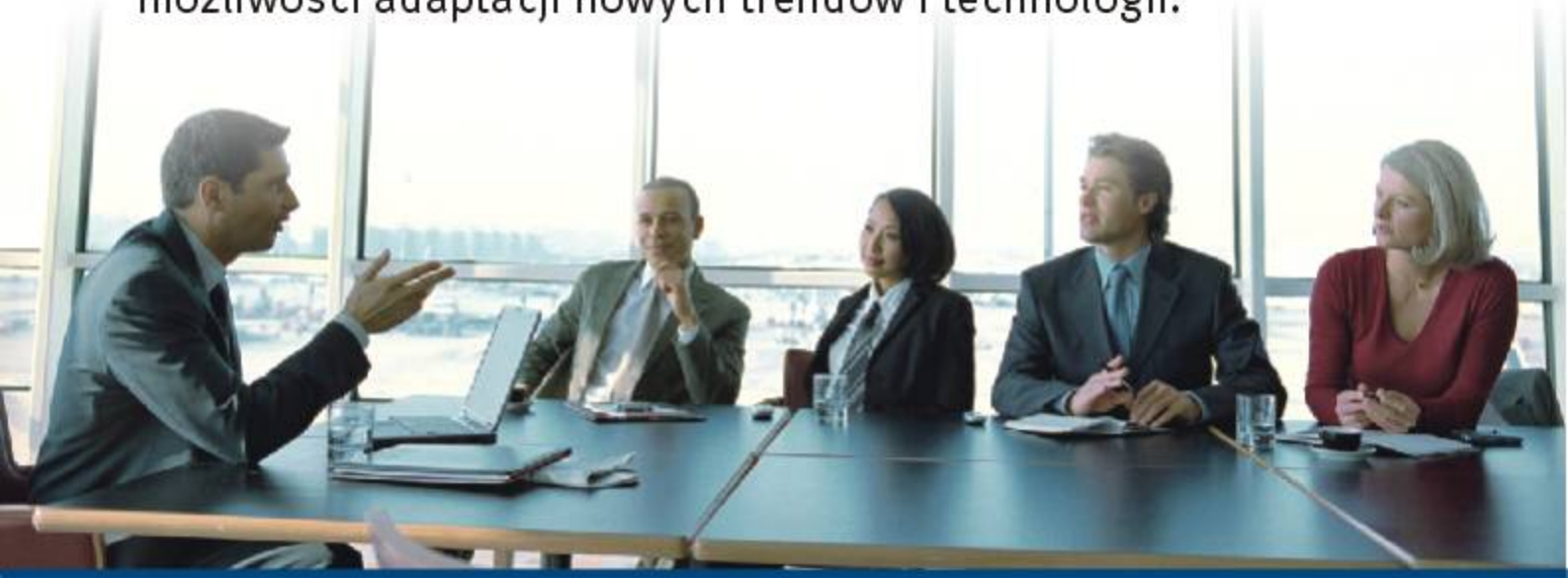
Termin spotkania:
- 18 września 2009 r. (piątek).

Miejsce spotkania:
- Bydgoszcz
  ul. Jagiellońska 96
  Hotel Sloneczny Mlyn

„Obniżanie kosztów w firmie poprzez inwestycje w nowoczesną komunikację elektroniczną"

Prezentacje nowoczesnych technologii telekomunikacyjnych i informatycznych mających wpływ na obniżenie kosztów w firmach i poprawienie warunków pracy.

Dynamika zmian nowoczesnych technologii w otaczającej nas rzeczywistości, zmienia także sam biznes. Trwałe miejsce na rynku i zdobywanie przewagi konkurencyjnej zależy od zdolności tworzenia i wprowadzania w życie usprawnień, możliwości adaptacji nowych trendów i technologii.



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

INFOTEL 1997

INDEKS 345237
numer 3 (103), rok dziesiąty
lipiec/wrzesień 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

Warto wiedzieć, że... 4–7

Telekomunikacja

Grzegorz Kantowicz
Dogonić Europę 8–12
VIII Kongres INFOTELA

VoIP w Polsce 14
Wartość dodana czy niezależny segment rynku

Grzegorz Kantowicz
Cena ważniejsza niż ekologia 15
Green IT w firmach sektora MŚP

Marcin Ułasik
Standard DOCSIS 3.0 a usługi dostępu do internetu 16–18
W pogoni za „szerokim pasmem"

Grzegorz Kantowicz
ICT a wydajność w pracy 20
Europejczycy tracą rocznie 39 dni roboczych na dojazdy do pracy

Grzegorz Kantowicz
Wideokonferencje przez firewall 21
NetPoint – Emblaze-VCON

Molex wprowadza rozwiązania do zaawansowanego zarządzania cyklem warstwy fizycznej sieci 22

Piotr Frączyk
Dystrybucja czasu w epoce globalnych technologii 24–25

Opłacalne inwestycje – komunikacja z partnerami biznesowymi na nowo 26–27
VDmaster firmy Activis Polska – kompleksowy system komunikacji kosztuje mniej

Grzegorz Kantowicz
Przełomowy interfejs ethernetowy 28–29
Interfejs 100 gigabitów do ruterów Juniper Networks

Christian Funk
Bezprzewodowe lato 30–33
Wakacje z internetem

Grzegorz Kantowicz
Wspieranie polskiej nauki 34
Najlepsze prace doktorskie z dziedziny radiokomunikacji i technik multimedialnych

Telewizja

Pierwsze studio do tworzemia wideo dla sieci 3G 35
Łatwa produkcja treści dla komórek

Informatyka

Rekord.ERP dla przedsiębiorstw 36

Grzegorz Kantowicz
MMS – kompleksowe zarządzanie usługami 37
Dla małych i średnich ISP

Maciej Ziarek
Res Publica – czyli o tym, co można znaleźć w publicznych komputerach 38–41
Biblioteki, kawiarenki internetowe, punkty ksero oraz pracownie szkolne na celowniku

Grzegorz Kantowicz
Zabezpieczenia przed wyciekami danych 42–43
Technologia kontroli „odcisków palców" DataDNA™

Grzegorz Kantowicz
Rosnące zagrożenia dla bezpieczeństwa firm 44–45
Raport bezpieczeństwa Cisco 2009

Regulacje

UKE analizuje ceny mobilnego Internetu

Prezes UKE przedstawił analizę cen usług dostępu do Internetu świadczonych przez operatorów telefonii ruchomej.

Z analizy wynika, że systematyczny wzrost zainteresowania konsumentów usługami mobilnego Internetu wymusza na operatorach aktywną walkę o potencjalnych klientów. W okresie od czerwca 2008 do czerwca 2009 roku na krajowym rynku podwoiła się liczba modemów bezprzewodowego Internetu, a nasycenie usługami osiągnęło blisko 5 procent.

Rynkowe ceny aktywacji usługi w abonamencie wahają się w przedziale od 1 do 189 zł z VAT. Średnia opłata miesięczna za korzystanie z usługi wynosi natomiast ok. 55 zł z VAT dla klienta post-paid oraz ok. 36 zł z VAT dla klienta biznesowego.

Zdecydowanie droższa jest usługa w systemie przedpłaconym. Ceny aktywacji wraz z modemem w pre-paid wahały się w analizowanych ofertach od 249 nawet do 919 PLN z VAT. Samo miesięczne wykorzystanie usługi w systemie pre-paid jest już zdecydowanie tańsze i wymaga wydatku średnio ok. 19 zł z VAT miesięcznie, przy utrzymaniu aktywnego konta przez co najmniej dwa lata.

Z kolei miesięczne ceny abonamentów oscylują w przedziale 29-160 zł z VAT dla klientów post-paid oraz od 25 do 157 zł z VAT dla klientów biznesowych. Na rynku jest coraz więcej ofert z początkowym okresem promocyjnym o obniżonej opłacie, który jednak nie zawsze zmniejsza całościowy koszt ponoszonych wydatków. Promocyjny abonament często łączy się z droższą aktywacją lub wyższymi cenami modemów i kart. Za wyborem oferty promocyjnej przemawia natomiast częsta możliwość próbnego wykorzystania usługi i rozwiązania umowy w przypadku braku satysfakcji klienta.

Zmiany w wybieraniu numerów

Z końcem września rozpocznie się ostatni etap wdrażania zmian w Planie Numeracji Krajowej. Prezes Urzędu Komunikacji Elektronicznej przypomina o zmianach w zasadach wybierania numeru krajowego w Polsce. Zmiana polega na rozpoczęciu od dnia 30 września 2009 r. procesu związanego z likwidacją prefiksu krajowego „0" ze schematu wybierania numerów.

Oznacza to, że w okresie od dnia 30 września 2009 r. do dnia 15 maja 2010 r. przedsiębiorcy telekomunikacyjni będą stopniowo wprowadzać zmiany w swoich sieciach i w tym okresie będą funkcjonować równolegle dwa schematy wybierania – z cyfrą „0" i bez cyfry „0" przed numerem krajowym. Nie oznacza to jednakże, że w początkowym okresie każda centrala telefoniczna będzie zapewniała możliwość wybierania podwójnego schematu połączenia. Podwójny schemat wybierania zapewnią centrale z wdrożoną możliwością wybierania numeru krajowego bez cyfry „0".

Dzięki rezygnacji z konieczności wybierania cyfry „0" przed numerem krajowym użytkownicy uzyskują uproszczenie sposobu wybierania numerów w połączeniach krajowych.

Strategia cyfryzacji telewizji naziemnej

MInisterstwo Infrastruktury opublikowało projekt Strategii cyfryzacji nadawania sygnału telewizyjnego który został przygotowany w ramach Międzyresortowego Zespołu ds. Telewizji i Radiofonii Cyfrowej, przez zespół: Prezesa Urzędu Komunikacji Elektronicznej, Przewodniczącego Krajowej Rady Radiofonii i Telewizji, Dyrektora Generalnego Ministerstwa Kultury i Dziedzictwa Narodowego i Podsekretarza Stanu w Ministerstwie Infrastruktury odpowiedzialnego za telekomunikację. W projekcie strategii określono podstawowe parametry, jakie powinny spełniać odbiorniki telewizji cyfrowej, aby poprawnie odebrać i zdekodować sygnały wizji i fonii cyfrowego naziemnego sygnału telewizyjnego nadawanego z obszaru Polski. Odbiornik te, w postaci odbiornika zintegrowanego (tzn. telewizora wyposażonego w tuner oraz dekoder) albo specjalnej przystawki do odbiornika analogowego, powinny spełniać podstawowe wymagania:

- standard emisji DVB-T,
- dla sygnału wizji obsługę formatu SD i HD kodowanych w systemie MPEG-4, część 10 (dokładniej H.264/AVC);
- dla sygnału fonii obsługę formatów od mono, poprzez stereo i dwa dźwięki aż do dźwięku dookólnego 5.1. kodowanych w systemie MPEG-2 Warstwa II albo AC- 3 (Dolby Digital) i E-AC-3 (Dolby Digital Plus).

Telewizja

ADB i CIVOLUTION – nowy sposób na ochronę kontentu

Advanced Digital Broadcast, wiodący dostawca technologii na światowe rynki telewizji cyfrowej, ogłosił wprowadzenie technologii watermarking. Integracja technologii watermarking firmy Civolution VTrack jest kolejnym narzędziem do ochrony kontentu.

„Zastosowanie Vtrack w dekoderach ADB pokazuje jak łatwo można zintegrować tę technologię na różnych platformach: kablowych, satelitarnych, naziemnych i IPTV. Obecnie, przy zwiększonej dostępności do kontentu przedpremierowego a także treści wysokiej rozdzielczości (HD), ważna jest skuteczna ochrona. Amatorska dystrybucja kopii staje się nowym zagrożeniem wymagającym szybkiego, skutecznego i ekonomicznego rozwiązania"– mówi **Alex Terpstra**, Dyrektor Naczelny firmy Civolution.

Wykorzystanie rozwiązania Vtrack pozwala dekoderom ADB znaczyć programy czy filmy (także te na życzenie) tak, by za każdym razem, kiedy transmitowane treści są nielegalnie kopiowane, dostawca mógł łatwo zidentyfikować swą własność, a także źródła potencjalnych kopii. Nawet obniżenie jakości spowodowane zamieszczeniem treści w internecie czy utrwalanie ich amatorską kamerą nie usuwa unikatowej identyfikacji kontentu.

Innowacja na rynku platform cyfrowych

CYFRA+ wprowadza nowe rozwiązanie technologiczne, które umożliwia niezależny odbiór różnych kanałów na dwóch telewizorach w ramach jednego abonamentu. To innowacyjna usługa na polskim rynku – niedostępna w ofercie innych platform cyfrowych.

Wprowadzona w usługa CYFRA+ MULTIROOM umożliwia odbiór programów CYFRY+ na dodatkowym odbiorniku telewizyjnym bez konieczności zawierania odrębnej umowy o abonament. Dzięki usłudze abonenci nie muszą rezygnować ze swych ulubionych programów – mogą pogodzić swe preferencje programowe z gustami innych domowników.

Zestaw CYFRA+ MULTIROOM składa się z dwóch modułów: głównego i dodatkowego. Moduł główny umieszczany jest w dekoderze podłączonym do najczęściej użytkowanego telewizora, moduł dodatkowy zaś współpracuje z dekoderem przy drugim telewizorze. Moduł dodatkowy należy aktywować co kilka godzin, zbliżając go do modułu głównego. Aby korzystać z usługi CYFRA+ MULTIROOM, niezbędne są dwa dekodery oraz instalacja z doprowadzonymi dwoma niezależnymi kablami antenowymi. Zestaw może być użytkowany wyłącznie w ramach jednego gospodarstwa domowego.

Motorola wdroży DVB-H dla INFO-TV-FM

Motorola INC poinformowała, że jej oddział Home & Networks Mobility został wybrany przez firmę INFO TV FM do zaprojektowania i wdrożenia sieci mobilnej telewizji w Polsce. Będzie ona zainstalowana w Warszawie i 9 innych miastach na terenie Polski do końca 2009 roku, zgodnie z warunkami wynikającymi z decyzji Urzędu Komunikacji Elektronicznej dotyczącej rezerwacji częstotliwości. Współpraca obejmuje również finansowanie. Motorola dostarczy kompletne rozwiązanie telewizji mobilnej oparte na

standardach DVB-H i OMA BCAST. Wdrożenie obejmie instalację centralnej stacji czołowej (headend) oraz infrastruktury sieciowej, a także świadczenie usług serwisowych. INFO TV FM będzie hurtowym dostawcą usług telewizji mobilnej oraz radiowych na terenie Polski. Dzięki tym usługom, operatorzy detaliczni będą mieli możliwość zaoferowania swoim klientom elastycznych, mobilnych usług medialnych, które staną się nowym źródłem przychodów.

Orange sport info na satelicie

Orange sport info, pierwszy polski sportowy program informacyjny, utworzony przez Telekomunikację Polską, można już oglądać również za pośrednictwem anteny satelitarnej. Dostępny jest w satelitarnej usłudze telewizyjnej Telekomunikacji Polskiej oraz w ofercie Cyfry+.

Orange sport info rozpoczął nadawanie 6 kwietnia 2009 r., w sieci IPTV Telekomunikacji Polskiej. Jest to kanał przeznaczony do bezpłatnej dystrybucji. Początkowo emisja satelitarna nie będzie kodowana. Po odpowiednim dostrojeniu dekodera (satelita Hot-Bird, transponder 83, częstotliwość 12.360 MHz, polaryzacja pozioma, Service ID: 14029) program będą mogli odbierać wszyscy zainteresowani. Począwszy od października tego roku sygnał satelitarny będzie szyfrowany. W ten sposób TP zapewnia wykorzystanie praw do transmisji wydarzeń sportowych zgodnie z warunkami licencji, czyli na terenie Polski.

Rynek

Eksperci doradzali samorządom

Na Portalu Krajowego Forum Szerokopasmowego – www.forum-szerokopasmowe.pl. Odbył się czat internetowy dotyczący budowy i rozwoju przez samorządy sieci szerokopasmowych.

Budowa i rozwój sieci szerokopasmowych stawia przed samorządami wiele wyzwań. Jednym z nich jest wybór odpowiedniej technologii, która umożliwi dostęp do szybkiego internetu instytucjom publicznym, takim jak biblioteki, szkoły, urzędy państwowe, ale także zwykłym użytkownikom, których nie stać na zakup indywidualnych usług.

Jak wybrać dostawcę, który zapewni łącza odpowiedniej przepustowości tak by spełniały one oczekiwania szerokiej rzeszy zainteresowanych? Jak zabezpieczyć projekt pod względem finansowania, m.in. poprzez wystąpienie o dotacje z Unii Europejskiej czy udział prywatnych inwestorów? Na te i inne pytania odpowiadali eksperci.

Sprzęt transmisyjny Netii trafi do P4

Netia SA zawarła umowę ze spółką P4, na podstawie której w ciągu najbliższego roku odsprzeda sprzęt transmisyjny wykorzystywany dotąd do świadczenia usług transmisji danych właśnie na rzecz tej firmy. Z tytułu sprzedaży tych aktywów Netia otrzyma ponad 65 mln złotych.

P4 nabędzie sprzęt w trzech transzach: o wartości blisko 23 mln zł 1 sierpnia 2009 r.; o wartości ponad 21 mln zł 1 stycznia 2010 r.; o wartości ponad 21 mln zł 1 lipca 2010 r. O wstępnym porozumieniu w tej sprawie spółka informowała w marcu br., kiedy to podpisano list intencyjny.

Jednocześnie Netia SA podpisała z P4 aneks do umowy dot. świadczenia usług transmisji danych. Zmiany, które wprowadza aneks są konsekwencją umowy sprzedaży sprzętu transmisyjnego. Spółki uzgodniły, że umowa ta jest zawarta na czas nieokreślony i wygaśnie w chwili zakończenia wypowiedzenia ostatniego z łączy, na których Netia świadczy usługi transmisyjne dla P4. Minimalny okres wypowiedzenia dla wszystkich usług transmisyjnych dla P4 został wydłużony z 12 do 24 miesięcy. W ramach renegocjowanej umowy Netia spodziewa się świadczenia usług transmisyjnych na rzecz P4 w kolejnych latach, przede wszystkim na bazie własnych sieci metropolitalnych i ogólnopolskiej, światłowodowej sieci szkieletowej.

Internet

Polacy a administracja publiczna w Internecie

Jak złożyć PIT przez internet wie 52 proc. osób korzystających z serwisów administracji publicznej. Z kolei 17 proc. użytkowników takich serwisów zadeklarowało, iż złożyło jakikolwiek dokument urzędowy za pośrednictwem internetu. Mimo to użyteczność załatwiania spraw urzędowych w internecie docenia większość osób, które zadeklarowały odwiedzanie stron instytucji publicznych, urzędów i administracji podczas realizacji badania „Mądry Internet", przeprowadzonego na zlecenie Netii.

Korzystanie z informacji zamieszczanych na stronach instytucji publicznych, urzędów i administracji rządowej oraz samorządowej deklaruje ponad 67 proc. respondentów badania. Najczęściej serwisy administracji publicznej odwiedzają osoby z wyższym wykształceniem (prawie 80 proc., wobec 59 proc. z wykształceniem średnim oraz niewiele ponad połowa z podstawowym), w dojrzalszym wieku (77 proc. respondentów w wieku 45-65 lat w porównaniu do 45 proc. w wieku 18-24 lat).

Prawie trzy czwarte (75 proc.) osób korzystających z serwisów administracji publicznej pobiera z tych stron dokumenty, ale składa je tą drogą zaledwie 17 proc. Warto przy tym zwrócić uwagę na fakt, iż niemal połowa takich osób (48 proc.) nie wie, jak złożyć przez internet PIT, a 86 proc. – jak zarejestrować firmę. Jednak użyteczność załatwiania spraw urzędowych w sieci oceniana przez tę grupę jest dość wysoko – 65 proc. ją docenia, a tylko 13 proc. uważa za nieużyteczne.

Grupa TP zapewni Internet gminnym bibliotekom

Grupa TP wspólnie z Ministerstwem Kultury i Dziedzictwa Narodowego, Ministerstwem Spraw Wewnętrznych i Administracji oraz Fundacją Rozwoju Społeczeństwa Informacyjnego podpisały Porozumienie w sprawie utworzenia programu internetyzacji polskich bibliotek publicznych.

Jego celem jest przekształcenie bibliotek gminnych w nowoczesne, wielofunkcyjne centra informacyjne, kulturalne i edukacyjne. W ramach projektu Grupa TP zapewni bibliotekom szerokopasmowy dostęp do Internetu.

Ze wstępnych analiz wynika, że blisko 40 proc. spośród 8500 polskich bibliotek nie ma dostępu do Internetu. Problem ten dotyczy szczególnie placówek położonych z dala od ośrodków miejskich. Takich bibliotek na wsi i w małych miastach jest 2500. Porozumienie zostało zawarte na 3 lata.

Potencjalne zagrożenia dla dzieci w internecie oczami rodziców

Pornografia, drastyczne materiały, erotyka to, zdaniem rodziców najbardziej niebezpieczne dla dzieci treści w internecie. Aż 70 proc. respondentów za bardzo szkodliwe uważa również niesprawdzone strony z treściami edukacyjnymi – wynika z badania „Mądry Internet", przeprowadzonego na zlecenie Netii przez MillwardBrown SMG/KRC.

Pornografia, drastyczne materiały, erotyka – to według niemal wszystkich internautów-rodziców, których dzieci korzystają internetu (odpowiednio 99, 91 i 85 proc.), najbardziej negatywne treści w sieci, z którymi mogą zetknąć się ich pociechy. Blisko 70 proc. respondentów twierdzi, że zagrożeniem są również niesprawdzone strony z treściami edukacyjnymi. Ograniczonym zaufaniem cieszą się komunikatory internetowe i serwisy społecznościowe, które są negatywnie oceniane przez co czwartego z badanych.

Badanie pokazuje także, że ogromna większość rodziców, posiadających dostęp do internetu (88 proc.) pozwala swoim dzieciom korzystać z sieci. Z kolei aż 75 proc. tych osób deklaruje, że monitoruje działania swoich pociech w internecie. Natomiast mniej niż połowa rodziców (45 proc.) blokuje dzieciom dostęp do stron z negatywnymi treściami!

Mobilny internet w Netii

Mobilny internet Netii jest dostępny jako usługa dodatkowa do łącza stacjonarnego w dwóch taryfach – z pakietem danych 100 MB lub 1 GB. Użytkownicy internetu i telefonu Netii na jej własnych łączach i liniach uwolnionych w ramach LLU, mogą korzystać z niższej taryfy bezpłatnie. Pozostali klienci zapłacą za nią 9,90 zł miesięcznie, a limit 1 GB jest dla wszystkich dostępny za 29 zł miesięcznie. Z mobilnego internetu Netii mogą korzystać zarówno użytkownicy indywidualni, jak i biznesowi. Użytkownicy, którym wyczerpie się pakiet transferu danych, nie muszą się obawiać rachunku za przekroczenie limitu. Aby kontynuować korzystanie z usługi mają do wyboru dwa warianty prostych doładowań: 100 MB za 19 zł lub 1 GB za 40 zł. Można je zamówić przez NetiaOnline lub telefonicznie. Prędkość pobierania danych w mobilnym internecie Netii sięga 1 Mb/s (sieć 3G - UMTS/HSDPA). W ramach usługi, Netia oferuje klientom po atrakcyjnej cenie mobilny modem USB firmy ZTE.

Bezpieczeństwo

W czasie kryzysu rośnie kradzież tożsamości

Od początku roku liczba komputerów zainfekowanych przez złośliwe oprogramowanie służące do kradzieży poufnych danych użytkowników wzrosła 600 proc. w porównaniu z tym samym okresem roku 2008. Każdego dnia pojawia się średnio 37 tys. nowych zagrożeń. Aż 71 proc.z nich to trojany, które zostały stworzone głównie do kradzieży tożsamości.

Według danych zebranych przez Laboratoria firmy Panda Security, lidera w dziedzinie zabezpieczeń działających w technologii Cloud Security, zagrożenia infekujące komputery służą do kradzieży poufnych, osobistych i bankowych danych. Oprócz trojanów, których jest najwięcej, użytkownicy powinni uważać na robaki, spyware oraz działania phishingowe.

Według Luisa Corronsa dyrektora technicznego Laboratorium PandaLabs: „Prawdopodobnie jedną z przyczyn wzrostu ilości zagrożeń jest kryzys ekonomiczny. Sprzedaż poufnych informacji na czarnym rynku (numery kart kredytowych, konta Paypal czy eBay itd.) może przynieść poważne zyski. Zauważyliśmy też wzrost dystrybucji oraz infekcji tego rodzaju złośliwych programów przez serwisy społecznościowe."

Wirus infekujący aplikacje stworzone w Delphi

Kaspersky Lab informuje o wykryciu szkodnika o nazwie Virus.Win32.Induc.a. Wirus ten rozprzestrzenia się poprzez CodeGear Delphi, środowisko programistyczne umożliwiające tworzenie bazodanowych aplikacji dla komputerów stacjonarnych i firm oraz aplikacji sieciowych.

Virus.Win32.Induc.a. infekuje środowisko programistyczne Delphi. Wszystkie aplikacje, które zostały stworzone przy pomocy zarażonego środowiska, zostaną zainfekowane i będą nieustannie powielać wirusa. Wirus nie stanowi obecnie zagrożenia – poza zarażaniem nie posiada żadnej szkodliwej funkcji. Został prawdopodobnie stworzony w celu zademonstrowania i przetestowania nowej procedury infekcji. Bardzo możliwe, że w przyszłości pomysł zostanie podchwycony przez cyberprzestępców, którzy zmodyfikują go w taki sposób, aby był bardziej destrukcyjny.

„Widzę duże możliwości ewolucji Virus.Win32.Induc.a. Trudno jednak powiedzieć, czy któryś z „poważnych" twórców szkodliwego oprogramowania pójdzie tą drogą. W końcu istnieją o wiele prostsze" – powiedział **David Emm**, starszy analityk regionalny z Kaspersky Lab UK.

Spowolnienie gospodarcze a dynamika zakupów online

Według badań przeprowadzonych przez firmę Harris Interactive na zlecenie firmy McAfee, spowolnienie gospodarcze nie wpłynęło na dynamikę zakupów online w takim stopniu, jak obawy dotyczące bezpieczeństwa transakcji. Aż 72 procent ankietowanych konsumentów stwierdziło, że stan gospodarki nie wpłynął na sposób przeprowadzania przez nich zakupów online. Natomiast najpoważniejszą przyczyną rezygnacji z transakcji online są obawy dotyczące bezpieczeństwa transakcji i danych osobowych – prawie połowa badanych porzuciła koszyk lub anulowała transakcję z tego powodu. Nawet szukając dobrej okazji, 63 procent konsumentów nie dokonałoby zakupu w e-sklepie, który nie ma opublikowanej polityki ochrony prywatności lub nie wyświetla uznanego znaku bezpieczeństwa.

Na Zachodzie rośnie liczba konsumentów, którzy wymagają od sklepów online posiadania znaku bezpieczeństwa i nie korzysta z serwisów, które nie mogą się nim wylegitymować. Badanie Harris Interactive pokazało, że co piąty konsument rezygnuje z dokonania zakupu w sklepach, które nie mają takiego certyfikatu, natomiast aż ok. 60 proc. konsumentów czuje się bezpieczniej korzystając ze stron certyfikowanych. Badanie wykazało również, że korzystanie z certyfikatów może być istotnym narzędziem marketingowym dla mniejszych sklepów. Ponad 90 proc. konsumentów obawiało się o bezpieczeństwo podczas zakupów w nowym lub nieznanym sobie e-sklepie, a 47 proc. szukało w takiej sytuacji certyfikatu, aby upewnić się o bezpieczeństwie strony. Co więcej – aż jedna trzecia konsumentów wolałaby kupować w mniejszym sklepie korzystającym ze znaku bezpieczeństwa, niż w dużym i znanym.

Komputery użytkowników neostrady bardziej bezpieczne

Telekomunikacja Polska wspólnie z dużymi serwisami pocztowymi zainicjowała zmiany w funkcjonowaniu poczty elektronicznej. Umożliwią one zmniejszenie ilości niechcianej korespondencji mailowej – spamu – poprzez przeniesienie komunikacji pomiędzy programami pocztowymi a serwerami z portu 25 na porty 587 i 465.

Przeniesienie komunikacji mailowej na porty 587 i 465 jest planowane na 1 grudnia 2009. Jednak już teraz TP oraz portale oferujące usługi poczty elektronicznej rozpoczynają akcję informacyjną, po to, aby dać wszystkim internautom wystarczająco dużo czasu na wprowadzenie odpowiednich zmian w ustawieniach programów pocztowych w swoich komputerach. Instrukcję można znaleźć na stronie www.tp.pl/cert/poczta, swoje instrukcje publikują także dostawcy usług pocztowych. Wszyscy klienci Telekomunikacji Polskiej otrzymają też informacje na temat planowanych zmian we wrześniu, razem z rachunkiem za usługi TP.

Komunikacja pomiędzy klientem pocztowym a serwerem usługi z wykorzystaniem portów innych niż 25 jest zgodna z ogólnoświatowymi standardami opisującymi funkcjonowanie sieci Internet (m. in. dokumentem RFC 4409). Zmiany dotyczą klientów korzystających z programów pocztowych, takich jak Outlook, Outlook Express. Nie dotyczą one tych internautów, którzy wysyłają maile logując się do serwisu internetowego (strony WWW dostawcy poczty).

112 z dofinansowaniem

Projekt „Ogólnopolska sieć teleinformatyczna na potrzeby obsługi numeru alarmowego 112" otrzyma dofinansowanie – ponad 145 mln zł. Projekt zakłada podłączenie do jednej sieci 868 lokalizacji, istotnych z punktu widzenia funkcjonowania Centrów Powiadamiania Ratunkowego oraz Wojewódzkich Centrów Powiadamiania Ratunkowego, a także Państwowej Straży Pożarnej, Policji oraz Państwowego Ratownictwa Medycznego. Jak informuje MSWiA, w tych lokalizacjach zostaną zapewnione wszystkie niezbędne usługi teletransmisji i łączności głosowej. Zbudowane zostaną nowoczesne systemy łączności, zarządzane niezależnie od operatorów telekomunikacyjnych (zostanie powołany Operator, realizujący zadania związane z zarządzaniem i utrzymaniem sieci). Pozwoli to racjonalnie wykorzystać wspólne zasoby teleinfor-

matyczne i poprawi efektywność gospodarowania środkami służb ratowniczych – wyjaśnia MSWiA.

Już ponad rok temu Komisja wezwała władze krajowe do upowszechniania wiedzy na temat numeru 112, ponieważ przeprowadzone badanie ujawniło, że tylko 22 proc. obywateli UE wie, że w razie zagrożenia mogą dzwonić pod ten numer z dowolnego miejsca na obszarze UE. Projekt OST 112 ma się zakończyć w grudniu 2011 roku.

Telekomunikacja

Netia wdraża rdzeń sieci o przepustowości 40 Gb/s

Firma Cisco poinformowała, że Netia wdrożyła system routerów Cisco CRS-1 Carrier Routing System. Ma to przygotować sieć operatora na wzrost wymagań odnośnie łączności szerokopasmowej. Routery Cisco CRS-1 Carrier Routing System zapewniają firmie Netia niezawodną sieć szkieletową o wyjątkowej skalowalności, wysokiej dostępności i poziomie bezpieczeństwa. Ponadto Netia znajduje się w grupie zaawansowanych technologicznie usługodawców, którzy jako pierwsi na świecie będą mogli korzystać z sieciowej technologii IPoDWDM (Internet Protocol over Dense Wavelength-Division Multiplexing) obsługującej przesył do 40 Gb/s. Technologia ta pozwoli korzystać z istniejącej ogólnokrajowej podstawowej infrastruktury światłowodowej 10 Gb/s, podwyższając czterokrotnie jej pojemność bez konieczności modernizacji istniejącego systemu DWDM.

HSPA Evolution w Polkomtelu

Ericsson dostarczył firmie Polkomtel, operatorowi sieci Plus technologię HSPA Evolution, występującą pod nazwą handlową HSPA + zwiększającą pojemność sieci i pozwalającą na uzyskanie trzykrotnie wyższej prędkości pobierania danych w sieci telekomunikacyjnej tego operatora we Wrocławiu.

Wdrożenie technologii HSPA Evolution w sieci Plus we Wrocławiu jest jednym z pierwszych na świecie. Polkomtel dołączył do grona operatorów, którzy już wcześniej zapewnili swoim klientom większy komfort korzystania z mobilnych sieci szerokopasmowych, takich jak mobilkom Austria, 3 Scandinavia oraz Telstra. Dzięki zastosowaniu technologii HSPA+ w sieci Plus we Wrocławiu Polkomtel posiada najszybszą mobilną sieć szerokopasmową w tym mieście. Jest to zarazem sieć udostępniająca największe prędkości mobilnego Internetu w Polsce, nawet 3 razy szybciej niż w przypadku HSDPA z 7,2 Mbps.

Technologia HSPA Evolution pozwala na lepsze wykorzystywanie możliwości łącza szerokopasmowego. Zapewnia znacząco szybsze wyszukiwanie internetowe i pobieranie plików. Dzięki zwiększeniu przepustowości sieci większa liczba użytkowników może korzystać z wyższej prędkości łącza szerokopasmowego, zwłaszcza w obszarach o wysokim obciążeniu.

Pierwsze licencje na technologie LTE

Ericsson, jeden z pionierów technologii LTE, potwierdził podpisanie umów licencyjnych na związane z nią patenty. Jako właściciel największej oferty patentów z zakresu technologii LTE, firma ta opowiada się zdecydowanie za stosowaniem opłat za wykorzystanie praw własności intelektualnej w rozsądnej wysokości.

Ericsson udostępnia swoje technologie innym w ramach licencji typu FRAND (ang. Fair, Reasonable and Non-Discriminatory – uczciwość, rozsądek i brak dyskryminacji), które popiera jako praktykę branżową. Warunki takich licencji są ustalane na podstawie procentowego udziału firmy Ericsson w standardowych prawach własności intelektualnej dotyczących produktów danej kategorii. Zgodnie z promowaną przez siebie praktyką Ericsson dołoży wszelkich starań, aby maksymalna skumulowana stawka dla technologii LTE była ograniczona do liczby jednocyfrowej. Zamierza to osiągnąć poprzez dwustronne negocjacje podejmowane w dobrej wierze.

Informatyka

Elektronicznie dzienniczki ucznia

Szkoły będą mogły prowadzić wyłącznie dzienniki elektroniczne za zgodą samorządu – zakłada nowelizacja rozporządzenia w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania.

Resort edukacji poinformował, że nowelizację rozporządzenia, które umożliwia prowadzenie dzienników elektronicznych zamiast tradycyjnych, papierowych podpisała już minister edukacji **Katarzyna Hall**.

Prowadzenie dzienników wyłącznie w formie elektronicznej będzie wymagało zgody samorządu jako organu prowadzącego.

– Wynika to m.in. stąd, że wprowadzenie systemu informatycznego, umożliwiającego prowadzenie dzienników w formie elektronicznej, wiąże się z koniecznością poniesienia określonych nakładów finansowych związanych z wyposażeniem placówki w odpowiedni sprzęt komputerowy i oprogramowanie, a nierzadko związanych również z potrzebą przeszkolenia kadry pedagogicznej – podkreśla resort edukacji.

Recepta elektroniczna w polskich aptekach

Przedstawiciele trzech firm: iMed24, ILC oraz EuroSoft zawarli porozumienie w sprawie wspólnych działań zmierzających do uruchomienia platformy obsługującej elektroniczne recepty o kodowej nazwie RX24. RX24 będzie innowacyjnym systemem, z którego korzyść odniosą pacjenci, aptekarze, lekarze oraz pośrednio NFZ. RX24 będzie pierwszą w Polsce cyfrową platformą obsługi recept, z której będą korzystali różni producenci oprogramowania dla aptek i placówek ochrony zdrowia.

Na systemach wytwarzanych przez iMed24, ILC i EuroSoft pracuje ponad dwa tysiące aptek i przychodni w Polsce. Tak duża liczba podmiotów sprawia, że efekty wdrożenia platformy RX24 powinny być widoczne w skali całego kraju. RX24 jest pierwszym tego typu przedsięwzięciem realizowanym wspólnie przez kilka firm z sektora informatyki medycznej.

Prawo

Sieć szerokopasmowa obowiązkiem samorządów

Prezes UKE zdecyduje czy samorząd będzie mógł prowadzić działalność w zakresie udostępniania Internetu za darmo lub po cenach niższych niż rynkowe – przewiduje projekt ustawy o sieciach szerokopasmowych przygotowany przez Ministerstwo Infrastruktury i Urząd Komunikacji Elektronicznej. Administracji lokalnej poświęcony jest cały II rozdział ustawy. Na jego podstawie samorząd będzie mógł budować infrastrukturę telekomunikacyjną, głównie jej elementy pasywne (kanalizacja kablowa, pomieszczenia kolokacyjne, słupy, maszty, kable) i przygotowywać ją na potrzeby wykorzystania przez lokalne firmy.

Możliwe będzie („jeżeli zapotrzebowanie użytkowników końcowych w zakresie dostępu do usług telekomunikacyjnych nie jest zaspokojone") także samodzielne świadczenie usług na rzecz użytkowników końcowych. Wszystko w zgodzie z przepisami o wolnej konkurencji.

W ramach upowszechniania sieci szerokopasmowych, projekt nakłada na zarządców dróg obowiązek budowy kanałów technologicznych przy okazji budowy lub przebudowy dróg publicznych. Wyjątek będzie dotyczył jedynie sytuacji, gdy żaden podmiot nie wyrazi zainteresowania korzystaniem z takiego kanału.

VIII Kongres INFOTELA

Grzegorz Kantowicz

Dogonić Europę

W dniach 3-6 czerwca br. w Jastrzębiej Górze odbył się VIII Kongres INFOTELA, jedna z najważniejszych imprez branży komunikacji elektronicznej w Polsce. Organizowane corocznie spotkania to najlepszy sposób na dyskusję i wymianę opinii z liderami rynku na temat przy- szłości komunikacji elektronicznej. Kongresy INFOTELA są spotkaniami adresowanymi zarówno do środowiska branżowego, jak i do innych sektorów gospodarki zainteresowanych wykorzystaniem nowoczesnych technologii teleinformatycznych. Podczas obrad kongresowych omawiane są problemy prawne i biznesowe, które pojawiają się w polskiej branży komunikacji elektronicznej (telekomunikacja, informatyka, telewizja, media).

Hotel Astor w Jastrzębiej Górze, miejsce VIII Kongresu INFOTELA

Tegoroczny kongres odbył się pod patronatem: **Anny Streżyńskiej** – prezesa Urzędu Komunikacji Elektronicznej; **Witolda Drożdża** – podsekretarza stanu w Ministerstwie Spraw Wewnętrznych i Administracji; Ministerstwa Infrastruktury oraz Krajowej Rady Radiofonii i Telewizji. Patronami branżowymi były: Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji, Polska Izba Informatyki i Telekomunikacji, Polska Izba Komunikacji Elektronicznej oraz Polska Izba Radiodyfuzji Cyfrowej.

Sponsorami kongresu były firmy: **TP Emitel**, **Dialog Telecom**, **Grupa ZPAS** oraz **Activis Polska**. Partnerzy kongresu to: **Grupa INEA**, **Netia**, **UPC**, **Eutelsat Communications** oraz **SalesManager Software**.

Pierwszym punktem programu debat, zaraz po otwarciu kongresu przez redaktora **Grzegorza Kantowicza**, było wystąpienie posła **Antoniego**

Grzegorz Kantowicz otwiera obrady kongresowe

Poseł Antoni Mężydło podczas wystąpienia w programie kongresu

Mężydły z Sejmowej Podkomisji ds. Transportu Kolejowego, Łączności i Nowoczesnych Technik Informacyjnych pt. **„Parlamentarne prace legislacyjne w sferze komunikacji elektronicznej”**.

Poseł Mężydło przedstawił stan prac i dyskusji w komisji nad projektami ustaw ułatwiających szybsze tempo budowy infrastruktury szerokopasmowej oraz informatyzację urzędów państwowych.

Wystąpienie to było doskonałym punktem wyjścia do „Debaty Okrągłego Stołu” – następnego punktu programu kongresu – prowadzonej przez **Tomasza Kulisiewicza** z firmy Audytel oraz **Grzegorza Kantowicza** – MSG-Media. W dyskusji udział wzięli:

- Witold Kołodziejski – przewodniczący Krajowej Rady Radiofonii i Telewizji;
- Magdalena Gaj – podsekretarz stanu w Ministerstwie Infrastruktury;
- Marzena Śliz – doradca prezesa Urzędu Komunikacji Elektronicznej;
- Antoni Mężydło – Sejmowa Podkomisja ds. Transportu Kolejowego, Łączności i Nowoczesnych Technik Informacyjnych;
- Wacław Iszkowski – prezes zarządu Polskiej Izby Informatyki i Telekomunikacji;
- Stefan Kamiński – prezes zarządu Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji;
- Henryk Biały – wiceprezes zarządu Polskiej Izby Radiodyfuzji Cyfrowej;
- Wojciech Dziomdziora – Kancelaria Prawna Cottyn Barbasiewicz Łyś-Gorzkowska i Dziomdziora;
- Eugeniusz Gaca – przewodniczący Sekcji Operatorów Telekomunikacyjnych KIGEiT;
- Krzysztof Szydłowski – prezes zarządu, Wielkopolska Telewizja Kablowa;
- Janusz Kosiński – prezes zarządu INEA;
- Józef Kot – prezes zarządu Vectra Inwestycje;

- Leszek Bujak – dyrektor ds. rozwoju ASTRA CEE;
- Zbigniew Kądzielski – dyrektor Instytutu Łączności.

Pierwsza część debaty dotyczyła głównych barier w rozwoju branży, metod pobudzania inwestycji w rozwój infrastruktury komunikacji elektronicznej oraz wykorzystania środków UE na inwestycje IT.

– *Potrzebna jest zmiana mentalności, nie tylko prawa, w branżach, które towarzyszą inwestycjom telekomunikacyjnym: budownictwie, leśnictwie, samorządach itp. Są jeszcze grupy branżowe, które czerpią cały czas korzyści z tego, że każde wykorzystanie infrastruktury drogowej lub komunalnej rodzi za sobą zmiany projektów, a to wiąże się z konkretnymi kosztami i przewlekłością procedur* – powiedział **Eugeniusz Gaca**, przewodniczący Sekcji Operatorów Telekomunikacyjnych w KIGEiT.

– *Musimy jak najlepiej wykorzystać środki unijne na budowę infrastruktury IT. Samorządy mogą wykorzystać je najbardziej efektywnie – do 85 proc. zwrotu kosztów kwalifikowanych. Myślę, że ze strony parlamentu nie powinno być problemów z wprowadzeniem daleko idących zmian w przepisach tzw. okołotelekomunikacyjnych, aby zlikwidować najbardziej uciążliwe z nich w celu usprawnienia procesów inwestycyjnych w budowie infrastruktury telekomunikacyjnej. Już teraz poruszamy się w ustawach na granicy z jednej strony konstytucyjności, a z drugiej – prawa unijnego. Jednak tak musimy działać chcąc zmienić cokolwiek w tej materii* – stwierdził **Antoni Mężydło**.

– *Robimy wszystko, aby dać jak najwięcej możliwości rozbudowy infrastruktury na terenach słabo zurbanizowanych. Nie należy się obawiać, że samorządy lokalne będą mogły budować własną infrastrukturę. Hasło „darmowego internetu" będzie realizowane w bardzo ograniczonym zakresie, tak aby nie zaburzać rynku komercyjnego. Natomiast samorząd jako właściciel infrastruktury będzie mógł powierzyć operatorowi komercyjnemu zarządzanie własną infrastrukturą* – uspokajała **Marzena Śliz**, doradca prezesa Urzędu Komunikacji Elektronicznej.

– *Bardzo chlubnym wyjątkiem jest realizowana inwestycja światłowodowa w Toruniu, gdzie przy okazji modernizacji sieci wodociągowej położono kilkaset kilometrów sieci światłowodowej. Obecnie infrastruktura jest gotowa na instalację urządzeń aktywnych przez operatora. Jest to ewenement na skalę krajową, który należy propagować* – dodał **Eugeniusz Gaca**.

Pierwsza część dyskusji zakończyła się wprowadzeniem do tematu drugiej części, w której poruszono zagadnienia regulacji rynku komunikacji elektronicznej oraz priorytetów regulacyjnych.

– *Czy istnieje możliwość, w określonym przedziale czasowym, całkowitego zniesienia regulacji rynku komunikacji elektronicznej? Jakie do tego muszą być spełnione warunki?* – zapytał **Wacław Iszkowski**, prezes Polskiej Izby Informatyki i Telekomunikacji.

– *Moim zdaniem, nie będzie nigdy takiej sytuacji* – stwierdziła **Magdalena Gaj**, podsekretarz stanu w Ministerstwie Infrastruktury. – *Organ regulacyjny będzie potrzebny zawsze, jednak możemy mówić o różnej skali jego aktywności. Ze względu na strukturę naszego rynku – z operatorem dominującym niechętnym do współpracy z konkurentami – poziom*

Sala konferencyjna podczas obrad

Uczestnicy „Debaty Okrągłego Stołu" – „Dogonić Europę"

Minister Magdalena Gaj podczas debaty

ingerencji regulatora musi być dość głęboki. Z czasem, wraz ze zmianami postaw podmiotów rynkowych, może dojść do mniejszej aktywności i ingerencji regulatora, jednak zawsze regulator, zintegrowany czy też w postaci dwóch podmiotów – jak obecnie, będzie potrzebny.

– Wydaje mi się, że regulacje rynku są potrzebne, ale wyłącznie „ex-post". Tak naprawdę wszystkie obecnie wydawane przez Krajową Radę Radiofonii i Telewizji koncesje są niepotrzebne. Szczególnie dotyczy to telewizji satelitarnej i kablowej. Wystarczyłoby zgłoszenie, jak to ma miejsce w przypadku działalności telekomunikacyjnej – powiedział mecenas **Wojciech Dziomdziora**. – *Jestem zwolennikiem pomysłu Pana Grzegorza Kantowicza, aby oddzielić komunikację elektroniczną od autostrad i powołać osobne ministerstwo. Jedno ministerstwo kierujące kilkoma strategicznymi sektorami nie może funkcjonować prawidłowo* – dodał.

Szeroko omawiana była problematyka praw autorskich, szczególnie obecnie – kiedy każdy z nas może być jednocześnie nadawcą treści, jak i odbiorcą. Przykładem mogą być wideoblogi oraz internetowe telewizje społecznościowe.

W sesji popołudniowej równolegle odbywały się warsztaty biznesowe firm **Activis Polska** i **MSG-Media** oraz seminaria firmowe. Firma **SalesManager Software** przedstawiła **„Technologie i rozwiązania software'owe dla realizacji multimedialnych usług komunikacji elektronicznej w czasie rzeczywistym i nierzeczywistym"**. **TP EMITEL** zaprezentował **„Ewolucję usług multimedialnych"**, a **Netia** w wystąpieniu pt. **„Rozbudowa infrastruktury sieciowej na potrzeby LLU – czy to się opłaca?"** przedstawiła studium przypadku realizacji LLU przez operatora. **Grupa INEA** przedstawiła profil działalności grupy i ofertę usługową.

Po bogatym merytorycznie dniu nadszedł czas na rekreację. Tradycyjnie już, po południu, odbył się finał turnieju o puchar INFOTELA w bowlingu oraz konkurs w rzucie komórką na odległość, a pierwszy merytoryczny dzień kongresu zakończyła uroczysta Gala Komunikacji Elektronicznej, podczas której rozstrzygnięto **11. edycję Ogólnopolskiego Konkursu o LAUR INFOTELA.** Honorowy patronat nad konkursem sprawowały: Ministerstwo Infrastruktury, Krajowa Rada Radiofonii i Telewizji, Urząd Komunikacji Elektronicznej, Ministerstwo Spraw Wewnętrznych i Administracji, Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji, Polska Izba Informatyki i Telekomunikacji, Polska Izba Komunikacji Elektronicznej oraz Polska Izba Radiodyfuzji Cyfrowej.

Bowling, bilard oraz rzut komórką na odległość stanowiły pierwszą część rekreacyjną kongresu

LAURY INFOTELA przyznała Komisja Konkursowa, która powołana została przez Radę Programową magazynu INFOTEL w styczniu bieżącego roku. W jej skład weszli:

- prof. **Ryszard Choraś** z Uniwersytetu Technologiczno-Przyrodniczego w Bydgoszczy;
- prof. **Józef Modelski** z Politechniki Warszawskiej, przewodniczący Sekcji Radiokomunikacji PAN;
- **Stefan Kamiński**, prezes Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji;
- **Grzegorz Kantowicz** – przewodniczący jury, redaktor naczelny magazynu INFOTEL.

W kategorii pierwszej, obejmującej **„Systemy komunikacji elektronicznej"** LAUR INFOTELA zdobyła firma **TP Emitel Sp. z o.o.** w Warszawie za **„EmiKam – platformę do tworzenia i transmisji kontentu"**.

W kategorii drugiej, obejmującej **„Elementy systemów"** LAUR INFOTELA przyznano firmie **P.H. Elmat Sp. z o.o.** w Rzeszowie za **„VERTICASA – system okablowania światłowodowego budynków mieszkalnych z kablami łatwego dostępu"**.

W kategorii trzeciej „Usługi" LAUR INFOTELA przyznano firmie **NETIA SA** w Poznaniu za **„Usługę ONE OFFICE"**.

W kategorii czwartej „Wdrożenia" LAUR INFOTELA przyznano firmie **„ksi.pl" Sp. z o.o.** w Krakowie za **„Kompleksową realizację wdrożenia systemu BlueSend na XX Międzynarodowych Targach Komunikacji Elektronicznej INTERTELECOM 2009"** oraz **Konsorcjum FEN** w Poznaniu za **„Wdrożenie infrastruktury sieci bezprzewodowej Meru Networks na Uniwersytecie Mikołaja Kopernika w Toruniu"**.

Podczas Gali wręczono także LAURY INFOTELA przyznane przez redakcję:

- w kategorii **„Firma"** LAUR INFOTELA otrzymała firma **Kujawsko-Pomorska Sieć Informacyjna** za **„realizację projektu Kujawsko-Pomorskiej Sieci Informacyjnej"**;
- w kategorii **„Osoba"** – **Romuald Szymański**, prezes zarządu firmy **TELETRA KOMTRANS** za **„szczególny wkład w rozwój komunikacji elektronicznej"**.

Redakcja INFOTELA przyznała także trzy Platynowe Laury Dekady dla:

- **Janusza Kosińskiego**, prezesa zarządu spółki INEA SA za **„wieloletnią realizację procesów konsolidacyjnych w branży telekomunikacyjnej w Wielkopolsce"**;

- firmy **VECTOR Sp. z o.o.** za **„wieloletni skuteczny rozwój rodzimego kapitału i myśli technicznej na rynkach krajowym i międzynarodowym branży telekomunikacyjnej”**;
- **Międzynarodowych Targów Łódzkich Sp. z o.o.** za **„dwudziestoletnie promowanie i integrację branży komunikacji elektronicznej poprzez organizację targów INTERTELECOM”**.

Redaktor Grzegorz Kantowicz ogłasza rozstrzygnięcie Konkursu o LAUR INFOTELA

W ramach Konkursu o LAUR INFOTELA redakcja przeprowadziła również plebiscyt wśród czytelników. A oto wyniki głosowań.

Laureaci XI edycji Konkursu o LAUR INFOTELA

Laury Czytelników otrzymali:

- **P4 Sp. z o.o., operator sieci Play** – najlepszy operator telefonii i internetu mobilnego;
- **UPC Polska Sp. z o.o.** – najlepszy operator telefonii i szerokopasmowego internetu stacjonarnego;
- **Eutelsat Polska Sp. z o.o.** – najlepszy operator satelitarny;
- **Vectra SA** – najlepszy operator telewizji kablowej;
- **Canal+ Cyfrowy Sp. z o.o.** – najlepszy nadawca telewizyjny i dystrybutor telewizyjny;

Duet Electrica Duo – Kasia & Paula zachwycił wszystkich, a Paweł Kluz czarował gości dosłownie i w przenośni

- **Polsat News** – najlepszy telewizyjny kanał tematyczny;
- **tvp.pl** – najlepsza witryna internetowa.

LAUR INFOTELA to statuetka zaprojektowana i wykonana przez bydgoskiego artystę rzeźbiarza – Marka Guczalskiego.

Galę uświetnił program artystyczny duetu **Electrica Duo – Kasia & Paula** oraz **Paweł Kluz**, który czarował gości dosłownie i w przenośni.

W drugim dniu kongresu zorganizowane zostały dwa ciekawe panele. Pierwszy to **„Nowe rodzaje treści i ich dystrybucji w kontekście cyfryzacji przekazów medialnych”**, prowadzony przez **Wojciecha Apela** – 3S Śląskie Sieci Światłowodowe.

W dyskusji udział wzięli:

- **Wojciech Dziomdziora** – Kancelaria Prawna Cottyn Barbasiewicz Łyś-Gorzkowska i Dziomdziora;
- **Janusz Kosiński** – prezes zarządu Grupy INEA;

Panel dyskusyjny „Nowe rodzaje treści i ich dystrybucji w kontekście cyfryzacji przekazów medialnych”

Szybkość, wiatr, emocje – przejażdżki na najszybszych łodziach motorowych PARKER 900 Baltic pływających na polskim wybrzeżu jednostek specjalnych Marynarki Wojennej „FORMOZA”

- **Mateusz Górecki** – Manager ds. Rozwoju Internet Group;
- **Krzysztof Świergiel** – dyrektor zarządzający Eurosport Poland;
- **Marek Cybulski** – dyrektor działu sprzedaży Zonemedia Poland;
- **Bartłomiej Czardybon** – prezes zarządu SGT;
- **Witold Kundzewicz** – członek zarządu, Wielkopolska Telewizja Kablowa.

W dyskusji poruszono m.in. kwestie relacji nadawca-operator na rynku polskim. Omówiono nowe technologie dystrybucji treści w sieciach naziemnych oraz nowe zachowania widzów.

Bardzo ciekawym wątkiem była problematyka personalizacji kanałów telewizyjnych. Modele biznesowe producentów i nadawców oparte są na pakietyzacji kanałów telewizyjnych. Jednocześnie dzisiejszy odbiorca nie chce płacić za pakiety, w których interesuje go tylko kilka kanałów. Operatorzy już dzisiaj przygotowani są do zmiany modeli dystrybucji w kierunku większej personalizacji, jednak dostawcy treści niechętnie przystosowują się do tych nowych wymagań.

Także w tej dyskusji przewijała się problematyka praw autorskich oraz organizacji zbiorowego zarządzania, które determinują niektóre zachowania i modele sprzedażowe na rynku.

Ostatnim punktem merytorycznego programu kongresu była dyskusja panelowa **„Dylematy i rozdroża rozwoju infrastruktury telekomunikacyjnej NGN”**, do której wprowadzili **Tomasz Kulisiewicz** oraz **Marek Średniawa** z Politechniki Warszawskiej. Udział w dyskusji wzięli:

- **Marzena Śliz** – doradca prezesa Urzędu Komunikacji Elektronicznej;
- **Eugeniusz Gaca** – przewodniczący Sekcji Operatorów Telekomunikacyjnych KIGEiT;
- **Jarosław Janiszewski** – prezes zarządu HAWE;
- **Janusz Kosiński** – prezes zarządu Grupy INEA;
- **Paweł Żytecki** – dyrektor Departamentu Rozwoju Sieci, NETIA;
- **Zbigniew Kądzielski** – dyrektor Instytutu Łączności.

Podczas dyskusji zdefiniowano NGN oraz omówiono nowe wyzwania stojące przed regulacjami komunikacji konwergentnej. Uczestnicy dyskusji przedstawili problemy inwestycyjne budowy sieci NGN/NGA oraz bariery ich rozwoju.

Był to ostatni punkt programu merytorycznego kongresu.

Po południu na uczestników czekały emocje związane z przejażdżkami na najszybszych łodziach motorowych PARKER 900 Baltic pływających na polskim wybrzeżu jednostek specjalnych Marynarki Wojennej „FORMOZA”. Wieczorem, podczas grillowania, wręczono puchary i nagrody zwycięzcom konkursu w rzucie komórką na odległość oraz Turnieju o Puchar Infotela w bowlingu. W ten sposób dobiegł końca drugi dzień merytoryczny i zarazem cały kongres INFOTELA.

– *Bardzo ciekawe dyskusje, o wielu sprawach usłyszałam po raz pierwszy. Mam kilka spostrzeżeń i wniosków, które będę chciała wykorzystać w mojej pracy* – powiedziała **Magdalena Gaj** na pożegnanie.

Bezpośredni kontakt uczestników z organizatorami kongresu zapewniał VoiceLink – nowatorska usługa głosowa ze stron internetowych

My także mamy nadzieję, że tegoroczny kongres przyczynił się do lepszego zrozumienia skomplikowanych zasad funkcjonowania rynku komunikacji elektronicznej w Polsce.

Wszystkie debaty kongresu były transmitowane on-line na stronie internetowej. Relacje wideo z wystąpień oraz paneli dyskusyjnych można obejrzeć na stronie ***www.techbox.pl.*** ■

Piomar

środowiska dla elektroniki

szafy zewnętrzne dla telekomunikacji
wyposażenie Data Center
stanowiska nadzoru

Generalny Dystrybutor KNÜRR AG w Polsce

knürr
environments for electronics

ul. Świderska 35
03-128 Warszawa

tel. 022-6769462
tel./fax 022-6769810

e-mail: piomar@piomar.com.pl

www.piomar.com.pl

www.knuerr.com

Wartość dodana czy niezależny segment rynku

VoIP w Polsce

Wartość rynku telefonii VoIP w Polsce na koniec 2008 r. wyniosła 440 mln zł. Największą część przychodów w segmencie wygenerowali operatorzy sieci kablowych. W ostatnich latach usługi VoIP wprowadzili do swojej oferty również operatorzy telefonii stacjonarnej.

Według firmy badawczej PMR, rynek VoIP w Polsce w dalszym ciągu stanowi niewielką część rynku telefonii stacjonarnej. W 2008 r. jego udział pod względem wielkości przychodów plasował się na poziomie nieprzekraczającym pięciu procent. Telefonia VoIP nadal jest traktowana przede wszystkim jako narzędzie do wykonywania bezpłatnych połączeń „z komputera na komputer" przez użytkowników indywidualnych. W przypadku sektora biznesowego cały czas zdecydowana większość firm podchodzi do rozwiązań VoIP z dystansem, traktując telefonię IP najczęściej jako narzędzie dodatkowe.

W segmencie użytkowników indywidualnych dominują operatorzy telewizji kablowych, świadcząc usługi telefonii internetowej jako element pakietu triple play. Na koniec 2008 r. posiadali ok. 450 tys. abonentów VoIP. Warto dodać, że oferta cenowa sieci kablowych pozycjonowana jest z reguły pomiędzy stawkami VoIP dostępnymi u dostawców wyspecjalizowanych w usługach telefonii internetowej a usługami tradycyjnej telefonii stacjonarnej. Z jednej strony pozwala to na przyciągnięcie klientów, z drugiej zaś – na generowanie relatywnie wyższych marż.

Aby zwiększyć przewagę konkurencyjną na rynkach lokalnych, swoją ofertę o VoIP poszerzają także lokalni dostawcy internetu. Przedstawiciele firm deklarują, że usługa nie przynosi wysokich przychodów, ale jest sposobem na utrzymanie klientów. Oprócz wdrożeń własnych systemów telefonii internetowej coraz częstszą praktyką jest korzystanie przez lokalnych ISP z platform większych dostawców.

Udział w rynku wyspecjalizowanych operatorów usług VoIP (m.in. *EasyCall*, *FreecoNet*, *HaloNet*) pod względem wielkości przychodów pozostaje niewielki. W sektorze pojawiają się opinie, że błędem było skupienie się w przeszłości na segmencie użytkowników indywidualnych. Obecnie operatorzy zaczynają koncentrować się na klientach biznesowych, licząc na wyższe przychody z tytułu większego ruchu i usług dodanych.

Usługi telefonii internetowej na coraz szerszą skalę pojawiły się także w ofercie operatorów telekomunikacyjnych świadczących usługi telefonii stacjonarnej. VoIP jest w tym przypadku uzupełnieniem oferty i sposobem na zatrzymanie klientów.

W ciągu najbliższych czterech lat dynamika wzrostu rynku VoIP w Polsce pozostanie na stabilnym poziomie. PMR oczekuje, że pozytywnie na wartość sektora wpłynie panujące w Polsce spowolnienie gospodarcze. Zarówno dla firm, jak i gospodarstw domowych poszukujących oszczędności na rachunkach telefonicznych VoIP może stanowić przynajmniej godną uwagi alternatywę. Ponadto telefonia internetowa będzie w dalszym ciągu zyskiwać popularność jako element pakietów usług telekomunikacyjnych. Przykłady krajów Europy Zachodniej – zwłaszcza Francji – pokazują, że taka forma oferowania usług VoIP cieszy się największą popularnością wśród klientów indywidualnych.

Z drugiej strony, różnice w cenach połączeń w tradycyjnej telefonii i VoIP stopniowo zaczynają się zacierać. W efekcie telefonia internetowa sukcesywnie traci swoją największą przewagę konkurencyjną – wyraźnie niższe stawki za połączenia. W dalszym ciągu jednak o zaletach telefonii IP będzie stanowić możliwość wykonywania bezpłatnych połączeń w sieci oraz szeroki zakres usług dodanych.

W dłuższym okresie spodziewamy się stopniowej migracji abonentów z telefonii tradycyjnej do VoIP, czemu będą sprzyjać przede wszystkim inwestycje operatorów w rozwój sieci NGN. Jednak ze względu na odsuwanie inwestycji w czasie, przeniesienie środka ciężkości w stronę telefonii komórkowej, a także wspomniane spadki cen połączeń w telefonii stacjonarnej, proces ten będzie przebiegał dużo wolniej, niż jeszcze kilka lat temu zakładali sami uczestnicy rynku.

Na podstawie raportu firmy PMR pt. „Rynek VoIP w Polsce 2009. Prognozy rozwoju na lata 2009-2012"

Green IT w firmach sektora MŚP

Grzegorz Kantowicz

Cena ważniejsza niż ekologia

Jak wynika z najnowszych badań D-Link Technology Trend przeprowadzonych wśród firm sektora MŚP, przy zakupie sprzętu IT walory ekologiczne stanowią marginalną rolę. Mimo wysokiej świadomości ekologicznej oraz świadomości korzyści wynikających z używania energooszczędnych urządzeń, firmy przy zakupach kierują się przede wszystkim ceną.

Najnowsze wyniki badań przeprowadzonych wśród małych i średnich przedsiębiorstw są zaskakujące.

Niemalże wszyscy ankietowani (94 proc.) zgodzili się z twierdzeniem, iż wykorzystanie energooszczędnych urządzeń przyczynia się do dbałości o środowisko naturalne, jednak przy zakupie sprzętu na posiadane przez producentów certyfikaty związane z ochroną środowiska zwraca uwagę niecała połowa (49 proc.) z nich. Jeszcze mniejszy odsetek firm (36 proc.) zwraca uwagę na poszanowanie środowiska przy produkcji sprzętu.

Aż cztery na pięć firm (81 proc.) uważa, iż czynnik energooszczędności powinien być brany pod uwagę przy zakupie sprzętu IT, przeciwnego zdania jest jedynie 6 proc. badanych.

Zgodnie z tymi deklaracjami postępuje jednak niespełna połowa ankietowanych. Co więcej, wśród firm z sektora MŚP, które organizują przetargi na dostawy sprzętu IT, prawie połowa (47 proc.) nigdy nie uwzględnia czynnika energooszczędności w specyfikacji przetargowej. Niecała jedna trzecia z nich (31 proc.) robi to rzadko, tylko jedna piąta zaś deklaruje, iż robi to często lub zawsze (22 proc.).

Mimo iż 37 proc. firm zadeklarowało gotowość do ponoszenia dodatkowych kosztów w związku z inwestycjami w Green IT, w praktyce to cena decyduje o zakupie. Według badań, w zeszłym roku jedynie 15 proc. firm dokonało zakupu jakiegokolwiek urządzenia IT kierując się jego walorami ekologicznymi.

Ankietowani zapytani wprost, na co zwracają uwagę przy zakupie, w pierwszej kolejności wskazywali właśnie cenę (85 proc.), jakość urządzeń (84 proc.) oraz gwarancje i serwis posprzedażowy (79 proc.). W dalszej kolejności wymieniali renomę producenta (29 proc.) oraz jakość obsługi klienta (13 proc.), a na „szarym" końcu – walory ekologiczne (12 proc.).

– *Polskie firmy są świadome korzyści wynikających z zastosowania produktów Green IT. Menedżerowie odpowiedzialni za inwestycje informatyczne nad wyraz chętnie przyznają, że zwracają uwagę na ekologiczne walory urządzeń podczas inwestycji w infrastrukturę informatyczną, jednak fakty przeczą tym deklaracjom. Jedynie 15 proc. polskich firm zakupiło w minionym roku sprzęt IT kierując się jego energooszczędnością. Czynnik „ekologiczności" urządzeń wciąż przegrywa konkurencję z bardziej wymiernymi cechami produktów, przede wszystkim z ceną urządzeń. Pełne sprzeczności wyniki badań wskazują na rozdarcie firm, które chciałyby inwestować w „zielone" rozwiązania informatyczne, jednak w obliczu słabszej koniunktury rynkowej na pierszym miejscu stawiają koszty zakupu sprzętu* – skomentował badanie **Mariusz Piaseczny**, PR Manager Eastern Europe, D-Link. ■

W pogoni za „szerokim pasmem”

Marcin Ułasik

Standard DOCSIS 3.0 a usługi dostępu do internetu

Rynek usług dostępu do internetu w ostatnich latach rozwija się bardzo dynamicznie. Obserwowane jest ciągłe zwiększanie oferowanych prędkości łączy, jak również stały wzrost średniej konsumpcji pasma. Zwiększaniu przepustowości sprzyjają z jednej strony abonenci korzystający z coraz bardziej wymagających usług, z drugiej zaś strony – sami operatorzy poprzez konkurencję pomiędzy operatorami DSL i kablowymi. Dzisiaj nikogo nie dziwią oferty 10 Mb/s czy nawet 30 Mb/s. Wiodący operatorzy kablowi już zapowiadają, że wkrótce dostępne będą łącza o przepustowości 100 Mb/s i więcej. Jak to możliwe?

Operatorzy kablowi zyskali bardzo silnego sprzymierzeńca, jakim jest nowa wersja znanego standardu DOCSIS (*Data Over Cable System Interface Specification*). DOCSIS 3.0, bo o tej wersji tu mowa, wprowadza kilka znaczących modyfikacji do systemu oraz do jego kluczowych elementów, czyli CMTS (*Cable Modem Termination System* – kontroler modemów kablowych) i modemu kablowego. Tworząc standard DOCSIS 3.0 postawiono przed nim kilka istotnych zadań:

- umożliwienie oferowania usług dostępu do internetu o szybkości powyżej 100 Mb/s;
- znaczące obniżenie kosztu oferowanych przepływności;
- zachowanie kompatybilności wstecz z istniejącymi obecnie w sieci urządzeniami.

W praktyce oznacza to bardzo dużą elastyczność konfiguracji systemów zgodnych z DOCSIS 3.0, tak aby zapewnić jak najbardziej efektywną realizację potrzeb biznesowych operatora. Szczególnie istotnym elementem w systemie jest CMTS i to jego dotyczy większość zmian wpływających na tę właśnie elastyczność.

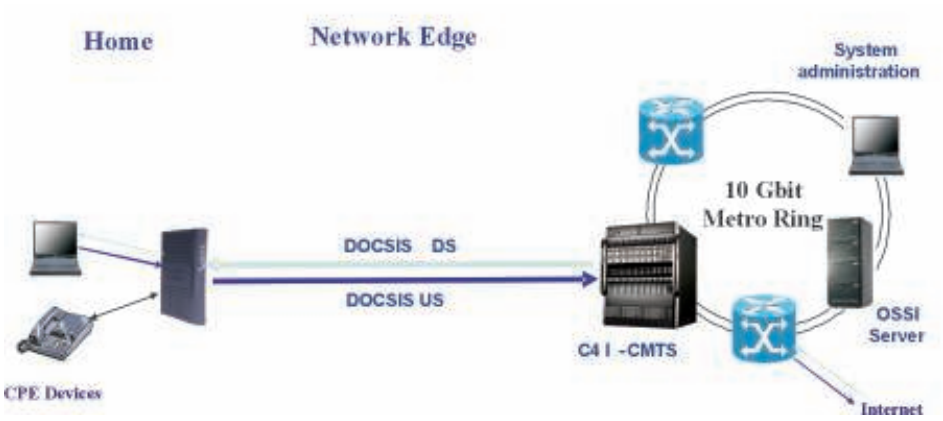
Największą zmianą, jaką wnosi nowy standard do systemu, jest wspomniana możliwość świadczenia usług o bardzo dużych przepływnościach (pow. 100 Mb/s). Wykorzystuje się tu technologię *channel bonding* – łączenia kanałów w taki sposób, że kilka dotychczasowych kanałów transmisyjnych transmituje dane do i od pojedynczego abonenta. Urządzenia końcowe (CMTS i modem kablowy) dbają o logiczną spójność danych wysyłanych w taki sposób. Oczywiście, aby wykorzystać taką możliwość, oba urządzenia końcowe muszą być zgodne z DOCSIS 3.0.

Oferowanie takich usług wymaga znaczącego zwiększenia liczby dostępnych kanałów transmisyjnych. Z uwagi na to, iż większość ruchu odbywa się w kierunku do abonenta (więcej pobieramy niż sami oferujemy), szczególnie istotne jest zwiększenie liczby kanałów, które transmitują dane w tym kierunku (*downstream*). W tym momencie z pomocą przychodzi postęp technologii, oferując jednoukładowe wielokanałowe modulatory i *upconvertery*. Dzięki temu można obniżyć koszy pojedynczego kanału, ale również zwiększyć gęstość upakowania sprzętu. To z kolei prowadzi do oszczędności miejsca, energii i … kosztów z tym związanych.

Wspomniana powyżej cecha asymetryczności ruchu abonenckiego spowodowała wprowadzenie w nowym standardzie całkowitego rozdzielenia sprzętowego kanałów do i od abonenta (*downstream* i *upstream*) w CMTS. Oznacza to, że w każdym urządzeniu CMTS zgodnym z DOCSIS 3.0 powinna istnieć możliwość niezależnej rozbudowy *upstream* i *downstream*. Jest to kolejna możliwość oszczędności kosztów zarówno bezpośrednich (wydatki na rozbudowę jedynie niezbędnych kanałów), jak i pośrednich (miejsce, energia).

Na szczególną uwagę zasługuje fakt, iż standard umożliwia świadczenie usług o szybkościach pow. 100 Mb/s, co nie oznacza, że wymusza na operatorze ich świadczenie. Standard nie jest tożsamy z usługą – nie ma czegoś takiego, jak usługi DOCSIS 3.0. Operator może uruchomić urządzenia zgodne z DOCSIS 3.0 (CMTS), skorzystać z ich elastyczności i obniżyć koszty, jednocześnie utrzymując usługi na dotychczasowym poziomie, używając nadal modemów kablowych w wersji DOCSIS 1.0, 1.1 i 2.0. Zgodność wstecz to jedna z ważniejszych cech w całej historii standardu DOCSIS.

Dzięki kompatybilności wstecz uruchomienie CMTS zgodnego z DOCSIS 3.0 nie wymusza wymiany wszystkich dotychczas instalowanych modemów w sieci. Można w dalszym ciągu z powodzeniem wykorzystywać je do świadczenia obecnych usług. Co ważne, można też bez pro-



Rysunek 1. Architektura I-CMTS systemu standardu DOCSIS 3.0

blemu instalować nowe modemy zgodne z poprzednimi wersjami standardu, o ile oferowane usługi nie wymagają nowego sprzętu. Podsumowując, dla wszystkich operatorów, którzy oferują usługi 5, 10 czy nawet 20 Mb/s, standard DOCSIS 3.0 wnosi znaczące obniżenie kosztów oferowanych usług bez konieczności ich zmiany.

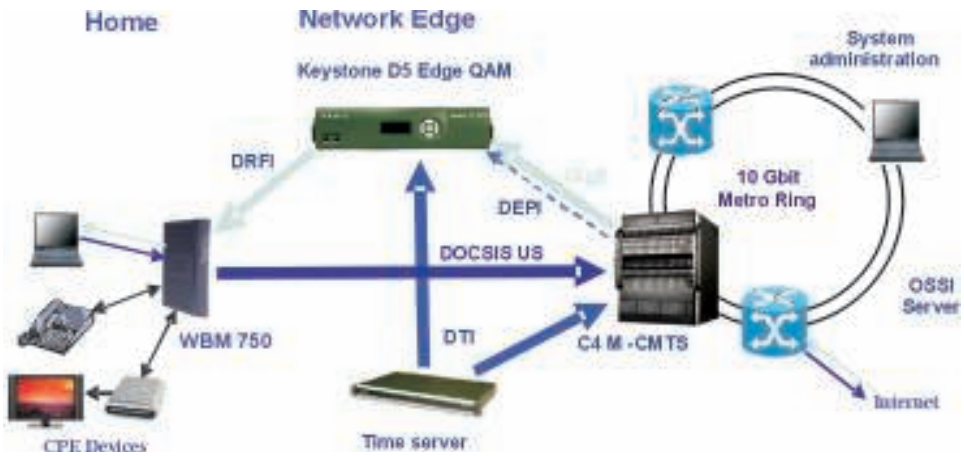
Standard DOCSIS 3.0 nie wymaga istotnej zmiany w architekturze samego CMTS (z wyjątkiem obsługi większej ilości danych), jednakże wprowadzone w standardzie DOCSIS 3.0 rozdzielenie kanałów *downstream* i *upstream* pozwala również na znaczącą modyfikację struktury systemu, lecz kosztem jego znaczącego skomplikowania. Mowa tu o architekturach I-CMTS (*Integrated CMTS*) i M-CMTS (*Modular CMTS*).

■ model I-CMTS (rys. 1)

Umożliwia niezależne skalowanie kanałów *downstream* i *upstream* oraz realizację funkcji DOCSIS 3.0 w pojedynczej, zintegrowanej obudowie. Ta architektura jest w zasadzie identyczna z obecnie stosowanymi – jedno urządzenie (potocznie zwane „szafką") zawiera moduły kanałów *upstream* i *downstream*, zapewniając niezawodność telekomunikacyjną, łatwość zarządzania pojedynczym elementem sieci IP, jednocześnie znacznie zwiększając gęstość, wydajność i skalowalność rozwiązania. W tym wypadku zmiana (*upgrade*) z poprzedniej wersji standardu do DOCSIS 3.0 sprowadza się do instalowania nowych modułów i nowej wersji oprogramowania. Struktura i koncepcja systemu nie różni się od obecnie stosowanego.

■ model M-CMTS (rys. 2)

Architektura M-CMTS dzieli funkcje CMTS pomiędzy dotychczasowe urządzenie CMTS oraz EdgeQAM. Z CMTS zostaje wyjęta obróbka końcowa kanałów *downstream* (modulacja i upkonwersja), pozostaje przetwarzanie i analiza pakietów (warstwa DOCSIS MAC) oraz odbiór kanałów *upstream*. Kanały *downstream* dosyłane są do zewnętrznych urządzeń EdgeQAM poprzez porty Gigabit Ethernet i protokół DEPI (*Downstream External Physical Interface*). Architektura ta w swojej idei ma umożliwić wykorzystanie wolnych kanałów QAM z istniejących w sieci urządzeń EdgeQAM stosowanych do potrzeb telewizji cyfrowej. W praktyce jednak systemy telewizji cyfrowej i transmisji danych są od siebie odseparowane i aby wykorzystać M-CMTS, trzeba instalować nowe urządzenia. Powoduje to niepotrzebną komplikację systemu, nie wnosząc obniżenia kosztów. M-CMTS wymaga również synchronizacji czasu pomiędzy CMTS i EdgeQAM z uwagi na zależność czasową transmisji od modemu do CMTS (TDMA – *Time Domain Multiple Access*). Konieczne jest więc również instalowanie serwerów czasu, utrzymywanie niezależnej



Rysunek 2. Architektura M-CMTS systemu standardu DOCSIS 3.0

sieci (DTI – *DOCSIS Timing Interface*) i administrowanie tymi urządzeniami.

Przykładem CMTS zgodnego z DOCSIS 3.0 jest ARRIS C4®. C4 jest kontrolerem modemów kablowych o bardzo wysokiej wydajności i niezawodności pozwalającym na zwiększenie satysfakcji abonentów z dostarczanych usług telefonii, transmisji danych i telewizyjnych. Kontroler umożliwia operatorom dopasowanie systemu do indywidualnych potrzeb biznesowych poprzez elastyczną rozbudowę, szeroką gamę opcji konfiguracyjnych oraz niezrównane możliwości doboru jakości świadczonych usług. ARRIS C4 CMTS pozwala operatorom na świadczenie zaawansowanych usług telefonii, transmisji danych i wideo poprzez konwergentną sieć IP zarówno dla klientów indywidualnych, jak i biznesowych.

Rysunek 3. ARRIS C4® CMTS

Funkcjonalności, jakie oferuje ARRIS C4, to m.in. pełny zestaw możliwości routingu warstwy 3, połączony z funkcjami warstwy DOCSIS RF w jednej architekturze. CMTS C4 jest kwalifikowany do pracy w sieciach DOCSIS 2.0, EuroDOCSIS 2.0 oraz PacketCable 1.0. Konstrukcja CMTS C4 gwarantuje realizację wszystkich funkcjonalności DOCSIS 3.0 zarówno poprzez architekturę I-CMTS, jak i M-CMTS, zapewniając pełną zgodność ze standardem DOCSIS 3.0.

Nowości sprzętowe architektury ARRIS C4 CMTS związane z DOCSIS 3.0:

karta kablowa 16D

Karta 16D *Cable Access Module* (CAM) posiada szesnaście (16) kanałów *downstream* zgodnych z DOCSIS/EuroDOCSIS 3.0. Kanały te są zgrupowane po cztery w nowoczesnych blokowych *upconwerterach*, umożliwiając użycie pełnej liczby szesnastu na zaledwie czterech złączach typu F. Każdy kanał *downstream* w ramach jednego *upconwertera* musi posiadać swoją unikalną częstotliwość, ale nie jest wymagane, aby kanały sąsiadowały ze sobą. Tak połączone cztery kanały *downstream* mogą znajdować się na przestrzeni 80 MHz w spectrum sieci kablowej, pozostawiając operatorowi elastyczność konfiguracji.

Korzyści z zastosowania karty 16D:

- wysoka gęstość (nawet 240 kanałów DOCSIS w chassis);
- *channel bonding* zgodny z DOCSIS 3.0;
- pełne wsparcie w pracujących w sieci CMTS'ach ARRIS C4;
- legendarna funkcjonalność CMTS'a C4 *hitless sparring* gwarantująca pełną redundancję.

karta kablowa 12U

Karta ARRIS C4 CMTS 12U *Cable Access Module* (CAM) posiada dwanaście (12) cyfrowych odbiorników kanału *upstream*. ARRIS C4 wspiera do szesnastu takich kart w jednej obudowie. C4 wyposażony w karty 12U otrzymał kwalifikację DOCSIS 3.0 Bronze. Co ważne – karta 12U różni się od znanej karty 2D12U jedynie oprogramowaniem. Każda obecnie pracująca w sieci karta 2D12U może być zamieniona na 12U poprzez prosty *upgrade* oprogramowania.

Korzyści z zastosowania kart 12U:

- wysoka gęstość;
- elastyczne mapowanie portów *upstream* i *downstream*;
- zgodność ze specyfikacją DOCSIS 3.0.

moduł RCM

Moduł C4® CMTS *Router Control Module* (RCM) odpowiada za routing pakietów oraz wsparcie dla usług DOCSIS 3.0 w kontrolerze ARRIS C4. Moduł posiada dedykowane układy FPGA dla wsparcia protokołu IPv6, dziesięć (10) portów typu Gigabit Ethernet SFP oraz jeden port 10 Gigabit Ethernet XFP.

Korzyści z zastosowania modułu RCM:

- wysoka gęstość;
- wysoka wydajność dla usług DOCSIS 3.0;
- zgodny sprzętowo z istniejącymi urządzeniami ARRIS C4;
- wsparcie dla legendarnej redundancji *hitless*.

Zalety architektury ARRIS C4 CMTS pozwalają na szybkie i elastyczne wdrożenia DOCSIS 3.0 oraz rozwój istniejących sieci DOCSIS 1.x i 2.0. Firma ARRIS jest bardzo mocno zaangażowana zarówno w inicjatywę M-CMTS, jak i I-CMTS. Od wielu lat produkty i rozwiązania ARRIS były projektowane dla i we współpracy z operatorami kablowymi. Dodatkowo inżynierowie ARRIS'a biorą udział w pracach CableLabs, pomagając definiować i tworzyć kolejne standardy. Żadna inna firma światowa nie jest tak zaangażowana w rozwiązania jedynie dla „świata kablowego".

Więcej informacji o DOCSIS 3.0, jak i o produktach firmy ARRIS, w tym o ARRIS C4, można uzyskać kontaktując się z firmą VECTOR lub na stronie: ***www.vector.com.pl.***

Autor jest Product Managerem w firmie Vector

Chcesz zapisać się na łamach historii branży?

Historia telekomunikacji i komunikacji elektronicznej w Polsce

!

Zabory i Królestwo Polskie 1877 – 1918

Powstanie sieci telefonów warszawskich 1880 – 1883

Pierwsze telefony w Warszawie pojawiły się już w 1877 r., czyli ponad rok od uzyskania patentu przez Aleksandra Grahama Bella. Do Królestwa Polskiego telefony dotarły poprzez Niemcy a o zainteresowaniu wynalazkiem świadczy fakt, iż w tym samym roku rozpoczęto ich produkcję nad Wisłą. Pierwsze oficjalne próby z telefonami przeprowadzono w Królestwie Polskim w dniach 7 i 9 grudnia 1877 r. Do próby transmisji telefonicznej wykorzystano jeden z torów telegraficznych telegrafu Kolei Warszawsko – Wiedeńskiej na odcinku Warszawa – Skierniewice o długości 9 mil. Temat był tak popularny, że o wynikach prób informowała nawet ówczesna prasa prowincjonalna:

„...głos jest wyraźny tylko przy zupełnej ciszy, jaka panowała w czasie prób czynionych o godzinie drugiej w nocy. W innym czasie dźwięki ciche przez telefon przesyłane giną zupełnie, a dźwięki mocniejsze zmącone są innymi odgłosami. Ponieważ dla oszczędności nie zakładano dla telefonu oddzielnych drutów, ale korzystano z telegraficznych, więc podczas prób w dzień robionych telefon sztucznie brzmiał odgłosem pukania telegrafistów na publikich stacyach."

Wyniki pierwszych prób, przeprowadzonych w 1877 r., wykorzystano praktycznie: w Królestwie Polskim od tego momentu budowano oddzielne linie dla potrzeb telegrafu i telefonu. Równolegle z próbami praktycznego wykorzystania łączności telefonicznej na dłuższych dystansach optycy, zajmujący się (jak głosiła XIX wieczna reklama w Królestwie Polskim) handlem przyrządami fizycznemi sprowadzali do kraju telefony oraz organizowali pokazy i próby uliczne w miastach. W Warszawie pierwsze pokazy publiczne zorganizowano w 1878 r. W styczniu linia telefoniczna połączyła aparaty telefoniczne zainstalowane: jeden w cukierni Siemaszkiego w Ogrodzie Saskim, drugi w zakładzie znanego optyka warszawskiego Jakuba Pika przy ul. Nieciałej. Drugą była próba transmisji koncertu muzycznego z Ogrodu Saskiego do gmachu Zarządu Wodociągów przy ul. Dobrej na Powiślu. Pierwsza sieć telefoniczna w Królestwie Polskim powstała w centrum administracyjno-gospodarczym, w Warszawie ale w 1882 r.! Koncesję na budowę tej sieci (i kilku innych na terenie Rosji) uzyskało amerykańskie towarzystwo „The International Bell Telephone Company" w dniu 25 września 1881 r. To właśnie tę datę, datę otrzymania koncesji przez Towarzystwo Bella większość historyków uważa za datę powstania warszawskich telefonów. Obecnie nikogo nie trzeba już przekonywać, że data uzyskania koncesji a data uruchomienia sieci – to dwie różne daty. Zanim uruchomiono łączność telefoniczną – zaistniała potrzeba zapoznania społeczeństwa miasta z zasadą funkcjonowania nowego środka porozumiewania się – 27 maja 1882 r. pisała gazeta:

„Towarzystwo telefonowe umie robić reklamę. Pragnie ono i szerzą publiczność obznajomić szczegółowo z użytkiem telefonu. W tym celu, jak nastarczają, połączy ono dwie najbardziej uczęszczane przez publiczność cukiernie Louvre w Saskim Ogrodzie i w Hotelu Europejskim, telefonowymi drutami. Doświadczenie z tą linią i objaśnienie katalogu, kto zechce poznać bliżej ich konstrukcje, rozpoczyna się z dniem 1 lipca b.r."

Upragnione telefony (był to przecież w owym czasie zwany cywilizacyjny miasta) otrzymali mieszkańcy Warszawy w dniu 13 lipca 1882 r. Wydarzenie zapowiadał artykuł prasowy:

„... w dniu jutrzejszym otwarte będzie czynność telefonów warszawskich. Sto połączeń zastrzeżonych przez ministerstwo w koncesji jest już dokonanych..."

To, co wydaje się nam dziwne w chwili obecnej, w XIX wieku w Królestwie Polskim było normalne. Wszystkie centrale telefoniczne były przekazywane do eksploatacji albo miały być uruchomione 13 stycznia, albo 13 lipca. Wynikało to z faktu obowiązywania w tym czasie w Królestwie Polskim dwóch różnych kalendarzy: juliańskiego i gregoriańskiego . Przekazywanie do eksploatacji central na początku lub w połowie roku związane było z abonamentem, pobieranym za cały rok lub pół roku z góry. Wiele nieporozumień wzbudza pojemność pierwszej centrali telefonicznej

Pierwsza sieć telefoniczna na ziemiach polskich powstała rzeczywiście w 1881 r., na terenie zaboru pruskiego. 12 stycznia 1881 r. przekazano do eksploatacji pierwszą centralę telefoniczną w Berlinie, a do końca roku – jeszcze siedem central telefonicznych w różnych miastach Rzeszy, w tym centralę we Wrocławiu, będącą tą pierwszą na ziemiach polskich.

Wnętrze centrali telefonicznej w Warszawie z 1882 roku

w Warszawie. Autorzy podają różne informacje: od 400 do 800 numerów. W rzeczywistości zainstalowano w 1882 r. tylko 4 łącznice, każda o pojemności 50 numerów . Stąd początkowa pojemność centrali: 200 numerów [abonentów]. W dniu uruchomienia było do niej włączonych 106 abonentów. Jak informowała ówczesna prasa:

„...w roku 1882, tj. pierwszym zaprowadzenia telefonów, było abonentów 163 [na koniec roku – przyp. autora], w roku 1883 cyfra ta podniosła się do 302, w roku 1884 do 416, a na koniec w obiegłym roku liczono 520 abonentów. Ogółem rozmów przeprowadzono w r.z. 651 497, najwięcej z nich było w czerwcu, a najmniej w marcu..."

Kalendarium

- 1881 r. – Warszawa – pierwsze aparaty telefoniczne, początkowo połączone bezpośrednio tj. „aparat - linia - aparat";
- 1882 r. – zostają uruchomione tę czasu centrale telefoniczne w Warszawie i w Łodzi; W Warszawie – pierwsza miejscowa sieć (200 NN) i początkowo cztery 50 NN telefoniczne centrale ręczne, typu „MB" (wywołanie – korbką prądnicy „indukiora" oraz zasilanie mikrofonu z apanatowego ogniwa baterylki);
- 1883 r. – w Warszawie, zainstalowano dużą centralę ręczną – „MB" 800 NN i dalej kolejno rozbudowano ją do 2000 NN (1900 r.).

Linie telefoniczne na budynku Głównej Stacji Telefonów w Warszawie w 1882 roku

Fragment opracowywanego przez wydawnictwo MSG Media wydania „Historia telekomunikacji i komunikacji elektronicznej w Polsce".

zostań partnerem wydania lub wykup reklamę w jedynym takim opracowaniu w Polsce!

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

Europejczycy tracą rocznie 39 dni roboczych na dojazdy do pracy

Grzegorz Kantowicz

ICT a wydajność w pracy

Najnowsze wyniki badań przeprowadzonych przez niezależną agencję badawczo-doradczą Dynamic Markets na zlecenie firmy Avaya pokazują, że dzięki elastycznym formom zatrudnienia pracownicy w Europie i Rosji mogą zaoszczędzić ponad godzinę dziennie, jeśli wyeliminują czasochłonne dojazdy do pracy.

Badania wykazały także, że zwiększa się konkurencyjność firm korzystających z tej formy zatrudnienia, ponieważ poprawie ulega produktywność oraz samopoczucie pracowników, którzy mogą lepiej pogodzić wymagania związane z życiem osobistym i pracą zawodową.

- 96 proc. pracowników korzystających z elastycznych form zatrudnienia ma więcej czasu, ponieważ nie muszą dojeżdżać do miejsca pracy.
- Wyeliminowanie dojazdów pozwala zaoszczędzić średnio 70 minut dziennie – dzięki elastycznym formom zatrudnienia każdy pracownik może w ciągu roku oszczędzić 39 dni roboczych*.
- 21 procent pracowników wykonuje w czasie oszczędzonym na dojazdach dodatkową pracę, a 56 proc. spędza ten czas z rodziną.
- Aktualnie tylko co dziesiąty pracownik nie musi dojeżdżać do miejsca pracy.

Powyższe wnioski zostały zawarte w raporcie „Flexible Working 2009” („Elastyczna praca 2009”), który odzwierciedla opinie ponad 3500 pracowników z Francji, Hiszpanii, Niemiec, Rosji, Włoch i Wielkiej Brytanii.

Czas zaoszczędzony przez wyeliminowanie dojazdów pracownicy na ogół spędzają z rodziną (56 proc.) oraz przeznaczają na odpoczynek (45 proc.) lub spotkania i zadania wykonywane zwykle w czasie pracy (42 proc.). 21 proc. pracowników poświęca zaoszczędzony czas na dodatkową pracę, natomiast jedna czwarta przeznacza go na zajęcia sportowe – odsetek ten wzrasta do 32 proc. w Niemczech i 35 proc. w Hiszpanii. Wyniki sugerują, że elastyczne formy pracy nie tylko ułatwiają pracownikom zachowanie równowagi między pracą a życiem prywatnym i rodzinnym, lecz mogą się także przyczynić do wyeliminowania problemów zdrowotnych spowodowanych brakiem aktywności fizycznej.

Raport zanalizował również rodzaje transportu najczęściej wykorzystywane w dojazdach do pracy wykazując, że nadal najpopularniejszym środkiem lokomocji jest samochód (60 proc.). Potwierdza to zatem tezę, że wprowadzenie na większą skalę elastycznych form zatrudnienia mogłoby radykalnie zmniejszyć liczbę samochodów na drogach.

– Rozwiązania Unified Communication mogą znacznie ułatwić firmom wprowadzanie elastycznych form zatrudnienia pracowników. Raport wykazuje, że takie zatrudnienie jest nie tylko proekologiczne, lecz daje także pracownikom lepszą kontrolę nad wykonywaną pracą. Związana z tą formą zatrudnienia redukcja dojazdów do pracy ma pozytywny wpływ na pracowników i środowisko naturalne. Najbardziej interesujące są jednak skutki finansowe – wzrost produktywności i deklarowany dodatkowy czas poświęcany na pracę przez jedną piątą pracowników mogą mieć istotne znaczenie dla europejskich firm. Ekstrapolacja tego zjawiska w skali gospodarki pozwala postawić tezę, że elastyczna praca może być turbodoładowaniem dla produktywności w całym regionie – powiedział **Jakub Abramczyk**, dyrektor zarządzający firmy Avaya w Polsce.

Inne wnioski z raportu:

- Wśród tych, którzy mają elastyczny czas pracy, prawie jedna piąta (19 proc.) pracuje w ten sposób pięć dni w tygodniu, a 16 proc. „w miarę potrzeby”.
- Elastyczne formy zatrudnienia obejmują więcej pracowników zatrudnionych w niepełnym wymiarze godzin niż pełnoetatowych (odpowiednio 75 proc. i 64 proc.).
- W ten sposób pracuje dodatkowo 90 proc. emerytów.
- Aktualnie 27 proc. pracowników chętnie dojeżdża do pracy, jeżeli mają taką możliwość.

W celach związanych z opisanymi badaniami elastyczne formy zatrudnienia zdefiniowano jako sytuację, w której pracownicy nie muszą przebywać w biurach firmy w wyznaczonych godzinach, ale sami wyznaczają sobie elastyczne godziny pracy i miejsce jej wykonywania. ■

** Przyjmując średnio w Europie 232 dni robocze w roku oraz przy założeniu, że dzień roboczy ma siedem godzin.*

NetPoint – Emblaze-VCON

Grzegorz Kantowicz

Wideokonferencje przez firewall

Nowe rozwiązanie Emblaze-VCON o nazwie NetPoint pozwala wyeliminować problemy związane z transmisją przez firewall i routery NAT podczas wideokonferencji.

NetPoint umożliwia połączenia pomiędzy dowolnymi terminalami lub programami wideokonferencyjnymi, które są zgodne ze standardami H.323 (wykorzystującymi publiczny numer IP).

Połączenia te mogą być bezproblemowo realizowane zarówno w sieciach LAN/WAN, jak i w internecie, bez względu na obecność po drodze firewalli czy NAT. NetPoint – za sprawą wykorzystywanego protokołu H.460 i swojego usytuowania w sieci publicznej – pełni rolę pośrednika w realizacji połączeń wideokonferencyjnych. Przejmuje połączenia wychodzące za firewalla i sprawia, że docelowy terminal wideokonferencyjny usytuowany za firewallem także nawiązuje połączenie z NetPointem. Po otrzymaniu obu sygnałów NetPoint je scala i umożliwia w ten sposób przeprowadzenie wideokonferencji.

Architektura rozwiązania NetPoint

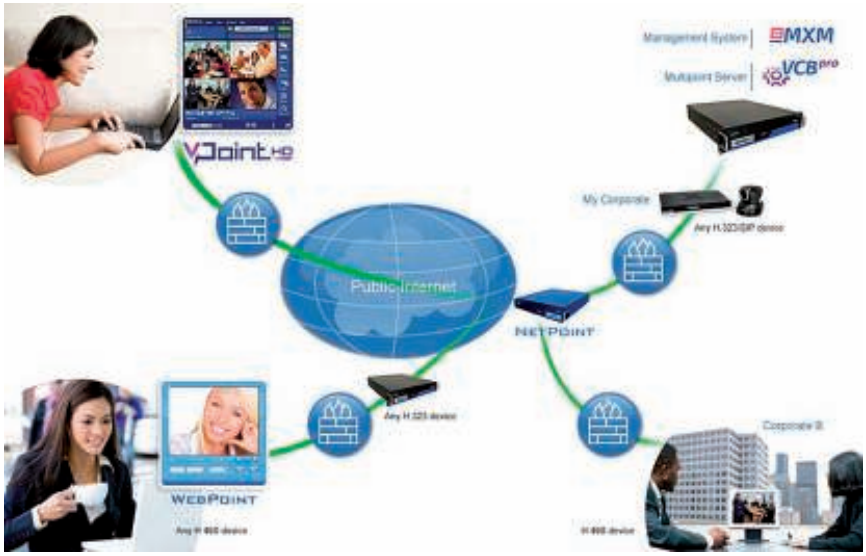
– Nowe rozwiązanie Emblaze-VCON jest przydatne dla tych organizacji, które wykorzystują programy lub terminale wideokonferencyjne zgodne ze standardem H.323.

W obrębie swojej sieci wewnętrznej lub pomiędzy oddziałami w ramach sieci VPN organizacje te mogą z reguły swobodnie prowadzić wideokonferencje, jednak w przypadku potrzeby nawiązania jakiegokolwiek połączenia wideo z osobą spoza sieci korporacyjnej pojawiają się problemy. Ich rozwiązanie najczęściej wiąże się z koniecznością zaangażowania administratora IT, który musi otworzyć dodatkowe porty na potrzeby tego jednego konkretnego połączenia wideokonferencyjnego, co z kolei naraża firmę na potencjalne ataki przez niezabezpieczoną sieć.

NetPoint eliminuje wszystkie te aktywności i zagrożenia, umożliwiając bezproblemowe i bezpieczne połączenia wideo z dowolną osobą spoza firmy – wyjaśnia **Dariusz Latecki**, prezes zarządu VCC Systems.

Ważną cechą NetPointa jest fakt, że może on współpracować zarówno z terminalami i oprogramowaniem wideokonferencyjnym od Emblaze-VCON, jak i od dowolnych innych producentów, którzy wspierają protokół H.460.

Godne uwagi jest także to, że NetPoint potrafi jednocześnie obsłużyć 75 połączeń wideokonferencyjnych, które są szyfrowane zgodnie ze standardem H.235. Urządzeniem można zarządzać w sposób zdalny – za pośrednictwem panelu administracyjnego, który jest dostępny przez internet. ■



Molex wprowadza rozwiązania do zaawansowanego zarządzania cyklem życia warstwy fizycznej sieci

Molex Premise Networks udostępnia, jako efekt globalnej restrukturyzacji oraz znaczących inwestycji, Zaawansowany System Zarządzania Cyklem Życia Warstwy Fizycznej Sieci (APLLM – Advanced Physical Layer Lifecycle Management) – przełomowy, nowy pakiet rozwiązań, dzięki którym przedsiębiorstwa mogą zarządzać warstwą fizyczną i infrastrukturą na niezrównanym w skali całej branży okablowania strukturalnego poziomie widoczności i integracji.

Rozwiązanie APLLM, obejmujące produkty z dziedziny oprogramowania, elektroniki i tradycyjnych rozwiązań do transmisji danych, umożliwia śledzenie inwestycji od planowania przez projekt, zakup, instalację, przeniesienia, rozbudowy i zmiany (MAC), aż po ewentualną modernizację infrastruktury i połączonych z nią zasobów, obejmując tym samym jej cały cykl życia.

Firmy muszą osiągać więcej mniejszymi środkami – Molex Premise Networks może w tym pomóc.

APLLM składa się z trzech zasadniczych grup produktów: INSIGHT, MIIM i tradycyjnych produktów do transmisji danych. Każdy z tych elementów wdrożony osobno zaspokaja określoną potrzebę związaną z infrastrukturą, ale zintegrowane, wdrożone w całości rozwiązanie APLLM zapewnia przedsiębiorstwom niespotykane dotychczas funkcje i zalety.

Wprowadzamy zarządzanie cyklem życia infrastruktury do przedsiębiorstw na całym świecie.

Dzięki swoim przełomowym technologiom Molex Premise Networks pokonuje dotychczasowe bariery i jako lider branży zapewnia niespotykany wcześniej wzrost efektywności, udoskonalenie procesów oraz stopniowy wzrost wartości. Skala tych korzyści dla zainteresowanych stron w procesach wdrażania i zarządzania infrastrukturą była wcześniej niewyobrażalna. Nie ulega wątpliwości, że nasz dorobek i doświadczenie w dziedzinie okablowania strukturalnego daje firmie Molex Premise Networks wyjątkowe możliwości, by podnieść poprzeczkę i zaoferować przedsiębiorstwom na całym świecie udoskonalenia wynikające z zaawansowanej współpracy, widoczności i kontroli nad warstwą fizyczną.

INSIGHT (*Infrastructure Lifecycle Management*):

INSIGHT to system zarządzania informacjami online do planowania, wdrażania i zarządzania infrastrukturą oraz połączonymi zasobami. Składający się z 3 podstawowych modułów – Project Control, Connectivity Management i MAC Management – system INSIGHT zwiększa widoczność, kontrolę, automatyzację i współpracę w zarządzaniu dowolną infrastrukturą na potrzeby określonych zainteresowanych stron. Wśród podstawowych funkcji można wymienić biblioteki najlepszych praktyk, dostosowane schematy organizacji pracy, uprawnienia i grupowanie wielu użytkowników, a także dostęp w czasie rzeczywistym do informacji z dowolnego miejsca na świecie. Wszystko to sprawia, że system ten jest efektywny i unikatowy.

MIIM™ (*Advanced Physical Layer Management*)

MIIM to wszechstronne rozwiązanie do zaawansowanego zarządzania warstwą fizyczną, skoncentrowane na udoskonalonym zarządzaniu siecią, bezpieczeństwie sieci, administrowaniu zasobami, zwiększonej wydajności i widoczności.

Oprócz zarządzania pracami MAC i zleceniami pracy MIIM nieustannie monitoruje i odwzorowuje warstwę fizyczną. Między innymi śledzi ciągłość okablowania od pomieszczenia telekomunikacyjnego do gniazd abonenckich, wykrywa wpięcia i wypięcia urządzeń w sieci, porównuje stan powykonawczy elementów sieci z zamierzeniami projektowymi, a także umożliwia realizację zleceń pracy, ułatwiając technikom orientację w połączeniach krosowych. Głównym czynnikiem wyróżniającym MIIM jest zdolność do monitorowania stanu kanału fizycznego nie tylko w szafie, ale aż po oddalone obszary robocze.

Tradycyjne produkty do transmisji danych

Molex Premise Networks nie zmienia swojego strategicznego podejścia do tego zestawu produktów. Transmisja danych pozostaje podstawową kompetencją, a firma nieustannie opracowuje nowe produkty i dba o ich jakość, podczas gdy zarówno MIIM, jak i INSIGHT znacząco ułatwiają zarządzanie nimi. Oferta naszych tradycyjnych produktów do transmisji danych współdziała harmonijnie z rozwiązaniami INSIGHT i MIIM.

molex
one company > a world of innovation

Eastern Europe Headquarters
Molex Premise Networks Sp. z o.o.
ul. Okrzei 1a; 03-715 Warszawa
Polska
tel. +48 22 333 81 50, faks +48 22 333 81 51

Zakład Produkcyjny w Polsce
Molex Premise Networks Sp. z o.o.
ul. Tczewska 2
Rokitki; 83-112 Lubiszewo
tel. +48 58 530 62 00, faks +48 58 530 62 01

www.molexpn.com.pl

1st International Conference on Image Processing & Communications
September 16-18, 2009 - Bydgoszcz, Poland

BYDGOSZCZ

IP&C

Call for papers

IP&C – First International Conference on Image Processing & Communications September 16–18, 2009 – Bydgoszcz, Poland

http://ipc2009.utp.edu.pl

General Chair:

Ryszard Tadeusiewicz (Poland)

Local Chairs:

Ryszard S. Choraś (Poland)
Antoni Zabludowski (Poland)

Program Committee:

Kevin W. Bowyer (USA)
Dumitru Dan Burdescu (Romania)
Christophe Charrier (France)
Leszek Chmielewski (Poland)
Adam Dąbrowski (Poland)
Andrzej Dąbrowski (Poland)
Andrzej Dobrogowski (Poland)
Marek Domański (Poland)
Kalman Fazekas (Hungary)
Ewa Grabska (Poland)
Andrzej Kasprzak (Poland)
Andrzej Kasiński (Poland)
Marek Kurzyński (Poland)
Witold Malina (Poland)
Andrzej Materka (Poland)
Wojciech Mokrzycki (Poland)
Zbigniew Papir (Poland)
Jens M. Pedersen (Denmark)
Jerzy Pejaś (Poland)
Leszek Rutkowski (Poland)
Khalid Saeed (Poland)
Konrad Wojciechowski (Poland)

Organizing Committee:

Tomasz Andrysiak
Michał Choraś
Bożydar Dubalski - Publication Chair
Adam Marchewka
Beata Marciniak
Tomasz Marciniak- Publication Chair
Łukasz Saganowski
Karolina Skowron - Conference Secretary
Mścisław Śrutek

Media patronage: INFOTEL

International Conference on Image Processing & Communications will be organized by Institute of Telecommunications, University of Technology and Life Sciences in Bydgoszcz, Poland from 16 to 18 September 2009. The conference aims to bring together the researchers working on fields image processing and communications. This Conference will be an important event and will provide us with a unique opportunity for disseminating the latest advances, applications and future trends in the field of Image processing and Communications.
There are 3 main tracks of the conference. We are inviting original, unpublished research manuscripts describing the results of theoretical, empirical and practical development experiences in the following technical areas (but not limited to):

Computer Vision	*Image Analysis*	*Communications*
Object Recognition	Image Compression	Next Generation Networks
Machine Vision	Medical Image Processing	Optical Backbone and Access Networks
Biometrics	Character and Document Analysis	Network Reliability
Intelligent Interfaces	Image Retrieval	New Services in IP Networks
Image Motion Analysis	Image Processing Applications	QoS in IP Networks
		Regular Structures of Communications Networks

Submission of Papers: Prospective participants are invited to electronically submit full papers of their work in English (max. 8 pages in LaTeX format), following the instructions available on the website. Each paper will be judged by at least two referees. Accepted papers will be included in the book published by AOW EXIT.
Selected best papers will be invited for further revisions and extensions for possible publications by journals (e.g.. IP&C).

15 March 2009: Early Registration
15 March 2009: Deadline for submission of proposals for Special Sessions
15 May 2009: Deadline for submission of full-length papers for Regular Sessions and Special Sessions.
20 June 2009: Acceptance/Rejection notification for regular papers and special session papers.
20 July 2009: Final camera-ready papers due in electronic form.

Organized by
Institute of Telecommunications,
University of Technology and Life Sciences in Bydgoszcz,

In cooperation

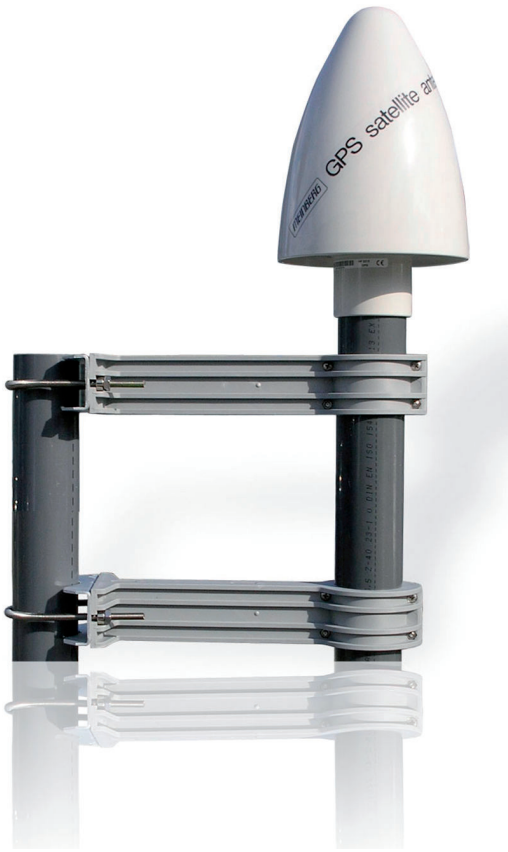
IEEE IPPT PAN

Conference Secretary:
tel. +48 52 340 83 28 mail: ipc2009@utp.edu.pl http://ipc2009.utp.edu.pl

dr Piotr Frączyk

Dystrybucja czasu w epoce globalnych technologii

W życiu prywatnym i publicznym, w obrocie prawnym i gospodarczym, przy nadzorze procesów przemysłowych niezbędna jest znajomość momentów zdarzeń. We współczesnym świecie wymagane jest by ta sama skala czasu obowiązywała na obszarze całego globu i w otaczającej przestrzeni kosmicznej. Wymagany zakres dokładności rozciąga się od doby po miliardową część sekundy. Istotna jest nie tylko dokładność datowania, równie ważne są pewność i niezawodność.



Źródła czasu

Pierwotnym wzorcem czasu jest międzynarodowa skala czasu atomowego TAI. Podstawą skal czasu używanych publicznie jest czas UTC, różniący się od TAI o całkowitą liczbę sekund dodawaną w celu zapewnienia zgodności z czasem słonecznym. W Polsce czas urzędowy, to czas środkowoeuropejski CET lub czas letni środkowoeuropejski CEST różniące się od UTC odpowiednio o 1 i 2 godziny.

Metody dystrybucji czasu

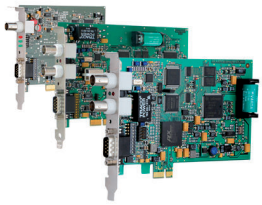
Podstawowym i powszechnym w skali globalnej środkiem dystrybucji czasu jest Globalny System Lokalizacyjny GPS. Lokalnie dostępne są sygnały radiowych nadajników sygnału czasu na falach długich na przykład DCF77. Powszechne staje się korzystanie z publicznych serwerów NTP dystrybuujących czas UTC w sieciach komputerowych. Serwery NTP Głównego Urzędu Miar są praktycznie jedynym dostępnym publicznie źródłem czasu UTC(PL) stanowiącego podstawę czasu urzędowego w Polsce. Inne metody dystrybucji czasu nie posiadają obecnie większego znaczenia w zautomatyzowanych systemach publicznych.

Protokół NTP

Do dystrybucji czasu w sieciach komputerowych powszechnie stosuje się protokół NTP (*Network Time Protocol*). Zawiera on mechanizmy zapewniające wysoką niezawodność oraz odporność na zmienne opóźnienia w przesyłaniu pakietów. Standardy NTP opisują między innymi: hierarchiczną architekturę struktury dystrybucji czasu, protokoły transmisji stempli czasowych, algorytmy synchronizacji, algorytmy szyfrowania transmisji. Dokładność NTP ograniczana jest głównie na etapie transmisji pakietów i zwykle nie jest lepsza od kilku tysięcznych części sekundy. Siła NTP tkwi w dostępności i pewności datowania jaką zapewniają serwery współpracujące w rozproszonym zespole zgodnie z regułami NTP.

Serwery NTP

Czas dystrybuowany przy pomocy protokołu NTP dostarczany jest przez serwery NTP. W przypadku potrzeb małej wagi serwer NTP może być uruchomiony na jednym z komputerów pracujących w lokalnej sieci. Bardziej niezawodnym rozwiązaniem jest zastosowanie sprzętowego serwera NTP. Jeśli bierze się pod uwagę całkowity koszt usługi dostarczania czasu, uwzględniający utrzymanie wysokiej dostępności, dwa serwery NTP często są tańszym rozwiązaniem niż jeden. Zastosowanie dwóch serwerów w miejsce jednego zmniejsza koszty związane z zapewnieniem wysokiej dostępności serwisu i zwiększa średni czas pomiędzy awariami usługi z 6,5 roku do 600



lat (dane dla serwerów serii LANTIME przy założeniu średniego czasu naprawy MTTR wynoszącego 2 tygodnie, dostępność odpowiednio 0,994 i 0,99993).

Źródła czasu dla serwerów NTP

Zalecanymi, ze względu na niezawodność, źródłami czasu dla serwerów NTP obsługujących lokalne sieci komputerowe są serwery NTP wyższych poziomów i system GPS. Izolację od internetu uzyskać można poprzez stosowanie serwerów NTP wyposażonych w niezależne porty sieciowe lub w przypadku zwiększonych wymagań co do bezpieczeństwa, stosowanie dodatkowego serwera NTP przekazującego czas do serwera obsługującego sieć lokalną za pośrednictwem dedykowanego interfejsu, np. IRIG-B.

Protokół PTP

Z myślą o zastosowaniach przemysłowych, dla potrzeb dystrybucji czasu poprzez sieci komputerowe z dokładnością ułamka milionowych części sekundy, opracowany został protokół PTP (*Precise Time Protocol*). Uzyskanie tak wysokiej dokładności możliwe jest w sieciach o strukturze zaprojektowanej pod kątem dystrybucji czasu, obsługiwanych przez urządzenia sieciowe wspomagające protokół PTP. Rosnące znaczenie transmisji pakietowej w telekomunikacji, związane z wprowadzeniem sieci trzeciej generacji 3G, wymusza opracowanie dokładnych metod dystrybucji czasu w istniejących i nowo powstających sieciach teletransmisyjnych opartych o protokół IP. Metody te są przedmiotem intensywnie opracowywanej normy IEEE 1588 PTP.

O autorze:

Dr Piotr Frączyk posiada ponad trzydziestoletnie doświadczenie w dziedzinie generacji oraz dystrybucji czasu i częstotliwości.
Jest Prezesem Zarządu NAVI sp. z o.o., przedsiębiorstwa dostarczającego najnowsze technologie z tego obszaru.

VDmaster firmy Activis Polska
– kompleksowy system komunikacyjny kosztuje mniej

Opłacalne inwestycje – komunikacja z partnerami biznesowymi na nowo

Obsługa połączeń telekomunikacyjnych to znacząca pozycja w budżecie dla wielu firm. Z uwagi na to, że w każdej firmie realizowane są połączenia pomiędzy oddziałami, kontrahentami i pracownikami mobilnymi, najczęściej korzysta się z kilku kanałów łączności i wielu rodzajów urządzeń. Nierzadko współpraca między nimi jest niemożliwa lub kosztowna. Wdrożenie procedur organizacyjnych zapewniających optymalne wykorzystywanie poszczególnych rodzajów łączności jest równie kosztowne, co uciążliwe dla pracowników.

Activis Polska oferuje **system VDmaster**, pozwalający wspomóc szefów firm w walce z kosztami związanymi z realizacją połączeń telekomunikacyjnych z kontrahentami i w ramach firmy. System VDmaster idzie o krok dalej niż dotychczasowe rozwiązania. Dzięki wykorzystaniu zalet technologii VoIP i zaimplementowanej inteligencji skupia najlepsze i najefektywniejsze znane mechanizmy zarządzania kosztami łączności, wprowadza kilka nowych, dając nową wartość i dodatkowe oszczędności dla posiadacza systemu. Z przeprowadzonych wdrożeń i analiz wynika, że dzięki zastosowaniu systemu VDmaster można zredukować całkowite koszty od 20 proc. do 50 proc. System jest modułowy, a więc dedykowany nie tylko dla firm średnich i dużych, ale pozwala również na kompleksową obsługę małego przedsiębiorstwa. W firmach wielooddziałowych, o stosunkowo dużym ruchu telekomunikacyjnym, średni czas zwrotu z inwestycji nie przekracza 10-12 miesięcy.

System VDmaster składa się z mechanizmów sprzętowych i programowych, umożliwiających integrowanie i optymalizowanie sieci komunikacyjnych (TDM, IP i GSM) w ramach spójnego, jednolitego, zarządzalnego i skalowalnego układu. Wdrożenie systemu daje w efekcie strukturę prywatnej rozproszonej sieci komunikacyjnej z zaimplementowanym wielopoziomowym systemem wyboru drogi o najniższym koszcie LCR (*Least Cost Route*), współpracującej z sieciami tradycyjnymi, IP i GSM.

Podstawowa zaleta systemu VDmaster

Podstawową zaletą systemu VDmaster jest optymalizowanie wykorzystania własnych i zewnętrznych (czyli udostępnianych przez operatorów) zasobów sieciowych poprzez wybór drogi o najniższym koszcie i wykorzystywanie możliwości realizacji połączeń z użyciem dróg alternatywnych. Moduły sprzętowe systemu pozwalają na wykorzystanie wszystkich dostępnych w danej lokalizacji rodzajów łączy ze szczególnym uwzględnieniem komunikacji VoIP jako obecnie najbardziej efektywnej możliwości.

Na czym polega optymalizowanie kosztów?

Optymalizację kosztów można podzielić na dwie podstawowe grupy. Pierwsza z nich to wstępne koszty implementacji systemu, a druga to bezpośrednie koszty późniejszych połączeń.

Koszty implementacji systemu:

- dzięki globalnemu podejściu koszty zaimplementowania systemu są zoptymalizowane;
- w ramach implementacji systemu wykorzystuje się istniejącą infrastrukturę, rozbudowując ją ewentualnie o konieczne elementy;
- system jest systemem otwartym i dalsza rozbudowa lub rekonfiguracja może się odbywać w dowolnym kierunku przy wykorzystaniu istniejących elementów i minimalnych nakładów.

Na optymalizowanie kosztów połączeń mają wpływ następujące funkcje systemu:

- wykorzystanie sieci IP i transmisji VoIP bazującej na własnych zasobach klienta;
- planowe wykorzystanie wyjść do sieci GSM i używanie kanałów w zależności od zastosowanego dla nich abonamentu i operatora (system kieruje tak połączeniami, aby równomiernie wykorzystać wykupione abonamenty i optymalnie kierować połączenia w zależności od wybranego numeru komórkowego);
- w przypadku wolnych, niewykorzystanych minut w ramach abonamentów GSM wykorzystywanie

tej sieci do połączeń na przykład z numerami stacjonarnymi;

- możliwość wykorzystania darmowych połączeń w ramach firmowej sieci IP i lokalnych połączeń w jednostkach zamiejscowych do realizacji połączeń poza własną strefę numeracyjną – na przykład w oddziałach zagranicznych.

Korzyści dla klienta

Wdrożenie systemu VDmaster niesie określone korzyści dla klienta, które w sposób zagregowany przedstawiono poniżej:

- system na podstawie wiedzy o strukturze sieci sam wybiera optymalną drogę połączenia;
- zmniejszenie kosztów w oddziałach – nawet o kilkadziesiąt procent;
- bardzo znaczące zmniejszenie kosztów w ramach całej firmy;
- pełna informacja o ruchu w ramach sieci i możliwości analizy jego rozkładu w ramach grup numerów, oddziałów, wykorzystania sieci IP, TDM i GSM;
- pełniejsze wykorzystanie infrastruktury i możliwość jej optymalizacji (na przykład redukcja nadmiarów);
- łatwa, szybka i tania rozbudowa infrastruktury w ramach jednostek poprzez wykorzystanie sieci LAN i telefonów IP;
- możliwość skojarzenia numeru z konkretnym aparatem (na przykład telefon IP, bramka VoIP, telefon bezprzewodowy) i migracja numeru z użytkownikiem – mobilny użytkownik loguje się w ramach tej sieci LAN, w której zasięgu aktualnie przebywa (na przykład w innym oddziale firmy);
- możliwości przekierowania i przerzucania połączeń w ramach sieci nawet do osób i oddziałów w innych miastach;
- możliwość obsługi telefonów IP znajdujących się poza siedzibą firmy – *home working*, bez dodatkowych kosztów ponoszonych na opłaty dla operatorów zewnętrznych;
- zaimplementowanie systemu nie powoduje konieczności zmian w stosowanych systemach wybierania, czyli nie wymusza zmiany przyzwyczajeń, informowania o zmianach kontrahentów i klientów;
- system umożliwia uruchomienie wielu funkcji trudno dostępnych w tradycyjnie budowanej sieci, przykładowe to: ujednolicenie numeracji, powiązanie z aplikacjami komputerowymi, centralne zarządzanie.

Bezpieczeństwo

Duże znaczenie dla klientów ma element bezpieczeństwa i hermetyzacji własnych sieci LAN. Te uwarunkowania zostały uwzględnione przy tworzeniu systemu i w związku z tym system VDmaster posiada następujące cechy:

- elementy systemu znajdują się pod ochroną firewalla klienta i są tak samo zabezpieczone, jak inne elementy sieci komputerowej klienta

- struktura rozproszona zabezpiecza system przed zakłóceniami w pracy w przypadku przeciążenia lub awarii;
- urządzenia użytkowników mobilnych, zmieniających lokalizację, logują się do serwera systemu same i mogą być ulokowane w sieci, w której w danej chwili się znajdują, zwykle bez konieczności dodatkowych uzgodnień z administratorem tej sieci.

Analizując kompleksowe koszty komunikacji nie można zapominać o kosztach połączeń przychodzących. W tradycyjnym podejściu te koszty są ponoszone przez kontrahentów i w zasadzie nie są uwzględniane. Jednak z punktu widzenia rynkowej oceny firmy, koszt i dostępność kontaktu (zwłaszcza jeżeli są to kontakty wielokrotne) stanowi istotny aspekt jej oceny. Stosuje się więc często rozwiązania zapewniające stałym i potencjalnym klientom bezpłatny kontakt (infolinie płatne przez firmę, numery 0800 itp). W tej sferze VDmaster ma znaczącą przewagę nad innymi systemami, ponieważ pozwala na łatwą integrację z usługą VoiceLink – systemem połączeń zestawianych bezpośrednio ze stron internetowych, bezpłatnych dla dzwoniącego. Usługa VoiceLink została wprowadzona na rynek przez Activis Polska w 2009 roku jako niezależny produkt, a jej zastosowanie w powiązaniu z systemem VDmaster pozwala w ramach jednej struktury komunikacyjnej zapewnić obsługę bezpłatnej łączności przychodzącej.

W zależności od potrzeb i możliwości inwestycyjnych Activis Polska oferuje realizację systemu VDmaster w formie najdogodniejszej dla klienta. System można budować od razu jako całość lub – co bywa ekonomicznie uzasadnione – etapowo. Każde wdrożenie wiąże się w pierwszej kolejności z przeprowadzeniem szczegółowego audytu istniejącej struktury oraz ponoszonych kosztów oraz wykonaniem projektu sieci docelowej. Na tej podstawie można już określić koszt całej inwestycji i prognozowane koszty eksploatacji. Zarządzanie systemem oraz jego konfigurowanie może być prowadzone samodzielnie przez klienta (po odpowiednim przeszkoleniu) lub realizowane przez Activis w oparciu o umowę serwisową. Oprogramowanie do zarządzania systemem może znajdować się na sprzęcie klienta w jego sieci LAN, poza siecią klienta – dostępnych poprzez bezpieczny kanał komunikacyjny, lub na zasadach dzierżawy aplikacji serwera w modelu ASP.

W celu uzyskania dodatkowych informacji prosimy o bezpośredni kontakt z przedstawicielami firmy.

Activis Polska Sp. z o.o.
60-321 Poznań, ul. Świerzawska 5,
tel. 061 44 82 00
www.activis.pl; www.vdmaster.pl
biuro@activis.pl

Interfejs 100 gigabitów do ruterów Juniper Networks

Grzegorz Kantowicz

Przełomowy interfejs ethernetowy

Pierwszy na rynku interfejs ruterowy 100 GE zapewni nowe możliwości skalowania sieci niezbędne do obsługi wirtualizacji i przetwarzania w chmurze.

Firma Juniper Networks wprowadza na rynek pierwszą dotąd kartę ethernetowego interfejsu ruterowego o przepływności 100 gigabitów (100 GE), która będzie dostarczana z ruterami szkieletowymi T1600. Ze względu na gwałtownie wzrastający ruch – wideo, zaawansowane usługi bezprzewodowe oraz pojawiające się nowe rozwiązania, takie jak przetwarzanie w chmurze – sieci szkieletowe wkrótce będą musiały być rozbudowywane do nowych przepustowości, a interfejsy 100 GE umożliwią w tym zakresie skok o rząd wielkości w porównaniu do większości interfejsów dostępnych obecnie na rynku.

Wprowadzając jako pierwsza interfejs 100 GE w ruterach szkieletowych firma zapewni długofalową ochronę inwestycji oraz skalowalność i elastyczność niezbędną do świadczenia usług wymagających wielkich przepustowości, takich jak *Long Term Evolution* (LTE) i wideo. Dzięki znaczącemu wzrostowi pojemności łączy, karta interfejsu 100 GE umożliwi dostawcom usług i centrom przetwarzania danych zmniejszenie liczby interfejsów niezbędnych w ich sieciach, co zaowocuje znaczącymi oszczędnościami płynącymi z uproszczenia topologii i większej sprawności eksploatacyjnej – dzięki czemu przyczyni się do spadku całkowitego kosztu posiadania systemów.

– *Firma Verizon zamierza komercyjnie wdrożyć 100 G w 2010 roku* – powiedział **Glenn Wellbrock**, dyrektor działu projektowania i architektury optycznych sieci transportowych w Verizon. – *Próby przeprowadzone dotychczas w naszej sieci były nastawione na zweryfikowanie, czy używane przez nas optyczne systemy transmisyjne są gotowe do przepustowości 100 G. Dotąd zdecydowanie nam brakowało interfejsu 100 G do klienckiej strony rutera szkieletowego, dlatego napawa nas nadzieją zapowiedź wprowadzenia przez Junipera interfejsów 100 GE do jego ruterów T1600. Biorąc pod uwagę rozwój naszych usług FiOS, bezprzewodowych i IP, 100 G jest warunkiem krytycznym sprawnej i prostej*

skalowalności sieci szkieletowej. Dodając interfejsy 100 GE do ruterów T1600 Juniper zapewnia możliwość wykorzystania posiadanych już zasobów przy rozbudowie szkieletu, co zapewni największą sprawność operacyjną.

Wprowadzane dziś na rynek interfejsy 100 GE wykorzystują i dalej będą rozwijały szereg przełomowych nowatorskich rozwiązań sieci szkieletowych wprowadzonych przez firmę Juniper w ciągu ostatnich kilku lat, w tym:

- **Ruter szkieletowy T1600:** wprowadzony na rynek w 2007 roku T1600 pozostaje jak dotąd największej pojemności szkieletowym ruterem jednokasetowym, najbardziej energooszczędnym ruterem szkieletowym i jedynym ruterem szkieletowym o przepływności 100 gigabitów/sekundę na gniazdo;
- **Juniper Control System (JCS) 1200:** pierwsza na rynku – i wciąż jedyna – wysoko wydajna skalowalna płaszczyzna sterująca, od której zaczął się rozdział pomiędzy zasobami sterującymi i przekazującymi ruch oraz sprzętowa wirtualizacja ruterów serii T;
- **TX Matrix Plus:** system pozwalający na sprzęganie wielu ruterów T1600 pod kontrolą JCS 1200, by tworzyć wysoce skalowalne uniwersalne rutery wirtualizowane sprzętowo.

Dzięki tym innowacjom 100 GE pomoże dostawcom usług przewodowych i bezprzewodowych, twórcom chmur obliczeniowych i centrów przetwarzania danych w pełnej realizacji możliwości wirtualizacji w zakresie konsolidacji zasobów informatycznych, zwiększania ich sprawności i obniżania kosztów. Juniper jest jedyną firmą, która zapowiedziała tak niepowtarzalną kombinację wysoce skalowalnych sprawnych ruterów szkieletowych, wirtualizacji na wielką skalę i interfejsów 100 GE – dlatego też znajduje się na unikatowej pozycji, pozwalającej jej pomagać klientom w świadczeniu przez nich usług następnej generacji, takich jak LTE, oprogramowanie dzierżawione (SaaS) i sieć dzierżawiona (NaaS).

– *Sieci zmieniają się od czasów, gdy szybkie łącza można było znaleźć wyłącznie w zasadniczym szkielecie sieci – teraz takie łącza są potrzebne aż do punktów brzegowych. Kończą się czasy, gdy wzrost przepustowości pozwalał tylko na obsługę większego ruchu, a zaczynają czasy niezbędności przepustowości do tworzenia infrastruktury zapewniającej wysoki poziom obsługi (QoS) konieczny do wirtualizacji aplikacji, serwerów i treści* – powiedział **Tom Nolle**, prezes i dyrektor generalny CIMI Corporation. – *Juniper wprowadza 100 GE i tę przepustowość oferuje obudowaną szeroką gamą narzędzi wspomagających zastosowania i rozwiązania sieciowe, dzięki którym 100 gigabitów stanie się powszechne. Wprawdzie ogłaszają wprowadzenie interfejsu 100 G, ale tak naprawdę zrealizują cały ekosystem 100 G.*

Dzięki wymienionym wcześniej innowacjom, ale nie tylko, seria T stała się najpowszechniej stosowaną w branży rodziną ruterów szkieletowych. Juniper dostarczył ich 5000 sztuk ponad 220 klientom na całym świecie – w tym 500 sztuk T1600 w ciągu nieco ponad roku ich dostępności. Według firmy Synergy Research, w ciągu ostatnich pięciu lat udział Junipera w rynku ruterów szkieletowych wzrósł o 44 procent – zwiększył udział o 11 punktów, podczas gdy inne firmy odnotowały spadek udziałów[1].

Wszystkie te platformy pracują pod kontrolą Oprogramowania JUNOS®, systemu operacyjnego o jednej wersji kodu źródłowego, który integruje usługi rutowania, przełączania i ochrony sieci. Umożliwiając klientom i partnerom opracowywanie aplikacji pod oprogramowanie JUNOS w ramach programu Platformy Opracowywania Rozwiązań przez Partnerów (za dodatkowymi opłatami), Juniper umożliwia klientom skalowanie płaszczyzny usług w zakresie usług niepowtarzalnych i specjalizowanych. Klienci i partnerzy mogą wykorzystywać Platformę do tworzenia i zapewniania nowych usług o wartości dodanej, zwiększających sprawność i rentowność ich działalności.

– *100 GE było nie do uniknięcia, kwestią było tylko, kiedy się pojawi. Nowe kierunki, takie jak przetwarzanie w chmurze, konsolidacja i wirtualizacja centrów przetwarzania danych, bardziej i pilniej wymuszają stosowanie 100 GE* – powiedział **Opher Kahane**, wiceprezes i dyrektor generalny działu High-End Systems Business w Juniper Networks. ■

1 Według Synergy Research, udział Junipera w rynku ruterów szkieletowych wynosił w I kw. 2004 roku 25 proc., zaś w I kw. 2009 roku – 36 proc.

Wakacje z internetem

Christian Funk

Bezprzewodowe lato

Nareszcie wakacje! Spakowałeś wszystko, czego potrzebujesz i oczywiście nie zapomniałeś o swoim laptopie. Komputer z pewnością się przyda – przecież chcesz mieć możliwość organizowania i archiwizowania swoich zdjęć, a możliwość bycia na bieżąco z informacjami oraz pocztą elektroniczną także jest kusząca. Hotele coraz częściej oferują dostęp do internetu, więc nie stracisz kontaktu ze światem.

W hotelu uruchamiasz komputer, włączasz bezprzewodowy dostęp do internetu i szukasz sieci Wi-Fi. Laptop wykrywa kilka punktów dostępowych o różnych nazwach (*SSID – Service Set Identifier*), jednak wybierasz ten nazwany tak samo jak Twój hotel. Po nawiązaniu połączenia najczęściej pojawia się strona z wyborem metody płatności za połączenie internetowe. I tutaj czeka Cię pierwsza niespodzianka – cena zazwyczaj jest astronomiczna. Niektóre hotele żądają nawet 100 zł za 24 godziny dostępu do internetu. Tyle samo, ile w domu płacisz miesięcznie za bardzo szybkie połączenie. Jednak teraz jesteś na wakacjach i nie masz innego wyjścia... a może masz? Na liście wykrytych sieci bezprzewodowych jedna wydaje się wyjątkowo kusząca. Chwali się wysoką prędkością i bardzo niską, w porównaniu z siecią hotelową, ceną – około 20 zł za jeden dzień. Szanujesz swoje pieniądze, więc łączysz się z tańszą siecią, wybierasz kartę kredytową jako formę płatności i wprowadzasz wszystkie żądane informacje, ciesząc się, że zaoszczędziłeś trochę pieniędzy.

Już po kilku chwilach cieszysz się dostępem do internetu. Sprawdzasz pocztę, po czym postanawiasz porównać ceny aparatu fotograficznego, który widziałeś wcześniej na wystawie w sklepie. Jak zwykle, porównujesz cenę lokalną z ofertą sklepów internetowych. Okazuje się, że cena lokalna jest znacznie wyższa, więc decydujesz się na zakup w internecie. I ponownie płacisz kartą kredytową, ponieważ jest to bardzo wygodne.

Powyższa sytuacja jest typowa dla większości z nas, przynajmniej w pewnym zakresie. Być może kilka osób uzna, że łączenie się z niepewną siecią bezprzewodową może być niebezpieczne, jednak większość nawet się nad tym nie zastanowi. Przecież nic nie może się stać...

Niestety, nie jest to prawda. Korzystanie z niepewnych sieci bezprzewodowych niesie ze sobą spore ryzyko.

Pod powierzchnią

Opisany powyżej przypadek to typowy atak *man-in-the-middle*. Ktoś w hotelu stworzył prostą stronę z formularzem logowania lub nawet skopiował stronę hotelową tak, aby użytkownik komputera pomyślał, że korzysta z oficjalnego punktu dostępowego. (Przygotowanie takiej strony nie wymaga specjalistycznej wiedzy ani umiejętności. Można tego nawet dokonać przy użyciu wielu routerów Wi-Fi ze zmodyfikowanym oprogramowaniem lub za pomocą laptopa, który działa w obrębie sieci *ad-hoc*). Za sfabrykowaną stroną logowania czeka już gotowe połączenie z internetem zaprojektowane tak, aby użytkownik myślał, że wszystko odbywa się szybko i bez żadnych problemów.

Wszelkie dane, które wprowadzamy podczas takiego połączenia, mogą zostać przechwycone przez cyberprzestępców. Jednym z celów ataku może być pozyskanie danych kart kredytowych, innym zgromadzenie adresów e-mail i innych informacji osobowych.

Rys. 1. Strona logowania się do hotelowej sieci Wi-Fi

Cyberprzestępca musi jedynie czekać – nawet gdy przynętę połknie tylko jedna ofiara, wysiłek się opłaci. Z punktu widzenia ofiary, teoretycznie taniej byłoby zapłacić za znacznie droższe oficjalne połączenie hotelowe. Nie zapominajmy jednak, że nawet legalne sieci nie są całkowicie wolne od zagrożeń.

Ze względu na to, że w sieciach Wi-Fi dane nie są przesyłane przewodami, mogą zostać łatwo przechwycone. Istnieją specjalne programy pozwalające na wyłapywanie pakietów danych z powietrza – jeżeli nie są szyfrowane – i szybkie ich interpretowanie. Zasięg, w jakim jest to możliwe, zależy od siły sygnału punktu dostępowego oraz od zastosowanego standardu Wi-Fi. Dostępne w sklepach routery Wi-Fi działające w standardzie 802.11b oferują zasięg w promieniu niemal 100 m. Ściany i inne obiekty zmniejszają siłę sygnału, jednak dostęp do niego będzie ograniczony do budynku, w którym router się znajduje. Oznacza to, że w wielu przypadkach dane można przechwytywać na przykład z ulicy lub parkingu.

Wspomniany zasięg dotyczy wyłącznie urządzeń sieciowych z wbudowanymi antenami. Istnieje jednak sprzęt pozwalający na przechwytywanie

nawet bardzo słabych sygnałów, co prowadzi do znacznego zwiększenia zasięgu. Instrukcję wykonania takiego urządzenia można bez problemu znaleźć w internecie.

Wiele programów służących do podsłuchiwania sieci bezprzewodowych (aplikacje takie zwane są snifferami) posiada wbudowane funkcje służące do interpretowania danych zaszyfrowanych przy użyciu protokołu SSL. Oznacza to, że nawet bezpieczne połączenia nie gwarantują całkowitej ochrony. W zależności od siły szyfrowania przechwycenie danych może wymagać od cyberprzestępcy większego wysiłku – a wszystko to w czasie, gdy ofiara spokojnie sprawdza pocztę i wprowadza swoje dane osobowe oraz informacje dotyczące systemów płatności online.

Konsekwencje

Potencjalne konsekwencje padnięcia ofiarą ataku *man-in-the-middle* zależą od działań, jakie użytkownik wykonywał w ramach sesji internetowej przechwyconej przez cyberprzestępcę.

W przedstawionym przykładzie jako pierwsze przechwytywane są informacje o koncie e-mail, które może zostać umieszczone na liście zasobów wykorzystywanych do wysyłania spamu. To jednak nie koniec – mając dostęp do konta, cyberprzestępca może zgromadzić informacje osobowe o użytkowniku oraz o osobach, z którymi koresponduje. W wiadomościach e-mail znajdują się cenne informacje – loginy i hasła do forów internetowych, dane dotyczące kont bankowych, prywatne adresy, zdjęcia itp. Jeżeli skradzione konto e-mail jest firmowe, potencjalne szkody będą znacznie większe. W przypadku przechwycenia danych finansowych oszacowanie całkowitych szkód może się okazać możliwe dopiero po latach. Jeżeli dojdzie do wycieku lub upublicznienia poufnych informacji – takich jak wewnętrzne raporty, dokumentacja techniczna lub dane klientów – skutki mogą być opłakane: utrata zaufania klientów i partnerów, spadek sprzedaży a nawet całkowite zerwanie więzi biznesowych. Musimy zatem ze szczególną ostrożnością korzystać z firmowych kont e-mail w obrębie sieci Wi-Fi, których nie znamy.

Ze szczególnie negatywnymi konsekwencjami musimy się liczyć, gdy dojdzie do kradzieży danych dotyczących naszych kart kredytowych lub systemów płatności online. Informacje takie mogą okazać się wystarczające do tego, aby cyberprzestępca zamawiał przeróżne towary z całego świata na nasz koszt. Będzie to możliwe, dopóki nie zorientujemy się o istnieniu problemu, co często dzieje się dopiero wtedy, gdy otrzymamy miesięczny wyciąg z banku. Zazwyczaj banki starają się być przychylne swoim klientom, pod warunkiem że 1) to nie oni dokonali takich zakupów oraz 2) nie traktowali danych swoich kart kredytowych nierozważnie. Podczas gdy punkt pierwszy najczęściej nie stanowi problemu, z drugim warunkiem nie jest już tak lekko i jest traktowany różnie przez poszczególne banki, a nawet jeżeli uda się odzyskać stracone pieniądze, kosztuje to dużo czasu i wysiłku. Z drugiej strony, korzystanie z karty kredytowej w obrębie niezabezpieczonej sieci bezprzewodowej – świadomie lub nie – może zostać potraktowane przez bank jako lekkomyślne, a wówczas ofiara cyberprzestępcy będzie musiała zapłacić za jego zakupy. Z pewnością nie będzie to tania lekcja bezpiecznego korzystania z internetu.

Rys. 2. Różne strony logowania

Większość stron zawierających pole logowania korzysta z zabezpieczenia w postaci protokołu SSL. Mimo że istnieje wiele narzędzi pozwalających cyberprzestępcom na łamanie – i odczytywanie – danych zaszyfrowanych w ten sposób, pewne informacje o logowaniu pozostają ukryte. Jednak nawet na to są sposoby. Jeszcze zanim loginy i hasła trafią do internetu, mogą zostać przechwycone lokalnie na naszym komputerze przy użyciu programu szpiegowskiego, takiego jak keylogger, który rejestruje wszystkie znaki wprowadzane z klawiatury. Gdy użytkownik loguje się na stronie punktu dostępowego kontrolowanego przez cyberprzestępcę, z łatwością może zostać przeprowadzony atak zwany *drive-by download*. Polega on na takim zmodyfikowaniu strony www, aby przy jej otwieraniu na komputer użytkownika automatycznie pobierał się szkodliwy program. To, co będzie się działo później, jest ograniczone wyłącznie wyobraźnią i umiejętnościami cyberprzestępcy.

Wszystkie te działania wykonywane są błyskawicznie, bez wiedzy i zgody użytkownika. Zupełnie inaczej niż miało to miejsce dawniej, kiedy celem komputerowych wandali było manifestowanie swojej działalności i niszczenie danych „dla zabawy". Dzisiaj cyberprzestępcy próbują za wszelką cenę pozostać niezauważeni – im dłużej nie odkryjemy ich działań, tym więcej danych i pieniędzy zdołają nam ukraść.

Oczywiście, przed atakami cyberprzestępców można się chronić. Najpierw jednak przeanalizujemy różne metody szyfrowania i konfigurowanie systemu operacyjnego. W ten sposób możemy

wyeliminować potencjalne słabe punkty naszych komputerów.

Szyfrowanie ruchu internetowego

Najefektywniejszą metodą szyfrowania ruchu internetowego jest VPN (*Virtual Private Network*). Mówiąc w dużym skrócie, metoda ta polega na skonfigurowaniu tunelu VPN między laptopem (komputerem klienckim) a punktem docelowym – serwerem. Cały ruch przesyłany między tymi dwoma punktami jest szyfrowany, co oznacza, że żadne urządzenia pośredniczące lub przekierowujące nie mogą zinterpretować jego zawartości. Ponadto drogą tą przechodzi cały ruch, dzięki czemu omijane są wszelkie mechanizmy blokujące porty. Port 80 (wykorzystywany do obsługi stron internetowych) najczęściej jest otwarty, podczas gdy inne usługi, takie jak komunikatory internetowe lub poczta elektroniczna, są często blokowane przez właściciela punktu dostępowego.

Serwer VPN działa jako cel połączenia i z tego względu musi działać w obrębie bezpiecznego środowiska. Każde żądanie uzyskania dostępu do strony www czy poczty e-mail jest na początku kierowane do serwera VPN i dopiero z niego trafia do serwerów docelowych. Następnie żądana zawartość wraca do użytkownika w postaci zaszyfrowanej. Logowanie do serwera VPN odbywa się poprzez podanie nazwy użytkownika i hasła.

Przedstawiony rodzaj serwera VPN może zostać ustanowiony na wiele sposobów i może tego dokonać każdy, kto posiada chociaż odrobinę wiedzy informatycznej. Podczas wyboru lokalizacji serwera mamy do dyspozycji kilka możliwości.

Serwer może być wynajętym komputerem znajdującym się w jednym z centrów obliczeniowych. Możemy mieć do czynienia zarówno z serwerem fizycznym, jak i wirtualnym. Opcja ta jest szczególnie atrakcyjna dla osób, które już korzystają z takiego komputera, na przykład w roli serwera WWW lub poczty. Do nawiązywania połączeń wymagany jest statyczny adres IP (lub DynDNS, jeżeli mamy do czynienia z dynamicznym IP).

Serwerem VPN może być także komputer znajdujący się w naszym domu. Wymaga to dość szybkiego łącza internetowego oraz możliwości dodania kolejnego komputera do domowej sieci. Taka opcja posiada dodatkową zaletę – będziesz mógł uzyskiwać dostęp do swoich danych w dowolnym momencie i z dowolnego miejsca.

Dostęp VPN często jest oferowany przez pracodawców, zwłaszcza dla tych pracowników, którzy często pracują poza siedzibą firmy. Zazwyczaj jest on jednak mocno ograniczony i pozwala jedynie na wykonywanie zadań związanych z pracą, takich jak sprawdzanie firmowej poczty lub uzyskiwanie dostępu do wewnętrznej sieci (intranet).

Istnieją także firmy oferujące usługi VPN dla podróżujących. Zwykle są one opłacane miesięcznie, a dostawcy oferują szereg planów taryfowych, tak aby każdy mógł znaleźć coś dla siebie.

Bardziej niezależną alternatywą bezpiecznego połączenia jest UMTS, który pozwala na korzystanie z internetu w dowolnym momencie, nawet bez dostępu do jakiejkolwiek sieci Wi-Fi. Zasięg tej usługi jest stosunkowo duży: pokryte jest 60-90 proc. powierzchni Europy, w zależności od odległości od dużych miast.

Mimo że ze względów kompatybilności UMTS bazuje na drugiej generacji technologii GSM, obsługiwana jest także jej trzecia generacja. Z punktu widzenia bezpieczeństwa, technologia 3G jest lepszym wyborem, ponieważ dokonano w niej wielu usprawnień w zakresie uwierzytelniania użytkowników i sieci.

Podstawowe środki ostrożności

Poza szyfrowaniem danych – przeprowadzanym głównie ze względów bezpieczeństwa – istnieją inne czynniki, które powinieneś wziąć pod uwagę podczas konfigurowania i wyposażania swojego komputera.

W celu zapewnienia wygodnej wymiany danych między komputerami, pliki i foldery mogą być udostępniane w sieci. Obiekty takie stają się dostępne niezależnie od rodzaju sieci (przewodowa lub Wi-Fi). W zależności od tego, jak skonfigurowane jest udostępnianie, członkowie sieci mogą z nich korzystać bezpośrednio (z uprawnieniami do odczytu i/lub zapisu) lub po uwierzytelnieniu poprzez podanie nazwy użytkownika i hasła. Z tego względu istotne jest, abyś przed wyjazdem na wakacje oraz podczas łączenia z jakąkolwiek nieznaną siecią wyłączył udostępnianie. Nie chciałbyś przecież, aby wszyscy członkowie sieci, do której jesteś aktualnie podłączony, mogli przeglądać Twoje pliki. Owszem, niektóre punkty dostępowe są wyposażone w mechanizmy, które izolują poszczególne komputery od siebie, jednak nie ma możliwości bezpośredniego zweryfikowania obecności takiej funkcji.

Chociaż wyłączenie udostępniania znacznie zwiększa poziom bezpieczeństwa, zawsze istnieje prawdopodobieństwo bezpośredniego ataku hakera na Twój komputer, w wyniku którego wszystkie Twoje dane staną się widoczne w sieci. Sytuacja taka jest niebezpieczna w każdych okolicznościach, jednak zagrożenie wzrasta, gdy w grę wchodzą poufne dane. Aby jeszcze bardziej poprawić ochronę tych wrażliwych informacji, możesz utworzyć na zewnętrznym nośniku (takim jak pendrive) specjalny szyfrowany folder i w nim przechowywać swoje dane. Możesz do tego celu wykorzystać darmowe rozwiązania dystrybuowane w oparciu o licencję GPL (*General Public License*). Uzyskanie dostępu do danych znajdujących się w zaszyfrowanym folderze będzie możliwe dopiero po podaniu hasła. Mechanizmy szyfrujące stosowane w takich roz-

wiązaniach są na tyle skuteczne, że łamanie zabezpieczeń chroniących skradzione dane będzie po prostu nieopłacalne. Oczywiście, duże znaczenie ma jakość użytego przez Ciebie hasła – pamiętaj, aby składało się ono przynajmniej z ośmiu znaków, zawierało małe i wielkie litery, a także cyfry i symbole nie alfanumeryczne. Po zakończeniu korzystania z danych przechowywanych na nośniku szyfrowanym odłącz go od komputera. Pamiętaj – nawet najlepszy sejf nie pomoże, jeżeli zapomnisz o jego zamknięciu. Poza zwiększeniem bezpieczeństwa podczas korzystania z nieznanych sieci Wi-Fi szyfrowanie ma dodatkową zaletę – nawet gdy Twój laptop zginie lub zostanie skradziony, nikt nie będzie mógł skorzystać z Twoich poufnych danych.

Do zapewnienia skutecznej ochrony niezbędne jest zastosowanie rozwiązania typu *Internet Security*. Poza podstawową funkcjonalnością (ochrona przed szkodliwymi programami) program taki powinien oferować moduł ochrony sieci, w szczególności zaporę sieciową oraz system zapobiegania włamaniom (HIPS – *Host Intrusion Prevention System*). Rozwiązanie bezpieczeństwa dokonuje analizy i wykrywa nieznane aplikacje działające w systemie i klasyfikuje je pod kątem zagrożenia. Klasyfikacja ta stanowi podstawę do przydzielenia poszczególnym aplikacjom odpowiednich uprawnień. Jeżeli program zostanie uznany za podejrzany, otrzyma ograniczone uprawnienia dostępu (lub nie otrzyma ich wcale) do ważnych zasobów, takich jak system operacyjny, sieć, poufne dane czy urządzenia podłączone do komputera. Dzięki takiemu podejściu prawdopodobieństwo infekcji szkodliwym programem jest minimalizowane.

Kolejnym czynnikiem wpływającym na ogólne bezpieczeństwo jest aktualizacja systemu operacyjnego i zainstalowanych w nim aplikacji. Dla wielu osób frustrujące jest to, że co kilka dni jakiś program chce pobierać uaktualnienia udostępnione przez producenta. Fakt – pobieranie takich aktualizacji zajmuje trochę czasu, w którym Ty chciałbyś sprawdzić pocztę lub zapoznać się z informacjami pojawiającymi się na ulubionych stronach www. Jednak ta chwila poświęcona na instalację łaty lub nowszej wersji programu może zapobiec późniejszemu atakowi cyberprzestępcy. Głównym celem publikowania uaktualnień jest likwidacja błędów i luk w zabezpieczeniach, poprzez które możliwe może być przejęcie kontroli nad naszym komputerem. Zatem w tym przypadku należy uzbroić się w cierpliwość i instalować wszystkie dostępne aktualizacje – producenci oprogramowania publikują je przecież dla naszego bezpieczeństwa.

W łańcuchu bezpieczeństwa nie możemy zapominać o najważniejszym, i często najsłabszym, jego ogniwie – użytkowniku. Musimy być świadomi tego, co robimy podczas korzystania z internetu. Ważne jest, w jakim stopniu ufamy sieciom Wi-Fi, z którymi się łączymy. Nieznane punkty dostępowe powinniśmy zawsze traktować z pewnym sceptycyzmem – w końcu nie mamy żadnego wpływu na to, w jaki sposób nasze dane są przesyłane ani kto ma do nich dostęp. Czasami lepiej się wstrzymać i poszukać bardziej zaufanego źródła internetu.

Podsumowanie

Rynek urządzeń sieciowych rośnie bardzo szybko. Globalna sprzedaż w tym segmencie zwiększyła się z 969 mln USD w 2005 r. do 3,46 mld USD w 2009 r. Tak silny wzrost jest spowodowany przede wszystkim coraz większą popularnością punktów dostępowych oferujących bezprzewodowy dostęp do internetu. Najwięcej sieci Wi-Fi instalowanych jest w przemyśle żywieniowym – znajdziemy je już nie tylko w fast-foodach, ale także w kawiarniach i restauracjach. Jak pokazują badania, trend ten został ciepło przyjęty. W Stanach Zjednoczonych 25 proc. wszystkich dorosłych (34 proc. wszystkich użytkowników internetu) korzysta ze swoich laptopów do łączenia się z internetem poza swoim domem lub miejscem pracy. Nie bez znaczenia jest także popularność laptopów – w ciągu kilku lat ich cena znacznie spadła i teraz każdy, kto planuje zakup komputera, może sobie pozwolić na takie urządzenie. Co ciekawe, w 2008 roku klienci zakupili więcej laptopów niż komputerów stacjonarnych.

Niestety, złożoność metod wykorzystywanych obecnie do szyfrowania danych przesyłanych bezprzewodowo znacznie przewyższa poziom wiedzy standardowego użytkownika. Nie powstało jeszcze rozwiązanie tak proste, aby poradzić sobie mógł każdy, kto właśnie wyjął z pudełka nowy laptop i wybrał się z nim na wycieczkę po mieście w celu znalezienia dostępu do internetu. Nawet jeżeli takie rozwiązanie powstanie, będą musieli je zaakceptować i zaoferować właściciele punktów dostępowych, nie wspominając o konieczności wprowadzenia obsługi takiego mechanizmu do systemów operacyjnych. Zatem sukces prostego rozwiązania tego problemu zależy od wielu czynników.

Technologia to jednak nie wszystko. Świadomość zagrożeń i znajomość zasad bezpieczeństwa jest niezbędna do tego, abyś mógł zapewnić ochronę swojego systemu. Jeżeli nie ufasz sieci, z którą próbujesz się łączyć – co zazwyczaj ma miejsce w przypadku nieznanych punktów dostępowych – musisz wiedzieć, jakie informacje z Twojego komputera przedostają się do „świata zewnętrznego". Lepiej być przesadnie zapobiegawczym, niż skończyć z pustym kontem bankowym.

Ostatecznie czynników bezpieczeństwa jest bardzo wiele. Mimo to każdy z nas może, nawet przy niewielkiej wiedzy technicznej, znacznie zwiększyć poziom ochrony i ryzyko potencjalnych problemów.

Autor jest analitykiem zagrożeń w firmie Kaspersky Lab

Najlepsze prace doktorskie
z dziedziny radiokomunikacji i technik multimedialnych

Grzegorz Kantowicz

Wspieranie polskiej nauki

Dnia 17 czerwca 2009 r., w Warszawie, w trakcie sesji otwarcia Krajowej Konferencji Radiokomunikacji, Radiofonii i Telewizji (KKRRiT 2009) odbyło się uroczyste ogłoszenie wyników i wręczenie nagród w ogólnopolskim konkursie Fundacji Wspierania Rozwoju Radiokomunikacji i Technik Multimedialnych na najlepszą pracę doktorską z dziedziny radiokomunikacji i technik multimedialnych.

Siódma edycja konkursu obejmowała rozprawy z dziedziny radiokomunikacji bądź technik multimedialnych obronione z wyróżnieniem pomiędzy 1 stycznia 2008 r. a 6 marca 2009 r. Zarząd Fundacji zaprosił do prac w Komisji Konkursowej 5 profesorów z wyższych uczelni technicznych, kierując się zasadą, że nie powinni to być ani promotorzy ani recenzenci zgłoszonych prac. W skład komisji weszli także przedstawiciele patronów medialnych oraz Fundacji.

Komisja Konkursowa 2009:

- prof. Andrzej Dąbrowski – przewodniczący, Politechnika Warszawska,
- prof. Marek Amanowicz – Wojskowa Akademia Techniczna;
- prof. Andrzej Jajszczyk – Akademia Górniczo-Hutnicza;
- prof. Andrzej Karwowski – Politechnika Śląska;
- prof. Krzysztof Wesołowski – Politechnika Poznańska;
- Marcin Bochenek – Telewizja Polska SA;
- Barbara Kiepas-Jeleńska – Polskie Radio SA;
- Grzegorz Kantowicz – INFOTEL;
- Bogdan Zbierzchowski – Przegląd Telekomunikacyjny;
- Andrzej Buchowicz – Fundacja WRRiTM.

Komisja Konkursowa po wstępnej ocenie merytorycznej zawartości prac oraz ich znaczenia dla rozwoju prezentowanej tematyki postanowiła, w porozumieniu z Zarządem Fundacji, zakwalifikować do grupy finałowej 5 prac z 3 ośrodków naukowych w Polsce. Ich autorzy zostali zaproszeni do wygłoszenia referatów w trakcie sesji tematycznych KKRRiT.

Po podsumowaniu i dyskusji ocen z list rankingowych Komisja Konkursowa w porozumieniu z Zarządem Fundacji postanowiła nie przyznawać drugiej nagrody.

Przyznano następujące nagrody i wyróżnienia:

pierwszą nagrodę w wysokości	10 000 PLN;
dwie trzecie nagrody w wysokości	5 000 PLN;
dwa wyróżnienia w wysokości	1 000 PLN.

Nagrody otrzymali:

I

- **dr inż. Gustaw Mazurek** za rozprawę **System radiowej identyfikacji obiektów z transmisją z bezpośrednim rozpraszaniem widma**, promotor – prof. Jerzy Szabatin, Politechnika Warszawska.

II

- **dr inż. Marek Garbaruk** za rozprawę **Układy antenowe ultraszerokopasmowych systemów radiokomunikacji**, promotor – prof. Giennadij Czawka, Politechnika Białostocka.

III

- **dr inż. Józef Kotus** za rozprawę **Ocena wpływu zagrożeń hałasowych na częstość występowania chorób słuchu z zastosowaniem systemów teleinformatycznych**, promotor – prof. Bożena Kostek, Politechnika Gdańska.

Wyróżnienia otrzymali:

- **dr inż. Łukasz Balewski** za rozprawę **Automatyczne projektowanie złożonych mikrofalowych układów filtrujących**, promotor – prof. Michał Mrozowski, Politechnika Gdańska;
- **dr inż. Piotr Szczuko** za rozprawę **Zastosowanie reguł rozmytych w komputerowej animacji postaci**, promotor – prof. Bożena Kostek, Politechnika Gdańska.

Nagrodzeni od lewej: dr inż. Piotr Szczuko (wyróżnienie), dr inż. Łukasz Balewski (wyróżnienie), dr inż. Józef Kotus (III nagroda), dr inż. Gustaw Mazurek (I nagroda), dr inż. Marek Garbaruk (III nagroda)

Dyplomy wręczali laureatom pani minister Magdalena Gaj wraz z prezesem Rady Fundacji, dr. Radomirem Gruczą

Patronami medialnymi konkursu były: Telewizja Polska, Polskie Radio, Magazyn INFOTEL, Przegląd Telekomunikacyjny. ■

Łatwa produkcja treści dla komórek

Pierwsze studio do tworzenia wideo dla sieci 3G

Francuska Firma Tetco-Voxpilot, znana już na rynku platform VoiceXML dzięki produktowi Open Media Platform, uruchamia nowy pakiet oprogramowania Videofy studio, umożliwiający zarówno profesjonalne tworzenie materiału wideo w dowolnym formacie, jak i wprowadzanie go do systemów nadających interaktywne materiały wideo.

Przez długi czas, z powodu wysokich kosztów i skomplikowanej procedury wdrożenia, takie rozwiązania nie były dostatecznie rozwijane. Obecnie Tetco-Voxpilot oferuje użytkownikom, niemającym nawet zaawansowanej wiedzy ani doświadczenia technicznego, możliwość aktualizowania treści wideo przy bardzo niskich kosztach, a przez to zwiększania ich atrakcyjności.

W ramach Videofy studio Tetco-Voxpilot upraszcza tworzenie materiałów wideo dzięki składnikowi Video Composer. W tym celu wystarczy:

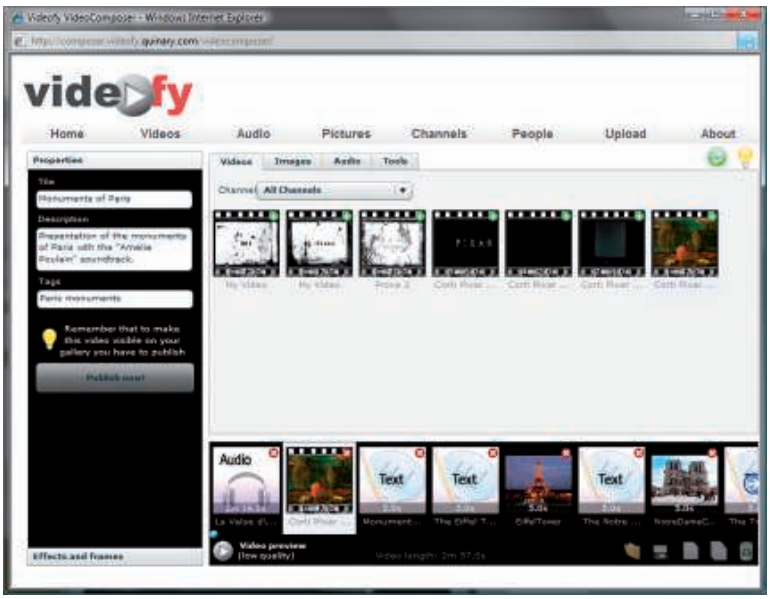
- zastosować „przeciągnij i upuść" (*drag and drop*) w odniesieniu do filmów, obrazów, plików audio i tekstowych, które składać się będą na przyszły materiał wideo,
- zmontować ten materiał ustalając kolejność sekwencji wideo,
- opublikować tak otrzymany materiał.

Do zastosowania tego programu nie jest wymagana wcześniejsza znajomość języka VoiceXML.

Video Portal Creator pozwala wykorzystać treści wideo, a także inne zewnętrzne elementy dynamiczne wyłącznie w oparciu o interfejs graficzny. Po zakończeniu tego etapu pozostaje już tylko załadowanie stworzonego materiału na serwery, z których stanie się on dostępny w czasie rzeczywistym.

– *Udało nam się wreszcie uwolnić od ograniczeń technicznych i finansowych związanych dotychczas z udostępnianiem materiałów wideo w sieciach komórkowych 3G* – komentuje **Tristan Dessain-Gelinet**, dyrektor generalny firmy Tetco-Voxpilot. – *Dzięki uproszczonej procedurze tworzenia treści wideo, dostawcy usług i operatorzy mają obecnie do dyspozycji narzędzie umożliwiające łatwe i szybkie aktualizowanie oferty serwisów wideo przy niskich kosztach, podnosząc przy tym liczbę połączeń i wielkość przychodów.*

Dostawcy usług i operatorzy telekomunikacyjni będą więc mogli oferować abonentom nowe treści dzięki regularnie aktualizowanym materiałom wideo, zawierającym profesjonalne bądź amatorskie nagrania (jak wideoblogi społecznościowe), dynamiczne reklamy kontekstowe na stronach z filmami wideo dla abonentów, klipy wideo łączące treści statyczne i zawartość dynamiczną, jak na przykład serwisy kartograficzne, prognozy meteo, bieżące wiadomości itd. ■



Rekord.ERP dla przedsiębiorstw

Zintegrowany system informatyczny Rekord.ERP jest w pełni polskim oprogramowaniem, doskonale dostosowanym do oczekiwań naszych przedsiębiorców, spełniając przy tym wymogi stawiane przed systemami klasy ERP/ERP II.

Program obsługuje **cały obszar działalności przedsiębiorstwa**, od momentu planowania **i zaopatrzenia**, poprzez **produkcję**, aż po **zbyt** i **dystrybucję wyrobów**. Główne funkcje modułów produkcyjnych to:

- definiowanie złożonych struktur wyrobu (BOM), budowanie wariantowych marszrut wytwarzania, elastyczne dopasowanie kalkulacji kosztowych;
- planowanie procesu wytwarzania w oparciu o spływające zamówienia, dane z poprzednich okresów oraz prognozy;
- harmonogramowanie produkcji z ograniczeniem zasobów pracy oraz materiałów;
- monitorowanie procesu wytwarzania w oparciu o rejestrację działań przez pracowników bezpośrednio produkcyjnych;
- wizualne zarządzanie zleceniami produkcyjnymi metodą Gantt'a;
- zarządzanie dokumentacją technologiczną (rysunki, instrukcje, karty kontroli itd.) oraz warsztatową (przewodniki, karty pracy);
- kontrolę wykorzystania zasobów krytycznych (wąskich gardeł) oraz śledzenie rzeczywistych kosztów produkcji;
- monitorowanie oraz korygowanie planów produkcyjnych (długookresowych, operacyjnych) w odniesieniu do zmiennych (materiały i zasoby).

Rekord.ERP pozwala na włączenie do systemu obiegu informacji partnerów biznesowych firmy. Dzięki zastosowaniu internetowego modułu **e-Sprzedaż**, klienci zyskują funkcjonalność składania online zamówień na wyroby typowe jak i podlegające konfiguracji w zakresie konstrukcji lub wykończenia oraz śledzenia stanu realizacji. Podobnie poprzez zastosowanie modułu **e-Dostawca**, harmonogram dostaw może podlegać weryfikacji i potwierdzaniu online przez naszych dostawców. Uzupełnieniem nowoczesnych, internetowych rozwiązań jest **e-Przedstawiciel** – moduł do zarządzania siecią przedstawicieli handlowych.

Pakiet posiada oczywiście moduły takie jak **Kadry-Płace**, **Finanse-Księgowość**, niezbędne do prowadzenia każdej firmy. Co ważne, są one w od podstaw zaprojektowane na bazie polskiej specyfiki i praktyki użytkowników.

Rekord.ERP jest wyposażony w doskonałe narzędzia do wspomagania zarządzania, takie jak: Generator Raportów, Alerty o zdarzeniach oraz internetowy system wspomagania decyzji – **LIDER** – narzędzie doceniane przez kadrę zarządzającą, łączącą informacje z wszystkich modułów, pozwalające na surfowanie od ogółu (np. wartość marży w rankingu klientów) do najgłębszego szczegółu (np. pozycja faktury, zamówienia lub szczegóły dekretu księgowego).

Najistotniejsze cechy pakietu Rekord.ERP:

- integracja wszystkich obszarów działalności organizacji;
- uporządkowanie i zarządzanie procesami przedsiębiorstwa;
- optymalizacja zasobów;
- wsparcie procesu decyzyjnego;
- możliwość dostosowania do specyfiki danego przedsiębiorstwa;
- otwartość systemu umożliwiająca integrację z urządzeniami oraz oprogramowaniem zewnętrznym;
- zapewnienie bezpieczeństwa informacji zarówno przed jej utratą, jak i dostępem osób niepowołanych;
- narzędzia umożliwiające niezależną rozbudowę systemu;
- zgodność z przepisami polskiego prawa.

Wdrożenie oprogramowania Rekord.ERP zapewnia integrację i automatyzację istotnych procesów, obniżenie kosztów i w efekcie pozwala na podniesienie konkurencyjności przedsiębiorstwa.

Szczegółowe informacje i dane kontaktowe:
www.rekord.com.pl, www. atssi.pl

Dla małych i średnich ISP

Grzegorz Kantowicz

MMS – kompleksowe zarządzanie usługami

Firma Forweb wprowadziła do oferty nową wersję platformy Multi Management System do obsługi Abonentów i zarządzania usługami telekomunikacyjnymi. Oprogramowanie przeznaczone jest dla małych i średnich firm ISP i umożliwia m.in. zarządzanie umowami i aneksami, fakturowanie wraz z rozliczeniami i kontrolą płatności czy też obsługę zgłoszeń i awarii.

Multi Management System jest autorskim systemem przygotowanym przez Forweb dla usprawnienia pracy firm świadczących usługi dostępu do internetu, telefonii VoIP oraz IPTV. Jest tańszy i prostszy w obsłudze niż systemy przeznaczone dla dużych ISP, ale posiada zbliżone funkcjonalności.

Funkcjonalności Multi Management System

Multi Management System składa się z platformy podstawowej oraz modułów dodatkowych. Platforma podstawowa MMS udostępnia takie funkcjonalności, jak:

- tworzenie, edycja, usuwanie usług i taryf;
- zarządzanie umowami i aneksami, w tym tworzenie wzorów i szablonów umów oraz wyświetlanie statystyk dla umów;
- fakturowanie wraz z rozliczeniami oraz kontrolą płatności (współpraca z zewnętrznymi programami księgowymi Optima i Enova);
- zarządzanie klientami i grupami klientów wraz z pełną historią klienta, statystykami oraz możliwością tworzenia korespondencji seryjnej;
- zarządzanie routerami, sieciami oraz adresami IP;
- zarządzanie osprzętem sieciowym;
- zarządzanie i ewidencja awarii;
- zarządzanie czasem pracowników oraz strukturą firmy;
- raportowanie umów, aneksów i awarii.

Instalacja modułów dodatkowych pozwala korzystać z kolejnych funkcjonalności:

- VoIP – telefonia internetowa w ramach własnej platformy ThePhone: konfiguracja cenników, provisioning, billingi miesięczne i ogólne;
- hosting – zarządzanie pocztą e-mail, www, FTP, serwer baz danych, zintegrowany e-BOK wraz z bazą do jego obsługi;
- DNS – zarządzanie domenami i serwerami DNS, obsługa Radiusa dla rozwiązań Poppe;
- ZABBIX – system statystyk i monitorowania sieci;
- system logów – logowanie aktywności klientów (ruch do limitów, przeglądane strony, wysyłana poczta);
- Proxy – zintegrowany system proxy oraz system blokad rodzicielskich;
- Backup – system utrzymania kopii zapasowych poszczególnych części systemu wraz z bazami danych, tworzenie backupów;
- router na karcie CF/module SSD – zarządzanie sieciami i ruchem na karcie CF lub module SSD;
- Optima lub Enova – systemy księgowe współpracujące z MMS.

Korzyści dla operatorów

Multi Management System przeznaczony jest dla małych i średnich firm ISP niezależnie od technologii, w oparciu o które są świadczone usługi, oferowanych pakietów, proponowanych promocji czy liczby obsługiwanych abonentów. Ma usprawnić pracę dostawcom usług telekomunikacyjnych oraz wyeliminować ograniczenia, z jakimi związane jest korzystanie z rozwiązań opensource. System pozwala zautomatyzować szereg czynności, które dotychczas musiały być wykonywane ręcznie, a tym samym umożliwia ograniczenie zatrudnienia w administracji (szybki zwrot z inwestycji). Jest prosty w obsłudze i posiada szerokie możliwości konfiguracyjne, a budowa modułowa pozwala w przyszłości na łatwe poszerzanie systemu o dodatkowe funkcjonalności.

Multi Management System już teraz gotowy jest do zarządzania usługami xPlay.

Wraz z platformą Klient otrzymuje dostęp do profesjonalnego wsparcia technicznego, a dla zainteresowanych możliwe jest również otwarcie części kodu.

Dostępne wersje, usługi dodatkowe

Multi Management System dostępny jest w czterech wersjach w zależności od wielkości sieci oraz usług oferowanych przez operatora. Obecnie dostępne wersje to:

- **BASIC LIGHT** – dla sieci do 1000 użytkowników, składa się z platformy podstawowej MMS;
- **BASIC LIGHT+VoIP** – dla sieci do 2000 użytkowników, składa się z platformy podstawowej MMS oraz modułu VoIP na serwerze z mms-base;
- **BASIC 1000** – dla sieci do 5000 użytkowników, zawiera wszystkie dostępne moduły instalowane oddzielnie lub częściowo na serwerze z mms-base;
- **BASIC Pro** – dla sieci do 10000 użytkowników, zawiera wszystkie dostępne moduły instalowane oddzielnie.

Oprócz platformy Forweb oferuje również całą gamę usług dodatkowych, np. zdalną administrację i nadzór nad systemem, możliwość zakupu ruchu VoIP po atrakcyjnych cenach czy konfigurację systemu do pracy z programami księgowymi Optima lub Enova. ■

Biblioteki, kawiarenki internetowe, punkty ksero oraz pracownie szkolne na celowniku

Maciej Ziarek

Res Publica – czyli o tym, co można znaleźć w publicznych komputerach

W dzisiejszych czasach internet jest coraz tańszy i szybszy. Coraz większymi krokami zbliża się czas, kiedy Sieć będzie w domach równie powszechna jak telewizja, jednak istnieją miejsca, w których można korzystać z internetu publicznego. Jest to wygodne, kiedy musimy sprawdzić pocztę będąc w innym mieście, czy wydrukować pracę w punkcie ksero bez konieczności zabierania laptopa. Niestety, często korzystając z takich komputerów nie przywiązujemy wagi do bezpieczeństwa. Zostawiamy dane o sobie, nasze prace, hasła i loginy. Nie zwracamy też uwagi na stan zainstalowanego oprogramowania, czy znajduje się tam antywirus lub czy system jest aktualny. To wszystko może się przyczynić do późniejszych ataków na nasze konta lub próby wyłudzenia danych.

Test bezpieczeństwa na publicznych stanowiskach

Aby dowiedzieć się, jakie informacje można znaleźć przy takich stanowiskach dostępnych publicznie oraz jak wygląda tam kwestia bezpieczeństwa, wybrałem się do kilkunastu punktów, gdzie oferowany jest dostęp do internetu. Były to biblioteki, kawiarenki internetowe, punkty ksero oraz pracownie szkolne. W każdym miejscu testowałem od dwóch do czterech stanowisk. Łącznie przebadanych zostało 35 komputerów. Na stanowiskach tych sprawdzałem, czy można uzyskać dostęp do następujących informacji:

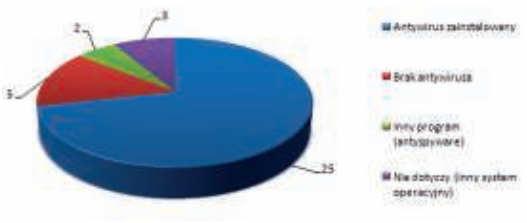
- haseł i loginów do stron i usług internetowych;
- haseł do komunikatora Gadu-Gadu;
- danych osobowych, zdjęć;
- prac i dokumentów powiązanych z osobami, które korzystały z komputera.

Jeżeli chodzi o bezpieczeństwo komputerów, zwracałem uwagę na czynniki takie, jak:

- uaktualniony program antywirusowy;
- data ostatniego skanowania dysku;
- aktualizacja systemu (w tym zainstalowane pakiety Service Pack);
- zainstalowane przeglądarki internetowe.

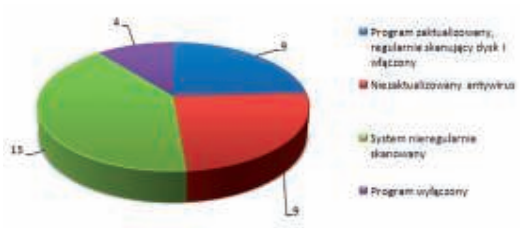
Chciałbym podkreślić, że żadne dane znalezione na testowanych stanowiskach nie zostały pobrane, nigdzie upublicznione ani w jakikolwiek sposób wykorzystane. Całość służyła jedynie sporządzeniu raportu. Jeżeli była taka możliwość, starałem się usunąć usterkę poprzez włączenie aktualizacji lub wykasowanie prywatnych danych, takich jak hasła i loginy. Żaden z plików nie był rozkodowywany ani odszyfrowany w celu odzyskania hasła czy loginu.

Zacznijmy od poziomu zabezpieczeń na przebadanych komputerach. Niestety, nie można powiedzieć, że jest dobrze. Wręcz przeciwnie – jest tragicznie. Na 35 komputerów jedynie 7 posiadało aktualne systemy z programem antywirusowym wyposażonym w świeże sygnatury i regularnie skanującym komputer. Na tych 7 komputerach znajdowały się też przeglądarki Internet Explorer 8 oraz Firefox. Na pierwszy ogień pójdą programy antywirusowe, które są trzonem bezpieczeństwa jeżeli chodzi o blokowanie możliwości rozprzestrzeniania się złośliwego oprogramowania.



Rys. 1. Obecność programu antywirusowego

Wydawać by się mogło, że z bezpieczeństwem komputerów publicznych nie jest wcale tak źle. Należy jednak pamiętać, że sam fakt posiadania antywirusa nie oznacza wcale, że komputer jest zabezpieczony. Dodać należy, że program anti-spyware nie zastępuje programu antywirusowego – powinien być jedynie dodatkiem do niego. Poniżej znajduje się wykres, który pokazuje, jak dużo brakuje, by mówić o bezpiecznych stanowiskach dla użytkowników.

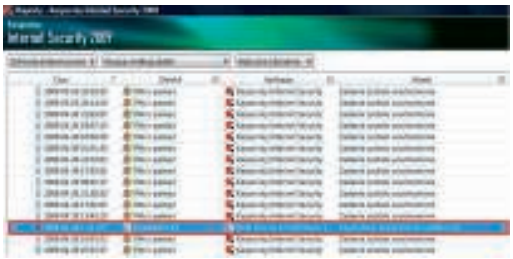


Rys. 2. Nieprawidłowości związane z zainstalowanym programem antywirusowym

Niektóre programy łączyły w sobie po kilka nieprawidłowości, np. brak aktualnych sygnatur oraz regularnego skanowania. W ekstremalnych przypadkach były to programy całkowicie wyłączone, które po uruchomieniu monitowały o konieczności aktualizacji oraz przeskanowania (często dopiero pierwszego) komputera. Najdłużej nieaktualizowany antywirus miał sygnatury z dnia 16.06.2008 r., natomiast jeżeli chodzi o skanowanie, niechlubny rekord przypadł maszynie, na której pełne przebadanie systemu wykonane zostało po raz ostatni dnia 31.07.2008 r. Obrazki, takie jak ten poniższy, nie należały do rzadkości. Bardzo często zdarzało się, że na testowanym komputerze były zainstalowane programy zabezpieczające, jak antywirus czy antispyware, ale okazywały się nieaktualne lub po prostu... wyłączone.

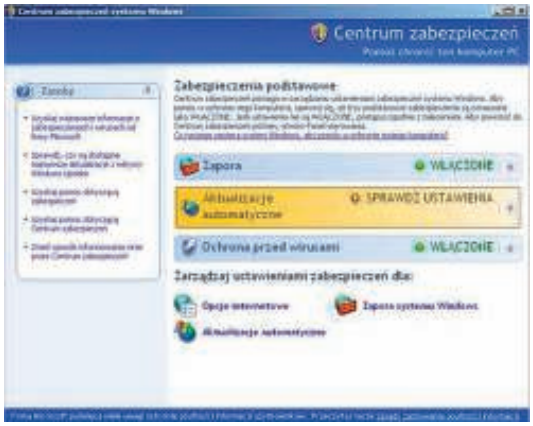
Rys. 3. Wyłączona ochrona antywirusowa i zapora sieciowa

Zagrożeniem bezpośrednio wynikającym z powyższego jest roznoszenie szkodników na inne komputery – głównie nasze notebooki czy domowe pecety. Kiedy idziemy do kawiarenki internetowej, aby poprawić pracę w edytorze tekstu czy też wydrukować coś, korzystamy z pamięci przenośnych. Jeżeli publiczny komputer jest zainfekowany, zaatakowany może zostać także podłączony pendrive. Kolejny komputer, do którego zostanie podłączona taka pamięć, również padnie ofiarą szkodliwego kodu. Oto jaką niespodziankę przyniosłem ze sobą po wizycie w jednej z kawiarenek...



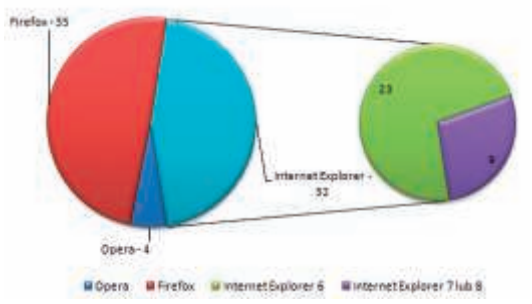
Rys. 4. Trojan wykryty na pamięci przenośnej przyniesionej z kawiarenki internetowej

Jest to robak, który automatycznie kopiuje się na pamięci przenośnej po jej podłączeniu. Jego głównym celem jest zbieranie informacji o użytkowniku, zwłaszcza haseł do gier online. Biorąc pod uwagę fakt, że większość osób ma tak skonfigurowany system, by odtwarzał automatycznie zawartość urządzenia zaraz po jego podłączeniu, trudno się dziwić, że współczesne robaki i wirusy rozprzestrzeniają się tak szybko nawet poza internetem. Sami im w tym pomagamy. Kolejną kwestią związaną z bezpieczeństwem komputerów są regularne aktualizacje systemu, w tym przeglądarek internetowych. Tutaj było już lepiej niż w przypadku programów antywirusowych, jednak nadal kilka kwestii pozostawiało wiele do życzenia. Aktualizacje automatyczne były albo wyłączone, albo włączone, lecz z zaznaczeniem, że to użytkownik sam wybiera, kiedy mają być pobrane i zainstalowane. W konsekwencji systemy były nieaktualne od kilku miesięcy.



Rys. 5. Wyłączone aktualizacje automatyczne

Jeżeli chodzi zaś o przeglądarki internetowe, to praktycznie na wszystkich komputerach były dwie lub trzy – Internet Explorer, Firefox oraz Opera. Poniższe dane prezentują rodzaj przeglądarek i ich liczbę na 35 przebadanych komputerach.



Rys. 6. Zainstalowane przeglądarki internetowe

Na każdym komputerze zainstalowany był Firefox. Należy jednak pamiętać, że wiele osób z przyzwyczajenia wybiera przeglądarkę Internet Explorer. Jak przedstawia wykres, większość komputerów posiadała leciwego już IE6, a jedynie na 4 zainstalowana była najnowsza przeglądarka Microsoftu: IE8. Na koniec dodam, że wśród 7 komputerów, które były zabezpieczone w sposób prawidłowy, znalazły się 3 stacje z systemem Linux. Znajdowały się one na jednej z uczelni. Każdy student mógł zalogować się na swoje własne konto (gdzie loginem był nr indeksu, a hasło musiało posiadać cyfry i znaki specjal-

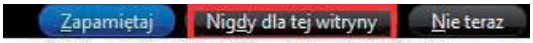
ne). Podczas procesu logowania przez kilka sekund wyświetlana była informacja o konieczności wylogowania po zakończeniu pracy na komputerze. Z pewnością taki system daje o wiele większe bezpieczeństwo dla użytkownika niż niezaktualizowany z wyłączonym programem antywirusowym.

Mylić się to rzecz ludzka...

Niestety, jak zwykle najsłabszym ogniwem okazuje się człowiek. Siadając przy jednej z wyżej wymienionych stacji z zainstalowanym Linuksem, miałem przed sobą gotowy system z niewylogowanym użytkownikiem... Mimo monitów, ktoś odszedł od komputera pozostając wciąż zalogowanym. Jest to tylko wierzchołek góry lodowej. Poniżej prezentuję informacje, jakie wiele osób zostawia po sobie w kawiarenkach internetowych. Na 9 komputerach znajdowały się zapisane loginy i hasła do wszelkiej maści serwisów:

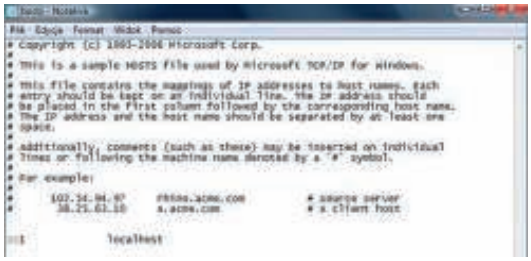
- Nasza-klasa.pl;
- Sympatia.pl;
- Fotka.pl;
- Poczta.

Wszystkie te informacje zostały zapamiętane przez przeglądarkę Firefox. Oczywiście wszystko odbywało się za zgodą użytkownika. Wychodzi na wierzch niedbalstwo i ignorowanie pojawiających się komunikatów. Bezmyślne klikanie skutkuje zapamiętaniem loginów i haseł. Za każdym razem kiedy pojawia się komunikat taki jak ten poniżej, winniśmy



byli kliknąć „Nigdy dla tej witryny” (zakładając oczywiście, że używamy komputera innego niż nasz). Wprawdzie większość przebadanych komputerów posiadała włączoną opcję konta z ograniczonymi prawami i to z niej mogli korzystać użytkownicy, jednak miały miejsce sytuacje, gdzie domyślnym kontem było konto administratora. W takim przypadku każdy mógł na używanej maszynie zainstalować trojana, programy szpiegujące czy też całkowicie wyłączyć ochronę komputera. Istniała także możliwość przekierowania przyszłych użytkowników danego komputera na fałszywe witryny. Nie wymagałoby to większych nakładów pracy. W każdym systemie Windows znajduje się plik hosts, w którym zgromadzone są informacje na temat stron internetowych (a dokładnie adres IP i nazwa). Przeglądarka, zanim połączy się z żądaną witryną, sprawdza plik hosts, dzięki czemu można przyspieszyć ładowanie stron lub blokować reklamy czy też niechciane witryny. Hosts jest zapisany jako plik tekstowy, jego działanie opiera się na zapisaniu nazwy strony i przypisanego do niej adresu IP. Atakujący może jednak umyślnie przypisać konkretną nazwę (np. banku) do innego adresu, przez co nawet wpisując w przeglądarce poprawny adres zostajemy przekierowani na fałszywą, lecz łudząco podobną stronę. Wszelkie dane, jakie wtedy wpiszemy, znajdą się w rękach atakującego. Obok znajduje się zrzut ekranu przykładowego pliku hosts.

Wiele skarbów znajduje się także na samym pulpicie. Znalazłem tam informacje mniej przydatne dla potencjalnego cyberprzestępcy, jak zdjęcia, prace



Rys. 8. Przykładowa zawartość pliku hosts

do szkoły/uczelni, tłumaczenia tekstów, ale także prawdziwe perełki, np. CV, listy motywacyjne, a nawet rozdziały prac licencjackich i magisterskich. Nie dość, że jak na tacy podajemy swoje dane osobo-

Rys. 9. Przykładowy pulpit komputera w kawiarence internetowej

we, to jeszcze zachęcamy do plagiatu. Powyżej znajduje się zrzut ekranu jednego z takich pulpitów... Ze względów bezpieczeństwa, wszystkie nazwy plików pozostawionych przez użytkowników tego komputera zostały zasłonięte.

Należy również liczyć się z faktem, że jeżeli zapiszemy dokument bądź plik na dysku twardym, to będzie on do odzyskania nawet po jego skasowaniu. W sieci jest dostępnych wiele aplikacji, także darmowych, które umożliwiają odzyskiwanie danych skasowanych ręcznie lub w wyniku formatowania. Pliki, które kasujemy poprzez umieszczenie ich w koszu systemowym, nie są zabezpieczone w ogóle, ponieważ ich przywrócenie jest banalne. Największe wrażenie zrobiła na mnie liczba komputerów, na których znajdowało się po kilka kont Gadu-Gadu. Łącznie na wszystkich komputerach było ich aż 46. Program ten nie oferuje praktycznie żadnego zabezpieczenia jeżeli chodzi o hasła. Znajdują się one w pliku config.dat i są banalnie proste do odkodowania. Wystarczy podłączyć pendrive i zgrać pliki z odpowiedniego katalogu, a w domu na spokojnie je rozkodować. W ten sposób posiadamy już czyjś nr gg i hasło do niego.

Pomijając możliwość robienia głupich dowcipów i podszywania się pod kogoś poprzez Gadu-Gadu czy wysyłanie e-maili, cyberprzestępca może wykorzystać te dane do znacznie bardziej destrukcyjnych celów. Nawiążę tutaj do socjotechniki, o której pisałem niedawno w artykule „Login i hasło raz proszę!". Wyobraźmy sobie następujący scenariusz: atakujący wydobywa z pliku config.dat hasło dla konkretnego numeru Gadu-Gadu. Kolejnym krokiem będzie wykorzystanie serwisów społecznościowych do odnalezienia po samym numerze gg konta danej osoby. W ten sposób ma już imię, nazwisko, miejscowość, czasami także nr telefonu. Korzystając z programu do rejestrowania wielu numerów gg jednocześnie, atakujący może wybrać sobie taki, który jest najprostszy do zapamiętania i najkrótszy. Teraz pozostaje napisać odpowiednią wiadomość, podając się za administratora. Na przykład:

Szanowny xxx yyy!
W związku z próbami włamań na nasze serwery, zmuszeni jesteśmy do wdrożenia nowych zabezpieczeń, które lepiej będą chronić naszych użytkowników. Pana hasło [abc] może okazać się niewystarczające do zabezpieczenia konta. Aby to zmienić, proszę zainstalować łatkę na program, która znajduje się pod następującym adresem [link do strony z trojanem]
– Pozdrawiam!
Administrator yyy zzz [Dane mogłyby być prawdziwe i pochodzić z oficjalnej strony aplikacji]

Scenariuszy może być wiele, a jego inna wariacja to zdobycie adresu e-mail i wykorzystanie faktu, że wielu użytkowników posiada takie same hasła do wielu usług. Jeżeli wydobyte z gg hasło będzie takie samo jak do poczty, atakujący może sfałszować nagłówek wiadomości, tak aby wyglądała na wiadomość od administratora portalu, gdzie ofiara posiada swoje konto, i wysłać wiadomość podobną do tej wyżej:

Od: administrator@nazwa_portalu.pl
Do: xxx yyy
Szanowna xxx yyy!

W związku z próbami włamań na nasze serwery, zmuszeni jesteśmy do wdrożenia nowych zabezpieczeń, które będą lepiej chronić naszych użytkowników. Pani hasło [abc] może okazać się niewystarczające do zabezpieczenia konta. Aby mieć pewność, że nikt nie przejął Pani konta, prosimy o wysłanie na adres [adres e-mail atakującego] zeskanowanego dowodu tożsamości. Prosimy tego dokonać w ciągu 7 dni roboczych. W przeciwnym wypadku konto zostanie nieodwracalnie zablokowane. Pozdrawiam serdecznie! Administrator yyy zzz [Dane mogłyby być prawdziwe i pochodzić z oficjalnej strony aplikacji]

Powyższe przykłady, niestety, są całkiem prawdopodobne do zrealizowania. Myślę, że wielu osobom wydałaby się wiarygodna wiadomość, w której podane jest hasło, imię i nazwisko, i która pochodzi od administratora. Wiadomość jest tym bardziej autentyczna, im bardziej uwierzytelniona, dlatego zwłaszcza ten drugi scenariusz ataku jest niebezpieczny, ponieważ sfałszowany nagłówek wskazuje administratora portalu.

Głos ludu

Na koniec zaprezentuję kilka wypowiedzi z sondy, jaką przeprowadziłem wśród osób korzystających z publicznych komputerów.

Czy zwracasz uwagę na stan bezpieczeństwa komputera, z którego aktualnie korzystasz (czy posiada aktualny program antywirusowy, kiedy wykonano ostatnie skanowanie, czy są zainstalowane różne przeglądarki, czy system jest zaktualizowany)?

„Raczej nie, nie przywiązuję większej uwagi do bezpieczeństwa komputera, z którego korzystam poza domem. Nie mam na to czasu. Za to na własnym komputerze mam zainstalowany program antywirusowy. Zdarzało mi się jednak przynosić na pendrive wirusy z ksero".

Czy korzystając z przeglądarki korzystasz z opcji „zapamiętaj dane formularzy/zapamiętaj hasła"? Czy po zakończeniu pracy używasz opcji „wyczyść prywatne dane"?

„Jeżeli zdarza mi się korzystać z kawiarenki internetowej, to po zakończeniu pracy czyszczę z przeglądarki prywatne dane. Nigdy nie wybieram też opcji zapamiętywania haseł. Wtedy każdy mógłby je wykorzystać".

Czy miała miejsce kiedyś sytuacja, że ktoś przejął/zmienił hasło do Twojego konta pocztowego/gg/inne?

„Nie jestem pewna. Miałam kiedyś problem z zalogowaniem się na konto gg i pomimo wpisywania prawidłowego hasła nie mogłam się na nie dostać. Niestety, nie używałam już maila do przypominania hasła i założyłam nowe konto. Nie wiem, czy był to skutek używania gg poza domem".

Jakie są wnioski?

Jak widać, bezpieczeństwo publicznych komputerów nie stoi na wysokim poziomie i pozostawia wiele do życzenia. Także użytkownicy powinni być bardziej czujni i nie traktować komputerów, do których ma dostęp większa liczba osób, jak swoich własnych. Należy pamiętać o każdorazowym wylogowaniu z systemu, jeżeli jest taka możliwość, używaniu Web Gadu-Gadu zamiast standardowego programu, usuwaniu plików z pulpitu i folderów, tak by nie zostały na dysku oraz o czyszczeniu prywatnych danych w przeglądarkach. W domu natomiast dobrze jest skanować pamięć przenośną po każdej wizycie w kawiarence internetowej. Rzecz publiczna to zjawisko dobre, jednak bezpieczeństwo nie zna kompromisów i dotyczy jednostki. Każdy musi zadbać o nią we własnym zakresie, bowiem nawet najlepszy program nie zapewni ochrony, jeżeli my sami ani trochę o nią nie zabiegamy.

Autor jest analitykiem zagrożeń,
Kaspersky Lab Polska
maciej.ziarek@vs.kaspersky.pl

Technologia kontroli „odcisków palców” DataDNA™

Grzegorz Kantowicz

Zabezpieczenia przed wyciekami danych

Firma Trend Micro przedstawiła nową wersję rozwiązania zapobiegającego wyciekom danych LeakProof 5.0, która została wyposażona w dodatkowe funkcje upraszczające wykrywanie, monitorowanie i blokowanie poufnych danych oraz obniżające związane z tym koszty.

Liczba włamań w celu skradzenia danych rośnie lawinowo – w 2008 r. zgłoszono kradzież ponad 35 mln rekordów z danymi[1], czyli ponad dwukrotnie więcej niż rok wcześniej. Prawie 80 proc.[2] włamań wewnętrznych jest dziełem uprawnionych użytkowników z samej firmy. Utrata własności intelektualnej powoduje spadek konkurencyjności i zmniejszenie udziału w rynku. Rozwiązanie zapobiegające utracie danych ma więc znaczenie krytyczne dla przedsiębiorstw, gdyż pozwala wyeliminować przypadkowe i celowe wycieki danych.

Rozwiązanie LeakProof chroni informacje poufne, takie jak dane klientów i pracowników oraz dane stanowiące własność intelektualną, poprzez monitorowanie wycieków informacji oraz zapobieganie im w różnych obszarach zagrożeń.

Rozwiązanie jest dostępne w dwóch wersjach. Wersja LeakProof Standard pomaga przedsiębiorstwom w zachowaniu zgodności z przepisami poprzez zapewnienie ochrony danych pracowników i klientów. Wersja LeakProof Advanced oferuje taką samą ochronę, a ponadto zaawansowaną technologię kontroli „odcisków palców” DataDNA™, co pozwala zabezpieczyć własność intelektualną i tajemnice handlowe.

Opatentowana przez firmę Trend Micro technologia DataDNA zapewnia maksymalną dokładność i skuteczność wykrywania poufnych danych, co pozwala klientom korzystającym z rozwiązania LeakProof zaoszczędzić wiele czasu i pieniędzy. W technologii tej wykorzystano zaawansowane algorytmy, które wyodrębniają „DNA” poufnych danych zawartych w plikach, rekordach, wiadomościach e-mail i innych materiałach, po czym zapisują je w postaci sygnatur. Podobnie jak prawdziwe odciski palców, sygnatury te stanowią sekwencję jednoznacznie identyfikującą informacje zawarte w dokumencie.

Metoda kontroli „odcisków palców” zastosowana w rozwiązaniu LeakProof zapewnia dokładność oraz praktycznie zerową liczbę fałszywych trafień, co umożliwia przedsiębiorstwom przeszukiwanie bazy danych z „odciskami palców” zawierającej wiele milionów rekordów, aby błyskawicznie określić, czy jest w niej odpowiednik określonych treści. Rozwiązanie to zajmuje niewiele pamięci, dzięki czemu można je zainstalować nawet w laptopach bez angażowania zbyt wielu zasobów czy spowalniania pracy komputera. Ponadto oparta na rozpoznawaniu znaków technologia firmy Trend Micro pozwala wyodrębniać „odciski palców” z dowolnego języka. W odróżnieniu od innych rozwiązań, w których moduły zarządzania „odciskami palców” muszą rozumieć język, aby tworzyć takie odciski, technologia zastosowana w rozwiązaniu LeakProof jest niezależna od języka.

NOWA usługa Active Update zapewnia natychmiastową ochronę

Usługa Active Update umożliwia łatwe aktualizowanie szablonów zgodności z przepisami, modułów weryfikujących oraz aplikacji.

Ta nowa funkcja umożliwia obsługiwanie zmian w aplikacjach (np. komunikatorach czy internetowej poczcie elektronicznej) w celu zapewnienia natychmiastowej ochrony. Automatyczne aktualizacje pozwalają uniknąć opóźnień i przyspieszają wprowadzanie zmian w aplikacjach.

– *Obecny kryzys gospodarczy uzmysłowił firmom oraz organom administracji publicznej potrzebę ochrony danych osobowych i własności intelektualnej* – powiedział **Punit Minocha**, dyrektor działu ochrony danych w firmie Trend Micro. – *Wiedząc, że za znaczną część włamań do systemów w celu skradzenia danych odpowiadają osoby z wewnątrz, klienci poszukują rozwiązania, które wyeliminowałoby przypadkowe i celowe wycieki danych. Wahają się jednak przy wyborze z uwagi na złożoność tego rodzaju rozwiązań. Rozwiązanie LeakProof 5.0 przełamuje barierę złożoności, która dotychczas uniemożliwiała wdrażanie rozwiązań zapobiegających utracie danych*.

Nowe funkcje rozwiązania LeakProof 5.0 zapewniają mniejszą złożoność, lepszą ochronę danych i większą skalowalność:

- gotowe szablony dotyczące zapewniania zgodności z przepisami pomagają firmom w przestrzeganiu takich przepisów, jak PCI, HIPAA, GLBA czy SB1386;

[1] Centrum badań nad kradzieżami tożsamości (*Identity Theft Resource Center*), 2008 r.
[2] Ponemon Institute, badania z 2006 r. nt. zapobiegania utracie danych.

- filtry kontrolują obszary, w których może dojść do utraty danych: drukarki sieciowe, współużytkowanie plików w systemie Windows (opcja Windows File Sharing), funkcja „wytnij i wklej”, nagrywanie płyt DVD w programie Roxio/IE, aplikacje P2P, program Skype, aplikacja MS ActiveSync;
- kontrola urządzeń (numer seryjny), kontrola dostępu do opcji Windows File Sparing;
- zdalne wyodrębnianie „odcisków palców” w systemach plików i na platformie Sharepoint ułatwia wykrywanie danych;
- sprawniejsza obsługa i ulepszone procedury pozwalają uprościć wdrożenie;
- elastyczne opcje wdrażania obniżają koszty. Serwer LeakProof dostępny jest jako urządzenie lub programowe urządzenie wirtualne, które można wdrożyć na „prawdziwym” sprzęcie lub w środowisku wirtualnym;
- integracja z usługą katalogową Active Directory ułatwia wdrożenie i zarządzanie.

– *Prostota rozwiązania LeakProof bardzo mi odpowiada* – powiedział **Thomas Gonzalez**. – *Skorzystałem z szablonów zgodności z przepisami HIPAA i PCI, po czym musiałem zmodyfikować jedynie kilka pól, aby dostosować rozwiązanie do wymagań naszego środowiska. LeakProof nie stwarza żadnych problemów i nie wymaga podejmowania żadnych dodatkowych kroków. Wystarczy tylko określić punkty końcowe oraz urządzenia sprzętowe i blokada zostaje wprowadzona*.

Ceny i dostępność w Europie

Rozwiązanie Trend Micro LeakProof 5.0 pojawiło się w sprzedaży pod koniec czerwca 2009 r. Cena na jednego użytkownika zależy od liczby stanowisk. Ponadto obowiązują upusty zależne od zamawianej liczby egzemplarzy. Najniższa cena rocznej licencji na rozwiązanie LeakProof 5.0 Client Standard dla 251-500 stanowisk wynosi 39,85 EUR na użytkownika. Najniższa cena rocznej licencji na rozwiązanie LeakProof 5.0 Client Advanced dla 251-500 stanowisk wynosi 56,93 EUR na użytkownika. Aby obniżyć całkowity koszt posiadania (TCO), LeakProof Server w postaci programowego urządzenia wirtualnego jest oferowany bezpłatnie. Rozwiązanie to można wdrożyć na „prawdziwym” sprzęcie lub w środowisku zwirtualizowanym. Dostępne jest również sprzętowe urządzenie do zarządzania.

Obie wersje rozwiązania LeakProof zawierają oprogramowanie klienckie i serwer zarządzający. Oprogramowanie klienckie LeakProof 5.0 obsługuje systemy operacyjne Windows 2008, 2003, Vista oraz XP. Programowe urządzenie wirtualne z serwerem zarządzającym obsługuje środowisko ESX 3.5 firmy VMware. ■

Raport bezpieczeństwa Cisco 2009

Grzegorz Kantowicz

Rosnące zagrożenia dla bezpieczeństwa firm

Firma Cisco opublikowała raport bezpieczeństwa (Cisco 2009 Midyear Security Report), który wskazuje, że przestępcy internetowi coraz częściej działają podobnie do przedsiębiorstw – zapożyczają najlepsze strategie funkcjonujące w świecie biznesu i nawiązują między sobą współpracę partnerską, aby ich nielegalna działalność była jeszcze bardziej lukratywna.

Najnowszy raport bezpieczeństwa przygotowany przez firmę Cisco przedstawia niektóre z najpopularniejszych strategii technicznych i biznesowych wykorzystywanych przez przestępców do włamywania się do sieci firmowych lub stron internetowych, a także kradzieży danych osobowych oraz pieniędzy. Raport zawiera także zalecenia firmy Cisco w zakresie ochrony przed niektórymi nowymi rodzajami ataków. Zalecenia te obejmują pracowników, procesy oraz technologie i stanowią kompleksowe rozwiązanie umożliwiające zarządzanie ryzykiem. Raport zwraca także uwagę na konieczność zachowania podwyższonej czujności w celu ochrony przed niektórymi starszymi sposobami ataków, które są tak samo wyrafinowane i szeroko rozpowszechnione, jak nowsze zagrożenia.

Najważniejsze wnioski

- „Robak" Conficker, który zaatakował systemy komputerowe pod koniec ubiegłego roku wykorzystując luki w zabezpieczeniach systemu Windows, w dalszym ciągu się rozprzestrzenia. W czerwcu 2009 roku pod kontrolą Confickera znajdowało się kilka milionów komputerów.
- Przestępcy internetowi doskonale orientują się w bieżących wydarzeniach i wykorzystują je w maksymalnym stopniu. Po nadejściu w kwietniu fali grypy H1N1 („świńskiej grypy") cyberprzestępcy zapełnili sieć spamem, w którym reklamowano leki zapobiegawcze i umieszczano łącza do fałszywych aptek. Cyberprzestępcy będą często wykorzystywać najnowsze wydarzenia do przeprowadzania tego typu ataków. Choć wielu spamerów nieustannie wysyła bardzo dużo wiadomości, niektórzy – aby uniknąć wykrycia – działają na mniejszą skalę, lecz z większą częstotliwością ataków.
- Prezydent Barack Obama kładzie duży nacisk na wzmocnienie zabezpieczeń amerykańskich systemów komputerowych przez obecną administrację i zamierza współpracować ze społecznością międzynarodową oraz przedstawicielami sektora prywatnego nad możliwością wykorzystania innowacyjnych technologii do ograniczenia przestępczości komputerowej. Oczekuje się, że te działania wywrą znaczny pozytywny wpływ na branżę w nadchodzących miesiącach.

Główne zagrożenia

- **Botnety**
  Sieci kontrolowanych komputerów stanowią efektywny środek umożliwiający przeprowadzenie ataku. Właściciele botnetów coraz częściej wynajmują posiadane sieci innym przestępcom, którzy skutecznie wykorzystują zasoby tego typu do rozsyłania spamu i szkodliwego oprogramowania stosując model udostępniania oprogramowania jako usługi (*software as a service, SaaS*).
- **Spam**
  Spam, jako jeden z najbardziej popularnych sposobów dotarcia do milionów komputerów z wiadomościami zawierającymi slogany reklamowe lub łącza do szkodliwych stron www, pozostaje główną metodą rozpowszechniania „robaków" komputerowych i szkodliwego oprogramowania, a także blokowania ruchu w internecie. Aż 180 miliardów wiadomości zawierających spam jest rozsyłanych każdego dnia. Stanowi to około 90 proc. ruchu poczty elektronicznej na świecie.
- **„Robaki" komputerowe**
  Rosnąca popularność serwisów społecznościowych ułatwiła prowadzenie ataków tego typu. Istnieje większa szansa, że uczestnicy społeczności internetowych klikną łącza lub pobiorą treści wysłane pozornie przez ludzi, których znają i którym ufają.
- **Spamdexing**
  Wiele przedsiębiorstw wykorzystuje techniki optymalizacji dla wyszukiwarek internetowych, aby znaleźć się wyżej na liście wyszukiwanych haseł w Google i innych serwisach. Spamdexing, metoda polegająca na dołącza-

niu do stron www bardzo dużej liczby słów kluczowych, jest coraz częściej wykorzystywany przez cyber-przestępców, którzy usiłują udostępniać szkodliwe oprogramowanie jako oryginalne. Ponieważ wielu użytkowników ufa rankingom wiodących wyszukiwarek, mogą oni nieświadomie pobrać jeden z fałszywych pakietów oprogramowania.

- **Oszustwa przez SMS**
  Od początku roku 2009 każdego tygodnia pojawiają się co najmniej 2-3 nowe kampanie, których celem są urządzenia przenośne. Cisco opisuje szybko rosnące grono użytkowników rozwiązań mobilnych jako grupę, do której dotarcie stanowi „nową granicę oszustwa, którą z łatwością przekraczają przestępcy". Na całym świecie z telefonii komórkowej korzysta około 4,1 mld abonentów. Dzięki temu przestępca może wyjątkowo szeroko „zarzucić sieć" i osiągnąć wysoki zysk, nawet jeśli atak powiedzie się tylko w przypadku niewielkiego odsetka ofiar.
- **Zagrożenia wewnętrzne**
  Wiele osób straciło pracę z powodu ogólnoświatowej recesji. W efekcie tej sytuacji osoby z wewnątrz organizacji będą stanowić poważne zagrożenie dla przedsiębiorstw w nadchodzących miesiącach. Oszustwa mogą być popełniane przez podwykonawców lub osoby trzecie, a także przez obecnych i byłych pracowników.

– Bezpieczeństwo w internecie jest coraz większym wyzwaniem, w miarę jak przestępcy opracowują bardziej wyrafinowane metody włamywania się do sieci firmowych i kradzieży cennych danych osobowych. W naszych najnowszych ustaleniach uderzający jest wysoki stopień znajomości świata biznesu wśród przestępców, a także ich zdolności techniczne wykorzystywane do zwiększenia skali działania oraz unikania wykrycia. Przestępcy współpracują ze sobą nawzajem, wykorzystują lęki i zainteresowania użytkowników, a także coraz częściej używają legalnych narzędzi internetowych, w tym wyszukiwarek oraz modelu udostępniania oprogramowania jako usługi (SaaS). Niektórzy przestępcy w dalszym ciągu z powodzeniem stosują dobrze udokumentowane metody, które w ciągu ostatnich kilku lat były bagatelizowane z powodu przewagi nowych zagrożeń. Przestępcy szybko wykrywają słabe punkty zarówno w zabezpieczeniach sieci, jak i w psychice użytkowników. Dlatego przedsiębiorstwa muszą wdrażać coraz bardziej zaawansowane metody walki z przestępczością komputerową oraz zachować czujność i kontrolować wszystkie kanały, za pomocą których mogą zostać przeprowadzone ataki – powiedział **Patrick Peterson**, dyrektor ds. badań nad bezpieczeństwem w Cisco.

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**.


KOMUNIKACJA ELEKTRONICZNA 2010
z wersją na CD
1
2
4
5
7
8
*
0
• podręczny format
• nowa szata graficzna
• wysoki poziom merytoryczny i edytorski
• raport o stanie rynku telekomunikacyjnego
• publikacja dla wszystkich podmiotów sektora rynku gospodarczego
MSG MEDIA
ul. Stawowa 110
83-323 Bydgoszcz
tel. (052) 325 83 10
fax (052) 373 52 43
office@msgmedia.pl
www.techbox.pl
KATALOG
JUŻ W SPRZEDAŻY!

INFOTEL

wykorzystaj naszą wiedzę i doświadczenie

W branży działamy od 12 lat. Dzięki zgromadzonej wiedzy, współpracy z wybitnymi ekspertami, bazie danych, możemy w sposób profesjonalny i kompleksowy komunikować się z rynkiem.

- prestiżowa nagroda w konkursie o Laur INFOTELA

- kongresy

- fora ekspertów

- debaty

- konferencje

- serwisy internetowe

- publikacje drukowane

12 lat doświadczenia

o nowoczesnej komunikacji elektronicznej wiemy wszystko

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

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