MSG MEDIA

ISSN 1429-0200

INFOTEL

2/2009

INDEKS 345237

Cena 15 zł
(w tym 0% VAT)

kwartalnik – KWIECIEŃ/CZERWIEC NOWOCZESNA KOMUNIKACJA ELEKTRONICZNA

TELEKOMUNIKACJA • INFORMATYKA • TELEWIZJA

VIII Kongres INFOTELA

3-6 czerwca 2009 r.

Hotel ASTOR, Jastrzębia Góra

program – str. 2-3

Komunikacja elektroniczna

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

Patronat honorowy:

MINISTERSTWO INFRASTRUKTURY

KRRiT | KRAJOWA RADA RADIOFONII I TELEWIZJI

Anna Streżyńska
Prezes Urzędu
Komunikacji Elektronicznej

Patronat branżowy:

PIIT PIKE KIGEiT PIRC

Sponsorzy i Partnerzy:

emitel inea eutelsat COMMUNICATIONS

netia DIALOG telecom Więcej możliwości... upc

ZPAS GROUP Activis POLSKA SalesManager software

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

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

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

IV. KATEGORIE „ZŁOTY LAUR CZYTELNIKÓW INFOTELA":
- operator telefonii mobilnej i internetu mobilnego;
- operator telefonii i szerokopasmowego internetu stacjonarnego;
- operator satelitarny;
- operator telewizji kablowej;
- nadawca i dystrybutor telewizyjny;
- telewizyjny kanał tematyczny;
- witryna internetowa

XI edycja konkursu o
LAUR INFOTELA

INFOTEL 1997

MSG MEDIA

Patronat honorowy:

Ministerstwo Infrastruktury
Urząd Komunikacji Elektronicznej
Krajowa Rada Radiofonii i Telewizji

Uroczyste wręczenie LAURÓW INFOTELA nastąpi podczas VIII Kongresu INFOTELA na uroczystej Gali Komunikacji Elektronicznej w dniu 4 czerwca 2009 r.

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

eutelsat
COMMUNICATIONS

Cały świat w zasięgu ręki

Informacja, wiedza, rozrywka – via satellite

Tylko satelity Eutelsat zapewniają wyjątkowo bogatą ofertę
polskich i zagranicznych kanałów TV
oraz dostęp do szerokopasmowego Internetu na terenie całego kraju.

www.eutelsat.com

Program VIII KONGRESU INFOTELA
„Komunikacja elektroniczna – technologie i usługi: mobilność, cyfryzacja, kontent, multimedia”
3–6 czerwca 2009 r. – „Hotel ASTOR”
JASTRZĘBIA GÓRA

3 czerwca (środa)

15.00 – 19.00 Rejestracja uczestników Kongresu, wydanie akredytacji i materiałów kongresowych.

19.00 – 22.00 Kolacja.

20.00 – 23.00 Czas na relaks – basen, siłownia, solarium, itp.

20.00 – 24.00 Bowling – Turniej o Puchar Infotela – eliminacje.

4 czerwca (czwartek)

08.00 – 09.30 Śniadanie.

10.00 – 10.15 Otwarcie VIII Kongresu Infotela – ***Grzegorz Kantowicz*** – redaktor naczelny INFOTELA. (Sala Broadway).

10.15 – 10.45 **Parlamentarne prace legislacyjne w sferze komunikacji elektronicznej**
Antoni Mężydło – Sejmowa Podkomisja ds. Transportu Kolejowego, Łączności i Nowoczesnych Technik Informacyjnych.

10.45 – 12.00 **Dogonić Europę – Okrągły Stół Komunikacji Elektronicznej cz. I.**

Prowadzenie:

Grzegorz Kantowicz – MSG Media, ***Tomasz Kulisiewicz*** – Audytel

Poruszane zagadnienia:

- Główne bariery w rozwoju branży;
- Metody pobudzania inwestycji w rozwój infrastruktury komunikacji elektronicznej;
- Wykorzystanie środków UE na inwestycje IT.

Udział w dyskusji zapowiedzieli:

Witold Kołodziejski – Przewodniczący Krajowej Rady Radiofonii i Telewizji.
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.
Piotr Muszyński – Członek Zarządu, Telekomunikacja Polska.
Przemysław Kurczewski – Prezes Zarządu TP EmiTel.
Krzysztof Szydłowski – Prezes Zarządu, Wielkopolska Telewizja Kablowa.
Janusz Kosiński – Prezes Zarządu INEA.
Tomasz Żurański – Prezes Zarządu VECTRA.
Leszek Bujak – Dyrektor ds. Rozwoju ASTRA CEE.
Zbigniew Kądzielski – Dyrektor Instytutu Łączności.

12.00 – 12.30 Przerwa na kawę – sponsorowana przez **Telefonię DIALOG**.

12.30 – 13.45 **Dogonić Europę – Okrągły Stół Komunikacji Elektronicznej cz II.**

Prowadzenie:

Grzegorz Kantowicz – MSG Media, ***Tomasz Kulisiewicz*** – Audytel

Poruszane zagadnienia:

- Jak spójnie regulować konwergentny rynek komunikacji elektronicznej?
- Priorytety w kształtowaniu i regulowaniu rynku;
- Czy rynek komunikacji elektronicznej jest motorem napędowym dla całej gospodarki?

Uczestnicy dyskusji:

Magdalena Gaj – Podsekretarz Stanu w Ministerstwie Infrastruktury.
Witold Kołodziejski – Przewodniczący Krajowej Rady Radiofonii i Telewizji.
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.
Eugeniusz Gaca – Przewodniczący Sekcji Operatorów Telekomunikacyjnych KIGEiT.
Wojciech Dziomdziora – Kancelaria Prawna Cottyn Barbasiewicz Łyś-Gorzkowska i Dziomdziora.
Piotr Muszyński – Członek Zarządu, Telekomunikacja Polska.
Przemysław Kurczewski – Prezes Zarządu TP EmiTel.
Krzysztof Szydłowski – Prezes Zarządu, Wielkopolska Telewizja Kablowa.
Janusz Kosiński – Prezes Zarządu INEA.
Tomasz Żurański – Prezes Zarządu VECTRA.
Leszek Bujak – Dyrektor ds. Rozwoju ASTRA C.E
Zbigniew Kądzielski – Dyrektor Instytutu Łączności.

14.00 – 15.00 Lunch – sponsorowany przez **Eutelsat**.

15.30 – 16.30 Warsztaty biznesowe **MSG Media i Activis Polska** (warsztaty zamknięte) (Sala Berlin).

Równolegle (Sala Broadway).

15.00 – 15.30 **Technologie i rozwiązania software’owe dla realizacji multimedialnych usług komunikacji elektronicznej w czasie rzeczywistym i nierzeczywistym.**

Marek Lewandowski – Prokurent SalesManager Software.

15.30 – 16.00 **Ewolucja usług multimedialnych**
Marcin Gralewski – Dyrektor Biura Usług Telekomunikacyjnych TP EMITEL.

16.00 – 16.15 **Prezentacja INEA**

Maciej Janas – Członek Zarządu Grupy INEA ds. Marketingu i Sprzedaży.

16.15 – 16.30 **Rozbudowa infrastruktury sieciowej na potrzeby LLU – czy to się opłaca?**
Paweł Żytecki – Dyrektor Departamentu Rozwoju Sieci, NETIA.

17.00 – 19.00 Bowling – Turniej o Puchar Infotela – finał.

Siódmy ogólnopolski konkurs w rzucie komórką na odległość.

20.00 – 02.00 **Uroczysta Gala Komunikacji Elektronicznej –** sponsorowana przez **ZPAS**
(Sala Manhattan).

Rozstrzygnięcie XI ogólnopolskiej edycji Konkursu o LAUR INFOTELA.

W programie artystycznym wystąpią: **Electrica Duo – Kasia & Paula** oraz **Paweł Kluz** – iluzjonista.

5 czerwca (piątek)

08.00 – 10.00 Śniadanie.

10.00 – 14.00 Warsztaty biznesowe **Grupy INEA** (warsztaty zamknięte).
(Sala Berlin).

Równolegle (Sala Broadway).

10.00 – 11.30 **Nowe rodzaje treści i ich dystrybucji w kontekście cyfryzacji przekazów medialnych.**

Panel dyskusyjny poprowadzi ***Wojciech Apel*** – 3S Śląskie Sieci Światłowodowe

Poruszane zagadnienia:

- Nowe technologie dystrybucji treści w sieciach naziemnych.
- Inwestycje operatorów kablowych.
- Pojawienie się nowych operatorów z produktem telewizyjnym.
- Czy są granice w dostępie satelitarnym?
- Nowe możliwości sprzętu
- Telewizor jako terminal sieci Internet.
- Relacje nadawca-producent sprzętu bez udziału operatora.
- Nowe zachowania widzów
- Postmodernizm w mediach
- Zachowania internetowe
- Relacje nadawca-operator na rynku polskim.
- Czy istniejące powiązanie trzech polskich nadawców z trzema operatorami platform satelitarnych jest zagrożenie dla rynku operatorów kablowych?
- Czy DVB-T coś zmieni?

Udział w dyskusji zapowiedzieli:

Wojciech Dziomdziora – Kancelaria Prawna Cottyn Barbasiewicz Łyś-Gorzkowska i Dziomdziora.
Janusz Kosiński – Prezes Zarządu Grupy INEA.
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.

11.30 – 12.00 Przerwa na kawę – sponsorowana przez **Telefonię DIALOG.**

12.00 – 13.30 **Dylematy i rozdroża rozwoju infrastruktury telekomunikacyjnej NGN.**

Wprowadzenie:

Tomasz Kulisiewicz – Audytel, ***Marek Średniawa*** – Politechnika Warszawska.

Poruszane zagadnienia:

- NGN i usługi konwergentne – w czym rzecz?
- Aspekty regulacyjne komunikacji konwergentnej – nowe wyzwania.
- Problemy inwestycyjne budowy sieci NGN/NGA.
- Bariery rozwoju infrastruktury.

Dyskusja:

„Co i jak można zrobić? – próba konstruktywnego spojrzenia ponad podziałami”.

Udział w dyskusji zapowiedzieli:

Marzena Śliz – Doradca Prezesa Urzędu Komunikacji Elektronicznej**.**
Eugeniusz Gaca – Przewodniczący Sekcji Operatorów Telekomunikacyjnych KIGEiT.
Jarosław Janiszewski – Prezes Zarządu HAWE.
Zbigniew Kądzielski – Dyrektor Instytutu Łączności.

13.30 – 13.40 **Podsumowanie i zamknięcie VIII Kongresu Infotela**.

14.00 – 15.00 Lunch.

15.00 – 20.00 **Biznes i rekreacja.**

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

20.30 – 01.00 Grillowanie na polanie sponsorowane przez firmę **Activis Polska**.

Wręczenie pucharów i nagród zwycięzcom konkursów w rzucie komórką na odległość oraz Turnieju o Puchar Infotela w bowlingu.

6 czerwca (sobota)

08.00 – 09.30 Śniadanie.

09.30 – 11.30 Czas wolny.

12.00 – 13.00 Wyjazd uczestników Kongresu.

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

INFOTEL 1997

INDEKS 345237
numer 2 (102), rok dziesiąty
kwiecień/czerwiec 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

Telekomunikacja

Neofon tp także na kartę

Telekomunikacja Polska rozszerzyła dotychczasową ofertę VoIP o usługę neofon na kartę, czyli możliwość korzystania z telefonii internetowej bez konieczności podpisywania umowy. Starter neofon tp zawiera indywidualny numer z zakresu 0399-XXX-XXX, z którego od razu można dzwonić wykorzystując na rozmowy całość kwoty zakupu, czyli 5 zł brutto. Numer jest aktywny przez 90 dni. Za pomocą karty zdrapki o nominałach: 5, 10, 30, 50 i 100 złotych, można doładować konto i przedłużyć aktywację numeru na kolejny okres, od 7 do 360 dni. By korzystać z neofonu nie trzeba mieć linii telefonicznej, wystarczy dowolny dostęp do internetu o prędkości co najmniej 128 kb/s i aplikacja typu softphone, którą można pobrać ze strony www.tp.pl. Z neofonu można korzystać również poprzez komunikator internetowy SPIK, telefon IP (dostępne w ofercie TP), softphone oraz telefon komórkowy obsługujący protokół komunikacji SIP.

Zarządzanie sieciami optycznymi nowej generacji

Na XI konferencji International Conference on Transparent Optical Networks (ICTON 2009) Comarch zaprezentuje „Platformę do zarządzania sieciami optycznymi nowej generacji". Jest ona rozwijana w ramach projektu MANGO i współpracy Comarch z firmami (TeliaSonera, Szwecja; Proximion, Szwecja), instytutami badawczymi (Acreo, Szwecja) oraz uniwersytetami (Królewski Instytut Technologii, Szwecja; Politechnika Warszawska), która odbywa się w ramach programu Eureka/Celtic. Taka współpraca gwarantuje, że proponowana platforma odpowie na oczekiwania operatorów oraz opiera się na najnowszych osiągnięciach. Platforma pomaga operatorom zarządzać komponetami oraz narzędziami potrzebnymi do tworzenia sieci optycznych (takimi jak włókna, ODFs, EDFA, SOA, ROADM, OXC's oraz inne). Pozwala to również na wielowarstwowe, zautomatyzowane zarządzanie wydajnością i błędami, Service Quality Management oraz zarządzanie połączeniami optycznymi.

Ruszyło „Krajowe Forum Szerokopasmowe"

Oddany do dyspozycji został zapowiadany przez Prezesa UKE portal „Krajowe Forum Szerokopasmowe" (*www.forumszerokopasmowe.pl*). Podstawowym celem działania Krajowego Forum Szerokopasmowego jest zbudowanie platformy komunikacji pomiędzy środowiskami dla których ważny jest rozwoju dostępu do usług szerokopasmowego Internetu w Polsce i aktywizacja społeczeństwa w tym zakresie. Portal adresowany jest do jednostek samorządu terytorialnego, jako potencjalnych inwestorów w budowę nowoczesnych sieci szerokopasmowych oraz osób szukających optymalnych rozwiązań technologicznych dla realizacji tych inwestycji. Forum ma się stać źródłem informacji związanych z przygotowaniem planów budowy i funkcjonowaniem sieci szerokopasmowej.

Ogólnopolski easyCALL

easyCALL w ostatnim czasie systematycznie poszerzał grupę obsługiwanych przez siebie stref lokalnych. Proces ten miał naturalny kres – mianowicie wprowadzenie obsługi wszystkich, czterdziestu dziewięciu lokalnych stref numeracyjnych. Ostatnimi przyłączonymi strefami były strefy nowosądecka (018), pilska (067) oraz trzy dolnośląskie – wałbrzyska (074), jeleniogórska (075) i legnicka (076), w których numeracja została udostępniona klientom operatora piątego maja 2009 roku. easyCALL umożliwia także przenoszenie numerów od innych operatorów, we wszystkich strefach, w których obecnie posiada numerację. Abonenci którzy nie zamierzają korzystać z numerów lokalnych, mogą zaś w easyCALL wybrać numerację niegeograficzną 0-39, na którą z dowolnego miejsca w kraju dzwoni się po stawce połączenia lokalnego.

Dzwoń i oglądaj reklamy

Na polskim rynku pojawił się zupełnie nowatorski serwis – Reklamofon.pl, który działa na platformie telekomunikacyjnej firmy TeleKontakt24 (www.telekontakt24.pl). Serwis umożliwia całkowicie bezpłatne telefonowanie na dowolny numer stacjonarny w Polsce i za granicą. Wszelkie koszty połączeń pokrywane są przez reklamy wideo wyświetlane na ekranie monitora w trakcie trwania rozmowy. Aby reklamy w czasie rozmowy nie były ignorowane co jakiś czas, obok reklam pojawia się specjalny migający zegar odmierzający sekundy. Jeżeli przed upływem 10 sekund użytkownik nie kliknie w zegar, jego połączenie zostaje zakończone.

Korzystajmy z bezpłatnych książek telefonicznych

Prezes Urzędu Komunikacji Elektronicznej opublikował komunikat na temat baz danych abonentów dostępnych w ramach usług OSA i OBN. W zamieszczonym na stronie internetowej komunikacie prezes UKE przypomina, że Telekomunikacja Polska zobowiązana jest do świadczenia **usług ogólnokrajowej informacji o numerach telefonicznych** (OBN) oraz **ogólnokrajowego spisu abonentów** (OSA). **Każdy użytkownik publicznej sieci telefonicznej, w tym użytkownik aparatów publicznych, ma prawo do otrzymania bezpłatnego OSA w formie drukowanej, na nośnikach elektronicznych lub w obu formach.** Uprawnieniem użytkownika jest możliwość otrzymania – jednego pełnego OSA, bądź po jednym egzemplarzu wybranych przez niego tomów tak w formie drukowanej, jak i elektronicznej.

Contact Center dla małych i średnich przedsiębiorstw

NextiraOne Polska we współpracy z firmą Genesys przygotowała interaktywną platformę NextiraOne SIP! To oparte o standardy branżowe rozwiązanie Contact Center umożliwia wdrożenie systemu wielokanałowej obsługi klienta w ciągu kilku dni. NextiraOne SIP! to pakiet zawierający cały niezbędny sprzęt i oprogramowanie Contact Center wraz z aplikacją biznesową konsultanta. System oparty jest na protokole SIP (*Session Initiation Protocol*), dzięki czemu profesjonalne Contact Center – bez konieczności ponoszenia wydatków na użytkowanie drogich i zamkniętych systemów telefonicznych (PBX) – będą mogły posiadać nawet małe firmy. Jest to szczególnie istotne w czasach spowolnienia gospodarczego, ponieważ umożliwia inwestowanie zaoszczędzonych środków w dalszy rozwój firmy, podnosząc tym samym jej konkurencyjność na rynku.

Technologia HSPA do 56 Mb/s

Na wystawie CTIA Wireless, która odbyła się w dniach 1-3 kwietnia 2009 w Las Vegas, Ericsson po raz pierwszy zademonstrował technologię HSPA multi-carrier połączoną z technologią MIMO, która umożliwia pobieranie danych z prędkością 56 Mb/s. To kolejny ważny krok w rozwoju technologii HSPA i mobilnej komunikacji szerokopasmowej. Nowy rekord prędkości został osiągnięty dzięki połączeniu dwóch technologii – MIMO (ang. *multiple-input-multiple-output*) oraz HSPA multi-carrier. Pierwsza z nich zwiększa szczytową prędkość przesyłania danych i efektywność spektralną, a tym samym – przepustowość sieci. Obecnie trwają prace nad standaryzacją technologii HSPA multi-carrier połączonej z MIMO, a jej wersja komercyjna ma zostać wprowadzona na rynek w 2010 r. Do końca 2009 r. Ericsson będzie obsługiwał komercyjne wdrożenia technologii multi-carrier o maksymalnej prędkości 42 Mb/s, którą z powodzeniem przedstawił na ostatniej konferencji Mobile World Conference w Barcelonie.

Rynek

Dobry początek roku dla Netii

Netia SA ogłosiła wyniki finansowe za I kwartał 2009 roku. Według podanych danych przychody z działalności kontynuowanej Netii wzrosły do poziomu 375,7 mln PLN tj. o 64 proc. w porównaniu do I kw. 2008 r. oraz o 2 proc. wobec IV kw. 2008 r. EBITDA wyniosła 69,9 mln PLN, co stanowiło wzrost o 107 proc. w stosunku do I kw. 2008 r. oraz o 21 proc. w porównaniu z IV kw. 2008 r. W I kw. 2009 r. Netia rozpoczęła realizację kompleksowego programu redukcji kosztów pod nazwą „Profit". Jego celem jest redukcja, począwszy od 2010 r., kosztów operacyjnych o 100 mln PLN w skali roku. Przewidywane oszczędności, uzyskane w wyniku tej inicjatywy w 2009 r. to około 20 mln PLN. Netia rozwija usługi oparte na dostępie do lokalnej pętli abonenckiej (LLU), zarówno dla klientów indywidualnych, jak i biznesowych. Planuje również migrację klientów na usługi LLU – zakończono fazę testową, poprzedzającą ten proces. Począwszy od II kw. 2009 r. spółka planuje przenieść do końca 2009 r. ponad 20.000 klientów BSA i BSA+WLR na LLU.

Inwestycje w IT w czasie kryzysu

Jak wynika z najnowszych badań D-Link Technology Trend co trzecia polska firma (30 proc.) zamierza zrealizować przyjęte wcześniej plany inwestycyjne w IT. Jednocześnie niemal tyle samo firm (31 proc.) deklaruje, że kryzys wstrzymał na razie ich inwestycje, które muszą być odłożone na przyszłość. Rezygnację z niektórych, wcześniejszych planów zapowiada co szósta firma (17 proc.). Jednak, co optymistyczne, niemal tyle samo firm (18 proc.) nie chce poddawać się

recesji i rezygnować z planów. Te przedsiębiorstwa będą szukać alternatywnych, tańszych produktów i usług, które umożliwią realizację wcześniejszych założeń inwestycyjnych przy trudniejszej sytuacji rynkowej. A jak te deklaracje przekładają się na budżety? Wzrost wydatków na inwestycje IT w porównaniu z rokiem 2008 planuje zaledwie 3 proc. polskich firm MŚP. Ponad jedna trzecia (36 proc.) deklaruje ograniczenie budżetu w porównaniu z rokiem ubiegłym. Jednak zdecydowana większość przedsiębiorców (61 proc.) zamierza utrzymać poziom wydatków z 2008 roku.

UKE zachęca inwestorów

W dniach 28-29 kwietnia przedstawiciele UKE odbyli w Londynie szereg spotkań z liczącymi się funduszami inwestycyjnymi oraz inwestorami branżowymi. Celem tego spotkania było przedstawienie możliwości inwestycyjnych na polskim rynku telekomunikacyjnym. Urząd Komunikacji Elektronicznej przedstawiał m.in. informację dotyczącą warunków przetargu na zakresy częstotliwości dla budowy mobilnych sieci szerokopasmowych w paśmie 2,5-2,69 GHz. Z dużym zainteresowaniem inwestorów spotkała się inicjatywa Prezesa UKE związana z przygotowaniem projektu Ustawy o wspieraniu rozwoju usług i sieci szerokopasmowych. Ustawa ta po wejściu do stosowania w znacznym stopniu usprawni procesy inwestycyjne i przyczyni się do rozwoju dostępu do nowoczesnych usług telekomunikacyjnych. Spotkania z inwestorami będą kontynuowane. Aktualnie przygotowywana jest nowa misja inwestycyjna skierowana do inwestorów z Azji.

Pieniądze na e-doradztwo

Ponad 66 mln zł – taką kwotę MSWiA przeznaczy na usługi doradcze dla projektów informatycznych, m.in. ePUAP2 oraz PL.ID. Zdaniem Witolda Drożdża, wiceministra spraw wewnętrznych i administracji, profesjonalne doradztwo jest niezbędne w procesie skutecznej budowy i wdrażania dużych systemów informatycznych. Stanowi również standardowy element projektów realizowanych przy współudziale środków unijnych, de facto niezbędny do efektywnej realizacji szeregu wymogów stawianych przez Komisję Europejską. 7 kwietnia zawarto umowę ramową, określającą zasady świadczenia usług doradczych w zakresie projektów realizowanych przez Centrum Projektów Informatycznych MSWiA. Umowa została zawarta z sześcioma Wykonawcami:

- Konsorcjum firm: Krajowa Agencja Informacyjna „INFO" Sp. z o.o. oraz Zakład Elektronicznej Techniki Obliczeniowej w Olsztynie Sp. z o.o.,
- Konsorcjum firm Ernst & Young Business Advisory spółka z o.o. i Wspólnicy sp. k., Ernst & Young Corporate Finance spółka z o.o., Pentegy S.A., Infostrategia – Krzysztof Heller i Andrzej Szczerba Spółka Jawna, Stowarzyszenie „Miasta w Internecie" oraz Nizielski & Borys Consulting Spółka Jawna.
- Konsorcjum firm: ComArch S.A., CA Services Spółka Akcyjna oraz PwC Polska Sp. z o.o.
- Konsorcjum firm KPMG Advisory Spółka z o.o. sp. k. oraz ITTI Spółka z o.o.
- Firma UNIZETO TECHNOLOGIES S.A.
- Firma INFOVIDE MATRIX S.A.

Oznacza to, iż każdorazowo CPI MSWiA będzie zapraszało każdego z tych Wykonawców do składania ofert w postępowaniach szczegółowych – wyjaśnia resort. Postępowania szczegółowe dotyczyć będą świadczenia usług doradczych w konkretnych projektach, w zakresie np. planowania projektów, analizy wymagań, opracowania architektury, opracowania dokumentacji, ewentualnych zmian w przepisach prawa dotyczących obszarów działania prowadzonych projektów.

Dostęp do internetu szerokopasmowego

Urząd Komunikacji Elektronicznej opublikował analizę dotyczącą rynku szerokopasmowego, udziałów operatorów na tym rynku oraz technologii dostępu do sieci Internet w Polsce. Zdaniem UKE pomimo niskiego miejsca w rankingu europejskim, rynek dostępu do internetu szerokopasmowego w Polsce jest obecnie jednym z najprężniej rozwijających się segmentów telekomunikacji, a rok 2008 i początek 2009 to dalszy jego rozwój. Oprócz utrzymującego się trendu wzrostu nasycenia rynku usługami szerokopasmowymi charakterystyczny dla rynku dostępu szerokopasmowego jest również inny trend. Podmioty świadczące usługi dostępu do sieci internet powoli zmieniają swój charakter – zarówno w Polsce jak i w pozostałych krajach UE. Do niedawna były to przede wszystkim tradycyjni operatorzy stacjonarni, natomiast obecnie coraz większy udział w tym rynku stanowią lokalni ISP, telewizje kablowe oraz operatorzy telefonii ruchomej. Wszystkie te podmioty oferują coraz więcej usług, w tym usług wiązanych – oferując na przykład dodatkowo usługi głosowe (w tym VoIP) lub telewizję. Nadal jednak poziom usług szerokopasmowych w Polsce na tle innych krajów UE pozostawia jeszcze wiele do życzenia.

Telestar da kontent dla telewizji mobilnej

Spółka medialna Telestar z grupy MNI ma umowę z Info-TV-FM, które wygrało konkurs na operatora telefonii mobilnej, poinformował prezes Witold Laskowski. Dzięki temu program telewizyjny iTV będzie jednym z pierwszych dostępnych w tej usłudze. Telestar przedstawił we strategię dzięki której jego kanał telewizyjny iTV ma zwiększyć na koniec roku oglądalność w grupie docelowej (16-49 lat) do 0,50 proc z 0,15 proc obecnie. Efekt ma zostać osiągnięty dzięki nowej ramówce i nowym audycjom własnym.

Bezpieczeństwo

Patent na technologię ochrony integralności danych

Kaspersky Lab uzyskał amerykański patent dla swojej zaawansowanej technologii umożliwiającej wykrywanie nieautoryzowanych modyfikacji danych. Nieautoryzowane modyfikacje danych, zarówno przypadkowe, jak i celowe, powodują uszkodzenie lub utratę danych. Nieautoryzowana modyfikacja kodu oprogramowania może przyczynić się do błędów w wykonaniu programu. Powszechnie wiadomo, że większość programów crimeware wstrzykuje kod do plików wykonywalnych, co powoduje wykonanie szkodliwego kodu podczas uruchomienia zainfekowanych plików. Z tego powodu zapewnienie integralności danych jest głównym wyzwaniem dla bezpieczeństwa IT. Zaawansowana technologia opracowana przez Michaiła Pawluszikowa z Kaspersky Lab szybko i skutecznie sprawdza integralność plików, bez pochłaniania znaczącej ilości zasobów. Patent nr 7 526 516 został przyznany tej technologii przez amerykański Urząd Patentów i Znaków Towarowych 28 kwietnia 2009 roku.

Monitorowanie bezpieczeństwa środowisk IT

Firma APC by Schneider Electric zaprezentowała nową generację rozwiązania NetBotz®, służącego do monitorowania bezpieczeństwa środowisk IT. Najważniejsze udoskonalenia linii produktów NetBotz to większe wsparcie kamer i okablowania, wsparcie technologii Power over Ethernet oraz ulepszona funkcjonalność i wygląd. NetBotz to rodzina urządzeń sieciowych wykrywających i informujących o ludzkiej aktywności mogącej zagrażać dostępności fizycznej infrastruktury sieciowej o znaczeniu krytycznym. Modułowość tego rozwiązania, skalowalnego od małych szaf sieciowych, przez duże centra danych aż po wdrożenia na skalę przemysłową, pozwala na konfigurację kamer dostosowaną do potrzeb klienta, w tym integrację z kamerami przemysłowymi.

Ponad 90 proc. wiadomości to spam

Firma Panda Security opublikowała kwartalny raport dotyczący przesyłanych do firm wiadomości spamowych. Niepożądana korespondencja pochodziła głównie ze Stanów Zjednoczonych, ale aktywna była również Polska, zajmując szóste miejsce pod względem udziału w produkcji spamu. Analizy wykazały dodatkowo, iż między styczniem a marcem 2009 r. międzynarodowa grupa hakerów zainfekowała ponad 300 tys. komputerów w celu ich dalszego wykorzystywania do rozsyłania złośliwych e-maili. W pierwszym kwartale 2009 r. firma Panda Security przeprowadziła analizę 69 milionów wiadomości, odbieranych przez firmowe konta pocztowe. Badania wykazały, iż tylko 7 proc. e-maili trafiających do firm stanowiło prawidłową korespondencję. Aż 90,92 proc. z nich zawierało spam, natomiast 1,66 proc. było zainfekowanych złośliwym oprogramowaniem. Ilość spamu wykrytego między styczniem a marcem 2009 r. wzrosła nieznacznie w porównaniu z analogicznym okresem ubiegłego roku, kiedy to spam stanowił 89,88 proc. wiadomości otrzymywanych przez firmy.

Panda USB Vaccine

Jest to bezpłatna aplikacja mająca na celu blokowanie złośliwych kodów, które rozprzestrzeniają się za pomocą przenośnych dysków,

m.in. pendrive'ów, płyt CD/DVD czy odtwarzaczy MP3.Według danych z laboratorium Panda Security coraz więcej złośliwych kodów, takich jak np. niebezpieczny robak Cornficker, rozprzestrzenia się za pomocą dysków i urządzeń przenośnych, m.in. memory sticks, odtwarzaczy MP3 czy aparatów cyfrowych. Jest to bezpłatne rozwiązanie, które pozwala użytkownikowi zablokować funkcję AutoRun zarówno na swoim komputerze, jak również na dyskach USB i innych urządzeniach.

Panda GateDefender Performa 9000

Panda Security wprowadziła nową serię urządzeń Panda GateDefender Performa 9000 zapewniających maksymalną ochronę styku sieci firmowej z internetem. Rozwiązanie blokuje przedostające się z witryn www złośliwe kody, spam oraz wszelkie niepożądane treści. Nowa seria urządzeń została zbudowana w oparciu o platformę sprzętową Sun Microsystems, co pozwoliło zwiększyć wydajność i skuteczność rozwiązania.

Fortinet chroni sieć Lotto

Veracomp SA, wyłączny dystrybutor produktów Fortinet w Polsce, dostarczył wraz z integratorem bezpieczne.it sprzęt do zabezpieczenia sieci informatycznej Totalizatora Sportowego. Rozwiązanie oparte na produktach FortiGate, FortiManager oraz FortiAnalyzer ma za zadanie chronić infrastrukturę sieciową we wszystkich placówkach na terenie naszego kraju. Główne korzyści ze zmian, to oszczędności i gwarancja ciągłości działania aplikacji. Wdrożenie, które koordynowała firma bezpieczne.it, obejmowało uruchomienie zabezpieczeń w sieci WAN dla Totalizatora Sportowego w całej Polsce. W skład rozwiązania weszły: klaster urządzeń FortiGate, FortiManager, oraz FortiAnalyzer dla centrali oraz dwadzieścia mniejszych urządzeń FortiGate dla lokalizacji terenowych. Wdrożenie trwało zaledwie 3 tygodnie od momentu wyłonienia wykonawcy.

Telewizja

Udany start Pinotv.pl

W dwa tygodnie po uruchomieniu pierwszej polskiej platformy telewizyjnej 2.0 Grupy Pino (spółki zależne giełdowej Internet Group) stworzono 120 autorskich kanałów telewizyjnych. Z pierwszych obserwacji wynika, że kanały popularno-naukowe mają szansę stać się hitem platformy telewizyjnej. Uczniowie preferują ten sposób zdobywania wiedzy, która jest przekazywana w sposób prosty i interesujący. Kanał Nowy Pitagoras jest szeroko komentowany przez obserwatorów internetu i inne media, czego dowodzą wpisy TVN24 czy Wykop.pl. PinoTV – telewizja 2.0 – łączy telewizję ze znanym trendem Web 2.0, w którym treści generowane są przez samych użytkowników. Takie narzędzie umożliwia współdzielenie emocji wytwarzających się pomiędzy widzami oglądającymi wybrany kanał.

Eska TV – nowy kanał telewizji muzycznej

Radio ESKA – uruchamia telewizyjną stację muzyczną. ESKA TV – nowa telewizja muzyczna podobnie jak sieć radiowa ESKI profilowana będzie jako „Hity na czasie". W ESKA TV pojawią się między innymi uwielbiane gwiazdy Radia ESKA: Jankes, Puoteck oraz Kinga Zdrojewska. Stacja ESKA TV startuje ekskluzywnie na paltformie telewizji nowej generacji n. ESKA TV i n-ka zapowiadają szeroko zakrojone wspólne działania reklamowe. Partnerami ESKA TV będą między innymi ONET.PL oraz Multikino. Sprzedaż czasu reklamowego prowadzona będzie jak w wypadku wszystkich produktów ESKA przez TIME SA.

TVP Sport w CYFRZE+

Platforma cyfrowa CYFRA+ wzbogaca ofertę programową o kolejny kanał sportowy – TVP Sport. Na mocy podpisanej umowy kanał jest dostępny dla abonentów platformy od 6 maja br. TVP Sport to przede wszystkim transmisje ze światowych i krajowych wydarzeń sportowych. Kluczowymi dyscyplinami kanału są: piłka nożna, lekkoatletyka, żużel, koszykówka, hokej na lodzie, piłka ręczna, pływanie oraz pełna gama sportów zimowych. Na antenie TVP Sport obecne są również sporty motorowe, tenis ziemny, sporty walki, golf i zawody hippiczne.

Trzy wymiary w kamerze Panasonic

Firma Panasonic, lider technologii High Definition, ogłosiła rozpoczęcie prac nad profesjonalnym system produkcji trójwymiarowego obrazu. System, który jest pierwszym tego rodzaju rozwiązaniem w branży, będzie składać się z profesjonalnej dwuobiektywowej kamery typu P2 oraz kompatybilnego z obrazem 3D wyświetlacza plazmowego. Panasonic przedstawił modele koncepcyjne systemu 3D podczas kwietniowych targów NAB w Las Vegas. Produkcja trójwymiarowych tytułów wymaga dużych nakładów finansowych i czasowych. Proponowany przez Panasonic system produkcyjny umożliwi łatwiejszą i bardziej wydajną produkcję materiału 3D. Tym samym firma Panasonic przyczyni się do popularyzacji produkcji realizowanych w technologii 3D.

Nowy kanał telewizyjny TP

Telekomunikacja Polska uruchamia kolejny kanał telewizyjny – Orange sport info. To pierwszy polski sportowy kanał informacyjny na rynku. W odróżnieniu od Orange sport, będzie kanałem „free-to-air", przeznaczonym do bezpłatnej dystrybucji. Prócz serwisów informacyjnych, które będą głównym elementem ramówki Orange sport info, w programie znajdą się też magazyny, wywiady i komentarze – będą to zarówno własne, autorskie programy jak i materiały producentów zewnętrznych. Ponadto, codziennie od poniedziałku do piątku, zaplanowana jest wieczorna rozmowa ze specjalnym gościem. Kanał telewizyjny Orange sport info będzie w części programowo powiązany z Orange sport, którego głównym atutem są transmisje na żywo piłkarskiej ekstraklasy. Podczas gdy transmisję meczów będzie można oglądać tylko w Orange sport, materiały towarzyszące spotkaniom – czyli wywiady, opinie, analizy, podsumowania – będą nadawane również przez Orange sport info.

Multimedia

Sieć na gniazdkach telewizji kablowej

NETGEAR wprowadził do sprzedaży w Ameryce Północnej zestaw **MoCA® Coax-Ethernet Adapter Kit (MCAB1001)** zaprojektowany do przesyłania strumieniowego wideo HD, multimediów i podłączania urządzeń z wyjściami Ethernet: odbiorników TV HD, odtwarzaczy Blu-ray™, cyfrowych nagrywarek wideo i konsol do gier do domowych sieci LAN i Internetu. Zestawy MoCA Coax-Ethernet Adapter Kit mogą być wykorzystywane z bezprzewodowymi lub przewodowymi routerami i bramkami. Urządzenia pozwalają tworzyć sieci na bazie istniejącego okablowania telewizji kablowej wykorzystującej kabale koncentryczne. estaw NETGEAR MoCA Coax-Ethernet Adapter Kit, dzięki doskonałym właściwościom transmisyjnym kabli koncentrycznych, izolowanym i ekranowanym o małym współczynniku zniekształceń oraz dużej przepustowości standardu MoCA 1.1, spełnia nawet najbardziej rygorystyczne potrzeby transmisji przez domowych użytkowników.

Linuksowy Moblin na każdym urządzeniu przenośnym

Firmy Intel Corporation i Novell Inc. poinformowały o podpisaniu umowy o współpracy mającej na celu doprowadzenie do szerokiego stosowania przez producentów komputerów i projektantów sprzętu systemu Moblin (zobacz: www.moblin.org). Jest to zoptymalizowany pakiet oprogramowania linuksowego i zestaw technologii zapewniający możliwość korzystania z bogatych multimedialnych treści internetowych na urządzeniach z procesorami Intel Atom, takich jak komputery kieszonkowe, netbooki i nettopy, samochodowe systemy informacyjno-rozrywkowe (IVI) oraz systemy wbudowane.

Multimedialny router

Na polskim rynku pojawił się pierwszy wielofunkcyjny router D-Linka przeznaczony do sieci domowych. Bezprzewodowy DIR-685, pracujący w drafcie standardu 802.11n, oprócz swej podstawowej funkcjonalności – dzielenia łącza internetowego – pełni rolę multimedialnej biblioteki w cyfrowym domu. Urządzenie posiada wbudowaną pamięć masową (NAS), służącą do przechowywania różnego rodzaju plików oraz ekran LCD, który pozwala na wyświetlanie komunikatów i zdjęć oraz na transmisje filmów video. Stylowy design sprawia, że router DIR-685 świetnie wkomponowuje się w wystrój każdego domu. Urządzenie D-Linka, pracuje w najnowszym drafcie standardu 802.11n, co zapewnia pełniejsze pokrycie sygnałem radiowym oraz

zdecydowanie wyższą przepustowość danych w porównaniu z urządzeniami starszej generacji.

Internet

Wielki popyt na e-PITy

System elektronicznych deklaracji podatkowych podpisywanych kwalifikowanym podpisem elektronicznym Ministerstwo Finansów wprowadziło już w zeszłym roku. Z rozwiązania tego na szeroką skalę skorzystały firmy. Natomiast wśród osób fizycznych akceptacja tej formy rozliczania się z Urzędem Skarbowym była prawie zerowa – właśnie ze względu na konieczność posiadania e-podpisu. Roczne zeznania podatkowe za pośrednictwem e-Deklaracji złożyło wówczas jedynie 419 osób. Wychodząc naprzeciw potrzebom tej ostatniej grupy użytkowników w bieżącym roku Ministerstwo Finansów przygotowało i udostępniło aplikację do składania zeznań podatkowych drogą elektroniczną bez e-podpisu. Zmiana ta szeroko otworzyła furtkę indywidualnym podatnikom – przez internet swoje PIT'y wysłało aż 89 000 osób.

Superszybki internet w kablówkach

Być może niebawem największe sieci kablowe będą oferować internet nawet z przepustowościami powyżej 100 Mbit/s. Wszystko za sprawą standardu transmisji danych DOCSIS 3.0 – który właśnie jest testowany także w Polsce. Jak podaje wortal PasjaGSM.pl – wszystko wskazuje na to, że w ciągu roku do oferty sieci kablowych zostaną wprowadzone superszybkie łącza internetowe. DOCSIS 3.0 jest testowane w największych polskich sieciach kablowych – UPC, Multimedia, Vectra oraz wielu innych. Jest on jest kolejną wersją funkcjonującego w sieciach kablowych standardu systemów szybkiej transmisji danych (*Data Over Cable System Interface Specification*).

Sam standard jest jeszcze niedopracowywany – dostawcy zapowiadają, że w przyszłym roku pojawią się odpowiednie technologie, które umożliwią transmisję danych z prędkościami do 160 Mbit/s ściągania danych oraz do 120 Mbit/s wysyłania.

Brak motywacji do korzystania z sieci

Podstawową barierą upowszechnienia informatyzacji nie jest dostęp do Internetu, a umiejętności i motywacje do korzystania z sieci – uważa dr Dominik Batorski, autor analiz dotyczących wykorzystania Internetu przez Polaków. Podczas konferencji dla samorządowców, która odbyła się na początku kwietnia w Warszawie, dr Batorski przypomniał najważniejsze wyniki badań, realizowanych przez CBOS od 2000 r. Wynika z nich, iż wiele osób nie korzysta z nowych technologii, mimo posiadania dostępu do nich we własnym gospodarstwie domowym. Aż ponad 16 proc. Polaków, to osoby które mają w domu komputer, a w ogóle z niego nie korzystają. W przypadku internetu, aż 11 proc. ma dostęp w domu, a mimo to z sieci nie korzysta. Zdaniem Dominika Batorskiego, to nie dostęp jest podstawową barierą upowszechniania informatyzacji, a umiejętności i motywacje do korzystania z internetu.

Regulacje

Netia ukarana za winy Tele2

Kara została nałożona w związku z niewypełnianiem, jeszcze w czerwcu i wrześniu 2008 roku, przez Tele2 Polska warunków zapewnienia dostępu telekomunikacyjnego, które było naruszeniem ustalonych w decyzjach Prezesa UKE zasad wzajemnej współpracy między przedsiębiorcami telekomunikacyjnymi i prowadziło do naruszania interesów użytkowników końcowych. Użytkownicy końcowi zostali bowiem narażeni na wydłużenie procedury przenoszenia numeru lub pozbawieni możliwości skorzystania z uprawnienia do przeniesienia przydzielonego numeru przy zmianie operatora.

Prezes Urzędu Komunikacji Elektronicznej wydał decyzję nakładającą na Netię, jako następcę prawnego Tele2 Polska, karę pieniężną w wysokości 300 000 złotych.

Cyfrowy Polsat ukarany

Prezes Urzędu Komunikacji Elektronicznej nałożył na Cyfrowy Polsat karę pieniężną w wysokości 300 000 złotych za niespełnienie obowiązku udzielenia informacji i dostarczenia dokumentów żądanych w treści zawiadomienia o wszczęciu kontroli. Kontrola UKE dotyczyła przestrzegania przez Cyfrowy Polsat obowiązków w sprawie trybu postępowania reklamacyjnego oraz warunków, jakim powinna odpowiadać reklamacja usługi telekomunikacyjnej, które to zasady powinny być zawarte w stosownych regulaminach.

Cyfrowy Polsat stwierdził iż dostarczanie abonentom programów radiowych i telewizyjnych nie jest usługą telekomunikacyjną, a zatem nie ma dla tych usług regulaminów, umów i cenników usług telekomunikacyjnych. Zdaniem UKE, charakter działalności Cyfrowego Polsatu objęty przedmiotem kontroli polega na świadczeniu usług dostarczania programów radiowych i telewizyjnych na rzecz Abonentów a oferta programowa jest udostępniana przez przesył sygnału w sieci telekomunikacyjnej.

Unia ustala zasady roamingowe

Wiadomość tekstowa wysłana z zagranicy na obszarze Unii Europejskiej będzie od 1 lipca kosztować nie więcej niż 0,11 EUR zamiast – jak obecnie – 0,28 EUR. Obniżenie opłat za transmisję danych to koniec czasów, kiedy konsumenci musieli spodziewać się „szokujących faktur" za pobranie z sieci zdjęcia lub filmu za pomocą telefonu komórkowego, korzystając z roamingu na terenie UE. Parlament Europejski znaczną większością głosów przyjął nowe unijne przepisy dotyczące SMS-ów i transmisji danych w roamingu, zaproponowane przez Komisję Europejską we wrześniu 2008 r. Obecny pułap cen za połączenie telefonii komórkowej wykonane zagranicą będzie stopniowo spadać z 0,46 EUR do 0,35 EUR za minutę do lipca 2011 r., a ceny za otrzymanie połączenia w roamingu międzynarodowym obniżą się z obecnego poziomu 0,22 EUR do 0,11 EUR. Operatorzy telefonii komórkowej będą również zobowiązani do naliczania sekundowego opłat roamingowych najpóźniej od 31 sekundy rozmowy, co ukróci obecną praktykę, z powodu której konsumenci ponoszą opłaty zawyżone nawet o 24 proc.

Prawo

Projekt ustawy o rozwoju sieci

W ramach Programu „Polska Cyfrowa", czyli programu upowszechnienia usług szerokopasmowych w Polsce do 2012 r., został opracowany przez UKE projekt ustawy o wspieraniu rozwoju usług i sieci szerokopasmowych w telekomunikacji. Projekt zawiera rozwiązania sprzyjające rozwojowi społeczeństwa informacyjnego, realizowane poprzez zniesienie barier dla inwestycji w infrastrukturę teleinformatyczną i stworzenie rozwiązań prawnych stymulujących rozwój sieci regionalnych oraz budowę infrastruktury telekomunikacyjnej przez samorządy oraz inwestorów prywatnych. Po zakończeniu wspólnych prac Urzędu Komunikacji Elektronicznej i Ministerstwa Infrastruktury w zakresie niezbędnych poprawek, projekt w dniu 5 maja 2009 r. został skierowany przez Ministerstwo Infrastruktury do uzgodnień wewnątrz- i międzyresortowych oraz do konsultacji społecznych.

Projekt w wersji skierowanej do konsultacji i uzgodnień wraz z uzasadnieniem jest opublikowany na stronie internetowej Ministerstwa Infrastruktury.

Instalacja telekomunikacyjna w każdym nowym budynku

12 marca br. Minister Infrastruktury podpisał rozporządzenie zmieniające rozporządzenie w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie. Rozporządzenie, oprócz usytuowania i szczegółowych warunków technicznych, jakie powinny spełniać budynki, reguluje również zasady wykonywania instalacji telekomunikacyjnych w budynkach.

Najważniejszą zmianą, wprowadzaną przez ww. rozporządzenie, jest nałożenie na inwestora obowiązku wyposażenia budynku w instalację telekomunikacyjną, obejmującą cały odcinek od połączenia z publiczną siecią telekomunikacyjną do gniazda abonenckiego. Dotychczas budynek nie musiał być wyposażony, a jedynie przystosowany do wyposażenia w instalację telekomunikacyjną. Wprowadzane przepisy zobowiązują inwestorów do należytego przygotowania budynków do potrzeb związanych z dostępem do sieci telekomunikacyjnych, tj. do zapewnienia instalacji wewnątrzbudynkowych i przyłączy telekomunikacyjnych umożliwiających podłączenie sieci telefonicznych, radia, telewizji i dostępu szerokopasmowego do internetu.

W ten sposób dostawcy komunikacji elektronicznej doczekali się równego traktowania wraz z dostawcami innych mediów (energii, wody, kanalizacji itp.).

Na horyzoncie światłowód do domu klienta

Bezprzewodowo w Grupie INEA

Z prezesem Grupy INEA, JANUSZEM KOSIŃSKIM rozmawiał Grzegorz Kantowicz.

– INEA jest stosunkowo młodą marką na rynku, ale już okrzepłą. Jak z perspektywy początków konsolidacji Grupy INEA, wygląda obecnie sytuacja na rynku komunikacji elektronicznej biorąc pod uwagę obecne spowolnienie gospodarcze?

– W obszarze usług powszechnych i pierwszej potrzeby, a do takich należy zaliczyć usługi telekomunikacyjne, spowolnienie gospodarki ma bardziej łagodny wpływ na wyniki operacyjne, ale niestety z reguły trwa dłużej. Z perspektywy grupy INEA traktujemy ten czas jako szansę zintensyfikowania współpracy z innymi firmami naszej branży.

Jesteśmy największym operatorem telekomunikacyjnym działającym na zamkniętym obszarze Wielkopolski i czujemy się odpowiedzialni za stworzenie platformy porozumienia, pozwalającej na skuteczną walkę i konkurencję z największymi telekomami polskiego rynku. W swoim rozwoju skupiamy się na wprowadzaniu usług najwyższych warstw. To samo proponujemy wszystkim współpracującym z nami operatorom. Przykładami takich usług jest telefonia, telewizja cyfrowa czy platforma obsługi abonentów. W najbliższym czasie zaoferujemy kolejne, nad którymi aktualnie pracujemy. Dzięki takiej polityce, współpracujący z nami operatorzy mogą się skupić na organicznym rozwoju, mając do dyspozycji w swojej ofercie wszystkie z możliwych do zaoferowania usług.

W zakresie współpracy z instytucjami finansowymi, których niestety dotknął kryzys, zauważamy usztywnienie stanowisk. Tym niemniej, nasze obecne zadłużenie jest marginalne i trudna sytuacja sektora finansowego nie ma obecnie wpływu na planowane przez nas inwestycje na ten rok.

– Sektor operatorów kablowych jest nadal jednym z najszybciej rozwijających się pod względem cyfryzacji przekazów multimedialnych. Dostęp infrastrukturalny do klienta końcowego ma tu szczególne znaczenie, ale czy tylko?

– Infrastruktura jest rzeczywiście istotną kwestią. Nie tylko należy ją rozpatrywać w kategoriach „jest" czy „nie ma", ale też – jaka jest i jakie usługi są możliwe do świadczenia.

Zawsze jednak sieć pozostanie tylko narzędziem w dyspozycji operatora. Dla abonenta ważne są usługi, które również podlegają rozwojowi i zmianom. Dla przykładu, nie wystarczy już analogowa transmisja kilkudziesięciu programów – abonenci oczekują jakości HD i pełnej interaktywności.

W naszym odczuciu, ważne, jeśli nie najważniejsze jest trafienie w potrzeby Klienta. Szukamy takich nisz, których nasz abonent oczekuje, a które nie są proste do zaspokojenia przez innych. Dlatego cały czas rozwijamy i zwiększamy serwisy lokalne. Wracając jeszcze na chwilę do samej infrastruktury, to zdaniem wielu ekspertów rynku, to właśnie sieci HFC mają najlepszą perspektywę rozwoju.

– Na jakim obszarze obecnie działa INEA? Do jakiego klienta kierujecie swoją ofertę?

– Kiedy czytają Państwo to wydanie INFOTELA, rozszerzyliśmy właśnie oficjalnie zakres świadczonych usług o ofertę skierowaną do klientów biznesowych i korporacyjnych. Dzięki konkurencyjnej ofercie INEA Biznes, przewiduję duży progres w pozyskiwaniu klientów z tego obszaru. Jestem przekonany, że za rok o tej porze będziemy mogli powiedzieć, że INEA odnosi sukces w dotarciu ze swoją ofertą nie tylko do klientów indywidualnych, ale także biznesowych w całej Wielkopolsce.

– Rozmawiając w ubiegłym roku na ten temat, powiedział Pan w kontekście lokalnego działania, że małe jest piękne, ale do czasu. Czy ten „czas" już nadchodzi?

– Coraz odważniej inwestujemy w sieci szkieletowe łączące nasze lokalizacje na terenie Wielkopolski, tym niemniej, pomimo lokalnego działania, zdążyliśmy urosnąć do średniej wielkości przedsiębiorstwa. Plan na ponad 100 mln przychodów w tym roku, przy wysokiej efektywności działania, pozwala nam na terenie Wielkopolski realizować projekty, które w zasadzie zarezerwowane są tylko dla największych wśród branży. Może inaczej powinniśmy zadać pytanie – czy jakikolwiek operator z naszej branży jest duży, no może poza UPC?

– W ostatnim czasie zintensyfikowały się prace wdrożeniowe standardu DOCSIS 3.0. Również w Polsce przeprowadzane są pierwsze wdrożenia. Czy INEA również testuje ten standard transmisji danych który umożliwia transmisję ok. 100 Mb/s?

– DOCSIS 3.0 to naturalne rozwinięcie aktualnie stosowanego przez operatorów kablowych standardu 2.0. Jest to o tyle istotne, że nie ma potrzeby wdrażania nowej technologii w warstwach provisioningu, diagnostyki czy obsługi. Etap standaryzacji i testów laboratoryjnych zakończył się wcześniej,

dlatego przygotowania do wdrożenia nowego standardu rozpoczęliśmy już w 2007 roku.

Efektem tego jest zastosowanie w stacjach czołowych urządzeń zgodnych z nowym standardem, a ostateczne uruchomienie wiąże się z zainstalowaniem dodatkowych modułów i zastosowaniem nowych modemów abonenckich. Testy modemów zgodnych z DOCSIS 3.0 rozpoczniemy w wakacje tego roku, komercyjne oferowanie usług w oparciu o ten standard – prawdopodobnie w roku przyszłym. Potencjał DOCSIS 2.0 pozwala nam na kolejny krok i zaoferowanie, bez zmiany technologii, jeszcze większych przepływności od aktualnie dostępnych 8 Mb/s.

Niezależnie jednak od tych działań, rozpoczęliśmy też prace nad budową sieci xPON, którymi dostarczać będziemy mogli abstrakcyjne i trudne do wyobrażenia na dzień dzisiejszy przepływności pojedynczych gigabajtów do końcowego użytkownika. Osobiście uważam, że doprowadzi nas to do tego, że każdy abonent telekomunikacyjny będzie miał do dyspozycji światłowód w domu.

– Czy w dobie coraz szybszego postępu w cyfryzacji przekazów medialnych przewiduje Pan coraz większą personalizację oferty operatorów? Czy jednak usługi pakietowe jeszcze długo będą dominującymi w ofertach? Czy jest szansa na zmianę polityki dystrybutorów w kierunku bardziej personalnego podejścia do klienta?

– Miałem nadzieję, że liczba programów na rynku i postępująca cyfryzacja sieci doprowadzą do sytuacji, w której nadawcy zweryfikują swoje konserwatywne podejście. Niestety, ich upór odnośnie braku chęci do udostępniania programów telewizyjnych w systemie a la card wciąż negatywnie zadziwia i nie sprzyja pozytywnemu rozwojowi oferty dostawców usług telewizyjnych. Mogę mieć tylko nadzieję, że nadawcy będą chętniej poddawali swoje produkty ocenie widzów.

– Jakie są najbliższe plany rozwoju Grupy INEA?

– Tak jak już wcześniej wspominałem w planach mamy rozpoczęcie budowy sieci NGN oraz uruchomienie usług na żądanie, a także całej gamy usług interaktywnych. Dużym dla nas wydarzeniem będzie również wprowadzenie usługi telefonii komórkowej. W kwietniu podpisaliśmy list intencyjny z firmą Telogic, która będzie wspierać nas w tym zakresie. Kolejne usługi, które mamy zamiar wprowadzić, to usługi z zakresu usług bezprzewodowych i mobilnych (wi-max, wi-fi). Ponadto cały czas rozwijamy i uruchamiamy nowe funkcjonalności e-BOA, czyli elektronicznego Biura Obsługi Abonenta. Cieszy się ono coraz większym zainteresowaniem i coraz częściej jest używane przez naszych abonentów.

– Dziękuję za rozmowę.

Cyfryzacja to priorytet

Wspieramy multimedialne aspiracje naszych Klientów

Z PRZEMYSŁAWEM KURCZEWSKIM – Prezesem Zarządu TP Emitel – rozmawiał Grzegorz Kantowicz.

– Emitel będąc spółką Grupy Kapitałowej TP już od siedmiu lat jest głównie operatorem naziemnej sieci radiowo-telewizyjnej. Czym, oprócz tego, zajmuje się firma?

– Emitel jest wiodącym operatorem naziemnej sieci radiowo-telewizyjnej w Polsce.

Świadczone przez nas usługi można podzielić na trzy grupy: radio, telewizja i telekomunikacja. W obszarze telewizji i radia oferujemy przede wszystkim transmisję sygnału telewizyjnego i radiowego dla nadawców. Dzięki posiadanej ogólnopolskiej sieci dosyłowej, oferujemy także usługę okazjonalnych transmisji z imprez plenerowych. Testujemy także cyfrową technologię – DVB-T (standard naziemnej telewizji cyfrowej) oraz DAB+ (standard cyfrowej transmisji radiowej).

Jako nowoczesny operator telekomunikacyjny rozwijamy innowacyjne rozwiązania w zakresie technologii bezprzewodowych (między innymi CDMA, WiMAX) i multimediów. Oferujemy usługi monitoringu, wewnętrznych instalacji antenowych. Dzierżawimy nasze łącza cyfrowe, świadczymy usługi radiokomunikacji morskiej i pomiary pola elektromagnetycznego. Nie mogę także pominąć naszego nowatorskiego projektu, jakim jest EmiKam – transmisja z kamer on-line.

– W ubiegłym roku Prezes Urzędu Komunikacji Elektronicznej nałożył na TP Emitel obowiązki regulacyjne. Jaki wpływ mają te decyzje na obecne funkcjonowanie firmy, w szczególności z punktu widzenia udostępniania własnej infrastruktury sieciowej?

– Funkcjonując na rynku telekomunikacyjnym trzeba liczyć się i być gotowym na możliwość administracyjnego regulowania pewnych segmentów działalności. Wierzymy w nasze doświadczenie (jesteśmy na rynku radiodyfuzyjnym od ponad 50 lat), a dzięki naszemu profesjonalnemu i innowacyjnemu podejściu, od lat, cieszymy się zaufaniem Klientów.

– Cyfryzacja przekazów radiowo-telewizyjnych to jeden z wiodących tematów w branży. Na jakim etapie są obecnie przygotowania do realizacji konwersji analogowo-cyfrowej przekazów medialnych w TP Emitel?

– Myślę, że cyfryzacja telewizji naziemnej to nie tylko ważna sprawa dla branży, ale praktycznie dla każdego. W Polsce mamy przecież ponad 13 milionów gospodarstw domowych, z tego około połowy odbiera telewizję drogą naziemną. Dlatego od lat pracujemy nad odpowiednim przygotowaniem się do procesu cyfryzacji telewizji. Od 2001 roku Emitel jest liderem w zakresie testowych emisji cyfrowego sygnału telewizji naziemnej. Dzięki testom zdobyliśmy niezbędne doświadczenia konieczne do szybkiego i efektywnego uruchomienia multipleksów. Stale współpracujemy z TVP, dzięki czemu obecnie w kilku miastach istnieje możliwość oglądania programów nadawanych cyfrowo (obecnie w ramach testów sygnał naziemnej telewizji cyfrowej jest dostępny m.in. na całym Mazowszu oraz w Poznaniu, Krakowie, Zielonej Górze, Rzeszowie i Wiśle). W sierpniu 2008, przy okazji Igrzysk Olimpijskich w Pekinie, Emitel wspólnie z telewizją publiczną rozpoczął emisję TVP HD – kanału telewizji publicznej nadawanego w wysokiej rozdzielczości Full HD. Jest to pierwszy taki projekt w Polsce.

Jesteśmy gotowi do cyfryzacji, w związku z tym prowadzimy aktywne rozmowy z nadawcami i instytucjami odpowiedzialnymi za cyfryzację. Pamiętajmy, że pierwszy multipleks ma ruszyć najpóźniej do końca września 2009 r. Podsumowując, mogę zapewnić, że jesteśmy przygotowani do włączenia pierwszego multipleksu cyfrowego DVB-T zgodnie z harmonogramem KRRiT.

– EmiKam to nowa usługa firmy Emitel, polegająca na tworzeniu i transmisji kontentu z różnego rodzaju eventów czy imprez sportowych. Jest to jeden z przykładów powstawania i rozwoju sektora usług multimedialnych. Co Pan sądzi o tworzących się nowych modelach powstawania i dystrybucji treści multimedialnych, głównie w internecie?

– W zeszłym roku udało nam się zrealizować wiele ciekawych projektów związanych z tworzeniem oraz transmisją kontentu. Warto tutaj wspomnieć między innymi o transmisji z prestiżowych zawodów żeglarskich Sopot Match Race czy 18. Rajdu Dolnośląskiego, którego prolog miał miejsce w Kłodzku. W ramach zrealizowanych projektów współpracowaliśmy z największymi portalami internetowymi: WP, Onet czy Interia. Transmisje online, prezentowane we współpracy z portalami, aktualnie są jeszcze nowinką techniczną, ale mogą się stać dochodowym przedsięwzięciem. Pojawienie się reklam w takich transmisjach jest tylko kwestią czasu.

– Jakie plany ma firma na najbliższą przyszłość?

– Najbliższa przyszłość to dla nas uruchomienie naziemnej telewizji cyfrowej. Jesteśmy gotowi, aby w tym procesie aktywnie uczestniczyć. Traktujemy ten projekt jako naturalne przejście do kolejnego etapu rozwoju technologii transmisji sygnału telewizyjnego. Planujemy także uczestnictwo w konkursie na aktywnego operatora drugiego multipleksu. Ponadto będziemy kontynuować i rozwijać testy cyfrowego radia w systemie DAB+. To rewolucyjny projekt, ale to już temat na kolejną rozmowę. W planach znajduje się także rozwój działań telekomunikacyjnych. Jesteśmy w trakcie przygotowywania innowacyjnych rozwiązań w zakresie zarządzania kontentem i usług multimedialnych.

Jedno jest pewne – wszystkie podejmowane działania są zgodne z misją naszej firmy, którą jest wspieranie multimedialnych aspiracji naszych Klientów.

– Dziękuję za rozmowę

Muzyczny internet

Internet przegonił tradycyjne media muzyczne

Aż 78 proc. polskich internautów słucha muzyki głównie online, np. przez YouTube – wynika z badania ankietowego przeprowadzonego przez sklep internetowy kolporter.pl. Serwisy społecznościowe i radia internetowe wypierają tradycyjne media muzyczne.

Muzyki w tradycyjnych mediach szuka tymczasem nieco ponad połowa badanych. – *To nadal dużo, ale już teraz widać, że internet dominuje jako medium muzyczne* – komentuje **Robert Sołkiewicz** z kolporter.pl. – *Głównym czynnikiem wpływającym na jego popularność wśród fanów muzyki jest zapewne łatwy dostęp do ogromnej liczby utworów oraz możliwość decydowania o tym, czego będą słuchać* – dodaje. Warto podkreślić, że **internauci są zainteresowani słuchaniem muzyki bez konieczności jej posiadania np. w postaci plików czy płyt CD.** Deklaruje to 76 proc. zapytanych osób.

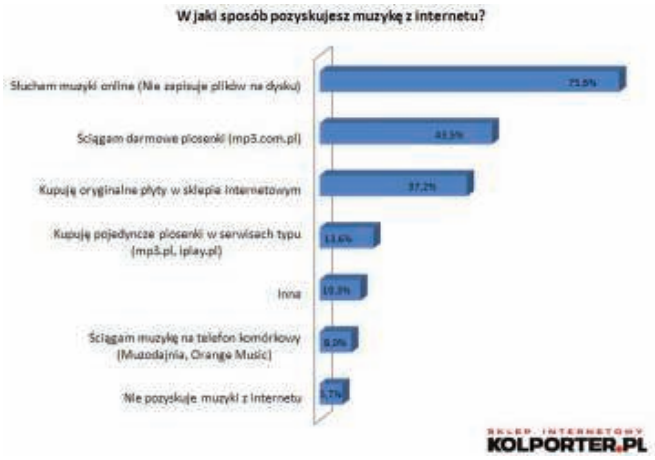
Polakom nie wystarcza już bierne słuchanie tego, co serwują media. Wykorzystując możliwości sieci, sami znajdują najciekawsze utwory w internecie. Zapewne z tego też powodu **największą popularnością wśród badanych cieszą się serwisy społecznościowe.** W celach muzycznych wykorzystuje je siedmiu na dziesięciu ankietowanych. Najmocniejszą pozycję ma serwis YouTube, który znacznie wyprzedza konkurencyjne LastFM, rodzimą Wrzutę czy MySpace. Jednak to nie aspekt społecznościowy jest największym atutem tych serwisów. Utwory ocenia tylko co trzeci badany, a wpis w postaci komentarza deklaruje co piąty. **Aktywność internautów zwiększa się jednak po odkryciu czegoś ciekawego.** Niemal połowa badanych deklaruje, że przesyła wówczas linka znajomym. Z kolei 46 proc. decyduje się wtedy na zakup płyty.

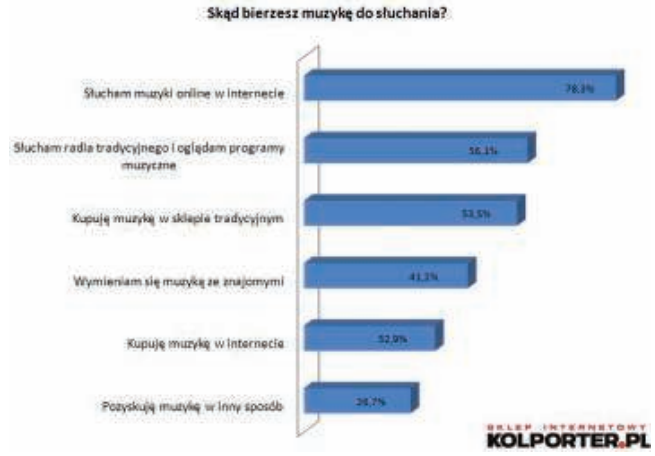
Radio online wciąż na fali

Świetnie radzą sobie także tradycyjne stacje radiowe, które zdecydowały się na nadawanie w sieci. **Internetowe wydania stacji tradycyjnych to drugie pod względem popularności źródło muzycznych hitów.** Korzysta z nich sześciu na dziesięciu internautów. Najpopularniejsze są RMF, Trójka, Eska i Radio Zet. Brak jednak zdecydowanego lidera. – *Starzy gracze uzyskują dobre wyniki w internecie, gdyż daje o sobie znać przywiązanie do sprawdzonych marek* – mówi **Robert Sołkiewicz** z kolporter.pl. – *Internauci stykają się z nimi przecież nie tylko w sieci, ale także gdy słuchają audycji w samochodzie lub za pomocą urządzenia przenośnego, np. telefonu komórkowego* – dodaje. Stacji stricte internetowych słucha 46 proc. badanych. W tej grupie królują Polska Stacja i Miasto Muzyki, których słucha co siódmy respondent.

CD ma się świetnie

Co ciekawe, pomimo coraz większej popularności internetu, **najczęściej muzykę przechowujemy nadal na płytach CD.** Zdecydowana większość badanych posiada utwory zarówno w takiej formie, jak i w postaci plików mp3. Co więcej, **całe albumy na płytach CD to wciąż najczęściej preferowany sposób nabywania muzyki,** wskazywany przez





ponad połowę ankietowanych. Dla porównania – kupno całych albumów w internecie w postaci plików mp3 deklaruje tylko co piąty respondent. Warto podkreślić, że **za album na płycie CD jesteśmy w stanie zapłacić więcej.** Co trzeci internauta jest w stanie wydać w tym celu 20-30 PLN, a co czwarty nawet 50 PLN. Za ten sam album, zakupiony w postaci plików mp3, co trzeci badany jest w stanie zapłacić tylko 5-10 PLN lub 10-20 PLN. **Wydatek rzędu 30 PLN deklaruje mniej niż 5 proc. osób.** Co dziesiąty internauta nie zamierza płacić za pliki mp3.

Przyszłość płyt CD nie jest jednak świetlana. **Internauci twierdzą, że pliki muzyczne z czasem wyprą nośnik CD.** Uważa tak 56 proc. respondentów. Co trzeci jest zdania, że utrzyma się obecny system z przewagą płyt.

W badaniu ankietowym przeprowadzonym przez sklep kolporter.pl i serwis Dziennik Internautów wzięło udział 1539 internautów.

Telewizory z „internetem”

Viera Cast w telewizorach Panasonic

Firma Panasonic wzbogaciła ofertę telewizorów Full HD o najnowszą serię G15. Prawdziwi fani domowej rozrywki otrzymają do dyspozycji najnowsze plazmy 42 i 46-cali (TX-P42G15E i TX-P46G15E) wykonane w rewolucyjnej technologii NeoPDP z częstotliwością odświeżania obrazu wynoszącą 600 Hz oraz ekran LCD – TX-L37G15E z panelem IPS Alpha. Dodatkowo w nowych telewizorach została zastosowana funkcja Viera Cast, umożliwiająca korzystanie z najpopularniejszych serwisów internetowych, takich jak YouTube, Picasa, Bloomberg.

TX-L37G15E/B

Wszystkie modele telewizorów z serii G15 wyposażone zostały w szereg funkcji ułatwiających korzystanie z nich, a także pozwalających na zbudowanie własnej domowej sieci rozrywki. Jedną z nich jest funkcja Viera Cast, która zapewnia domownikom dostęp do zasobów internetu bezpośrednio na ekranie telewizora. Ponadto telewizory serii G15 są kompatybilne ze standardem DLNA (DivX/JPEG/MPEG2), co umożliwia pełne zintegrowanie odbiornika z domową cyfrową siecią. Dzięki niej z łatwością odtworzymy nagrania przechowywane w komputerze, np. zdjęcia czy filmy. Odtwarzanie plików w formatach AVCHD, DivX i JPEG ułatwia także Viera Image Viewer, który przy użyciu wbudowanego slotu na karty SDHC pozwala w prosty i szybki sposób przeglądać fotografie i filmy zapisane na karcie. W telewizorach serii G15 nie zabrakło także funkcji Viera Link, która pozwala kontrolować wszystkie urządzenia służące do domowej rozrywki za pomocą jednego pilota oraz trybu Game Mode.

Użytkownicy paneli plazmowych Panasonic Full HD serii G15 otrzymają do dyspozycji szereg funkcji, które wpływają na poprawę jakości obrazu. Do najważniejszych należy sterowanie podpolowe 600 Hz z funkcją Intelligent Frame Creation Pro (*600 Hz Sub-field Drive Intelligent Frame Creation Pro*), które zapewnia niezwykle płynny i wyraźny obraz bez tzw. efektu smużenia. Korzystny ich wpływ zauważymy podczas oglądania dynamicznych scen, np. filmów akcji czy rozgrywek sportowych. Funkcje te sprawiają także, że dzięki wysokiej płynności obrazu panele plazmowe serii G15 nie męczą wzroku, przez co są bezpieczne dla wrażliwych oczu dziecka. Znakomitą jakość obrazu panele NeoPDP serii G15 zawdzięczają także najwyższej rozdzielczości ruchomego obrazu (*Moving Picture Resolution*) na poziomie 1080 linii. Oznacza to precyzyjną reprodukcję programów w pełnej rozdzielczości HD o dowolnej szybkości scen, bez utraty jakichkolwiek szczegółów.

Obraz uzyskiwany na nowych ekranach plazmowych Panasonic – **TX-P42G15E** i **TX-P46G15E** – wyróżnia głęboka czerń i olśniewające kolory. Na efekt taki wpływa kontrast natywny na poziomie 40.000:1 i niespotykany kontrast dynamiczny na poziomie 2.000.000:1, który został osiągnięty dzięki poprawionej jasności i głębszej czerni. Ponadto kinową jakość obrazu na ekranach plazmowych zapewnia znakomite odwzorowanie naturalnych kolorów. Telewizory NeoPDP gwarantują doskonałe kolory dzięki zastosowaniu wielu innowacyjnych technologii, takich jak realizowanie gradacji od jasnych do ciemnych odcieni w 6144 stopniach.

Telewizory plazmowe wyposażone zostały w tzw. VIERA Tough Panel – warstwę szkła chroniącą panel przed mechanicznymi uszkodzeniami. Sprawia to, że telewizor ten jest odporny nawet na uderzenie dziecięcą zabawką lub pilotem. Warto także podkreślić długą żywotność panelu aż do 100 tys. godzin.

Telewizory, dzięki wykorzystaniu najnowszych technologii, zapewniają znakomitej jakości obraz, co szczególnie sprawdzi się podczas oglądania filmów wysokiej rozdzielczości, a także wydarzeń sportowych. Dzięki technologii x.v. Colour i Deep Colour zapewniają realistyczne odtwarzanie kolorów i czystsze barwy.

Nowy telewizor LCD z serii G15 – **TX-L37G15** zapewnia wysokiej jakości obraz m.in. dzięki zastosowaniu w nim funkcji inteligentnego tworzenia klatki 100 Hz, która zamienia strumień 50 klatek na sekundę pochodzący z sygnału wejściowego 50 Hz na strumień 100 klatek na sekundę. Poza tym znaczne zwiększenie rozdzielczości w tym modelu uzyskiwane jest poprzez wykorzystywanie technologii wykrywania ruchu. Telewizor wykrywa obszary, w których następuje ruch i włącza rozjaśnienie tylnego podświetlenia tylko w tych obszarach.

Telewizor wyposażony został w panel IPS-Alpha Full HD, który zapewnia 178-stopniowy kąt widzenia pozwalając na oglądanie telewizji z niemal każdego miejsca w pokoju. Panel ten wyprodukowany został w technologii 10-bitowej, dzięki czemu widzowie mogą cieszyć się naturalnymi i pełnymi głębi kolorami. O jakości obrazu decyduje tu także kontrast 50.000:1 z funkcją inteligentnej kontroli sceny, która powoduje zmniejszenie intensywności światła podczas odwzorowania czarnych fragmentów obrazu.

Telewizor LCD wyposażony został w funkcję 24 Smooth Film, która zapewnia idealnie płynny ruch w filmach poprzez zwiększenie liczby wyświetlanych klatek. Funkcja ta zamienia standardowe 24 klatki na sekundę na 96 klatek, co skutkuje znacznym podniesieniem komfortu oglądania obrazów wysokiej rozdzielczości.

Panel LCD Panasonic z serii G15 cechuje żywotność do 60 tys. godzin. ■

MISJA

[Misją Emitel jest **dostarczanie wysokiej jakości** usług transmisyjnych,
w oparciu o **innowacyjne platformy technologiczne,**
aby **wspierać multimedialne aspiracje** naszych Klientów]

Oferta Emitel obejmuje usługi, które są każdorazowo dostosowane do specyficznych wymagań Klientów. Świadczone usługi zostały podzielone na trzy grupy:

TELEWIZJA

- analogowa emisja naziemna
- naziemna telewizja cyfrowa DVB-T
- cyfrowe stacje czołowe
- dosył sygnałów telewizyjnych
- spływy reporterskie do ośrodków telewizyjnych
- transmisje okazjonalne z imprez sportowych, kulturalnych itp.
- planowanie radiowe

RADIO

- emisja naziemna programów radiowych
- dosył modulacji
- planowanie radiowe na potrzeby budowy sieci radiodyfuzji naziemnej

TELEKOMUNIKACJA

- dzierżawa łączy transmisji danych
- dzierżawa łączy cyfrowych
- dostępowe usługi bezprzewodowe
- pozyskiwanie i zarządzanie kontentem
- budowa stacji w technologii GSM, CDMA, WiMax
- EmiKam – transmisja z kamer online
- dzierżawa infrastruktury obejmującej maszty wieże i budynki na obszarze całej Polski
- wewnętrzne systemy antenowe – Indoor
- pomiary pola elektromagnetycznego
- utrzymanie systemów radiokomunikacyjnych
- radiokomunikacja morska
- monitoring wizyjny
- mobilna telewizja cyfrowa w standardzie DVB-H

www.emitel.pl

TP EmiTel sp. z o.o. (siedziba spółki)
ul. Pilotów 4c, 31-462 Kraków
tel. 012 627 31 00, faks: 012 627 31 02
sekretariat@emitel.pl

Pion Sprzedaży i Marketingu
ul. Domaniewska 50, 02-672 Warszawa
tel. 022 578 33 00, faks: 022 578 33 02
marketing@emitel.pl

emitel

Jubileuszowe XX Targi INTERTELECOM w Łodzi

Grzegorz Kantowicz

Targi z recesją w tle

Jubileuszowe XX Targi INTERTELECOM w Łodzi odbyły się w tym roku w wyraźnej atmosferze zapowiadanego kryzysu gospodarczego. W dniach 16-19 marca br. przy ul. Wólczańskiej spotkali się przedstawiciele rynku komunikacji elektronicznej z ponad 100 firm z Chin, Danii, Holandii, Korei Południowej, Niemiec, Polski, Węgier, USA i Wielkiej Brytanii. Zdecydowaną grupę wystawców stanowili stali klienci, wystawiający się w Łodzi i należący do sektora MSP.

Paweł Fendler, Dyrektor Generalny Międzynarodowych Targów Łódzkich, wita uczestników XX Targów INTERTELECOM w Łodzi

Tegoroczne targi były objęte patronatem: Ministerstwa Infrastruktury, Prezesa Urzędu Komunikacji Elektronicznej, Marszałka Województwa Łódzkiego oraz Prezydenta Miasta Łodzi.

Jubileuszowa edycja targów charakteryzowała się w większości propozycjami B2B. Wystawcy prezentowali przede wszystkim rozwiązania przeznaczone dla integratorów, biznesu wykorzystującego nowoczesne rozwiązania sieci bezprzewodowych, systemów światłowodowych dla końcowego klienta oraz usług biznesowych. Charakterystyczną cechą INTERTELECOMU staje się udział nowych małych firm poszukujących swojego miejsca w branży. Nowatorskie pomysły oraz rozwiązania w bardzo wyspecjalizowanych dziedzinach sektora MSP stają się dominującą ofertą wystawową targów.

Jedno z ciekawszych stoisk należało w tym roku do **Konsorcjum FEN Sp. z o.o.**, które zaprezentowało ekspozycję w myśl koncepcji „Welcome to IP World".

Na stoisku poznańskiej firmy w dziale Video zgromadzono najnowocześniejsze rozwiązania do monitoringu IP firmy ACTi oraz dedykowane do nich rejestratory IP marki Koukaam. W sekcji poświęconej systemom NAS znalazły się urządzenia sieciowe Linksys by Cisco, Cisco, Square One oraz QNAP. W przypadku marki QNAP, po raz pierwszy w Polsce został zaprezentowany serwer danych QNAP TS-809U-RP z możliwością obsługi do 16 TB danych.

Osobną część ekspozycji FEN stanowił temat Unified Communications, pokazany jako szansa na pełną realizację idei pracy zdalnej. W tym dziale królowały urządzenia spod znaku Cisco SB oraz biznesowe telefony IP marki SNOM.

– Bardzo cieszy mnie spore zainteresowanie ekspozycją FEN. Od kilku lat obserwuję targi INTERTELECOM i zawsze brakowało mi interaktywności stoisk. Te targi odwiedza grono specjalistów i inżynierów, którzy zamiast czytać materiały marketingowe, dużo bardziej cenią możliwość przejrzenia paneli konfiguracyjnych, oprogramowania rejestrującego lub podglądu przez komórkę. Dlatego tak duże wrażenie budził zaprezentowany przez nas „IP World" – czyli sprawnie funkcjonujący organizm, gdzie Video, NAS, IP Core, Unified Communications oraz WLAN stanowią integralną całość. Dodatkowo optymistycznym jest fakt, że targi odwiedzane były licznie przez młodzież kształcącą się w kierunkach technicznych oraz z placówek oświatowych, z którymi FEN współpracuje w ramach długofalowego projektu wspierania sektora edukacyjnego. Wierzymy, że następna edycja targów przyniesie kolejne rozwiązania i wdrożenia, a świat stanie się bardziej IP – mówi **Bartosz Boczkaja**, Prezes Zarządu Konsorcjum FEN Sp. z o.o.

System WLAN udostępniony podczas targów bazował na urządzeniach **Meru Networks**. Każdy z wystawców oraz odwiedzających mógł skorzystać z sieci bezprzewodowej Meru, której punkty dostępowe zostały zainstalowane we wszystkich halach targowych.

Na stoisku firmy **SGT SA** z Gliwic mogliśmy zapoznać się z bardzo nowoczesną propozycją kablówki 3 generacji, jak nazwali ją twórcy – JAMBOX HD. Oprócz oferty ponad 70 programów w pakiecie wielotematycznym jest jedną z pierwszych propozycji personalizacji programów tematycznych. Dodatkowe programy można dokupować za pomocą pilota telewizyjnego prosto z ekranu telewizora. Oprócz standardowych właściwości i funkcji – jak: obraz HD, Time Shifting, przewodnik po programach (EPG), nagrywarka PVR, kontrola rodzicielska, przypomnienie o programie i autoprzełączenie, wybór języka audio oraz języka napisów, ulubione kanały – mamy do dyspozycji funkcje 3 generacji.

Należą do nich:

Moje zdjęcia – możliwość oglądania własnych albumów ze zdjęciami. Wygodna i prosta obsługa wprost z pilota. Łatwa konfiguracja. Wspiera jeden z najpopularniejszych portali zdjęciowych Picasa WebAlbums.

Internet www – możliwość korzystania z dostępu do stron www czy poczty elektronicznej wprost na ekranie telewizora. Aby przeglądanie stron było bardziej wygodne, można skorzystać z klawiatury oraz myszki komputerowej podłączonej do dekodera przez złącze USB.

Radio + HD – niesamowity radioodtwarzacz, który pozwala na wybór jednej z wielu stacji radiowych oraz podkładu wideo w jakości HD, takiego jak Kominek czy Akwarium

Kamery – możliwość obejrzenia obrazu z miejskich kamer monitorujących

TV Portal – to nasza strona domowa w telewizorze. Umożliwia w łatwy i wygodny sposób dostęp do szeregu usług JAMBOX. Poruszamy się na portalu przy pomocy pilota, podobnie jak w internecie czy też naszej komórce. Z tego miejsca można przeczytać newsy z kraju i ze świata, komunikaty z platformy operatora oraz przejść do podstawowych funkcji, takich jak przewodnik EPG, wygaszacze w HD, stacje radiowe, nagrywarka PVR (w modelu z dyskiem) oraz wielu innych.

Interaktywne gry – kultowe klasyki gier, które wciąż podbijają nasze serca, tym razem na ekranie telewizora. Lista rekordów umożliwia rywalizację pomiędzy wszystkimi abonentami telewizji JAMBOX lub pomiędzy domownikami.

– Jako wystawca muszę powiedzieć, że targi przeszły moje najśmielsze oczekiwania. Od pierwszego dnia mieliśmy tak dużą grupę zainteresowanych klientów, że nie zdążyłem nawet obejrzeć wystawy targowej. Jednak widać wyraźnie, że same targi kurczą się z roku na rok. Obecnie tylko nowe rozwiązania na rynku przyciągają uwagę specjalistów, bo w większości z takimi mamy do czynienia. Targi ewoluowały w kierunku ofert małych i średnich firm dla siebie wzajemnie. Duzi operatorzy i dostawcy już się nie prezentują. Jednak my, z punktu widzenia zainteresowania naszą ofertą, jesteśmy zadowoleni – powiedział **Bartłomiej Czardybon**, Prezes Zarządu SGT SA.

Jedyny operator wywodzący się z tradycyjnych operatorów telekomunikacyjnych – **Telefonia DIALOG SA** prezentowała **Domową Platformę Multimedialną DIALOGmedia** (wprowadzoną do oferty Dialogu z końcem lutego br.), która łączy telewizję cyfrową (IPTV), wideo na żądanie (VoD), telefonię stacjonarną oraz szerokopasmowy internet.

– Targi zostały potraktowane przez nas prosprzedażowo – powiedziała **Marta Chorzempa,** Specjalista ds. Komunikacji Marketingowej Telefonia DIALOG. **–** *Szczególnie chodziło nam o zaprezentowanie naszego biura handlowego w Łodzi. Targi były świetną okazją do zaproszenia gości, klientów i potencjalnych klientów na rozmowy handlowe. Założenia zostały zrealizowane i jesteśmy z tego zadowoleni.*

Tradycyjnie już obecna była na INTERTELECOMIE **firma FCA Sp. z o.o.** z Niepołomic, gdzie z dniem 1 maja przeniosła się do nowej siedziby z Krakowa. Znana na rynku i specjalizująca się w rozwiązaniach światłowodowych zaprezento-

wała na swoim stoisku m.in. System OptiHome – światłowód do abonenta (FTTH) oraz platformę GPON – optycznego dostępu abonenckiego, które zwracają coraz częściej uwagę operatorów chcących dostarczać coraz bardziej zaawansowane usługi szerokopasmowe dla swoich klientów.

– Osobiście jestem na tych targach od kilkunastu lat. Obserwując ewolucję tej imprezy mogę powiedzieć, że obecnie targi są skoncentrowane na firmach oferujących sprzęt do budowy końcowej infrastruktury sieciowej. Mniej jest dostawców systemów i nie ma operatorów telekomunikacyjnych, dlatego z naszego punktu widzenia, jako dostawcy infrastruktury sieciowej, światłowodowej, te targi są trafionym spotkaniem branżowym. Jest to świetna okazja do umówionych spotkań z naszymi klientami i partnerami w jednym miejscu i czasie.

– Trudno byłoby sobie wyobrazić takie spotkania osobiste poza targami. My w tych targach uczestniczyliśmy i zamierzamy uczestniczyć. Szacuję, że na naszym stoisku podczas targów odbędzie się ok. stu kilkudziesięciu spotkań. Wszyscy klienci, którzy nas interesują, są tu obecni i jest to jedyna okazja w roku do takich spotkań. Takim pozornym minusem jest jakby zmniejszenie się rangi tych targów. Jednak paradoksalnie wychodzi to na dobre nam, wystawcom, ponieważ spotkania są obecnie konkretne, wśród specjalistów i osób zainteresowanych. Oczywiście, na targach odcisnęła swoje piętno obecna recesja, ponieważ zauważyliśmy brak paru firm, które tu zawsze były obecne. Nas, na szczęście, ten problem jeszcze nie dotyczy, może dlatego, że nasza specjalizacja światłowodowa jest obecnie jedną z bardziej innowacyjnych i o sporym potencjale popytowym. Generalnie jesteśmy zadowoleni z udziału w tegorocznym INTERTELECOMIE – powiedział **Prosper Biernacki** z FCA.

Tradycyjnie na targach nie zabrakło również firmy **Schroff** należącej do grupy **Pentair Technical Products**. Firma, z siedzibą w Straubenhardt w Niemczech, jest jednym ze światowych liderów w zakresie projektowania i produkcji obudów elektronicznych dla potrzeb elektroniki, automatyki, teleinformatyki i in.

Ryszard Płatek, kierownik sprzedaży z **Pentair Poland Sp. z o.o.** biura handlowego **Schroff**, powiedział: *– Mimo widocznego kryzysu, który odciska swoje piętno również na obecnych targach, jesteśmy zadowoleni ze sporego zainteresowania naszą propozycją. Szkoda tylko, że targi z roku na rok kurczą się. Myślę, że organizatorzy będą musieli zastanowić się nad zmianą formuły tej imprezy. Brakuje obecnie dużych firm operatorskich oraz dostawców technologii globalnych. To one były zawsze magnesem przyciągającym zarówno inne firmy partnerskie, jak i zwiększały zainteresowanie zwiedzających specjalistów. Niestety, zmieniła się polityka promocyjna tych firm i obecnie niechętnie angażują się one w tego typu przedsięwzięcia.*

– Już w pierwszym dniu targów mieliśmy ponad 80 kontaktów biznesowych. I z tego powodu jesteśmy bardzo zadowoleni z naszej obecności tutaj – powiedział **Piotr Baranowski**, Prezes Zarządu **Grupy ZPAS SA** z Przygórza. *– Brakuje tu jednak największego potencjalnego inwestora, jakim jest Telekomunikacja Polska. Z ciekawą inicjatywą wyszła dyrekcja targów, która podczas prezentacji na temat budowy nowej infrastruktury centrum wystawienniczo-konferencyjnego zaprosiła wystawców do udziału w realizacji tego przedsięwzięcia. Z uwagi na to, iż mamy do zaoferowania serwerownie, kioski multimedialne, systemy zasilania itp., jesteśmy zainteresowani tą propozycją. Tradycyjnie wystawiamy się na INTERTELECOMIE z prostego powodu, jest to okazja do zaproszenia w jednym czasie i miejscu naszych partnerów i klientów biznesowych. Z racji naszego położenia geograficznego (prawie przy granicy z Czechami) jest to doskonała okazja, aby spotkać się w centrum Polski i nawiązać lub zacieśnić kontakty. Mieliśmy trzy bardzo ważne spotkania biznesowe, które mogą zaowocować konkretnymi kontraktami. Jednak we wszystkich rozmowach można wyczuć pewną obawę przed kryzysem, który również na tych targach niejako wisi w powietrzu.*

Podczas targów prezentowany był na „żywo" system informacji targowej oparty na technologii Bluetooth. Firma **KSI.PL** z Krakowa, będąca Partnerem Technologicznym targów, stworzyła sieć punktów dostępowych **Systemu BlueSend** – autorskiego rozwiązania pozwalającego na przesyłanie kontentu na urządzenia mobilne. Premiera systemu BlueSend była jedną z imprez towarzyszących pierwszemu, przeznaczonemu sctricte dla profesjonalistów, dniu targów.

– Na tle obecnej sytuacji rynkowej jesteśmy bardzo pozytywnie zaskoczeni zainteresowaniem oraz liczbą zwiedzających – powiedział **Jacek Mirecki**, Prezes Zarządu KSI.PL. – *Ta liczba przekłada się również w jakość, zwiedzający pytają o sprawy konkretne. Jeszcze w dalszym ciągu są to jedyne targi naszej branży w Polsce, na których warto się wystawić. Jesteśmy również mile zaskoczeni zainteresowaniem naszym systemem, który zresztą pracuje na targach i dostarcza szeregu informacji zwiedzającym*.

Nie zabrakło również stałego wystawcy, firmy **Eutelsat**.

– Tradycyjnie prezentujemy na targach INTERTELECOM naszą markę. Przyjeżdżaliśmy tutaj z pewną obawą spowodowaną atmosferą kryzysową, jednak już w pierwszym dniu okazało się, że zwiedzający dopisali, a organizatorzy poradzili sobie z przezwyciężeniem kryzysowych tendencji – powiedziała **Marlena Dylewska** z Eutelsat Polska.

Pierwszego dnia targów, tj. 17 marca, odbyła się organizowana przez nasze wydawnictwo konferencja z cyklu „Przyszłość telekomunikacji elektronicznej w Polsce", z głównym panelem dyskusyjnym „Cyfrowa Polska – wyzwania i nadzieje". Dyskusję prowadził **Wojciech Hałka** – Zastępca Dyrektora ds. Rozwoju, Instytut Łączności, a udział w niej wzięli:

- **Witold Kołodziejski** – Przewodniczący Krajowej Rady Radiofonii i Telewizji;
- **Magdalena Gaj** – Podsekretarz Stanu w Ministerstwie Infrastruktury;
- **Anna Streżyńska** – Prezes Urzędu Komunikacji Elektronicznej;
- **Piotr Guziewicz** – Dyrektor Departamentu Rozwoju Technologicznego i Wdrożeń Telefonii DIALOG;
- **Stefan Kamiński** – Prezes Zarządu Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji;
- **Jacek Mirecki** – Prezes Zarządu KSI.PL Sp. z o.o.

Relację wideo z panelu dyskusyjnego obejrzeć można na stronie www.techbox.pl.

INTERTELECOM to również XVI edycja prestiżowego konkursu o Złoty Medal. Do konkursu zgłoszono 12 produktów. Kapituła konkursu wyróżniła aż 7 firm. Nagrody za poniższe produkty wręczono podczas wieczoru galowego:

- **VoiceIP-PBX – konwergentny serwer telekomunikacyjny telefonii IP** – firmy AVSystem Sławomir Wolf.
- **Router MultiLink 2 – rodzina produktów** – firmy **GORAMO** – Janusz Górecki.
- **Asterisk Enterprise Edition Mark II** – firmy DIR.
- **VoiceIP-ACS TR69 Auto Configurator Server** – firmy AVSystem Sławomir Wolf.
- **DIALOGmedia – Domowa Platforma Multimedialna** – firmy Telefonia DIALOG.
- **Kamera IP Mobotix Q 22 – Sec** – firmy LINC.
- **System Automatycznego Rozliczania Abonentów ARA** – firmy KSI.PL.

Również wydawnictwo **MSG-Media** wyróżnione zostało statuetką za znaczący wkład w rozwój targów INTERTELECOM. ■

14. Raport Implementacyjny

Rynek telekomunikacyjny w Polsce okiem Komisji Europejskiej

W marcu br. Komisja Europejska opublikowała 14. Raport Implementacyjny w sprawie jednolitego rynku usług telekomunikacyjnych. Raport ten pozwala obiektywnie, niejako „z lotu ptaka", przyjrzeć się dotychczasowym działaniom legislacyjnym oraz regulacyjnym na europejskim rynku komunikacji elektronicznej. Przedstawiamy część raportu dotyczącą Polski.

Wprowadzenie

Sytuacja na polskim rynku łączności elektronicznej była stosunkowo stabilna w 2008 r. Z jednej strony można było zaobserwować dalsze ożywienie konkurencji na rynku telefonii ruchomej, z drugiej strony – operator zasiedziały nadal zajmował pozycję dominującą zarówno na rynku szerokiego pasma, jak i telefonii stacjonarnej. Penetracja usług szerokopasmowych, choć wciąż jedna z najniższych w UE, znacznie wzrosła w 2008 r.

Polska nie zakończyła pierwszej rundy analiz rynkowych w 2008 r. Podobnie jak w latach poprzednich, regulator skupił się na wspieraniu interesów konsumentów oraz konkurencji, natomiast mniej uwagi poświęcono stworzeniu warunków dla niezbędnych inwestycji, takich jak zorientowanie kosztowe albo ustalanie cen zgodnie z drabiną inwestycyjną. Regulator wszczął procedury zmierzające do wprowadzenia funkcjonalnej separacji operatora zasiedziałego. Sześć postępowań o naruszenie przez Polskę prawa wspólnotowego w zakresie łączności elektronicznej było w toku w 2008 r.

Otoczenie regulacyjne

Główne działania regulacyjne

Długo oczekiwana duża nowelizacja ustawy *Prawo telekomunikacyjne* z 2004 roku została rozdzielona na dwie części, w celu przyspieszenia procesu legislacyjnego. Pierwsza część, mająca na celu dostosowanie polskiego prawa do wspólnotowych ram regulacyjnych oraz transponująca unijną dyrektywę w sprawie zatrzymywania danych, została przyjęta przez Rząd oraz przekazana do Parlamentu w październiku 2008 r. Pozostała część zmian była wciąż w przygotowaniu przez Ministerstwo.

Wiosną 2008 r. Prezes UKE przedstawił nową strategię regulacyjną na lata 2008-2010. Strategia w dalszym ciągu skupia się na zwiększaniu dostępności oraz wykorzystania usług łączności elektronicznej dla obywateli, jednak pewien nacisk położono w niej również na stymulowanie inwestycji w infrastrukturę.

W grudniu regulator podjął kroki celem wprowadzenia funkcjonalnej separacji operatora zasiedziałego, po zapoznaniu się z wynikami szczegółowej analizy, która stwierdzała w konkluzji, że narzędzie regulacyjne w postaci FS byłoby skuteczne w zwalczaniu taktyk dyskryminacyjnych, chociaż nie usunęłoby innych barier.

Do końca 2008 r. cztery z sześciu postępowań przeciwko Polsce o naruszenie prawa wspólnotowego z powodu nieprawidłowej transpozycji lub zastosowania prawa wspólnotowego w sektorze łączności elektronicznej zostały skierowane przez Komisję do Europejskiego Trybunału Sprawiedliwości. Komisja zamknęła postępowanie w sprawie usługi ogólnopolskiego biura numerów oraz braku identyfikacji miejsca przebywania osoby dzwoniącej na numer alarmowy 112.

Organizacja NRA

Kwestia legalności procesu powołania Prezesa UKE została ostatecznie rozstrzygnięta w 2008 r. wyrokiem Sądu Najwyższego, który w lutym orzekł na korzyść Prezesa UKE.

Odpowiedzialność za regulację polskiego rynku łączności elektronicznej jest obecnie dzielona pomiędzy Prezesa UKE a Ministerstwo Infrastruktury. Prezes UKE ma kompetencje w zakresie większości zadań przypisanych organowi regulacyjnemu na podstawie wspólnotowych ram prawnych, natomiast Ministerstwo jest odpowiedzialne za określanie rynków właściwych na potrzeby analiz rynkowych oraz za akty prawne, w tym szereg rozporządzeń. Współpraca między dwoma organami była napięta w ciągu poprzedniego roku; UKE oskarżało Ministerstwo o rzekomą bierność, z kolei Ministerstwo kwestionowało podstawy prawne niektórych decyzji regulacyjnych. Zarówno regulator, jak i Ministerstwo (oba organy są finansowane w pełni z budżetu państwa) miały trudności z rekrutacją oraz zatrzymaniem należycie wykwalifikowanej kadry, co spowodowało znaczne obciążenie zadaniami zatrudnionych już pracowników.

Zgodnie z planowaną zmianą polskiego prawa telekomunikacyjnego, odpowiedzialność za definicje rynków właściwych zostanie przekazana UKE, co umożliwi regulatorowi całkowitą kontrolę procesu analiz rynkowych. Ponadto zmiana, o której mowa, przywróci stałą, pięcioletnią kadencję Prezesa UKE i ustanowi listę przesłanek uzasadniających od-

wołanie osoby stojącej na czele regulatora. Ograniczy to swobodę Prezesa Rady Ministrów do odwołania Prezesa UKE w dowolnym czasie oraz bez potrzeby wskazywania powodów takiego odwołania, co było przedmiotem zaniepokojenia Komisji. Komisja przekazała powyższą sprawę o naruszenie prawa wspólnotowego przez Polskę do Europejskiego Trybunału Sprawiedliwości w lipcu 2008 r.

O dodatkowych sędziów poszerzył się skład Sądu Ochrony Konkurencji i Konsumentów, który wraz z Wojewódzkim Sądem Administracyjnym jest odpowiedzialny za rozpatrywanie spraw związanych z sektorem łączności elektronicznej, co spowodowało wzrost całkowitej liczby sędziów z 4 do 11. Zwiększenie liczby sędziów przyczyniło się do nieznacznego skrócenia procesu odwoławczego, który obecnie nie przekracza dwóch lat. Jednak operatorzy podkreślają, że sądy skupiają się na kwestiach proceduralnych, natomiast nie odnoszą się do kwestii merytorycznych. Wzrasta liczba zaskarżonych decyzji; w momencie opracowywania raportu 500 spraw odwoławczych było w toku.

Proces decyzyjny

Prezes UKE realizował politykę regulacyjną zgodną z kierunkiem wytyczonym w poprzednich latach.

Regulator nie ukończył pierwszej rundy analiz rynkowych w 2008 r. Ponowna notyfikacja ostatniego rynku świadczenia usługi hurtowej dzierżawy odcinków łączy nie będących zakończeniami łączy została zarejestrowana w grudniu, a następnie została częściowo wycofana. W notyfikacji wskazano na brak skutecznej konkurencji oraz zaproponowano zróżnicowanie obowiązków regulacyjnych stosownie do poziomu konkurencji na różnych rynkach produktowych. Druga runda analiz rynkowych rozpoczęła się w połowie 2008 r., a plany UKE przewidywały ponowne przeanalizowanie wszystkich 18 rynków określonych w poprzednim zaleceniu Komisji. Nowe zalecenie nie zostało do tej pory w Polsce wdrożone, gdyż Ministerstwo nie wydało jeszcze nowego rozporządzenia.

W celu ułatwienia dostępu nowym graczom rynkowym zatwierdzone zostały w 2008 r. nowe oferty ramowe w zakresie połączenia sieci, dostępu typu bitstream oraz uwolnienia pętli lokalnej (LLU). Nowy plan stopniowego obniżania stawek za zakańczanie połączeń w sieciach ruchomych (MTR) został wprowadzony w październiku, a na jego podstawie ustalono większe obniżki w stosunku do tych, które były przewidziane w roku poprzednim. W celu zwalczania wykluczenia cyfrowego UKE organizował w 2008 r. przetargi na widmo radiowe na potrzeby bezprzewodowego dostępu do szerokiego pasma oraz opracował mapę białych plam, pokazującą obszary, na których Internet szerokopasmowy wciąż nie był dostępny. Europejski numer 116 został uruchomiony w listopadzie. Pomimo silnego zaangażowania ze strony UKE, nie uległy znacznej poprawie takie elementy, jak penetracja Internetu szerokopasmowego, warunki dostępu lub inwestycje. Proces decyzyjny pozostał co do zasady niezmieniony, charakteryzując się częstym wykorzystywaniem rozstrzygania sporów jako narzędzia regulacyjnego oraz uciekaniem się do metody ręcznego sterowania przez Prezesa UKE.

Na rynku wciąż przynosiły pozytywne skutki decyzje wydane w latach poprzednich, na podstawie których wprowadzono hurtową odsprzedaż abonamentu (WLR) czy dostęp typu bitstream (BSA), jednak pewne obawy budził brak spójnej strategii czy też podejścia do ustalania cen, które umożliwiłoby alternatywnym operatorom przesunąć się w górę drabiny inwestycyjnej. Po tym, jak powiązana z operatorem zasiedziałym spółka świadcząca usługi telefonii ruchomej rozpoczęła świadczenie usług detalicznego Internetu szerokopasmowego oraz usług głosowych po cenach konkurencyjnych, korzystając z dużej zniżki uzyskanej na poziomie hurtowym dzięki metodzie „mniej o cenę detaliczną" (*retail minus*), konieczne okazało się zbliżenie cen hurtowych do kosztów. Urząd Ochrony Konkurencji i Konsumentów, równolegle z UKE, analizował, czy zostały w opisanym przypadku naruszone zasady konkurencji.

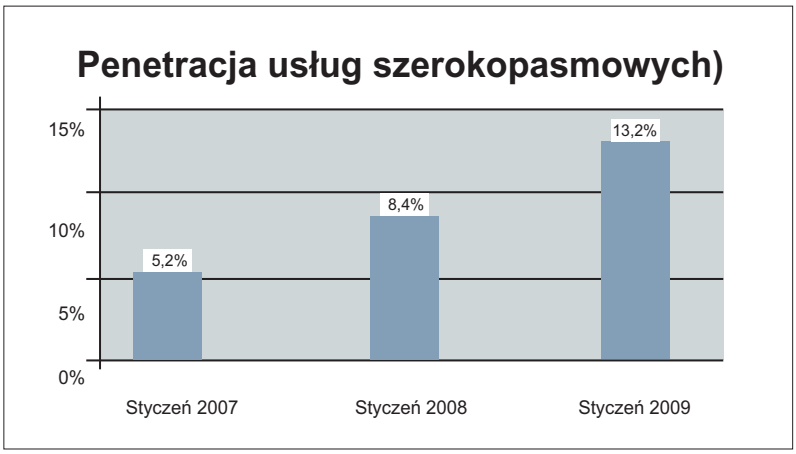
Operatorzy nadal uciekali się do procedury rozstrzygania sporów oraz korzystali z prawa do odwołania w celu doprecyzowania szerokiego wachlarza nie zawsze dostatecznie szczegółowych środków regulacyjnych nałożonych przez regulatora. Do października departament odpowiedzialny w UKE za rozstrzyganie sporów wydał 130 decyzji regulacyjnych, z których około połowa dotyczyła WLR, BSA i LLU. Proces wydawania wyżej wspomnianych decyzji trwał zazwyczaj znacznie dłużej niż przewidziane cztery miesiące, przy czym niektóre sprawy trwały nawet ponad dwa lata. Opisane podejście regulatora polegające na wydawaniu licznych decyzji i zmian wydaje się naruszać spójność, przejrzystość oraz pewność prawną dla graczy rynkowych.

Ponadto większość obowiązków regulacyjnych będących obecnie w mocy jest wciąż oparta na tzw. benchmarkach (zestawieniach porównawczych) lub na metodologii „mniej o cenę detaliczną" (*retail minus*), pomimo że obowiązek orientacji kosztowej został nałożony na operatora zasiedziałego, po zatwierdzeniu kalkulacji kosztowej przez niezależnego audytora. Pozytywna opinia w tej sprawie została wydana już drugi rok z rzędu w czerwcu 2008 r. Podczas prac nad niniejszym raportem regulator prowadził rozmowy z operatorem zasiedziałym na temat stopniowego dostosowania do kosztów. Komisja badała sprawę w wyniku formalnej skargi złożonej w tej sprawie.

Zmiany rynkowe i regulacyjne

Przychody w sektorze telekomunikacyjnym w 2007 roku wyniosły 13,16878 miliarda euro, co stanowi wzrost o około 27 proc. w stosunku do roku poprzedniego. Przychody z rynków stacjonarnych wyniosły 2,81 miliarda euro w 2007 roku, podczas gdy przychody wygenerowane przez rynek telefonii komórkowej wyniosły 5,97 miliarda euro. Ogólna wartość inwestycji materialnych w sektorze komunikacji elektronicznej wzrosła do 2,64 miliarda euro, przy czym większość inwestycji pochodziła od operatorów komórkowych.

W roku 2008 nie zanotowano znaczących inwestycji w sieci następnej generacji (NGN), jak również podejście regulacyjne do inwestycji w NGN nie zostało jasno zdefiniowane. 18 grudnia Prezes UKE



przedstawił do konsultacji opinię dotyczącą budowy i eksploatacji sieci NGN w Polsce. We wrześniu operator zasiedziały opublikował strategię na ten temat, szacując koszt koniecznych inwestycji na od 14 do 28 miliardów PLN (ok. 4,1 miliarda euro i 8,2 miliarda euro) oraz wskazując, że przyszłe inwestycje będą zależały od współpracy z władzami publicznymi. Oznajmił ponadto, że ilość danych przesyłanych przez sieci stacjonarne powiększyła się trzykrotnie w ciągu ostatnich 24 miesięcy i czterokrotnie w przypadku telefonii komórkowej. Część alternatywnych operatorów potwierdziła gotowość do unowocześnienia swoich technologii i inwestycji w sieci światłowodowe, wykorzystując dostępność funduszy UE.

Zastępowanie telefonii stacjonarnej telefonią komórkową było bardzo wyraźne, gdyż liczba wydzwanianych minut z telefonów stacjonarnych spadła o 14,3 proc. Wraz z wejściem na rynek telefonii komórkowej czwartego operatora, i osiągnięciem przez niego ok. 4,75 proc. rynku, oraz kilku wirtualnych operatorów telefonii komórkowej (MVNOs) konkurencja stała się bardziej zaciekła. Na rynku telefonii stacjonarnej udział operatora zasiedziałego uległ zmniejszeniu oraz zaobserwowano znaczące konsolidacje wśród operatorów alternatywnych.

Oferty pakietowe stawały się coraz bardziej popularne, poprzez fakt, iż operatorzy wchodzili na nowe rynki oferując dodatkowe usługi. Jednakże oferty pakietowe na dwie usługi były nadal najpopularniejsze, z uwagi na cenę jako czynnik decydujący.

Opierając się na wnioskach płynących z pogłębionej analizy kosztów i zysków opublikowanej w listopadzie, regulator postanowił rozpocząć procedurę funkcjonalnej separacji operatora zasiedziałego. Raport stwierdzał, że ekonomiczne koszty separacji oraz zyski z jej wdrożenia będą porównywalne. Podczas gdy narzędzie to będzie efektywne w walce z zachowaniami dyskryminującymi na rynku telefonii stacjonarnej oraz wzmocni stopień pewności prawnej, to jednak nie wyeliminuje innych barier, takich jak niska jakość sieci dostępowej; konieczna będzie znaczna liczba poprawek legislacyjnych przed implementacją. W tym samym czasie UKE negocjował z operatorem zasiedziałym alternatywne możliwości wobec pełnej separacji, włączając w to dobrowolne poddanie się restrukturyzacji i opracowanie wskaźników wydajności, pozwalających na dostęp alternatywnym operatorom na niedyskryminujących warunkach.

Usługi szerokopasmowe

Sytuacja rynkowa

Penetracja usług szerokopasmowych w Polsce podlegała ciągłemu wzrostowi i zwiększyła się o 57,69 proc. w opisywanym okresie, osiągając 13,2 proc. w styczniu 2009 roku. Jednakże wynik ten sytuuje się ciągle wśród najniższych w UE-27 i jest znacząco niższy niż średnia UE, która wynosi 22,9 proc. Oferowane prędkości są również jedne z najwolniejszych, 83,1 proc. z nich mieści się między 144 Kbps i 2 Mbps, natomiast europejska średnia wynosi 25,1 proc. w tym segmencie. Udział operatora zasiedziałego w rynku usług szerokopasmowych spadł do 50,3 proc., lecz jego udział w segmencie łączy DSL pozostał wysoki (80 proc. w styczniu 2009 r.). Wzrost zanotowano głównie w odniesieniu do technologii innych niż DSL, gdzie liczba łączy podwoiła się w ciągu opisywanego okresu, osiągając ponad 2 miliony w styczniu 2009 roku.

Jeśli chodzi o usługi szerokopasmowe w telefonii komórkowej, były one dostępne tylko w większych miastach i stopień ich penetracji wyniósł 3,9 proc., czyli poniżej średniej UE, która wyniosła 13 proc. Jednakże penetracja rynku dedykowanych komórkowych kart pamięci (*mobile dedicated data cards*) wyniosła 2,8 proc., co jest zgodne z unijną średnią. Co więcej, rosła popularność tych usług, gdyż zgodnie z danymi operatorów 11 proc. nowych abonamentów na usługi szerokopasmowe dotyczy telefonów komórkowych, w porównaniu do 6 proc. rok wcześniej. Wynika to głównie z obniżki cen, która wystąpiła po wprowadzeniu na rynek oferty szerokopasmowych usług komórkowych przez czwartego operatora od lipca 2008 r., a także z obecności na rynku ofert polegających na dofinansowaniu komputerów w zamian za zawarcie umowy długoterminowej.

Niska penetracja telefonii stacjonarnej (w szczególności na terenach wiejskich) oraz brak inwestycji w dotychczasową sieć wciąż stanowią nieodłączną barierę wzrostu penetracji szerokopasmowych usług telefonii stacjonarnej. Cyfrowy podział między obszarami wiejskimi, gdzie zasięg szerokopasmowych usług w technologii DSL wynosi 42,5 proc., a średnią krajową większą o 21,5 proc. stanowi istotny problem. Wzrost konkurencji usługowej, w sytuacji gdy 12 operatorów alternatywnych świadczy usługi w oparciu o hurtowe ceny dostępu bitstream, doprowadził do kolejnej obniżki cen. Duża liczba samorządów lokalnych również oferuje darmowy dostęp do Internetu z ograniczonymi prędkościami w celu walki z wykluczeniem cyfrowym. Uwolnienie lokalnej pętli abonenckiej ciągle nie funkcjonowało prawidłowo, ponieważ tylko 1554 linie zostały uwolnione do stycznia 2009. Jednakże operator zasiedziały zagwarantował dostęp do 143 punktów kolokacji, pozwalając na uwolnienie 1,9 miliona linii. Kolejnych 20 punktów jest w trakcie przygotowań.

Głównymi konkurentami operatora zasiedziałego w zakresie usług szerokopasmowych byli operatorzy telewizji kablowej, których udział w rynku rósł stopniowo, osiągając około 1,3 miliona łączy w styczniu 2009 r., i którzy – ogólnie rzecz biorąc – byli

w stanie zaoferować większe prędkości, osiągające 20 Mbps, w porównaniu do DSL. Sektor telewizji kablowej jest jednak rozczłonkowany i nie obejmuje terenów wiejskich.

W grudniu 2008 roku spółka-córka operatora zasiedziałego uruchomiła dostęp do Internetu używając technologii CDMA, która pozwala na szybkość transferu wynoszącą około 1 Mbps i wykorzystuje częstotliwość 450 MHz, wcześniej zarezerwowaną dla analogowej telefonii komórkowej. Ruch ten potencjalnie udostępni usługi szerokopasmowe dla około 2 milionów gospodarstw domowych na terenach wykluczonych cyfrowo. Przewiduje się, że zasięg, który w 2008 roku objął 50 proc. populacji, wzrośnie do 90 proc. w 2009 roku.

Kwestie regulacyjne

W grudniu 2008 r. po konsultacjach (nie odnoszących się do cen) UKE opublikował nową ofertę ramową dotyczącą uwolnienia pętli lokalnej (RUO). Oferta całkowicie zmieniła propozycję operatora zasiedziałego i poważnie obniżyła ceny z 36 PLN do 22 PLN (około 10,6 euro i 6,5 euro) oraz koszty kolokacji. Ponadto UKE zmienił sam proces poprzez skrócenie czasu implementacji oraz minimalizację uczestnictwa abonentów. Operator zasiedziały wyrażał obawy, że nałożone stawki nie biorą pod uwagę kalkulacji kosztów i rezultatów negocjacji.

Według danych UKE, do października trzej operatorzy uwolnili zaledwie 1544 linie. Jednakże tylko jeden z nich efektywnie konkurował na rynku detalicznym. Winę za opóźnienia w procesie uwalniania pętli operatorzy alternatywni przypisywali dyskryminującym działaniom operatora zasiedziałego, które przybierały formy częstych problemów technicznych lub przekazywania niekompletnych bądź błędnych informacji. W tym samym czasie operator zasiedziały wskazywał brak spójności między cenami różnych produktów hurtowych jako przyczynę takiego stanu rzeczy. Jednakże wprowadzenie nowej oferty ramowej dotyczącej uwolnienia lokalnej pętli abonenckiej (LLU) w grudniu odwróciło sytuację poprzez zmniejszenie ceny LLU w stosunku do WLR i dostępu bitstream.

Na początku maja 2008 r. Prezes UKE zatwierdził nową ofertę ramową dotyczącą dostępu bitstream, która rozszerzyła zakres obowiązków świadczenia dostępu na wszystkich poziomach, włączając w to DSLAM i ATM, a także poziom zarządzanego i niezarządzanego IP. Operatorzy byli zaniepokojeni brakiem konsultacji w sprawie ustalenia cen hurtowych. Z aprobatą natomiast należy odnieść się do faktu, że UKE odstąpił od regulacji opartej na środkach przejściowych na rzecz ofert ramowych opartych na analizach rynku.

Wiele samorządów lokalnych finansowało darmowy dostęp do Internetu o ograniczonych prędkościach (do 250 Kbps) i z ograniczonym dostępem do treści. Jako część strategii w walce z cyfrowym wykluczeniem UKE zdecydowanie popiera ten proces poprzez lokalne przetargi na częstotliwości 3600-3800 MHz. Rząd obniżył również opłaty za prawo do dysponowania częstotliwością dla mniej zaludnionych terenów. W październiku Prezes UKE konsultował przetarg na bezprzewodowy dostęp szerokopasmowy (obejmujący 18 rezerwacji na częstotliwości krajowe z zakresu 2010-2025 MHz i 2500-2690 MHz), którego jednym z warunków jest przeznaczenie 20 proc. widma na bezpłatny bezprzewodowy dostęp szerokopasmowy z pewnymi ograniczeniami w transmisji danych. Operatorzy byli zaniepokojeni wspieraniem darmowego Internetu przez UKE, w szczególności z powodu braku określenia dolnych limitów transferu.

Po wyroku Sądu Odwoławczego z dnia 10 kwietnia 2008 r. sądy krajowe podtrzymały decyzje UKE z lat 2006 i 2007 dotyczące regulacji detalicznego dostępu szerokopasmowego podjęte bez uprzedniej analizy rynku. Dopiero w listopadzie, po decyzji Komisji o skierowaniu sprawy do Europejskiego Trybunału Sprawiedliwości, Sąd Ochrony Konkurencji i Konsumentów zdecydował o zawieszeniu postępowania do momentu otrzymania dodatkowych informacji o wniosku Komisji.

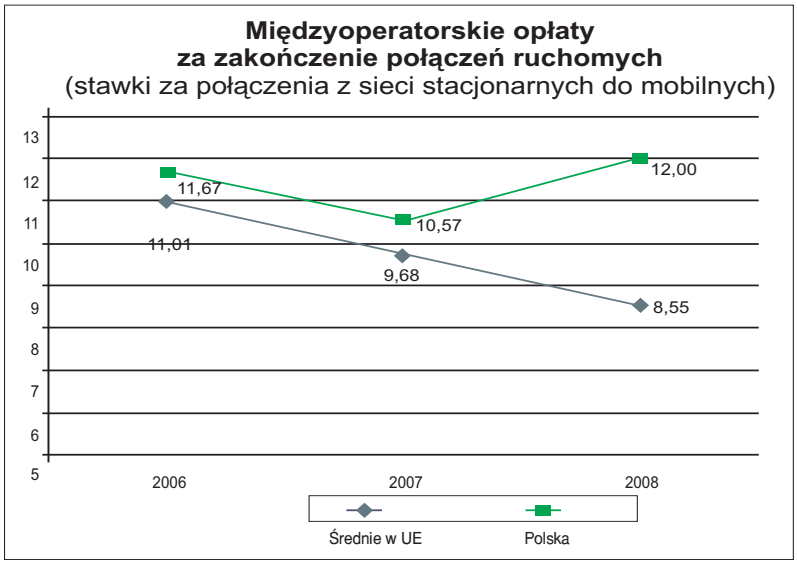
Rynki telefonii mobilnej

Sytuacja na rynku

Po kolejnym roku intensywnego wzrostu (około 9 punktów procentowych w okresie sprawozdawczym) współczynnik penetracji rynku telefonii ruchomej osiągnął w październiku 2008 r. pułap 101 proc., który jednakże wciąż jest niższy od średniej unijnej, wynoszącej 118,9 proc. W roku 2008 nastąpił także duży wzrost natężenia ruchu w telefonii ruchomej, który zwiększył się o 32 proc. w okresie sprawozdawczym. Trzech największych operatorów sieci na polskim rynku telefonii ruchomej zachowało swoje udziały w rynku, wynoszące odpowiednio 33,07 proc., 31,96 proc. i 34,97 proc. (pod względem liczby abonentów w październiku 2008 r.). Czwarty (mniejszy) gracz od czasu wejścia na rynek w zeszłym roku zdołał zdobyć ponad 1,67 miliona klientów i osiągnął udział w rynku na poziomie około 4,75 proc. Jednakże z jedenastu wirtualnych operatorów telefonii ruchomej tylko jeden zdołał zdobyć ponad 100 000 abonentów, co stanowi mniej niż 1 proc. udziału w rynku. W miarę dojrzewania rynku nowi jego uczestnicy wraz z wirtualnymi operatorami telefonii ruchomej przyciągają klientów dzięki zdecydowanym działaniom marketingowym oraz kierowaniu swojej oferty do klientów niszowych.

W odniesieniu do tendencji panujących na detalicznym rynku telefonii ruchomej, po dużych redukcjach cen z lat poprzednich, abonenci uzyskali dalsze obniżki w 2008 r., zwłaszcza w odniesieniu do popularnych koszyków usług dla mniej aktywnych użytkowników, a ceny w ramach taryf detalicznych plasują się wśród najniższych w UE; minuta połączenia głosowego kosztowała średnio 0,10 euro (podczas gdy średnia cena w UE wynosi 0,14 euro). Gwałtowny wzrost penetracji rynku telefonii ruchomej pokazuje, że cena nie jest już barierą dla konsumentów. Operatorzy telefonii ruchomej w ciągu ostatnich kilku lat intensywnie inwestowali w modernizację swoich sieci i polepszenie zasięgu technologii 3G, a także w innowacyjne usługi, takie jak możliwość dokonywania opłat przy użyciu telefonu komórkowego lub sprawdzanie lekarskich terminarzy w celu umówienia wizyty.

Konsorcjum czterech operatorów telefonii ruchomej wyraziło zainteresowanie konkursem na częstotliwo-



ści z zakresu 470-790 MHz, które pozwoliłyby im na świadczenie usługi telewizji ruchomej w 31 miastach do 2015 r., a następnie na całym terytorium Polski. W razie zrealizowania powyższego planu konsorcjum oferowałoby tego typu usługi na rynku hurtowym dla wszystkich zainteresowanych stron.

Dwóch operatorów, którym w 2007 r. przyznano częstotliwości w paśmie 1800 MHz, nie zaczęło jeszcze budowy swoich sieci. Podczas gdy jeden z nich był w trakcie podpisywania niezbędnych umów i zamierzał rozpocząć budowę sieci na początku następnego roku, drugi z nich doświadczył trudności w uzyskaniu finansowania i nie podjął jeszcze starań o roaming krajowy. Zgodnie z wymaganiami dotyczącymi rozwoju sieci, operatorzy powinni objąć usługami 15 proc. ludności do końca 2009 r.

Liczba graczy na rynku telefonii ruchomej prawdopodobnie dalej wzrośnie, w następstwie przeprowadzonego w listopadzie przetargu na dwie rezerwacje, z których każda obejmuje 25 kanałów dupleksowych w paśmie GSM 900 MHz. Czwartemu operatorowi telefonii ruchomej przyznano obie rezerwacje, chociaż finalnie wybrał jedną z nich, a druga została przyznana nowemu podmiotowi na rynku związanemu z dużym nadawcą.

Kwestie regulacyjne

W sierpniu 2008 r. Prezes UKE zakończył analizę rynku dostępu do telefonii ruchomej poprzez zamknięcie procedury mającej określić, czy jest on w pełni konkurencyjny. Choć nie stwierdzono wyraźnie, czy rynek ten jest konkurencyjny, to jednak nie został on poddany regulacji.

Stawki za zakańczanie połączeń u trzech dużych operatorów sieci ruchomej spadły do poziomu 0,3387 zł (0,09 euro) w maju 2008 r., zgodnie z przyjętym harmonogramem (*glidepath*) z kwietnia 2007 r. W celu dalszych redukcji cen płaconych przez użytkowników końcowych za rozmowy w telefonii ruchomej UKE wydał decyzje zobowiązujące operatorów do ustalenia stawek hurtowych zgodnie z nowo ustalonym harmonogramem obniżek. Powinny one zostać ustalone na poziomie 0,2162 zł (0,06 euro) od stycznia 2009 r. i osiągnąć 0,1667 zł (0,05 euro) w lipcu 2009 r. Według informacji opublikowanych na stronie internetowej, UKE planuje dalej redukować stawki za zakańczanie połączeń w telefonii ruchomej, o około 10 proc. rocznie, w celu uzyskania poziomu 0,11 zł (0,03 euro) w lipcu 2013 r. Prezes UKE poddał także konsultacjom możliwość wprowadzenia rozliczeń typu „*bill and keep*" („taryfikuj i zatrzymaj"). Operatorzy telefonii ruchomej wyrazili zaniepokojenie, iż nie skonsultowano się z nimi w sprawie tych decyzji oraz że zostały one wydane w trakcie przeprowadzania analizy rynku właściwego, a także w czasie obowiązywania poprzednio ustalonego harmonogramu obniżek, obowiązującego do 2010 r., co negatywnie wpływa na prawną i ekonomiczną stabilność. Planowali ich zaskarżenie. Komisja wyraziła zaniepokojenie faktem, że wyżej opisane decyzje nie zostały notyfikowane.

Obecnie stawki za zakańczanie połączeń czwartego operatora sieci ruchomej oraz wirtualnych operatorów sieci ruchomej nie podlegają reżimowi stopniowych obniżek pułapów cenowych, ponieważ UKE zdecydował nie stosować w stosunku do nich kontroli cenowej. Prezes UKE planuje redukować tę nierówność co roku, zaczynając od poziomu 157 proc. w dniu 1 stycznia 2009 r., w celu osiągnięcia poziomu 0,11 zł (0,3 euro) dla wszystkich operatorów w 2014 r., zgodnie z informacją opublikowaną na stronie internetowej.

Kolejna niepewność została wywołana przez swobodnie definiowane obowiązki pokontrolne, nałożone na trzech operatorów sieci ruchomej w lipcu 2008 r., wymagające od nich usunięcia naruszeń obowiązku „braku dyskryminacji" w odniesieniu do ustalania cen za rozmowy wewnątrz sieci. Operatorzy telefonii ruchomej zinterpretowali to posunięcie jako próbę regulacji ich ofert detalicznych, gdyż stawki za zakańczanie połączeń zostały już ustalone w rozporządzeniu. Według UKE, celem decyzji było pokazanie dysproporcji cen między połączeniami wewnątrz sieci a między sieciami.

Kwestia nałożenia obowiązku zapewnienia dostępu wirtualnym operatorom telefonii ruchomej przez jednego z operatorów sieci ruchomej, bez względu na jego siłę rynkową, została ostatecznie rozstrzygnięta, po tym jak w grudniu 2008 r. Prezes UKE poddał konsultacjom projekt decyzji odmawiającej dostępu. Nastąpiło to po listopadowym orzeczeniu Europejskiego Trybunału Sprawiedliwości, dotyczącym niewłaściwej implementacji dyrektywy o dostępie w Polsce (sprawa C-227/07), które potwierdziło opinię Komisji o naruszeniu przez Polskę ram regulacyjnych poprzez zobowiązanie operatorów do podejmowania negocjacji w sprawie dostępu telekomunikacyjnego, bez względu na ich siłę rynkową. Wskazało ono jednakże również, że Komisja nie przedstawiła wystarczających dowodów w odniesieniu do uprawnień krajowego regulatora do podejmowania interwencji zgodnie z dyrektywą.

Sieć stacjonarna

Sytuacja na rynku

Pomimo wzmożonej konkurencji ze strony alternatywnych operatorów, operator zasiedziały pozostał największym graczem na rynku telefonii stacjonarnej, a jego udział spadł jedynie nieznacznie do 69,8 proc. rynku rozmów telefonii stacjonarnej

(w grudniu 2007 r., liczony w kategoriach minut ruchu). We wrześniu 2008 r. alternatywni operatorzy obsługiwali ponad 700 000 linii na bazie umów o hurtową odsprzedaż abonamentu (WLR). Na rynku dokonała się także znacząca konsolidacja dużych alternatywnych graczy, co oznacza, że operator zasiedziały musiał zmierzyć się z bardziej jednolitą konkurencją, wraz z głównym alternatywnym operatorem, mającym 15 proc. udziałów w rynku (w grudniu 2007 r.) w rozumieniu osiąganych przychodów. Alternatywni operatorzy byli jednakże zaniepokojeni faktem, że operator zasiedziały zaczął transferować świadczone przez siebie usługi detaliczne do spółki zajmującej się telefonią ruchomą, która rozpoczęła świadczenie stacjonarnych usług głosowych w listopadzie. Możliwości wyboru dla konsumenta na rynku telefonii stacjonarnej wzrosły w 2008 r. w związku z tym, że 85 operatorów zapewniało publicznie dostępne usługi telefoniczne od lipca 2008 r.

W związku z tym, że abonamenty na telefonię stacjonarną stały się mniej popularne, a objętość ruchu zmalała o niemal 4 miliardy minut, operatorzy podjęli szereg kroków w celu powstrzymania odpływu konsumentów. Klienci mogli teraz czerpać korzyści z niższych taryf (włączając także te zapewniane przez operatora zasiedziałego), pakietów darmowych minut lub ulepszonych usług telefonii internetowej (VoIP).

Wzrost w zakresie liczby abonentów usług telefonicznych świadczonych drogą kablową zwolnił w 2008 r., osiągając 440 000 w połowie 2008 r., w porównaniu z 420 000 rok wcześniej (zgodnie z danymi dostarczonymi we wrześniu przez stowarzyszenie operatorów kablowych (Polska Izba Komunikacji Elektronicznej – PIKE)). Ich ogólny udział w rynku pozostaje marginalny.

Kwestie regulacyjne

8 kwietnia 2008 r. Prezes UKE zaaprobował nową ofertę ramową w zakresie połączenia sieci (RIO), ustalającą ceny hurtowe za inicjowanie i zakańczanie połączeń, zgodnie z wynikami kalkulacji kosztów operatora zasiedziałego na 2007 r. Jednakże ceny za hurtową odsprzedaż abonamentu (WLR) oraz płaską stawę interkonektową pozostały niezmienione i wciąż ustalane były zgodnie z własną metodologią krajowego regulatora. Dla operatora zasiedziałego niepokojące było to, że oferta ramowa nie została skonsultowana z graczami rynkowymi oraz zawierała usługi, które nie stanowiły części definicji rynku właściwego, więc zasugerował on UKE ponowne przeanalizowanie oferty, co stanowiło pierwszy krok w procedurze odwoławczej.

Niepewność regulacyjna była do pewnego stopnia obecna wciąż w 2008 r., ponieważ hurtową odsprzedaż abonamentu nadal wdrażano na podstawie 17 decyzji wydanych w związku z rozwiązywaniem sporów między operatorami. Tylko w jednej umowie handlowej, podpisanej ze spółką operatora zasiedziałego zajmującego się telefonią ruchomą, koszty zostały oszacowane przy użyciu metodologii „*retail minus*". Słaby prawnie status decyzji w sprawie WLR stał się widoczny, kiedy w czerwcu polski sąd apelacyjny zakwestionował jedną z nich i zawiesił jej wykonanie. UKE zareagował wydaniem nowej decyzji z urzędu i bez konsultacji, na okres sześciu miesięcy. Powoływał się na pilną potrzebę ochrony użytkowników końcowych oraz zapewnienia ciągłości świadczenia usług.

Asymetria stawek za zakańczanie połączeń w telefonii stacjonarnej pozostała bardzo wysoka w Polsce w roku 2008, osiągając 500 proc. Był to efekt indywidualnych decyzji UKE mających w założeniu pozwolić alternatywnym operatorom bardziej efektywnie konkurować, a także niektórych umów handlowych zawartych przez operatora zasiedziałego w 2007 r. Zgodnie z informacjami opublikowanymi na jego stronie internetowej w październiku, Prezes UKE planuje stopniowo usunąć różnice w stawkach, aby osiągnąć pełną symetrię w styczniu 2014 r. Powinna jednakże zostać podjęta formalna decyzja w tej sprawie.

Radiodyfuzja

Sytuacja rynkowa

W 2008 roku rynek doświadczył dalszego zmniejszenia o 0,9 miliona liczby abonentów analogowej transmisji naziemnej jako głównego środka odbioru treści telewizyjnych (w porównaniu z 38,8-proc. udziałem w rynku w połowie 2008 na podstawie danych przekazanych przez PIKE). Użytkownicy przenieśli się głównie do trzech cyfrowych platform satelitarnych, które we wrześniu 2008 r. posiadały 27,6 proc. udziału w rynku (wzrost o 1,1 miliona abonentów), jak i do operatorów kablowych, którzy posiadali 33,6 proc. udziałów i świadczyli usługi 140 programów telewizyjnych, włączając w to kanały w formacie HD.

Penetracja usług telewizji kablowej nie uległa zmianie, osiągając 6 milionów biernych oraz 4,5 miliona aktywnych użytkowników u około 630 operatorów. Główny wzrost odnotowano w obszarze cyfrowych sieci kablowych, które – zdaniem PIKE – miały osiągnąć pod koniec roku liczbę 500 000 abonentów, z uwagi na to, iż w maju duży gracz rynkowy uruchomił usługi cyfrowej telewizji satelitarnej. Mimo postępu, jest to wciąż mała baza abonentów w porównaniu do cyfrowych usług satelitarnych.

Operator zasiedziały, który w październiku posiadał około 60 000 abonentów IPTV, poszerzył swoją ofertę włączając w nią usługi oparte na technologiach satelitarnych. Pozwoli to na zwiększenie pokrycia, ponieważ operator zasiedziały zamierza zdobyć ponad milion użytkowników usługi IPTV w ciągu najbliższych dwóch lat. Jego główny konkurent testował usługi IPTV w ramach umowy z platformą satelitarną i zamierzał wprowadzić usługi na rynek w pierwszej połowie 2009 roku.

Kwestie regulacyjne

Pomimo iż w roku 2008 nie przyjęto formalnie nowej strategii przejścia na nadawanie cyfrowe, Polska planuje wyłączenie nadawania analogowego do końca 2014 roku. Choć pierwszy multipleks zostanie zarezerwowany dla obecnych nadawców analogowych, pojawiły się pewne nieporozumienia pomiędzy poszczególnymi organami dotyczące procedury przydzielania nadawców do drugiego multipleksu. Opóźnienia są również spowodowane niechęcią prywatnych nadawców do zaprzestania użytkowania częstotliwości analogowych do 2014 roku, w zamian

za częstotliwości cyfrowe, bez przedstawienia konkretnych planów.

W listopadzie UKE przeprowadził konsultacje publiczne mające na celu ocenę zainteresowania usługami cyfrowego nadawania radiowego w paśmie 1452-1492 MHz.

Regulacje horyzontalne

Zarządzanie widmem

Polityka regulatora skierowana jest na ułatwianie dostępu do widma oraz skuteczne użytkowanie ograniczonych zasobów, celem zwiększenia ekonomicznych i społecznych korzyści. Żadne decyzje nie zostały podjęte w odniesieniu do dywidendy cyfrowej.

Obrót widmem pomiędzy przedsiębiorstwami jest dozwolony, pod warunkiem że obie strony się na to zgadzają. Jednakże nie dotyczy to widma przydzielonego w wyniku przetargu, w przypadku którego wymagana jest przychylna decyzja regulatora oraz organu do spraw konkurencji.

Polska jest na dobrej drodze do zaimplementowania wszystkich decyzji Komisji w sprawie widma radiowego, włączając w to decyzję 2008/294/WE dotyczącą usług łączności w sieciach komórkowych na pokładzie samolotów. Prezes UKE zamierza autoryzować stacje bazowe na pokładzie polskich samolotów, co nie będzie wymagało odrębnej rezerwacji częstotliwości i będzie nieodpłatne.

Prawo drogi oraz współdzielenie urządzeń

Operatorzy skarżyli się na nieskuteczność i długość procedur (około 18 miesięcy) uzyskiwania pozwoleń. Operatorzy są również zdania, że brak planów zagospodarowania przestrzennego lub klauzul w obecnych planach blokuje możliwość budowy infrastruktury w znacznej części Polski. Operatorzy chcieliby również być bardziej włączani w proces konsultacji projektów aktów prawnych.

Prezes UKE miał opóźnienia w wydawaniu pozwoleń na użytkowanie widma radiowego, a toczące się kontrole lokalne zakończyły się w przypadku niektórych operatorów sieci komórkowych nałożeniem kar za brak zezwoleń na nadajniki.

Konsumenci

Przejrzystość taryf i jakość usług

Mimo iż taryfy są, ogólnie rzecz ujmując, skomplikowane i trudne do porównania, jeden z operatorów świadczących usługi przedpłacone oferował płaską taryfę z połączeniami do państw Unii po tej samej stawce jak stawki za połączenia krajowe, celem przyciągnięcia abonentów. Prezes UKE powziął działania mające na celu zbudowanie narzędzia umożliwiającego porównywanie taryf, celem wsparcia konsumentów przy wyborze właściwej oferty (kalkulator taryfowy). W tej sprawie zostały przeprowadzone konsultacje publiczne, które zakończyły się 14 listopada 2008 roku.

Usługa powszechna

W oparciu o komunikat Komisji dotyczący przeglądu zakresu świadczenia usługi powszechnej, Prezes UKE przeprowadził konsultacje publiczne odnoszące się do możliwości włączenia szerokopasmowego dostępu do Internetu w zakres świadczenia usługi powszechnej.

Operator zasiedziały świadczący usługi w sieci stacjonarnej, który został wyznaczony do świadczenia usługi powszechnej w maju 2006 roku, zawnioskował w tym roku o uzyskanie zwrotu w wysokości 220 milionów PLN (około 64,7 miliona euro), do podziału między wszystkich operatorów, których przychody przekroczyły 4 miliony PLN (1,1 miliona euro).

W myśl orzeczenia Wojewódzkiego Sądu Administracyjnego, który sprzeciwił się zeszłorocznej odmowie przyznania zwrotu w oparciu o przesłanki proceduralne, Prezes UKE obecnie podjął próby zweryfikowania kalkulacji kosztów. Jednakże decyzja w tej sprawie jest spodziewana nie wcześniej niż w drugiej połowie 2009 roku, w związku z ograniczeniami budżetowymi w zatrudnianiu ekspertów zewnętrznych.

Operatorzy alternatywni utrzymują, że kwota zwrotu została zawyżona przez taryfę socjalną, której cena została ustalona poniżej kosztów i była dostępna dla wszystkich nowych abonentów, a nie tylko dla użytkowników niepełnosprawnych lub będących w trudnej sytuacji finansowej. Taryfa była dostępna dla nowych abonentów jedynie do grudnia i została zastąpiona inną, dostępną tylko dla najbardziej potrzebujących osób.

Mimo ogólnej poprawy świadczenia usług, w listopadzie operator zasiedziały został ukarany za łamanie warunków świadczenia usługi powszechnej, w tym w szczególności z powodu czasu oczekiwania użytkowników końcowych na przyłączenie do sieci.

Przenośność numerów

Mimo iż przenośność numerów zarówno w sieciach stacjonarnych, jak i komórkowych jest dostępna od 2006 roku, procedura ta pozostaje skomplikowana i nieefektywna. Choć przeniesienie numeru w sieci stacjonarnej zajmuje obecnie średnio 23 dni, liczba przeniesionych numerów w sieci stacjonarnej wzrosła czterokrotnie w roku 2008, osiągając w październiku 2008 roku liczbę 294 691.

Liczba numerów przeniesionych w sieciach komórkowych wzrastała powoli, osiągając w październiku 2008 r. liczbę 228 055 numerów. Stanowi to nikły odsetek (1,2 proc.) całkowitej liczby numerów w sieciach komórkowych i związane jest z długością procedur sięgającą 38 dni dla usług abonamentowych i około tygodnia dla numerów usług przedpłaconych. Na razie próby poprawy tej sytuacji na gruncie prawodawstwa wykonawczego nie przyniosły skutku.

Skargi konsumenckie oraz pozasądowe rozwiązywanie sporów

Choć polscy konsumenci stają się coraz bardziej asertywni i uważnie kontrolują swoje wydatki, korzystają oni również z usług regulatora, takich jak Centrum Informacji Konsumenckiej czy też z procedury mediacyjnej. ■

ZPAS

Szafy nie z tej ziemi!

for your connections

Obudowy teleinformatyczne i energetyczne

ZPAS S.A.
Tel. 074 8720100
Fax 074 8724074
info@zpas.pl
www.zpas.pl

Światłowody polimerowe POF vs okablowanie UTP

Mieczysław Świerszczewicz

OPTRONIK PIT Sp. z o.o.

Sytuacja rynkowa

Szybkość transmisji w sieciach dostępowych jest coraz większa w wyniku powszechnego stosowania kabli światłowodowych w sieciach szkieletowych oraz udoskonalania systemów transmisji na odcinku „ostatniej mili", włącznie z realizacją abonenckich przyłączy światłowodowych FTTB i FTTH .

Dla odbiorców oznacza to możliwość korzystania z usług TriplePlay, takich jak telewizja cyfrowa (DVB), wideo na życzenie (VoD), internet, telefonia internetowa (VoIP) oraz interaktywne serwisy informacyjne. O tym, czy rzeczywista dostępność tych usług nie skończy się na progu domu lub biura decyduje odpowiednia budynkowa instalacja kablowa.

Wymagania w stosunku do tych instalacji dotyczą nie tylko odpowiednio dużej szybkości transmisji, niezawodności i łatwości instalacji, ale również możliwości integracji wszystkich funkcji i usług dostępnych w sieciach rozległych (WAN) i sieci lokalnej (LAN) w każdym gniazdku sieciowym w budynku.

Powyższe funkcje mogą być realizowane w dobrej jakości przy wykorzystaniu Fast Ethernet o szybkości 100 MBit/s.

Wymaganą szybkość transmisji zapewnia klasyczna skrętka UTP kat. 5e/6 oraz Polymer Opitcal Fiber (POF).

Światłowody polimerowe (POF)

Światłowody polimerowe są syntetycznymi światłowodami wykonanymi z poliakrylanów (PMMA) do transmisji w zakresie światła widzialnego, najczęściej czerwonego.

Przy średnicy 1mm włókna POF mają bardzo gruby rdzeń. Prostota cięcia i łączenia oraz możliwość kontroli/identyfikacji światłem czerwonym sprawiają, że włókna POF są łatwiejsze w aplikacji niż kable UTP.

- Profil współczynnika refrakcji skokowy (SI, NA=0,5).
- Średnica rdzenia/płaszcza 980/1000 μm.
- Promień gięcia min. 20 mm.
- Siła rozciągająca max 45 N.
- Tłumienność 160 dB/km.
- Pasmo min 100 Mbit/s @100m.
- Zakres temperatur pracy -40°C...+80°C.

Charakterystyka sieci POF Fast Ethernet 100 Mbit/s (RPNet)

Podstawowymi komponentami sieciowymi POF RPNet są:

- switch sieciowy główny 100/1000 Mbit/s z portami SFP;
- transceiver SFP ze złączami zaciskowymi Optoclamp do POF;

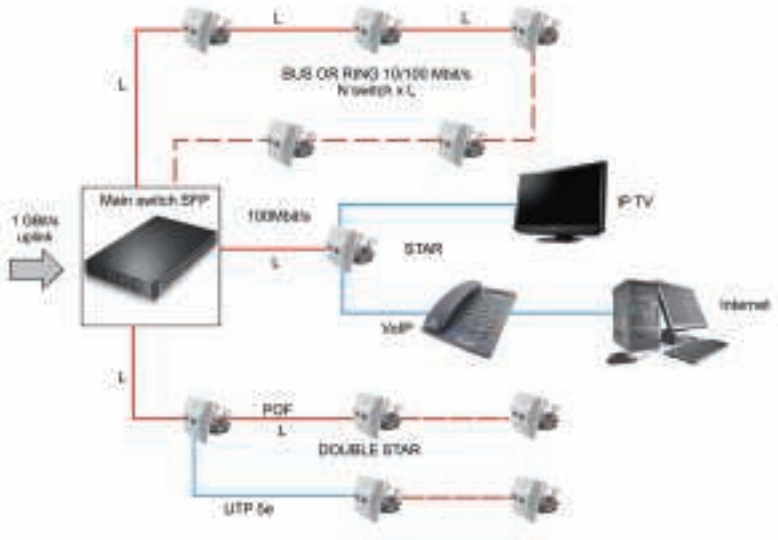
Porównanie sieci strukturalnych POF i UTP

	POF	UTP
Kompatybilność elektromagnetyczna (EMC)	++	-
Izolacja galwaniczna	++	- -
Odporność na zakłócenia/ochrona przeciwprzepięciowa	++	- -
Ochrona danych	++	-
Zachowanie w środowisku wybuchowym	++	-
Masa okablowania	+	-
Wymagania przestrzenne	++	-
Promienie gięcia	+	+
Instalacja okablowania	++	+
Montaż I uruchomienie	+	-
Koszty całkowite	+	++
++ bardzo dobre + dobre - problematyczne - - bardzo problematyczne		

- rzełącznik (media-konwerter) gniazdkowy (2 porty optyczne ze złączami zaciskowymi Optoclamp do POF oraz 2 porty RJ45, z opcją PoE);
- włókno POF duplex.

Przełączniki (media-konwertery) gniazdkowe można łączyć włóknem POF duplex w dowolnych konfiguracjach: gwiazda, magistrala (bus), pętla (ring), podwójna gwiazda. Poprzez zdalne zarządzanie każdy port przełącznika można przypisać do określonej wirtualnej podsieci (VLAN). Podstawowe ograniczenia przy projektowaniu sieci POF RPNet dotyczą odległości pomiędzy gniazdkami (L ≤ 70 m) oraz liczby przełączników w każdej pętli lub magistrali (N ≤ 8 szt.). Zasilanie przełączników może odbywać się z zasilacza centralnego lub lokalnie.

Dla porównania – okablowanie UTP wykonuje się wyłącznie w konfiguracji gwiazdy na odległość max 100 m.



Szerokopasmowy system przesyłu danych

Optymalne wyposażenie sieci FTTx i koncentrycznych

Wymagania dotyczące multimedialnych usług szerokopasmowych rosną nieustannie. Telewizja poprzez przyłącze cyfrowe czy też rozmowy wideo poprzez Skype podbijają domowe pokoje. Aby zaspokoić potrzeby użytkownika końcowego, firma Elcon oferuje rozwiązania szerokopasmowe do budowy nowych sieci oraz optymalnego wykorzystania istniejących infrastruktur kablowych.

ELCON, jako jeden z czołowych dostawców FTTH-CPES, oferuje szerokie portfolio produktów „Made in Germany".

Światłowodowy system ELCONnect dla klientów prywatnych i biznesowych podłącza urządzenia bezpośrednio do przyszłościowych sieci danych i umożliwia użytkownikom natychmiastowy dostęp do szybkich aplikacji internetowych. W szczególności unikatowa jest odmiana produktu, która opiera się na technologiach takich, jak Fast Ethernet, Gigabit Ethernet i GPON.

Daje ona użytkownikowi prawie nieograniczone możliwości – korzystanie z profesjonalnych telefonów ISDN, W-LAN dla bezgranicznej wolności, IP-TV dla szeroko zakrojonej rozrywki lub integracja interfejsów DECT oraz różnorodne urządzenia spełniające dzisiejsze i przyszłe wymagania w zakresie sieci łączności. Z innowacyjnymi produktami światłowodowymi serii ELCONnect powstaną nowe, unikatowe standardy w zakresie funkcjonalności i instalacji zestawu.

Product Manager **René Raudies** z firmy ELCON: – *Celem jest nie tylko wysoka przepustowość i wynikające z tego usługi dla użytkownika końcowego, ale zaoferowanie kompletnego pakietu od instalacji do niedrogiego i łatwego użytkowania.*

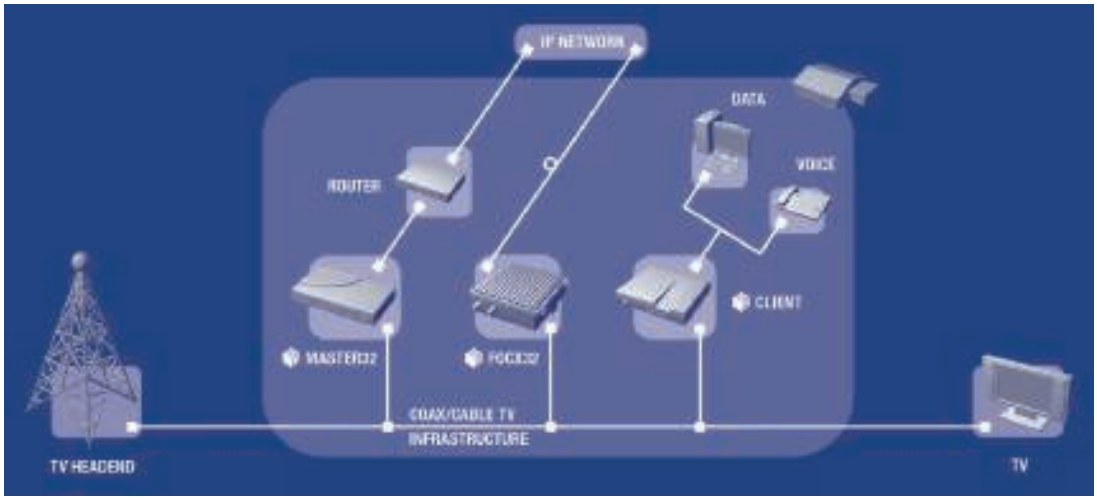
Rozwiązania światłowodowe ELCONnect jako wysoce zintegrowane i kompaktowe IADs są jedynymi produktami z wewnętrznym zarządzaniem włóknami, a więc są idealnymi urządzeniami sieciowymi do instalacji FTTH.

W preinstalacyjnej skrzynce ze zintegrowanym optycznym włóknem, która obejmuje żądane podłączenia, bezproblemowo można utworzyć połączenie u klienta poprzez podłączenie CPE. Natychmiast użytkownik ma dostęp do świata aplikacji internetowych z maksymalną 1 GB dwukierunkową przepustowością.

Niezależnie od wymaganych interfejsów procedura instalacji dla operatora sieci jest jednolita w odniesieniu do każdego klienta. Dzięki temu operatorzy sieci mają możliwość oferowania swoim klientom wszystkich dostępnych usług tanio, szybko i w doskonałej jakości.

Jako pośredni krok w migracji z istniejących sieci kablowych do FTTx, ELCON oferuje ELCONnect coax FOCX32 jako najbardziej opłacalne rozwiązanie.

Brama między włóknem światłowodowym a infrastrukturą okablowania koncentrycznego jest dzięki dużemu zasięgowi i wysokiej przepustowości optymalnym produktem do budowy nowych sieci i przyszłościowej rozbudowy istniejących struktur sieciowych.



Uzupełniając wielofunkcyjne produkty światłowodowe ELCON oferuje rozwiązania sieciowe najwyższej technologii dla sieci korporacyjnych oraz sieci publicznych (takich, jak hotele, szpitale).

Każdy dostawca telewizji kablowej, którego sieci bazują na kablu koncentrycznym, stoi dziś przed wyzwaniem ogromnych inwestycji na modernizację istniejących sieci telewizji kablowej w celu zapewnienia ruchu dwukierunkowego, co jest warunkiem koniecznym do oferowania szybkiego internetu.

Ponadto w wielu przypadkach wymiana okablowania wymaga ingerencji w strukturę budynku i bywa utrudniona ze względu na usytuowania prawne lub jest nawet zabroniona. Profesjonalny i z powodzeniem przetestowany system ELCONnect wykorzystuje istniejącą kablową infrastrukturę, a więc z pominięciem wyżej wymienionych problemów. ELCONnect zapewnia szerokopasmowy internet i VoIP doskonałej jakości.

System zapewnia zwłaszcza wysoki zakres bezpieczeństwa, dobrą dostępność, niskie promieniowanie oraz prostą instalację. Do jednego urządzenia bazowego „Master32" może być podłączonych wiele urządzeń klienckich, takich jak „Client Base" lub „Client VIP". Bez struktury repeater'a do każdego urządzenia bazowego „Master32" można przyłączyć do 32 urządzeń klienckich, do których podłączony zostanie komputer z kartą sieciową.

Tym samym funkcje sterowania i zarządzania pakietami na podstawie MAC adresów urządzeń klienckich przejmuje urządzenie bazowe „Master32".

Dzięki urządzeniu bazowemu „Master32" poszczególne urządzenia struktury sieciowej (Repeater, Client) pobierają z serwera DHCP swoje numery IP, a z serwera TFTP pliki konfiguracyjne. Ewentualnie może być ustawiona stała konfiguracja statyczna.

System ELCONnect jest idealnym rozwiązaniem dla modernizacji istniejących sieci operatorów kablowych, a zwłaszcza w budynkach mieszkalnych i hotelach. Na przykład można zaoferować gościom hotelowym usługi takie, jak szerokopasmowy dostęp do internetu oraz telefonia internetowa.

Dodatkowo technologia pozwala na spokojny sen, ponieważ system nie wydziela żadnego promieniowania. Hotel ma możliwość oferowania swoim gościom więcej usług, a tym samym zwiększenia wypełnienia hotelu.

Kontakty:

DIOMAR Sp. z o.o.
ul. Na Skraju 34
02-197 Warszawa
Tel.: +48 22 846 04 88
Fax: +48 22 868 64 83
e-mail: info@diomar.com.pl
www.diomar.pl

Wireles
ul. Surowieckiego 12a
02-785 Warszawa
Tel.: +48 22 424 56 55
Fax: +48 22 644 94 78
e-mail: office@wls.pl
www.wls.pl

Wyzwania dla wysoko wydajnych sieci

Andy Ingram

„Przetwarzanie w chmurze" i nowe reguły ekonomiczne rządzące sieciami

Sieci centrów przetwarzania danych leżą w epicentrum wielkich zmian technicznych i ekonomicznych. „Przetwarzanie w chmurze" (Cloud Computing) wraz ze wszystkimi umożliwiającymi je rozwiązaniami technicznymi z zakresu obliczeniowego, pamięci i oprogramowania już obciąża do granic możliwości istniejące sieci, mimo że to dopiero początek transformacji. Sposób, w jaki obecnie firmy zaplanują swe migracje sieciowe, zdecyduje o tym, jak przez wiele lat będzie się kształtowała ich struktura kosztów, wydajność i skalowalność – co zwiększy konkurencyjność jednych, ale innym będzie kłodą u nogi.

Centra „przetwarzania danych w chmurze" to w zasadzie „fabryki" tworzące i dostarczające usługi klientom, partnerom, pracownikom i regulatorom. O tym, co mogą robić, decydują rozwiązania techniczne, ale to, co muszą robić, wymusza ekonomia i sytuacja rynkowa – czyli muszą na przykład poprawiać jakość usług mimo kurczących się budżetów, czy też radzić sobie z lawinowo przyrastającą liczbą danych bez kompromisów ze strony jakości usług. Takie nowe środowiska produkcyjne muszą spełniać nowe wymagania. Nowe techniki umożliwiają wirtualizację przetwarzania i pamięci, centralizację infrastruktury i radykalną oraz natychmiastową rozbudowę działalności. Jednocześnie przedsiębiorstwa i konsumenci domagają się więcej treści – bogatszych i szybciej dostarczanych do dowolnego urządzenia znajdującego się w dowolnym miejscu. „Przetwarzanie w chmurze" może spełniać te nowe wymagania i zapewniać szersze możliwości – ale tylko wtedy, gdy w centrach przetwarzania danych zostaną pokonane problemy nierozerwalnie związane z budową dotychczasowych sieci obsługujących takie ośrodki.

Złożoność sieci: co się stało i dlaczego to jest ważne

Z rzadkimi wyjątkami, współczesne sieci centrów przetwarzania danych stały się zbyt skomplikowane i kosztowne, by pozwalać na realizację „przetwarzania w chmurze". Większość kierowników ośrodków przyzna, że u nich też pojawiają się poniższe tendencje:

- Nowe architektury aplikacji – stary model aplikacji „klient serwer z rozpoznawaniem stanów" ograniczał ruch aplikacji do połączeń „północ/południe" między serwerami i klientami, ale nie pozwalał na skalowanie rozwiązania do poziomu dziesiątek tysięcy użytkowników, o milionach nawet nie mówiąc. Współczesne architektury usługowe i zastosowania Web 2.0 rozprowadzają ruch do wielu specjalizowanych serwerów, stwarzając nowe wymagania w stosunku do sieci.
- Nowe treści – ponieważ współcześnie wszystko, od szkoleń do rozmów telefonicznych, jest ucyfrowiane, zachodzi potrzeba przemieszczania i magazynowania lawinowo wzrastającej ilości coraz bogatszych danych. A każda poprawa wydajności owocuje kolejnym wzrostem popytu.
- Nowe klienty – eksplozja popularności klientów bezprzewodowych i ruchomych plus całej infrastruktury serwerowej i pamięciowej niezbędnej do ich obsługiwania gwarantuje, że ruch w sieci będzie większy, a połączenia sieciowe bardziej skomplikowane. Próby wyprzedzania tych trendów są jedynie chwilowym odciążeniem, mogącym nawet prowadzić do dalszego skomplikowania sieci. Na przykład:
  więcej urządzeń sieciowych – dodawanie ich jako szybkiego sposobu na pokonanie ograniczeń przepustowości prowadzi tylko do wzrostu komplikacji, ponieważ nowe połączenia i obciążenia wprowadzają większe opóźnienia i podnoszą koszty.
- Sieci specjalizowane pod kątem jednego zastosowania – problemy w centrach przetwarzania danych często obchodzi się budując w nich dodatkowe sieci specjalizowane. Ethernetem płyną dane, Fibre Channel SAN łączą macierze dyskowe z serwerami, zaś niskozwłoczne sieci, takie jak InfiniBand przenoszą łączność międzyserwerową. Ale pofragmentowanie sieci ogromnie komplikuje próby jej wirtualizacji, a także bieżące zarządzanie.
- Koncentracja zasobów i zarządzania – konsolidowanie infrastruktury i jej eksploatacji we własnych, zleconych na zewnątrz lub współdzielonych centrach przetwarzania danych poprawia stopień wykorzystania, sprawności i kontroli, ale stwarza konieczność poświęcenia większej uwagi sprawom wydajności, dostępności i bezpieczeństwa infrastruktury sieciowej.
- Wirtualizacja – będąca zasadniczo innym sposobem koncentrowania zasobów – umożliwia budowanie zasobów pamięci, serwerów i partycji sieci z użyciem mniejszej liczby urządzeń fizycznych. W takim podejściu wiele aplikacji czy grup użytkowników może używać tej samej infrastruktury fizycznej, co prowadzi do jej lepszego wykorzystania i elastyczności dzięki możliwości rozkładania obciążeń roboczych na pule zasobów. Ale

uruchamianie i migracja wirtualnych obciążeń roboczych stwarza ogromne wymagania na wydajność i elastyczność sieci.

Nie są to problemy dotyczące wyłącznie centrów przetwarzania danych, ale z zasady objawiają się w najbardziej wyśrubowanych otoczeniach. A dotyczą także firm, które nie planują oferowania usług „przetwarzania w chmurze", jednak wykorzystują ich technologie składowe.

Ekonomia uproszczenia sieci

Współcześnie przeciążone zasoby komutacyjne i powszechna agregacja oraz warstwy szkieletowe sieci to problemy odziedziczone. Większość sieci pierwotnie projektowano do obsługi ograniczonych przepustowości i z uwzględnieniem gęstości upakowania portów w starszych generacjach ruterów i przełączników, zaś natężenie i rozpływy ruchu przewidywano dla aplikacji w architekturze klient-serwer.

Ale nie trzeba już projektować sieci w tak ułomny sposób. W sytuacji idealnej moglibyśmy zaprojektować scentralizowaną sieć podzieloną wirtualnie na partycje jako jeden „logiczny" przełącznik, który jest rozproszony fizycznie (ze względów niezawodnościowych), zapewniający wysokie parametry, małe opóźnienia i możliwość łączenia wszystkiego ze wszystkim w centrum przetwarzania danych dla każdego rodzaju ruchu.

Niewiele ze współczesnych sieci w centrach przetwarzania danych nawet zbliża się do tego ideału, ale większość z nich może skorzystać na nowym podejściu, którego nadrzędną zasadą jest upraszczanie. Nowe techniki umożliwiają projektantom zmniejszanie złożoności sieci i kosztów jej posiadania poprzez ograniczenie liczby warstw komutacji, liczby łączy skrośnych, konsolidację infrastruktury zabezpieczającej i przyjęcie jako standard jednego systemu operacyjnego pozwalającego na automatyzację działania sieci w infrastrukturze komutacyjnej, rutingowej i usług sieciowych. Takie uproszczenie podejścia pozwala już dziś przygotować się na wysoką wydajność, szybkie zmiany i rozrost jutra, niezależnie od tego, czy firma zamierza w pełni wdrożyć wysoce zwirtualizowane intensywnie wykorzystujące sieć usługi „przetwarzania w chmurze".

Bardzo interesujący jest aspekt zmniejszenia kosztów eksploatacji. Można je zmniejszyć już samym tylko ograniczeniem liczby przełączników. Ale gdy racjonalizacja dotyczy całej warstwy sieciowej, oszczędności pojawiają się wszędzie:

- Ekonomiczny projekt powoduje, że infrastruktura sieciowa jest skonsolidowana w mniejszej liczbie urządzeń, co oszczędza miejsce, energię zasilającą, do chłodzenia, a także zmniejsza koszty ogólne zarządzania.
- „Spłaszczone" sieci pozwalają na centralizację i wirtualizację urządzeń zabezpieczających i zastąpienie nimi licznych oddzielnych urządzeń realizujących SSL, VPN, NAT i inne zabezpieczenia. Konsolidacja urządzeń zabezpieczających ogranicza koszty i ułatwia zarządzanie sieciami, przez co stają się one sprawniejsze i bezpieczniejsze.
- Ekonomiczniejsze zarządzanie mnoży oszczędności. Zmniejszenie liczby i zróżnicowania urządzeń upraszcza zarządzanie nimi. Znormalizowanie interfejsów zwiększa wydajność pracy wysoko kwalifikowanego personelu i pozwala na stosowanie zautomatyzowanych narzędzi do zarządzania siecią i jej rutynowej konserwacji.

Wydajność uproszczonych sieci

Oprócz niższych kosztów budowy i zarządzania, bardziej płaskie sieci działają sprawniej. Przejście pakietu danych przez każdy kolejny przełącznik czy urządzenie zwiększa opóźnienie w torze transmisji danych, tak że eliminacja warstw komutacji zmniejsza opóźnienie całościowe. W bardziej płaskich sieciach sprawniej też działają współczesne aplikacje – na przykład te oparte na architekturze usługowej (*Service Oriented Architecture – SOA*) korzystają na tym, że sieci centrów przetwarzania danych są w stanie na bieżąco obsługiwać cały ruch międzyserwerowy przez nie generowany.

Wysoko wydajne sieci o niskich opóźnieniach są szczególnie istotne dla firm planujących zwiększenie swego zaangażowania w wirtualizację. Aby ją wprowadzić na dużą skalę, niezbędne jest zaplanowanie migracji sieci; powinno być dokonane na jak najwcześniejszym etapie.

Lepsze usługi i wyniki gospodarcze

Opisywane powyżej ograniczenia kosztów i zwiększenie wydajności będą obiektem bezpośredniego zainteresowania firm zamierzających w pełni wykorzystać możliwości stwarzane przez nowe techniki obliczeniowe, w dziedzinie pamięci masowych i oprogramowania. Ale korzyści płynące z szybszych, prostszych, elastyczniejszych i tańszych rozwiązań podstawowych będą odczuwalne w całych centrach przetwarzania danych i firmach przez nie obsługiwanych – w postaci długofalowych usprawnień operacyjnych.

Pojedyncza wysoce skalowalna sieć centrum przetwarzania danych ułatwia grupowanie zasobów serwerowych i pamięci celem skuteczniejszego rozkładania obciążeń i lepszego wykorzystania zasobów. Upraszcza też uruchamianie usług, skracając czas niezbędny do wprowadzania nowych czy cyklicznego ustawicznego ulepszania usług już oferowanych. A interesujący jest wynik ostateczny – im wyższej jakości usługi można świadczyć w krótszym czasie, tym niższe będą koszty.

Niezależnie od tego, czy organizacja planuje przejście na „przetwarzanie w chmurze" szerokim frontem czy też tylko stopniowe wykorzystywanie korzyści płynących z wirtualizacji, pamięci sieciowych i nowych modeli udostępniania aplikacji, powinna dobrze się przyjrzeć wymaganiom na swoje sieci. Spłaszczona i prostsza konstrukcja sieci szybko się zwróci i pozwoli firmie szybciej dostosowywać się do wyzwań, które pojawią się w przyszłości.

Autor jest wiceprezesem do spraw marketingu produktów i rozwoju działalności w dziale Data Center Business Group w firmie Juniper Networks

Być bliżej Klienta

Integracja rozwiązań VoIP oferowanych przez Activis Polska

Artykuł pokazuje jak integracja pozornie odrębnych co do zastosowania rozwiązań daje nową jakość w przedsiębiorstwie. Omówiono oferowany od kilku lat system łączności korporacyjnej VoIP – VDmaster w jego najnowszej wersji oraz nowo opracowaną przez Activis Polska usługę VoiceLink. Zaprezentowano jak powiązanie tych produktów prowadzi do wykreowania kolejnego – konfiguracji ułatwiającej budowanie rozwiązań typu help desk szczególnie przydatnych w przedsiębiorstwach, dla których kontakt z końcowym klientem pełni kluczową rolę.

Od lat Activis Polska specjalizuje się w projektowaniu i produkcji rozwiązań VoIP. Firma jako jedna z pierwszych w Polsce rozpoczęła prace nad transmisją głosu w sieciach IP. Pozwoliło to na stworzenie autorskiego opracowania – kompleksowego systemu wykorzystującego własny sprzęt i oprogramowanie uwzględniającego jednocześnie światowy standard sygnalizacji SIP. Bogate doświadczenie pozwoliło stworzyć system telefonii IP, który umożliwia integrowanie i optymalizowanie sieci IP, TDM i GSM w ramach wspólnej sieci telekomunikacyjnej.

VDmaster[1] to system komunikacyjny adresowany głównie do obsługi firm. Dzięki uniwersalności obsługiwanych interfejsów pozwala on użytkownikowi zintegrować z systemem IP również sieci TDM i GSM w ramach wspólnej sieci telekomunikacyjnej i wykorzystać posiadane zasoby teleinformatyczne. System VDmaster może zostać wykorzystany do rozbudowy istniejących central PABX o kolejne porty abonenckie (analogowe lub IP) w miejscu niezależnym od lokalizacji centrali lub z powodzeniem funkcjonalnie zastąpić klasyczną centralę telefoniczną w firmie. Łącząc kilka oddziałów ze sobą można utworzyć rozproszony węzeł telekomunikacyjny dający użytkownikowi logicznie scaloną sieć korporacyjną z wieloma dodatkowymi usługami.

System posiada kilka elementów funkcjonalnych odpowiedzialnych za możliwość dokonywania połączeń telekomunikacyjnych:

- Serwer SIP jest to element systemu zarządzający pracą zakończeń abonenckich wykorzystujących do przesyłania sygnalizacji protokół SIP. Zarządza również współpracą z zewnętrznymi operatorami VoIP.
- Centrala IP PABX steruje pracą wszystkich elementów tworzących sieć VDmaster. Dzięki zaimplementowanym w nim mechanizmom, system realizuje standardowe funkcje central abonenckich PABX (jak przenoszenie, grupowanie łączy, automatyczne zapowiedzi – DISA itp.) oraz dodatkowe usługi dostępne dzięki wykorzystaniu sieci IP.
- Zakończenie liniowe ZA (centralowe lub abonenckie) umożliwia dołączenie do systemu centrali telefonicznej i abonentów korzystających z aparatów analogowych.
- Moduły dodatkowe jak IVR, DISA i inne pozwalające na rozszerzanie funkcjonalności instalacji zależnie od potrzeb użytkownika.

Serwer SIP pozwala na obsługę:

- 250 abonentów IP (telefony IP, bramki wyposażone w porty FXS, bramki SIP-ISDN);
- 30 wyjść do sieci publicznej (bramki z portami FXO, bramki SIP-GSM, bramki SIP-ISDN);
- 30 „kanałów”(domen i użytkowników) dostępu do serwerów SIP zewnętrznych operatorów oferujących usługi VoIP.

System można rozbudować o kolejne serwery SIP rozszerzając tym samym ilość przyłączonych abonentów, liczbę możliwych wyjść do sieci publicznej oraz zewnętrznych operatorów VoIP.

Drugim równie ważnym elementem jest oprogramowanie centrali IP PABX, które steruje pracą wszystkich elementów tworzących sieć VDmaster. Dzięki zaimplementowanym tam mechanizmom, system realizuje standardowe funkcje central abonenckich PABX (jak przenoszenie, grupowanie łączy, automatyczne zapowiedzi – DISA itp.) oraz dodatkowe

[1] VDmaster – jest zastrzeżonym znakiem towarowym firmy Activis Polska Sp z o.o.

usługi dostępne dzięki wykorzystaniu sieci IP. Umożliwia tworzenie rozległej sieci VDmaster (np. wykorzystując Internet) bez naruszania ochrony opartej na elementach typu firewall.

Centrala IP-PBX umożliwia:

- obsługę 200 urządzeń podległych (np. serwerów SIP VDmaster);
- wykreowanie 2000 numerów katalogowych;
- grupowanie łączy i abonentów w ramach całej sieci (np. utworzenie wiązki PABX),
- sterowanie ruchem wychodzącym do operatorów publicznych w oparciu o system wyboru drogi o najniższym koszcie – LCR,
- prowadzenie nadzoru ruchu i analizy połączeń w ramach całego systemu dzięki aplikacji PART.

Kolejnym elementem funkcjonalnym systemu VDmaster jest zakończenie liniowe (centralowe lub abonenckie) umożliwiające dołączenie do systemu centrali telefonicznej i abonentów korzystających z aparatów analogowych. System VDmaster w odróżnieniu od wielu innych podobnych rozwiązań jest systemem otwartym, co umożliwia dołączanie zaimplementowanych wcześniej u klienta urządzeń VoIP czy GSM.

Trzeba podkreślić, że wyżej opisane elementy systemu to pakiety oprogramowania, które mogą być lokalizowane na jednym lub kilku modułach sprzętowych.

Zakończenia liniowe, jako elementy związane z otoczeniem sprzętowym są oferowane w postaci modułów z wyspecjalizowanym oprogramowaniem o różnych konfiguracjach co daje możliwość wyboru optymalnej kombinacji sprzętu zarówno ze względu na rodzaj zastosowanych interfejsów jak i lokalizację.

W ofercie znajdują się urządzenia umożliwiające zaimplementowanie odpowiednich elementów funkcjonalnych oraz dołączenie systemu za pośrednictwem portów centralowych cyfrowych oraz analogowych. Główną różnicą pomiędzy poszczególnymi urządzeniami wchodzącymi w skład systemu VDmaster jest liczba interfejsów umożliwiających przyłączenie do sieci wewnętrznej i operatorskiej:

- VDmaster ZTA 2*FXS, 2*FXO, 1*WAN, 4*LAN;
- VDmaster SVR 1*WAN, 1*LAN;
- VDmaster MIX 2*FXS, 8*FXO, 4*GSM, 1*WAN, 4*LAN;
- VDmaster IMIX 14*FXS, 2*FXO, 1*WAN, 4*LAN;
- VDmaster PRA 2*E1, 1* WAN, 4* LAN.

Stosując wymienione elementy oraz ich kombinacje użytkownik może zbudować nowoczesny system łączności gwarantujący optymalne wykorzystanie posiadanych zasobów. Zasady pracy definiuje się poprzez odpowiednie skonfigurowanie serwera lub kilku serwerów występujących w danej sieci.

W ramach systemu można dołączyć od kilku (w przypadku małych firm) do kilku tysięcy abonentów. Istotną jego zaletą jest funkcja LCR umożliwiająca automatyczny wybór najtańszej drogi połączeniowej. Jednym słowem – nie użytkownik systemu wybiera drogę połączenia (PSTN, GSM, VoIP), ale system po przeanalizowaniu numeru docelowego zestawia najtańsze z możliwych połączenie. Jest to najefektywniejszy sposób wprowadzenia znacznych oszczędności w firmie.

System został opracowany pod kątem wygody użytkownika, nie wymaga zmiany sposobu wybierania numerów i pozwala zachować dotychczasową strukturę sieci.

Częścią strategii firmy Activis jest wprowadzanie kolejnych opracowań i poszerzanie kompetencji w zakresie technologii Voice over IP. Dlatego też kolejnym obszarem zainteresowania są aplikacje związane z wykorzystaniem internetu.

W Activisie ubiegłym roku roku powstała koncepcja zrealizowania nowej usługi komunikacji głosowej w technologii VoIP, wykorzystującej zupełnie nowe w skali światowej podejście a mianowicie zestawianie połączenia za pomocą aplikacji która nie jest zainstalowana na komputerze użytkownika a jedynie na czas trwania połączenia przesyłana z serwera i kasowana „po użyciu".

Bliższa analiza dowiodła, że takie podejście niesie za sobą rewolucyjne zmiany w zasadach korzystania z połączeń VoIP. Nie wymaga instalacji, rejestrowania użytkownika, nie angażuje zasobów operatora ani komputera internauty poza czasem, kiedy połączenie jest aktywne. Innymi słowy w sposób idealny nadaje się do realizacji połączeń „tu i teraz". Na przykład w celu uzyskania informacji, pomocy, realizacji zamówienia wszędzie tam, gdzie można skorzystać ze stron internetowych jako pierwotnego źródła. Nowa usługa została nazwana VoiceLink[2]. Ze względu na swoją innowacyjność oraz fakt, że okres przewidziany na realizację projektu był zbieżny z harmonogramem naboru wniosków do Programu Operacyjnego Innowacyjna Gospodarka, projekt VoiceLink znakomicie nadawał się do startu w konkursie.

Activis przygotował aplikację – zgłoszenie do kolejnej edycji naboru wniosków o dofinansowanie. Proces przygotowania wniosku udało się zakończyć dosłownie w ostatniej chwili – już po wydaniu przez PARP komunikatu, że pula środków na ta edycję została wyczerpana. Projekt zyskał wysoką ocenę Komisji i został zakwalifikowany do dofinansowania. Activis założył bardzo krótki 6-miesięczny okres realizacji prac badawczych oraz półroczny okres wdrożenia projektu.

W wyniku realizacji projektu wprowadzono na rynek nową usługę, o charakterze marketingowym. Usługa VoiceLink umożliwia nawiązanie rozmowy telefoni-

[2] VoiceLink – jest zastrzeżonym znakiem towarowym (CTM) firmy Activis Polska Sp z o.o.

cznej poprzez kliknięcie ikony zamieszczonej na stronie internetowej. Ikona jest skojarzona z jednym lub wieloma telefonami VoIP, na stanowiskach konsultantów właściciela witryny. Internauta jednym kliknięciem nawiązuje BEZPŁATNE połączenie z konsultantem. Wystarczy, że Internauta ma podłączony mikrofon oraz słuchawki lub głośnik.

Aplikacja VoiceLink wraz z oprogramowaniem zlokalizowanym na serwerze podczas obsługi zgłoszenia informuje internautę o stanie połączenia, w razie potrzeby kolejkuje zgłoszenia, cyklicznie rozdziela wywołania kolejnym konsultantom oraz zbiera statystyki.

Łatwość, szybkość i wygoda w nawiązaniu rozmowy przyczynia się do tego, że internauta – potencjalny klient, kontaktuje się z właścicielem witryny na bieżąco. Badania rynkowe potwierdzają, że to pierwsze minuty i dobry kontakt decydują o wyborze oferty, oraz że po znalezieniu pożądanego towaru lub usługi, klient przestaje analizować ofertę konkurencji.

Aby wykonać bezpłatne połączenie, odwiedzający witrynę internetową nie potrzebuje żadnego dodatkowego sprzętu, za wyjątkiem mikrofonu i słuchawek (lub głośnika). Firma, która chce umożliwić swoim stałym i potencjalnym klientom bezpłatną rozmowę ze swoimi konsultantami musi jedynie dysponować łączem do Internetu i zakupić pakiet startowy VoiceLink. Platforma umożliwiająca komunikowanie się internautów z konsultantami jest obsługiwana przez firmę zewnętrzną – operatora usługi VoiceLink

Voicelink jest przykładem nowego modelu świadczenia usług związanych z Internetem, gdzie bezpo-

średni użytkownik aplikacji postrzega nowe możliwości jako darmowe a usługi są finansowane pośrednio – przez firmę, która korzystając z zalet marketingowych jest gotowa pokrywać koszty jej eksploatacji.

Narzucającym się krokiem było powiązanie usługi Voicelink z istniejącą już i pracującą w wielu przedsiębiorstwach platformą VDmaster. Punkty wspólne obu rozwiązań to przede wszystkim wykorzystana technologia VoIP bo ułatwia ona integrowanie różnych aplikacji dając do dyspozycji jednorodne środowisko komunikacyjne. Ponadto w wielu zastosowaniach niezbędne jest ułatwienie komunikacji wykraczające poza możliwość przeprowadzenia bezpłatnej rozmowy.

W rezultacie prowadzonych równolegle z opracowywaniem VoiceLinka prac został zrealizowany kolejny projekt – kolejny moduł funkcjonalny dla platformy komunikacyjnej VDmaster czyli moduł sprzętowo-programowy VDmaster VL. Jest to dedykowany serwer połączeń generowanych ze stron internetowych a więc pozwala on utworzyć w firmie eksploatującej telefonię VoIP własne centrum obsługowe dla internautów za cenę stanowiącą ułamek kosztów typowego call center.

Jest to szczególnie interesujące dla firm, które muszą się liczyć z częstym kontaktem z klientami.

Równolegle realizowano również kolejne plany rozwojowe mające na celu pełne zintegrowanie typowej instalacji platformy VoiceLink z systemem VDmaster. Te prace pozwoliły na uzyskanie w pełni kompatybilnego systemu, który oferuje użytkownikowi wszystkie najbardziej istotne obecnie kanały dostępu:

- tradycyjne łącza telefoniczne;
- połączenia GSM;
- połączenia VoIP z sygnalizacją SIP;
- połączenia VoIP generowane bezpośrednio ze stron www.

Centrum informacyjne czy tez help desk w takiej postaci oferujący możliwość bezpłatnego kontaktu ze strony internetowej to też oferta dla organów administracji czy urzędów, dla których kontakt z obywatelem to podstawowa działalność.

Wydaje się, że szczególnie ta ostatnia funkcjonalność jest przykładem dobrze ilustrującym coraz bardziej popularny obecnie model usługi, gdzie dowolny klient korzysta z niej wtedy, kiedy potrzebuje bez wcześniejszych rejestracji, instalacji i zakupu usługi. jest to zgodne z coraz powszechniejszym przekonaniem, że wymiana informacji (w tym połączenia między ludźmi) staję się prawem a nie dobrem deficytowym czy luksusowym.

ksi.pl
KOMPLEKSOWE SYSTEMY INFORMACYJNE

Lider w dziedzinie rozwiązań mobilnych

ROZWIĄZANIA MOBILNE

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

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

BLUETOOTH MARKETING

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

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

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

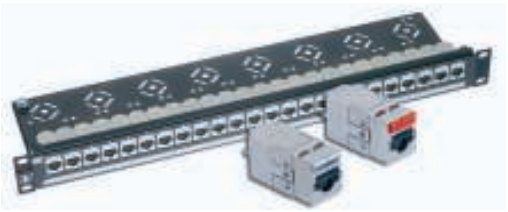
Zastosowanie nowoczesnych narzędzi, takich jak Bluetooth Marketing ściśle wiąże markę z takimi przymiotami jak innowacyjność, czy skuteczność.

Okablowanie dla szybkich sieci

molex
one company › a world of innovation

Rozwiązanie PowerCat™ 6A

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



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

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

Technologia

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

Rozwiązanie kategorii 6A firmy Molex

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

Złącze DataGate™ odlewane pod ciśnieniem z przesłoną

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

Panele krosowe

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

PowerCatTM 6A – informacja dla zamawiających – *Kable*

Numer katalogowy	Opis
CAA-0322L-VL	Kabel U/FTP PowerCat 6A, 4 pary, LSOH, 500m, fioletowy
CAA-0322C-VL	Kabel U/FTP PowerCat 6A, 4 pary, PVC, 500m, fioletowy

PowerCatTM 6A – informacja dla zamawiających– *Kable krosowe*

Numer katalogowy	Opis
PCD-00700-**	Ekranowany kabel krosowy RJ45, 568B, linka, PowerCat 6A, PVC 1m
PCD-00701-**	Ekranowany kabel krosowy RJ45, 568B, linka, PowerCat 6A, PVC 2m
PCD-00702-**	Ekranowany kabel krosowy RJ45, 568B, linka, PowerCat 6A, PVC 3m
PCD-00703-**	Ekranowany kabel krosowy RJ45, 568B, linka, PowerCat 6A, PVC 5m
PCD-00704-**	Ekranowany kabel krosowy RJ45, 568B, linka, PowerCat 6A, PVC 7m
PCD-00705-**	Ekranowany kabel krosowy RJ45, 568B, linka, PowerCat 6A, PVC 10m

PowerCatTM 6A – informacja dla zamawiających – *Panele krosowe*

Numer katalogowy	Opis
PID-00217	Panel ekranowany 19-calowy, 24xRJ45, PowerCat 6A, 1U
PID-00218	Panel ekranowany skośny 19-calowy, 24xRJ45, PowerCat 6A, 1U
PID-00219	Panel ekranowany 19-calowy, 48xRJ45, PowerCat 6A, 2U
PID-00220	Panel ekranowany skośny 19-calowy, 48xRJ45, PowerCat 6A, 2U

PowerCatTM 6A – informacja dla zamawiających – *Gniazda Abonenckie*

Numer katalogowy	Opis
MMS-00017-02	Moduł ekranowany Mod-Snap III, kat.6A – biały
MMS-00017-04	Moduł ekranowany Mod-Snap III, kat 6A – czarny
MGB-00006-02	Moduł ekranowany Contura, kat.6A – biały
MEU-00065-02	Moduł ekranowany Euromod II, kat.6A – biały
MEU-00065-04	Moduł ekranowany Euromod II, kat.6A – czarny
MLG-00030-02	Moduł ekranowany 22.5 x 45mm Mod-Mosaic, kat.6A – biały
MLG-00030-04	Moduł ekranowany 22.5 x 45mm Mod-Mosaic, kat.6A – czarny
MLG-00031-02	Moduł ekranowany 45 x 45mm 2xMod-Mosaic, kat.6A – biały
MLG-00031-04	Moduł ekranowany 45 x 45mm 2xMod-Mosaic, kat.6A – czarny
MIT-00018-04	Moduł ekranowany Vimar, kat.6A – czarny
MIT-00019-04	Moduł ekranowany kompatybilny z Bticino, kat.6A – czarny
MCZ-00009-04	Moduł ekranowany kompatybilny z ABB Tango, kat.6A – czarny
WNC-00044-02	Moduł ekranowany, 1 Port DIN, kat.6A – biały
WNC-00045-02	Moduł ekranowany, 2 Port DIN, kat.6A – biały
WNC-00044-06	Moduł ekranowany, 1 Port DIN, kat.6A – migdałowy
WNC-00045-06	Moduł ekranowany, 2 Port DIN, kat.6A – beżowy

Kabel U/FTP

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

Kable krosowe

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

Wybrane zalety rozwiązania Molex PowerCat kategorii 6A

- połączenie ekranowane na 360° dzięki odlewanemu pod ciśnieniem złączu DataGate;
- ochrona – wyjątkowa przesłona sprężynowa złącza DataGate nie tylko chroni przed kurzem i zabrudzeniami, ale też odrzuca nieprawidłowo wpięte bądź uszkodzone kable krosowe;
- niezawodność – funkcje porządkowania przebiegów kablowych zmniejszają naprężenie kabli i zapewniają spójną jakość działania, a złącze DataGate zmniejsza poziom szkód i przyspiesza instalację;
- doskonałe parametry – rozwiązanie ekranowane end-to-end spełniające wymagania kategorii 6A Ekranowany kabel skutecznie zmniejsza efekt przesłuchu obcego.

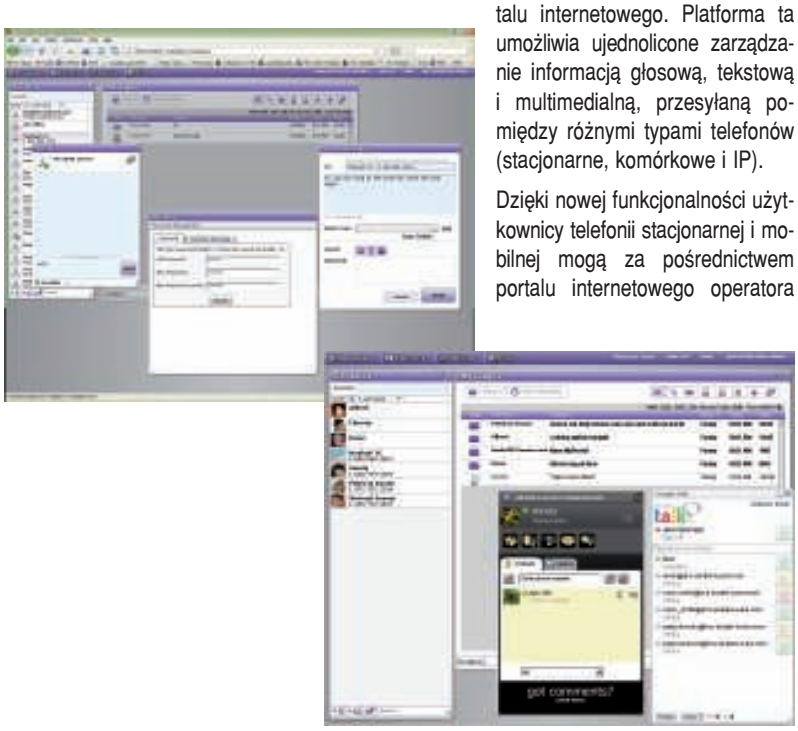
Molex Premise Networks
Eastern Europe Headquarters
ul. Okrzei 1a, 03–715 Warszawa
tel. +48 22 333 81 50, fax +48 22 333 81 51
www.molexpn.com.pl

Nowoczesne aplikacje komunikacyjne Alcatel-Lucent

Zunifikowana komunikacja nowej generacji

Rich Communications Manager firmy Alcatel-Lucent to platforma operatorska, która umożliwia klientom ujednolicenie całej ich komunikacji głosowej realizowanej za pomocą różnych urządzeń i w różnych sieciach – łącznie z integracją usług Web 2.0. Platforma udostępnia usługodawcom narzędzia, które znacznie usprawniają i upraszczają sposób komunikacji użytkowników poprzez połączenie różnych usług w ramach jednego portalu.

Rozwiązanie umożliwia zarządzanie różnorodnymi wiadomościami multimedialnymi za pośrednictwem jednego portalu internetowego. Platforma ta umożliwia ujednolicone zarządzanie informacją głosową, tekstową i multimedialną, przesyłaną pomiędzy różnymi typami telefonów (stacjonarne, komórkowe i IP).



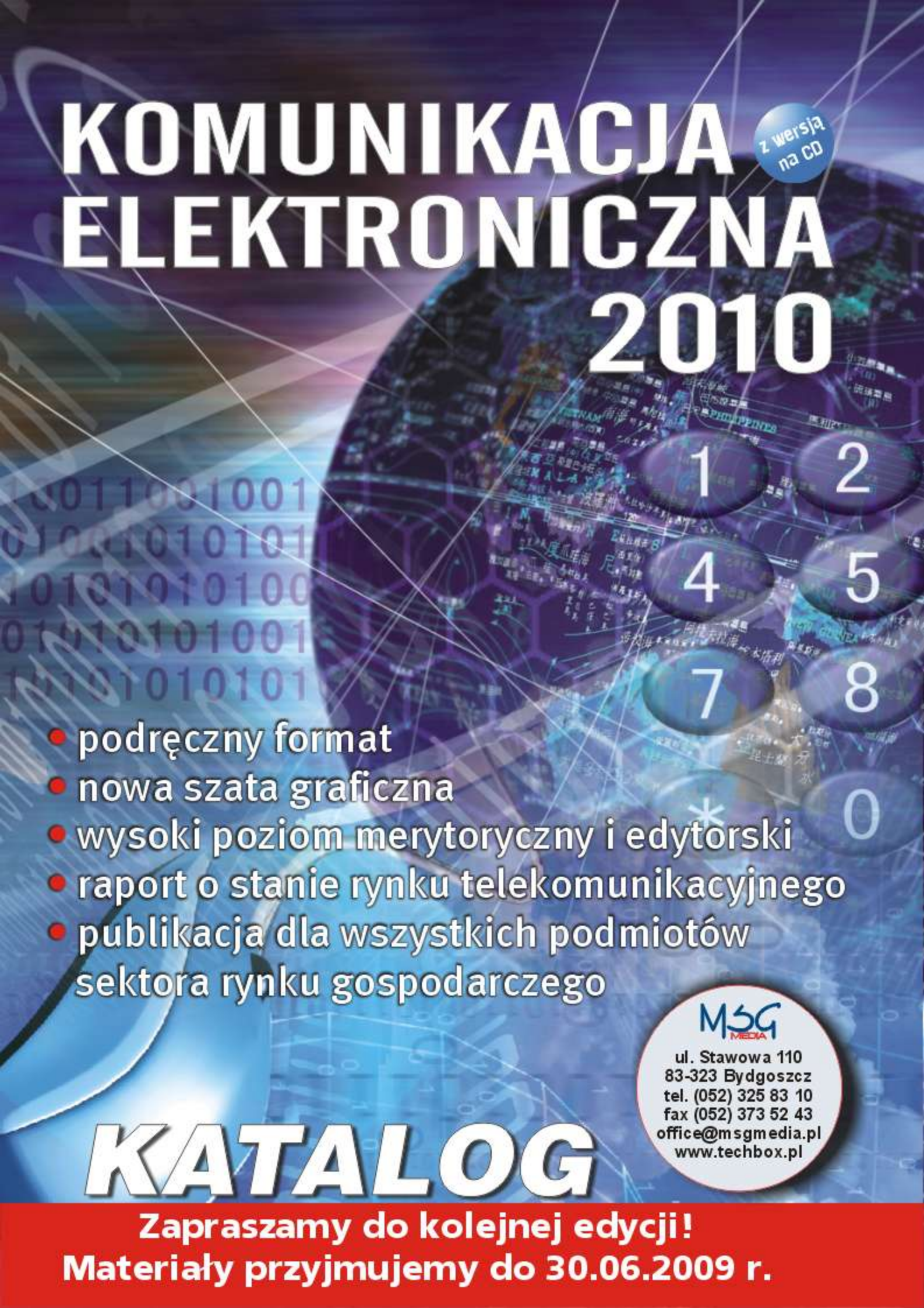
Dzięki nowej funkcjonalności użytkownicy telefonii stacjonarnej i mobilnej mogą za pośrednictwem portalu internetowego operatora odbierać, przeglądać i przesyłać dalej filmy, zdjęcia i wiadomości tekstowe. Z poziomu portalu można również zarządzać zintegrowaną książką adresową obejmującą wszystkie urządzenia użytkownika. Wykorzystując prosty i znany interfejs użytkownicy mogą metodą „przeciągnij i upuść" (*drag-and-drop*) dowolnie zarządzać wiadomościami głosowymi, SMS, MMS i e-mail oraz faksami, kalendarzami i książkami adresowymi. Do korzystania z Rich Communications Managera wystarcza jeden login i hasło, w ten sposób platforma eliminuje konieczność pamiętania różnych loginów, haseł i specyfiki obsługi poszczególnych urządzeń i aplikacji użytkownika. Dzięki RCM użytkownik zarządza swoją informacją wyłącznie ze względu na treść, a nie medium, za pośrednictwem którego została ona przekazana.

Rozwiązanie C zapewnia użytkownikom wygodny dostęp do ich skrzynek multimedialnych w domu, pracy i za pomocą telefonów komórkowych. Pozwala także zarządzać całą komunikacją multimedialną oraz zwizualizować konwergentną kolejkę wiadomości, określić źródło wiadomości głosowych i odsłuchać je online. Udostępnia także funkcję zamiany głosu na tekst umożliwiając odczytanie wiadomości głosowej w formie tekstowej.

Równolegle Alcatel-Lucent przedstawiła nową generację opartego na technologii Rich Communications Suite „widgeta do komunikacji". Może być on rozwijany wraz innymi dostawcami aplikacji, aby zapewnić intuicyjną, bezpieczną komunikację i możliwość przesyłania wiadomości bezpośrednio z poziomu portalu firmy trzeciej (np. portale społecznościowe). Ta przyszłościowa funkcja rozwiązania Rich Communications Manager jest zgodna ze strategią współtworzenia aplikacji realizowaną przez firmę Alcatel-Lucent oraz pomaga operatorom sieciowym pokazywać potencjał tkwiący w komunikacji i instant messagingu, a tym samym stymulować jego rozwój w bardziej ukierunkowany sposób.

Informacje o rozwiązaniu Alcatel-Lucent 5155 Rich Communications Manager

Alcatel-Lucent 5155 Rich Communications Manager wersja 2.1 to pierwsza wersja tej platformy dostępna na rynku. Oferuje ona znakomite możliwości technologii Web 2.0 z rozszerzonymi funkcjami przesyłania wiadomości przez internet. Rozwiązanie udostępnia abonentom interfejs internetowy umożliwiający zarządzanie ich potrzebami komunikacyjnymi online. Umożliwia użytkownikom pobieranie wiadomości głosowych, SMS, MMS i e-mail oraz faksów z portalu internetowego oraz ich przeglądanie, przesyłanie dalej i odpowiadanie na nie. W portal jest wbudowana sieciowa książka adresowa, w której są przechowywane wszystkie kontakty użytkowników. Obsługiwana sieciowa książka adresowa jest zgodna z pakietem GSM Association Rich Communications Suite (RCS) w wersji 1.0. Produkt może również obsługiwać funkcje zarządzania wiadomościami online znajdującymi się w systemach poczty głosowej innych producentów. Rozwiązanie Rich Communications Manager wykorzystuje środowisko o otwartym dostępie do kodu źródłowego. Dzięki temu pozwoli tworzyć usługi w przyszłości, umożliwiając usługodawcom wdrażanie nowych wieloekranowych usług komunikacyjnych łączących funkcje przesyłania wiadomości z komunikacją internetową (komunikacja głosowa, funkcja presence, czat), korzystaniem z portali społecznościowych oraz usługami zarządzania treścią i usługami reklamowymi.


KOMUNIKACJA ELEKTRONICZNA 2010
z wersją na CD
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
Zapraszamy do kolejnej edycji!
Materiały przyjmujemy do 30.06.2009 r.

Bezpieczeństwo WLAN

Dariusz Koralewski

Jak NIE zabezpieczać swojej sieci bezprzewodowej

Biorąc pod uwagę wzrost produktywności, mniejsze koszty struktury i udogodnienia, które technologia wireless zapewnia w środowisku pracy, wiele firm wdrożyło u siebie lokalną sieć bezprzewodową (WLAN). Poza warunkami biurowymi sieci WLAN wdrażane są również w magazynach, halach produkcyjnych, laboratoriach – w zasadzie w każdym miejscu pracy.

Wartość sieci WLAN jest szczególnie atrakcyjna dla małych i średnich przedsiębiorstw. Bezprzewodowa sieć lokalna jest najszybszą, najbardziej elastyczną i najekonomiczniejszą strategią budowania lub poszerzania sieci. Łącza WLAN eliminują okablowanie i pozwalają użytkownikom uzyskać dostęp do sieci, jeśli tylko znajdują się w jej zasięgu. Kolejnym powodem popularności sieci WLAN wśród małej wielkości przedsiębiorstw jest fakt, iż wiele z tych firm nie posiada na własność swoich siedzib. W takim wypadku wolą nie podpisywać ciągnących się w nieskończoność umów z dostawcami internetu. WLAN pozwala tego uniknąć. Dodatkowo większość tego typu firm nie zatrudnia pełnoetatowych pracowników IT.

Mimo wszystko, niektóre małe i średnie przedsiębiorstwa odnoszą mylne wrażenie, że sieci bezprzewodowe są mniej bezpieczne od ich kablowych konkurentów, podczas gdy prawdą jest, że z racji wykorzystywania radiowej częstotliwości połączeń sieci WLAN są w pewien sposób podatne na wszelkie formy ataków. Mogą jednak być równie dobrze zabezpieczone jak sieci kablowe. Tak jak i w sieciach przewodowych, bezpieczeństwo WLAN koncentruje się na:

- zapobieganiu łączenia się z siecią nieautoryzowanych użytkowników, którzy najczęściej mają na celu przechwytywanie, czytanie, zmianę lub kradzież ważnych informacji osobistych i zawodowych lub wprowadzanie szkodliwych wirusów czy robaków;
- powstrzymywaniu przed łączeniem się stałych użytkowników z nieautoryzowanymi, podejrzanymi punktami dostępowymi;
- pewności, że normalna transmisja nie zostanie zakłócona;
- trzymaniu na odległość wszystkich mających zamiar włamać się do sieci amatorów darmowego ściągania.

Media obfitują w propozycje, jak można zabezpieczyć sieć WLAN. Niestety, niektóre „porady" nie są tak rozsądne i powinny być dokładnie przeanalizowane. Przykładami mylących porad są:

1. Ukryj swoje SSID

Każdy WLAN posiada unikalną nazwę zwaną SSID (*Service Set Identifier*). Wszystkie urządzenia bezprzewodowe (stacje bazowe, klienci, itp) we WLAN-ie muszą używać tego samego SSID, aby komunikować się ze sobą. Niektórzy właściciele sieci ukrywają swoje SSID przed intruzami, tak aby ich sieć była niewidoczna na liście dostępnych sieci. SSID jednakże nadawane jest poprzez cztery inne mechanizmy, więc jest to równoznaczne z zatykaniem jednej z czterech dziur przeciekającego okrętu!

2. Umieść antenę w Centrum Strefy Pracy

Niektórzy „eksperci" twierdzą, że jednym ze sposobów zapobiegania łączeniu się nieupoważnionych stron z firmową siecią jest umieszczenie anteny w samym środku przestrzeni, którą objąć ma zasięg sieci. Poprzez dostosowanie siły sygnału do objętości powierzchni sieć nie będzie rzekomo wydostawać się poprzez ściany i okna. Trzeba być jednak świadomym, że poważni intruzi niemal zawsze mają silniejszą antenę! Natomiast odnośnie do obniżania siły sygnału – możesz skończyć z na wpół martwą strefą na obrzeżach powierzchni, którą chciałeś objąć siecią, co czyni sam fakt posiadania WLAN-u bezsensownym.

3. Używaj WEP

WEP (*Wired Equivalent Privacy*) jest standardową metodą szyfrującą ruch w sieciach bezprzewodowych. Istnieją jednak znane słabości w sposobie, w jaki odbywa się szyfrowanie. Tak więc WEP zatrzyma przypadkowych amatorów darmowego ściągania, ale zapewnia małą ochronę przed poważnymi atakami, podczas których klucze WEP łamane są w ciągu kilku minut.

4. Wyłącz DHCP

Dynamic Host Configuration Protocol (*DCHP*) automatycznie przydziela adresy IP do urządzeń w sieci. To oznacza, że jakiekolwiek urządzenie będące w zasięgu twojego WLAN może być w stanie otrzymać adres IP z twojego routera i być zaakceptowane w sieci bez twojej wiedzy. Wyłączenie DHCP nie jest jednak właściwą ochroną. Zaawansowani hakerzy domyślą się twojego schematu nadawania IP i przydzielą sobie sami adresy, aby uzyskać dostęp do twojej sieci w ciągu kilku minut.

5. Filtruj adresy MAC

MAC (*Media Acces Control*) adresy są podstawą unikalnych name-tagów dla adapterów bezprzewodowych. Filtrowanie zapewnia, że tylko potwierdzeni klienci są dopuszczeni do połączenia z siecią. Problem w tym, że wysyłane adresy MAC nie są szyfrowane i atakujący sieć może z łatwością podrobić obowiązujący adres korzystając z interfejsu karty sieciowej i narzędzi analizujących protokół. Innym minusem jest fakt, że ręczne konfigurowanie każdego „dopuszczonego" adaptora wymaga dużych technicznych umiejętności oraz wiele czasu i środków, których małe i średnie przedsiębiorstwa najczęściej nie mają do dyspozycji.

Nierozwaga tego typu „porad", mimo dobrych intencji, może nasuwać firmom pytanie, czy korzyści wypływające z użytkowania WLAN oznaczają jednocześnie pójście na kompromis w sprawach bezpieczeństwa. Odpowiedź brzmi – **NIE**. Oba cele mogą być osiągnięte, jeśli infrastruktura WLAN jest uważnie rozplanowana, pilnie wdrożona i sensownie zarządzana – tak, jak w przypadku samego biznesu.

Poniżej znajduje się kilka podstawowych zasad bezpiecznego WLAN-u:

Nie używaj ustawień domyślnych

Zmień wszystkie ustawienia domyślne dla SSID, haseł administracyjnych i haseł użytkowników w routerze, punktach dostępowych i kartach bezprzewodowych. Domyślne SSID i hasła są publikowane przez producentów w internecie i są przeznaczone do celów przyspieszenia instalacji, a nie zapewniania ochrony.

Wybierz unikalne SSID

Wybieraj SSID, które są trudne do odgadnięcia. Nie używaj imienia szefa, numeru rejestracyjnego twojego samochodu, adresu biura, numeru telefonu lub faxu, lub nazwy, czy inicjałów firmy.

Używaj szyfrowania WPA

WPA (*Wifi Protected Access*) jest nowsze i dużo mocniejsze od WEP oraz niezwykle skomplikowane i trudne do odgadnięcia. Jeśli Twój system posiada WPA i oferuje szyfrowanie dzielonych kluczy, włącz je.

Uwierzytelniaj użytkowników

Dla organizacji posiadających katalog Microsoft Active, Microsoft IAS czy serwer Radius zalecane jest włączenie loginu sieciowego 802.1x. To sprawia, że bezprzewodowy punkt dostępu uwierzytelnia użytkownika przez serwer przed dopuszczeniem go do sieci.

Instaluj firewalle

Jeśli do twojego access pointu lub routera dodano firewalla, użyj go. Jeśli nie, zainstaluj sprzęt firewallowy dla całej sieci i zainstaluj jego oprogramowanie na każdym komputerze łączącym się z WLAN-em.

Sprawdzaj logi

Większość access pointów ma wbudowane logowanie. Przeglądaj access logi regularnie i zwracaj uwagę na nieprawidłowości.

Wprowadź zasady bezpiecznego użytkowania sieci

Upewnij się, że pracownicy nie odwiedzają niedozwolonych witryn, które mogą powodować konsekwencje zarówno prawne, jak i społeczne. Nieodpowiednie użytkowanie sieci niepotrzebnie trwoni dostępne pasmo i osłabia produktywność. Zasady korzystania z sieci mogą być egzekwowane poprzez korzystanie z zewnętrznych serwisów filtrujących.

Autor jest inżynierem systemowym w firmie 3Com

Biznesowa komunikacja mobilna nie musi wiązać się z ryzykiem

Piotr Kupczyk

Podróżuj bezpiecznie ze swoim smartfonem

Jeśli dużo podróżujesz, prawdopodobnie musisz często się komunikować. Jeżeli jesteś właścicielem firmy i Twoi pracownicy uzyskują dostęp do wiadomości e-mail i adresów za pośrednictwem smartfonów, konieczne są odpowiednie zabezpieczenia. Współczesne oprogramowanie bezpieczeństwa może zapobiec poważnym stratom i zagrożeniom.

Bycie osiągalnym przez cały czas, możliwość odpowiedzenia na e-maile lub sprawdzenia cennika podczas podróży – wymagania te odnoszą się nie tylko do dużych firm, ale również wielu małych i bardzo małych przedsiębiorstw. Natychmiastową łączność umożliwiają wprowadzane od pewnego czasu niedrogie pakiety danych wliczone w ceny abonamentów. Na obszarach obsługiwanych przez UMTS osiągane są rzeczywiste prędkości DSL, a do e-maili i okazjonalnych transferów danych wystarczy nawet GPRS czy EDGE. Smartfony to najpopularniejsze mobilne urządzenia. Wielu producentów oferuje bogaty wachlarz telefonów komórkowych wyposażonych w dodatkowe funkcje. Mimo bogatego zestawu funkcji, większość modeli nie kosztuje więcej niż tradycyjne telefony komórkowe kilka miesięcy temu. Smartfon bardziej przypomina mały komputer niż telefon. Na przykład system operacyjny Windows Mobile jest bardzo podobny do swojego odpowiednika dla komputera PC. Ponadto smartfony oferują wydajność taką, jak komputery. Poczta elektroniczna, książka adresowa, lista zadań czy pakiet biurowy – wszystko to znajdziecie teraz w urządzeniu mieszczącym się w dłoni. Klienci doceniają to bogactwo możliwości komunikacyjnych. Przewiduje się, że w 2010 roku liczba smartfonów będzie dwukrotnie większa niż liczba notebooków. W tym samym badaniu Gartner ustalił, że już dzisiaj liczba smartfonów jest równa liczbie notebooków dostępnych na rynku.

Bezpieczeństwo nadal ma niski priorytet

Podczas gdy praktycznie każdy firmowy pecet, nawet w najmniejszym biurze, jest wyposażony przynajmniej w oprogramowanie bezpieczeństwa, sytuacja jest o wiele gorsza w przypadku smartfonów. Obecnie prawie nikt nie instaluje ochrony na smartfonie. Nie ma wątpliwości, że istnieje poważne zagrożenie na tym obszarze. W zeszłym roku 94 proc. menedżerów IT oceniło zagrożenia bezpieczeństwa przedostające się za pośrednictwem smartfonów wyżej niż te przedostające się za pośrednictwem urządzeń przenośnych (88 proc.) lub laptopów (79 proc.). Dane te pochodzą z badania przeprowadzonego przez firmę Credant, dostawcę technologii szyfrowania. Badanie to ujawniło niepokojący fakt: ponad połowa menedżerów przyznała, że nie „zaprząta sobie głowy" hasłem podczas korzystania z telefonów komórkowych lub smartfonów. Jest to tym bardziej niepokojące, że te „łatwe do nabycia" mobilne urządzenia stają się celem ataków coraz większej liczby cyberprzestępców. Niezabezpieczony smartfon nie musi nawet zostać skradziony. Istnieją narzędzia, które umożliwiają ściągnięcie zawartości smartfonów poprzez Bluetootha, nawet z pewnej odległości.

Brak skutecznych zabezpieczeń oznacza szeroko otwarte „drzwi" dla cyberprzestępcy. Istotne znaczenie ma fakt, że w przeciwieństwie do prywatnych telefonów komórkowych, urządzenia firmowe zawierają krytyczne dane biznesowe, które nie powinny dostać się w niepowołane ręce, ponieważ mogłoby to spowodować poważne szkody. Z badania przeprowadzonego przez Business Performance Management Forum w 2006 roku wynika, że już wtedy co najmniej 25 proc. wszystkich urządzeń PDA, telefonów komórkowych i smartfonów zawierało poufne informacje. Dwa lata później badanie przeprowadzone przez Toshiba Mobile Communications wykazało, że liczba ta wzrosła do prawie 90 proc.

Kod PIN nie stanowi wystarczającego zabezpieczenia

Obecnie bezpieczeństwo telefonów komórkowych często ogranicza się do kodu PIN wprowadzanego podczas włączania telefonu. Jednak w ten sposób zabezpieczamy się tylko przed wykorzystaniem karty SIM. Poza tym takie zabezpieczenie działa, pod warunkiem że w momencie kradzieży lub zgubienia telefon był wyłączony. A przecież telefon zostaje zainfekowany oprogramowaniem crimeware wtedy, gdy jest włączony: w miejscach publicznych lub gdy posiadacz telefonu znajduje się w większym tłumie, np. na stacji kolejowej lub metra. Niektóre szkodliwe programy od razu wykorzystują sposobność, próbując zainfekować telefony komórkowe znajdujące się w zasięgu za pośrednictwem Bluetootha. Inne programy, zorientowane na destrukcję, wysyłają wiadomości tekstowe do wszystkich kontaktów w książce telefonicznej, co powoduje zablokowanie telefonu.

Oprogramowanie crimeware, takie jak Trojan.SymbOS.Skuller i Rommwar całkowicie blokuje telefon komórkowy. Trojan.SymbOS.Cardblock i Worm.MSIL.Cxover automatycznie usuwają dane znajdujące się w urządzeniu. Wirus CardBlock specjalizuje się w kartach pamięci. Po tym, jak ofiara uruchomi szkodliwy kod zamaskowany jako narzędzie SIS, dostęp do karty pamięci zostanie zablokowany, wszystkie aplikacje zostaną uszkodzone, a wiadomości SMS i MMS – usunięte. Szkody te są nieodwracalne, nie pomoże nawet leczenie telefonu komórkowego. Zainfekowanie telefonu komórkowego oprogramowaniem crimeware prawie zawsze

wymaga przeinstalowania oprogramowania sprzętowego. Poza tym należy liczyć się z utratą ustawień i danych. Odzyskanie informacji oraz przywrócenie wszystkich funkcji smartfonu kosztuje dział IT lub dostawcę czas i pieniądze.

Program chroniący przed oprogramowaniem crimeware sprawdza dane wysyłane na telefon za pośrednictwem Bluetootha, WLAN, GPRS lub UMTS i natychmiast blokuje podejrzaną aktywność. Ponieważ w każdym czasie możesz stać się ofiarą jednego z tych ataków, niezbędne jest posiadanie stale aktywnej ochrony. Taką koncepcję ochrony producenci oprogramowania nazywają ochroną „w czasie rzeczywistym". Istotne znaczenie ma również fakt, że oprogramowanie bezpieczeństwa aktywnie chroni również urządzenia podczas procesów synchronizacji z domowym pecetem w celu powstrzymania szkodliwego oprogramowania przed przedostawaniem się z urządzenia mobilnego na komputer PC.

Zszargana reputacja to problem, którego nie można lekceważyć

Jak pokazują skandale związane z ochroną prywatności, jakie miały miejsce w ciągu ostatnich miesięcy, klienci doskonale zdają sobie sprawę, w jaki sposób firma postępuje z poufnymi informacjami. Aktualne badanie przeprowadzone przez Ponemon Institute pokazało, że liczba klientów, którzy odwrócili się od firmy po skandalu związanym z naruszeniem prywatności, wzrosła o 3,24 proc. Jedna z firm uczestniczących w badaniu odnotowała nawet 8-proc. wzrost liczby utraconych klientów. To oznacza, że w przypadku utraty smartfonu utrata poufnych danych stanowi nawet większy problem niż materialna utrata telefonu. Ponieważ urządzenia mobilne oferują tak wiele funkcji, często zawierają te same informacje co komputer PC w siedzibie firmy. Cyberprzestępcy zdają sobie z tego sprawę i w coraz większym stopniu wybierają łatwiejszy cel, tj. smartfony.

Istotne jest to, aby rozwiązanie bezpieczeństwa obejmowało wszystkie obszary, w których konieczna jest ochrona. Oznacza to zabezpieczenie przed konsekwencjami zarówno pozostawienia telefonu w pociągu, jak i przed atakami szkodliwego kodu za pośrednictwem Bluetootha lub poczty elektronicznej. To, czy urządzenie mobilne zostało skradzione czy zgubione, nie robi początkowo żadnej różnicy. Nie ma wątpliwości, że dane należy chronić przed tym, aby nie uzyskały do nich dostępu obce osoby, niezależnie od tego, czy znalazcą będzie zwykły ciekawski czy też złodziej szukający określonych informacji. Pakiet Kaspersky Mobile Security Enterprise Edition firmy Kaspersky Lab oferuje wiele funkcji, które zapewniają taką ochronę. Najważniejszą dla ochrony danych jest funkcja blokowania urządzenia poprzez SMS. Po zauważeniu kradzieży lub zgubienia sprzętu użytkownik może natychmiast wysłać SMS z innego telefonu do swojego smartfonu. Po otrzymaniu wiadomości urządzenie jest blokowane, a jego odblokowanie możliwe jest tylko za pomocą odpowiedniego, zdefiniowanego wcześniej, kodu. Jeśli chcesz większego bezpieczeństwa, możesz użyć funkcji czyszczenia za pośrednictwem SMS-a. Procedura jest taka sama: po tym, jak urządzenie otrzyma wiadomość, wszystkie dane przechowywane w smartfonie zostaną usunięte. Kontakty, wiadomości e-mail, SMS-y, dane dostępu do wirtualnej sieci prywatnej firmy lub zawartość pamięci i kart pamięci – można z góry określić, co trafi do cyfrowej „niszczarki".

Halo, ukradłeś mój telefon komórkowy

Ograniczenie szkód to jedna rzecz, należy jednak pamiętać, że urządzenie również ma wartość. Czy nie byłoby miło, gdyby utracone urządzenie mogło skontaktować się z tobą, jak tylko zostanie podłączone do sieci mobilnej? Taką możliwość oferuje Mobile Security Enterprise Edition firmy Kaspersky Lab. Jeżeli złodziej będzie próbował wymienić kartę SIM na nową, funkcja SIM Watch wyśle wiadomość tekstową z nowym numerem do predefiniowanego odbiorcy, po czym natychmiast zablokuje urządzenie. Uniemożliwi to cyberprzestępcom „recycling" telefonu i zwiększy szanse na jego odzyskanie.

Oprogramowanie antywirusowe musi być stale uaktualniane. Jeśli dystrybucja nowych sygnatur oznacza dodatkową pracę, stosunek kosztów do zysków przesuwa się na niekorzyść firmy. Dlatego ważne jest, aby oprogramowanie automatycznie szukało i pobierało uaktualnienia całkowicie automatycznie. Jeżeli pakiety sygnatur są niewielkie, również koszty ich pobierania nie będą wysokie, nawet bez stawki ryczałtowej w abonamencie. Koszty kryją się również gdzie indziej. Spam mobilny to prawdziwy pochłaniacz czasu, nawet jeśli jego ilości nie dorównują jeszcze liczbie niechcianych wiadomości w skrzynkach e-mailowych. Według wyników badania przeprowadzonego przez University of St. Gallen, problem spamu przychodzącego na telefony komórkowe dotknął ponad 80 proc. wszystkich użytkowników. Producent rozwiązania do ochrony przed spamem w Stanach Zjednoczonych, Cloudmark, stwierdził, że w 2007 roku otrzymano 1,1 miliona mobilnego spamu, a w 2008 roku liczba ta zwiększyła się o ponad 50 proc. Rozwiązanie ochrony powinno pomóc uniknąć takich kosztów. Nieodzownym narzędziem są czarne i białe listy, które mogą być skonfigurowane centralnie w siedzibie firmy i wysłane do wszystkich smartfonów. W celu zaoszczędzenia pracy administracyjnej wewnętrzne kontakty z twojej książki adresowej powinny być automatycznie przeniesione do białej listy.

Smartfony mogą pozwolić małym firmom na uzyskanie zdecydowanej przewagi konkurencyjnej. Te wielofunkcyjne urządzenia oferują dużą wydajność i stanowią swego rodzaju okno na miejsce pracy współpracownika, który przebywa właśnie w podróży służbowej. Urządzenia te należy jednak traktować jako integralną część infrastruktury IT. Nie należy oszczędzać na rozwiązaniach bezpieczeństwa dla smartfonów, ponieważ w ten sposób można osłabić wszystkie zabezpieczenia w całej firmowej sieci komputerowej. Współczesne oprogramowanie bezpieczeństwa może kontrolować zagrożenia, a dobrze rozwinięte narzędzia zarządzania mogą przy niewielkim wysiłku utrzymać rozwiązanie bezpieczeństwa pod kontrolą.

Jedno jest pewne: koszty ponoszone w wyniku skutecznego ataku na smartfon są o wiele wyższe niż inwestycje w bezpieczeństwo. Dodatkową korzyścią, którą trudno przecenić, jest poczucie bezpieczeństwa!

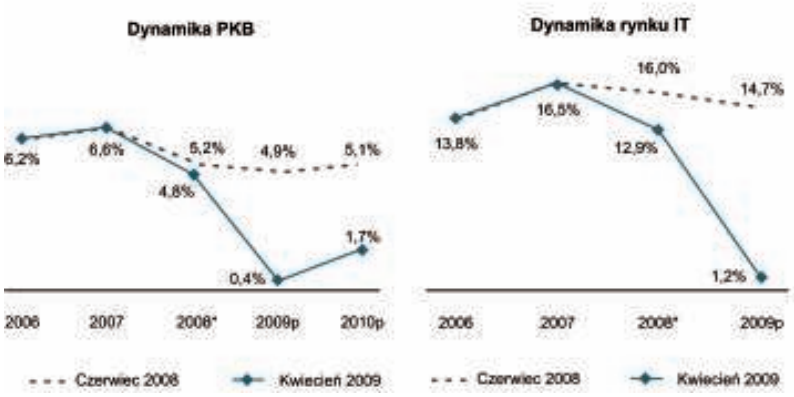
Autor jest dyrektorem działu prasowego Kaspersky Lab Polska

IT z kryzysem w tle

Rewizja prognoz dla rynku IT w Polsce

Kryzys gospodarczy, mimo iż w mniejszym stopniu, dotyka również branży IT. Wyraźne pogorszenie danych makroekonomicznych dla regionu środkowoeuropejskiego spowodowało konieczność rewizji prognoz dla rynku informatycznego. O wzrosty w roku 2009 będzie bardzo trudno.

Dynamika PKB i rynku IT w Polsce (proc.) według danych i prognoz PMR z czerwca 2008 r. i kwietnia 2009 r., 2006-2010



**** odpowiednio prognoza i szacunek***
p – prognoza
ródło: Raport „Rynek IT w Polsce 2008. Prognozy rozwoju na lata 2008-2012 – aktualizacja. Wpływ kryzysu na kluczowe dane i prognozy". PMR Publications, dział PMR, 2009.

Chociaż globalny kryzys gospodarczy branża informatyczna odczuwa relatywnie słabiej niż wiele innych sektorów gospodarki, spowolnienie gospodarcze będzie mieć swoje odzwierciedlenie również w wynikach firm IT. W ciągu najbliższych dwóch lat rynki IT we wszystkich krajach środkowoeuropejskich czeka bardzo wyraźne wyhamowanie dynamicznych wzrostów widocznych w poprzednich latach, a nawet spadek wartości.

Powodem jest przede wszystkim spodziewana recesja gospodarcza, co odbije się na wydatkach zarówno firm, jak i konsumentów. W branżę IT uderzą m.in. oszczędności inwestycyjne sektora finansowego, który jest jednym ze strategicznych odbiorców IT.

W ocenie firmy badawczej PMR, w 2009 r. skumulowana wartość rynku IT w trzech największych krajach rynku środkowoeuropejskiego – w Rosji, na Ukrainie i w Polsce – spadnie o 10,5 proc. do ok. 22 mld euro.

Dla rynku polskiego najbardziej prawdopodobny scenariusz to minimalny, jednocyfrowy wzrost wartości rynku w kolejnych dwóch latach.

Zakładany przez PMR poziom średniorocznego wzrostu PKB w latach 2009-2012 przy formułowaniu prognoz rozwoju rynku IT w Polsce wynosił w ubiegłym roku ok. 5,3 proc. Obecnie, w ocenie PMR, wskaźnik nie przekroczy 3 proc. Bardziej pesymistyczne prognozy dotyczą również nakładów na środki trwałe w gospodarce. W maju ubiegłego roku spodziewany był wzrost na poziomie 10-12 proc. w dwóch kolejnych latach, podczas gdy obecnie możliwa jest ujemna dynamika w bieżącym roku.

Większość dużych firm IT deklaruje, że nie odczuła jeszcze skutków spowolnienia gospodarczego w Polsce i spodziewa się pozytywnych wyników w 2009 r. Dotyczy to przede wszystkim dostawców oprogramowania i usług IT, którzy często związani są długoterminowymi umowami. Bardziej pesymistyczne oczekiwania co do rozwoju rynku IT w ciągu najbliższego roku mają natomiast dystrybutorzy sprzętu.

Właśnie w przypadku tego ostatniego segmentu widać najbardziej wyraźną różnicę między prognozami PMR z połowy ubiegłego roku a sytuacją bieżącą. Już w 2008 r. mieliśmy bowiem do czynienia z wyraźnym spadkiem sprzedaży komputerów stacjonarnych oraz monitorów, w szczególności w ostatnich miesiącach roku. Mniejszemu popytowi na desktopy i monitory towarzyszył wzrost cen importowanego sprzętu spowodowany wzrostem kursu dolara. W konsekwencji dostawcy musieli godzić się na obniżanie już i tak niskich marż lub oferować sprzęt po wyższych cenach, co dodatkowo odbijało się na poziomie sprzedaży.

Spadki w segmencie desktopów zrównoważyła tylko w części rosnąca sprzedaż komputerów przenośnych, których udział w całkowitej sprzedaży komputerów w Polsce przekroczył już wyraźnie 50 proc.

Bieżący rok będzie dla dostawców sprzętu okresem minimalizacji strat. W czasie kryzysu zostaną zdecydowanie wydłużone cykle wymiany. Klienci biznesowi ograniczający koszty działalności będą zainteresowani maksymalnym opóźnieniem procesu wymian. Należy spodziewać się także większej popularności technologii energooszczędnych i wirtualizacyjnych. ■

Nowe techniki cyberprzestępców

Grzegorz Kantowicz

Manipulacje wynikami wyszukiwarek internetowych

Panda Security wykryła strony internetowe do promowania fałszywych programów antywirusowych w wyszukiwarkach. Witryny te wykorzystują informacje oferowane przez Google Trends. Analizy wykazały także, że szkodliwe serwisy internetowe oferują różne treści w zależności od sposobu, w jaki użytkownicy docierają do danej strony.

Według doniesień firmy Panda Security – dostawcy rozwiązań zabezpieczających z sektora IT, cyberprzestępcy manipulują wynikami wyszukiwarek internetowych w celu rozprzestrzeniania złośliwych kodów, a w szczególności fałszywych programów antywirusowych. Przyczyny takiego działania są proste – aby móc dokonać infekcji komputerów, przestępcy muszą zachęcić użytkowników do odwiedzenia szkodliwych witryn. Interesująca jest jednak nowa technika przyciągania użytkowników na te właśnie witryny.

Google Trends pomaga zwabić ofiary

Dawniej ofiary wabiono na niebezpieczne strony za pomocą masowo rozsyłanego spamu. Użytkownik czytał treść wiadomości, klikał na zawarte w niej linki, a następnie – nie będąc tego świadomym – był przekierowywany na szkodliwą stronę www. Jednak z uwagi na rosnącą nieufność użytkowników wobec wiadomości otrzymywanych od nieznanych nadawców, cyberprzestępcy zaczęli stosować skuteczniejsze spo-soby wabienia nowych ofiar. Jeden z nich polega na wykorzystaniu narzędzia Google Trends (http://www.google.com/trends), które między innymi prezentuje najbardziej popularne frazy wyszukiwane w danym dniu (przykładowo: „przemówienie inauguracyjne prezydenta Obamy" czy „nominacje do Oscarów").

Po uzyskaniu danych o najpopularniejszych frazach i tematach danego dnia cyberprzestępcy tworzą blog, który zawiera te słowa (np. Obama, Penelope Cruz itp.) oraz materiały wideo rzekomo powiązane z tymi informacjami. Te nieetyczne działania pozwalają uplasować fałszywą stronę na wyższej pozycji w wyszukiwarce. – *Użytkownicy, którzy uwierzą w prawdziwość tych wyników, odwiedzają witrynę, na której są zachęcani do pobrania kodeka lub innej aplikacji, umożliwiających obejrzenie pliku wideo. Kliknięcie odsyłacza powoduje jednak pobranie złośliwego oprogramowania, najczęściej fałszywego programu antywirusowego* – wyjaśnia **Maciej Sobianek**, specjalista ds. bezpieczeństwa w Panda Security Polska.

Fałszywe programy antywirusowe symulują działanie prawdziwych systemów zabezpieczeń, próbując przekonać użytkowników, że ich komputery zostały zainfekowane złośliwymi kodami. Ofiary zachęca się do zakupu oprogramowania, które pozwoliłoby usunąć fikcyjne infekcje. Cyberprzestępcy coraz częściej stosują tego rodzaju oszustwa i uzyskują znaczne korzyści finansowe.

Techniki SEO

Ten typ ataku wykorzystuje zaawansowane techniki SEO (*Search Engine Optimization*). Są to legalne sposoby tworzenia serwisów internetowych, których celem jest zwiększenie ilości i jakości ruchu na witrynie, a także poprawienie jej pozycji na liście wyników wyszukiwania (głównie w wyszukiwarce Google). Przykładem jest witryna www sprzedająca fałszywy program antywirusowy Malwaredoctor, stworzony specjalnie w celu osiągnięcia wysokiej pozycji w wyszukiwarce.

Oprócz wyżej opisanych standardowych technik pozycjonowania, atakujący uciekają się także do sposobów znanych jako Black Hat SEO. Są to nielegalne techniki pozycjonowania, niezgodne z zasadami ustanowionymi przez twórców wyszukiwarek i polegają na stosowaniu alternatywnej treści lub wpływaniu na odczucia użytkowników. Czasami trudno określić, czy dana technika jest prawidłowa czy też nie, z uwagi na zasady stosowane przez daną wyszukiwarkę.

Sposoby ukrywania ataków

Cyberprzestępcy starają się utrudnić producentom oprogramowania zabezpieczającego identyfikację własnych stron. W tym celu stosują coraz bardziej zaawansowane sposoby przeprowadzania ataków. Na przykład niektóre ze złośliwych witryn, jakimi posługują się cyberprzestępcy, zachowują się inaczej i prezentują różne treści w zależności od pochodzenia odwiedzającego je użytkownika.

W celu ukrycia ataku cyberprzestępcy stosują skrypt, który określa pochodzenie odwiedzającego. Jeżeli użytkownik wprowadzi adres URL witryny, którą chce odwiedzić, na pasku adresu przeglądarki prezentowana jest prawidłowa treść. Jeżeli jednak użytkownik korzysta ze zmanipulowanych wyników wyszukiwarki Google, zostanie przeniesiony na szkodliwą witrynę www.

MSAntispyware 2009

Laboratorium PandaLabs wykryło witrynę www, która reprezentuje nowy przykład zastosowania techniki Black Hat SEO. Zazwyczaj strony sprzedające fałszywe programy antywirusowe (zarówno te, które zawierają określone znaczniki, jak i pozostałe) są tworzone w taki sposób, aby ich pozycja w wyszukiwarkach była jak najwyższa. Jednak w przypadku witryny wykorzystywanej do dystrybucji MSAntispyware 2009 sytuacja wyglądała zupełnie inaczej. Wszystkie znaczniki i procesy zaprojektowane zostały w taki sposób, aby strona nie została zaindeksowana w wyszukiwarkach.

Celem takiego postępowania było znaczne utrudnienie analitykom złośliwego oprogramowania oraz producentom zabezpieczeń działań mających udaremnić infekcje z wykorzystaniem blokowania adresów URL. ■

Nowe technologie wśród młodzieży

Elektroniczna legitymacja studencka na polskich uczelniach

Co studenci sądzą o elektronicznych legitymacjach studenckich? Gdzie i do czego wykorzystywane są studenckie karty? Co studenci sądzą o podpisie elektronicznym? Ilu z nich chciałoby go wykorzystywać i w jakim celu? Na te i wiele innych pytań odpowiada raport Gemalto: „Elektroniczna legitymacja studencka na polskich uczelniach – jedna karta, wiele możliwości".

Elektroniczne karty studenckie zaczęto wprowadzać w Polsce na szeroką skalę pod koniec 2007 roku. W chwili obecnej korzysta z nich 115 szkół wyższych w Polsce, a kolejnych 300 przygotowuje się do ich wprowadzenia w najbliższym czasie. Jest to część procesu informatyzacji polskich uczelni.

Gemalto we współpracy z lokalnym partnerem (VAR-em) – firmą OPTeam wprowadziło ponad milion kart na polski rynek. Firma postanowiła sprawdzić, jak polscy studenci przyjęli nową formę identyfikacji studenckiej i w jakich obszarach oczekiwaliby dalszych usprawnień. Badanie Gemalto zostało przeprowadzone przez TNS OBOP w lutym br.

Studenci – fani nowych technologii

Wyniki badania potwierdzają trend, że młodzi ludzie swobodnie poruszają się w świecie nowych technologii. Komunikacja wirtualna i korzystanie z internetu w codziennych czynnościach sprawiają, że studenci również w zakresie elektronicznych nośników oczekują efektywnych i prostych rozwiązań, takich jakie daje elektroniczna legitymacja studencka. 100 proc. badanych ma dostęp do internetu.

Blisko 70 proc. preferuje dokonywanie opłat i zakupów przez internet, taka sama liczba woli płacić kartą niż gotówką, 84 proc. posiada internetowe konto bankowe. Karta elektroniczna, dzięki możliwości dodawania kolejnych aplikacji, umożliwia skonsolidowanie na jednym nośniku dużej liczby funkcji, na co dzień wykorzystywanych przez studentów.

Nowoczesne rozwiązania oparte na elektronicznej legitymacji studenckiej są entuzjastycznie przyjmowane przez młodych ludzi.

Wysoka ocena wielofunkcyjnej legitymacji studenckiej

Studenci polskich uczelni bardzo dobrze przyjęli wymianę papierowych legitymacji na elektroniczne, wielofunkcyjne karty. Aż 80 proc. studentów jest zadowolonych z elektronicznej legitymacji studenckiej, a blisko 40 proc. ankietowanych uważa, że nowa karta nie posiada żadnych wad. Studenci podkreślają, że jest to nowoczesny, poręczny nośnik różnego rodzaju danych (48 proc. ankietowanych), 25 proc. za największą zaletę uważa jej wielofunkcyjność. Blisko 80 proc. studentów używających elektronicznych legitymacji poleciłoby taką formę identyfikacji innym studentom korzystającym z papierowych legitymacji, a 86 proc. zadeklarowało, że gdyby sami podejmowali decyzję w sprawie formy legitymacji studenckiej, wybraliby kartę elektroniczną.

Elektroniczna legitymacja studencka dziś

Najczęściej poza funkcją legitymacyjną studenci wykorzystują kartę jako kartę wstępu do obiektów studenckich (bibliotek, akademików, basenów itp.) – 77 proc. respondentów. Ponadto studenci wymieniają jeszcze funkcje biletu komunikacji miejskiej – 43 proc. oraz karty pomocnej przy logowaniu się do uczelnianych komputerów i systemów – 20 proc. Połączenie w jednym nośniku legitymacji i biletu komunikacji miejskiej najczęściej wymieniali studenci z Warszawy, a jako karty identyfikacyjnej i wstępu do uczelnianych obiektów ankietowani z Gdańska.

Wyrobienie pierwszej karty i jej przedłużenie

Dla władz uczelni wdrożenie nowego systemu identyfikacji studenckiej było ważnym przedsięwzięciem. W opinii studentów, uczelnie w miarę sprawnie poradziły sobie z realizacją projektu. 64 proc. ankietowanych jest zadowolonych z łatwości wyrobienia pierwszej elektronicznej legitymacji studenckiej. Pozytywnie studenci również ocenili czas oczekiwania na pierwszą legitymację i łatwy proces przedłużania ważności legitymacji studenckiej – 60 proc. badanych. Najlepszą ocenę pod tym względem uzyskały uczelnie z Krakowa i Gdańska.

Elektroniczna legitymacja studencka jutro

Studenci są zadowoleni z elektronicznych legitymacji, jednak wiedzą, że karty mogą być wyposażone w większą liczbę funkcji. Co trzeci z nich chciałby dysponować większą liczbą opcji na swojej karcie. W podziale na miasta najbardziej zainteresowani zwiększeniem liczby dostępnych funkcji są studenci z Wrocławia – ponad 90 proc. respondentów. Spośród funkcji, które studenci najczęściej wymieniają spontanicznie, znalazły się: bilet komunikacji miejskiej, karta płatnicza, elektroniczny indeks oraz karta rabatowa. W odpowiedzi na to samo pytanie, przy pomocy wspomaganej listy, w największym stopniu studenci są zainteresowani, aby przy użyciu legitymacji studenckiej mieli zdalny dostęp do wyników egzaminów, planów etc. – 93 proc., chcieliby „załadować" na swoją kartę bilet do teatru, kina czy na samolot – 91 proc., czy bilet wstępu na imprezę masową – 88 proc. respondentów.

Studencka legitymacja a podpis elektroniczny

Legitymacja studencka w formie karty elektronicznej umożliwia dodawanie kolejnych aplikacji, co stwarza pole rozwoju dla nowych produktów i funkcjonalności, wykorzystywanych również w komunikacji z innymi, pozastudenckimi podmiotami, m.in. urzędami czy bankami.

Społeczność studencka zna pojęcie podpisu elektronicznego i wie, do czego on służy. Ogółem termin rozpoznaje 79 proc. badanych, z czego najlepiej studenci uczelni ekonomicznych – 95 proc. respondentów. Studenci zastosowanie podpisu elektronicznego widzą w komunikacji z urzędami państwowymi – na pytanie, do czego służy podpis elektroniczny, wskazywali: podpisywanie dokumentów urzędowych przez internet – 62 proc. respondentów i potwierdzenie tożsamości przez internet (51 proc. ankietowanych).

69 proc. ankietowanych chciałoby mieć na swojej studenckiej karcie własny podpis elektroniczny. ■

W sieci z głową na karku…

Maciej Ziarek

Wirtualna kradzież, prawdziwe pieniądze…

Bankowość elektroniczna jest jednym z najszybciej rozwijających się sektorów ekonomii. Daje ona nowe możliwości omijania szerokim łukiem kolejek przy okienkach kasowych, płacenia rachunków przez internet czy robienia zakupów. Banki starają się coraz bardziej uatrakcyjnić swoje oferty i sprawiać, by bankowość była coraz łatwiejsza w użyciu. Jednak wygoda przeważnie nie idzie w parze z bezpieczeństwem, które często musi być zdegradowane na rzecz łatwości obsługi konta przez klienta.

W Polsce zabezpieczenia bankowości elektronicznej stoją na wysokim poziomie. Największe banki, które obsługują większość Polaków, stosują po kilka zabezpieczeń, począwszy od lepszego uwierzytelnienia i zabezpieczenia przed podsłuchem podczas logowania, aż po ochronę środków zgromadzonych na koncie. W dalszej części artykułu będę prezentował te zabezpieczenia. Wskażę również, co powinien zrobić sam klient, aby ochronić swój dorobek.

Bezpieczeństwo po stronie banku

Banki tworzą coraz doskonalsze metody zabezpieczania kont swoich klientów. Istotne jest jednak to, aby sposoby uwierzytelniania klienta nie były dla niego kłopotliwe w obsłudze, a sam proces logowania nie przebiegał zbyt długo. Obecnie stosowane formy zabezpieczeń omawiam poniżej. Możemy je podzielić na te, które bronią dostępu do samego konta (procesu logowania) oraz te, które chronią nasze środki zgromadzone na koncie i ustawienia konta przed jakąkolwiek zmianą.

Login i hasło

Zarówno login, jak i hasło stanowią pierwszą barierę przed nieupoważnionym dostępem do konta. Bank ma tylko częściowy wpływ na to, jak mocne będzie to zabezpieczenie. O ile login zostaje nam najczęściej przydzielony, o tyle hasło musi spełnić pewne standardy wyznaczone przez sam bank. Są to najczęściej:

- wymóg stosowania hasła składającego się z przynajmniej 7 znaków (w zależności od banku, to minimum może wynosić nawet 10 znaków);
- hasło musi zawierać cyfry, małe i duże litery oraz znaki specjalne.

Ponadto banki starają się zwrócić uwagę klienta (poprzez sekcję FAQ na stronie czy konsultantów telefonicznych, za pośrednictwem których wykonujemy pewne operacje) na to, aby nie udostępniał swojego loginu oraz hasła, a także by nigdzie go nie zapisywał. Bardziej świadomy ryzyka klient to przecież także mniejsze straty dla samego banku. Fakt, że login jest nam z góry nadany, nie jest tutaj również bez znaczenia. Gdyby to klient wybierał login, byłby on łatwy do odgadnięcia – na przykład, Anna1978. Bank nadaje zbiór cyfr, czasami także liter, które potencjalnemu atakującemu trudniej zdobyć. Mało prawdopodobne jest także to, że cyberprzestępca odgadnie taki login.

Hasło maskowane

Hasło maskowane ma zapobiec skutkom posiadania w systemie keyloggera lub trojana, który przechwytuje wszystkie znaki, jakie wprowadzamy przy pomocy klawiatury. Metoda ta polega na wymaganiu podania jedynie niektórych znaków z naszego hasła. Za każdym razem system banku prosi o podanie innych znaków. Aby pokazać, jak działa to w praktyce, poniżej prezentuję pewien schemat. Załóżmy, że nasze hasło to Kaspersky:

_**_*_**_

System automatycznie wpisał pięć znaków (*), natomiast nas prosi o podanie pozostałych czterech (_). Będą to oczywiście K, p, r, i. Przy kolejnym logowaniu schemat może się całkowicie zmienić i wymagane mogą być inne znaki:

*_**_*_*

Tym razem są to a, e, s, i. Dzięki takiemu zabezpieczeniu, nawet w przypadku zainfekowania systemu keyloggerem atakujący przechwyci jedynie kilka znaków, które nie dadzą mu możliwości zalogowania się na konto, bowiem przy kolejnej próbie na pewno wymagane będą inne znaki.

Klawiatura ekranowa

Klawiatura ekranowa jest znana od dawna, ponieważ stanowi standardowy dodatek wielu systemów operacyjnych. Banki zauważyły wiele korzyści płynących z jej stosowania. Jeżeli użytkownik loguje się do banku z komputera, który jest zainfekowany, jednak stosuje do tego klawiaturę ekranową, to nie ma możliwości, by przechwycił jakimś programem treść czy hasła wpisywane na stronie logowania.

Klawiatura ekranowa wchodząca w skład systemu Windows

Token generujący hasła jednorazowe

Znaki z klawiatury ekranowej wybieramy i wciskamy używając myszki, dzięki temu keylogger nie rejestruje żadnej aktywności.

Obrazek antyphishingowy

Kolejną metodą, która zwiększa bezpieczeństwo logowania, jest obrazek antyphishingowy. Sam sposób jest banalny, ale w swojej prostocie bardzo skuteczny. Jak sama nazwa wskazuje, mechanizm chroni przed wyłudzeniem danych po przekierowaniu klienta na spreparowaną stronę. Użytkownik wybiera (najczęściej w ustawieniach własnego konta) jeden z dostępnych obrazków, który będzie się pojawiał przy każdym logowaniu. Jego brak podczas logowania świadczyć może o tym, że padliśmy ofiarą oszustwa. Wówczas należy jak najszybciej zaprzestać wpisywania jakichkolwiek danych, opuścić witrynę i poinformować o zdarzeniu bank.

Kody jednorazowe

To zabezpieczenie nie chroni bezpośrednio dostępu do konta – banki nie wymagają podawania kodów jednorazowych podczas logowania. Jest to jednak bardzo dobre zabezpieczenie w przypadku kiedy ktoś uzyska nieautoryzowany dostęp do naszego konta. Najpierw jednak kilka słów o samej metodzie. Jak sama nazwa wskazuje, mamy do czynienia z kodami, które są wymagane jedynie raz do przeprowadzenia newralgicznej dla konta procedury, np. przelewu czy zmiany danych. Po jednorazowym użyciu kod staje się nieważny. Klient może uzyskać taki kod na kilka sposobów: Przy pomocy karty kodów, na której jest umieszczonych kilkadziesiąt kodów, przykrytych folią zabezpieczającą, zdzieraną w momencie uzyskiwania dostępu do konkretnego kodu.

Karta z kodami jednorazowymi w postaci zdrapek

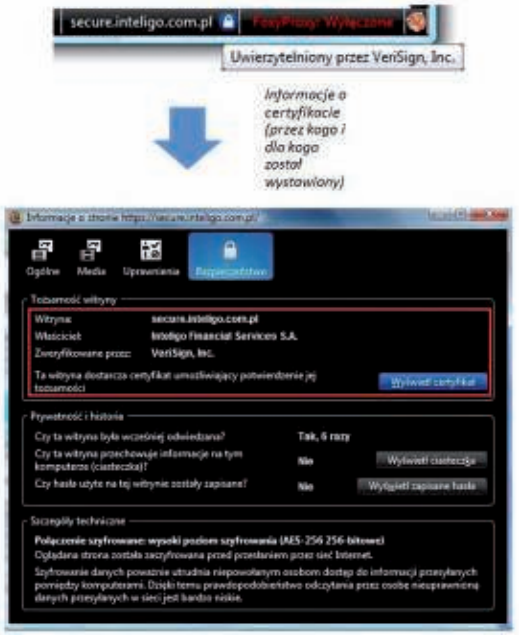
Za pomocą wiadomości SMS, wysyłanej na wcześniej wskazany przez klienta nr telefonu komórkowego.

Przy pomocy tokenu, który sam generuje kody jednorazowe ważne jedynie przez minutę. Po upływie tego czasu wyświetlany jest nowy kod, a stary jest unieważniany.

Dzięki kodom jednorazowym, nawet w przypadku przejęcia loginu i hasła do konta, atakujący nie będzie w stanie przelać pieniędzy na własny rachunek. Nie znaczy to oczywiście, że daje to 100-proc. zabezpieczenie przed kradzieżą. Żaden system nie daje takiej gwarancji. Ponadto ważne jest też, aby chronić także te dane, które widoczne są już po zalogowaniu się na konto i nie wymagają kodów jednorazowych (o czym napiszę później).

Certyfikaty

Certyfikat jest jednym z najważniejszych zabezpieczeń, ponieważ pozwala stwierdzić autentyczność witryny i jej przynależność do banku. Należy zwrócić uwagę, że samo szyfrowanie (https w pasku adresu) nie oznacza, że strona jest zabezpieczona poprzez certyfikat wystawiony przez jedno z centrów certyfikacyjnych. Podczas logowania na konto warto przyjrzeć się temu szczegółowi, zwłaszcza jeżeli dokonujemy zakupów przez sieć i sklep internetowy przekierowuje nas do strony logowania banku. Poniżej znajduje się przykład autentycznego certyfikatu.



Certyfikat

Ponadto banki starają się informować swoich klientów o sytuacjach, które mogą być ryzykowne, jak logowanie się na konto z kawiarenki internetowej czy z miejsca pracy.

Nie mając pewności, czy ktoś nie monitoruje naszych czynności przeprowadzanych w sieci, nie powinniśmy ryzykować i zaprzestać logowania.

Co może zrobić klient?

Sam klient nie jest zdany jedynie na łaskę banków i stosowane przez nie metody zabezpieczające. Można się nawet pokusić o stwierdzenie, że to od samego klienta zależy tak naprawdę bezpieczeństwo jego konta. To człowiek jest najsłabszym ogniwem we wszystkich zabezpieczeniach elektronicznych. Podatny na sugestię i oddziaływanie cyberprzestępców, instalujący przypadkowe programy okazujące się szkodliwymi aplikacjami, logujący się z różnych miejsc do konta. Poniżej wymienię najważniejsze warunki, jakie powinny zostać spełnione, aby nie zastać swojego konta pustego.

- Regularne aktualizacje systemu operacyjnego, oprogramowania zainstalowanego na komputerze oraz samych przeglądarek. Wiele szkodników wykorzystuje dziury w oprogramowaniu, aby przejąć kontrolę nad maszyną i zainstalować np. keylogger lub trojana. Także Linux nie jest tutaj w 100 proc. bezpieczny. Rzeczywiście nie ma wielu wirusów napisanych dla tego systemu, a te, które istnieją, nie stwarzają większego zagrożenia, jednak dziura w aplikacji to potencjalna szansa na wykorzystanie exploita, który pomoże przejąć kontrolę nad systemem.

- Stosowanie zaktualizowanego oprogramowania zabezpieczającego. Posiadanie samego antywirusa może w dzisiejszych czasach okazać się niewystarczające. Aby kompleksowo chronić komputer przed atakami, powinniśmy zainstalować pakiet typu Internet Security, w skład którego najczęściej wchodzą antywirus, firewall i narzędzie do wykrywania phishingu oraz zwalczania spyware.

- Korzystanie z systemów LiveCD. W przypadku konieczności logowania się do konta w kawiarenkach (przykładowo w czasie urlopów), powinniśmy zaopatrzyć się w jedną z dystrybucji Linuksa typu LiveCD, które uruchamiane są bezpośrednio z płyty i korzystają tylko z pamięci tymczasowej komputera, a nie z dysku twardego. Dzięki temu, nawet jeżeli na dysku znajdują się keyloggery, nic nie zostanie zapisane. Po przeprowadzeniu transakcji i wyłączeniu systemu nie pozostają po nas żadne ślady.

- Zachowanie informacji o koncie tylko dla siebie. Nie powinniśmy z nikim dzielić się wiedzą na temat naszego konta: jak długo je prowadzimy, ile mamy kart kredytowych czy debetowych, czy zaciągnęliśmy kredyt itp. Ma to o tyle istotne znaczenie, że niektóre banki w celu uwierzytelnienia klienta przez kanały telefoniczne zadają mu pytania dotyczące jego konta. Taka wiedza pomogłaby komuś podszyć się pod nas.

- Stosowanie się do wskazówek banku. Wszystkie zabezpieczenia, o jakich wspominałem wyżej przy okazji banków, są po to, by chronić nasze środki, a nie utrudnić nam korzystanie z konta... Jeżeli bank daje taką możliwość, używajmy klawiatury ekranowej; kiedy logujemy się, zerknijmy na dół strony, czy strona jest autentyczna i potwierdzona certyfikatem; nie zapisujmy haseł i loginów do banku w telefonie komórkowym ani – tym bardziej – na karteczkach przylepianych do monitorów.

A jednak się da... Przypadki włamań na bankowe konta internetowe

Chociaż zabezpieczenia bankowości internetowej uchodzą ogólnie za bardzo dobre, to w przypadku nieprzestrzegania pewnych wzorców zachowań i łamania zasad bezpiecznego korzystania z sieci jej bezpieczeństwo może być złudne. Poniżej prezentuję kilka sytuacji wziętych z życia, gdzie klienci banków stali się ofiarami oszustów i złodziei. Szczególnie pierwsza historia daje nam do myślenia, zwłaszcza w kontekście tego, o czym pisałem wcześniej (dlaczego wszystkie dane dotyczące naszej tożsamości, jak i rachunku bankowego powinny być niedostępne dla innych).

Znany prezenter telewizyjny – Jeremy Clarkson, prowadzący m.in. program motoryzacyjny Top Gear, w jednym z odcinków programu, w którym mowa była o głośnej w listopadzie 2007 r. sprawie utraty danych osobowych 25 milionów Brytyjczyków przez HM Revenue & Customs (Brytyjski Urząd Podatkowy i Celny), stwierdził, że media robią niepotrzebny szum w sprawie zaginięcia tych danych. Aby udowodnić swoją rację, iż takie dane nikomu się nie przydadzą, podał numer swojego konta oraz inne dane osobowe. Bardzo szybko się jednak zdziwił i odwołał wszystko, o czym mówił na temat nieistotności zaginionych danych. Do zmiany poglądu przyczyniło się zniknięcie 500 funtów z jego konta – nawet bank nie był w stanie stwierdzić, jak dokładnie do tego doszło. Pieniądze zostały przelane na konto organizacji British Diabetic Association. Oto, co powiedział Jeremy Clarkson po zajściu:

– Bank nie był w stanie stwierdzić, kto to zrobił i nie mógłby go powstrzymać przed zrobieniem tego ponownie. Myliłem się i zostałem ukarany za swój błąd.

W Szwecji bardzo popularny jest bank Nordea. Na początku 2008 roku stał się on celem licznych ataków, w wyniku których ucierpiała część klientów. Łączne straty, jakich doświadczył bank, sięgnęły miliona euro. Wprawdzie w oświadczeniu dla mediów bank przyznał, że zagrożenie nie dotyczy polskich klientów banku (dzięki nowocześniejszym od skandynawskich zabezpieczeń stosowanych w Polsce), jednak wiele osób wyrażało obawy o swoje środki zgromadzone na koncie. Atak przeprowadzany był za pomocą trojana wysyłanego pocztą elektroniczną.

W marcu i kwietniu 2008 r. do klientów banku BZ WBK rozsyłane były fałszywe wiadomości, które prowadziły do witryny z formularzem. Jego wypełnienie skutkowało wysłaniem danych do oszusta, a nie do banku. Pierwsza fala wiadomości była przygotowana mało starannie, druga natomiast mogła zostać odebrana przez wielu klientów jako autentyczna informacja z banku. Ten przypadek opiszę bardziej szczegółowo później, w celu zobrazowania, czym jest phishing w odniesieniu do bankowości elektronicznej.

Bardzo groźny atak został przeprowadzony na klientów banku PKO BP w czerwcu 2008 roku. Początkowo użytkownik był zachęcany do aktualizacji aplikacji Flash Player, która jest potrzebna do przeglądania wielu witryn. Plik ten jednak był trojanem, który zmieniał w systemie plik hosts, przez co przy wpisywaniu adresu banku w przeglądarce użytkownik był zawsze przekierowany na fałszywą stronę banku. Po wpisaniu loginu i hasła pojawiała się kolejna strona, na której trzeba było wpisać 5 kolejnych kodów jednorazowych ze zdrapki. Jeżeli ktoś to zrobił, dał przestępcy nie tylko login i hasło do konta, ale także możliwość wykonania przelewu z własnych środków na konto oszusta. Powyższe przykłady bardzo dobitnie pokazują, że niestosowanie się do zaleceń banku, a przede wszystkim brak rozwagi w tym, co się robi i nieświadomość zagrożeń może doprowadzić do sporych kłopotów.

Jak oni to robią?

Wspominałem już o tym, że banki stosują bardzo dobre zabezpieczenia. Ktoś może się zdziwić, dlaczego w takim razie dochodzi do kradzieży w bankowości elektronicznej. Dochodzi do nich, gdyż najsłabszym ogniwem tych zabezpieczeń jest człowiek. Jesteśmy podatni na manipulację i wpływ innych. To właśnie poprzez taką manipulację cyberprzestępca stara się uzyskać dostęp do konta. Oczywiście, istnieją metody bardziej wyrafinowane, ale mało kto je stosuje, ponieważ są trudniejsze do przeprowadzenia i nie dają szansy na zaatakowanie wielu osób naraz.

Socjotechnika

...To czynnik ludzki jest piętą achillesową systemów bezpieczeństwa ...Częściej jednak ataki takie są skuteczne (socjotechniczne), ponieważ ludzie nie rozumieją sprawdzonych zasad bezpieczeństwa.

Powyższe zdanie pochodzi z książki „Sztuka podstępu", napisanej przez Kevina Mitnicka. Opisuje on w niej, jak wielkim niebezpieczeństwem może być sam człowiek i jak łatwo można kogoś przekonać do tego, by podał hasło czy login. Szczególnie dobrze znane i najczęściej używane metody, które zostały opisane przez psychologów, to „stopa w drzwiach" oraz „drzwiami w twarz". Pierwsza polega na poprzedzaniu naszej prośby innymi, mniej istotnymi. Dzięki temu nie ma dużego kontrastu między kolejnymi prośbami i osoba je spełniająca nie czuje z tego powodu dyskomfortu. Druga metoda jest odwrotna. Ofiara proszona jest o spełnienie prośby, która jest wygórowana w stosunku do tej właściwej. Taki zabieg sprawia, że osoba ulegająca socjotechnikowi nie chce odmawiać kolejny raz, podając te dane, które faktycznie są mu potrzebne.

Zjawisko socjotechniki jest szczególnie groźne w dzisiejszych czasach, bowiem obecnie bardzo łatwo poprzez czaty, komunikatory czy fora internetowe nawiązać znajomość z obcymi dla nas osobami. Poznając kogoś przez sieć należy zachować ostrożność i nigdy nie odpowiadać na pytania będące z pozoru niegroźne, dotyczące banku w jakim mamy konto czy też stosowanych przezeń metod uwierzytelniania, np. kody jednorazowe na karcie lub przez token.

Phishing

Jedną z najczęściej stosowanych metod ataku na banki jest phishing. Phishing to zwrot wskazujący na łowienie (*fishing*), lecz zapisany w anglojęzycznej „gwarze" internetowej, gdzie literę F zapisuje się często jako PH. Metoda ta ma faktycznie wiele wspólnego z łowieniem. Atakujący wysyła najpierw masowo maile skierowane do konkretnej grupy osób. Wiadomość zazwyczaj graficznie prezentuje się tak, jakby została nadana przez daną instytucję (np. bank). Posiada treść skierowaną do klienta, grafika przypomina tę ze strony banku. W wiadomości takiej znajduje się także link, będący kluczem do sukcesu atakującego i do porażki ofiary. Link do witryny banku może nie wzbudzać podejrzeń, jednak po szczegółowym przyjrzeniu się mu widać, że nie prowadzi do witryny banku, który rzekomo ją wysłał, lecz zupełnie gdzieś indziej. Po kliknięciu zostajemy przekierowani na fałszywą witrynę lub pobrany zostaje trojan modyfikujący DNS lub plik hosts. Witryna przypomina zawsze prawdziwą stronę banku, gdzie możemy się zalogować. Różnica jest taka, że wszystko co wpisujemy, wysyłane jest do cyberprzestępcy. Aby lepiej zobrazować tę metodę, posłużę się przykładem wcześniej wspomnianego banku BZ WBK.

Początkowo, w marcu 2008 r., rozsyłane były wiadomości mające znamiona phishingu, na które mało kto dałby się nabrać z kilku prostych powodów. Jak widać poniżej – strona była przygotowana niedbale od strony graficznej, a do tego w języku angielskim. Pomijając fakt, że ktoś mógł najzwyczajniej w świecie nie znać angielskiego, to raczej każdemu wyda się podejrzane, że bank na terenie Polski pisze do polskich klientów wiadomości w obcym języku.

Przykład phishingu

Atak ten nie wywołał większego zamieszania wśród użytkowników banku. Niestety, niebawem w sieci zaczęła pojawiać się kolejna wiadomość, tym razem przygotowana bardziej starannie. Była napisana po polsku, grafika bardziej przypominała autentyczną wiadomość od banku, a link nie rzucał się w oczy jako fałszywy.

Na obrazku (strona 54) widać bardzo dobrze to, o czym wspominałem wcześniej. Widoczny link o treści „Kliknij tutaj, aby uaktywnić konto" to w rzeczywistości odsyłacz, którego prawdziwy adres widzimy w czerwonej ramce. Nie ma on nic wspólnego z bankiem. Po kliknięciu odnośnika użytkownik zostaje przekierowany na poniższą stronę, która

Przykład phishingu

okazuje się formularzem. Jego wypełnienie i wysłanie pozwoliłoby atakującemu na uzyskanie cennych informacji, które mogłyby posłużyć do włamania na konto.

Przykład phishingu

Phishing jest pewną formą socjotechniki, ponieważ zachęca użytkownika (pod pretekstem blokady konta lub nieprawidłowych operacji) do kliknięcia odnośnika i wypełnienia formularza/podania kodów jednorazowych czy numeru karty kredytowej (bywają i takie wiadomości phishingowe). Najważniejsze jest uświadomienie sobie, że banki nigdy nie wysyłają tego typu próśb drogą elektroniczną. Nigdy nie proszą o podanie maila, daty urodzenia, hasła czy loginu. Nie proszą też o kody jednorazowe.

Jedyne maile, jakie można otrzymać od banku, to oferta handlowa, ewentualnie wyciąg z naszego konta.

Inne wyjście?

Istnieją systemy, które znacząco zwiększają bezpieczeństwo naszych oszczędności. W przypadku zagranicznych sklepów internetowych typowym rozwiązaniem jest dokonywanie płatności przez specjalny system, na przykład PayPal. Jest to akceptowany na całym świecie system płatności, który ma za zadanie zwiększyć bezpieczeństwo prowadzenia zakupów online. Pieniądze mogą być wysłane do osoby, która posiada konto w PayPal. System ten oferuje wyjątkowo wysokie standardy bezpieczeństwa.

- Wszystkie transakcje monitorowane są przez 7 dni w tygodniu 24 godziny na dobę. Każda operacja jest sprawdzana w celu wykrycia nieprawidłowości i jak najszybszego podjęcia działań.
- Współpraca z organami bezpieczeństwa celem wyeliminowania fałszywych witryn oraz monitoring zapobiegający oszustwom na koncie i wykradaniu danych, czynią ten serwis wyjątkowo bezpiecznym.
- Niewątpliwie jedną z największych zalet jest możliwość korzystania z kardy kredytowej bez ujawniania jej numeru. Poufne dane nie muszą być przekazywane sprzedającemu.
- Użytkownik jest informowany o każdej nieprawidłowości wykrytej na jego koncie.

PayPal pośredniczy i obsługuje aukcje elektroniczne (np. eBay). Do niedawna, mimo obecności tego systemu w Polsce, jego użytkownicy nie mogli wykonywać transakcji innych niż wpłata pieniędzy innym użytkownikom. Obecnie możliwa jest również wypłata środków zgromadzonych na koncie, dzięki czemu PayPal zyskuje coraz większą popularność w naszym kraju. Warto się więc zastanowić nad korzystaniem z tego typu usług, zwłaszcza jeżeli robimy często zakupy w sieci, a w szczególności w sklepach zagranicznych.

Alternatywą dla wspomnianej wyżej usługi może być system Epassporte. Działa on na zasadzie wirtualnej karty, na której lokujemy pieniądze i możemy z nich skorzystać podczas zakupów w sklepach obsługujących kartę Visa.

System ten można porównać do telefonu na kartę – możemy w każdej chwili doładować konto i natychmiast korzystać z naszych środków. W tym przypadku pieniądze są przelewane na wirtualną kartę, przy użyciu której możemy dokonywać płatności w sieci, a także wypłacać pieniądze w różnych krajach. Jest to o tyle bezpieczne, że do dyspozycji są jedynie środki wpłacone na wirtualną kartę, jeżeli zaś chodzi o zabezpieczenia, to są podobne do tych stosowanych w systemie PayPal. Tutaj także mamy monitorowane podejrzane działalności czy ochronę poufnych danych.

Jeszcze jednym pomysłem na zwiększenie bezpieczeństwa zakupów online jest założenie subkonta w ramach naszego głównego konta bankowego. Możliwość taką oferują praktycznie wszystkie banki. Mechanizm działa następująco:

- Zakładamy subkonto i zamawiamy dla niego oddzielną kartę płatniczą. Subkonto oraz zamówio-

na dla niego karta będą nam służyć wyłącznie do zakupów internetowych.

- Bezpośrednio przed dokonaniem zakupu online zasilamy subkonto wymaganą kwotą (jeżeli dokonujemy zakupu w zagranicznym sklepie, warto zasilić subkonto kwotą nieco większą niż wymagana, aby nie okazało się, że po przeliczeniu walut środki okażą się niewystarczające).

- Po dokonaniu płatności przelewamy pozostałe środki na nasze główne lub inne konto.

Dzięki takiemu prostemu mechanizmowi nie musimy się obawiać, że numer karty zamówionej dla subkonta zostanie przechwycony. Nawet jeżeli tak się stanie, cyberprzestępca nie będzie miał dostępu do naszych pieniędzy, ponieważ znajdują się one na subkoncie tylko przez krótką chwilę.

Jak kupować, to z głową...

Na koniec chciałbym przytoczyć kilka zasad bezpiecznego kupowania w sieci:

- Loginy i hasła do konta bankowego powinny być trudne do odgadnięcia.

- Korzystając z bankowości internetowej, należy pamiętać o przestrzeganiu zasad bezpieczeństwa, a także stosowaniu się do zaleceń banku w kwestii logowania.

- Przed zalogowaniem się do banku należy sprawdzić autentyczność strony.

- Kupujmy tylko w dużych i znanych sklepach, które są już na rynku dostatecznie długo i istnieje możliwość bezproblemowego skontaktowania się z nimi – najlepiej telefonicznie, a nawet osobiście.

- W razie potrzeby dokonania zakupu w nieznanym nam sklepie poszukajmy w Sieci opinii o nim. Uważajmy w szczególności na firmy, które po sprzedaniu kilku artykułów znikają z rynku lub oferują markowe towary w podejrzanie atrakcyjnych cenach.

- Sprawdzajmy komentarze i aukcje, których dotyczą. Jeżeli ktoś sprzedaje drogi towar, a wcześniej handlował drobnymi przedmiotami, może to oznaczać próbę uprzedniego nabicia sobie pozytywnych komentarzy w celu wzbudzenia większego zaufania.

- Uważajmy na gorące i atrakcyjne oferty, oszuści często w ten sposób starają się zachęcić do brania udziału w ich aukcjach.

Przykładem takiej atrakcyjnej oferty kupna może być przypadek kupującego z Nigerii, który swego czasu osoby wystawiające aukcje internetowe napotykały bardzo często:

„Hi Seller, My name is Mrs faith eric from the Spain,i saw your item on the Auction,I am interested in buying the item from you,provided its in good working condition and quality am ready to add US$ 30.00 to the price listed so as to close the auction on the items which is needed urgentlly by a client of mine in Africa.Expecting your reply ASAP so as to proceed with the payment via Bidpay Auction Payments,Let me know if my offer is okay. Thanks Mrs Faith Eric".

Tłumaczenie:

„Drogi Sprzedawco. Nazywam się Faith Eric i jestem z Hiszpanii. Natknęłam się na Twoją aukcję i jestem zainteresowana zakupem, pod warunkiem że przedmiot jest w dobrym stanie i wysokiej jakości. Jestem w stanie zapłacić o 30 dolarów więcej niż oczekujesz, jeżeli zamkniesz aukcję przed czasem – mój klient z Afryki potrzebuje pilnie sprzedawanego przez Ciebie produktu. Oczekuję na jak najszybszą odpowiedź, po odebraniu której rozpocznę starania związane z płatnością za pośrednictwem Bidpay Auction Payments. Proszę o informację, czy moja oferta jest atrakcyjna. Dziękuję, Faith Eric".

Oczywiście, wszystko to okazywało się oszustwem. Ktoś pisał maile do osób wystawiających drogi sprzęt elektroniczny, np. telefony komórkowe i dawał bardzo korzystną cenę za towar. Było w tym wiele niejasności, ostatecznie jednak osoby, które zdecydowały się wysłać towar, nie otrzymały ani grosza. Dlatego należy podchodzić z rezerwą do takich ofert.

Podsumowując – jeżeli nie zadbamy o nasze pieniądze, ktoś „zrobi" to za nas...

Autor jest analitykiem Kaspersky Lab Polska

Ataki *drive-by download*

Rayan Naraine

Sieć w oblężeniu

Ewolucja sposobów rozprzestrzeniania się wirusów komputerowych i szkodliwego oprogramowania odzwierciedla ewolucję sposobów przesyłania informacji.

Na początku informacje były fizycznie przenoszone z jednego komputera na inny przy użyciu różnych przenośnych nośników danych. We wczesnych latach 80. ubiegłego wieku informacje „podróżowały" za pośrednictwem kosztownych prywatnych sieci danych. W wyniku nacisków amerykańskiego rządu na korporacyjnych dostawców, aby ujednolicili sposób wysyłania oraz format informacji, nastąpił prawdziwy rozkwit internetu. Firmy dowolnego rozmiaru uzyskały możliwość przesyłania informacji poprzez tę „darmową" sieć, najczęściej wykorzystując do tego celu wiadomości e-mail i załączniki do takich wiadomości. W późnych latach 90. te nowe możliwości zaczęły wykorzystywać wirusy, które atakowały zarówno firmy, jak i osoby fizyczne na całym świecie – szkodniki te wykorzystywały pocztę elektroniczną do rozmnażania i rozprzestrzeniania się.

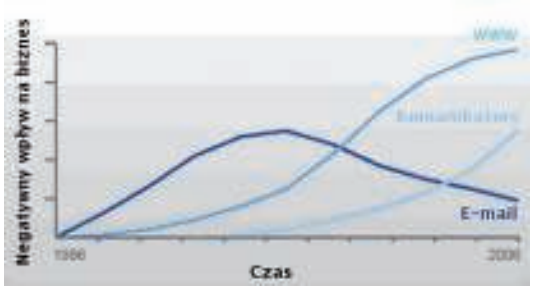
Sieć World Wide Web szybko przekształciła się w nieocenioną platformę służącą do wymiany informacji, ułatwiającą globalny handel i zwiększającą produktywność pracowników. Powoli, ale konsekwentnie, zaczęliśmy dostrzegać zalety podejścia polegającego na tym, że zamiast wysyłać informacje do wszystkich, którym mogą się przydać, wysyłane jest tylko powiadomienie zawierające odsyłacz pozwalający użytkownikom przeglądać konkretne informacje za pośrednictwem sieci. Dzisiaj wiele osób nadal uważa, że używanie przeglądarki internetowej to to samo co oglądanie wystaw sklepowych lub pójście do biblioteki w fizycznym świecie – bez wiedzy osoby zainteresowanej nic się nie może stać. W rzeczywistości umyka im wiele rzeczy, które dzieją się „za kulisami", ponieważ są one dla nich niewidoczne. Jednak większość użytkowników indywidualnych oraz ekspertów korporacyjnych (spoza branży IT) byłaby zaskoczona intensywnością tej „zakulisowej" komunikacji, zachodzącej podczas cichej interakcji przeglądarek internetowych z danymi przechowywanymi na komputerach PC, aplikacjami oraz serwerami sieciowymi.

Niestety, tę „złożoność" zaczęły wykorzystywać również dobrze zorganizowane grupy zajmujące się rozprzestrzenianiem szkodliwego oprogramowania, które obecnie dostarczają swoje wirusy, programy spyware, trojany, boty, rootkity oraz fałszywe programy bezpieczeństwa głównie za pośrednictwem sieci. W branży antywirusowej tego rodzaju ukryte pobieranie szkodliwych programów ze stron internetowych bez wiedzy użytkownika określa się terminem *drive-by download.* W artykule tym zbadamy, co w rzeczywistości ma miejsce podczas ataku „drive-by", jakie przynęty i technologię wykorzystuje się do przeprowadzania takich ataków oraz w jaki sposób wykorzystuje się te ataki do kradzieży danych osobowych oraz przejmowania kontroli nad komputerami.

Zrozumieć eksplozję

Zanim przeprowadzimy bardziej szczegółowe badanie ataków *drive-by download*, wyjaśnimy najpierw, w jaki sposób „eksplodował" ten rodzaj ataków w ostatnich latach. W tym miejscu warto pamiętać, że ten sam szkodliwy program (wirus, spyware, trojan, bot, rootkit oraz fałszywe oprogramowanie bezpieczeństwa) może być, i często jest, rozprzestrzeniany na wiele różnych sposobów – czasami za pośrednictwem poczty elektronicznej, czasami na skutek odwiedzenia strony internetowej, czasami przy użyciu innych metod.

Rozprzestrzenianie szkodliwych programów za pośrednictwem ataków „drive-by" staje się coraz popularniejsze wśród cyberprzestępców, ponieważ ten sposób infekcji jest bardziej ukradkowy i prowadzi do większej liczby skutecznych ataków. Rysunek 1 przedstawia dane pochodzące od ScanSafe, firmy śledzącej zagrożenia rozprzestrzeniające się za pośrednictwem sieci, i ilustruje, w jaki sposób w ciągu dekady, od 1996 roku, trend przesunął się z poczty elektronicznej na sieć oraz komunikatory internetowe.



Rys. 1. Ewolucja metod dostarczania szkodliwego oprogramowania

Według nowszych danych firmy ScanSafe, 74 procent wszystkich szkodliwych programów zidentyfikowanych w trzecim kwartale 2008 roku było wynikiem odwiedzenia zainfekowanych stron internetowych.

Teraz, gdy zwróciliśmy uwagę na coraz większą wagę tego problemu, wyjaśnimy, w jaki sposób przeprowadzane są tego rodzaju ataki, przedstawimy techniki wykorzystywane w celu zwabienia ofiar na zainfekowane strony internetowe, zaawansowane zestawy exploitów oraz atakowane przez nie aplikacje, skomplikowany labirynt przekierowań sieciowych oraz szkodliwe funkcje wykorzystywane do przeprowadzania kradzieży tożsamości oraz ataków polegających na przejmowaniu kontroli nad komputerami.

Ataki wykorzystujące przeglądarkę

Aby w pełni zrozumieć gwałtowny wzrost popularności wykorzystywania przeglądarki internetowej jako narzędzia ataków, należy przyjrzeć się historii największych ataków przeprowadzanych na komputery za pośrednictwem internetu. W „okresie robaków internetowych", gdy w sieciach korporacyjnych spustoszenie siały takie robaki, jak Code Red, Blaster, Slammer oraz Sasser, hakerzy wykorzystywali luki w systemie operacyjnym Windows przy użyciu zdalnych exploitów. (O zdalnym exploicie mówimy wtedy, gdy szkodliwy program znajduje się na serwerze podłączonym do sieci i wykorzystuje legalny kod na komputerze użytkownika, jednak w celu wykorzystania luki w zabezpieczeniach nie musi uzyskiwać dostępu do komputera użytkownika). Zainfekowane pliki wykonywalne, takie jak Melissa, często dołączane były do wiadomości e-mail lub przedostawały się do systemów za pośrednictwem komunikatorów internetowych i aplikacji P2P.

Microsoft zareagował na ataki robaków w pozytywny sposób. Firma dodała zaporę sieciową, która w systemie Windows XP SP2 jest domyślnie włączona, oraz zaimplementowała kilka mechanizmów osłabiających ataki robaków. Włączona funkcja automatycznych aktualizacji w systemie Windows pomagała użytkownikom regularnie instalować łaty dla systemu operacyjnego. Zmądrzały zarówno firmy, jak i użytkownicy, którzy zaczęli blokować załączniki i przestali klikać nietypowe pliki wykonywalne. Oba te czynniki skłoniły cyberprzestępców do zmiany taktyki: zaczęli atakować aplikacje innych producentów oraz doskonalić sztukę socjotechniki.

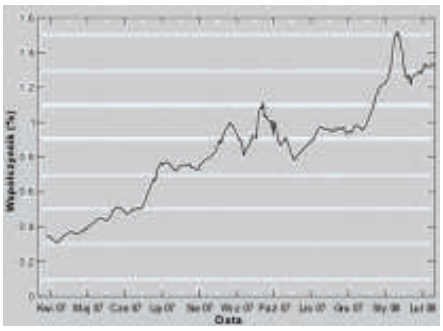
Ewolucja ta przyczyniła się również do wyłonienia się nowej techniki ukradkowych ataków określanych jako *drive-by download*. Opierają się one na wykorzystywaniu przeglądarki jako mechanizmu, za pomocą którego użytkownicy komputerów łączą się z serwerami, na których umieszczono exploity. W ataku „drive-by" szkodliwy program jest automatycznie pobierany na komputer użytkownika bez jego wiedzy oraz zgody. Atak odbywa się w dwóch etapach. Użytkownik odwiedza stronę internetową zawierającą szkodliwy kod, który przekierowuje to połączenie na zainfekowany serwer należący do osoby trzeciej i zawierający exploity. Rysunek 2, od Google Anti-Malware Team, pokazuje podstawowy schemat ataku *drive-by download*. Exploity te mogą wykorzystywać luki w zabezpieczeniach przeglądarki internetowej, niezałatane wtyczki do przeglądarki, podatne na ataki formanty ActiveX oraz błędy w oprogramowaniu innych producentów.

Jak widać na rysunku, zanim zostanie pobrany exploit, może nastąpić dowolna liczba przekierowań na różne strony internetowe.

Według danych Kaspersky Lab, jak również innych firm z branży bezpieczeństwa, jesteśmy w środku epidemii ataków *drive-by download*. Przez ostatnie dziesięć miesięcy grupa Google Anti-Malware Team odwiedziła miliardy stron internetowych w poszukiwaniu aktywności szkodliwego oprogramowania, znajdując ponad trzy miliony adresów URL, z których inicjowane były ataki *drive-by download*.

„Jeszcze bardziej niepokojącym odkryciem było to, że około 1,3 procent zapytań w wyszukiwarce Google zwróciło co najmniej jeden adres URL oznaczony na stronie wyników jako zainfekowany" – wynika z badania opublikowanego przez Google. Rysunek 3, pochodzący z badania, pokazuje niepokojący wzrost odsetka wyszukiwań, których wyniki zawierały zainfekowane strony.

Rys. 2. Struktura ataku drive-by download



Rys. 3. Wyniki wyszukiwania zawierające adresy zainfekowanych stron

W początkowym okresie przeprowadzania ataków *drive-by download* cyberprzestępcy zwykle tworzyli zainfekowane strony internetowe i wykorzystywali socjotechnikę w celu przyciągnięcia na nie użytkowników. Chociaż nadal jest to główne źródło szkodliwej aktywności online, ostatnio hakerzy częściej włamują się na legalne strony internetowe i ukradkiem wykorzystują skrypt lub umieszczają kod przekierowujący, który niezauważenie uruchamia ataki za pośrednictwem przeglądarki.

Anatomia ataku *drive-by*

Na początek pokażmy, w jaki sposób przeprowadzane są ataki *drive-by download* na komputery użytkowników. Jako przykładu użyjemy jednego z głośnych incydentów, którego ofiarą w 2007 roku padł znany portal internetowy. W tygodniach poprzedzających finałową rozgrywkę o mistrzostwo amerykańskiej zawodowej ligi hakerzy włamali się na stronę stadionu Miami's Dolphin Stadium, umieszczając na niej fragment kodu JavaScript (zobacz rysunek 4).

Osoba posiadająca komputer z niezałatanym systemem Windows, która odwiedziła tę stronę, została ukradkiem połączona ze zdalnym użytkownikiem,

Rys. 4. Kod JavaScript użyty na stronie stadionu Miami's Dolphin Stadium

➢ który próbował wykorzystywać znane luki w zabezpieczeniach opisane w biuletynach bezpieczeństwa firmy Microsoft (MS06-014 oraz MS07-004). Jeżeli exploit okazał się skuteczny, na komputer instalował się niepostrzeżenie trojan, który umożliwiał osobie atakującej pełny dostęp do atakowanego komputera. Taki komputer mógł zostać następnie wykorzystany do kradzieży poufnych informacji lub przeprowadzenia ataków DoS.

W tym samym roku hakerzy porwali posiadającą dużą odwiedzalność stronę internetową Banku Indii. Hakerzy przeprowadzili wyrafinowany atak wykorzystujący wielokrotne przekierowania, w wyniku których użytkownicy systemu Windows wysyłani byli na serwer, na którym został umieszczony plik robaka pocztowego, dwa rootkity, dwa trojany downloadery oraz trzy backdoory. Atak na stronę Banku Indii łączył zaciemniane za pomocą JavaScript liczne przekierowania przy użyciu ramki iFrame oraz techniki fast-flux[1]. Rysunek 5 pokazuje zrzut ekranu zhakowanej strony Banku Indii zawierającej szkodliwy skrypt wykorzystywany do przeprowadzania ataku *drive-by download*.

Rys. 5. Szkodliwy skrypt na stronie Bank of India

Opisane wyżej przykłady ataków pokazują skalę problemu, jaki dotyka legalne strony internetowe. Śledząc zagrożenia wykorzystujące sieć, firma ScanSafe ustaliła, że do połowy 2008 roku większość szkodliwych programów została wykryta na legalnych stronach. Raport firmy ScanSafe za trzeci kwartał 2008 roku zawiera kilka interesujących faktów:

- W trzecim kwartale 2008 roku liczba szkodliwego oprogramowania wykorzystującego sieć wzrosła o 338 proc. w porównaniu z pierwszym kwartałem 2008 r. oraz o 553 proc. w porównaniu z czwartym kwartałem 2007 r.
- Około 31 procent wszystkich zagrożeń we wrześniu 2008 roku stanowiły zagrożenia zero-day (zagrożenie zero-day to takie, dla którego nie istnieje żadna łata).
- Ryzyko ze strony backdoorów i trojanów kradnących hasła wzrosło we wrześniu 2008 roku o 267 proc. w porównaniu ze styczniem 2008 roku.

Osoby atakujące wykorzystywały również „zatrute" serwery reklamowe osób trzecich w celu przekierowywania użytkowników systemu Windows na oszukańcze serwery, na których umieszczany był kod wykorzystywany do przeprowadzania ataków *drive-by download*. Te zainfekowane reklamy (*malvertisement*) zwykle tworzone są we Flashu i wykorzystują niezałatane aplikacje.

Zestawy exploitów

Zestawy szkodliwych exploitów stanowią motor ataków *drive-by download*. Zestawy te to profesjonalnie tworzone komponenty oprogramowania, które mogą być umieszczone na serwerze. Są sprzedawane na stronach hakerskich i zawierają exploity dla luk w zabezpieczeniach różnych popularnych aplikacji dla komputerów, takich jak Quick-Time firmy Apple, programy Adobe Flash Player, Adobe Reader, RealPlayer firmy RealNetworks oraz WinZip.

Wykorzystywane były również exploity dla konkretnych przeglądarek, takich jak Internet Explorer, Firefox, Safari oraz Opera. Kilka zestawów exploitów zwierało jedynie kod umożliwiający ataki wykorzystujące luki w zabezpieczeniach Adobe PDF lub znane błędy w formantach ActiveX.

Złodzieje tożsamości oraz inni twórcy szkodliwego oprogramowania kupują zestawy exploitów i umieszczają je na zainfekowanym serwerze. Następnie w stronach internetowych osadzany jest kod przekierowujący ruch na ten serwer. Użytkowników zachęca się do odwiedzenia takich stron za pomocą spamu rozprzestrzenianego za pośrednictwem poczty elektronicznej lub forów.

Serwer zawierający zestaw exploitów może wykorzystywać nagłówki żądania HTTP z odwiedzin strony za pomocą przeglądarki do określenia typu oraz wersji przeglądarki odwiedzającego, jak również jego systemu operacyjnego. Po zidentyfikowaniu systemu operacyjnego zestaw exploitów może zdecydować, które exploity należy uruchomić.

[1] Zaciemnianie za pomocą JavaScript – aby uniknąć wykrycia przez narzędzia służące do zapewnienia bezpieczeństwa, autorzy szkodliwego oprogramowania wykorzystują tę technikę w celu utrudnienia odszyfrowania szkodliwego kodu
* przekierowania przy użyciu ramki iFrame – ramka iFrame to element HTML-a , który pozwala webmasterowi osadzić dokument w HTML-u w istniejącym dokumencie. Autorzy szkodliwego oprogramowania wykorzystują tę technikę do osadzania kodu przekierowującego ofiary na zainfekowane serwery.
* Fast-flux – jest to technika DNS wykorzystywana przez botnety w celu ukrycia stron, poprzez które rozprzestrzeniane są ataki phishingowe oraz szkodliwego oprogramowania przy pomocy ciągle zmieniającej się sieci zainfekowanych hostów.

Exploit	Microsoft Bulletin (jeżeli istnieje)
MDAC remote code execution	MS06-014
ShockwaveFlash.ShockwaveFlash.9 exploit	
WebViewFolderIcon setSlice() exploit	MS06-057
Msdds.dll exploit	MS05-052
Microsoft Works exploit	MS08-052
Creative Software AutoUpdate Engine exploit	
Online Media Technologies NCTsoft NCTAudioFile2 ActiveX buffer overflow	
Ourgame GLWorld GLIEDown2.dll exploit	
DirectAnimation.PathControl buffer overflow	MS06-067

W niektórych przypadkach wysyłanych jest jednocześnie kilka exploitów, które próbują atakować maszynę poprzez luki w zabezpieczeniach aplikacji innych producentów. Niektóre z bardziej wyrafinowanych zestawów exploitów są utrzymywane i aktualizowane o nowe exploity co miesiąc. Zestawy zawierają interfejs, w którym przechowywane są szczegółowe dane dotyczące udanych ataków. Dane te obejmują takie informacje, jak wersje wykorzystanych systemów operacyjnych, państwo, w jakim znajdował się cel ataku, które z exploitów zostały wykorzystane oraz efektywność exploitów na podstawie ruchu do zainfekowanej strony.

Powyższa tabela pokazuje różne exploity znajdujące się w jednym zestawie exploitów przechwyconym podczas ataku polegającego na przekierowywaniu z wykorzystaniem JavaScript. Przykład ten pokazuje nie tylko popularność exploitów w oprogramowaniu firmy Microsoft, ale również jednoczesne wykorzystywanie innych programów w celu potencjalnego zwiększenia wartości zestawu exploitów dla cyberprzestępców.

Niezałatana monokultura

Epidemia ataków *drive-by download* w dużej mierze spowodowana jest tym, że użytkownicy nie łatają systemów Windows. Z nielicznymi wyjątkami krążące obecnie exploity wykorzystują znane luki w zabezpieczeniach oprogramowania – takie, dla których dostępne są łaty. Z różnych powodów użytkownicy końcowi nie spieszą się z instalowaniem niezbędnych poprawek dla oprogramowania.

Mechanizm Automatycznych Aktualizacji Microsoftu oferuje użytkownikom końcowym wygodny sposób łatania luk w zabezpieczeniach systemu operacyjnego. Niestety, nie można powiedzieć tego samego o aplikacjach innych producentów. Secunia, firma zajmująca się wyszukiwaniem luk w zabezpieczeniach oprogramowania, szacuje, że prawie jedna trzecia wszystkich aplikacji zainstalowanych na komputerach jest podatna na znane ataki (wykorzystujące luki, które zostały już załatane).

Przyglądając się istniejącym zestawom exploitów, możemy dostrzec kilka starych luk w zabezpieczeniach, takich jak MS06-014 oraz MS05-052, które istnieją jeszcze wiele lat po tym, jak udostępniono dla nich łaty (trzeci i czwarty znak wskazuje rok publikacji biuletynu). Pakiety exploitów wykorzystujących wyłącznie błędy w programie Adobe PDF Reader okazały się niezwykle skuteczne mimo usprawnień procesu reagowania przez firmę Adobe na kwestie związane z bezpieczeństwem. Innym popularnym celem exploitów jest program Flash Player, który – zainstalowany na komputerach podłączonych do internetu – w niemal 100 proc. pada ofiarą ataków, podobnie jak RealPlayer firmy RealNetworks.

Wnioski: Jak uniknąć ataków

Na koniec warto zauważyć, że większość współczesnych przeglądarek internetowych, takich jak Internet Explorer, Firefox oraz Opera, zawiera mechanizmy blokujące szkodliwe programy, zapewniające systemy wczesnego ostrzegania, które alarmują użytkowników w momencie, gdy próbują odwiedzić zainfekowaną stronę internetową. Chociaż mechanizmy te cechują się niezłą skutecznością, opierają się na czarnej liście, w związku z tym nie zapewniają 100 proc. ochrony osobom surfującym po internecie.

Najpraktyczniejsze podejście do ochrony przed atakami *drive-by download* polega na zwróceniu szczególnej uwagi na zarządzanie łatami. W szczególności użytkownicy powinni:

- Wykorzystywać rozwiązanie do zarządzania łatami, które pomaga znaleźć – i naprawić – wszystkie pochodzące od innych producentów aplikacje zainstalowane na komputerach. Secunia oferuje dwa takie narzędzia – Personal Software Inspector oraz Network Security Inspector. Mogą one pomóc zidentyfikować niezałatane aplikacje.
- Wykorzystywać przeglądarkę zwierającą mechanizmy blokowania ataków phishingowych oraz szkodliwego oprogramowania. Zarówno Internet Explorer, Mozilla Firefox, jak i Opera posiadają funkcje blokowania zainfekowanych stron.
- Włączyć zaporę sieciową i instalować wszystkie aktualizacje dla systemu operacyjnego Microsoftu. Unikać wykorzystywania pirackiego oprogramowania.
- Zainstalować oprogramowanie do ochrony przed wirusami i innymi szkodliwymi programami i dopilnować, aby jego bazy były zawsze aktualne. Upewnić się, czy ich dostawcy rozwiązań bezpieczeństwa wykorzystują skaner ruchu internetowego, który może pomóc zidentyfikować potencjalne problemy związane z atakami *drive-by download.*

Działania te, mające na celu zarządzanie lukami w zabezpieczeniach, stanowią najlepszą ochronę przed atakami *drive-by download*.

Autor jest ekspertem ds. bezpieczeństwa w firmie Kaspersky Lab

Widoczność, koordynacja i kontrola przy niskim koszcie całkowitym

Gilles Trachsel

Adaptacyjne zwalczanie zagrożeń

Jeszcze nie tak dawno temu robak czy wirus w sieci firmowej oznaczał zarwaną noc administratora systemów przeszukującego logi grodzi ogniowej czy systemu wykrywania włamań w poszukiwaniu problemu i sposobu opanowania zagrożenia.

Było to pracochłonne i niezbyt sprawne rozwiązanie w wypadku prostszych zagrożeń spotykanych w przeszłości. Niestety, wielu współczesnych najniebezpieczniejszych zagrożeń nie daje się wykryć indywidualnymi mechanizmami ochronnymi, nawet pod czujnym nadzorem administratorów, ponieważ:

- złożone wielopłaszczyznowe ataki mogą przemycać się poniżej progów reagowania pojedynczych mechanizmów ochronnych;
- personel może sobie nie radzić z szybkością i rozległością ataków – a nowe ataki pojawiają się szybciej, niż administratorzy są w stanie zdobywać o nich wiedzę;
- ataki mają miejsce tam i wtedy, gdy administratorzy nie są dostępni – w oddalonych biurach lub podczas awarii dotyczących całej okolicy;
- jednym ze źródeł najgroźniejszych i najkosztowniejszych ataków bywają czasem sami niezadowoleni lub przekupieni administratorzy.

Kluczem do zwalczania takich zagrożeń przedsiębiorstw jest podejście kompleksowe z automatyczną korelacją pracy wielu mechanizmów zabezpieczających. Po latach inwestowania sieci są wyposażone w bardzo rozbudowane, ale autonomiczne rozwiązania ochronne. Problem w tym, że są to rozwiązania specjalizowane i działające niejako w próżni. Rozwiązania współczesne posuwają rozpoznanie, eliminację i raportowanie zagrożeń o krok dalej poprzez koordynację ochrony sieci na poziomie wielu urządzeń znajdujących się w jej infrastrukturze i dostosowywanie się do zagrożeń zmiennych. Dzięki takim nowym rozwiązaniom adaptacyjnym oszczędza się czas i pieniądze, można utrzymać zgodność z przepisami regulującymi kwestie systemów opieki zdrowotnej, bankowe, obrót papierami wartościowymi, ochronę poufności, itd., jednocześnie upraszczając procesy dokumentowania zagrożeń i sprawozdawczości.

Adaptacyjne zwalczanie zagrożeń

Adaptacyjne zwalczanie zagrożeń (*Adaptive threat management – AdTM*) to rozwiązania tworzące system współpracujący dynamicznie, który zapewnia wgląd w całą sieć i dostosowuje swoje działanie do zmieniających się zagrożeń i ryzyka. Takie rozwiązania nazywamy adaptacyjnymi, ponieważ zmieniają one profil ochrony sieci w odpowiedzi na rodzaje i stopień zagrożeń, na przykład poddając kwarantannie podejrzany komputer, użytkownika, czy segment sieci, gromadzą dodatkowe informacje podczas próby włamania, czy też w czasie ataku na sieć dławią przepustowość przydzieloną określonym aplikacjom.

W skład AdTM wchodzą takie elementy zabezpieczające, jak grodzie ogniowe/VPN w kluczowych bramach sieciowych, urządzenia wykrywające i uniemożliwiające włamania (IDP), blokujące ataki na sieć i aplikacje oraz mechanizmy kontroli dostępu, wymuszające przestrzeganie polityk bezpieczeństwa w funkcji tożsamości użytkowników.

Działając w ścisłej koordynacji takie otwarte platformy rozwiązań:

- korelują informacje przychodzące z różnych systemów ochronnych, by wykrywać zagrożenia, których pojedyncze urządzenia nie wykryją i nie zasygnalizują;
- wykrywają skomplikowane i zamaskowane ataki, które pokonują klasyczne mechanizmy zabezpieczeń;
- reagują przeciwdziałaniem ograniczającym skuteczność ataku, jednocześnie informując o nim administratorów i gromadząc bardzo szczegółowe informacje o ataku, zgodnie z wytycznymi polityk bezpieczeństwa;
- zarządzają i egzekwują przestrzeganiem polityk bezpieczeństwa, w tym sterują stosowaniem i aktualizacją ochronnego oprogramowania klienckiego, podpisami, politykami i społecznościami użytkowników w wypadku ich nowych lub powracających członków;
- dokumentują i przekazują informacje potrzebne do weryfikacji zgodności działań z prawem oraz dochodzeń kryminalnych, poczynając od związanych z działaniem polityk, do informacji o zdarzeniach w skali sieci całego przedsiębiorstwa.

Warto zastanowić się nad opcjami

Większość współczesnych organizacji wdrożyła wiele zabezpieczeń, zarówno programowych, jak i sprzętowych.

Rozwiązania „punktowe”

Atutem rozwiązań „punktowych” jest ich zdolność do rozwiązywania konkretnego problemu. Ale ten atut jest zarazem ich piętą achillesową. Nastawione na konkretne zagrożenia, są całkowicie krótkowzroczne i nie widzą szerszego kontekstu sytuacji. Tego rodzaju rozwiązania punktowe oferują najczęściej nowo powstające firmy, dlatego należy się zastanowić nad ich skalowalnością, niezawodnością i długofalowym wsparciem decydującym o użyteczności.

Rozwiązania nieznormalizowane

Rozwiązania sprzętowe z nieznormalizowanymi architekturami są kupowane w przekonaniu, że elementy pochodzące od jednego producenta będą ze sobą gładko współpracowały i zapewnią ciągłość ochrony sieci. Ale nawet w wypadku jednego producenta integracja może być płytka, a nawet

żadna. Wiele tak zwanych „suit" składa się z elementów kiedyś opracowanych przez różne firmy, potem kupionych przez obecnego dostawcę, więc jedyne co je łączy, to nowa marka. A nieoptymalna integracja czy stosowanie różnych systemów operacyjnych może prowadzić do drastycznego spadku parametrów sieci, a nawet wprowadzać do niej słabe punkty.

Po stronie ekonomicznej doskonale są znane koszty i ryzyko przywiązania się do jednego dostawcy, dlatego twierdzenia producentów na temat interoperacyjności i kompleksowości ich produktów należy dobrze przeanalizować przed decyzją o zastosowaniu nieznormalizowanej architektury systemu zabezpieczeń. Prawdziwie oparte na rozwiązaniach podejście wymaga swobody stosowania przez firmę rozwiązania bez ograniczenia się do jednego dostawcy, a także działającego na jednym systemie operacyjnym. To minimalizuje i optymalizuje koszty zakupu oraz późniejsze ciągłe koszty eksploatacji.

Elastyczność i swoboda wyboru dzięki zabezpieczeniom zaawansowanym

Rozwiązania AdTM oparte na platformie otwartej zapewniają ogromną elastyczność i swobodę wdrażania zabezpieczeń, jednocześnie ograniczając całkowite koszty udostępniania bezpiecznych aplikacji i usług.

Rozwiązania oparte na platformie otwartej integrują i koordynują elementy infrastruktury sieciowej i ochronnej ograniczając zagrożenia, z którymi nie poradziłyby sobie indywidualne produkty działające samodzielnie:

- nowe zagrożenia – wykrywanie zdarzeń wskazujących na ataki, nawet jeżeli jeszcze nie opublikowano ich definicji i sygnatur;
- kompleksowe ataki wielodrożne – korelacja pracy wielu urządzeń zabezpieczających umożliwia wykrywanie zagrożeń nawet wtedy, gdy w poszczególnych urządzeniach nie przekraczają one progów alarmowania;
- ataki uprawnionych użytkowników wewnętrznych – integracja z mechanizmami kontroli dostępu wykrywająca próby naruszenia integralności sieci.

Rozwiązania AdTM oferują szerokie możliwości reagowania w czasie rzeczywistym, w tym na przykład natychmiastową kwarantannę zagrożenia, alarmowanie personelu ochrony sieci, odcięcie niebezpiecznego zakończenia sieci czy ograniczenie pasma przesyłowego w niebezpiecznym zakończeniu lub segmencie sieci. Niezależnie od tego, czy skonfiguruje się je na podejmowanie działań automatycznie, półautomatycznie czy ręcznie, rozwiązania AdTM dostosowują się w czasie rzeczywistym, tak by chronić bezpieczeństwo całej sieci przy ustawicznie zmieniającym się krajobrazie zagrożeń. Tak inteligentna współpraca poprawia zakres, skalę i sprawność zarządzania ochroną, uwalniając od tych zadań specjalistyczny personel, który może się zajmować sprawami ochrony naprawdę wymagającymi jego wysokich kwalifikacji.

Specjaliści do spraw zabezpieczeń sieci firmowych powinni przy ocenie rozwiązań AdTM dla swoich sieci uwzględniać następujące kryteria:

- Możliwość pełnej integracji zabezpieczeń – obejmującej grodzie ogniowe/VPN, mechanizmy wykrywania i zapobiegania włamaniom, kontroli dostępu do sieci (NAC) oraz szkieletową architekturę rutingową. Rozwiązania powinny dobrze współpracować z oprogramowaniem antywirusowym i antyspamowym, sprzętowymi systemami zabezpieczającymi i istniejącą infrastrukturą sieci;
- Możliwość szczegółowego sterowania działaniem systemu w oparciu o polityki – rozwiązania do zarządzania siecią i jej ochrony powinny wymuszać kontrolę dostępu z rozdzielczością do pojedynczych użytkowników i ich grup;
- Automatyczne wdrażanie z możliwością klonowania i dostosowywania polityk do różnych rodzajów urządzeń podnosi zarówno bezpieczeństwo, jak i zgodność prawną, szczególnie w dużych rozproszonych organizacjach;
- Zarządzanie reakcjami – AdTM wymaga, aby rozwiązania dostosowywały profil ochrony sieci do zmian w krajobrazie zagrożeń – zwiększały ochronę dostępu, izolowały segmenty sieci, zmieniały uprawnienia, aktualizowały definicje i sygnatury oraz podejmowały inne działania dyktowane polityką bezpieczeństwa. Dla szybkich sukcesów krytyczna jest dostępność ustawień domyślnych i narzędzi upraszczających czynności administracyjne;
- Monitoring, sprawozdawczość i kontrola – długofalowa ochrona sieci wymaga, aby specjaliści od jej ochrony mieli dostęp do danych pochodzących z wielu źródeł, co umożliwia tworzenie polityk optymalizujących ochronę i wydajność sieci. Szczegółowe sprawozdania i narzędzia audytorskie pomagają w działaniach na rzecz długofalowego utrzymania bezpieczeństwa sieci, zgodności z politykami i sprawności;
- Kompromisy między wydajnością a bezpieczeństwem – bezpieczeństwo nie powinno być zapewniane kosztem wydajności. Należy wystrzegać się kompromisów takich, jak analiza stanów w grodziach ogniowych zwiększająca prawdopodobieństwo spadku wydajności sieci w miarę „załączania" kolejnych mechanizmów ochronnych. Dokładne rozważenie przyszłych potrzeb biznesowych i uważna analiza podejścia producenta do kompromisów między bezpieczeństwem a wydajnością pomoże się ustrzec ślepych uliczek czy rozwiązań stwarzających problemy z wydajnością;
- Skalowalność – rozwiązania zabezpieczające powinny być skalowalne w ślad za przyszłym rozrostem i zmianami sieci. Skalowalność możliwa jest po części dzięki dobremu zaprojektowaniu sieci, a po części dzięki elementom infrastruktury sieciowej zapewniającym nowe możliwości bez zbędnych dodatkowych instancji systemów operacyjnych, warstw sieciowych czy nieoptymalnych przepływów pakietów.

Podsumowanie

Podejście oparte na rozwiązaniach stanowi kwantowy skok w przyszłość w walce o utrzymanie bezpieczeństwa organizacji i zapewnia swobodę wyboru. AdTM zwiastuje koniec wdrażania zabezpieczeń systemów informatycznych „po kawałku". Dzięki korelowaniu informacji pochodzących z licznych systemów ochronnych, koordynowaniu ich reakcji na ataki i konsolidowaniu informacji w celu zapewnienia zarówno doraźnej, jak i długofalowej adaptacji do zmiennego krajobrazu zagrożeń, systemy AdTM ogromnie podnoszą poziom bezpieczeństwa przy racjonalnych kosztach działania. Dokładna ocena technik alternatywnych i uważna analiza wyważenia zabezpieczeń i wydajności sieci pozwoli firmom najlepiej wykorzystać posiadane sieci, budżety oraz czas i umiejętności personelu.

Autor jest
Enterprise Marketing Solutions Manager, EMEA,
Juniper Networks

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**.

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 Zabłudowski (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

INFOTEL 1997

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.

12 lat doświadczenia

- prestiżowa nagroda w konkursie o Laur INFOTELA

- kongresy

- fora ekspertów

- debaty

- konferencje

- serwisy internetowe

- publikacje drukowane

o nowoczesnej komunikacji elektronicznej wiemy wszystko

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

Wszechstronna pomoc związana z siecią **od koncepcji do realizacji**

Czy określają Państwo dopiero swoje wymagania? A może wdrażają już Państwo nową infrastrukturę sieciową? Pomoc możemy okazać na każdym etapie projektu.

Dysponujemy wysokiej jakości procesami produkcyjnymi, globalną siecią profesjonalnych, wyszkolonych instalatorów oraz wyspecjalizowanym personelem technicznym i obsługi klientów. Oferowanie Państwu pomocy jest naszym celem.

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

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

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

molex®
one company › a world of innovation

www.molexpn.com.pl