MSG MEDIA

ISSN 1429-0200

4/2010

INDEKS 345237

INFOTEL

Cena 15 zł
(w tym 0% VAT)

kwartalnik – PAŹDZIERNIK/GRUDZIEŃ NOWOCZESNA KOMUNIKACJA ELEKTRONICZNA

TELEKOMUNIKACJA • INFORMATYKA • TELEWIZJA • INTERNET

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. Chwytowo 2, 85-223 Bydgoszcz; tel. (52) 325 83 10; fax (52) 3737 52 43
e-mail: office@msgmedia.pl; www.techbox.pl

INFOTEL 1997
KWARTALNIK NOWOCZESNA KOMUNIKACJA ELEKTRONICZNA

INDEKS 345237
numer 4 (108), rok dziesiąty
październik/grudzień 2010
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. Chwytowo 2, 85-223 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. 696 07 75 63
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: MULTIGRAF, R. Ellert, J. Tomczuk
ul. Bielicka 76C; 85-135 Bydgoszcz
tel./fax: (052) 340-41-37
e-mail: biuro@multigrafdruk.pl
www.multigrafdruk.pl

SPIS TREŚCI

Telekomunikacja

INEA i ASTA-NET partnerami WSS

Spółki INEA SA i ASTA-NET Maładziński, Ryczek sp.j zostały partnerami projektu kluczowego w ramach WRPO –– „Budowa Wielkopolskiej Sieci Szerokopasmowej" realizowanego przez spółkę Wielkopolska Sieć Szerokopasmowa SA. na zlecenie Województwa Wielkopolskiego. Celem projektu jest wypełnienie luki w dostępie do sieci internetowej następnej generacji (NGA). Dzięki podpisanej umowie do połowy 2014 roku wszystkie wielkopolskie gminy mają być włączone do Wielkopolskiej Sieci Szerokopasmowej. Całkowity koszt projektu netto to prawie 368 milionów złotych.

Bezpieczeństwo

Aresztowania chińskich hakerów

Od stycznie do listopada 2010 w Chinach oskarżono o hakerstwo ponad 460 osób. Minister Bezpieczeństwa Publicznego jest zdania, że choć liczba aresztowanych jest duża, nie przestraszy ona innych i szanse na zmniejszenie przestępczości tego typu są niewielkie. Oświadczenie tej treści zostało sformułowane w poniedziałek, a do publicznej wiadomości podano je dzień po tym, jak z Departamentu Stanu USA wyciekły intrygujące informacje, dotyczące między innymi bezpieczeństwa systemów komputerowych. Według anonimowego informatora z Chin, chińskie Biuro Polityczne kierowało ingerencją w system komputerowy Google. Akcja była tylko częścią większej skoordynowanej kampanii sabotażowej, przeprowadzanej przez chińskich agentów rządowych, prywatnych ekspertów w dziedzinie bezpieczeństwa i przestępców internetowych. Urzędnik chiński, którego danych nie podano, poinformował, że mimo postępów w zwalczaniu przestępczości internetowej, jej poziom w Chinach jest nadal wysoki. Liczba wykroczeń popełnianych przez hakerów wciąż niepokoi.

Technologie

LTE w Plusie

Jednoczesna transmisja wielu kanałów telewizyjnych i filmów w jakości HD oraz bezpośrednie dwukierunkowe przekazy telewizyjne, w tym w 3D – to wszystko przy użyciu jednego modemu w technologii LTE zaprezentował jako pierwszy operator w Polsce Polkomtel, operator sieci Plus, na pokazie prasowym. Już w pierwszym kwartale 2011 roku Plus planuje przeprowadzenie testów LTE wśród wybranych użytkowników. Long Term Evolution (LTE) to obecnie najszybsza na świecie technologia mobilnego dostępu do sieci. Oferowane przez nią szybkości mobilnej transmisji danych do 160 Mbps przewyższają możliwości HSPA+ ponad czterokrotnie. Minimalne czasy opóźnień i duże przepływności wysyłania danych stwarzają możliwości dwukierunkowych transmisji multimedialnych wysokiej jakości, m.in. TV na żywo lub VOD w formacie HD.

Nowy patent na identyfikację spamu

Kaspersky Lab informuje o uzyskaniu amerykańskiego patentu dla swojej innowacyjnej technologii pozwalającej identyfikować elektroniczne wiadomości tekstowe jako spam. Opatentowana przez firmę Kaspersky Lab technologia opiera się na opisanym wyżej systemie wykorzystywania słów kluczowych i fraz, który pomaga wykryć spam. Wspomniana technika została zarejestrowana w Amerykańskim Urzędzie Patentów i Znaków Towarowych 16 listopada 2010 roku pod numerem 7 836 061. Opatentowana metoda klasyfikuje elektroniczne wiadomości tekstowe w oparciu o hierarchiczną listę kategorii wiadomości. Każda kategoria jest definiowana za pomocą zbioru słów kluczowych i szablonów tekstowych. Wiadomość przychodząca zostaje skategoryzowana w następujący sposób: najpierw obliczana jest jej waga względem każdej kategorii zawierającej słowa kluczowe obecne w e-mailu. Następnie określany jest stopień podobieństwa do każdego z szablonów. Jeżeli wiadomość zawiera określoną liczbę słów kluczowych lub jest wystarczająco podobna do jednego z szablonów, zostaje sklasyfikowana do odpowiedniej kategorii, łącznie ze spamem.

Internet

Grupa Avanti dostarczy Internet przez satelitę

Grupa Avanti Communications umieściła na orbicie satelitę, który umożliwi obywatelom Polski szerokopasmowy dostęp do Internetu o dużej przepustowości i w atrakcyjnej cenie. Projekt przyczyni się do ograniczenia zjawiska wykluczenia cyfrowego i tym samym pomoże zniwelować różnice w dostępie i korzystaniu z komputerów i Internetu pomiędzy osobami o różnej płci, wieku, statusie społeczno-ekonomicznym i różnym miejscu zamieszkania. **Satelita o nazwie HYLAS 1** jest pierwszym tego typu satelitą umieszczanym na orbicie poza terenem Stanów Zjednoczonych. Satelita zostanie wyniesiony w przestrzeń rakietą Ariane 5 z kosmodromu w Gujanie Francuskiej. Firma Avanti, prowadzi już zaawansowane prace nad budową drugiego satelity o nazwie HYLAS 2, który zostanie umieszczony na orbicie wiosną 2012 roku. Satelita ten zapewni jeszcze lepszy dostęp do Internetu na terenie Europy, obejmując również swoim zasięgiem część Bliskiego Wschodu i Afryki. Oba satelity będą mogły obsłużyć łącznie milion klientów indywidualnych. Avanti świadczy swoje usługi za pośrednictwem firm telekomunikacyjnych, współpracując na terenie Europy z 60 partnerami. W Polsce są nimi COMPUTEX TELECOMMUNICATIONS i TTComm.

Europejskie dziedzictwo kulturowe w sieci

Dzięki europejskiej bibliotece cyfrowej Europeana każdy na świecie ma teraz dostęp do ponad 14 milionów książek, map, fotografii, obrazów, fragmentów filmów i utworów muzycznych w wersji cyfrowej, pochodzących z instytucji kultury z całej Europy. Zainicjowana w 2008 r. i zawierająca początkowo dwa miliony obiektów Europeana osiągnęła już z nadwyżką pierwotny cel, jakim było 10 milionów obiektów do 2010 r. W dniu dzisiejszym grupa analityczna (tzw. „Comité des Sages" – Maurice Lévy, Elisabeth Niggemann, Jacques de Decker), ustanowiona przez Komisję w celu badania nowych sposobów digitalizowania europejskiego dziedzictwa kulturowego zaprezentuje się Radzie Ministrów Kultury oraz parlamentarnej Komisji Kultury. Sprawozdanie grupy analitycznej zostanie opublikowane na początku 2011 r.

Rynek

Hyperion może przejąć Stream Communications

Na początku września Hyperion SA, kontrolowany pośrednio przez fundusz MNI SA, zawarł wstępną umowę zakupu pośrednio 77,27 proc. akcji Stream Communications Sp z o.o., siódmego operatora telewizji kablowej w Polsce (świadczy usługi telewizji cyfrowej i analogowej, dostępu do Internetu, telefonii stacjonarnej) od funduszu Penta Investments. Strony uzgodniły wartość transakcji na 92,5 mln zł, a jej zakończenie przewidziano do końca 2010 r. Transakcja miała dojść do skutku po wypełnieniu kilku warunków zawieszających. Hyperion SA przekazał już na rzecz Penta Investments 9,25 mln zł zaliczki. Ważnym warunkiem było jednak uzyskanie zgody prezesa Urzędu Ochrony Konkurencji i Konsumentów na dokonanie koncentracji. Spółka otrzymała ją 22 listopada. Zakup większościowego pakietu Stream Communications zrealizowany zostanie za pieniądze z kredytu bankowego, zarząd Hyperion nie planuje podwyższania kapitału spółki i tym samym rozwadniania udziału obecnych akcjonariuszy.

Fuzja Novella z Attachmate Corporation

Firma Novell poinformowała o zawarciu ostatecznej umowy o fuzji, na mocy której Attachmate Corporation nabędzie Novella płacąc gotówką po 6,10 USD za akcję; całkowita wartość transakcji wyniesie około 2,2 mld USD. Attachmate Corporation stanowi własność grupy inwestycyjnej, na czele której stoją Francisco Partners, Golden Gate Capital i Thoma Bravo. Novell poinformował także o zawarciu ostatecznej umowy o jednoczesnym zbyciu części zasobów własności intelektualnej na rzecz CPTN Holdings LLC, konsorcjum firm technologicznych skupionych wokół Microsoft Corporation, za 450 mln USD w gotówce; należność ta ma zostać w ramach fuzji opłacona przez Attachmate Corporation. Kwota 6,10 USD za akcję Novella przewyższa o 28% cenę zamknięcia z 2 marca 2010 r., ostatniego dnia obrotu przed ujawnieniem przez Elliott Associates, L.P. propozycji nabycia wszystkich pozostających w obrocie akcji Novella po 5,75 USD za akcję, jest też wyższa o 9% od ceny zamknięcia z 19 listopada 2010 r. Plany Attachmate Corporation przewidują funkcjonowanie Novella jako dwóch jednostek biznesowych, Novell i SUSE, które dołączą do dwóch innych holdingów, Attachmate i NetIQ.

Prawo

Prezydent podpisał nowelizację Prawa telekomunikacyjnego

Dzięki nowym przepisom, porozumienia zawierane między UKE a operatorami telekomunikacyjnymi będą miały moc prawną. Ustawa została uchwalona w październiku br. Z chwilą wejścia w życie, porozumienia Urzędu z operatorami telekomunikacyjnymi staną się aktami administracyjnymi. W październiku 2009 r. UKE podpisał Porozumienie z Telekomunikacją Polską. Urząd zobowiązał się w nim, że nie będzie obniżał przez trzy lata stawek hurtowych, które Telekomunikacji Polskiej płacą inni operatorzy za korzystanie z infrastruktury spółki. W zamian za to w ciągu trzech lat TP ma wybudować i zmodernizować 1,2 mln linii telekomunikacyjnych. Porozumienie dotyczy też zawieszenia postępowania UKE w sprawie podziału TP na część hurtową i detaliczną. W związku z tym, że Porozumienie nie jest decyzją administracyjną, obecnie UKE nie może wykorzystać posiadanych narzędzi administracyjnych, w przypadku gdyby operator nie wywiązywał się z warunków Porozumienia. Nowelizacja Prawa telekomunikacyjnego ma to zmienić. Ustawa jest pozytywna również dla operatorów, gdyż wynegocjowane z regulatorem rozwiązania mogą być ujęte w ramy decyzji administracyjnej, której nie można zmienić bez zgody strony.

Informatyka

Firmy mogą śledzić interakcj w mediach społecznościowych

Firma Cisco Systems poinformowała o wprowadzeniu na rynek oprogramowania Cisco® SocialMiner, które pozwala firmom wyszukiwać i z wyprzedzeniem reagować na potrzeby obecnych i potencjalnych klientów komunikujących się za pośrednictwem publicznych sieci społecznościowych, takich jak Twitter i Facebook oraz innych forów lub serwisów blogerskich. Oprogramowanie umożliwia monitorowanie w czasie rzeczywistym zmian statusu, wpisów na forach i blogach klientów oraz powiadamianie przedsiębiorstw o rozmowach dotyczących ich marki. Oferowane przez Cisco rozwiązanie pozwala firmom nie tylko monitorować sieci społecznościowe w celu skuteczniejszej analizy danych biznesowych, ale także nawiązywać kontakt z klientami.

AMD wspiera otwartą platformę MeeGo

Podczas konferencji MeeGo, firma AMD poinformowała, o rozpoczęciu współpracy z Linux Foundation nad budową otwartego systemu MeeGo. AMD wesprze MeeGo swoim doświadczeniem inżynierskim, by pomóc w budowie i rozwoju platformy dla urządzeń mobilnych nowej generacji. MeeGo to otwarty system operacyjny zaprojektowany przede wszystkim z myślą o mobilnych platformach sprzętowych, takich jak notebooki, tablety, samochodowe systemy multimedialne i smartfony. Projekt MeeGo jest prowadzony przez Linux Foundation, konsorcjum typu non-profit, którego głównym celem jest rozwój systemu Linux. AMD ma obecnie status „gold member" w Linux Foundation i dysponuje miejscem w zarządzie fundacji.

Telewizja

Postępy cyfryzacji telewizji w Europie

Konsumenci w Wielkiej Brytanii mają najlepszy dostęp do usług telewizyjnych w Europie – wynika z najnowszego rankingu Instytutu Globalizacji. Polska uplasowała się w środku stawki. Co robi Brytyjczyk, gdy za oknem pada deszcz? Ogląda cyfrową telewizję w jakości HD! Z najnowszego rankingu Instytutu Globalizacji, przedstawiającego zaawansowanie cyfryzacji w Europie, wynika, że liderami cyfryzacji są Brytyjczycy, Francuzi i Finowie. Nasz kraj należy do średniaków, ale jest niekwestionowanym liderem w Europie Środkowo-Wschodniej. Odkładana z roku na rok data wyłączenia nadawania sygnału analogowego w Polsce przyczyniła się do słabego wyniku naszego kraju w rankingu. Z kolei brak telewizji naziemnej skutkuje relatywnie niskim stopniem nasycenia kraju sygnałem cyfrowym na poziomie 40 proc.

Regulacje

Internet powinien pozostać otwarty

Z konsultacji społecznej zapoczątkowanej przez Komisję Europejską 30 czerwca i dotyczącej otwartego Internetu oraz neutralności sieci wynika, że niemal wszyscy uznają znaczenie zachowania otwartego Internetu. W konsultacji wzięło udział 318 zainteresowanych podmiotów reprezentujących wszystkie poziomy łańcucha wartości. Były to między innymi Organ Europejskich Regulatorów Łączności Elektronicznej (BEREC), operatorzy, dostawcy usług internetowych, organy państw członkowskich, zrzeszenia konsumentów i organizacje społeczeństwa obywatelskiego oraz obywatele. Konsultacja nie wykazała potrzeby dalszych uregulowań prawnych na poziomie UE. Oczekuje się jednak, że w przyszłości mogą być konieczne dodatkowe wytyczne.

UKE i UOKiK walczą z SMS-owymi naciągaczami

Do Urzędu Komunikacji Elektronicznej ciągle napływają skargi użytkowników telefonów komórkowych, którzy padają ofiarą firm proponujących skorzystanie z usług w zamian za wysłanie wiadomości na numery SMS Premium. Może to Cię kosztować nawet ponad 40 zł. Internetowi i telefoniczni oszuści znajdują coraz to nowe sposoby, aby namówić użytkowników na wysłanie drogiego SMS. W sieci jest coraz więcej stron, dzięki którym można poznać horoskop, datę śmierci, spotkać ciekawych ludzi czy śledzić swojego partnera lokalizując położenie jego telefonu komórkowego. Najnowsze oferty kuszą też tanim zakupem programów komputerowych czy informacją o wartościowych wygranych – wystarczy tylko wysłać wiadomość. Na stronie Centrum Informacji Konsumenckiej Urzędu Komunikacji Elektronicznej film, który opowiada, jak rozpoznać kosztownego SMS-a. Zachęcamy również do zapoznania się z postępowaniami prowadzonymi przez Urząd Ochrony Konkurencji i Konsumentów przeciwko nieuczciwym podmiotom.

Fundusze na rozwój badań

Grzegorz Kantowicz

780 mln euro na badania w dziedzinie technologii informacyjno-komunikacyjnych

27 września 2010 r. Komisja Europejska złożyła jedno z największych w historii zaproszenie do składania wniosków badawczych w dziedzinie technologii informacyjno-komunikacyjnych (TIK) w ramach unijnych programów ramowych w zakresie badań i rozwoju technologicznego. Miało to miejsce w trakcie największej europejskiej imprezy związanej z badaniami i innowacjami TIK, ICT 2010-Digitally Driven. W ramach tej inicjatywy sfinansowane zostaną w 2011 r. projekty o wartości 780 mln euro. Środki przeznaczone zostaną na badania w dziedzinie Internetu przyszłości, robotyki, inteligentnych i wbudowanych systemów, fotoniki, TIK w zakresie efektywności energetycznej, opieki zdrowotnej w starzejącym się społeczeństwie, i innych. W ramach „Europejskiej agendy cyfrowej" Komisja zobowiązała się utrzymać 20-procentowe tempo zwiększania co roku budżetu na badania i rozwój w dziedzinie TIK, przynajmniej do 2013 r.

Wiceprzewodnicząca Komisji **Neelie Kroes**, odpowiedzialna między innymi za agendę cyfrową, wyjaśnia: *Zwiększanie ogólnych inwestycji w badania TIK ma kluczowe znaczenie dla przyszłości. Unijnemu wsparciu naszych światowej klasy naukowców muszą towarzyszyć dodatkowe pokaźne inwestycje ze strony samych beneficjentów. Badania te pozwolą europejskiemu przemysłowi zwiększyć swoją konkurencyjność.*

Zaproszenie do składania wniosków o wartości 780 mln euro (zaproszenie 7 TIK) jest elementem największego w historii rocznego programu roboczego, będącego częścią siódmego unijnego programu ramowego w zakresie badań i rozwoju technologicznego. W budżecie na 2011 r. przewidziano na ten cel prawie 1,2 mld euro. 220 mln euro przekazano już w lipcu 2010 r. na rzecz partnerstw publiczno-prywatnych zajmujących się TIK w dziedzinie inteligentnych samochodów, ekologicznych budynków, fabryk działających z poszanowaniem zasad zrównoważonego rozwoju oraz Internetu przyszłości.

W bieżącym zaproszeniu 120 mln euro przeznacza się na finansowanie badań i rozwoju technologicznego w dziedzinie infrastruktury sieciowej, mediów i usług cyfrowych na rzecz Internetu przyszłości. Ma to zasadnicze znaczenie, jeśli w najbliższym dziesięcioleciu Europa chce sprostać wyzwaniom stojącym przed coraz bardziej cyfrowym społeczeństwem. Prawie 100 mln euro zostało już zarezerwowanych dla partnerstwa „Internet przyszłości", aby wykorzystać rosnące zapotrzebowanie na innowacyjne aplikacje internetowe pozwalające uczynić bardziej „inteligentną" infrastrukturę w dziedzinie systemów zdrowotnych, sieci energetycznych i systemów zarządzania ruchem.

Aby wzmocnić pozycję Europy jako wiodącego dostawcy systemów elektronicznych i komponentów fotonicznych, ponad 200 mln euro przeznaczono na badania w tej dziedzinie. Dzięki temu wzrośnie konkurencyjność przemysłu motoryzacyjnego, telekomunikacji, automatyki przemysłowej, technologii oświetleniowych oraz przemysłu medycznego w Europie. Ich sukces zależy od zintegrowania innowacyjnych komponentów i systemów z wyrobami i usługami we wszystkich sektorach. Postęp w technologii laserowej na przykład ma kluczowe znaczenie dla stymulowania rozwoju łączności optycznej i uzyskania ultraszybkich prędkości internetowych dostępnych dla wszystkich Europejczyków. W bieżącym zaproszeniu do składania wniosków przewidziano prawie 200 mln euro na badania TIK w dziedzinie zdrowia i starzenia się społeczeństwa. Liczba Europejczyków w wieku powyżej 60 lat rośnie średnio o 2 miliony rocznie. TIK mają kluczowe znaczenie jeśli chodzi o stworzenie trwałych rozwiązań i maksymalizację możliwości rynkowych, które pomogą ograniczyć koszty socjalne i opieki zdrowotnej.

Ponadto 135 mln euro przeznaczono na badania TIK, które podniosą efektywność energetyczną budynków, transportu i logistyki. Powyższe środki uzupełniają 220 mln euro udostępnionych w lipcu 2010 r. partnerstwom publiczno-prywatnym na rzecz gospodarki opartej na samochodach, budynkach i fabrykach o niskiej emisji dwutlenku węgla (zob. Powyżej). W ramach zaproszenia 7 TIK o finansowanie projektów mogą ubiegać się uniwersytety, ośrodki badawcze, MŚP, duże firmy i inne organizacje w Europie, a także spoza Europy. Wnioski można składać do dnia 18 stycznia 2011 r. Następnie zostaną one ocenione przez niezależne grupy eksperckie, które dokonają wyboru w oparciu o jakość wniosków.

Kontekst

ICT 2010-Digitally Driven zgromadziło w dniach 27-29 września w Brussels Expo naukowców, biznesmenów, inwestorów i decydentów zajmujących się TIK i innowacyjnymi rozwiązaniami cyfrowymi. Głównymi tematami konferencji były badania na rzecz zrównoważonego rozwoju w gospodarce o niskiej emisji dwutlenku węgla, wkład TIK w życie codzienne oraz znaczenie środków publicznych i finansowania badań i innowacji TIK. Poza tym zaprezentowanych zostało ponad 100 eksponatów przedstawiających najnowsze osiągnięcia cyfrowe finansowane przez UE. Wydarzenie to ma miejsce co dwa lata i organizowane jest przez Komisję Europejską. W tym roku gospodarzem była belgijska prezydencja wraz z Radą Ministrów UE.

Siódmy unijny program ramowy obejmuje lata 2007-2013, a jego budżet na badania i rozwój TIK wynosi 9 mld euro. Roczny wzrost finansowania badań TIK jest zgodny z „Europejską agendą cyfrową", flagowym programem strategicznym UE, który przewiduje podwojenie do 2020 r. rocznych wydatków publicznych na badania oraz rozwój TIK i zachęca do podobnego wzrostu w zakresie finansowania prywatnego, aby zrealizować cele strategii „Europa 2020" na rzecz zatrudnienia i wzrostu gospodarczego.

Finansowane przez UE projekty badawcze TIK dotyczą każdego roku ponad 15 000 naukowców oraz stymulują innowacyjny rozwój Europy i wzrost gospodarczy w przemyśle. Dają także istotne możliwości w zakresie innowacji MŚP, które są szeroko reprezentowane w tych strategicznych obszarach rozwoju. ■

wideokonferencja w zasięgu Twojej dłoni

VideoViator Suite v. 1.2

oszczędzaj czas i pieniądze

Panaceum na ograniczenie kosztów dla firm i instytucji

MSG MEDIA
ul. Chwytowo 2, 85-223 Bydgoszcz; tel. (52) 325 83 10, fax (52) 373 52 43
e-mail: office@msgmedia.pl, www.techbox.pl

Polska i Węgry w tyle

Grzegorz Kantowicz

FTTH/B w Europie Środkowowschodniej

Kraje Europy Środkowowschodniej (Central Eastern Europe – CEE) plasują się na czele europejskich rankingów jeśli chodzi o wzrost liczby abonentów Internetu w oparciu o łącza światłowodowe doprowadzane do budynku (ang. Fibre to the Home/Business – FTTH/B). Technologia FTTH/B najszybciej rozwija się tam, gdzie dostęp do lokalnej sieci abonenckiej operatorów zasiedziałych (ang. Local Loop Unbundling – LLU) nie został umożliwiony lub nie zdobył popularności ze względu na wysokie ceny. Według Frost & Sullivan, inwestycje w technologię FTTH/B będą jednym z najważniejszych elementów przewagi konkurencyjnej dostawców Internetu stacjonarnego w walce z szybko rozwijającym się Internetem mobilnym.

– *Liderem w zakresie wprowadzenia FTTH/B w regionie CEE jest Litwa, gdzie penetracja wśród gospodarstw domowych wynosi ponad 20 procent* – stwierdza **Edyta Kosowska**, analityczka z warszawskiego oddziału Frost & Sullivan, globalnej firmy doradczej, i dodaje: *Duże rozpowszechnienie technologii światłowodowej w krajach bałtyckich jest w znacznym stopniu wynikiem silnej pozycji operatorów skandynawskich w tym regionie*. Najnowsze rozwiązania wdrożone w Skandynawii są w stosunkowo krótkim czasie również wprowadzane na Litwie, Łotwie i w Estonii. Co więcej, wszystkie nowe sieci budowane na Litwie są oparte na światłowodach. Kable miedziane są tam uznawane za technologię przestarzałą i wyeksploatowaną.

Jakkolwiek w Rosji poziom penetracji technologii FTTH/B pozostaje dość niski, z dostępu za pomocą światłowodów korzysta tam ponad milion odbiorców – najwięcej w całej Europie. W związku z tym, że możliwości uzyskania dostępu do infrastruktury operatora zasiedziałego były ograniczone, FTTB stało się rozwiązaniem przyjętym przez wielu największych operatorów, takich jak VimpelCom, Comstar, ER-Telecom i TTK. Wszystkie firmy planują znaczące inwestycje w rozwój sieci światłowodowej. – *Co ciekawe* – zauważa Edyta Kosowska – *kilka przedsiębiorstw zależnych od zasiedziałego operatora również ogłosiło plany inwestycji w FTTB.* Z uwagi na dużą populację i niewielką ogólną penetrację sieci szerokopasmowych, Rosja pozostaje jednym z najbardziej obiecujących rynków dla rozwoju technologii światłowodowych w Europie.

W innych krajach regionu, takich jak Bułgaria i Rumunia, większość abonentów FTTH/B obsługiwana jest przez niewielkich operatorów. Około 40-50 procent łączy internetowych pochodzi od dostawców LAN/MAN, z których wielu wykorzystuje technologię FTTB. W konsekwencji wiele linii w Bułgarii i Rumunii oferuje prędkości ponad 10 Mbps. Do najważniejszych firm zapewniających Internet szerokopasmowy za pomocą technologii FTTH/B w Bułgarii należą

Vestitel, SpectrumNet i Netone. W Rumunii ważnym dostawcą jest firma RCS&RDS, rozwijająca również sieci światłowodowe na Węgrzech.

– *Wart uwagi jest fakt, że ważne rynki Internetu szerokopasmowego w regionie, takie jak Polska i Węgry, nie znalazły się w czołówce rankingu krajów wykorzystujących FTTH/B* – stwierdza Edyta Kosowska. – *Jedną z przyczyn może być stosunkowo większa popularność modeli umożliwiających operatorom alternatywnym uzyskanie dostępu do infrastruktury zasiedziałych operatorów telekomunikacyjnych, jak na przykład dostęp do lokalnej sieci abonenckiej (LLU) lub bitstream access (BSA). Wynajmowanie infrastruktury „ostatniej mili" od zasiedziałego operatora w perspektywie krótko- czy średnioterminowej jest bardziej uzasadnione ekonomicznie niż inwestycja w technologie światłowodowe.*

Nie należy spodziewać się, że w ciągu najbliższych kilku lat technologia światłowodowa zdominuje tradycyjną DSL (z ang. *Digital Subscriber Line*), jednakże zapotrzebowanie na FTTH/B będzie wciąż rosło, przede wszystkim w Rosji i krajach bałtyckich. Znaczącego wzrostu można się także spodziewać w Czechach oraz w Bułgarii i Rumunii, gdzie ogólny stopień penetracji Internetu szerokopasmowego wciąż pozostaje niski.

– *W krajach takich jak Polska i Węgry, z silną obecnością modelu BSA, nie należy się spodziewać rozpowszechnienia technologii FTTH/B przed rokiem 2012. Najbardziej prawdopodobnym scenariuszem w przypadku operatorów alternatywnych jest kontynuacja wykorzystywania infrastruktury „ostatniej mili" zasiedziałych operatorów* – podsumowuje Edyta Kosowska. – *Można jednak spodziewać się rosnących inwestycji w sieci światłowodowe w odpowiedzi na coraz większe zapotrzebowanie na szybki Internet i zaawansowane usługi multimedialne. Pomocne okażą się także fundusze unijne na rozwój nowych technologii.* ■

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

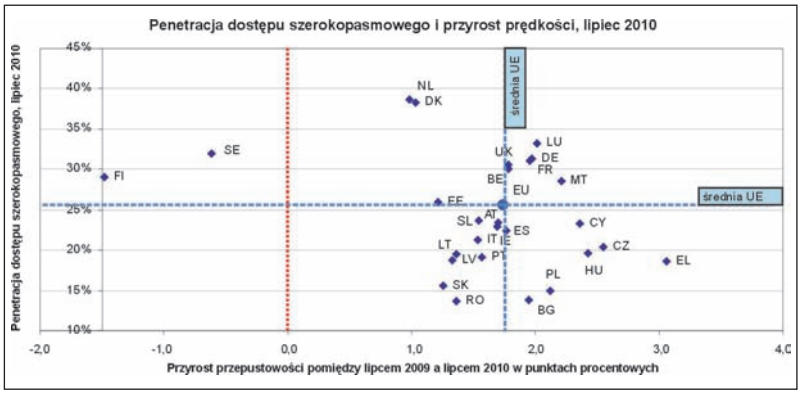
Agenda cyfrowa

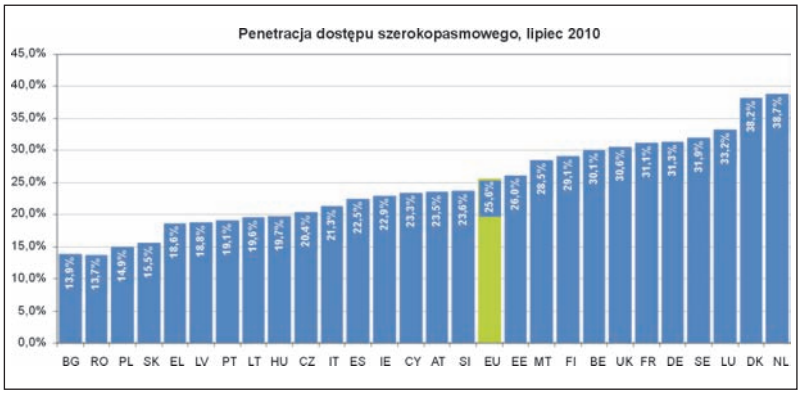
Marta Angrocka-Krawczyk

Internet szerokopasmowy w Europie jest coraz szybszy, ale nadal pozostaje wiele do zrobienia

Według danych statystycznych opublikowanych przez Komisję Europejską, szerokopasmowe łącza internetowe w Europie są szybsze niż rok temu. W lipcu 2010 r. 29 proc. łączy szerokopasmowych w UE miało przepustowość wynoszącą co najmniej 10 megabitów na sekundę (Mb/s) (o 15 proc. więcej niż rok wcześniej).

Dostęp do Internetu szerokopasmowego staje się w Europie coraz powszechniejszy: na stu obywateli przypada 25,6 abonamentu, podczas gdy rok wcześniej wskaźnik ten wynosił 23,9. Aż o 45 proc. wzrosła liczba osób korzystających z Internetu mobilnego: na stu obywateli przypada już 6 urządzeń zapewniających mobilny dostęp szerokopasmowy (kluczy USB lub kluczy sprzętowych). Nadal pozostaje jednak wiele do zrobienia, aby osiągnąć cele zapisane w europejskiej agendzie cyfrowej. UE zobowiązała się w niej do zapewnienia wszystkim Europejczykom do 2013 r. dostępu do podstawowego Internetu szerokopasmowego, a do 2020 r. – do szybkiego i bardzo szybkiego Internetu szerokopasmowego. We wrześniu 2010 r. Komisja Europejska przedstawiła pakiet środków, które umożliwią wprowadzenie i powszechne wykorzystanie szybkiego i bardzo szybkiego Internetu szerokopasmowego w UE.





Neelie Kroes, wiceprzewodnicząca Komisji odpowiedzialna za europejską agendę cyfrową, powiedziała: *Szybki Internet jest jak cyfrowy tlen, niezbędny dla zdrowia i dobrobytu Europy. Liczba użytkowników Internetu i jego prędkość ciągle rosną, ale musimy dołożyć większychj starań, aby osiągnąć nasze cele dotyczące dostępu szerokopasmowego o bardzo dużej przepustowości. Szczególnie ważne jest szybkie osiągnięcie porozumienia w sprawie naszego wniosku dotyczącego udostępnienia odpowiednich częstotliwości widma radiowego na potrzeby mobilnego Internetu, którego wykorzystanie rośnie w bardzo szybkim tempie.*

W lipcu 2010 r. prawie jedna trzecia łączy szerokopasmowych w UE zapewniała przepustowość wynoszącą ponad 10 Mb/s (w lipcu 2009 r. odsetek ten wynosił 15 proc.) Dzięki większym prędkościom przesyłania danych klienci mają na ogół większy wybór usług lepszej jakości po niższej cenie za megabit. W przypadku 5 proc. łączy internetowych w UE średnia przepustowość wynosi 30 Mb/s lub więcej (ale tylko 0,5 proc. łączy zapewnia przepustowość wynoszącą 100 Mb/s lub więcej).

Nowe usługi w branży rozrywkowej i w świecie biznesu, takie jak telewizja o wysokiej rozdzielczości i wideokonferencje, wymagają wprowadzenia Internetu o większej przepustowości niż ta, jaka jest na ogół dostępna w Europie. Dopiero wtedy UE będzie mogła dorównać światowym liderom w tej dziedzinie, takim jak Korea Południowa i Japonia. Cele na 2020 r. zapisane w europejskiej agendzie cyfrowej to zapewnienie wszystkim Internetu o przepustowości wynoszącej co najmniej 30 Mb/s oraz zapewnienie połowie europejskich gospodarstw domowych dostępu szerokopasmowego o przepustowości przekraczającej 100 Mb/s.

Według najnowszych danych statystycznych, między lipcem 2009 r. a lipcem 2010 r. liczba łączy szerokopasmowych w całej UE wzrosła o 8 proc. (wzrost był więc nieco wolniejszy niż w roku poprzednim, kiedy wynosił 11 proc.). Według stanu z lipca 2010 r., w UE jest ponad 128 mln stałych szero-

kopasmowych łączy internetowych, z czego 9 milionów zainstalowano w okresie od lipca 2009 r. Liczba gospodarstw domowych w UE wynosi około 220 milionów.

Holandia i Dania nadal utrzymują się w światowej czołówce pod względem liczby użytkowników Internetu szerokopasmowego (prawie 40 linii dostępowych na stu obywateli, dzięki czemu z Internetu szerokopasmowego korzysta prawie 80 proc. gospodarstw domowych). Tempo wzrostu zaczyna jednak maleć ze względu na nasycenie rynków (w państwach członkowskich będących liderami, takich jak Finlandia i Szwecja, liczba użytkowników stacjonarnego Internetu szerokopasmowego spada, ponieważ przechodzą oni na Internet mobilny).

W dziewięciu państwach członkowskich UE (Belgia, Dania, Finlandia, Francja, Niemcy, Luksemburg, Holandia, Szwecja i Wielka Brytania) odsetek użytkowników Internetu szerokopasmowego jest wyższy niż w Stanach Zjednoczonych (według danych statystycznych OECD z maja 2010 r., w USA na stu mieszkańców przypada 26,4 abonamentu). W ubiegłym roku największe postępy odnotowano w Czechach i w Grecji (wzrost na jednego mieszkańca).

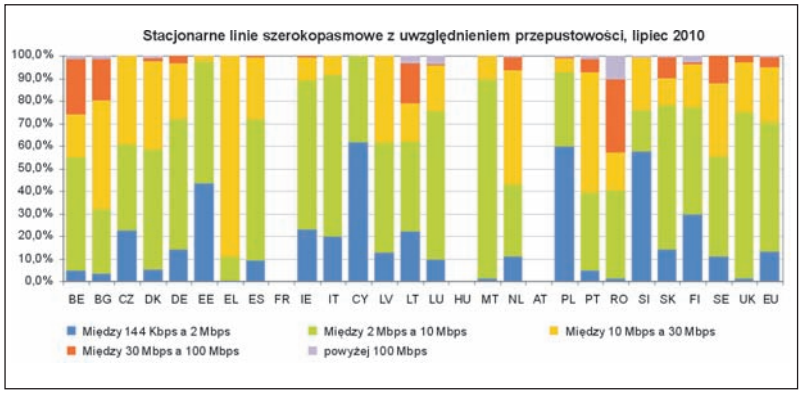
Technologią najczęściej wykorzystywaną w celu uzyskania dostępu szerokopasmowego w Europie pozostaje technologia DSL (*Digital Subscriber Line*), która zapewnia 100 milionów łączy, ale jej udział w rynku maleje na rzecz szybszych sieci światłowodowych oraz łączy kablowych (opartych na DOCSIS 3.0, czyli ulepszonych sieciach kablowych zapewniających bardzo szybki Internet). Dostęp do łączy światłowodowych dla odbiorców domowych wzrósł w okresie od lipca 2009 r. do lipca 2010 r. o 40 proc., ale stanowi obecnie nie więcej niż 1,7 proc. ogółu łączy w Europie i oferowany jest jak dotąd w niewielu państwach (np. w Szwecji, gdzie 24 proc. łączy szerokopasmowych działa w oparciu o sieci światłowodowe).

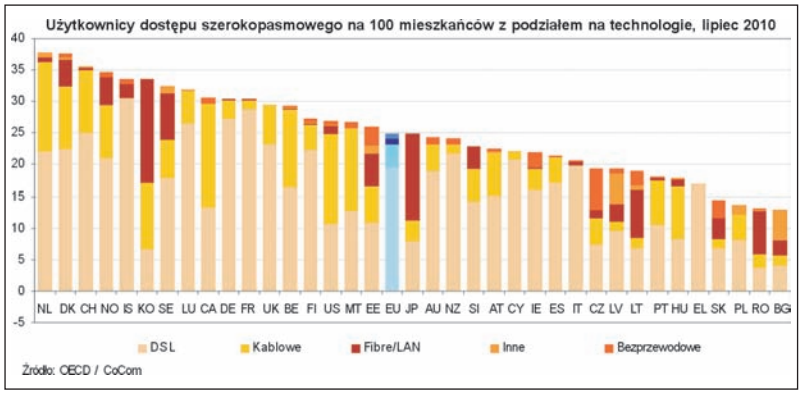
Szybki rozwój mobilnego Internetu szerokopasmowego

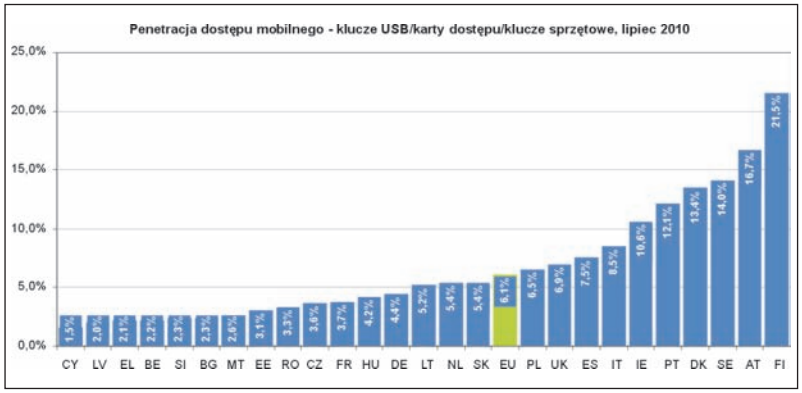
Mobilny dostęp szerokopasmowy (np. poprzez klucze sprzętowe dla laptopów) staje się coraz popularniejszy w kilku państwach członkowskich, zwłaszcza w Finlandii (21,5 mobilnych łączy szerokopasmowych przez klucze USB/karty dostępu/klucze sprzętowe na stu obywateli), w Austrii (16,7), Szwecji (14), Danii (13,4) i w Portugalii (12,1). Obecny poziom rozpowszechnienia mobilnych usług szerokopasmowych w Europie wynosi 6 proc., czyli o 45 proc. więcej niż w lipcu 2009 r.

Średni udział w rynku zasiedziałych operatorów telekomunikacyjnych w UE nieznacznie spadł do około 44 proc. Najwyższy jest na Cyprze (76 proc.), w Finlandii (68 proc.) i w Luksemburgu (66 proc.), a najniższy w Rumunii i Wielkiej Brytanii (28 proc.) oraz w Bułgarii (32 proc.). Tym niemniej udział operatorów zasiedziałych w rynku łączy szerokopasmowych (w tym również w odniesieniu do hurtowej odsprzedaży łączy) systematycznie maleje, z korzyścią dla operatorów konkurujących z nimi w oparciu o infrastrukturę (głównie dzięki uwalnianiu lokalnych pętli abonenckich, które otwiera stronom trzecim dostęp do sieci). Uwolnione lokalne pętle abonenckie i współdzielone linie dostępowe stanowią 74,8 proc. wszystkich linii typu DSL wykorzystywanych przez operatorów alternatywnych, podczas gdy przed rokiem odsetek ten wynosił 71,4 proc. Wzrost liczby uwolnionych lokalnych pętli abonenckich, choć już nie tak szybki jak w ubiegłym roku, odbywa się kosztem odsprzedaży, czyli formy oferowania dostępu dla nowych podmiotów niewymagającej dużych nakładów, której udział we wszystkich liniach DSL, wynoszący w 2009 r. 10,6 proc., zmniejszył się do 8,9 proc. Nowi uczestnicy rynków telekomunikacyjnych dokonują więc coraz większych inwestycji, co przyczyniło się do powstania bardziej konkurencyjnego rynku usług szerokopasmowych.

Pakiet dotyczący dostępu szerokopasmowego przedstawiony we wrześniu 2010 r. obejmuje zalecenie Komisji w sprawie regulowanego dostępu do sieci dostępu nowej generacji (NGA), który ma się przyczynić do osiągnięcia równowagi między przyciąganiem inwestycji a ochroną konkurencji, wniosek w sprawie decyzji dotyczącej utworzenia programu polityki w zakresie widma radiowego, której jednym z celów jest zapewnienie dostępności widma na potrzeby bezprzewodowego dostępu szerokopasmowego oraz komunikat w sprawie Internetu szerokopasmowego, w którym przedstawiono, jak skutecznie przyciągać inwestycje. ■







Urządzenie do badań baterii akumulatorów

Współczesne systemy telekomunikacyjne muszą funkcjonować także podczas awarii sieci elektroenergetycznej i dlatego mają własne rezerwowe źródła energii. Takim rezerwowym źródłem są z reguły dwie 48V baterie akumulatorów kwasowo-ołowiowych, o pojemności od 100 Ah do 3 000 Ah, wspierane stacjonarnymi lub przewoźnymi agregatami prądotwórczymi. Stosowane wcześniej „otwarte" akumulatory klasyczne od lat 90. są zastępowane akumulatorami wyposażonymi w zawory regulacyjne (typ VRLA – Valve Regulated Lead Acid), z elektrolitem w postaci żelu lub uwięzionym w macie z włókna szklanego (typ AGM).

Wstęp

Gwarantujące ciągłość pracy urządzeń telekomunikacyjnych baterie akumulatorów należy okresowo kontrolować lub profilaktycznie wymieniać. Operator sieci telekomunikacyjnej może zróżnicować swoje procedury, uzależniając je od umiejscowienia obiektu w hierarchii, typu, pojemności i masy baterii oraz kosztów prowadzenia badań. Baterie o dużych pojemnościach (300 Ah – 3 000 Ah), ze względu na masę i wymiary, mogą być kontrolowane jedynie w obiekcie telekomunikacyjnym.

Uszkodzenia akumulatorów można wykrywać monitorując napięcia ich monobloków podczas pracy w systemie zasilania obiektu telekomunikacyjnego lub/i poprzez okresowy pomiar ich konduktancji, natomiast wiedzę o faktycznej pojemności akumulatorów typu VRLA można uzyskać wyłącznie poprzez kontrolne wyładowanie-ładowanie znamionowym prądem.

Klasyczną metodą pomiaru pojemności jest wyładowanie kontrolne z wykorzystaniem opornicy o manualnej zmianie rezystancji. Konserwator odłącza wyznaczoną baterię od siłowni i odbiorów (pozostawiając dołączoną drugą baterię), dołącza do niej opornicę i zmieniając jej nastawy utrzymuje stały prąd wyładowania, a w ustalonych odstępach czasu notuje temperaturę oraz napięcie baterii i jej poszczególnych monobloków. Po osiągnięciu minimalnego napięcia baterii lub któregoś z jej bloków/ogniw lub po upływie wymaganego czasu (np. 8 godzin przy 10-godzinnym prądzie wyładowania) odłącza się opornicę i oblicza pojemność baterii. Jeżeli bateria jest sprawna, to dołącza się ją do wydzielonego zespołu prostownikowego w celu powrotnego naładowania, po czym łączy baterię z siłownią.

W miarę rozwoju technologii opornice wyposażano w funkcję utrzymywania stałego prądu rozładowania oraz wyłączania tego prądu po osiągnięciu zadanego, końcowego napięcia wyładowania, ale manualna rejestracja napięć monobloków i przełączanie z wyładowania na ładowanie powrotne pozostały.

W latach 90. podejmowano próby wprowadzenia na rynek europejski autonomicznego urządzenia do kontrolnego wyładowywania i ładowania baterii akumulatorów, lecz ze względu na założoną uniwersalność (baterie o napięciu od 2 V do 50 V i pojemności od 50 Ah do 1 000 Ah, oddawanie energii do sieci elektroenergetycznej poprzez układy tyrystorowe) okazało się ono ciężkie i zbyt kosztowne.

Automatyzacją procesu wyładowywania i ładowania baterii w obiektach telekomunikacyjnych zajmuje się, od roku 2000, Instytut Łączności w Warszawie, z powodzeniem wdrażając do eksploatacji urządzenia TBA2-IŁ oraz TBA150-IŁ.

Urządzenie TBA160-IŁ

W roku 2009 Instytut Łączności rozpoczął realizację Projektu pt. „Nowa generacja urządzenia do kontroli baterii VRLA telekomunikacyjnych systemów zasilających", współfinansowanego ze środków Unii Europejskiej w ramach Programu Operacyjnego Innowacyjna Gospodarka, Priorytet 1 „Badania i rozwój nowoczesnych technologii", Działanie 1.3. „Wsparcie projektów B+R na rzecz przedsiębiorców realizowanych przez jednostki naukowe", Poddziałanie 1.3.1 „Projekty rozwojowe". Głównym produktem Projektu jest prototyp urządzenia TBA160-IŁ.

Urządzenie przeznaczone jest do kontrolnego wyładowywania i ładowania baterii kwasowo-ołowiowych, zwłaszcza VRLA, w obiektach telekomunikacyjnych. Podczas pracy w takich obiektach urządzenia są zasilane napięciem siłowni, a energię pobieraną z rozładowywanej baterii przekazują do odbiorów siłowni, odciążając czasowo jej zespoły prostownikowe.

Urządzenie TBA160-IŁ (Rys. 1) umożliwia zaprogramowanie cyklu badaniowego obejmującego: ładowanie wyrównawcze, kontrolne wyładowanie oraz ładowanie powrotne – baterii akumulatorów w obiekcie telekomunikacyjnym. Zadaniem konserwatora jest podłączenie urządzenia do kontrolowanej baterii (odłączonej od siłowni), zaprogramowanie badań, a po ich zakończeniu przesłanie wyników (LAN, pamięć SD) do komputera PC i przywrócenie uprzedniego układu pracy siłowni.

Urządzenie TBA160-IŁ umożliwia (dla baterii 24 V, 36 V, 46 V, 48 V lub 50 V, odłączonej na czas badań od siłowni):

- wyładowywanie zadanym prądem z zakresu do 160 A jednej baterii na odbiory siłowni, przy równoczesnej pracy buforowej siłowni DC z drugą (lub pozostałymi) baterią;
- wyładowywanie baterii na wewnętrzne rezystory – podczas takiego wyładowania urządzenie oddaje energię (maks. 420 W) w postaci ciepła;
- ładowanie powrotne, uprzednio wyładowanej baterii, zadanym prądem z zakresu do 160 A;

- okresowe ładowanie wyrównawcze baterii, zadanym podwyższonym napięciem (do napięcia zaprogramowanego ok. 2,4 V/ogniwo);
- realizację sekwencji złożonej z procesu wyładowaniaładowania ew. poprzedzonego ładowaniem wyrównawczym, bez udziału obsługi oraz zdalne powiadomienie (Internet, sieć GSM) obsługi o zakończeniu lub przerwaniu procesu.

Zasady pracy urządzenia TBA160-IŁ

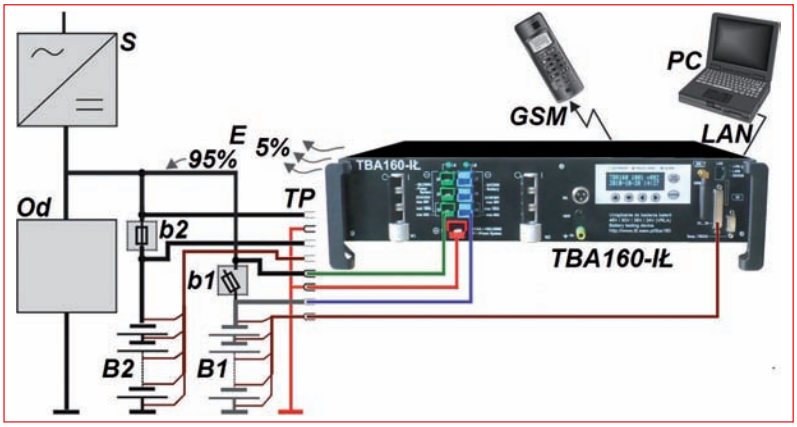
Urządzenia TBA160-IŁ operacje ładowania i wyładowywania baterii realizują w sposób opisany poniżej.

Ładowanie wyrównawcze ma na celu doprowadzenie wszystkich ogniw baterii do stanu pełnego naładowania, co pozwala na ocenę faktycznej pojemności baterii nawet w sytuacji, gdy badanie prowadzono po zaniku napięcia w sieci elektroenergetycznej i bateria nie była w pełni naładowana. Ładowanie wyrównawcze powinno być dokonywane prądem 10- lub 20-godzinnym. Prowadzi się je do napięcia wyższego niż napięcie pracy buforowej, co zmniejsza wpływ niedoładowania płyt ujemnych baterii i wydłuża w ten sposób czas jej eksploatacji. Ładowanie wyrównawcze wspomagają układy wyrównujące napięcia poszczególnych ogniw, tzw. „wyrównywacze napięcia".

Wyładowanie kontrolne jest z reguły prowadzone prądem 10-godzinnym. Dla uzyskania jednoznacznych i powtarzalnych wyników, jest prowadzone prądem o stałej wartości – do osiągnięcia zadanej wartości końcowej wartości napięcia wyładowania baterii, osiągnięcia przez ogniwo/blok dolnego dopuszczalnego napięcia lub do pobrania zadanego (np. stanowiącego 80% pojemności znamionowej) ładunku. Urządzenie TBA160-IŁ mierzy ładunek pobrany z baterii i przelicza na wartość równoważną dla temperatury +20°C.

Ładowanie powrotne zapewnia przywrócenie stanu pełnego naładowania baterii po jej wyładowaniu i powinno być dokonywane prądem 10- lub 20-godzinnym. Po osiągnięciu zadanego napięcia końcowego ładowania baterii (wyższego niż napięcie pracy buforowej), prąd ładowania jest stopniowo zmniejszany. Urządzenie TBA160-IŁ monitoruje napięcia ogniw/bloków baterii i tak ogranicza prąd, aby nie przekraczać ich dopuszczalnego napięcia. Ładowanie jest kończone, gdy prąd spadnie do zaprogramowanej wartości.

Urządzenie TBA160-IŁ pozwala na realizację opisanych powyżej operacji przy minimalnym zaangażowaniu konserwatora. Kontrola wszystkich istotnych parametrów baterii eliminuje możliwość uszkodzenia baterii. Dostarczane wraz z urządzeniem oprogramowanie na komputer PC umożliwia: archiwizację wyników pomiaru, ich przeglądanie i sporządzanie raportów z badań.



Rys. 1. Układ pracy urządzenia TBA160-IŁ w obiekcie telekomunikacyjnym
Oznaczenia:
***S** – siłownia; **Od** – odbiory siłowni; **B1** – kontrolowana bateria akumulatorów; **B2** – druga bateria akumulatorów; **b1**, **b2** – bezpieczniki-odłączniki baterii; **TP** – opcjonalna tablica pośrednicząca; **E** – energia z rozładowywanej baterii (5% w postaci ciepła, 95% do odbiorów energii w siłowni); **GSM** – komunikacja za pomocą SMS; **LAN** – komunikacja poprzez Internet/Intranet; **PC** – komputer typu PC*

Podstawowe dane techniczne urządzenia TBA160-IŁ

Obsługiwane baterie akumulatorów:	24/36/46/48/50 V, 50 ÷ 3000 Ah
Wymagane napięcie siłowni podczas ładowania i wyładowywania:	27/41/54 V±3V
Programowany prąd ładowania i wyładowywania baterii:	5 ÷ 160 A
Rodzaje pracy:	wyładowywanie, ładowanie powrotne, ładowanie wyrównawcze, ładowanie wyrównawcze+wyładowywanie +ładowanie powrotne
Nadzorowane parametry:	napięcie baterii i jej bloków, prąd, ładunek, temperatura, czas
Wymiary (wys. x szer. x głęb.)/masa:	88 x 440 x 320 mm/13 kg

Więcej informacji o Projekcie i urządzeniu TBA160-IŁ: http://www.itl.waw.pl/tba160.

Zakład Zastosowań Technik Łączności Elektronicznej Z-10, Instytut Łączności – Państwowy Instytut Badawczy (IŁ-PIB) http://www.itl.waw.pl

Bibliografia

[1] Chojnacki B., Godlewski P., Kobus R.,: Ocena sprawności baterii akumulatorów. Krajowym Sympozjum Telekomunikacji i Teleinformatyki KSTiT 2010, Wrocław 8-10 września 2010 r.

[2] Godlewski P.: Urządzenie TBA150-IŁ do kontroli baterii w siłowniach obiektów telekomunikacyjnych. Telekomunikacja i Techniki Informacyjne, 2008, nr 3-4, s.67-76.

Integracja w telefonach WLAN

Grzegorz Kantowicz

Telefony Voice-over-Wi-Fi nowej generacji

Firma Polycom rozszerza swoją ofertę telefonów Wi-Fi (VoWi-Fi) i wprowadza aparaty telefoniczne nowej generacji Polycom® SpectraLink® 8400 służące do bezprzewodowej obsługi transmisji głosu oraz danych.

Nowe aparaty serii SpectraLink 8400 jako pierwsze w branży charakteryzują się nowatorską, opartą na standardach platformą aplikacyjną, niezawodną formą ułatwiającą użytkowanie przez firmy, zintegrowanym czytnikiem kodów kreskowych, wysoką jakością głosu, jak również najwyższym poziomem interoperacyjności zgodnie z 802.11a/b/g/n, co pozwala na współpracę z infrastrukturą bezprzewodową i innymi platformami UC.

Telefony SpectraLink VoWi-Fi umożliwiają łatwy dostęp do ważnych danych z każdej lokalizacji w obrębie firmowej sieci Wi-Fi. Nowe rozwiązania zostały zaprojektowane w celu ułatwienia pracy pracownikom mobilnym. Spełniają wymagania związane z komunikacją w służbie zdrowia, przemyśle, handlu.

Zastosowania SpectraLink 8400

– Wraz z wprowadzeniem serii telefonów 8400 firma Polycom podnosi klasę VoWi-Fi na wyższy poziom funkcjonalności i wydajności – powiedział **Craig Mathias**, dyrektor Grup Farpoint, firmy konsultingowej specjalizującej się w komunikacji bezprzewodowej oraz usługach mobilnych.

Obsługa najważniejszych aplikacji branżowych

Otwarta platforma aplikacyjna oraz proste funkcje przeglądarki w aparatach Polycom SpectraLink 8400 służą do obsługi specyficznych funkcji, takich jak np. systemy przywoławcze w szpitalach, kontrola stanów magazynowych w sklepach, jak również systemy monitorowania urządzeń w fabrykach przemysłowych. Telefony posiadają zintegrowany czytnik kodów kreskowych stanowiąc rozwiązanie łączące w sobie doskonałą jakość głosu, możliwość obsługi aplikacji oraz danych w odróżnieniu od innych platform aktualnie dostępnych na rynku.

Na przykład, w środowisku szpitalnym zintegrowany czytnik kodów kreskowych oraz interfejs umożliwia personelowi placówki szybkie skanowanie i transfer informacji zawartych w kodzie kreskowym umieszczonym np. na opakowaniu leków czy recepcie. Pozwala to ulepszyć praktyki medyczno-administracyjne, co z kolei pomoże zredukować liczbę błędów medycznych.

Konstrukcja dostosowana do potrzeb klientów

Aparaty Polycom SpectraLink 8400 zostały zaprojektowane przy aktywnym udziale klientów. Posiadają duży kolorowy wyświetlacz oraz prosty, intuicyjny interfejs użytkownika. Charakteryzują się dużą trwałością, jak również szeroką gamą akcesoriów.

Najniższy całkowity koszt użytkowania

Aparaty pełnią funkcję radia do komunikacji dwustronnej, pagera, skanera kodów kreskowych, intercomu, jak również wysokiej jakości aparatu do prowadzenia konferencji w jednym, w pełni zintegrowanym urządzeniu. Dzięki temu zapewniają nawet o 33 proc. niższy całkowity koszt użytkowania w porównaniu z rozwiązaniami konkurencyjnymi.

Wysoki poziom interoperacyjności oraz zgodność ze standardami

Telefony są zgodne ze standardami 802.11a/b/g/n radia oraz posiadają certyfikat Polycom Voice Interoperability for Enterprise Wireless (VIEW), dlatego mogą działać w infrastrukturach bezprzewodowych (LAN), jak również oferują wszechstronną obsługę serwera połączeń dla różnych platform UC.

Telefony Polycom SpectraLink 8400 będą w sprzedaży w pierwszej połowie 2011 roku w sieci autoryzowanych partnerów Polycom. ■

Polskie akcenty w badaniach jądrowych

Grzegorz Kantowicz

Mały Wielki Wybuch w CERN

Listopad 2010 roku na trwałe wpisze się w historię nauki. Naukowcom z Europejskiej Organizacji Badań Jądrowych po wielu miesiącach starań udało się odtworzyć warunki przypominające te, które panowały prawie 14 miliardów lat temu, czyli zaraz po Wielkim Wybuchu, który – według aktualnych teorii – dał początek Wszechświatowi. Naukowcy są zgodni – wydarzenie to jest wielkim sukcesem. Swój wkład w sukces Europejskiej Organizacji Badań Jądrowych mają także nasi rodacy – w CERN pracuje ponad 200 Polaków, a polskie serwery Actina Solar wspierają pracę Wielkiego Zderzacza Hadronów.

Wielki Zderzacz Hadronów (LHC) umieszczony jest od 50 do 175 m pod ziemią, na granicy francusko-szwajcarskiej. Akcelerator cząstek skonstruowany jest na planie torusa, a jego obwód wynosi 27 kilometrów. Wielki Zderzacz Hadronów jest najbardziej zaawansowanym i największym urządzeniem badawczym skonstruowanym do tej pory przez ludzi.

Dzięki eksperymentom z wykorzystaniem akceleratora cząstek naukowcy chcą odpowiedzieć na pytania dotyczące tajemnic wszechświata – jak powstał, czym jest ciemna energia, dlaczego materia ma masę.

Do tej pory Wielki Zderzacz Hadronów zderzał ze sobą protony. 7 listopada naukowcy rozpoczęli proces zderzania ze sobą jonów ołowiu – działania odbywały się w ramach eksperymentu o nazwie ALICE. W akceleratorze cząstek po raz pierwszy w historii zderzone zostały dwie wiązki ciężkich jonów ołowiu, w wyniku czego odnotowano powstanie tzw. „gorącej zupy", która według naukowców istniała przez krótką chwilę tuż po Wielkim Wybuchu. Podczas eksperymentu jony w Wielkim Zderzaczu Hadronów zderzyły się z prędkością zbliżoną do prędkości światła. Po kolizji, w miejscu zderzenia się jonów, na mikrosekundy powstają warunki, jakie panowały na początku Wszechświata.

Zaawansowane badania prowadzone w CERN wymagają zastosowania najnowszych rozwiązań technologicznych. Ich zadaniem jest wspieranie wysiłków naukowców w ich codziennej pracy.

Wśród maszyn wspomagających pracę Wielkiego Zderzacza Hadronów znajdują się także polskie urządzenia – najnowszym i największym spośród wszystkich wdrożeń przeprowadzonych przez polskie firmy w CERN jest dostawa do instytutu badawczego w Genewie 1132 serwerów marki Actina Solar. Bez wsparcia technologicznego nie byłaby możliwa analiza ogromnej liczby danych napływających z wielu detektorów – szacuje się, że każde zderzenie generuje petabajty danych (czyli biliardy bajtów – 1015). Serwery Actina Solar wykorzystywane są do analizowania, przetwarzania i magazynowania danych w CERN. ■

Sala kontroli eksperymentu w CERN

Tunel akcelatora cząstek

– Wytworzenie warunków zbliżonych do tych, które panowały po Wielkim Wybuchu, to wielkie osiągnięcie Europejskiej Organizacji Badań Jądrowych. Sukces naukowców z CERN jest także sukcesem polskiej nauki i myśli technologicznej. Trzeba pamiętać o tym, że w Europejskiej Organizacji Badań Jądrowych pracuje ponad 200 Polaków. Równie istotne jest to, że w pracę laboratorium CERN wspierają także polskie rozwiązania technologiczne – m.in. serwery Actina Solar, które zostały dostarczone przez firmę ACTION SA. Jestem dumny z tego, że Polacy biorą udział w tak ważnych dla nauki pracach prowadzonych przez Europejską Organizację Badań Jądrowych – mówi **Edward Wojtysiak**, Wiceprezes Zarządu firmy ACTION SA.

Jak zarabiać na sieciach mobilnych?

Piotr Czechowicz

Bliższe spojrzenie na business case dla LTE

Ewolucja do systemu LTE ma zasadniczo zmienić ekosystem mobilny, zarówno pod względem architektury, jak i od strony komercyjnej.

Projekt LTE dynamicznie się rozwija przy udziale największych dostawców sprzętu, którzy dostarczają już kompatybilne urządzenia dla klientów w Europie, Azji i Ameryce Północnej.

Wraz ze wzrostem zainteresowania nowym standardem, wszyscy członkowie ekosystemu telekomunikacji mobilnej, a szczególnie operatorzy, szczegółowo analizują business case dla projektu wdrożenia LTE.

Gdy ruszały pierwsze sieci 3G, dyskusje koncentrowały się na technologii, pomijając aspekt komercyjny.

W efekcie, wdrożenia UMTS u wielu operatorów mobilnych przyniosły wyniki finansowe dalekie od oczekiwań.

Mając to na uwadze, przed decyzją o szerszym zastosowaniu modelu LTE, należy krytycznie ocenić business case. Dostawcy usług pytają najczęściej: *Jaki będzie koszt inwestycji i jakie korzyści LTE zaoferuje?* W większości przypadków operatorzy poszukują odpowiedzi na te pytania oraz badają potencjał LTE poprzez próbne wdrożenia i testy.

Czy nadszedł właściwy czas, aby zainwestować w LTE? W jaki sposób operatorzy mogą wygenerować zyski z LTE, które uzasadnią tę inwestycję?

Ekonomiczne korzyści technologii LTE wynikają z nowych możliwości, jakie ona oferuje. Wyższe przepływności i małe opóźnienie znacząco poprawią wrażenia użytkownika z odbioru treści wymagających wysokich przepływności oraz innych wrażliwych aplikacji. Architektura All-IP zastosowana w LTE, wyższa efektywność widmowa oraz elastyczność w oferowanych szybkościach transmisji do użytkownika gwarantują poprawę ekonomiki sieci względem obecnych technologii.

Aby zrozumieć znaczenie nowych możliwości dla business case'u LTE, warto rozważyć ich potencjalny wpływ na użytkownika.

ARPU (*Average Revenue Per User*) w sieciach mobilnych obniża się. Na przykład, w Europie zachodniej ARPU obniżył się z 36 dolarów w 2007 roku do 32 dolarów dzisiaj. LTE ma odwrócić tą tendencję poprzez zaoferowanie nowych usług szerokopasmowych oraz innowacyjnych treści i aplikacji.

Jednakże przejście do architektury All-IP w LTE spowoduje, że bardzo atrakcyjnym modelem działalności stanie się *Over-the-top* (OTT). W tym modelu użytkownicy w coraz większym stopniu będą korzystać z aplikacji internetowych, np. Skype, istotnie ograniczając możliwości generowania przychodu przez operatora.

Architektura All-IP stworzy bardziej otwarte środowisko dla aplikacji OTT, które sprowadzają operatora do roli tzw. *bit pipe*. Aby oddalić to zagrożenie oraz wygenerować przychody z LTE, operatorzy muszą nawiązać partnerstwa z dostawcami treści i aplikacji, zbudować portale z aplikacjami (przykładem mogą być Google, Nokia, a nawet Samsung) i być może przygotować API w celu udostępnienia szerokich dodanych funkcjonalności sieci dostawcom aplikacji i treści za określoną opłatą. Zjawisko to obecnie potęguje się w związku z ogromną popularyzacją smartphone'ow.

Po stronie kosztów, jedną z zalet LTE jest możliwość wykorzystania infrastruktury sieci 3G. Maszty, okablowanie pozostają, a najnowocześniejsze stacje bazowe są już gotowe na LTE po aktualizacji oprogramowania. Dalsze oszczędności w LTE mogą być uzyskane poprzez powtórne użycie częstotliwości, ograniczając liczbę wymaganych licencji na nowe częstotliwości.

Architektura IP w LTE oraz szersze wykorzystanie Ethernetu w dostępie do stacji bazowych (*backhaul*) może znacznie ograniczyć koszty transmisji w przeliczeniu na 1 Mbps. Co więcej, wyższa efektywność widmowa LTE oraz elastyczne dopasowanie szybkości transmisji dla każdego użytkownika powinny ograniczyć liczbę lokalizacji stacji bazowych w sieci. Jednakże, z biegiem czasu, te korzyści mogą zostać ograniczone, gdy wykorzystanie usług wymagających wysokich przepływności transmisji wzrośnie, a operatorzy zwiększą gęstość komórek i przepływności sieci dostępowych, aby zbudować pokrycie i zapewnić odpowiednią jakość.

LTE ma potencjał innowacyjności, jaką sieci 3G ledwie zaczęły oferować. Pozostaje jednak pytanie, czy operatorzy będą w stanie przekształcić swój wertykalny model biznesowy w model oparty na wartości. To pytanie pozostaje otwarte.

Podsumowując, gdy rozpocznie się już migracja do LTE, stworzenie skutecznego modelu biznesowego, innowacyjnego środowiska we współpracy z partnerami oraz znalezienie źródeł przychodów pozostanie zadaniem dla operatorów. Przy braku odpowiedniego planu, grozi nam los, jaki spotkał wiele innych przedsięwzięć, które nie ewoluowały i nie dostosowały się do dynamicznego otoczenia. ■

Portugal Telecom i Alcatel-Lucent przeprowadzają pierwszy test

Grzegorz Kantowicz

Symetryczna technologia 10G GPON

Firma Alcatel-Lucent poinformowała o nawiązaniu współpracy z portugalskim operatorem Portugal Telecom, w ramach której zostaną przeprowadzone pierwsze w Europie testy symetrycznej gigabitowej pasywnej sieci optycznej (GPON – ang. Gigabit Passive Optical Network) 10 Gb/s.

Dzięki tej technologii można wykorzystać szybkie połączenia szerokopasmowe – 10 Gb/s w obu kierunkach – aby udostępnić użytkownikom indywidualnym i klientom biznesowym zaawansowane innowacyjne usługi. Zgodnie z zawartym porozumieniem, firma Portugal Telecom rozpoczęła już testowanie łączy szerokopasmowych, których szybkość pozwoli użytkownikom zapisać w zdalnej lokalizacji zawartość dysku twardego o pojemności 200 GB w ciągu trzech minut.

Zalety symetrycznej technologii 10G GPON tkwią w potencjale jej przepustowości – zarówno w przypadku pobierania, jak i wysyłania danych. Szybkość wysyłania danych będzie zyskiwać na znaczeniu wraz z pojawieniem się na rynku takich usług, jak przetwarzanie przez Internet (ang. *cloud computing*), zdalna pamięć masowa (prowadząca do znacznego wzrostu liczby wysyłanych plików), aplikacje udostępniane jako usługi (SaaS – ang. *Software as a Service*), w przypadku których oprogramowanie, takie jak edytory tekstu, jest uruchamiane na zdalnych serwerach zamiast na komputerach osobistych, a także backhauling sieci komórkowych, w tym technologia LTE.

– *Firma Portugal Telecom zajmuje czołową pozycję w zakresie innowacyjnych usług i technologii. Dużo inwestuje w światłowodowe łącza abonenckie FTTH, korzystając przy tym z technologii GPON, aby zapewnić swoim klientom największą przepustowość i najwyższą jakość usług* – powiedział **Alfredo Baptista**, dyrektor ds. technicznych w firmie Portugal Telecom. – *Wraz z szybkim wzrostem wymagań w zakresie usług i przepustowości niezbędne jest nieustanne analizowanie i testowanie najnowszych innowacji, takich jak symetryczna technologia 10G GPON, którą Alcatel-Lucent dostarcza do tych testów.*

Ponadto (symetryczna) technologia 10G GPON jest w stanie funkcjonować wraz z obecnie stosowaną technologią GPON w ramach tej samej sieci dostępowej. Dzięki temu intensywne użytkowanie nowej technologii nie wpływa na istniejące łącza optyczne poza centralą.

To ważny argument dla operatorów z całego świata, którzy inwestują dziś w technologię GPON.

– *Firma Portugal Telecom działa na niezwykle konkurencyjnym rynku i już wiele zainwestowała w technologię GPON. Potwierdzenie, że technologia ta umożliwia sprawną, bezzakłóceniową modernizację sieci do rozwiązań nowej generacji, ma więc kluczowe znaczenie zarówno dla Portugal Telecom, jak i dla wszystkich innych operatorów* – powiedział **Dave Geary**, szef działu sieci przewodowych w firmie Alcatel-Lucent. – *Portugal Telecom i Alcatel-Lucent wspólnie przeprowadzają testy symetrycznej technologii 10G GPON – pierwsze w Europie i oparte na funkcjonującej już współpracy w zakresie rozwiązań GPON. Celem testów jest udowodnienie, że technologia ta faktycznie umożliwia bezproblemową modernizację, na której tak zależy operatorom, i że poradzi sobie ona z usługami oferowanymi przez nich w przyszłości.*

Alcatel-Lucent tworzy najnowocześniejsze technologie na długo przed ich ustandaryzowaniem. W tym roku firma zdobyła na konferencji FTTH Council nagrodę Innovation Award w kategorii *„Innowacji technicznych”* za swoje rozwiązanie 10G GPON, oparte na platformie dostępu IP ISAM (ang. *Intelligent Services Access Manager*).

Standardy symetrycznej technologii 10G GPON wciąż nie są dostępne, jednak Alcatel-Lucent pokazał, że jest ona już gotowa i może, w razie potrzeby, zapewnić większą prze-pływność w sieciach dostępowych klientów. ■

Narzędzia operatorskie

Piotr Czechowicz

Juniper Networks dla bezpieczeństwa mobilnego

Osobiste urządzenia mobilne szybko stają się standardem w dostępie do sieci korporacyjnych, będąc tym samym newralgicznym punktem bezpieczeństwa danych biznesowych, jak i osobistych. Po raz pierwszy przy użyciu oprogramowania Junos Pulse Mobile Security Suite, konsumenci oraz przedsiębiorstwa otrzymują rozwiązanie zapewniające pełną ochronę i zabezpieczenie wyników swojej pracy i danych osobistych, co otwiera nowe możliwości dla całego rynku mobilnego.

Piotr Czechowicz – Regional Manager EE, Juniper Networks

Na przełomie października i listopada 2010 Juniper przedstawił Junos Pulse, zestaw oprogramowania bezpieczeństwa do ochrony urządzeń mobilnych w zastosowaniach biznesowych a także domowych. Mobile Security Suite, zbudowane w oparciu o rozwiązanie SSL VPN, jest częścią większej platformy Junos Pulse Mobile Security Suite i zintegrowanym rozwiązaniem na rynku do ochrony wszystkich urządzeń mobilnych. Pozwala ono przedsiębiorstwom zagwarantować pracownikom bezpieczeństwo dostępu do korporacyjnych aplikacji lub poczty na praktycznie każdym urządzeniu mobilnym. Operatorom daje narzędzie bezpieczeństwa dla klientów i firm korzystających ze smartphone'ów, a także zapewnia ochronę dzieci przed dostępem do nieodpowiednich treści.

Na zlecenie Juniper Networks KRC Research oraz Synovate przeprowadziły badanie na grupie 6 000 użytkowników smartphone'ów i tabletów w 16 krajach. Wyniki badania wskazują na zanikającą granicę między korzystaniem z urządzeń mobilnych w celach prywatnych lub biznesowych i podkreślają potrzebę silniejszych i bardziej zintegrowanych zabezpieczeń dla tego typu rozwiązań.

Badanie pokazało, że 81 proc. ankietowanych łączy się z korporacyjną siecią bez wiedzy lub zezwolenia pracodawcy, a 58 proc. z nich robi to codziennie. Ponadto ponad 80 proc. właścicieli urządzeń mobilnych przechowuje na nich dane osobiste – w tym wrażliwe informacje, dotyczące stanu zdrowia czy finansów.

Z Pulse Mobile Security Suite operatorzy mogą zapewnić bezpieczeństwo tych danych i zaoferować usługę dodaną ochrony przed wirusami, spamem, ochronę przed nieodpowiednimi treściami, złośliwym oprogramowaniem itd. Klienci będą mogli również zlokalizować zagubione lub skradzione urządzenie wykorzystując posiadany przez nie GPS lub zdalnie usunąć wszystkie dane.

Platforma pozwala operatorom zaoferować klientom usługi oparte na chmurze, ale również wykorzystać tę samą inwestycję, aby dostarczyć przedsiębiorstwom wiodące rozwiązanie SSL VPN oraz bezpieczeństwo mobilne.

Pierwsze na świecie centrum badania zagrożeń bezpieczeństwa mobilnego

Ośrodek mający swoją siedzibę w Columbus (Ohio) jest pierwszym i jedynym na świecie centrum, które śledzi i odpowiada na zagrożenia bezpieczeństwa osobistych, firmowych czy wrażliwych informacji. Podstawowym zadaniem Juniper Global Threat Center jest monitorowanie i odpowiadanie na pięć najważniejszych typów zagrożeń, takich jak złośliwe oprogramowanie, bezpośrednie ataki, fizyczne zagrożenie, przechwycenie danych czy nieprawidłowe korzystanie z urządzenia.

Centrum powstało z Threat Center działającego w ramach SMobile Systems, który od ponad siedmiu lat prowadzi badania dotyczące bezpieczeństwa mobilnego. Ośrodek zatrudnia ekspertów rynku posiadających szeroką wiedzę i doświadczenie w dziedzinie bezpieczeństwa mobilnego. Pracownicy centrum posiadają następujące certyfikaty: Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) oraz Certified Hacking Forensic Investigator (CHFI). Zespół regularnie publikuje artykuły dotyczące tematyki bezpieczeństwa oraz wykłada na konferencjach IT na całym świecie.

Oprogramowanie Junos Pulse wprowadza nowy poziom bezpieczeństwa do mobilnych urządzeń końcowych. Użytkownicy przechowują na smartphonach emaile, kontakty, dane finansowe i inne wrażliwe aplikacje.

Większość z nich nie zdaje sobie jednak sprawy z konsekwencji zgubienia lub kradzieży telefonu. Global Threat Center dzięki szerokiej aktywności w obszarze bezpieczeństwa przyczynia się do bardziej kompleksowego potraktowania tych zagadnień i opracowania rozwiązań, które zapewnią wysoką ochronę przed istniejącymi i nowymi zagrożeniami. ■

Fortinet wzmacnia bezpieczeństwo usług w chmurze

Grzegorz Kantowicz

Nowa rodzina wirtualnych rozwiązań

Fortinet przedstawił cztery nowe rozwiązania, które umożliwiają dostarczanie usług „cloud computing" zapewniając bezpieczeństwo wirtualnych środowisk. Zwirtualizowane systemy FortiGate, FortiManager, FortiAnalyzer i FortiMail adresowane są głównie do administratorów dużych sieci i operatorów oferujących swoje usługi w chmurze.

Nowe, wirtualne FortiGate®, FortiManager™, FortiAnalyzer™ i FortiMail™ zostały zaprojektowane do pracy w zgodzie z technologią VMware ESX oraz ESXi. Zwirtualizowane modele współpracują ze swoimi sprzętowymi odpowiednikami dając możliwość wyboru między formą fizyczną a wirtualną w celu eliminowania zagrożeń płynących ze stref niekontrolowanych i gwarantując zarządzanie bezpieczeństwem w środowiskach infrastruktury zwirtualizowanej. Połączone rozwiązanie zapewnia lepszą integrację ze środowiskami wirtualnymi i pozwala chronić usługi oferowane w zwirtualizowanej strukturze sieciowej.

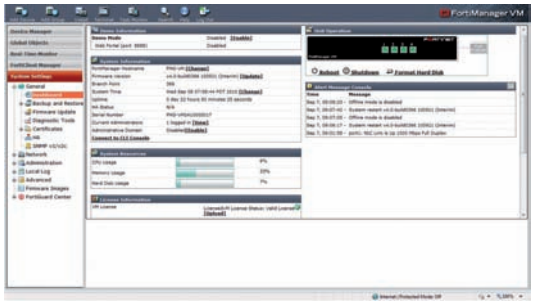
Wirtualny FortiGate, podobnie jak tradycyjne modele, stanowi zintegrowaną wirtualną bramę bezpieczeństwa chroniąc infrastrukturę przed wieloma zagrożeniami. Rozwiązanie umożliwia integrację dotąd oddzielnych technologii oraz ogranicza koszty i stopień złożoności infrastruktury bezpieczeństwa. Klienci mogą połączyć zaporę sieciową, funkcję VPN, mechanizm zapobiegania penetracji, zapobiegania oprogramowaniu złośliwemu, zabezpieczenia aplikacji i kompleksową ochronę treści, mechanizm zapobiegania utracie danych, filtrowanie sieci WWW czy funkcje przeciwspamowe i mają dodatkową możliwość kontroli ruchu międzystrefowego. Ponadto wirtualny FortiGate może być używany w powiązaniu z tradycyjnymi urządzeniami FortiGate w celu zapewnienia ochrony zarówno w warstwie brzegowej, jak i w wirtualnych strefach bezpieczeństwa.

Wirtualny FortiManager dostarcza narzędzi niezbędnych do skutecznego zarządzania infrastrukturą bezpieczeństwa. Bazując na zdefiniowanych strategiach, rozwiązanie oferuje scentralizowane udostępnianie, konfigurację i zarządzanie aktualizacjami dla FortiGate, FortiWiFi i FortiMail, jak również dla agentów punktów końcowych FortiClient.

Wirtualny FortiAnalyzer bezpiecznie agreguje dane z dzienników urządzeń Fortinet i innych urządzeń kompatybilnych z narzędziem syslog. Dzięki zastosowaniu kompleksowego systemu raportowania użytkownicy mogą filtrować i przeglądać raporty, łącznie ze sprawozdaniami dotyczącymi ruchu, zdarzeń, wirusów, ataków, treści WWW i danych poczty elektronicznej oraz uszczegóławiać dane w celu określenia sytuacji bezpieczeństwa i zapewnienia zgodności z wymogami regulacyjnymi.

FortiAnalyzer udostępnia również zaawansowane funkcje zarządzania bezpieczeństwem, takie jak archiwizacja plików poddanych kwarantannie, korelowanie zdarzeń, ocena punktów wrażliwych, analiza ruchu oraz archiwizacja treści poczty elektronicznej, dostępu do sieci WWW, komunikatorów internetowych oraz przesyłu plików.

Wirtualny FortiMail do ochrony poczty elektronicznej został zaprojektowany w celu blokowania przychodzącego spamu i oprogramowania złośliwego, zanim zdoła ono zakorkować sieć i zainfekować użytkowników. Urządzenie pomaga również zapobiegać wysyłaniu spamu lub oprogramowania złośliwego (w tym również w ruchu mobilnym 3G), co może spowodować, że inne bramki przeciwspamowe umieszczą użytkowników na czarnych listach.



Wirtualne rozwiązania Fortinet pracują w sposób zbliżony do swoich fizycznych odpowiedników – firma Fortinet w dalszym ciągu udostępnia technologie domeny wirtualnej (*Virtual Domain*, VDOM) oraz domeny administracyjnej (*Administrative Domain*, ADOM) do celów zabezpieczania i zarządzania środowiskami wirtualnymi i obsługującymi wielu dzierżawców.

Technologie wirtualizacji współpracują z branżowymi standardami dla sieci VLAN (wirtualna sieć LAN), dzięki czemu jedno wirtualne lub fizyczne urządzenie Fortinet jest w stanie obsługiwać setki domen leżących w obrębie środowiska, zapewniając niezbędną widoczność i możliwości kontroli zabezpieczeń między strefami, a jednocześnie zachowując wszelkie korzyści płynące z wirtualizacji.

Fortinet zajmuje się ochroną wirtualnej architektury sieciowej od wprowadzenia technologii domeny wirtualnej (VDOM) w 2004 roku. Firma rozszerzyła swoje kompetencje w zakresie wirtualizacji po nabyciu w 2006 roku praw do własności intelektualnej i technologii CoSine Communications, jednego z pierwszych liderów branży wirtualnych urządzeń.

Dzięki stosowaniu tych rozwiązań, dostawcy usług mają do dyspozycji wysokiej klasy platformę zwirtualizowanych usług bezpieczeństwa sieci. Duże przedsiębiorstwa z pełnym zaufaniem korzystają z technologii Fortinet w celu ochrony danych w ich prywatnych i hybrydowych chmurach.

Wirtualne urządzenia FortiGate i FortiManager są już dostępne w Polsce. Obecnie dostępne są trzy opcje licencjonowania, które reprezentują trzy wirtualne modele systemu FortiGate-VM. Każdy model licencjonowany jest na określoną liczbę wirtualnych procesorów (vCPU): 2, 4 lub 8. Do każdego modelu – tak jak w wersji sprzętowej systemów FortiGate – należy doliczyć serwisy FortiCare oraz subskrypcję FortiGuard. ■

Cybernetyczny ekspert

Oleg Zajcew

Sztuczna inteligencja w świecie bezpieczeństwa IT

Czy da się opisać ludzką inteligencję wystarczająco precyzyjnie, aby można było ją naśladować przy użyciu maszyn? To pytanie nadal stanowi kość niezgody wśród naukowców. Naukowcy próbujący stworzyć sztuczną inteligencję stosują różne podejścia, wielu jednak sądzi, że kluczem do sukcesu są sztuczne sieci neuronowe. Jak na razie żadne urządzenie zawierające sztuczną inteligencję nie przeszło testu Turinga. Według sławnego brytyjskiego informatyka Alana Turinga, maszyna może zostać uznana za inteligentną, jeżeli użytkownik nie jest w stanie rozróżnić, czy ma do czynienia z maszyną czy z innym człowiekiem. Jednym z możliwych obszarów zastosowań całkowicie autonomicznej sztucznej inteligencji jest wirusologia komputerowa oraz rozwój systemów do zdalnego leczenia zainfekowanych komputerów.

Głównym zadaniem stojącym dzisiaj przed naukowcami zajmującymi się sztuczną inteligencją jest stworzenie autonomicznego urządzenia, które potrafi uczyć się, podejmować inteligentne decyzje oraz modyfikować własne zachowanie w zależności od zewnętrznych bodźców. Stworzenie takich wysoko wyspecjalizowanych systemów jest możliwe, podobnie jak prawdopodobne jest zbudowanie bardziej uniwersalnych i złożonych urządzeń opartych na sztucznej inteligencji, jednak takie systemy zawsze opierają się na doświadczeniu i wiedzy człowieka w postaci wzorców, reguł i algorytmów zachowania.

Dlaczego tak trudno stworzyć autonomiczną sztuczną inteligencję? Dlatego, że maszyna nie posiada typowo ludzkich cech, takich jak świadomość, intuicja, umiejętność rozróżniania między rzeczami ważnymi i tymi mniej istotnymi oraz – co najważniejsze – chęć zdobywania nowej wiedzy. Wszystkie te cechy pozwalają człowiekowi rozwiązywać problemy, nawet gdy nie są one linearne. Wykonanie jakiegokolwiek działania przez sztuczną inteligencję wymaga obecnie algorytmów stworzonych przez człowieka. Mimo to, naukowcy wciąż próbują stworzyć prawdziwie sztuczną inteligencję i niekiedy odnoszą pewne sukcesy.

Koszty nieautomatycznego przetwarzania

Proces wykrywania szkodliwego oprogramowania i przywracania normalnych parametrów operacyjnych na komputerze składa się z trzech głównych kroków. Nie ma tu znaczenia, kto lub co podejmuje te kroki: człowiek czy maszyna. **Pierwszy krok** obejmuje gromadzenie obiektywnych danych o badanym komputerze oraz działających na nim programach. Ten krok najlepiej przeprowadzić przy użyciu szybkiego automatycznego sprzętu, który potrafi generować raporty nadające się do przetwarzania automatycznego oraz działać bez interwencji człowieka.

W **drugim kroku** zebrane dane są poddawane szczegółowej analizie. Na przykład, jeżeli raport zawiera informację o wykryciu podejrzanego obiektu, taki obiekt należy poddać kwarantannie i dokładnej analizie w celu określenia, jakie stanowi zagrożenie, a następnie trzeba podjąć decyzję odnośnie do dalszych działań.

Trzeci krok stanowi rzeczywistą procedurę rozwiązania problemu, dla której można wykorzystać specjalny język skryptowy. Zawiera ona polecenia niezbędne do usunięcia wszelkich szkodliwych plików oraz przywrócenia prawidłowych parametrów operacyjnych komputera.

Jeszcze kilka lat temu **kroki 2** i **3** były wykonywane jedynie przez analityków firm bezpieczeństwa IT oraz ekspertów działających na wyspecjalizowanych forach niemal bez użycia jakiejkolwiek automatyzacji. Jednak wraz ze wzrostem liczby użytkowników padających ofiarą szkodliwego oprogramowania, a tym samym potrzebujących specjalistycznej pomocy, pojawiło się wiele problemów:

- Jeżeli protokoły i pliki kwarantanny są przetwarzane ręcznie, analityk wirusów otrzymuje ogromne ilości nieustannie zmieniających się informacji, które wymagają zintegrowania i pełnego zrozumienia – taki proces nie może być szybki.
- Człowiek posiada naturalne ograniczenia psychiczne i fizjologiczne. Specjalista może zmęczyć się i popełnić błąd; im bardziej złożone zadanie, tym większe prawdopodobieństwo popełnienia błędu. Na przykład przeciążony pracą ekspert od szkodliwego oprogramowania może pominąć szkodliwy program lub usunąć nieszkodliwą aplikację.
- Analiza plików umieszczonych w kwarantannie jest bardzo czasochłonną operacją, ponieważ ekspert musi przeanalizować unikatowe cechy każdej próbki – tj. gdzie i w jaki sposób pojawiła się i co jest w niej podejrzanego.

Jedynym rozwiązaniem tych problemów jest całkowita automatyzacja analizy oraz leczenia szkodliwego oprogramowania, jednak dotychczasowe próby wykorzystujące różne algorytmy nie przyniosły pozytywnych rezultatów. Głównym powodem tych niepowodzeń jest nieustanna ewolucja szkodliwego oprogramowania oraz fakt, że każdego dnia w Internecie pojawiają się dziesiątki nowych szkodliwych programów wykorzystujących coraz bardziej wyrafinowane metody osadzania się i ukrywania. Dlatego algorytmy wykrywania muszą być niezwykle złożone. Sprawę komplikuje ponadto fakt, że algorytmy

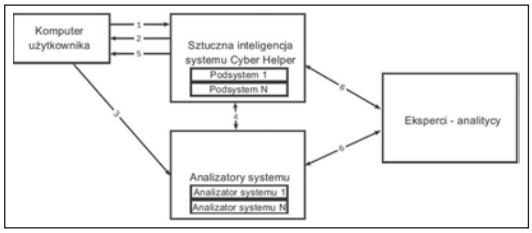
te bardzo szybko dezaktualizują się – należy je nieustannie aktualizować i usuwać z nich błędy. Kolejnym problemem jest to, że skuteczność każdego algorytmu ograniczają umiejętności jego twórców.

Nieco skuteczniejsze wydaje się wykorzystanie do „łapania wirusów" systemów eksperckich. Jednak twórcy antywirusowych systemów eksperckich borykają się z podobnymi problemami do tych wymienionych wyżej – skuteczność takiego systemu zależy od jakości wykorzystywanych przez niego reguł i baz wiedzy. Ponadto bazy wiedzy muszą być nieustannie aktualizowane, co wymaga inwestycji w zasoby ludzkie.

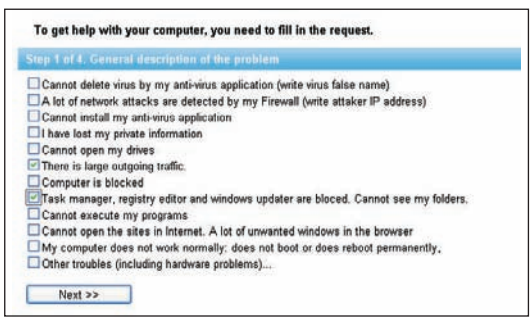
Ogólne zasady działania systemu Cyber Helper

Mimo trudności, z upływem czasu eksperymenty prowadzone na omawianym polu dały pewne pozytywne wyniki. Przykładem jest stworzenie systemu Cyber Helper, który stanowi udany krok w kierunku wykorzystywania w walce ze szkodliwym oprogramowaniem prawdziwie autonomicznej sztucznej inteligencji. Większość autonomicznych podsystemów Cyber Helpera potrafi zsynchronizować się, wymieniać dane i współdziałać ze sobą, jak gdyby były jednością. Naturalnie, zawierają one pewne „twarde" algorytmy i reguły – tak jak konwencjonalne programy – jednak w większości działają z wykorzystaniem logiki rozmytej i w trakcie rozwiązywania różnych zadań niezależnie definiują swoje zachowanie.

W samym sercu systemu Cyber Helper znajduje się narzędzie o nazwie AVZ, które zostało stworzone przez autora tego artykułu w 2004 roku. Celem AVZ jest automatyczne gromadzenie danych z potencjalnie zainfekowanych komputerów, jak również próbek szkodliwego oprogramowania i przechowywanie ich w postaci nadającej się do przetwarzania automatycznego do użytku innych podsystemów. AVZ tworzy raporty w formacie HTML przeznaczone do analizy przez człowieka oraz w formacie XML – do analizy maszynowej. Od roku 2008 główny program AVZ jest integrowany do rozwiązań antywirusowych firmy Kaspersky Lab.



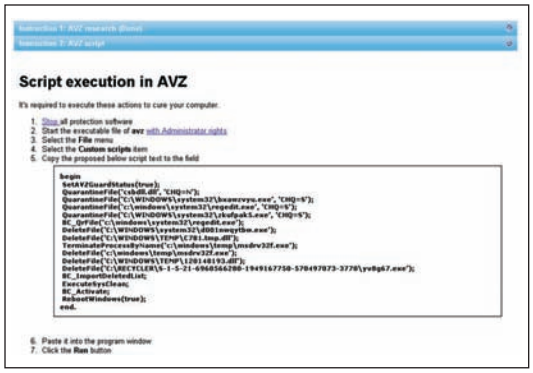
Ogólny algorytm działania systemu Cyber Helper – kroki 1-6



W przypadku żądania leczenia należy dostarczyć odpowiedzi na wszystkie pytania dotyczące systemu

Algorytm działania systemu składa się z sześciu kroków. W pierwszym kroku główny program AVZ wykonuje skanowanie antywirusowe zainfekowanego komputera, a uzyskane wyniki w formacie XML przesyła do innych podsystemów Cyber Helpera w celu analizy.

System analizuje otrzymany protokół przy użyciu ogromnej ilości dostępnych danych dotyczących podobnych szkodliwych programów oraz wcześniejszych działań naprawczych podjętych w podobnych przypadkach, jak również innych czynników. Pod tym względem Cyber Helper przypomina aktywny mózg ludzki, który w celu przetworzenia informacji musi zgromadzić wiedzę o otoczeniu. Aby dziecko mogło się w pełni rozwinąć, musi być stale świadome tego, co się dzieje w jego świecie, i móc komunikować się z innymi ludźmi. W tym przypadku maszyna posiada przewagę nad człowiekiem, ponieważ w określonym przedziale czasowym potrafi przechowywać, wydobywać i przetwarzać znacznie większe ilości informacji niż ludzie.



Przykład instrukcji i skryptu leczenia/poddawania kwarantannie napisany przez system Cyber Helper bez udziału człowieka

Kolejnym podobieństwem pomiędzy systemem Cyber Helper a człowiekiem jest to, że Cyber Helper potrafi niezależnie i niemal bez żadnej podpowiedzi rozpocząć proces analizy protokołu, jak również nieustannie uczyć się w stale zmieniającym się środowisku. Jeżeli chodzi o samodzielne uczenie się, Cyber Helper musi popracować nad trzema głównymi problemami: błędy ekspertów-ludzi, których maszyna nie jest w stanie rozwiązać, ponieważ nie jest wystarczająco intuicyjna; fragmentaryczność i niespójność informacji programu oraz wielokrotne uściślenia danych i opóźnienia we wprowadzaniu danych do systemu. Przyjrzyjmy się tym kwestiom bliżej.

Trudności implementacji

Eksperci przetwarzający protokoły i pliki poddane kwarantannie mogą popełniać błędy lub wykonywać działania, których nie można wyjaśnić logicznie z perspektywy maszyny. Oto typowy przykład: jeżeli specjalista widzi w protokole nieznany plik o nazwie %System32%\ntos.exe, który posiada cechy szkodliwego oprogramowania, usuwa go bez dalszej ana-

lizy czy poddawania go kwarantannie, opierając się na swoim doświadczeniu oraz intuicji. Dlatego szczegóły działań wykonywanych przez specjalistów oraz sposób, w jaki doszli do swoich wniosków, nie zawsze można bezpośrednio przełożyć na postać umożliwiającą uczenie maszyny. Informacje dotyczące leczenia często mogą być niekompletne lub sprzeczne. Na przykład, przed poproszeniem o pomoc eksperta użytkownik mógł próbować samodzielnie naprawić problem na swoim komputerze i usunął tylko część szkodliwego programu – przywracając pliki zainfekowanego programu bez wyczyszczenia rejestru. Trzeci typowy problem: podczas procedury analizy protokołu dostępne są tylko metadane z podejrzanego obiektu, natomiast po analizie pliku poddanego kwarantannie – tylko informacje początkowe o podejrzanym obiekcie. Następnie przeprowadzana jest kategoryzacja obiektu – albo jest on szkodliwy, albo „czysty". Takie informacje są zwykle dostępne dopiero po wielokrotnym uściśleniu i po długim czasie – wynoszącym od kilku minut do kilku miesięcy. Proces definiowania może odbywać się zarówno zewnętrznie, w laboratorium usług analitycznych, jak i wewnątrz własnych podsystemów Cyber Helpera.

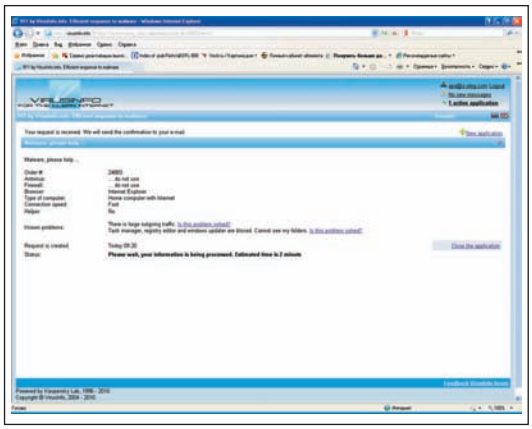
Oto typowy przykład: analizator sprawdza plik, ale nie znajduje w jego zachowaniu nic groźnego i przekazuje tę informację do systemu Cyber Helper. Po pewnym czasie analizator zostaje udoskonalony i powtórnie przeprowadza analizę badanego wcześniej podejrzanego pliku, z tym że tym razem wydaje inny werdykt. Podobny problem może dotyczyć wniosków wyciąganych przez wyspecjalizowanego analityka wirusów dla programów, których klasyfikacja jest problematyczna, na przykład programów do zdalnych systemów zarządzania lub narzędzi zacierających ślady użytkownika – ich klasyfikacja może zmienić się po opublikowaniu kolejnej wersji. Ze względu na wspomnianą wyżej właściwość – zmienność i niejednoznaczność parametrów analizowanych programów, wszelkie decyzje podejmowane przez Cyber Helpera opierają się na ponad pięćdziesięciu niezależnych analizach.

Na podstawie dostępnych informacji analizator Cyber Helper dostarcza wiele hipotez odnośnie do tego, który z obiektów znajdujących się w protokole może stanowić zagrożenie, a który można dodać do bazy „czystych" plików. Na podstawie tych hipotez AVZ automatycznie pisze skrypty odpowiadające za umieszczanie w kwarantannie podejrzanych obiektów. Następnie skrypt jest przesyłany do maszyny użytkownika w celu wykonania. (**Krok 2** ogólnego algorytmu działania systemu Cyber Helper).

Na etapie pisania skryptu inteligentny system może wykryć dane, które są wyraźnie szkodliwe. W takim przypadku skrypt może włączyć polecenie usunięcia znanych szkodliwych programów lub odwołać się do specjalnych procedur cofnięcia szkody z systemu. Takie sytuacje mają miejsce dość często i wynikają z tego, że Cyber Helper jednocześnie przetwarza setki żądań; jest to typowe w sytuacjach, gdy kilku użytkowników zostało zainfekowanych tym samym szkodnikiem i ich maszyny proszą o pomoc. Po otrzymaniu i przeanalizowaniu wymaganych próbek z maszyny jednego z takich użytkowników Cyber Helper może dostarczyć innym użytkownikom skrypty leczenia, całkowicie pomijając etap kwarantanny, a tym samym oszczędzając czas użytkownika i zmniejszając ruch danych. Obiekty otrzymane od użytkownika są analizowane pod kontrolą systemu Cyber Helper, a wyniki tej analizy, niezależnie od tego, jakie są, zasilają jego bazę wiedzy. W ten sposób inteligentna maszyna może sprawdzić dowolne hipotezy sformułowane w **kroku 1** ogólnego algorytmu działania, potwierdzając lub odrzucając ich wynik.

Techniczne podsystemy Cyber Helpera

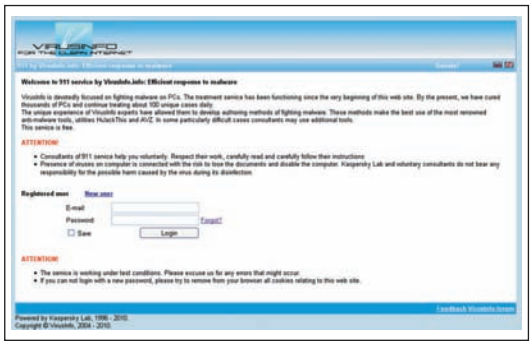
Główne podsystemy Cyber Helpera to autonomiczne jednostki analizujące pliki programów pod względem zawartości i zachowania. Dzięki nim Cyber Helper może analizować szkodliwe programy oraz uczyć się na wynikach swoich działań. Jeżeli analiza wyraźnie potwierdza, że dany obiekt jest szkodliwy, jest on przesyłany do laboratorium antywirusowego z mocnym zaleceniem umieszczenia go w antywirusowej bazie danych; następnie tworzony jest skrypt leczenia dla użytkownika (**krok 5** ogólnego algorytmu). Należy zauważyć, że pomimo analizy obiektu Cyber Helper nie zawsze jest w stanie podjąć kategoryczną decyzję odnośnie do szkodliwości obiektu. W takiej sytuacji wszystkie zebrane dane początkowe i wyniki są przekazywane ekspertowi w celu analizy (**krok 6**). Następnie ekspert dostarcza odpowiednie rozwiązanie. Cyber Helper nie bierze udziału w tym procesie, nadal jednak analizuje otrzymane dane i protokoły, generując raporty dla eksperta, tym samym wykonując lwią część jego pracy.



Po sformułowaniu żądania system po raz kolejny wyświetla je operatorowi w celu sprawdzenia, czy wszystkie dane wejściowe są poprawne

Jednak „polityka nieinterweniowania" systemów sztucznej inteligencji w pracę analityka szkodliwego oprogramowania nie zawsze jest stosowana; znamy dziesiątki przypadków, gdy inteligentna maszyna wykryła błędy w działaniu człowieka dzięki odwołaniu się do zgromadzonego doświadczenia oraz wyników własnej analizy obiektu. W takich przypadkach maszyna może najpierw przerwać proces analityczny i decyzyjny i wysłać ekspertowi ostrzeżenie, zanim przejdzie do zablokowania skryptów wysłanych użytkownikowi, co z perspektywy maszyny mogłoby zaszkodzić systemowi użytkownika. Podobną kontrolę maszyna sprawuje nad własnymi

działaniami. W czasie rozwijania skrypty leczenia są jednocześnie oceniane przez inny podsystem w celu wyeliminowania błędów. Najprostszym przykładem takiego błędu jest zastąpienie przez szkodliwy program ważnego składnika systemu. Z jednej strony, konieczne jest zniszczenie szkodliwego programu, z drugiej – może to spowodować nieodwracalną szkodę w systemie.



Z usług 911 dostępnych na stronie VirusInfo mogą korzystać wszyscy

Obecnie Cyber Helper jest zintegrowany z portalem antywirusowym http://virusinfo.info i stanowi podstawę eksperymentalnego systemu 911 http://virusinfo.info/911test/. W „systemie 911" Cyber Helper komunikuje się bezpośrednio z użytkownikiem: żądając protokołów, analizując je, pisząc skrypty skanowania wstępnego oraz przeprowadzenia analizy plików poddanych kwarantannie. Zgodnie z wynikami swojej analizy maszyna może przeprowadzić leczenie zainfekowanego komputera. Co więcej, Cyber Helper pomaga ekspertom w ich pracy, znajdując i eliminując wszelkie niebezpieczne błędy, przeprowadzając wstępne analizy wszystkich plików umieszczonych w kwarantannie przez ekspertów oraz przetwarzając dane zawarte w kwarantannie przed dodaniem ich do bazy „czystych" plików. Technologia, na której opiera się Cyber Helper, jak również jej zasada działania są chronione patentami firmy Kaspersky Lab.

Wnioski

Współczesne szkodliwe programy działają i rozprzestrzeniają się w niezwykle szybkim tempie. Natychmiastowa reakcja na tego typu programy wymaga inteligentnego przetwarzania dużej ilości niestandardowych danych. Sztuczna inteligencja idealnie nadaje się do tego zadania, ponieważ potrafi przetwarzać dane o wiele szybciej niż człowiek. Cyber Helper to efekt jednej z niewielu udanych prób przybliżenia się do celu, jakim jest stworzenie autonomicznej sztucznej inteligencji. Jako inteligentny twór, Cyber Helper jest zdolny do samodzielnego uczenia się i niezależnego definiowania swoich działań. Analitycy wirusów i inteligentne maszyny rewelacyjnie dopełniają się – dzięki współpracy działają efektywniej i zapewniają użytkownikom większą ochronę.

Autor jest ekspertem w firmie Kaspersky Lab

Jeszcze bliżej potencjalnego klienta

Grzegorz Kantowicz

Jak śledzić interakcje w mediach społecznościowych?

Firma Cisco Systems poinformowała o wprowadzeniu na rynek oprogramowania Cisco® SocialMiner, które pozwala firmom wyszukiwać i z wyprzedzeniem reagować na potrzeby obecnych i potencjalnych klientów komunikujących się za pośrednictwem publicznych sieci społecznościowych, takich jak Twitter i Facebook oraz innych forów lub serwisów blogerskich. Oprogramowanie umożliwia monitorowanie w czasie rzeczywistym zmian statusu, wpisów na forach i blogach klientów oraz powiadamianie przedsiębiorstw o rozmowach dotyczących ich marki. Oferowane przez Cisco rozwiązanie pozwala firmom nie tylko monitorować sieci społecznościowe w celu skuteczniejszej analizy danych biznesowych, ale także nawiązywać kontakt z klientami.

Według Nielsena w serwisie Tweeter co godzinę pojawia się ponad 1 milion wpisów (tzw. tweetów), a 34 proc. Amerykanów mających dostęp do Internetu korzysta z Facebooka, Twittera lub innych mediów społecznościowych, aby wygłaszać opinie na temat produktów, firm i marek. Za pośrednictwem platform społecznościowych prowadzi się teraz coraz więcej rozmów internetowych, dlatego szczególnie ważne jest, aby firmy mogły dowiadywać się, co ich klienci o nich mówią, oraz reagować na pytania ogólne i eliminować problemy z obsługą klientów, dbając o upowszechnienie i reputację swojej marki.

Firmy z całego świata wykorzystują technologię Cisco Contact Center do rutynowej obsługi milionów kontaktów z klientami dziennie, w tym połączeń głosowych i wideo, poczty elektronicznej, czatów i interakcji internetowych. Obserwuje się prawdziwy boom mediów społecznościowych, ale firmy korzystają z nich ad hoc, w sposób nieusystematyzowany i bez możliwości skalowania. Doświadczenia w dziedzinie zapewniania sprawności operacyjnej i technologii skalowania sieci pozwalają oferować przedsiębiorstwom rozwiązanie klasy korporacyjnej do prewencyjnej opieki nad klientami korzystającymi z mediów społecznościowych.

Firma Cisco poinformowała również o wprowadzeniu do oferty rozwiązania Cisco Finesse – jest to pulpit do współpracy w technologii Web 2.0 przeznaczony dla agentów obsługujących klientów. Rozwiązanie to zestawia wszystkie potrzebne agentom informacje w postaci jednej, możliwej do zmodyfikowania konsoli, dzięki czemu może pomóc osobom dzwoniącym szybciej, lepiej i z większą dokładnością realizować swoje zadania. Pozwala to firmom obniżyć koszty operacyjne i zwiększyć liczbę zadowolonych klientów. Firma zakończyła prezentację najnowszych produktów, informując o wprowadzeniu do oferty nowej sieciowej platformy do rejestrowania multimediów, która obsługuje nagrywanie, odtwarzanie, strumieniowe przesyłanie na żywo oraz przechowywanie multimediów, w tym plików dźwiękowych i wideo. Rozwiązanie to stanowi wydajną i ekonomiczną platformę do rejestrowania, przechowywania i eksplorowania rozmów na potrzeby analizy danych biznesowych.

Oferowany przez Cisco pakiet oprogramowania do współpracy z klientami składa się z następujących elementów:

- **Cisco SocialMiner:** Rozwiązanie to oferuje funkcje do monitorowania mediów społecznościowych, kolejkowania i zarządzania przepływem pracy, umożliwiając porządkowanie wpisów klientów w mediach społecznościowych i ich dostarczanie do zespołów opiekujących się klientami korzystającymi z takich mediów. Pozwala to firmom reagować na wypowiedzi klientów w czasie rzeczywistym za pośrednictwem pierwotnej sieci społecznościowej.
  - Oprogramowanie Cisco SocialMiner umożliwia taki rodzaj zaangażowania, który zapewnia klientom realne korzyści. Klienci dostrzegają szybką reakcję firm, które oferują im zaawansowaną obsługę. Klienci indywidualni dostrzegą też korzyści wynikające z faktu, że to firmy zajmują się nimi, oferując im usługę i informacje, zamiast oczekiwać, że klient znajdzie te informacje na własną rękę w serwisach internetowych firmy.
  - Klienci indywidualni będę mogli nadal zarządzać prywatnością swoich kontaktów online w mediach społecznościowych, dokonując samodzielnie aktywacji lub dezaktywacji pewnych funkcji w sieciach społecznościowych.
  - Dzięki aktywnym kontaktom z klientami firmy mogą szybko zacieśnić relacje z internautami, rozwiązywać potencjalne problemy, generować z wyprzedzeniem możliwości sprzedaży i zarządzać percepcją ich marek.
  - Wewnętrznie, zespół Cisco ds. produktów dla klientów indywidualnych, w tym rozwiązania Cisco Flip® Video, wykorzystuje oprogramowanie Cisco SocialMiner do zarządzania kontaktami z klientem za pośrednictwem mediów społecznościowych.
- **Cisco Finesse:** To nowe rozwiązanie łączy tradycyjne funkcje centrum kontaktowego z możliwościami korporacyjnego oprogramowania społecznościowego Cisco Quad®.
  - Przeznaczona do wspomagania pracy agentów architektura w technologii Web 2.0, pozwoli firmom zintegrować technologię współpracy z aplikacjami biznesowymi, aby udostępnić agentom centrów kontaktowych narzędzia do jak najlepszej obsługi klientów.
- **Rejestrowanie multimediów:** Dzięki rejestrowaniu rozmów odbywanych w sieci agenci centrów kontaktowych będą mieć dostęp do nagranych multimediów. Dostęp ten będzie zapewniany przez różne aplikacje za pośrednictwem prostych interfejsów, co upraszcza architekturę, pomagając jednocześnie obniżyć koszty i zapewnić firmom optymalną skalowalność.
  - Dzięki takiemu ekosystemowi przedsiębiorstwa uzyskują wgląd w problemy osób telefonujących, mogą instruować agentów obsługujących klientów jak szybko rozwiązywać problemy już w czasie pierwszej rozmowy, poprawiać produktywność agentów oraz zwiększać zadowolenie klientów.

John Hernandez, wiceprezes i dyrektor działu współpracy z klientami (*Customer Collaboration Business Unit*) w firmie Cisco:

– Firmy zdają sobie sprawę, że ignorując kanał komunikacji jakim jest Internet, otwierają szanse przed firmami konkurencyjnymi i pozwalają, aby dialog na temat ich marki toczył się bez nich – powiedział **John Hernandez**, wiceprezes i dyrektor działu współpracy z klientami w firmie Cisco. – *Jako aktywny użytkownik mediów społecznościowych, Cisco dostrzega znaczenie interakcji za pośrednictwem tych mediów dla działalności biznesowej firmy. Nasi pracownicy byli jednymi z pierwszych użytkowników takich serwisów społecznościowych, jak MySpace, Twitter, Facebook, YouTube. Nasz własny dział produktów dla klientów indywidualnych (Consumer Products Group) wykorzystuje już oprogramowanie Cisco SocialMiner do współpracy ze swoimi klientami.* ■

Nowe określenia na stare procesy

Jarosław Żeliński

Cloud computing – czy aby na pewno nowinka...

Osobiście zastanawiam się nad „rynkowym" pojęciem „chmurki", bo to nie takie „nowe rozwiązanie". Dla mnie owa chmura (oportunista jednak jestem) to znane od dawna, komponentowe, obiektowe systemy, projektowane obiektowymi metodami zorientowanymi na tak zwany kontrakt (obiekt lub komponent świadczy określone usługi wystawiając stosowny, udokumentowany interfejs).

Cloud computing to, moim zdaniem, kolejny rynkowy buzzword. Metodą tą, świadczenie usług zdalnego przetwarzania poprzez udostępnione interfejsy, od lat pracuje poprzez sieć wiele rodzajów oprogramowania OpenSource, a także komercyjnego. Przeciętny CMS (*Content Management System*, System zarządzania treścią – są to programy używane do zarządzania zaawansowanymi serwisami WWW) czy blog (odmiana CMS) potrafi użyć, automatycznie zainstalować (użyć) plug-in (wtyczka rozszerzająca możliwości) do zrealizowania nowej funkcjonalności, lokalnie lub zdalnie (np. popularne od lat systemy tworzenia statystyk ruchu dla stron WWW). Z punktu widzenia samej aplikacji, nie ma znaczenia, czy kod realizujący daną funkcjonalność jest uruchamiany lokalnie, czy poprzez sieć (to cecha systemów o obiektowej konstrukcji).

Uogólniając (**diagram poniżej**, źr. WIKI), poszczególne wymagane funkcjonalności realizowane przez oprogramowanie mogą być *zlecane* innym pakietom oprogramowania, jeżeli te tylko udostępniają stosowny interfejs. Nic nie stoi więc na przeszkodzie, by np. pakiet SaleForce wysyłał dane ze sprzedaży do zaksięgowania do pakietu Microsoft DynamixXL i pobierał dane do wyliczenia prowizji dla sprzedawców. Takich połączeń można zbudować więcej, jeśli tylko te pakiety oprogramowania będą otwarte na taką współpracę (interfejsy). Taki sposób pracy jest wykorzystywany od lat w wielu rozwiązaniach opensource.

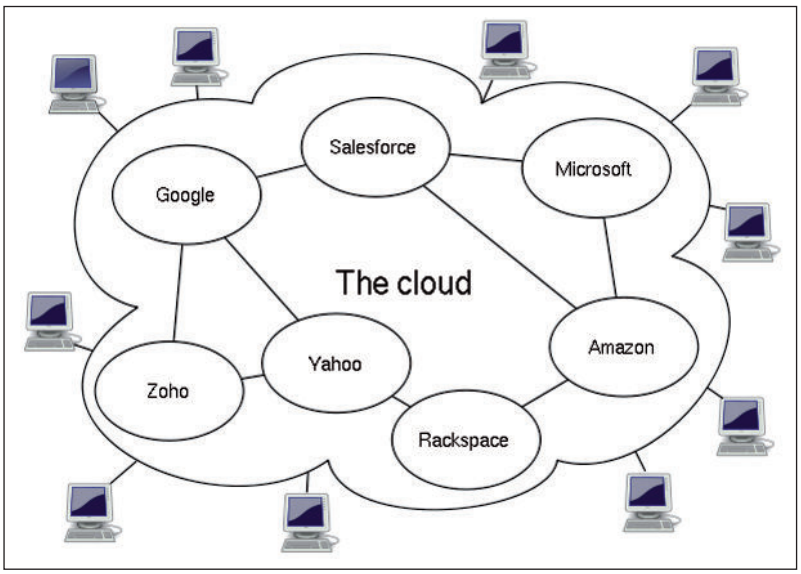
Wygląda więc na to, że cloud computing to kolejny przykład komercyjnej adaptacji pomysłów środowisk opensource'owych, które jako społeczności skazane są na pracę rozproszoną i taka architektura niejako *musiała powstać*. Moim zdaniem, każdy chcący liczyć się na rynku dostawca ERP w zasadzie musi się z tym pogodzić lub wypadnie z rynku. Najpierw rynek zmusił dostawców ERP do udostępniania interfejsów integracyjnych, tak zwanych API (ang. *Application Programming Interfejs*), choć nadal są oportuniści wśród dostawców tych systemów. Teraz pora pogodzić się z tym, że powstają (będą) komponenty rozszerzające funkcjonalności podstawowych wersji ERP, a koszt udostępnienia API (licencjonowanie) będzie spadał. Możliwości udostępniane przez te API od pewnego czasu pozwalają już na budowanie „chmur".

Osobiście widzę to tak, że w przyszłości będą na rynku systemy z podstawowymi modułami wymaganymi przepisami zbudowanymi wokół podstawowego modułu finansowego (chodzi o księgowanie kontowe). Do tego będą opcjonalne „plug-iny" typu magazyn, produkcja, kontaktmanager itp. i tu będzie na rynku konkurencja. Wykształci się rynek firm specjalizujących się we wdrażaniu konkretnych ERP i konkretnych „plug-inów". Jest bardzo prawdopodobne, że interfejsy API ulegną pewnej standaryzacji i wiele komponentów będzie współpracowało z wieloma systemami ERP. Uważam, że producent ERP, który nie otworzy się na świat z dobrze udokumentowanym API, z czasem *rynkowo umrze*.

Jeżeli miałbym coś polecić tym, którzy patrzą na *cloud computing* jak na potencjalne narzędzie uzyskania przewagi konkurencyjnej, to sugeruję po zanalizowaniu potrzeb i wyspecyfikowaniu wymagań dokonanie oceny, które wymagane funkcjonalności są *biznesowo ryzykowne*, ocenę, na ile można je zdobyć na rynku w postaci usług innych aplikacji. W zasadzie jest to model SaaS (*Software as a Service*), ale tu mamy do czynienia z dedykowanymi usługami, a nie kompletnym, zdalnie używanym oprogramowaniem.

„W poprzedniej epoce firmy wiązały się na wiele lat z jednym dostawcą systemów IT, rozprzestrzeniając wybrane systemy w całej organizacji, czego efektem było często powstanie trudno zarządzalnej, sztywnej infrastruktury, w niewielkim stopniu podatnej na zmiany. Analitycy Gartnera są zdania, że rozpoczęła się epoka projektów, które trzeba będzie rozpoczynać bez znajomości wszystkich wymagań użytkownika, aby nie spóźnić się na rynek z nowym produktem i wykorzystać sposobną chwilę, która może się nie powtórzyć. Przed nami epoka systemów, które budowane są z myślą o ich ustawicznych modyfikacjach w odpowiedzi na zmieniającą się sytuację rynkową" (źr. Gartner/ERPStandart).

It-consulting.pl

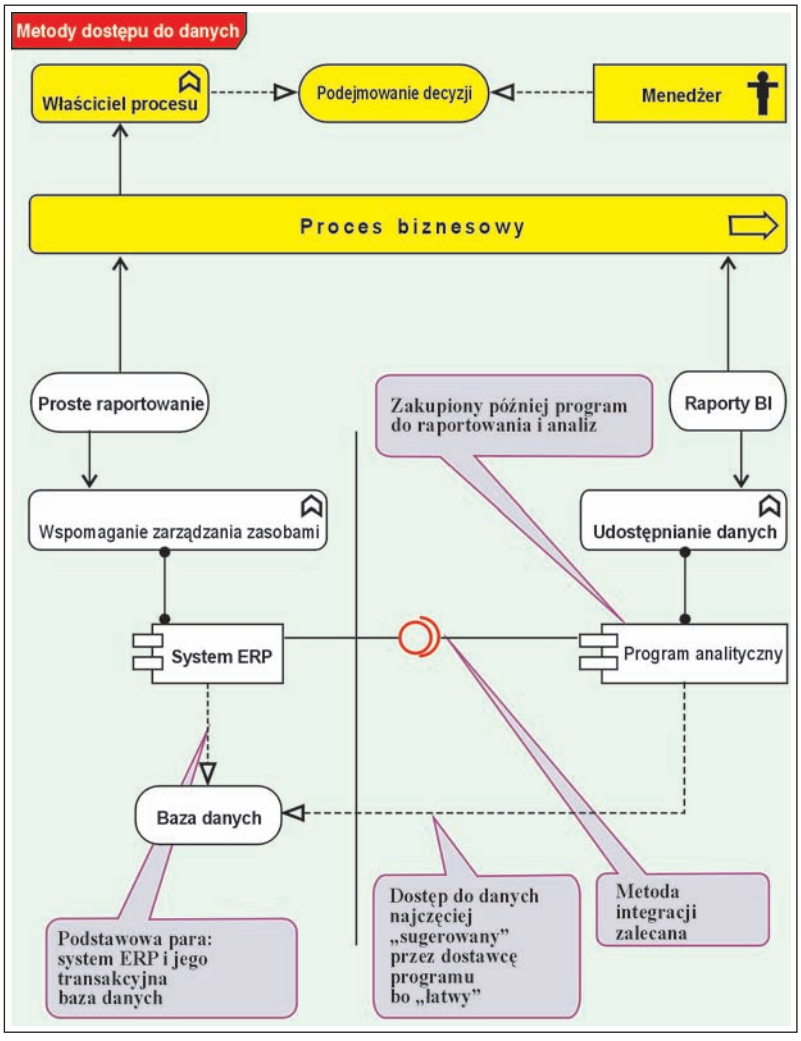


Bezpieczeństwo a procesy biznesowe

Jarosław Żeliński

Kto odpowiada za bezpieczeństwo danych?

Z badania przeprowadzonego na zlecenie firmy Informatica wynika, że statystycznie aż w 86 proc. firm dostęp do środowisk bazodanowych mają pracownicy działów biznesowych. W co trzeciej firmie dostęp do środowisk bazodanowych nie jest w żaden sposób ograniczany – prawa dostępu i modyfikacji informacji zapisanych w bazie danych mają wszyscy pracownicy. Jednocześnie w wielu firmach funkcjonuje wiele odrębnych baz danych, często nieobjętych korporacyjną polityką bezpieczeństwa. Własnym środowiskiem bazodanowym najczęściej dysponują działy sprzedaży i marketingu. Bazy danych stworzone i zarządzane przez pracowników działów handlowych i marketingowych funkcjonowały aż w 94 proc. analizowanych firm. Średnio w jednej firmie funkcjonuje dziewięć różnych środowisk bazodanowych, którymi zazwyczaj zarządzają inne osoby. W firmach zatrudniających więcej niż 1000 osób liczba funkcjonujących równolegle baz danych jest jeszcze wyższa (źródło: IDG).



Po przeczytaniu tego artykułu przypomniałem sobie pewien projekt, ale po kolei.

Mógłby ktoś powiedzieć, że to (wiele baz i wielu uprawnionych) sztuczny problem, bo „jakoś z tym żyjemy". Jednak okazuje się, że po pewnym czasie…

Krótka historyjka

Swego czasu zatrudniono mnie do projektu związanego z modelowaniem (tak to zostało nazwane) „istniejącego systemu". Celem było udokumentowanie architektury logicznej i powiązanych z nią zasobów oraz przyporządkowanie funkcji biznesowych (elementów procesów biznesowych) do poszczególnych aplikacji. Nie rozwodząc się, okazało się to wręcz niemożliwe w czasie, jaki zaplanowano na tę pracę. System IT w tej firmie rósł wraz z nią. Informatycy programiści, na polecenie zarządu, dopisywali ad-hoc kolejne „użytki", robili to pod presją czasu (nowe produkty, kolejne promocje, wszystko na wczoraj). Po pewnym czasie, jakkolwiek wiadomo było, jakie programy są (dostałem ich specyfikację), nikt nie wiedział, co jest z czym powiązane, gdzie i na czym. O wiedzy na temat uprawnień w tych wzajemnych połączeniach (funkcje dopisywane albo w procedurach wbudowanych, albo w rozwijanych aplikacjach, wzajemne odwołania po ODBC czy bezpośrednio do bazy) nie wspomnę, takie pytanie było tam tabu.

Po co ten model? Otóż w trakcie było wdrożenie systemu CRM, który miał to uporządkować, zastąpić znaczną część tych „drobnych systemów", ale nie wszystkie. Pytanie brzmiało: Co i w jakiej kolejności można wyłączać i zastępować nowymi modułami systemu CRM? Powiem tak: Nie udało się. Bardzo długo (nie znam końca wdrożenia) nie udało się przejść na nowy CRM.

Szkodliwe oferty

Drugim, poza powyższym, powodem narastającego bałaganu (to się nazywa spaghetti systems) jest czasami wręcz szkodliwa działalność dostawców różnego rodzaju systemów raportowania, BI, rozbudowanych makr do arkuszy kalkulacyjnych itp. Pada magiczne i niewinne polecenie: „Proszę mi podać jakiś login i hasło do bazy danych finansowych, to pokażę Pani, jak można robić analizy danych", „To jest bardzo tani, dużo tańszy od hurtowni danych, także bardzo dobry system Business Intelligence". Często nabywcami tych rozwiązań są menedżerowie, więc ich prośby „hasło i login do bazy, proszę" raczej „nie znoszą sprzeciwu". W efekcie mamy to co opisał dziennikarz IDG.

Jak to wygląda? To co spotykam często (patrz – diagram obok).

Po kolei. Każdy proces biznesowy ma jakiegoś właściciela (nie zawsze formalnie, ale zawsze

jest ktoś, kto „oberwie”, jak coś się tu nie uda **;)**). Rolą właściciela procesu jest podejmowanie decyzji i robi ktoś konkretny ze struktury organizacyjnej (jakiś konkretny menedżer).

Do bieżącej pracy wykorzystuje on raporty dostępne np. we wdrożonym systemie ERP. Pojawia się nagle ktoś z ofertą na „supersystem BI, tani i skuteczny, trzeba tylko się podłączyć do bazy tego ERP”. Wariant właściwy (jeśli już podłączamy się do tej bazy, a nie tworzymy pośredniej np. hurtowni danych) powinien polegać na ich pobieraniu za pośrednictwem aplikacji zarządzającej tymi danymi, tu jest to nasz ERP. Powinien powstać (powinno się użyć istniejącego) interfejs (**na diagramie kulka w kieliszku pomiędzy ERP a programem analitycznym :)**). To jednak wymaga małego „projektu”, a po drugie – od razu wyjdzie na jaw, że ktoś kupuje taki „program analityczny”.

Co więc się robi? Łamiąc zasady „podpinamy” program analityczny bezpośrednio do danych (linia przerywana program analityczny – Baza danych). Na wszelki wypadek, żeby nie wieszał się, dajemy mu największe możliwe uprawnienia (dobrze, gdy tylko do odczytu) i z głowy. Efekt? Po kilku latach w dużych firmach nikt nie wie, kto i do czego ma dostęp.

Architektura korporacyjna

Wdrożenie hurtowni danych i systemu BI to nie tylko raporty itp., ale właśnie centralizacja dostępu do danych i panowanie nad tym, kto do czego ma dostęp. W małej firmie, gdzie najczęściej taki programik analityczny jest jeden i zainstalowany za czyjąś zgodą, nie ma dużego problemu – w większych firmach stanowi to poważne zagrożenie. To kolejny powód, by przestrzegać zasad projektowania architektury, mimo że wielu administratorów, i nie tylko, uważa, że „to utrudnianie sprawnego działania”.

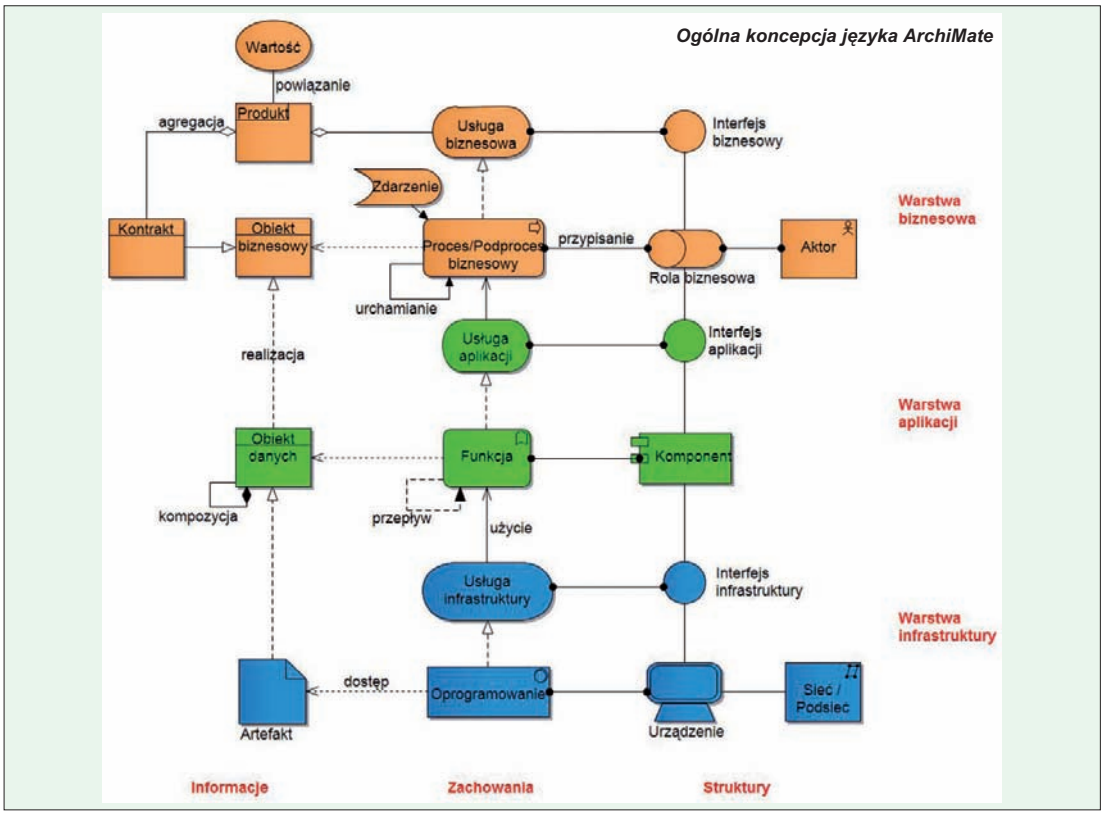
Powyższy diagram uproszczony to namiastka właśnie czegoś, co nazywa się architekturą korporacyjną (diagram wykonany w notacji ArchiMate, stosowanej do dokumentowania architektury korporacyjnej). Nie chodzi o to, by narysować każdy szczegół, chodzi o to, by jednak wiedzieć, co się ma i z czym jest powiązane.

To kosztowne i po co? Między innymi po to, by w dowolnym momencie można było powiedzieć, czy i jak coś można zmienić. Mogę oszacować, ile powyższa firma oszczędziła na poprawnym projektowaniu poprzedzającym implementacje i tworzeniu dokumentacji. Mogę także oszacować, ile straciła na kilkuletnim opóźnieniu wdrożeniu systemu CRM, który kupiła, i wiem, że ten drugi koszt wielokrotnie przerósł pierwotne oszczędności na panowaniu nad rozwojem i systemu, i jego dokumentacji, której po prostu nie było.

Kto za to odpowiada?

Nie sądzę, by miał to być jakiś informatyk, sądzę, że ktoś powinien być obciążony odpowiedzialnością za całą logikę procesów i zasobów IT je wspierających. Im bardziej ta wiedza będzie rozproszona (pionami, dziedzinowo itp.), tym większe ryzyko, że „coś pójdzie nie tak”. Jakakolwiek ingerencja w istniejący system lub oszacowanie skutków (analiza ryzyka) jakiejś usterki (np. awaria UPS’a) może być łatwe przy centralnym zarządzaniu architekturą korporacyjną. Przy rozproszeniu tej wiedzy każda decyzja będzie wymagała wręcz burzy mózgów, a i tak będzie obłożona niemałym ryzykiem. Centralizacja tej wiedzy to niekoniecznie stosowny „etat”, to może być po prostu aktualizowana dokumentacja.

it-consulting.pl



Kompendium dla małych i średnich przedsiębiorstw

Grzegorz Kantowicz

Sieciowe magazynowanie danych

Jeszcze nie tak dawno temu istniało wyraźne rozróżnienie pomiędzy potrzebami magazynowania danych małych przedsiębiorstw i ich większych odpowiedników. Małe firmy opierały się głównie na pamięciach masowych umieszczonych w komputerach rozmieszczonych po całym biurze oraz może jednym małym komputerze z systemem operacyjnym Windows lub serwerze wykorzystywanym do dzielenia plików i drukowania dokumentów. Większości małych przedsiębiorstw brakowało personelu IT albo w ogóle kogokolwiek z doświadczeniem potrzebnym do obsługi skomplikowanych technologii. Jeżeli pliki były niedostępne przez kilka godzin, czasami nawet cały dzień, była to niedogodność, nie katastrofa. Większość dużych przedsiębiorstw miała skomplikowaną infrastrukturę sieciową ze szczelną ochroną i wymaganiami wydajności.

Linia rozgraniczająca potrzeby pamięci magazynowej małych i średnich przedsiębiorstw zamazała się w ciągu ostatniej dekady. Dzisiaj małe firmy bardzo często borykają się z tymi samymi problemami, co ich większe odpowiedniki, na przykład:

Jak spełnić coraz większe zapotrzebowanie na przestrzeń do magazynowania danych. Zapotrzebowanie na przestrzeń magazynową niesamowicie wzrosło w związku z digitalizacją dokumentów, które wcześniej miały formę papierową, zwiększone użycie telefonii internetowej i wideokonferencji, Internetu i przepisów określających, jak długo należy przechowywać pewne pliki. Wiele firm obserwowało, jak ich zapotrzebowanie na przestrzeń magazynową podwaja czy potraja się rok po roku. Potrzebują one efektywnych sposobów magazynowania i dzielenia dużych ilości danych, bez przekraczania budżetów i zatrudniania personelu IT.

Rodzina urządzeń pamięci masowych

Jak chronić krytyczne dla działania przedsiębiorstwa dane. Jak ich więksi odpowiednicy, wiele małych przedsiębiorstw jest tak zależnych od swoich komputerów, oprogramowania czy danych, że nawet w przypadku tylko kilkugodzinnej przerwy w dostępie do nich nie są w stanie funkcjonować. Muszą znaleźć nadające się do zastosowania tanie sposoby na tworzenie kopii zapasowych i ochronę dostępu do napędzających ich firmę informacji.

Jak zredukować albo wyeliminować okresy przestoju. Małe przedsiębiorstwa coraz częściej współpracują z dużymi korporacjami w ogólnoświatowym środowisku albo świadczą usługi klientom w innych strefach czasowych. Potrzebują one prostych, tanich i wydajnych sposobów utrzymania swoich danych dostępnych 24 godziny na dobę, 7 dni w tygodniu, bez utraty możliwości tworzenia kopii zapasowych czy wykonania czynności konserwacyjnych.

Jak wypełnić rygorystyczne wymogi przepisów i audytu. Nie tylko duże firmy muszą spełniać wymogi audytów i przepisów, takich jak np. ustawy o ochronie danych osobowych. Mnóstwo mniejszych przedsiębiorstw potrzebuje prostych, skutecznych strategii przechowywania i ochrony informacji poufnych, o takim samym poziomie efektywności i równie wyrafinowanych, jakie posiadają ich odpowiednicy w korporacjach.

Jak efektywnie wykorzystywać przestrzeń magazynową w infrastrukturze wirtualnej. Ponieważ wiele małych firm wykorzystuje zalety aplikacji bazujących na sieci lub serwerach, takich jak e-mail czy CRM, wiele z nich przeniosło się na platformę serwerów wirtualnych. Zrobiły to, aby ograniczyć koszty zakupu sprzętu i obsługi serwerów. Te firmy potrzebują rozwiązań magazynowania danych, które sprawdzają się w środowisku wirtualnym.

Wszystkie te kwestie wydają się być mocno zniechęcające dla małych przedsiębiorstw, które mają niewiele funduszy i zasobów na zbyciu. Dobrą wiadomością jest, że nowa i ciągle rozwijająca się linia rozwiązań magazynowania danych dla małych przedsiębiorstw może rozwiązać wszystkie te problemy. Dobrą wiadomością jest również to, że nie jest ona zbytnio skomplikowana oraz nie wymaga zatrudniania fachowca z branży IT.

Dzięki uprzejmości agencji INVENTIVE Communication przedstawiamy efektywne, oszczędne sposoby rozwiązania wymienionych powyżej kwestii przechowywania danych w małych przedsiębiorstwach bez nadwerężania budżetu czy zatrudniania specjalisty z branży IT.

Pomocy! Moja firma gwałtownie się rozrosła, moim komputerom brakuje pamięci, a ważne informacje są rozproszone!

Jak w przypadku większości małych firm, zaczynałeś od małych inwestycji w technologię. Najpierw zainwestowałeś w komputer dla siebie i kilku swoich pracowników. Być może zatrudniasz grafika, który używa do pracy Maca, albo upartego technika, który lubi Linuxa. Każdy z pracowników przechowuje swoje pliki na swoim komputerze; kiedy ktoś czegoś potrzebuje, pliki przenoszone są na podręcznych dyskach USB albo przesyłane pocztą elektroniczną. Możliwe, że aktywowałeś opcję dzielenia plików w systemie Windows, aby pracownicy mogli się dzielić plikami między sobą.

Nagle twój biznes się rozrósł. I co się dzieje? Niektórym twoim komputerom zaczyna brakować pamięci na dyskach twardych. Pliki rozrzucone są po wszystkich komputerach, przez co nie możesz znaleźć tego, którego szukasz. Masz różne wersje tego samego pliku w różnych miejscach. Który z nich jest najbardziej aktualną wersją? W wielu przypadkach nie wie tego nikt.

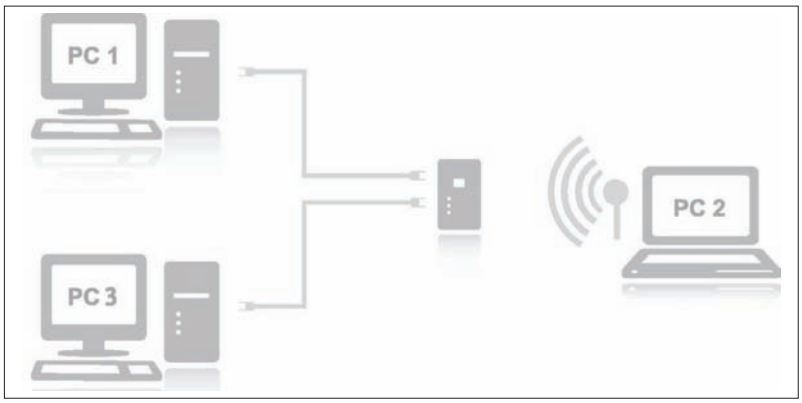
W wielu małych firmach nadchodzi w końcu taki moment, kiedy zbiór osobnych komputerów stacjonarnych czy przenośnych już się nie sprawdza. To jest właściwy moment na konsolidację, centralizację oraz dzielenie plików poprzez sieć.

Dlaczego konsolidować? Jest wiele powodów

Jest to bardziej wydajne. Przechowywanie plików na poszczególnych komputerach jest z natury nieelastyczne i nieefektywne. Niektóre z twoich komputerów mogą mieć ogromne ilości niewykorzystanej pamięci, ale nie mają żadnego sposobu na podzielenie się nią, natomiast inne stale borykają się z problemem braku pamięci i wymagają nieustannego wewnętrznego usprawniania pamięci albo podłączania zewnętrznych dysków twardych. Kiedy scentralizujesz i dzielisz pamięć magazynową, otrzymujesz jedno pole pamięci, które możesz dowolnie dzielić na obszary i przydzielać użytkownikom i aplikacjom. Efektywnie i prosto, bez potrzeby podłączania do komputerów dodatkowych wewnętrznych bądź zewnętrznych dysków twardych. Aktualizacje są rzadsze, a posiadana przez ciebie przestrzeń do magazynowania danych jest wykorzystywana o wiele bardziej efektywnie.

Jest to lepiej zorganizowane. Kiedy wszystkie twoje pliki są przechowywane w jednym miejscu, są one łatwiejsze do odnalezienia. Prościej jest śledzić, który z plików jest najnowszą wersją. A ponieważ nie musisz przechowywać tego samego pliku w różnych wersjach rozrzuconego po całej sieci, oszczędzasz przestrzeń magazynową na dysku.

Jest to łatwiejsze do ochrony. Wiesz, że wszyscy twoi pracownicy powinni regularnie tworzyć kopie zapasowe swoich plików, ale powiedzmy sobie szczerze: Kto tak robi? Jest to tyko kwestia czasu, zanim jakieś ważne pliki zostaną utracone bez możliwości odzyskania ich. Zbierz całą swoją przestrzeń magazynową w jednym miejscu, a o wiele prościej będzie zaimplementować wydajną strategię tworzenia kopii zapasowych, która jest sprawna, efektywna i łatwa do egzekwowania.



OK, więc już wiesz, że powinieneś skonsolidować i dzielić swoją przestrzeń do magazynowania danych, ale jak to zrobić?

Istnieją trzy podstawowe sposoby:

Pamięci podłączane bezpośrednio (*Direct-Attached Storage* – DAS)

Pamięci podłączane bezpośrednio są to urządzenia do magazynowania danych podłączane bezpośrednio do komputera bądź serwera. Możesz dzielić się plikami zgromadzonymi na jednym z dysków twojego komputera albo zakupić serwer i dzielić jego wewnętrzną pamięć. Jak wspominaliśmy wcześniej, możesz również podłączyć dodatkową przestrzeń dyskową do wewnętrznej kieszeni twojego serwera albo podłączyć zewnętrzny dysk poprzez USB albo FireWire.

Są to realne rozwiązania, ale jeżeli jeszcze nie dokonałeś skoku do świata serwerów, rozważ dokładnie inne opcje. Dlaczego?

Złożoność. Musisz bardzo dokładnie zastanowić się nad wyborem serwera, aby spełniał on twoje potrzeby. Potem musisz nabyć sprzęt, zainstalować oraz skonfigurować sprzęt i system operacyjny dla twojej sieci użytkowników. Jeżeli nie jesteś zaznajomiony z technologią serwerów, może to zająć ci dużo czasu i kosztować cię sporo nerwów. Oczywiście możesz zatrudnić kogoś, kto zrobi to wszystko za ciebie – za drobną opłatą.

Kiedy już twój serwer zostanie zainstalowany, ten luźno zintegrowany zbiór urządzeń, systemów operacyjnych i oprogramowania będzie wymagał nieustannego nadzoru, poprawek i rozwiązywania drobnych problemów. System operacyjny serwera i oprogramowanie będzie najprawdopodobniej wymagać częstych poprawek i uaktualniania, aby zachować odpowiedni poziom bezpieczeństwa i wydajności.

Dostępność. DAS jest dostępny tylko poprzez serwer albo komputer, do którego jest podłączony. Jeżeli ten serwer zepsuje się albo zostanie wyłączony z jakiegokolwiek powodu, przestrzeń dyskowa nie będzie dostępna dla sieci.

Aktualizacje. Jeżeli skończy ci się dostępna przestrzeń do przechowywania danych, najprawdopodobniej będziesz musiał wyłączyć serwer, aby zainstalować nowy dysk twardy. Wymaga to okresu przestoju i wykwalifikowanego personelu. Niektóre serwery i zewnętrzne rozwiązania do przechowywa-

nia danych pozwalają wymieniać dyski twarde w trakcie pracy, ale są to urządzenia wysokiej klasy, raczej stosowane w średnich i dużych przedsiębiorstwach.

Wydajność. Typowy system operacyjny serwera jest zaprojektowany tak, aby obsługiwał wiele różnych aplikacji, zapewniał wiele różnego typu usług i wypełniał wiele różnych zadań jednocześnie. Pełnoprawny system operacyjny może mieć niezamierzony wpływ na wydajność, jeżeli jedyne, czego będziesz chciał, to móc dzielić pliki.

Elastyczność. Możesz się w przyszłości natknąć na ten sam problem z DAS podłączonymi do serwerów, na który natknąłeś się z DAS podłączonymi do twoich komputerów. Kiedy twój biznes będzie się rozwijał i będziesz dodawał nowe serwery do twojej sieci, bardziej zużyte serwery i jednostki DAS będą miały coraz częściej kłopoty z brakiem pamięci, przez co będą wymagać częstych usprawnień. Natomiast nowsze serwery będą miały nadmiar pamięci, ale nie będzie sposobu, aby mogły się nią podzielić ze starszymi braćmi.

Pomimo tych ograniczeń DAS może być tanim, realnym rozwiązaniem, dla wielu sieci, zwłaszcza dla takich, które chcą też wykorzystywać inne funkcje serwera, jak obsługa aplikacji e-mail, CRM i innych rozwiązań dotyczących baz danych.

Sieć pamięci masowej (*Storage Area Network* – SAN)

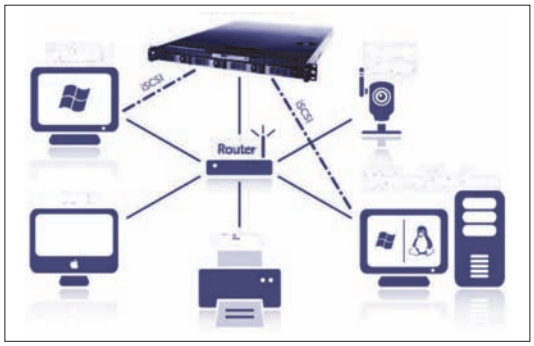
Alternatywą dla użycia DAS jest oddzielenie przestrzeni do przechowywania danych od serwerów i stworzenie z niej wyspecjalizowanej, wysoko wydajnej sieci przechowywania danych nazywanej siecią pamięci masowej (SAN). Dzięki SAN przestrzeń magazynowa nie jest przypisana do poszczególnych serwerów, ale niezależnie znajduje się w SAN, gdzie może być dzielona, kawałkowana i przydzielana do serwerów, użytkowników i aplikacji z ogólnej puli. Przez lata SAN była obsługiwana przez skomplikowaną technologię zwaną Fibre Channel, która była tak kosztowna i skomplikowana, że mogły sobie na nią pozwolić tylko te małe firmy, którym naprawdę zależało na maksymalnej wydajności, aczkolwiek ostatnio nowa technologia SAN nazywana iSCSI oferuje bardzo wysoką wydajność, wykorzystując te same urządzenia jak twoja sieć Ethernet i jest relatywnie prosta w użyciu.

Mimo to, tak samo jak DAS, SAN ma niskopoziomową blokową architekturę przestrzeni dyskowej, która wymaga serwera z systemem operacyjnym, aby móc prezentować pliki użytkownikom. Każdy serwer potrzebuje swój własny adapter iSCSI lub oprogramowanie inicjacyjne, aby mógł komunikować się z SAN. Dlatego właśnie, jeżeli chcesz tylko dzielić pliki i drukarki, pełnoprawna sieć pamięci masowej będzie czymś stanowczo przekraczającym twoje potrzeby. Sieci SAN są najbardziej przydatne, jeżeli potrzebujesz wysokiej wydajności dla obsługi baz danych, bazujących na serwerach aplikacji biznesowych czy obsługi e-maili.

Pamięci dyskowe podłączane bezpośrednio do sieci (*Network-Attached Storage* – NAS)

Małe przedsiębiorstwa szukające dodatkowej pamięci do dzielenia plików i drukarek powinny bliżej przyjrzeć się pamięciom dyskowym podłączanym bezpośrednio do sieci. Tak jak serwer, urządzenie NAS jest podłączane bezpośrednio do sieci i tak jak serwer obsługuje pliki – nie gołe bloki pamięci – dla użytkowników i aplikacji, aczkolwiek, w przeciwieństwie do serwera, nie wymaga instalacji, konfiguracji, strojenia i uaktualniania wielozadaniowego systemu operacyjnego. W przeciwieństwie do SAN, nie potrzebuje osobnego serwera, aby obsługiwać bloki danych i pliki. Zamiast tego NAS ma wstępnie skonfigurowane te części systemu operacyjnego niezbędne do obsługi plików dla użytkowników i aplikacji.

Większość urządzeń NAS wykorzystuje albo Network File System (NFS), który jest systemem plików otwartego oprogramowania, albo Common Internet File System (CIFS), który jest systemem używanym przez Windows, aby dostarczać pliki do użytkowników. Wiele urządzeń może używać obydwu. Coraz większa popularność komputerów firmy Apple spowodowała, że wiele urządzeń obsługuje również Apple File Protocol (AFP).



Urządzenia NAS mają kilka zalet:

Niezależność. Urządzenie NAS może być podłączone w dowolnym punkcie sieci, niezależnie od serwera, i podsyłać pliki do każdego podłączonego do sieci komputera czy serwera. Jeżeli serwer lub komputer ulegnie awarii, NAS jest ciągle w pełni funkcjonalny. Jeżeli zabraknie zasilania, nie ma potrzeby wykonywania skomplikowanej rekonfiguracji. Dzięki swojej prostej architekturze i konfiguracji, NAS może zostać włączony i być gotowy znowu do pracy w ciągu kilku minut

Łatwość użycia. Urządzenia NAS zwykle dostarczane są do nas jako wcześniej skonfigurowane rozwiązania, które wystarczy tylko podłączyć. Nie ma potrzeby instalacji adaptera czy systemu operacyjnego. Po prostu podłączasz NAS do sieci i, zależnie od łatwości obsługi interfejsu, dokonujesz bardo łatwej konfiguracji poprzez przeglądarkę sieciową. Trochę więcej czasu może zająć skonfigurowanie komputerów i serwerów, aby miały one dostęp do urządzenia, ale w większości przypadków NAS rozpocznie pracę po kilku minutach. W porównaniu z tradycyjnymi serwerami, urządzenia NAS wymagają o wiele mniej czynności konserwacyjnych, kilku uaktualnień i bardzo mało rozwiązywania problemów. Wszystkie czynności administracyjne zwykle mogą zostać wykonane przez zwykłą przeglądarkę internetową.

	DAS	SAN	NAS
Co to jest?	Wewnętrzny dysk twardy serwera albo podłączony przy pomocy USB, Fire Wire lub Seata.	Specjalistyczna sieć opracowana do obsługi pamięci do przechowywania danych.	Macierz dyskowa ze swoim własnym sieciowym adresem IP o odchudzonym systemem plików.
Na jakim poziomie następuje dostęp?	Bloków	Bloków	Plików
Za	Pliki mogą być dzielone poprzez sieć LAN. Dostępne w bardzo stabilnych konfiguracjach, takich jak RAID.	Przestrzeń magazynowa jest niezależna od serwerów. Ogólna pula dzielonej pamięci. Tworzenie kopii zapasowych odbywa się poza siecią lokalną. Wysoka wydajność, zwłaszcza w przypadku aplikacji baz danych.	Może zostać umieszczony w dowolnym punkcie sieci. Łatwe tworzenie kopii zapasowych. Nie potrzebuje tradycyjnego serwera do obsługi plików. Przestrzeń dyskowa jest dalej dostępna w przypadku awarii serwera. Łatwa rozbudowa. Odchudzony system plików w celu lepszej wydajności.
Przeciw	Przestrzeń magazynowa jest przywiązana do jednego serwera i nie może być dzielona z innymi serwerami. Może być trudna do zainstalowania, skonfigurowania i utrzymania. Może być niesprawna. System operacyjny ogólnego przeznaczenia może powodować spadek wydajności dzielenia plików.	Może być trudna w konfiguracji i konserwacji. Wymaga tradycyjnego serwera z kontrolerem adaptera SAN lub oprogramowania, aby móc obsługiwać pliki. Może być bardzo kosztowna.	Nie zawsze odpowiednia dla wysoko wydajnych aplikacji bazy danych.

Prosta rozbudowa. Dodawanie dodatkowej pamięci do serwera zwykle wymaga wyłączenia go, wymiany lub podłączenia nowego dysku i ponownego uruchomienia serwera. Aby uzyskać więcej przestrzeni dyskowej w rozwiązaniu NAS, po prostu podłącz kolejny NAS do sieci i w ciągu kilku minut będziesz miał dodatkową działającą dzieloną przestrzeń dyskową. Dodatkowo niektóre urządzenia NAS pozwalają na wymianę dysków albo na podłączanie dodatkowych wewnętrznych lub zewnętrznych dysków w czasie pracy. (Potocznie taką opcję nazywa się „hot swap").

Trzy sposoby konsolidacji

Elastyczność. Wiele urządzeń NAS może łatwo dzielić swoje pliki pomiędzy komputery posiadające systemy operacyjne Windows, Mac, Unix i Linux. Niektóre z nich są na tyle elastyczne, że mogą być używane jako NAS, DAS dla pojedynczego serwera albo jako urządzenie magazynujące w sieci SAN. Wiele z nich obsługuje dzielenie opcji wydruku.

Łatwość tworzenia kopii zapasowej. Urządzenia NAS mogą być świetnym nośnikiem dla tworzenia kopii zapasowych opartych na komputerze. Wiele z tych urządzeń jest dostarczanych razem z łatwym w konfiguracji i użyciu oprogramowaniem do ochrony danych. Świetnie się sprawdzają, kiedy zabezpieczamy dane z komputera użytkownika na NAS, jak i tworząc kopię zapasową z NAS na innym nośniku typu taśma czy zewnętrzna usługa ochrony danych.

Kiedy wszystkie twoje pliki znajdują się w jednym miejscu, tworzenie kopii zapasowej jest oczywiście prostsze niż wtedy kiedy są rozproszone po całym biurze. Niektóre urządzenia NAS są również wyposażone w narzędzia do migracji danych do urządzeń i replikacji danych poprzez sieć z jednego urządzenia magazynowego do drugiego.

Podsumowując, zależnie od potrzeb twojej małej firmy i twojego doświadczenia technicznego, najlepszym rozwiązaniem dla ciebie może być rozwiązanie DAS, SAN lub NAS. Jeżeli interesuje cię tylko proste dzielenie plików i drukarek, a twoi pracownicy nie mają wielkiego doświadczenia komputerowego, NAS wydaje się być dla ciebie najlepszym rozwiązaniem.

Ja mam PC, mój technik ma Linuxa, a grafik ma Maca. W jaki sposób możemy łatwo dzielić się plikami?

Podczas kiedy w większości małych przedsiębiorstw działa tylko na komputerach z systemem operacyjnym Windows lub Mac, nie jest niczym dziwnym spotkać firmy, w których występują komputery z różnymi systemami. Może twoja firma ma 5-10 albo więcej komputerów z systemem Windows i jednego lub dwa Macintoshe, używane przez grafików. A może twój szef na Maca w domu i chciałby go używać również w pracy. Możesz również mieć technika, który uwielbia Linuxa albo używa go dla jednej wyspecjalizowanej aplikacji.

Jak twoja firma ma poradzić sobie z dzieleniem plików pomiędzy różnymi użytkownikami? Masz trzy wyjścia:

- Możesz skonfigurować jeden lub więcej komputerów, tak by dzielił się plikami z innymi.
- Możesz zainstalować w swojej sieci serwer z systemem operacyjnym Windows lub Mac i skonfigurować go tak, aby obsługiwał klientów wszystkich trzech systemów operacyjnych lub na odwrót. Właściwie wszystkie te systemy operacyjne obsługują komputery klientów z innym systemem operacyjnym, aczkolwiek skonfigurowanie ich wymaga dużej wiedzy technicznej, doświadczenia i nie obędzie się bez problemów. Nie jest sekretem, że serwery Windows mają tendencję do faworyzowania klientów Windows, a serwery Mac klientów Mac.

Dlatego właśnie przedsiębiorstwa, które chcą dzielić pliki i drukarki pomiędzy komputery z systemami Windows, Linux i Mac, często wybierają trzecią opcję, którą jest pamięć dyskowa podłączana bezpośrednio do sieci (NAS).

Urządzenie NAS jest najprostszym sposobem dodania pamięci magazynowej do twojej sieci i dzielenia plików z różnymi klientami. Po prostu należy podłączyć urządzenie NAS bezpośrednio do sieci, przejść prosty proces konfiguracji i w ciągu kilku minut mamy działające urządzenie.

Jeżeli pracujesz w środowisku wymieszanych klientów systemów operacyjnych, powinieneś się upewnić, że twój NAS będzie obsługiwał następujące protokoły wymiany plików:

Network File System (NFS), protokół wymiany plików powszechnie znany komputerom z systemem Linux;

Common Internet File System (CIFS), znany również jako Server Message Block, popularny protokół wymiany plików używany w sieciach opartych na systemie operacyjnym Windows;

Bonjour, protokół używany przez komputery Mac do wykrywania drukarek i innych komputerów i ich usług w sieci;

Apple FileProtocol (AFP), protokół podawania plików wykorzystywany przez systemy operacyjne Mac i Mac X.

Wiele urządzeń NAS obsługuje większość lub wszystkie wymienione wyżej protokoły, co czyni bardzo prostym połączenie wszystkich twoich komputerów z różnymi systemami operacyjnymi w sieć, aby mogły one dzielić miedzy sobą pliki i podpięte do NAS drukarki. Aby to uczynić, prawie nie potrzeba nic konfigurować. Magicznie wszystko po prostu działa.

Wszyscy mówią mi, że powinniśmy tworzyć kopie zapasowe naszych komputerów i serwerów, ale nie możemy sobie pozwolić na przestój. Co powinniśmy zrobić?

Na pewno wiesz, że powinieneś tworzyć kopie zapasowe swoich komputerów, tak aby przechowywać w firmie jak najbardziej aktualne informacje. Niestety, smutna prawda jest taka, że ani ty, ani twoi koledzy najprawdopodobniej tego nie robicie. Dlaczego? Tworzenie kopii zapasowej jest czasochłonne i nie tak proste jak powinno być, więc odkładasz to w czasie raz za razem.

Jeżeli któryś z twoich pracowników rzeczywiście zadaje sobie trud tworzenia kopii zapasowej swojego komputera, najprawdopodobniej robi to niezbyt często i właściwie może to robić nieprawidłowo. Kiedy nadejdzie czas, aby rzeczywiście odzyskać utracone pliki, może być niemile zaskoczony.

Prowadzenie działalności biznesowej bez strategii tworzenia kopii zapasowych jest ryzykownym zachowaniem, zwłaszcza jeżeli twoja firma jest wysoce zależna od aplikacji i informacji. Jeżeli twoja firma podlega szczególnym przepisom, możesz znaleźć się w nieprzyjemnej sytuacji i być zmuszony zapłacić wysokie grzywny. Nie musisz prowadzić dużego szpitala, aby musieć spełniać wymagania HIPAA, wystarczy, że prowadzisz mały gabinet lekarski.

Właśnie dlatego prawie każda firma musi opracować działającą strategię tworzenia kopii zapaso wych komputerów stacjonarnych i przenośnych, a co ważniejsze – sposób odzyskiwania plików na wypadek utraty pliku, jego uszkodzenia albo kiedy z powodu awarii zasilania lub klęski żywiołowej wyłączony zostanie cały system.

Dla większości małych i średnich przedsiębiorstw istnieją cztery podstawowe sposoby tworzenia kopii zapasowych:

- Zapisywanie kopii zapasowej na taśmie.
- Zapisywanie kopii zapasowej na dysku – DAS.
- Zapisywanie kopii zapasowej na dysku – NAS.
- Zapisywanie kopii zapasowej na dysku – SAN.

Zapisywanie kopii zapasowej na taśmie

Taśma była docelowym nośnikiem tworzenia kopii zapasowych przez wiele lat dzięki niskim kosztom i wysokiej niezawodności. Zaletą taśmy jest również możliwość wyniesienia jej poza miejsce pracy.

Ciągle jest ona dzisiaj znaczącym nośnikiem tworzenia kopii zapasowych, aczkolwiek posiada kilka wad w stosunku do dzisiaj stosowanych rozwiązań:

Jest powolna. W porównaniu z magazynowaniem danych na dyskach, proces zapisywania danych na taśmie jest bardzo wolny. O ile w przeszłości kopie zapasowe informacji biznesowych tworzono na taśmach, o tyle dzisiaj ilość informacji, które trzeba skopiować, tak się rozrosła, a okres tworzenia kopii zapasowej tak się skurczył w większości organizacji, że nie starcza po prostu czasu w trakcie dnia czy nocy na wykonanie pełnej kopii zapasowej na taśmie.

Jest skomplikowana i czasochłonna. Ktoś musi być odpowiedzialny za regularne ładowanie, obracanie i zmienianie taśm – zwykle co dzień lub co tydzień, wiele małych firm nie ma odpowiednio wykwalifikowanego personelu, aby to robić.

Nie jest łatwo dostępna. Z taśmy nie możemy odzyskać dowolnego pliku. Odzyskiwanie plików wymaga znacznego nakładu pracy, aby znaleźć, załadować i uzyskać dostęp do pliku z taśmy.

Nie zawsze jest niezawodna. Urządzenia do tworzenia kopii zapasowych na taśmach, takie jak automatyczne ładowniki czy biblioteki taśmowe, zawierają mechaniczne części, które mogą zawieść. Jeżeli tworzenie kopii zapasowej na taśmie nie jest właściwie nadzorowane, możesz nigdy nie dowiedzieć się o tym, że nastąpiła awaria mechaniczna lub błąd użytkownika, dopóki nie będziesz chciał odzyskać danych.

Pomimo tych wad niskie koszty i mobilność taśm czynią z nich realne, niskokosztowe rozwiązanie tworzenia kopii zapasowych – o ile oczywiście masz odpowiednio dużo czasu, siły woli i specjalistycznej wiedzy.

Tworzenie kopii zapasowej na dysku

Dyski twarde były kiedyś nośnikami drogimi I niepewnymi, ale w ciągu ostatnich lat ceny zmalały, a stabilność tego nośnika wzrosła na tyle, że obecnie dyski twarde są bardzo rentownym nośnikiem kopii zapasowych.

Tworzenie kopii zapasowych na dyskach posiada wiele zalet:

Nośniki i metody tworzenia kopii zapasowych	Taśma	DAS	SAN	NAS
Za	Niedrogi nośnik. Łatwy do przeniesienia Łatwo można wynieść go poza miejsce pracy.	Szybkie tworzenie kopii zapasowej i odzyskiwania danych. Możliwa jest bardzo pewna konfiguracja. Można przywrócić dowolny plik z dysku. Alternatywne sposoby ochrony danych, takie jak replikacja czy migawka. Migawka niw wpływa na sposób dostępu do danych.	Bardzo szybka metoda. Tworzenie kopii zapasowej się obniża wydajności sieci LAN.	Łatwa w instalacji i konserwacji. Wiele rozwiązań NAS ma zintegrowane oprogramowanie do tworzenia kopii zapasowych. Można podłączyć w dowolnym miejscu sieci LAN. Niektóre rozwiązania sieci NAS oferują szybkie blokowe tworzenie kopii zapasowej, jak w przypadku SAN.
Przeciw	Powolne tworzenie kopii zapasowej i odzyskiwanie danych. Sekwencyjny dostęp do danych. Wymaga zasobów i wiedzy, aby ładować, obracać i zmieniać taśmy. Mechaniczne części mogą ulec uszkodzeniu.	Tworzenie kopii zapasowej i przywracanie danych może obniżać przepustowość sieci. Tworzenie kopii zapasowych komputerów może wymagać świadomej współpracy pracowników.	Może być drog i skomplikowana do skonfigurowania i zarządzania.	Może być nie tak szybka, jak SAN. Tworzenie kopii zapasowej odbywa się przez LAN.

Jest szybkie. Nie ma porównania pomiędzy wydajnością tworzenia kopii zapasowej i odzyskiwaniem danych na dysku a na taśmie. To, co może zajmować kilka godzin, kiedy korzystasz z taśmy, zajmuje kilka minut, kiedy tworzysz kopię i przywracasz dane z dysku twardego.

Dodatkowo, oprócz tradycyjnych sposobów tworzenia kopii zapasowych, istnieją również inne użyteczne metody ochrony danych na dyskach. Dla przykładu, replikacja danych z jednego dysku twardego na inny dysk twardy znajdujący się w innym miejscu. Dla firm, które mają bardzo mało czasu na tworzenie kopii zapasowych albo nie mają go wcale, nie istnieje praktycznie żadna alternatywa dla wydajności dyskowej ochrony danych.

Jest łatwe w użyciu. Kiedy dysk jest już zainstalowany, nie ma już potrzeby ładowania, obracania czy zmieniania niczego przez długi czas. Można skonfigurować automatyczną strategię tworzenia kopii zapasowej i pozostawić ją samą sobie.

Jest łatwo dostępne. Z dysku twardego możemy odzyskać dowolnie przez nas wybrany plik, więc odzyskiwanie plików jest prawie natychmiastowe. Tworzenia kopii zapasowej na dysku można dokonywać używając DAS, NAS albo SAN.

Tworzenie kopii zapasowej na DAS może bazować na komputerze albo na serwerze:

Bazujące na komputerze. Możesz podłączyć zewnętrzny dysk twardy do każdego komputera i skonfigurować oprogramowanie do tworzenia kopii zapasowych. Będzie to praktyczne rozwiązanie w przypadku dwóch, trzech komputerów, ale może stać się niepraktyczne dla szybko rozwijającej się małej firmy z wieloma komputerami. Musisz polegać na użytkownikach, że będą oni wykonywali kopie zapasowe, co jest mocno ryzykowne, zwłaszcza jeżeli często są oni w terenie.

Bazujące na serwerze. Możesz zainstalować serwer tworzenia kopii zapasowych z osobnym DAS i tworzyć kopie zapasowe wszystkich swoich komputerów poprzez sieć LAN. Jest to świetny sposób, aby mieć kontrolę nad procesem tworzenia kopii zapasowych, aczkolwiek wymaga to zakupu i utrzymywania serwera i systemu operacyjnego serwera, z wszystkimi wymaganymi usprawnieniami i uaktualnieniami. Serwer może się również stać wąskim gardłem sieci, jeżeli będzie pobierał dane przez LAN z kilku komputerów naraz.

Mimo to tworzenie kopii zapasowych oparte na DAS może być bardzo dobrym rozwiązaniem dla małych firm i szybszym niż tworzenie kopii na taśmach. Niektóre firmy stosują system łączony, tworząc najpierw kopie bezpieczeństwa na dyskach DAS z powodu ich wydajności, a potem kopiują te dane na taśmy, aby wynieść je poza miejsce pracy, zabezpieczając się przed skutkami ewentualnej katastrofy.

NAS

NAS jest świetnym rozwiązaniem dla wielu małych firm, ponieważ jest ono bardzo proste do zainstalowania i utrzymania. Jak w przypadku pamięci DAS podłączonej do serwera, pozwala ci tworzyć kopie zapasowe wszystkich twoich komputerów w jednej lokalizacji, ale w przeciwieństwie do DAS, który musi być podpięty do serwera, NAS może być podpięty w dowolnym punkcie sieci LAN.

Nośniki i metody tworzenia kopii zapasowych

Niektóre rozwiązania NAS są wyposażone w swoje własne oprogramowanie do tworzenia kopii zapasowych i replikacji, które jest wstępnie skonfigurowane i dopasowane do tego urządzenia. Czyni to instalację i implementowanie strategii tworzenia kopii zapasowych szybkim i łatwym. Proces tworzenia kopii zapasowych może odbywać się automatycznie, dzięki czemu nie trzeba odrywać pracowników od ich codziennych obowiązków, jak zdarza się to w przypadku napędów taśmowych.

Jeżeli poszukujesz rozwiązania, które będzie chroniło przed skutkami klęsk żywiołowych, należy bliżej zapoznać się z rozwiązaniem NAS mogącym replikować dane poprzez sieć do innego urządzenia magazynującego. Zyskujesz zalety napędu taśmowego, ponieważ przechowujesz dane poza miejscem pracy, bez jego wad.

SAN

Dzięki swojej szybkiej, blokowej architekturze dysków, SAN są świetnym rozwiązaniem dla wysoko

wydajnego tworzenia kopii zapasowych. Ponieważ przestrzeń magazynowa umieszczona jest w specjalnej sieci magazynowej, SAN nie obciąża twojej normalnej sieci LAN, dzięki czemu przy tworzeniu kopii zapasowych nie spadają osiągi innych aplikacji sieciowych.

Nie musisz znać technologii Fibre Channel, aby obsługiwać SAN. iSCSI jest prostszy w użyciu, a oferuje równie dobre osiągi oraz działa na zwykłych przełącznikach sieci Ethernet.

Jeszcze prostsze jest wykorzystanie zalet iSCSI, oferowanych przez niektóre obecnie dostępne na rynku produkty NAS. Wiele jednostek NAS może stanowić część szybkiej, blokowej przestrzeni magazynowej iSCSI sieci SAN. Podłącz swój komputer albo serwer tworzenia kopii zapasowych do macierzy dyskowej kablem Ethernet, przeprowadź prostą konfigurację urządzenia magazynującego oraz serwera bądź komputera i możesz mieć szybką sieć w stylu SAN stworzoną z części twojego NAS, podczas gdy reszta urządzenia będzie obsługiwała pliki poprzez LAN.

Czasami przez przypadek skasuję jakiś plik albo jest on uszkodzony. Jak mogę go szybko odzyskać?

Jedną z zalet kopii zapasowych tworzonych na dyskach jest to, że może to być zrobione szybko i tylko w niewielkim stopniu zakłóci pracę twoich operacji i aplikacji biznesowych. Jednym ze sposobów ochrony danych jest zautomatyzowane tworzenie kopii zapasowych na dyskach DAS lub NAS. Większość rozwiązań do tworzenia kopii zapasowych pozwala ci na tworzenie pełnej kopii zapasowej od czasu do czasu i bardzo częstych przyrostowych kopii zapasowych – są to kopie danych, które uległy zmianie od ostatniego pełnego tworzenia kopii zapasowej – codziennie albo nawet kilka razy w ciągu dnia.

Dzięki szybkim dyskowym przyrostowym kopiom zapasowym, w razie przypadkowego usunięcia pliku, katalogu albo w przypadku utraty całego systemu w związku z zarażeniem wirusem lub błędem ludzkim bądź sprzętowym, możesz odzyskać ten plik lub dane w ich stanie pierwotnym. Zrobisz to szybko i łatwo, dzięki czemu szybko będziesz mógł wrócić do pracy.

Jeżeli używasz rozwiązania NAS do przechowywania kopii zapasowych, upewnij się, że jest ono wyposażone albo bezproblemowo współpracuje z oprogramowaniem, które oferuje opcje tworzenia kopii zapasowej i przywracania danych według konkretnego punktu w czasie. Dzięki temu rozwiązaniu możesz być pewny, że nigdy tak naprawdę nie utracisz wartościowych plików lub danych, które są niezbędne twojej firmie.

Pomocy! Moim serwerom ciągle brakuje wolnej pamięci!

Zobaczmy, jak może się rozwinąć taka sytuacja. Możliwe, że używasz serwera do dzielenia plików i drukarek albo możesz używać go do obsługi Microsoft Exchange, albo aplikacji CRM. Możliwe, że posiadasz dwa albo trzy serwery, które obsługują kombinację tych funkcji i każdy z nich ma własne urządzenie DAS.

Co najprawdopodobniej stanie się w przyszłości?

Mała wydajność pamięci. Może się okazać, że jeden z twoich serwerów, najprawdopodobniej twój serwer e-mail, cierpi na chroniczny brak wolnego miejsca na dyskach, podczas gdy inne serwery mają za dużo przestrzeni magazynowej, ale nie ma sposobu, aby się nią podzielić. Jest to bardzo niewydajny scenariusz i największy powód, dlaczego rozwiązanie DAS jest na dłuższą metę niewydajne dla małego, rozwijającego się przedsiębiorstwa.

Kłopoty z zarządzaniem. Większość rozwiązań DAS posiada własne opatentowane oprogramowanie do zarządzania i komunikacji. Znane są one z tego, że są trudne w zdalnym zarządzaniu. Możesz również znaleźć się w sytuacji, w której będziesz używał kilku różnych rozwiązań DAS, każde ze swoim własnym zestawem dziwactw i przykrości związanych z zarządzaniem nimi.

Konsolidacja

Tak jak w przypadku komputerów, odpowiedzią na przeładowanie serwerów jest konsolidacja przestrzeni magazynowej, oddzielenie jej od serwerów i umieszczenie jej w sieci, gdzie może być dzielona pomiędzy kilka serwerów i komputerów. Dlaczego?

Jest to wydajne. Otrzymujesz dzieloną pulę sieciowej przestrzeni magazynowej, którą możesz dowolnie dzielić, kawałkować i przydzielać użytkownikom, aplikacjom i serwerom, wedle uznania. Rozwiązuje to problem przeładowanych serwerów sąsiadujących z prawie pustymi serwerami.

Jest to łatwe do rozbudowy. Nie będziesz musiał już wyłączać swojego serwera aplikacji, aby powiększyć przestrzeń dyskową. Możesz dodać przestrzeń dyskową do sieci i uczynić ją od razu dostępną, bez żadnego wpływu na działanie twoich aplikacji.

Kiedy nadchodzi czas na wymianę serwerów na lepsze, nie jest już konieczne wyrzucanie przestrzeni magazynowej razem z serwerem albo poświęcanie czasu na przerzucanie danych z jednego serwera do drugiego. Po prostu podłączamy nowy serwer do sieci i konfigurujemy go tak, aby uzyskał dostęp do twojej sieciowej przestrzeni magazynowej.

Jest to tanie. Przestrzeń magazynowa stanowi istotną część ceny i wnętrza serwera. Oddziel przestrzeń magazynową w sieci i będziesz mógł wydać trochę więcej na serwery albo zakupić urządzenia bardziej pewne i wydajne. Możesz również umieścić więcej serwerów na mniejszej przestrzeni, jeżeli tego chcesz, wykorzystując zwarte obudowy serwerów typu szafowego bądź kasetowego.

Masz do wyboru dwa możliwe rozwiązania sieciowego magazynowania danych: SAN i NAS.

SAN

Sieci pamięci masowej (SAN) oddzielają przestrzeń magazynową od serwerów I umieszczają ją w wyspecjalizowanej wysoko wydajnej sieci pamięci masowej, gdzie może być ona zbierana w pule i przypisywana do serwerów i aplikacji. Kiedy serwerowi skończy się wolna pamięć, należy mu po

prostu przydzielić więcej pamięci z SAN, a nie wyłączać serwer, aby fizycznie dołożyć pamięci.

NAS

Nic nie jest w stanie pobić prostoty NAS w spełnianiu potrzeb typowej małej firmy. Urządzenie NAS podłączane jest bezpośrednio do sieci i tak jak serwer obsługuje pliki, nie bloki magazynowe. Istnieje wiele zalet NAS jako rozwiązania magazynowego dla małego przedsiębiorstwa.

Niezależność. Urządzenie NAS może zostać podłączone w dowolnym punkcie sieci, kompletnie niezależnie od serwerów, dostarczając pliki do każdego podłączonego do sieci komputera bądź serwera. Jeżeli komputer lub serwer ulegnie uszkodzeniu, NAS będzie dalej pracować. Jeżeli nastąpi awaria prądu, nie ma potrzeby przeprowadzać skomplikowanej rekonfiguracji. Dzięki swojej prostocie NAS może zostać włączone i po kilku minutach jest znowu w pełni funkcjonalne.

Łatwość użycia. Urządzenia NAS zwykle przysyłane są już wstępnie skonfigurowane i wystarczy je tylko podłączyć. Nie ma potrzeby przeprowadzać skomplikowanych instalacji adapterów czy systemu operacyjnego serwera. Po prostu podłączasz NAS i przeprowadzasz bardzo szybką i łatwą konfigurację, zwykle przy pomocy przeglądarki internetowej, i twój NAS jest w pełni funkcjonalny i dostępny dla twoich komputerów.

Łatwa rozbudowa. Aby uzyskać więcej przestrzeni magazynowej dzięki NAS, wystarczy, że podłączysz kolejne urządzenie NAS i w ciągu kilku minut masz w pełni działającą dodatkową przestrzeń magazynową, gotową do pracy.

Elastyczność. Obecnie niektóre rozwiązania NAS wyposażone są również we wbudowane zdolności iSCSI, które mogą zapewnić szybkie blokowe magazynowanie dla aplikacji serwerowych, które wymagają wysokiej wydajności, podczas gdy wciąż są w stanie dzielić i drukować pliki. W niektórych przypadkach nie potrzebujesz nawet przełącznika czy specjalnego adaptera. Po prostu podłącz twój serwer bezpośrednio do portu iSCSI w obudowie NAS. Dzięki temu będziesz mógł się cieszyć najlepszymi cechami obydwu światów w jednym łatwym do użycia i skonfigurowania urządzeniu.

Nie zwróciłem uwagi, kiedy moje serwery stały się niezbędne dla działalności firmy. Jak mogę je chronić nie ponosząc nadmiernych kosztów?

Jeżeli twoja firma jest podobna do większości, staje się ona w coraz większym stopniu zależna od danych i technologii. O ile kiedyś okresy awarii sprzętu i utraty danych były tylko niedogodnością, o tyle dzisiaj spowodowałyby całkowitą blokadę działalności twojej firmy, szczególnie jeżeli większość zawieranych przez ciebie transakcji ma miejsce w Internecie. Wiele małych firm musi obecnie spełniać również warunki rządowych regulacji dotyczących ochrony danych personalnych klientów.

Jak chronić swoje dane bez zbytniego nadszarpnięcia budżetu? Efektywna strategia tworzenia kopii zapasowych, połączona z technologią zwaną RAID (*Redundant Array of Independent Dinks* – nadmiarowa macierz niezależnych dysków) może zapewnić wysoki poziom ochrony twoich danych i nie zrujnować cię. Obydwie rzeczy można osiągnąć przy użyciu pamięci masowych podłączanych bezpośrednio, ale o wiele prostsza jest ich implementacja, jeżeli są one już wcześniej skonfigurowane w urządzeniu NAS.

RAID

Dyski twarde są o wiele pewniejszymi nośnikami niż były kiedyś, ale ciągle posiadają one części mechaniczne, które mogą zawieść. Najlepszym sposobem ochrony danych przechowywanych na dysku twardym jest przechowywanie ich na kilku dyskach twardych. Jest to technika zwana nadmiarowością i jest to dokładnie to, co robi nadmiarowa macierz niezależnych dysków (RAID).

RAID jest po prostu zestawem dwóch lub więcej dysków twardych, połączonych razem oprogramowaniem albo kontrolerem oprogramowania układu, który pozwala drugiemu albo trzeciemu dyskowi przejąć przechowywanie informacji. Kiedy RAID działa prawidłowo, wszystkie twoje dane pozostają bezpieczne i dostępne po awarii dysku twardego.

Istnieją różne techniki RAID wykorzystywane do ochrony danych, znane również jako poziomy RAID. Każda technika ma przypisany do siebie numer.

- RAID 0 jest to prosta organizacja dysków dla lepszej wydajności. W przypadku RAID 0 części pakietu danych są rozkładane pomiędzy cały pakiet dysków twardych, dzięki czemu wszystkie one mogą pracować naraz dla większej wydajności. RAID 0 nie jest systemem nadmiarowym, więc nie zapewnia ochrony danych.
- RAID 1, najprostsza forma ochrony danych. Twoje dane są zapisywane na dwóch dyskach twardych jednocześnie, więc jeżeli jeden z nich zawiedzie, drugi dalej zapewnia dostęp do twoich danych.

Parzystość w poprzek dysków

- Inne popularne formy ochrony danych to poziomy RAID 5 i 6. Zapisują one twoje dane w poprzek czterech lub większej liczby dysków twardych, razem z czymś zwanym parzystością informacji, dzięki czemu można odzyskać dane, w razie awarii któregokolwiek dysków.
- RAID 10 jest kombinacją RAID 1 i RAID 0, zapisując twoje dane na wielu parach dysków jednocześnie, aby zapewnić wysoką wydajność i bezpieczeństwo danych.

Dlaczego potrzebujesz RAID, jeżeli regularnie tworzysz kopię zapasową? Ponieważ przywracanie danych i systemów kopii zapasowej wymaga znaczącej ilości czasu i zasobów, i utracone zostaną dane niezapisane na dysk po utworzeniu kopii zapasowej. Najlepiej jest przede wszystkim chronić się przed utratą danych, aby zminimalizować przerwy w działaniu firmy. W ciągu ostatnich pięciu lat RAID stał się bardzo opłacalnym sposobem na uzyskanie tego efektu.

Porównanie popularnych poziomów RAID

Istnieją trzy podstawowe sposoby wykorzystywania zalet RAID:

	RAID1	RAID3	RAID5	RAID6
Jak działa	Dane zapisywane są jednocześnie na dwóch osobnych dyskach.	Dystrybuuje dane pomiędzy kilka dysków. Parzystość informacji przechowywana jest na osobnym dysku.	Dystrybuuje dane pomiędzy kilka dysków. Parzystość informacji rozrzucona jest w poprzek dysków.	Dystrybuuje dane pomiędzy kilka dysków. Parzystość informacji rozrzucona jest w poprzek dysków, ale urzywa drugiej parzystości na wypadek, gdyby pierwsza zawiodła.
Za	Dysk „lustrzany" dostępny jest zaraz po awarii dysku głównego.	Wymaga pamięci większej tylko o 1,25 raza od przechowywania danych (w 5-dyskowej konfiguracji). Wysoka wydajność.	Rozrzucona parzystość oznacza szybsze jej zapisywanie. Wymaga pamięci większej od przechowywanych danych tylko 1,25 raza. Wyższa wydajność nią RAID1	Toleruje więcej błędów nią RAID5 Wyższa wydajność niż RAID1.
Przeciw	Wymaga dwóch pełnych kopii danych. Niedydajny. Drogi Nie zapewnia tak wysokiej wydajności jak inne poziomy RAID	Dedykowany dysk parzystości może być miejscem wystąpienia awarii i wąskim gardłem systemu. W przypadku awarii dane muszą zostać odtworzone.	Nie tak wysoka wydajność w przypadku mediów strumieniowych, jak RAID3. W przypadku awarii dane muszą zostać odtworzone.	Mniej wydajne użycie przestrzeni magazynowej niż w przypadku RAID5 czy RAID3.
Przydatne dla	Każdej aplikacji nie wymagającej wysokiej wydajności.	Wysoko wydajne aplikacje strumieniowe.	Aplikacje baz danych wymagające wydajności i stabilności.	Te same, co w przypadku RAID 5, ale wymagające dodatkowej ochrony.

DAS RAID. Możesz nabyć tradycyjny serwer zawierający pomięć podłączaną bezpośrednio z wbudowaną ochroną RAID lub możesz podłączyć zewnętrzny RAID do twojego serwera. W obydwu przypadkach twoje dane będą doskonale chronione.

Wady:

Potrzebujesz wiedzy fachowej i czasu, aby nabyć, skonfigurować i zarządzać tradycyjnym serwerem, systemem operacyjnym i pamięcią magazynową RAID. Jeżeli twój serwer ulegnie awarii, utracisz dostęp do twoich danych. Jeżeli masz kilka serwerów, na niektórych zacznie się kończyć wolna pamięć, kiedy inne będą prawie puste, ale nie będzie sposobu podzielenia się tą wolną przestrzenią. Jeżeli posiadasz wiele rozwiązań RAID, a każde z nich zarządza się innym programem, będziesz potrzebował czasu i wykwalifikowanych pracowników, aby nauczyć się ich obsługi.

SAN RAID. Jeżeli już posiadasz sieć pamięci masowej, możesz zainstalować macierz dyskową, RAID w sieci SAN. Uzyskasz niesamowitą wydajność, ale będziesz również potrzebował wykwalifikowanych pracowników i wiedzę fachową, aby zarządzać siecią SAN, co może być dość skomplikowane. Właśnie dlatego, jeżeli nie potrzebujesz wydajności do obsługi baz danych albo podobnych aplikacji, dla małej firmy lepiej jest nie inwestować w rozwiniętą sieć SAN.

NAS RAID. RAID opierający się na rozwiązaniu NAS jest świetnym rozwiązaniem dla przedsiębiorstw, które nie potrzebują wydajności SAN, ale chciałyby skorzystać z zalet magazynowania sieciowego. Dlaczego?

- NAS jest prosty w instalacji i konserwacji. Po prostu należy podłączyć go do sieci w dowolnym punkcie, przeprowadzić prostą konfigurację przez przeglądarkę internetową i już wszystko działa.
- NAS pozwala dzielić sieciową przestrzeń magazynową pomiędzy wszystkie twoje komputery i serwery. Jeżeli będziesz potrzebował więcej pamięci, wystarczy podłączyć kolejny NAS.

Jeżeli zamierzasz przechowywać na NAS informacje krytyczne dla działalności twojej firmy, upewnij się, że jest on wyposażony we wbudowany RAID. Wiele z tych rozwiązań jest. Na który poziom RAID się zdecydujesz, zależy już tylko od twojego budżetu oraz poziomu wydajności i ochrony, jaki pragniesz uzyskać. RAID 10 zapewnia maksymalny poziom ochrony, zaraz za nim są RAID 6 i RAID 1, ale w ich przypadku wykorzystywana przestrzeń użytkowa będzie o wiele mniejsza niż uzyskałbyś w standardowej konfiguracji RAID 5.

Jeżeli wymagasz wydajności przestrzeni dyskowej opartej na NAS dla obsługi konkretnej aplikacji, na przykład e-mail czy bazy danych, powinieneś zainteresować się urządzeniami NAS obsługującymi iSCSI i mogącymi przydzielić część przestrzeni dla szybkiej blokowej wydajności. Jeżeli nabędziesz jedno z tych urządzeń NAS/SAN, będziesz miał to, co najlepsze w obydwu rozwiązaniach – prostotę NAS i wydajność SAN.

Kopia zapasowa

RAID zapewni, że twoje dane będą dostępne nawet w przypadku awarii dysku, ale nie ochroni ich w przypadku poważnej awarii systemu, klęski żywiołowej, uszkodzenia danych czy zarażenia wirusem. Dlatego właśnie powinieneś również tworzyć kopie zapasowe swoich danych jako drugi stopień ich ochrony i najlepiej przechowywać je poza miejscem pracy.

Zagadnienia tworzenia kopii zapasowych serwerów są bardzo podobne do zagadnień związanych z tworzeniem kopii zapasowych komputerów, które zostały omówione wcześniej.

Rozwiązania taśmowe mają wiele zalet jeżeli chodzi o tworzenie kopii zapasowych serwerów. Są one tanie i łatwo je przenosić. Niestety, są one zbyt wolne dla wielu firm prowadzących interesy na całym świecie, będących ściśle powiązanymi z kooperantami. Po prostu nie są oni w stanie pozwolić sobie na tak długie okresy przestoju. Zarządzanie taśmami wymaga wykwalifikowanej obsługi, jak również potrzebny jest serwer, aby zaimplementować

i zarządzać tworzeniem kopii zapasowych poprzez sieć.

Dlatego właśnie tyle organizacji wybrało rozwiązania tworzenia kopii zapasowych serwerów oparte na dyskach twardych. Dysk jest szybkim i relatywnie tanim nośnikiem kopii zapasowej, który może pomóc zredukować albo nawet wyeliminować okres przestoju potrzebny na stworzenie kopii zapasowej.

Dysk twardy pozwala również na użycie innych technologii, które mogą zapewnić dodatkowy poziom ochrony danych:

Migawka (Snapshot) tworzy obraz systemu plików i danych na dysku w tym danym momencie, bez zakłócania pracy aplikacji.

Replikacja tworzy i utrzymuje repliki twojego dysku twardego w wybranej lokacji. Repliki mogą być tworzone i uaktualniane poprzez sieć internetową asynchronicznie, co znaczy od czasu do czasu – na przykład kilka razy dziennie – albo mogą być uaktualniane synchronicznie, co oznacza, że za każdym razem, kiedy nowe dane zapisywane są na oryginalnym dysku, zapisywane są one również w replice. Replikacja synchroniczna bywa nazywana metodą dysków lustrzanych (mirroring). Replikacja może być dość kosztowna i trudna w zarządzaniu, ale jest to potężne rozwiązanie do ochrony danych dla firm, które potrzebują bardzo wysokiego poziomu ochrony danych.

Piękno dyskowych rozwiązań do ochrony danych polega na tym, że wszystkie te procesy mogą zostać zautomatyzowane i będą się odbywać bez potrzeby ingerencji ze strony pracowników.

Dyskowe tworzenie kopii zapasowej może się odbywać poprzez DAS, NAS, a nawet SAN.

Tworzenie kopii zapasowej przez DAS. Jeżeli masz mało serwerów, użycie pamięci podłączanej bezpośrednio jako nośnika kopii zapasowej jest wykonalnym rozwiązaniem, ale może się ono stać nieporęczne wraz ze wzrostem liczby serwerów, a tworzenie kopii zapasowej stworzy wąskie gardło przepustowości w twojej sieci LAN.

Tworzenie kopii zapasowej przez SAN. Tworzenie kopii zapasowej poprzez SAN jest świetnym rozwiązaniem, ponieważ odciąża twoją sieć danych z tworzenia kopii zapasowej, gdzie mogłyby pojawiać się problemy z przepustowością. Jeżeli masz już zainstalowaną sieć SAN albo potrzebujesz dodatkowej stabilnej wydajności, którą SAN zapewni twoim aplikacjom baz danych czy aplikacjom powiadamiającym, to tworzenie kopii zapasowej przez SAN ma sens. Z drugiej strony, SAN wymaga znaczących nakładów czasu i wiedzy fachowej, aby nim zarządzać, nie ma więc sensu wprowadzać go tylko jako rozwiązania do tworzenia kopii zapasowych w małej firmie.

Tworzenie kopii zapasowej przez NAS. Tworzenie kopii zapasowej poprzez NAS jest świetnym rozwiązaniem dla małych firm, ponieważ urządzenia NAS są łatwe w instalacji i utrzymaniu. Wiele urządzeń jest wyposażonych we własne wbudowane oprogramowanie do tworzenia kopii zapasowych, które może zostać użyte do tworzenia kopii zapasowych twoich serwerów sieciowych na urządzeniu NAS. Wiele z tych urządzeń posiada również wbudowane możliwości kopiowania plików z NAS do NAS albo z NAS do zewnętrznej pamięci magazynowej, w celu jeszcze lepszego zabezpieczenia danych. Jeszcze inne urządzenia NAS pozwalają na tworzenie kopii zapasowych w internetowych usługach ochrony danych, dzięki czemu twoje krytyczne dane mogą być przechowywane poza miejscem pracy, skąd mogą zostać odzyskane w razie klęski żywiołowej. Zaleta: otrzymujesz kopię zapasową poza siedzibą firmy, bez wszystkich kłopotów związanych z taśmami.

Jeżeli zdecydujesz się na rozwiązanie NAS, szukaj produktów, które zawierają te cechy i pozwalają w pełni zautomatyzować i zaplanować tworzenie pełnych i przyrostowych kopii zapasowych. Przyrostowe kopie zapasowe kopiują tylko te dane, które uległy zmianie lub zostały utworzone od ostatniej kopii zapasowej.

Jeżeli zdecydujesz, że jest ci niezbędne tworzenie kopii zapasowej poprzez SAN dla danych z jednej albo dwóch aplikacji, takich jak baza danych czy email, rozejrzyj się za urządzeniem NAS, które pozwala podzielić je, aby częściowo obsługiwało bazującą na SAN pamięć magazynową. Dzięki temu uzyskasz to, co najlepsze w obydwu rozwiązaniach: prostotę NAS i szybkie tworzenie kopii zapasowych SAN.

E-mail jest najpopularniejszą aplikacją w mojej firmie. Jaki jest najlepszy sposób przechowywania danych Microsoft Exchange?

Jeżeli twoja firma jest taka jak inne, najprawdopodobniej działacie w dużym stopniu w oparciu o e-mail. Właściwie większość firm obecnie bardziej opiera się, jeżeli chodzi o komunikację, na mailu niż na telefonie. Bardzo często listy elektroniczne służą jako zapis transakcji i muszą być one z powodów prawnych przechowywane przez długi czas. W końcu zacznie nam brakować na nie miejsca.

Przestrzeń magazynowa podłączana bezpośrednio (*Direct Attached Storage* – DAS) jest oczywistym rozwiązaniem dla przechowywania danych Microsoft Exchange, aczkolwiek po pewnym czasie, w którym twój system Exchange i jego dane będą rosły, może się okazać, że na DAS też zaczyna brakować wolnej pamięci.

Niestety, w przeciwieństwie do dzielenia plików i drukarek, NAS nie jest specjalnie dobrą, wysoko wydajną przechowalnią danych dla Microsoft

Exchange. Właściwie to Microsoft Exchange nie obsługuje magazynowania na NAS. Dlaczego? Microsoft Exchange jest środowiskiem magazynowania bazy danych, który o wiele lepiej współpracuje z przestrzeniami dyskowymi opartymi na blokowej architekturze niż z opartym na plikowej architekturze NAS, aczkolwiek istnieją już na rynku urządzenia NAS obsługujące poza standardowymi protokołami NAS dodatkowo iSCSI. Dzielona przestrzeń magazynowa w urządzeniu iSCSI wygląda dla głównego serwera jak jeden z jego dysków wewnętrznych i czyta on z niego i zapisuje na nim dane nie w plikach a blokach. Wiele urządzeń NAS może być używanych jednocześnie do obsługi plików, jak i jako urządzenie magazynujące iSCSI.

Upewnij się, że urządzenie NAS obsługujące iSCSI, które chcesz nabyć, zostało certyfikowane przez Microsoft, to znaczy, że zostało przetestowane przy standardach Microsoft i spełnia wszystkie wymagania techniczne i bez żadnych problemów współpracuje z Microsoft Exchange.

Co zrobię, jeżeli nastąpi problem z obsługą magazynowania danych, kiedy nie będzie mnie w biurze?

Jest weekend albo późne popołudnie, a ktoś z twoich pracowników nie może dostać się do swoich plików. Czy ty albo ktoś z twoich współpracowników musicie rzucić wszystko i udać się do biura, aby naprawić ten błąd? A może musicie powiedzieć temu pracownikowi, że musi poczekać do jutra albo końca weekendu, nim dostanie się do swoich plików?

Jeżeli twoja przestrzeń magazynowa działa w oparciu o NAS, może ona oferować oparty na przeglądarce internetowej interfejs do zarządzania, który pozwoli ci uzyskać bezpieczny zdalny dostęp do NAS. Dzięki przeglądarce internetowej możesz nawet monitorować i rozwiązywać problemy z twojego iPhona, kiedy spacerujesz po ulicy.

W zależności od tego, jakiego urządzenia NAS używasz, będziesz w stanie zmienić jego ustawienia, stworzyć i przydzielić foldery, zaplanować tworzenie kopii zapasowych, a nawet odebrać generowany przez system alarm, nim twoi użytkownicy odkryją problem.

Jeżeli szukasz rozwiązania dla małej firmy, którym będziesz w stanie bez problemów zarządzać, urządzenie NAS z opartym na przeglądarce zdalnym zarządzaniem wydaje się być doskonałym wyborem.

Jestem w podróży, a potrzebuję jakiegoś pliku. Co powinienem zrobić?

Ile razy zdarzyło ci się być na ważnym spotkaniu biznesowym, podczas którego uświadamiałeś sobie, że nie masz ze sobą ważnego pliku z prezentacją czy arkusza z danymi? Na szczęście, istnieje proste rozwiązanie, które może zapobiec takim sytuacjom.

Wiele urządzeń NAS posiada opcję zdalnego dostępu, która pozwala ci podłączyć się i używać przestrzeni magazynowej NAS za pośrednictwem zwykłej przeglądarki internetowej. Po prostu wpisujesz wcześniej skonfigurowany adres URL urządzenia NAS, logujesz się swoją nazwą użytkownika i hasłem, i już masz dostęp do swoich plików i folderów. Możesz czytać i ściągać pliki z NAS albo ładować uaktualnione dokumenty, zdjęcia, filmy wideo z twojego laptopa do urządzenia NAS w każdym momencie, z dowolnego punktu na świecie.

Upewnij się, że urządzenie NAS oferuje bezpieczny szyfrowany dostęp, który jest zwykle zapewniany przez SSL. Upewnij się również, że zapewnia ono możliwość ustanowienia bezpiecznego wejścia dla gości, abyś mógł udzielić częściowego dostępu swoim zaufanym pracownikom, partnerom czy wykonawcom do niektórych plików i aby nie mieli oni dostępu do reszty zawartości dysku.

Pomocy! Mam zbyt dużo serwerów! Słyszałem coś o wirtualizacji serwerów, co to jest i co to oznacza dla mojego magazynowania danych?

Serwery mają czasami nawyk mnożenia się jak króliki, zwłaszcza jeżeli twój biznes opiera się w dużym stopniu na sieci i aplikacjach sieciowych. Nim się zorientujesz, będziesz otoczony masą serwerów, które są drogie, energochłonne i trudne w zarządzaniu. Może się również okazać, że twoje starsze, niezwykle ważne dla działalności przedsiębiorstwa aplikacje działają na starych, niewydolnych serwerach, podczas gdy najnowsze, mniej ważne aplikacje działają na nowiutkim sprzęcie, posiadającym jeszcze dużo niewykorzystanej mocy przerobowej.

Ta sytuacja jest powszechnie znana jako **„mnożenie się serwerów”** i jak w przypadku DAS jest ona niewydajna i kosztowana. Aczkolwiek istnieje na nią lekarstwo, a nazywa się ono **„wirtualizacja serwerów”.**

Wirtualizacja serwera obejmuje cały serwer, włączając w to system operacyjny oraz oprogramowanie i abstrahuje go od elementów konstrukcyjnych serwera.

Dzięki wirtualizacji serwera można upakować kilka takich zamkniętych wirtualnych serwerów, każdy ze swoim własnym systemem operacyjnym i oprogramowaniem, w jeden fizyczny serwer, bez martwienia się, że będą sobie nawzajem przeszkadzać. Można nawet umieścić serwer z systemem operacyjnym Windows obok serwera z Linuxem (albo innym dowolnym systemem operacyjnym) na jednym fizycznym serwerze i nic się nie będzie działo. Wszystkie te zamknięte serwery pracują na warstwie zwanej hypervisiorem wirtualizacji, która izoluje i zarządza oddziaływaniami pomiędzy wirtualnymi serwerami i serwerem fizycznym. Rozwiązania do wirtualizacji serwerów dostępne są u wielu różnych dostawców, z których najlepszy jest Vmware – pionier w tej dziedzinie na serwerach X86, Microsoft i Citrix.

Zalety wirtualizacji są wielorakie:

Nie występuje „mnożenie się serwerów”. Dzięki wirtualizacji możesz pomieścić kilka serwerów wirtualnych w jednym serwerze fizycznym i zredukować liczbę serwerów fizycznych o połowę, a nawet więcej. Oszczędzasz na sprzęcie, kosztach zasilania i chłodzenia, jak i na obciążeniu związanym z zarządzaniem dużą liczbą serwerów fizycznych.

Zwiększona elastyczność biznesowa. W przeciwieństwie do serwerów fizycznych, które muszą zostać zamówione, dostarczone i skonfigurowane, serwery wirtualne mogą zostać stworzone na istniejącym serwerze fizycznym w ciągu kilku minut. Przeniesienie serwera wirtualnego z jednego do drugiego serwera fizycznego też trwa tylko kilka minut i jest niezwykle proste. Dzięki wirtualizacji serwerów, firmy mogą wyposażyć nowe inicjatywy w sprzęt w ciągu kilku godzin lub dni, zamiast tygodni czy miesięcy.

Opłacalne odzyskiwanie danych w razie awarii. Wyszukane biznesowe scenariusze zachowania ciągłości biznesowej, takie jak replikacja z jednego miejsca do innego, kiedyś wymagały identycznego

sprzętu w każdej lokacji. Serwer w lokacji zapasowej zasadniczo nie robił nic, do momentu aż był potrzebny podczas awarii. Wirtualizacja pozwala na replikację fizycznego lub wirtualnego serwera do wirtualnego serwera pracującego na jakimkolwiek serwerze fizycznym.

Serwery znajdujące się w lokacji zapasowej mogą nawet obsługiwać inne aplikacje w czasie przejmowania wirtualnych replik, dzięki czemu koszty zachowania ciągłości biznesowej znacząco spadają.

Magazynowanie sieciowe jest najbardziej rentownym rozwiązaniem wirtualizacji serwerów, zwłaszcza jeżeli zamierzasz używać narzędzi takich, jak VMware's VMotion, aby przenosić wirtualne serwery z jednego serwera fizycznego do drugiego.

Rozwiązania do wirtualizacji generalnie współpracują tak z urządzeniami NAS, jak i z SAN.

NAS tworzy świetne, umiarkowanie drogie rozwiązanie, które jest łatwe w konfiguracji i użyciu do implementacji wirtualizacji serwerów. Upewnij się, że twoje urządzenie NAS było testowane i uzyskało certyfikat twojego rozwiązania do wirtualizacji, czy jest to VMware, Microsoft, Citrix, czy jakikolwiek inny dostawca. Dla opartych na wirtualnych serwerach aplikacji, które wymagają blokowej wydajności SAN, poszukaj urządzenia NAS, które pozwoli ci przydzielić część pamięci dla opartej na SAN przestrzeni magazynowej.

Każdy rodzaj magazynowania sieciowego musi mieć bardzo wysoki poziom niezawodności, jeżeli ma on być dzielony pomiędzy wiele aplikacji bądź użytkowników. Jeżeli zamierzasz połączyć wirtualizację z NAS, upewnij się, że wybrane przez ciebie urządzenie oferuje tolerujące błędy, niezawodne rozwiązania, takie jak RAID i obsługuje zasilacze awaryjne, które będą dostarczać zasilanie w przypadku przerwy w dostawie prądu. Niektóre urządzenia NAS są dostarczane również z dyskami wymienialnymi przez użytkownika, dzięki czemu możesz je szybko przywrócić do pracy w razie awarii dysku twardego.

Z jakich innych przydatnych dla małych firm aplikacji mógłbym skorzystać dzięki mojemu urządzeniu NAS?

Zaletą urządzeń NAS, poza niskimi kosztami użytkowania i łatwością obsługi, jest to, że często są one wyposażone w cechy, które czynią niezwykle prostymi implementacje bardzo ważnych dla małych przedsiębiorstw funkcji.

Serwer medialny. Niektóre urządzenia NAS mają wbudowany serwer medialny, który pozwala na strumieniowe podawanie filmów i innej zawartości komputerom i innym urządzeniom poprzez sieć albo Internet.

Ładowanie zdjęć. Niektóre urządzenia NAS są wyposażone w proste narzędzia do automatycznego ładowania zdjęć do sieciowej przestrzeni magazynowej przy użyciu portu USB albo bezprzewodowego Blutotooth. Te cechy mogą być szczególnie przydatne w branżach takich, jak ubezpieczenia czy nieruchomości, gdzie dość często robi się zdjęcia w terenie. Dzięki zdalnemu dostępowi można załadować zdjęcia do pamięci sieciowej z dowolnej lokalizacji zaraz po ich zrobieniu.

Monitoring wideo. Wiele sklepów detalicznych i innych małych przedsiębiorstw może bardzo dużo zyskać dzięki taniemu i łatwemu w użyciu monitoringowi wideo. Sieciowe kamery IP są idealnym rozwiązaniem dla monitoringu wideo. Niektóre urządzenia NAS wyposażone są w narzędzia, które automatycznie wykrywają kamery i zapewniają prosty interfejs w celu ustawienia twojego systemu monitoringu. Możesz obserwować obraz „na żywo" z dowolnego podłączonego do sieci komputera przy użyciu zwykłej przeglądarki internetowej, a nawet z twojego iPhone'a, jeżeli twój NAS oferuje zdalny dostęp oparty na przeglądarce. Możesz również zaplanować nagrywanie w wybranych przez ciebie godzinach. Upewnij się, czy twoje urządzenie NAS będzie współpracować z wybranymi przez ciebie kamerami sieciowymi.

Monitory reklamowe. Monitory reklamowe pojawiają się w coraz większej liczbie miejsc, informując klienta o specjalnych promocjach czy okazjach.

Zgodnie z badaniami przeprowadzonymi przez firmę Arbitrom, 75 proc. badanych klientów uznaje monitory reklamowe za przydatne, a 29 proc. z nich dokonało nieplanowanego zakupu po obejrzeniu reklamy produktu na monitorze reklamowym. Monitory reklamowe mogą być drogie, ale niektóre urządzenia NAS są wyposażone we wbudowane serwery medialne, które mogą przesyłać obraz wideo do cyfrowych ramek na zdjęcia. Podłącz swoją cyfrową ramkę na zdjęcia do sieci LAN gdziekolwiek w sklepie i możesz przesłać do niej dowolną zawartość ze swojego NAS, nieważne czy mają to być zdjęcia, muzyka czy film wideo.

Możliwości są nieograniczone i zależą głównie od potrzeb twojej firmy, a otrzymujesz również solidną, przystępną cenowo macierz dyskową dla twoich plików.

Nie należy niepotrzebnie niczego komplikować

Przez wszystkie wymagania, nakazy i przepisy dotyczące małych firm i przechowywania przez nie informacji, prowadzenie firmy i zapewnienie danym odpowiedniego poziomu ochrony może być momentami przytłaczające. Dlatego tak ważne jest, aby nie komplikować niczego niepotrzebnie. Jeżeli twoje potrzeby mogą zostać spełnione przez NAS, zamiast przez w pełni oprzyrządowany serwer, to wybierz NAS. Jeżeli wydaje ci się, że potrzebujesz wydajności SAN dla konkretnych aplikacji albo ochrony plików, zobacz, czy nie dałoby się spełnić tych potrzeb dzięki NAS, który oferuje część przestrzeni magazynowej SAN.

Jeżeli żyjesz na obszarze, na którym zdarzają się huragany, powodzie albo trzęsienia ziemi i musisz posiadać kopię zapasową swoich danych poza miejscem pracy, zastanów się, czy nie lepiej będzie ci wykupić usługę sieciowego przechowywania danych niż ustanawiać własne zapasowe centrum przechowywania danych. Nie komplikuj niepotrzebnie spraw, a będziesz mógł poświęcić więcej czasu i środków na prowadzenie firmy, niż na rozwiązywanie problemów związanych ze złożonością rozwiązań technicznych. ■

Przyszłość Internetu do roku 2025

Grzegorz Kantowicz

Ewolucja Internetu

Cisco oraz Global Business Network (GBN) Grupy Monitor, światowy lider w dziedzinie planowania scenariuszy, opublikowały raport pt. „Ewolucja Internetu". Raport omawia siły napędowe i czynniki niepewności, których kombinacja ukształtuje Internet w perspektywie najbliższych 15 lat.

W wyniku trwających ponad rok badań, gromadzenia danych i wywiadów opracowano cztery różne możliwe scenariusze, które zostały szczegółowo opisane w raporcie. Ze scenariuszy tych wynika, jaki wpływ mogą mieć różne istotne czynniki, takie jak polityka neutralności sieciowej, inwestycje w infrastrukturę, reakcja konsumentów na nowe modele pobierania opłat czy przyswajanie nowych technologii.

Jeden ze scenariuszy opisuje dobrze znaną prognozę, zgodnie z którą Internet będzie się w dalszym ciągu rozwijać bez skrępowania, nadal wprowadzając nowatorskie produkty i usługi. Pozostałe scenariusze kwestionują te przewidywania, wskazując na różne czynniki ryzyka oraz możliwości stojące przed decydentami biznesowymi i politycznymi.

Jak zauważa **Enrique Rueda-Sabater**, współautor raportu i dyrektor ds. strategii i ekonomii rynków wschodzących w Cisco:

– Kolejne dwa czy trzy miliardy użytkowników Internetu to ludzie głównie na rynkach wschodzących, bardzo różni od pierwszych dwóch miliardów. Globalne modele biznesowe i polityki krajowe zawiodą, jeśli będą oparte na nieaktualnych oczekiwaniach dotyczących zachowań, preferencji i sukcesu.

Zaś **Peter Schwartz**, współzałożyciel GBN, udziałowiec Grupy Monitor i jeden z głównych autorów pracy, dodaje:

– Nie możemy przewidzieć przyszłości, ale wiemy, że decyzje dotyczące Internetu podjęte w 2010 roku będą miały długofalowe konsekwencje, w tym również niezamierzone. Mamy nadzieję, że scenariusze te będą sprzyjać pogłębionej debacie strategicznej na temat przyszłych skutków dzisiejszych decyzji, prowadzonej zarówno wewnątrz poszczególnych grup odpowiedzialnych za technologie i decyzje, jak i pomiędzy takimi grupami.

Interdyscyplinarny zespół kierowany przez Cisco i GBN zbadał siły napędowe i czynniki niepewności, które będą kształtować Internet (oraz związany z nim rynek, wart obecnie 3 bln USD i stale rosnący) do roku 2025. Wnioski z tych badań są przedstawione w formie czterech poglądowych scenariuszy, które mają na celu ułatwienie decydentom, firmom technologicznym oraz instytucjom rządowym zrozumienie i przewidywanie głównych zmian, czynników ryzyka i możliwości, a także zarządzanie nimi, tak aby potencjał Internetu w zakresie tworzenia wartości ekonomicznych i społecznych został wykorzystany w skali globalnej.

Poniżej przedstawiono strukturę raportu i jego ustalenia:

Pięć przesłanek:
Raport przedstawia pięć silnych tendencji, które już występują, stwarzając wspólną podstawę dla wszystkich scenariuszy dotyczących przyszłości Internetu. Tendencje te są związane z globalną strukturą Internetu, sposobem zarządzania nim, różnicami pokoleniowymi, technologią interfejsów oraz modelami pobierania opłat za połączenie:

- Wzrost rynku związanego z Internetem będzie miał miejsce głównie poza krajami o rozwiniętej gospodarce, czyli o wysokich dochodach.
- Sposób zarządzania Internetem w skali globalnej pozostanie zasadniczo bez zmian.
- Generacja wychowana w świecie cyfrowym będzie używać Internetu w sposób zasadniczo odmienny niż wcześniejsze generacje.
- Klawiatura QWERTY przestanie być głównym interfejsem do Internetu.
- Konsumenci będą płacić za dostęp do Internetu w sposób znacznie bardziej zróżnicowany, a stała opłata abonamentowa będzie rzadkością.

Trzy wymiary czynników niepewności:
Wiele innych czynników zmian jest w wysokim stopniu niepewnych, ale będzie wywierać istotny wpływ na przyszłość Internetu. Czynniki te można sklasyfikować w trzech wymiarach:

- Czy rozbudowa sieci szerokopasmowej będzie intensywna w wyniku skumulowanego efektu inwestycji prywatnych i publicznych, czy też będzie bardziej ograniczona?
- Czy postęp technologiczny będzie polegać bardziej na przełomowych zmianach, czy też raczej na przyrostowych udoskonaleniach?
- Czy zachowania użytkowników (w tym apetyt na coraz bogatsze aplikacje internetowe) doprowadzą do nieograniczonego wzrostu popytu, czy też popyt będzie bardziej ograniczony?

Jaki będzie Internet w roku 2025?
Jak bardzo wzrośnie w porównaniu ze stanem obecnym, gdy ma 2 mld użytkowników, a wartość obrotów na związanym z nim rynku wynosi 3 bln USD?
Czy wykorzysta w pełni swój potencjał, aby połączyć całą ludzkość, wpływając korzystnie na globalny dobrobyt, produktywność przedsiębiorstw, edukację i stosunki społeczne?
A może jego znaczenie będzie mniejsze?

Cztery scenariusze:
Występowanie tych niepewnych czynników powoduje, że można wskazać dużą liczbę możliwych scenariuszy rozwoju Internetu do roku 2025. Raport koncentruje się na czterech scenariuszach, które przedstawiają pełne wyzwań i odmienne drogi możliwego rozwoju świata:

- **PŁYNNE GRANICE:**
  Świat, w którym Internet staje się wszechobecny i działa odśrodkowo. Postęp technologiczny sprawia, że dostęp do Internetu i urządzenia stają się coraz bardziej przystępne cenowo (pomimo ograniczonych inwestycji w rozbudowę sieci), zaś globalizacja biznesu i ostra konkurencja zapewniają szybkie zaspokajanie różnorodnych potrzeb na całym świecie, w bardzo zróżnicowanych konfiguracjach i miejscach.
- **NIEPEWNY ROZWÓJ:**
  Świat, w którym silne uzależnienie od Internetu jest zahamowane, zarówno jeśli chodzi o użytkowników indywidualnych, jak i biznesowych. Bezlitosne ataki hakerów kierujących się różnymi motywami są w stanie przełamać środki ochrony stosowane przez władze i organizacje międzynarodowe. Powstają bezpieczne rozwiązania alternatywne, ale są one bardzo kosztowne.
- **NIESPEŁNIONE OBIETNICE:**
  Skromny rozwój Internetu spowodowany przedłużającą się stagnacją gospodarczą w wielu krajach. Brak jest przełomowych technologii, które kompensują te czynniki hamujące, a polityka protekcjonistyczna w odpowiedzi na kryzys gospodarczy pogarsza tylko sytuację, zarówno pod względem ekonomicznym, jak i pod względem rozpowszechnienia technologii sieciowych.
- **PĘKANIE W SZWACH:**
  Świat, w którym Internet staje się ofiarą własnego sukcesu. Zapotrzebowanie na usługi IP rośnie w sposób niepohamowany, ale ograniczenia pojemności i występujące wąskie gardła stwarzają lukę pomiędzy oczekiwaniami a realiami użycia Internetu. Międzynarodowe standardy technologiczne nie są przyjmowane, między innymi wskutek gwałtownej negatywnej reakcji w skali globalnej na dziesięciolecia dominacji USA w dziedzinie technologii.

Dwa zbiory konsekwencji:
Na koniec raport proponuje dwie osnowy badania strategii biznesowych i konsekwencji decyzji dla każdego scenariusza.

- Jakie modele biznesowe najlepiej zapewnią trwałą i zyskowną pozycję wobec Internetu na przyszłość?
- Na jakie wyzwania powinni odpowiedzieć decydenci w skali krajowej i międzynarodowej?

Zawarte w raporcie poglądowe zbiory konsekwencji pokazują, w jaki sposób opracowane scenariusze mogą pomóc decydentom w dostrzeżeniu możliwości i podjęciu już dzisiaj mądrzejszych decyzji na przyszłość. ■

Kto zarabia na internautach?

Jewgienij Asjejew

Niebezpieczeństwa Internetu

W jaki sposób Twój komputer może zostać zainfekowany, nawet gdy tylko surfujesz po Internecie? Jak cyberprzestępcy zarabiają pieniądze, oszukując użytkowników? Odpowiedzi na te pytania znajdziesz w artykule.

Cel

W ostatnich latach zagrożenie infekcją z Internetu stale wzrasta. Częściowo wynika to z rosnącej liczby internautów oraz zasobów online. Z drugiej strony, wiąże się z faktem, że cyberprzestępcy chcą zarobić jak najwięcej pieniędzy. Obecnie ataki przeprowadzane za pośrednictwem Internetu są zarówno najliczniejszym, jak i najniebezpieczniejszym typem zagrożeń.

Nasze miesięczne statystyki dotyczące szkodliwego oprogramowania potwierdzają istnienie ogromnej liczby ataków online, które stają się coraz bardziej zaawansowane. Do najbardziej złożonych zagrożeń, jakie pojawiły się w ostatnim czasie, należą ZeuS, Sinowal oraz TDSS, a wszystkie rozprzestrzeniają się za pośrednictwem Internetu. W sieci panuje również plaga fałszywych rozwiązań antywirusowych oraz programów blokujących.

Operacja Aurora – ukierunkowany atak, który cieszył się sporym zainteresowaniem mediów – również została przeprowadzona przy użyciu strony internetowej (zobacz: http://en.wikipedia.org/wiki/Operation_Aurora). Jest to zaledwie wierzchołek góry lodowej.

W atakach internetowych głównym celem cyberprzestępców jest umieszczenie i zainstalowanie szkodliwego pliku wykonywalnego na komputerze ofiary. Naturalnie, istnieją ataki, takie jak Cross-Site Scripting zwane również XSS (http://pl.wikipedia.org/wiki/Cross-site_scripting) oraz Cross-Site Forgery Requests (http://en.wikipedia.org/wiki/Cross-site_request_forgery), które nie wymagają pobierania i instalowania plików wykonywalnych na komputerach ofiar.

Jednak możliwość kontrolowania zainfekowanego systemu od wewnątrz otwiera wiele możliwości; skuteczny atak zapewnia cyberprzestępcom dostęp do danych użytkownika i zasobów systemowych. Cyberprzestępcy wykorzystają to, w ten czy inny sposób, do zarabiania pieniędzy na swoich ofiarach.

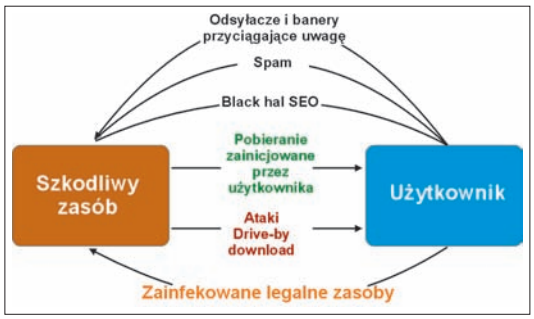
Atak

Ogólnie atak składa się z dwóch kroków: przekierowania użytkownika do zainfekowanego zasobu oraz pobrania szkodliwego pliku wykonywalnego na jego komputer.

Cyberprzestępcy wykorzystują każdy możliwy kanał do zwabienia użytkowników do swoich zainfekowanych zasobów: e-mail, komunikatory internetowe, portale społecznościowe, wyszukiwarki, reklamy – szkodliwe odsyłacze można znaleźć wszędzie. Czasami cyberprzestępcy nie muszą nic robić, aby przyciągnąć użytkowników – po prostu włamują się na legalną stronę internetową o dużej odwiedzalności. Ostatnio cyberprzestępcy coraz częściej uciekają się do tej metody.

Gdy użytkownik otworzy zainfekowany zasób, pozostaje tylko pobranie i zainstalowanie szkodliwego programu na jego komputerze. Cyberprzestępcy mają dwie możliwości: nakłonić użytkownika, aby samodzielnie pobrał program, lub przeprowadzić atak drive-by download. W pierwszym przypadku powszechnie stosowane są metody socjotechniki (zobacz: http://pl.wikipedia.org/wiki/Inżynieria_społeczna_(informatyka)), w których cyberprzestępcy żerują na naiwności i/lub braku doświadczenia użytkowników. W drugim przypadku cyberprzestępcy wykorzystują lukę w oprogramowaniu działającym na komputerze ofiary.

Na schemacie poniżej pokazano, w jaki sposób w atakach internetowych są pobierane i instalowane szkodliwe pliki:



Atak internetowy, w którym jest pobierany i instalowany szkodliwy plik

Przyjrzyjmy się dokładnie, w jaki sposób użytkownicy korzystają na co dzień z Internetu i jak mogą trafić na „złą" stronę internetową, która spowoduje infekcję komputera.

Spam

Spam jest jedną z najczęściej stosowanych taktyk przez cyberprzestępców w celu zwabienia użytkowników na zainfekowaną stronę. Ten rodzaj spamu w pełni wykorzystuje możliwości dzisiejszego Internetu. Kilka lat temu słowo „spam" kojarzyło się tylko z e-mailami reklamowymi. Obecnie spam jest rozprzestrzeniany za pośrednictwem wielu różnych kanałów: komunikatorów internetowych, portali społecznościowych, blogów, forów, a nawet wiadomości SMS.

Często wiadomości spamowe zawierają szkodliwe pliki wykonywalne lub odsyłacze do zainfekowanych zasobów. Cyberprzestępcy agresywnie wykorzystują socjotechnikę w celu przekonania użytkowników do kliknięcia odsyłaczy i/lub pobrania szkodliwych plików: umieszczają w wiadomościach odsyłacze, które rzekomo prowadzą do gorących newsów lub popularnych zasobów i firm internetowych. Ogólnie cyberprzestępcy żerują na ludzkich słabościach: strachu, ciekawości i ekscytacji. Celem tego artykułu nie jest szczegółowe zbadanie metod socjotechniki. Sporo przykładów pokazujących, w jaki sposób szkodliwe programy są rozprzestrzeniane za pomocą socjotechniki, zostało już zaprezentowanych na naszej stronie www.viruslist.pl.

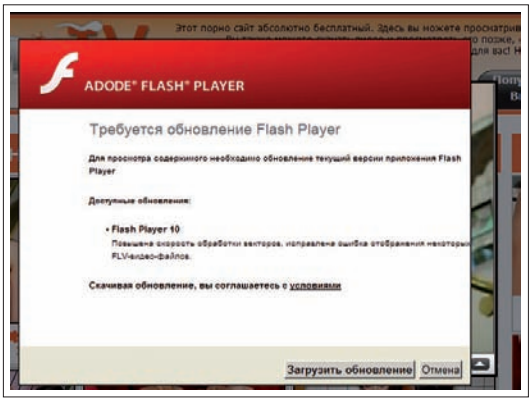
Zwracające uwagę odsyłacze i banery

Jedną z metod wykorzystywanych obecnie do przyciągania użytkowników na zainfekowane zasoby są banery reklamowe i ciekawie wyglądające odsyłacze. Z reguły metody te są najczęściej stosowane na legalnych stronach oferujących nielicencjonowane oprogramowanie lub treści dla dorosłych.

Poniżej przykład takiego ataku. Gdy użytkownik wpisał do wyszukiwarki Google hasło „download crack for assassin's creed 2" – popularne wyszukiwanie w maju 2010 roku – wśród wyników pojawiał się adres strony internetowej, która po załadowaniu wyświetlała baner pływający reklamujący Forex-Bazar.

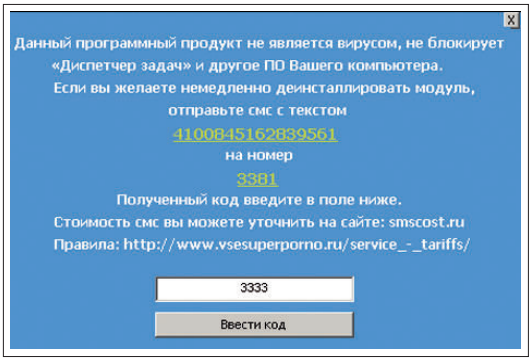
Baner pływający na stronie internetowej oferującej nielicencjonowane oprogramowanie

Próba zamknięcia banera powodowała otwarcie nowego okna przeglądarki. Okno to wyświetlało stronę internetową oferującą filmy dla dorosłych. Po kliknięciu „preview" dowolnego z tych filmów pojawiał się komunikat informujący o konieczności zainstalowania aktualizacji programu Adobe Flash Player w celu obejrzenia materiału.



Wiadomość wyświetlana na stronie internetowej w wyniku próby obejrzenia filmu dla dorosłych
[Komunikat ten informuje użytkowników, że nie będą mogli obejrzeć żądanej zawartości, dopóki nie zainstalują najnowszej wersji Flash Playera.]

Kliknięcie „pobierz aktualizację", a następnie „zainstaluj aktualizację" powodowało zainstalowanie się na komputerze użytkownika nie aktualizacji firmy Adobe, ale jednego z najnowszych wariantów Trojan-Ransom.Win32.XBlocker. Program ten otwierał okno na innych oknach i wyświetlał komunikat, w którym informował, że należy wysłać wiadomość tekstową na krótki numer, aby otrzymać klucz umożliwiający „natychmiastową dezinstalację tego modułu" i zamknąć okno.



Okno pojawiające się po zainstalowaniu Trojan-Ransom.Win32.XBlocker
[Tłumaczenie: Ten program nie jest wirusem, nie blokuje Menedżera zadań ani innego oprogramowania na twoim komputerze. Jeżeli chcesz natychmiast odinstalować ten moduł, wyślij SMS o treści 4100845162839561 na numer 3381. W polu poniżej wprowadź otrzymany kod. Koszt SMS-a można sprawdzić na stronie smscost.ru. Warunki: http://www.vsesuperporno.ru/service_-_tariffs/]

Black hat SEO

SEO (*Search Engine Optimization*) oznacza metody wykorzystywane w celu poprawy pozycji danej strony internetowej w wynikach wyświetlanych przez wyszukiwarkę w odpowiedzi na określone frazy zapytania. Obecnie wyszukiwarki stanowią kluczowe narzędzie podczas poszukiwania informacji; im

łatwiej znaleźć stronę internetową, tym większe będzie zapotrzebowanie na oferowane przez nią usługi.

Istnieje wiele metod SEO – zarówno legalnych, jak i zakazanych przez wyszukiwarki. Firmę Kaspersky Lab szczególnie interesuje stosowanie niedozwolonych metod SEO, znanych również jako hat SEO (http://pl.wikipedia.org/wiki/Spamdexing). Techniki te są powszechnie wykorzystywane przez cyberprzestępców do promowania zainfekowanych zasobów.

Poniżej ogólny opis, w jaki sposób użytkownicy trafiają na „zoptymalizowane" zasoby, oraz co robią cyberprzestępcy, aby ich zasoby były bardziej widoczne.

Przy użyciu słów kluczowych, które mogą być wprowadzane ręcznie lub automatycznie (na przykład przy pomocy Google Trends), cyberprzestępcy tworzą strony internetowe o określonej zawartości. Zwykle odbywa się to automatycznie: boty tworzą zapytania do wyszukiwarek i kradną zawartość ze stron, które pojawiają się na najwyższych miejscach w wynikach wyszukiwania.

Aby zagwarantować pojawienie się nowej strony internetowej w najwyższych wynikach wyszukiwania, ich twórcy muszą „zmusić" roboty sieciowe, lub pająki, do zindeksowania takiej strony. Najprościej jest zapoczątkować proces indeksowania ręcznie, wykorzystując, na przykład, strony na http://www.google.com/addurl" target=blank. Następnie na nowo utworzonej stronie jest umieszczany skrypt, który przy użyciu przetwarzania nagłówków http może zostać wykorzystany do zidentyfikowania odwiedzających. Jeżeli odwiedzającym jest robot sieciowy, „wyświetlana" jest strona z zawartością związaną z wybranymi słowami kluczowymi. W rezultacie strona będzie widniała wyżej na liście zwróconych wyników wyszukiwania. Jeżeli użytkownik trafi na tę stronę z wyszukiwarki, zostanie przekierowany na zainfekowaną witrynę.

Black hat SEO: tworzenie i prezentowanie danych

Strony promowane przy użyciu nielegalnych lub wątpliwych metod są natychmiast usuwane przez wyszukiwarki z wyników wyszukiwania.

Dlatego właśnie cyberprzestępcy wykorzystują z reguły zautomatyzowane procesy tworzenia i optymalizacji takich stron; powoduje to przyspieszenie procesu i zwiększenie liczby nowych zainfekowanych zasobów sieciowych.

Automatycznie tworzone strony internetowe mogą zostać umieszczone w dowolnym miejscu: w zasobach cyberprzestępców, zainfekowanych legalnych zasobach, darmowych serwisach hostingowych lub platformach blogowych.

Opisane wyżej metody infekcji są skuteczne tylko wtedy, gdy użytkownik zgodzi się na pobranie programu. Użytkownik często pobiera taki plik, szczególnie gdy jest niedoświadczony lub nie zwraca uwagi na detale.

W tym procesie wykorzystywane są również ludzkie słabości. Na przykład, jeżeli pojawia się okienko wyskakujące, informujące, że komputer został zainfekowany, użytkownik może zaniepokoić się, a jeżeli jest niedoświadczony może jak najszybciej kliknąć „usuń wszystkie zagrożenia". Okienko sugerujące użytkownikowi, aby pobrał aktualizację dla Adobe Flash Player lub kodek, nie wzbudzi podejrzeń, zwłaszcza gdy wygląda na legalne; ponadto użytkownik pewnie wielokrotnie klikał już takie odnośniki podczas pobierania standardowych, legalnych aktualizacji.

Zainfekowane legalne zasoby

Szczególną popularność zyskała jedna z metod rozprzestrzeniania szkodliwych programów: ukryte ataki typu drive-by download. Tego typu atak polega na infekowaniu komputera bez wiedzy i udziału użytkownika. Większość ataków drive-by download jest przeprowadzana z zainfekowanych legalnych zasobów.

Zainfekowane legalne zasoby należą do najpoważniejszych problemów w Internecie. Media publikowały informacje o takich nagłówkach, jak: „W wyniku masowego ataku tysiące stron internetowych zostały zainfekowane szkodliwym oprogramowaniem", „Luki w zabezpieczeniu prowadzą do masowych ataków hakerskich. Czy twój blog będzie następny?" oraz „Lenovo Strona pomocy Lenovo infekuje odwiedzających trojanem".

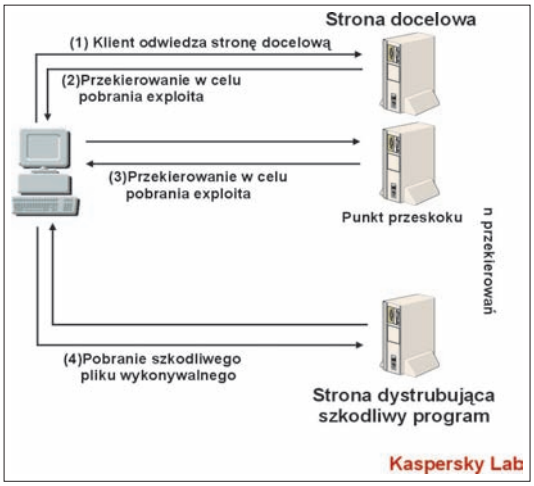
Każdego dnia Kaspersky Lab identyfikuje tysiące zainfekowanych zasobów, które pobierają szkodliwy kod na komputer użytkownika bez jego wiedzy i zgody.

Z reguły ataki drive-by nie wymagają przekonywania użytkownika, aby odwiedził określoną stronę; użytkownik sam trafia na tę stronę. Może to być na przykład legalna (ale zainfekowana) strona, którą odwiedza codziennie, aby przeczytać wiadomości lub zamówić określony produkt.

Zasób zwykle jest infekowany na jeden z dwóch sposobów: za pośrednictwem luki w zasobie (na przykład: SQL injection) lub przy użyciu wcześniej skradzionych poufnych danych dostępu do strony internetowej. Najpopularniejszą metodą jest dodawanie do kodu źródłowego strony ukrytego znacznika o nazwie iframe. Iframe zawiera odsyłacz do zainfekowanego zasobu i automatycznie przekierowuje użytkownika, gdy odwiedza on zainfekowaną stronę internetową.

Zainfekowany zasób zawiera exploita lub pakiet exploitów, który zostaje uruchomiony, jeżeli użytkownik posiada na swoim komputerze podatne na atak

oprogramowanie. Powoduje to pobranie i uruchomienie szkodliwego pliku wykonywalnego.



Jak działa typowy atak drive-by

Rysunek poniżej (z Google) pokazuje, jak działają takie ataki:

Pakiety exploitów

W dzisiejszych atakach typu drive-by powszechnie stosuje się pakiety exploitów. Pakiet exploitów to zestaw programów, które wykorzystują luki w legalnym oprogramowaniu uruchomionym na komputerze ofiary. Innymi słowy, exploity otwierają swego rodzaju tylne drzwi, poprzez które szkodliwe programy mogą zainfekować komputer.

Ponieważ ataki w Internecie odbywają się za pośrednictwem przeglądarki, cyberprzestępcy wykorzystują luki w przeglądarce, w dodatkach do przeglądarki lub oprogramowaniu innego producenta wykorzystywanym do przetwarzania zawartości. Głównym celem pakietów exploitów jest pobieranie i uruchamianie wykonywalnych szkodliwych plików bez wiedzy użytkownika.

Typowy zestaw dodatków do przeglądarki Firefox

Poniższy zrzut ekranu pokazuje typowy zestaw dodatków dla Firefoksa. Zaznaczono na nim wersje posiadające luki w zabezpieczeniach, które zostały wykorzystane we wcześniejszych atakach na użytkowników. Co więcej, luki zidentyfikowano również (i wykorzystano) w samym Firefoksie.

Obecnie pakiety exploitów stanowią najwyższe osiągnięcie w ewolucji ataków typu drive-by download i są regularnie modyfikowane oraz uaktualniane. W ten sposób cyberprzestępcy chcą mieć pewność, że pakiety te zawierają exploity na nowe luki i potrafią skutecznie zwalczać mechanizmy bezpieczeństwa.

Pakiety exploitów tworzą niszę na rynku usług cyberprzestępczych. Obecnie na czarnym rynku można znaleźć wiele pakietów exploitów; różnią się ceną, liczbą exploitów w pakiecie, funkcjonalnością interfejsu administratora i poziomem oferowanej obsługi klienta. Oprócz gotowych pakietów tworzy się również zestawy exploitów na zamówienie – z usługi tej korzystają niektóre gangi cyberprzestępcze.

Najpowszechniejsze pakiety tworzone na zamówienie to te wykorzystywane w atakach z udziałem szkodników Gumblar i Pegel (downloadery skryptów).

Tym, co wyróżnia najnowszą wersję Gumblara, jest zautomatyzowany proces infekowania stron internetowych i komputerów użytkowników końcowych.

W atakach wykorzystywane są zarówno exploity, jak i pliki wykonywalne, które są umieszczane w zhakowanych zasobach. Gdy użytkownik odwiedzi zainfekowany przez Gumblara zasób, zostanie przekierowany na inną zainfekowaną stronę, która zainfekuje jego komputer.

W atakach Gumblara wykorzystywane są znane luki w zabezpieczeniach programów Internet Explorer, Adobe Acrobat/Reader, Adobe Flash Player oraz tych stworzonych w języku programowania Java.

Również Pegel rozprzestrzenia się za pośrednictwem zainfekowanych legalnych stron, jednak komputery ofiar są infekowane przy użyciu serwerów kontrolowanych przez cyberprzestępców.

Metoda ta ułatwia cyberprzestępcom modyfikację pliku wykonywalnego oraz pakietu exploitów, pozwalając na szybką reakcję na nowe luki w zabezpieczeniach. Na przykład, jeden cyberprzestępca dodał do pakietu exploita wykorzystującego lukę w Java Deployment Toolkit. Zrobił to niemal natychmiast po tym, jak udostępniono kod źródłowy. Downloader Twetti jest kolejnym trojanem, który wykorzystuje interesujące techniki. Szkodnik ten tworzy wiele żądań do API Twittera, a otrzymane dane wykorzystuje do wygenerowania pseudolosowej nazwy domeny. W rezultacie użytkownicy są przekierowywani do domeny o tej nazwie.

Cyberprzestępcy stosują podobny algorytm w celu uzyskania nazwy domeny, zarejestrowania jej, a następnie umieszczenia na stronie szkodliwych programów, które mają być pobierane na maszyny ofiar.

Pieniądze

Kto zarabia na tych atakach i w jaki sposób?

Ataki wykorzystujące banery reklamowe to świetny interes dla właścicieli zasobów sieciowych wyświetlających takie banery, ponieważ otrzymują oni pieniądze za umieszczenie ich w swoich zasobach. Jeżeli XBlocker zostanie pobrany i zainstalowany na maszynie ofiary, skorzystają na tym cyberprzestępcy wykorzystujący tego szkodnika, ale tylko wtedy, gdy użytkownik wyśle SMS na krótki numer. Jednak niedoświadczeni użytkownicy często chwytają przynętę.

W przypadku techniki black hat SEO i ataków wykorzystujących zoptymalizowane w ten sposób strony korzyści odnoszą osoby, które stworzyły system dystrybucji, osoby, które rozwinęły oprogramowanie do automatycznego tworzenia fałszywych stron internetowych, oraz pośrednicy między tymi stronami. Jeżeli użytkownik pobierze i zainstaluje fałszywy program antywirusowy, skorzystają na tym cyberprzestępcy, którzy przeprowadzili atak.

Mniej doświadczeni użytkownicy zwykle zgadzają się na instalację i zapłacenie za fałszywe programy antywirusowe, co przynosi dochody osobom, które rozwijają takie oprogramowanie. Twórcy pakietów exploitów zarabiają na atakach drive-by, podobnie jak osoby, które wykorzystują te pakiety. Przykładem może być pakiet exploitów ZeuS Toolkit – efektywny sposób gromadzenia poufnych danych użytkowników, które są następnie sprzedawane na czarnym rynku. W wyniku regularnych ataków przy użyciu programu Pegel przeprowadzonych przez szkodliwych użytkowników powstał botnet składający się z komputerów zainfekowanych backdoorem o nazwie Backdoor.Win32.Bredolab.

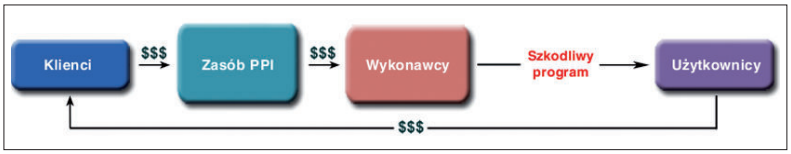
Botnet ten może być wykorzystywany do pobierania innych szkodliwych programów na komputery ofiar. Czy to oznacza, że cyberprzestępcy zarabiają pieniądze, gdy użytkownicy pobierają szkodliwe programy? Naturalnie! Przy pomocy programów partnerskich (zwanych w języku rosyjskim „partnerka") zyski z tej działalności są przekazywane odpowiedniemu partnerowi lub partnerom.

Sieci partnerskie

Programy partnerskie działają już od jakiegoś czasu; początkowo były wykorzystywane głównie do rozprzestrzeniania oprogramowania adware powiązanego z darmowymi aplikacjami. Wraz z bezpłatnymi aplikacjami pobierany był „bonus" w postaci programu adware. Obecnie programy partnerskie są często wykorzystywane do rozprzestrzeniania szkodliwego oprogramowania.

„Czarny", czyli nielegalny model PPI (*pay-per-install*) obejmuje następujących uczestników (tj. partnerów):

- Klientów: cyberprzestępców, którzy posiadają trochę pieniędzy i szkodliwe oprogramowanie, które chcą rozprzestrzeniać
- Wykonawców: osoby, które rozprzestrzeniają program i otrzymują za to pieniądze. Często taki partner nie zadaje żadnych pytań na temat programu, który rozprzestrzenia; w rezultacie może bezwiednie stać się narzędziem do przeprowadzania cyberprzestępstw (trzeba jednak pamiętać, że niewiedza nie stanowi o niewinności).
- Zasobu PPI: jest to organizacja, która łączy klientów z wykonawcami i pobiera prowizję od ich transakcji.



Działanie modelu PPI

Oprócz modeli PPI, w których każdy może brać udział, istnieje również wiele „zamkniętych" programów partnerskich. Wstęp do nich mają tylko główni gracze na scenie cyberprzestępczej, tacy jak na przykład właściciele botnetów. Nie trzeba mówić, że przez takie sieci partnerskie przepływają ogromne sumy pieniędzy.

Pozostaje pytanie: Skąd lub od kogo pochodzą te pieniądze? Odpowiedź naturalnie brzmi: Od użytkowników. Łupem padają ich własne środki, poufne dane oraz/lub moc obliczeniowa ich komputerów.

Wnioski

Naturalnie opisane wyżej podejścia i techniki nie wyczerpują wszystkich metod wykorzystywanych przez cyberprzestępców. Internet stanowi obecnie niebezpieczne miejsce – wystarczy kliknąć odsyłacz wyświetlony w wynikach wyszukiwania lub odwiedzić ulubioną stronę internetową, która niedawno została zainfekowana, i zanim się zorientujemy, komputer staje się częścią botnetu.

Głównym celem cyberprzestępców jest pozbawienie użytkowników pieniędzy i poufnych danych; dane te mogą posłużyć do osiągania korzyści finansowych. Z tego powodu cyberprzestępcy wykorzystują każdą broń, jaką posiadają w swoim arsenale, aby „zagnieździć" szkodliwe programy na komputerach użytkowników.

Aby zapewnić sobie ochronę, użytkownicy muszą regularnie aktualizować swoje oprogramowanie, zwłaszcza oprogramowanie, które współpracuje z przeglądarką. Ważną rolę odgrywa również aktualne rozwiązanie bezpieczeństwa.

Najważniejsze jest jednak to, aby użytkownicy zachowali ostrożność podczas udostępniania swoich informacji przez Internet.

Autor jest analitykiem zagrożeń w Kaspersky Lab

Spam na portalach społecznościowych

Karolina Karwowska

Przyjaciel widmo atakuje Facebooka

Techniki jakie stosują spamerzy, stają się coraz bardziej wyrafinowane. Są też na bieżąco, bardzo zręcznie dopasowywane do specyfiki serwisów społecznościowych i zmieniających się upodobań internautów. Okazuje się też, że mimo rosnącej świadomości użytkowników Facebooka, spam nadal trafia tam na bardzo podatny grunt.

Nowe, wirtualne FortiGate®, FortiManager™, FortiAnalyzer™ i FortiMail™ zostały zaprojektowane do pracy w zgodzie z technologią VMware ESX oraz ESXi. Zwirtualizowane modele współpracują ze swoimi sprzętowymi odpowiednikami dając możliwość wyboru między formą fizyczną a wirtualną w celu eliminowania zagrożeń płynących ze stref niekontrolowanych i gwarantując zarządzanie bezpieczeństwem w środowiskach infrastruktury zwirtualizowanej. Połączone rozwiązanie zapewnia lepszą integrację ze środowiskami wirtualnymi i pozwala chronić usługi oferowane w zwirtualizowanej strukturze sieciowej.

Wirtualny FortiGate, podobnie jak tradycyjne modele, stanowi zintegrowaną wirtualną bramę bezpieczeństwa chroniąc infrastrukturę przed wieloma zagrożeniami. Rozwiązanie umożliwia integrację dotąd oddzielnych technologii oraz ogranicza koszty i stopień złożoności infrastruktury bezpieczeństwa. Klienci mogą połączyć zaporę sieciową, funkcję VPN, mechanizm zapobiegania penetracji, zapobiegania oprogramowaniu złośliwemu, zabezpieczenia aplikacji i kompleksową ochronę treści, mechanizm zapobiegania utracie danych, filtrowanie sieci WWW czy funkcje przeciwspamowe i mają dodatkową możliwość kontroli ruchu międzystrefowego. Ponadto wirtualny FortiGate może być używany w powiązaniu z tradycyjnymi urządzeniami FortiGate w celu zapewnienia ochrony zarówno w warstwie brzegowej, jak i w wirtualnych strefach bezpieczeństwa.

Wirtualny FortiManager dostarcza narzędzi niezbędnych do skutecznego zarządzania infrastrukturą bezpieczeństwa. Bazując na zdefiniowanych strategiach, rozwiązanie oferuje scentralizowane udostępnianie, konfigurację i zarządzanie aktualizacjami dla FortiGate, FortiWiFi i FortiMail, jak również dla agentów punktów końcowych FortiClient.

Wirtualny FortiAnalyzer bezpiecznie agreguje dane z dzienników urządzeń Fortinet i innych urządzeń kompatybilnych z narzędziem syslog. Dzięki zastosowaniu kompleksowego systemu raportowania użytkownicy mogą filtrować i przeglądać raporty, łącznie ze sprawozdaniami dotyczącymi ruchu, zdarzeń, wirusów, ataków, treści WWW i danych poczty elektronicznej oraz uszczegóławiać dane w celu określenia sytuacji bezpieczeństwa i zapewnienia zgodności z wymogami regulacyjnymi. FortiAnalyzer udostępnia również zaawansowane funkcje zarządzania bezpieczeństwem, takie jak archiwizacja plików poddanych kwarantannie, korelowanie zdarzeń, ocena punktów wrażliwych, analiza ruchu oraz archiwizacja treści poczty elektronicznej, dostępu do sieci WWW, komunikatorów internetowych oraz przesyłu plików.

Wirtualny FortiMail do ochrony poczty elektronicznej został zaprojektowany w celu blokowania przychodzącego spamu i oprogramowania złośliwego, zanim zdoła ono zakorkować sieć i zainfekować użytkowników. Urządzenie pomaga również zapobiegać wysyłaniu spamu lub oprogramowania złośliwego (w tym również w ruchu mobilnym 3G), co może spowodować, że inne bramki przeciwspamowe umieszczą użytkowników na czarnych listach.

Wirtualne rozwiązania Fortinet pracują w sposób zbliżony do swoich fizycznych odpowiedników – firma Fortinet w dalszym ciągu udostępnia technologie domeny wirtualnej (*Virtual Domain*, VDOM) oraz domeny administracyjnej (*Administrative Domain*, ADOM) do celów zabezpieczania i zarządzania środowiskami wirtualnymi i obsługującymi wielu dzierżawców. Technologie wirtualizacji współpracują z branżowymi standardami dla sieci VLAN (wirtualna sieć LAN), dzięki czemu jedno wirtualne lub fizyczne urządzenie Fortinet jest w stanie obsługiwać setki domen leżących w obrębie środowiska, zapewniając niezbędną widoczność i możliwości kontroli zabezpieczeń między strefami, a jednocześnie zachowując wszelkie korzyści płynące z wirtualizacji.

Fortinet zajmuje się ochroną wirtualnej architektury sieciowej od wprowadzenia technologii domeny wirtualnej (VDOM) w 2004 roku. Firma rozszerzyła swoje kompetencje w zakresie wirtualizacji po nabyciu w 2006 roku praw do własności intelektualnej i technologii CoSine Communications, jednego z pierwszych liderów branży wirtualnych urządzeń. Dzięki stosowaniu tych rozwiązań, dostawcy usług mają do dyspozycji wysokiej klasy platformę zwirtualizowanych usług bezpieczeństwa sieci. Duże przedsiębiorstwa z pełnym zaufaniem korzystają z technologii Fortinet w celu ochrony danych w ich prywatnych i hybrydowych chmurach.

Wirtualne urządzenia FortiGate i FortiManager są już dostępne w Polsce. Obecnie dostępne są trzy opcje licencjonowania, które reprezentują trzy wirtualne modele systemu FortiGate-VM. Każdy model licencjonowany jest na określoną liczbę wirtualnych procesorów (vCPU): 2, 4 lub 8. Do każdego modelu – tak jak w wersji sprzętowej systemów FortiGate – należy doliczyć serwisy FortiCare oraz subskrypcję FortiGuard. ■

www.info-tel.pl

Od stycznia 2011 roku Infotel będzie wydawany wyłącznie elektronicznie poprzez witrynę www.info-tel.pl, którą już udostępniamy w wersji Beta.

- wywiady i konferencje online
- artykuły Infotela i Infotel w PDF i E-Pub
- serwisy:
  - ☑ informacyjny
  - ☑ kalendarz wydarzeń
  - ☑ dotychczasowe archiwa
  - ☑ Kongres
  - ☑ Konkurs

Zapraszamy do prenumeraty!

Roczna elektroniczna prenumerata to koszt **200 zł netto**

www.info-tel.pl

INFOTEL 1997 MSG MEDIA
ul. Chwytowo 2, 85-223 Bydgoszcz, tel. (052) 325 83 10, fax (052) 373 52 43
e-mail: office@msgmedia.pl, www.techbox.pl

INFOTEL 1997

wykorzystaj naszą wiedzę i doświadczenie

W branży działamy od 13 lat. Dzięki zgromadzonej wiedzy, współpracy z wybitnymi ekspertami, bazie danych, możemy w sposób profesjonalny i kompleksowy komunikować się z rynkiem.

13 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 MEDIA
ul. Chwytowo 2, 85-223 Bydgoszcz; tel. (52) 325 83 10; fax (52) 373 52 43
e-mail: office@msgmedia.pl; www.techbox.pl

ANKIETA CZYTELNIKA

XIII edycja konkursu o LAUR INFOTELA

„Złoty Laur Czytelników INFOTELA" w kategoriach:

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

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

operator satelitarny .....
(nazwa operatora)

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

nadawca i dystrybutor telewizyjny .....
(nazwa nadawcy)

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

witryna internetowa .....
(nazwa witryny)

Drogi Czytelniku,

budowanie przyjaznych relacji między firmą a klientem
opiera się na wzajemnym zaufaniu oraz wykorzystaniu
nowych technologii w maksymalnym uproszczeniu procedur
związanych z wprowadzeniem innowacyjnych usług
ukierunkowanych na użytkownika.

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

..... e-mail

..... telefon

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

6.05.2011 r.

ORGANIZATOR:
ul. Chwytowo 2, 85-223 Bydgoszcz, tel. (052) 325 83 10, fax (052) 373 52 43
e-mail: office@msgmedia.pl, www.techbox.pl

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

II. KATEGORIE:
- innowacyjna gmina;
- innowacyjna firma;
- innowacyjna usługa /innowacyjny produkt

III. KATEGORIE:
- osoba;
- firma;
- instytucja

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

INFOTEL 1997 TECHBOX.PL MSG MEDIA

XIII edycja konkursu o
LAUR INFOTELA

Patronat honorowy:

- **Ministerstwo Infrastruktury**
- **Urząd Komunikacji Elektronicznej**

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

MSG MEDIA
ul. Chwytowo 2, 85-223 Bydgoszcz, tel. (052) 325 83 10, fax (052) 373 52 43
e-mail: office@msgmedia.pl, www.techbox.pl

X Kongres INFOTELA

8–11 czerwca 2011 r.

Hotel Gołębiewski MIKOŁAJKI

20 LAT INTERNETU W POLSCE

REGULACJE • BIZNES • TECHNOLOGIE

- Historia, dzień dzisiejszy i przyszłość Internetu;
- Regulacje w komunikacji elektronicznej;
- Główne trendy rozwoju w komunikacji elektronicznej i ich wpływ na biznes;
- Technologie i usługi: mobilność, cyfryzacja, kontent, multimedia;
- Telewizja cyfrowa;
- Przyszłość mobilnych usług multimedialnych;
- Strategie rozwoju usług szerokopasmowych;
- Czy nowoczesne technologie bezprzewodowe rozwiążą problem powszechnego dostępu do szerokopasmowego Internetu?

Imprezy towarzyszące:

- Rozstrzygnięcie XIII edycji ogólnopolskiego konkursu o LAUR INFOTELA;
- Uroczysta Gala Komunikacji Elektronicznej;
- Wieczór w Oberży u Markiza;
- Rejs statkiem po mazurskich jeziorach;
- Turniej o Puchar INFOTELA w bowlingu;
- Ogólnopolski konkurs w rzucie komórką na odległość.

MSG MEDIA
ul. Chwytowo 2, 85-223 Bydgoszcz, tel. (052) 325 83 10, fax (052) 373 52 43
e-mail: office@msgmedia.pl, www.techbox.pl