NASK

BIULETYN NASK

nr 3/4/99

To już dziesięć lat...

Tym razem zaczynamy od wspomnień. Skłania do tego pamiątkowe zdjęcie zrobione przy samochodzie, który jest dla nas symbolem Naukowej i Akademickiej Sieci Komputerowej. To stare czerwone volvo, kupione już jako używany samochód, było z nami od początku. W czasach, gdy powstawała sieć NASK i później – w czasie jej eksploatacji, nasi technicy przejechali nim Polskę wzdłuż i wszerz. Było pakowne i niezawodne. Jego żywot w niełatwej służbie NASK zakończył się definitywnie w październiku tego roku. Kończy się też pionierska epoka sieci NASK. Czas płynie, zmienia się Internet, zmienia się również nasza firma. Zanim wkroczymy w rok 2000 popatrzmy wstecz. Pomogą nam w tym relacje dyrektora NASK, Tomasza Hofmokla i wieloletniego dyrektora technicznego NASK, Andrzeja Zienkiewicza.

W grudniu mija właśnie 10 lat od chwili, gdy przedstawiciele środowiska akademickiego Warszawy odbyli decydujące spotkanie z Prof. Stefanem Amsterdamskim, sekretarzem w Urzędzie Postępu Naukowo-Technicznego i Wdrożeń, w sprawie dołączenia Polski do sieci komputerowych (spotkanie odbyło się 15 grudnia 1989 r.) Były to czasy, które przeszły do historii tej części Europy. Przypomnijmy:

- początek września 1989: powstaje rząd Tadeusza Mazowieckiego;
- początek listopada 1989: wali się mur berliński;
- połowa listopada: w Pradze zaczyna się aksamitna rewolucja, a w Warszawie pada pomnik Feliksa Dzierżyńskiego.

W dziedzinie technologii można w skrócie określić ten czas jako koniec embarga na łączność komputerową dla krajów Europy Wschodniej. Powiedzmy od razu, że wizyta u Prof. Amsterdamskiego zaowocowała przyznaniem środków na dołączenie Polski do europejskiej sieci naukowo-akademickiej EARN (marzec 1990) i pierwszym połączeniem komputerowym Polski z węzłem sieci EARN w Kopenhadze (sierpień 1990).

O początkach mówi Prof. Tomasz Hofmokl: W Polsce pierwsze przymiarki do budowy sieci komputerowych w środowisku akademickim miały miejsce w końcu lat siedemdziesiątych w ramach problemu resortowego RI.14 we Wrocławiu oraz w Warszawie – w ramach problemu IV.6. W 1987 r. nastąpiły pierwsze rozmowy z partnerami zagranicznymi, mające na celu połączenie niektórych placówek badawczych w Polsce z Francją i Niemcami. Niestety, na przeszkodzie stały przepisy regulujące transfer zaawansowanej technologii. W 1987 r. został uruchomiony Centralny Program Badawczo Rozwojowy CPBR 8.13 pod nazwą „Budowa Krajowej Akademickiej Sieci Komputerowej KASK". Programem tym kierował Prof. Daniel J. Bem z Politechniki Wrocławskiej. Realizacja tego programu umożliwiła coś bezcennego: wykształcenie kadry, gotowej do działania w późniejszym okresie.

W 1987 r. fizycy wysokich energii z ośrodków w Warszawie i Krakowie zwrócili się do współpracujących laboratoriów w Niemczech i Francji z prośbą o przyłączenie polskich laboratoriów linią stałą do komputerów pracujących w tych ośrodkach. Dyrekcje

Spis treści

ośrodków wyraziły pełne poparcie dla projektu, ale obowiązujące przepisy COCOM-u uniemożliwiały jego realizację.

Politechnika Wrocławska wystąpiła jako pierwsza do EARN (*European Academic and Research Network*), organizacji zarządzającej europejską odnogą sieci Bitnet, z wnioskiem o przyjęcie Polski do tej organizacji i przyłączenie jej do sieci. W połowie 1989 r. EARN był już w posiadaniu wniosków z Polski, m.in. pochodzących z Wydziału Fizyki Uniwersytetu Warszawskiego i z Politechniki Łódzkiej. Zmiany polityczne w Polsce pozwoliły na rozwiązanie problemów formalnych. Przyczyniły się do tego intensywne działania wielu ludzi. Należał do nich współtwórca Bitnet-u, Ira Fuchs z Princetown, który w wywiadzie dla pisma „Science" wyraził pogląd, że należy udzielić pozwolenia na przyłączenie krajów Europy Wschodniej do sieci komputerowych.

Równolegle intensywne starania rozwinęli Dennis Jennings i Frode Greisen – kolejni prezydenci EARN-u. Ich starania zostały uwieńczone powodzeniem. W początku 1990 r. centrum informacyjne Bitnet-u otrzymało od biura ds. technologii amerykańskiego Departamentu Stanu zgodę na podłączenie krajów Europy Wschodniej do sieci. W tym samym czasie COCOM zgodził się na znaczne złagodzenie ograniczeń eksportowych w zakresie technologii sieciowych do tej części Europy.

W Polsce trwały intensywne przygotowania organizacyjne do połączenia kraju ze światem. W grudniu 1989 r. z inicjatywy Jacka Gajewskiego z Wydziału Fizyki Uniwersytetu Warszawskiego, Macieja Kozłowskiego z Centrum Astronomicznego im. Mikołaja Kopernika PAN oraz Andrzeja Zienkiewicza, dyrektora ówczesnego Centrum Obliczeniowego Uniwersytetu Warszawskiego, odbyło się wspomniane już spotkanie u Prof. Amsterdamskiego.

Niezależne wysiłki wielu środowisk zostały uwieńczone powodzeniem. Połączenie fizyczne pierwszego węzła, zlokalizowanego w Centrum Informatycznym Uniwersytetu Warszawskiego, z węzłem EARN w Kopenhadze nastąpiło 17 sierpnia 1990 r. Od tej chwili datuje się gwałtowny rozwój polskiej sieci. W kolejności powstały węzły EARN-u we Wrocławiu (10.11.1990), Krakowie (20.11.1990), Katowicach (28.11.1990), Lublinie (15.01.1991), Poznaniu (10.02.1991), Toruniu (21.03.1991) i w Białymstoku (20.12.1991). □

Cisi i nieznani bohaterowie NASK... czyli wspomnienia starego mamuta

Andrzej Zienkiewicz

Gdzieś w latach siedemdziesiątych spotkałem Jerzego Biłobrana. Wychowawca i nauczyciel kilku pokoleń inżynierów telekomunikacji z Bydgoszczy, wieloletni pracownik resortu łączności, uczył nas profesjonalnej telekomunikacji; z nami uczył się teleinformatyki. To z nim zmontowaliśmy pierwszy w Polsce system wieloprotokołowy, pozwalający pracować z monitorów w ówczesnym Ministerstwie Nauki, Szkolnictwa Wyższego i Techniki na maszynach ODRA (George 3), IBM (SNA) oraz MERA 400 (X3), między innymi poprzez TCK 24, uruchomiony dla tego celu. To nic, że w tamtych latach za „switch" służyła przełącznica sznurowa; fakt, że w określonych godzinach można było pracować w ministerstwie z różnymi systemami z jednolitego zestawu monitorów STANSABA. Jerzy Biłobran, będąc zaufanym człowiekiem zarówno ludzi z łączności jaki i nas, odegrał ogromną rolę w rozwiązywaniu naszych problemów telekomunikacyjnych, kiedyś w resorcie, obecnie w TP S.A. To dzięki niemu NASK jest chyba jedyną firmą nie narzekającą na współpracę z TP S.A. (i chyba odwrotnie).

Któregoś słonecznego poranka w1991 r. zadzwonił do mnie jeden z dyrektorów w Ministerstwie Łączności z prośbą, abyśmy się zajęli jakimś Szwedem polskiego pochodzenia, który chce go namówić na zupełnie dziwne rzeczy. W ten sposób poznałem Henryka Maltborga. Z Henrykiem, który był wtedy dyrektorem szwedzkiej firmy DATA DELECTA, tworzyliśmy pierwsze wspólne polsko-szwedzkie przedsięwzięcie, polegające na wykorzystaniu mieszanego sprzętu szwedzkiego NETLAN i naszych węzłów oraz koncentratorów MERA 60.

Kiedy Henryk montował połączenie Polski z siecią EARN w Danii, przy okazji zainstalował multipleksery i zestawił również połączenie sieci X.25. Było to połączenie nie całkiem oficjalne, polegające na zestawieniu gateway'a za pośrednictwem jego firmy. Gdy jeden z "dowcipnych" młodych ludzi wykorzystał sieć X.25 do prób połączenia z lotniskowcem USA w Zatoce Perskiej, spowodował małą aferę międzynarodową, ponieważ został oczywiście namierzony przez ochronę kontrwywiadowczą. Amerykanie śledzili, skąd Polska ma technologię X.25 nie wierząc, że urządzenia wykonaliśmy sami. Skończyło się wyłącznie na półrocznym nękaniu firmy naszego szwedzkiego przyjaciela. Henryk do dziś jest naszym ambasadorem i kreatorem podstawowych interesów międzynarodowych NASK.

Teraz kilka słów o Adamie Bardachu, tym razem Kanadyjczyku polskiego pochodzenia. Adam Bardach, doradca rządu Kanady, wpadł na pomysł wykorzystania odsetek bankowych od funduszu stabilizacyjnego na zakup sprzętu dla NASK. Po pokonaniu wielu biurokratycznych przeszkód w kraju otrzymaliśmy bardzo nowoczesny, jak na ówczesne czasy, zestaw urządzeń sieci X.25 firmy MEMOTEC. Jest to chyba do dziś jedyny przypadek, kiedy fundusze pomocowe zostały przeznaczone w całości na realne dostawy (doradztwo zostało wykonane gratis). Z tym sprzętem wiąże się anegdota. Jeden z naszych pracowników, testując połączenia z później powstającą siecią POLPAK, proponował jej wyrzucenie ze względu na zbyt przestarzałe rozwiązania – już w trakcie powstawania.

Adam Bardach okazał się później znajomym dziś już nie żyjącego Andrzeja Habrzyka, z którym uruchamialiśmy system sterowania lotami, przy okazji ćwicząc przeniesienie naszych rozwiązań sieciowych, bazowanych na MERA 60, na platformę nowszych technologii PC. W okresie braku środków zamówienia wojskowe bardzo wspomogły nieprzerwany rozwój wiedzy i technologii wykorzystany w następnym okresie w NASK.

Sieć NASK już od początku była wieloprotokołowa. Połączenia międzywęzłowe oparte na multiplekserach statystycznych, znacznie bardziej wydajnych od TDM, pozwalały na obsługę czterech równoległych protokołów EARN (SNA), X.25, DecNet oraz IP. Poszukując urządzenia dla wymiany informacji pomiędzy sieciami trafiłem na kolejnego Kanadyjczyka polskiego pochodzenia, Stanisława Michalaka z firmy GANDALF. Dostarczony przez niego STARMASTER tej firmy długie lata skutecznie pozwalał posiadaczom terminali sieci X.25 na korzystanie z Internetu i odwrotnie. Podobnie do EARN-u można było połączyć się z sieci Internet i X.25. Terminalowe końcówki STARMASTER-a pozwalały na korzystanie z pełnej gamy usług. W późniejszym okresie Stanisław Michalak odegrał podstawową rolę dla NASK opracowując ekspertyzę na temat możliwości zastosowania protokołu ATM w sieci NASK. Ta właśnie ekspertyza, pomimo niejasnej kontr-ekspertyzy i wielu innych wyrażanych obaw, pozwoliła na przeforsowanie budowy sieci WARMAN (wtedy największej i jedynej takiej sieci w Europie) od razu w technologii ATM.

Szukając nietypowych i prototypowych rozwiązań w sieci telekomunikacyjnej trafiłem na dwóch naukowców z Politechniki Warszawskiej, którzy, nie mogąc rozwinąć swoich możliwości w ramach uczelni, założyli własną firmę. Tak spotkałem Janusza Góreckiego i Bogdana Rawicza. Do dziś wszystkie nietypowe interfejsy, zgrywanie zegarów i temu podobne wymyślne jednostkowe urządzenia, wykonują dla NASK nasi dawni przyjaciele, oferując produkty klasy światowej, ale szybciej i znacznie taniej.

Myślę, że warto wspomnieć o licznej grupie naszych dawnych współpracowników, dziś często konkurentów, którzy z nami tworzyli firmę, jaką dziś jest NASK. Myślę o kolegach z wielu uczelni i środowisk, jak Marian Budka z zespołem konstruktorów z Gliwic, Cezary Citko z Białegostoku, Jurand Czermiński z Gdańska, Krzysztof Gaweł z Krakowa, Maria Górecka z Torunia, Józef Janyszek z Wrocławia, Zygmunt Mazurkiewicz z Zielonej Góry, Jerzy Pawlus z Krakowa, Zbigniew Sender z Kielc, Zbigniew Skorzyński z Lublina, Edward Solarski z Gliwic, Stanisław Starzak z Łodzi, Przemysław Stolarski z Poznania, Tomasz Wolniewicz z Torunia i Jerzy Żenkiewicz, też z Torunia.

Jest jeszcze wielu innych naszych przyjaciół, którzy spowodowali, że NASK jest uznaną firmą w kraju i poza jego granicami. Jednak dziś, dla ich i naszego dobra, mogę tylko obiecać, że, jeśli będą pisał wspomnienia na przyszłe dziesięciolecie, na pewno o nich nie zapomnę. □

NASK wygrywa precedensową sprawę przed Sądem Antymonopolowym

W dniu 29 września 1999 r. NASK wygrał bardzo długotrwałą, trudną pod względem formalnym i merytorycznym, a przed wszystkim precedensową sprawę, która przez długi czas była przedmiotem wielu informacji prasowych i dyskusji środowiska. Sąd Antymonopolowy wydał wyrok w sprawie rzekomych praktyk monopolistycznych NASK - wyrok, który całkowicie podważył decyzję Urzędu Ochrony Konkurencji i Konsumentów i na mocy którego umorzone zostało postępowanie administracyjne wobec NASK. Zainteresowani: ATM S.A., Internet Technologies Sp z o.o. oraz SM-Media zostali zobowiązani do zapłacenia NASK kosztów procesu.

W dniu 29 września 1999 r. Sąd Okręgowy w Warszawie - Sąd Antymonopolowy po rozpoznaniu w dniu 15 września 1999 r. sprawy z odwołania Naukowej i Akademickiej Sieci Komputerowej od decyzji Prezesa Urzędu Ochrony Konkurencji i Konsumentów z dnia 24 listopada 1998 r. DDI-II-53S/21/98/EA przeciwko Prezesowi Urzędu Ochrony Konkurencji i Konsumentów z zainteresowanymi: ATM - S.A., Internet Technologies Polska Sp z o.o., SM-Media Sp z o.o., o przeciwdziałanie praktykom monopolistycznym, wydał wyrok, mocą którego zmienił decyzję Urzędu Ochrony Konkurencji i Konsumentów w całości w ten sposób, że umorzył postępowanie administracyjne oraz zasądził na rzecz NASK koszty procesu.

Przypominamy, że Urząd Ochrony Konkurencji i Konsumentów prowadził postępowanie wyjaśniające w związku z wprowadzeniem przez NASK cennika świadczenia usług telekomunikacyjnych w grudniu 1995 r. W czerwcu 1997 r. ATM S.A., Internet Technologies Sp. z o.o. oraz SM-Media złożyły wniosek o wszczęcie postępowania w sprawie stosowania przez NASK niedozwolonych praktyk monopolistycznych przejawiających się między innymi w tym, że wprowadzone przez NASK opłaty za ruch telekomunikacyjny generowany, zamiast dotychczasowych opłat ryczałtowych, miały charakter antykonkurencyjny, eliminujący zainteresowanych z rynku usług operatorskich świadczonych na rzecz abonentów końcowych.

W listopadzie 1997 r. Urząd Ochrony Konkurencji i Konsumentów wszczął postępowanie antymonopolowe zarzucając NASK narzucanie zainteresowanym uciążliwych warunków umów poprzez odmowę wskazania szczegółowego sposobu naliczania opłat za ruch w sieci oraz pobierania opłat za ruch, który nie doszedł do sieci abonenta.

W grudniu 1998 r. Urząd Ochrony Konkurencji i Konsumentów oddalił część zarzutów stawianych NASK przypisując mu jednak wykorzystywanie pozycji dominującej, które przejawiało się w niewłaściwej taryfikacji. Od tej decyzji NASK się odwołał, w efekcie czego sprawę rozstrzygnął Sąd Antymonopolowy wydając wyrok, który w całości oczyścił NASK z zarzutu stosowania praktyk monopolistycznych. □

Rozmowa na koniec roku

z dyrektorem technicznym NASK, Wiktorem Krzanowskim, rozmawia Aneta Mazurkiewicz

– ***Jak postrzega Pan sytuację na polskim rynku usług teleinformatycznych, jakie stwarza ona możliwości rozwoju dla świadczących tego rodzaju usługi firm oraz jakie miejsce, jaką rolę przewiduje Pan w takiej sytuacji dla NASK?***

– Ocena sytuacji Polski na rynku teleinformatycznym jest związana z zasobnością społeczeństwa i wzrostem rozwoju gospodarczego. Zachodzące zmiany są generalnie pozytywne, ale z drugiej strony – daleko nam jeszcze do poziomu rozwoju innych krajów europejskich. Nadrabiamy zapóźnienia cywilizacyjne wiążące się z brakiem infrastruktury telekomunikacyjnej, z małą liczbą komputerów osobistych w domach czy z mniejszą niż na Zachodzie popularnością kart płatniczych. W takiej sytuacji trudno oczekiwać, aby na polskim rynku np. handel elektroniczny funkcjonował tak samo, jak na rynku amerykańskim. Póki co w Polsce zarówno handel, bankowość, jak i możliwość prowadzenia operacji giełdowych przy użyciu Internetu, są usługami dostępnymi dla stosunkowo niewielkiej grupy społeczeństwa. Jest to zupełnie inna sytuacja niż np. w Stanach Zjednoczonych, gdzie za pośrednictwem Internetu gra na giełdzie 30 do 40 proc. Amerykanów.

Z drugiej strony sytuacja gwałtownie się zmienia. Dla dużych zagranicznych firm polski rynek jest już na tyle atrakcyjny, że warto tu inwestować. Sądzę, że zachodnie inwestycje w polski rynek teleinformatyczny stanowią w chwili obecnej przygotowanie do ostrej walki konkurencyjnej, która nastąpi lada moment – za dwa, trzy lata, gdy ten rynek rzeczywiście zacznie intensywnie funkcjonować. Potencjalnie jest to rynek duży, na pewno atrakcyjny, i – jak widać – wiele firm podziela ten pogląd. Dla rynku oznacza to również, że na użytkownika będzie czekała coraz ciekawsza oferta. Wszystkie inwestujące firmy muszą zachęcić i ściągnąć klientów, przygotować ich do korzystania ze proponowanych aplikacji i narzędzi.

– ***Jak w tym kontekście rysuje się sytuacja NASK?***

– Dla NASK obecna sytuacja oznacza pojawienie się konkurentów z dużymi pieniędzmi, którzy mają długofalowe plany i którzy – w moim przekonaniu – w tych planach zakładają zyski po stosunkowo długim okresie czasu. My jesteśmy firmą, która nie ma takich możliwości. NASK musi zarobić na bieżącą działalność i na inwestycje, wśród których te większe, o znaczeniu strategicznym, nie mogą się obejść bez kredytów. Jest to sytuacja znacznie trudniejsza, bowiem ponosimy ryzyko związane ze spłatą zadłużenia. Inwestycje, które teraz planujemy, będą w pewnej części finansowane właśnie z kredytów.

Duże firmy mają niewątpliwie większe zasoby i bardziej komfortową sytuację z punktu widzenia finansowania. NASK, m.in. dzięki swemu kapitałowi wieloletnich doświadczeń i profesjonalizmu, nadal jest liderem na rynku – i to nie tylko polskim, ale także usług międzynarodowych. To, co obecnie oferujemy, ma istotny związek z naszymi partnerami i realnym zapotrzebowaniem przychodzącym ze światowych rynków, gdzie firmy, korzystające z różnych narzędzi i produktów teleinformatycznych, przenoszą je do Polski i wdrażają – czy to w swoich filiach, czy w firmach partnerskich. NASK nigdy nie będzie firmą oferującą masowy produkt. To zadanie dla dużych operatorów, takich jak TP SA. Mają oni ku temu znacznie lepszą pozycję wyjściową, bo, po pierwsze, zarabiają choćby na impulsach, po drugie, dysponują systemami masowej obsługi klienta. My zaś kierujemy uwagę na rynek bardziej elitarny – rynek sieci korporacyjnych, gdzie spodziewamy się rosnącego popytu.

Rynek, na którym działamy, wymaga i będzie wymagał coraz lepszej jakości. Powoli, także w Polsce, rozwija się *outsourcing* – usługa nie ograniczająca się tylko do styku abonenta z portem w węźle operatora, lecz obejmująca infrastrukturę klienta, czyli linię dostępową, router brzegowy po jego stronie, nadzorowanie systemu. Aby zlecić tego typu obsługę firmie zewnętrznej, trzeba przejść przez długi proces związany ze określeniem potrzeb, policzeniem wszystkich kosztów etc. Przypomnę, że CISCO, jeden z największych dostawców technologii sieciowych, będący liderem w dziedzinie obsługi klientów przez sieć, ma system sieciowy obsługiwany przez zewnętrzną firmę. CISCO specjalizuje się w produkcji urządzeń sieciowych, ale niekoniecznie chce być operatorem własnej dużej sieci. Firma ta chce po prostu mieć sprawnie działającą sieć, obsługiwaną przez specjalistów, wobec czego dawno już uznała, że utrzymanie własnych służb jest drogie i często nieefektywne. To segment rynku, na który chcemy wejść, segment wymagający naprawdę fachowej wiedzy. To nie jest usługa, którą można zdjąć z półki. Wymaga ona zaawansowanych działań – przede wszystkim nadzorowania pracy sieci.

Wszystko to wiąże się z przebudową sieci NASK. Ta sieć musi być jednolita; musimy mieć odpowiednie narzędzia zarządzania – już nie tylko samą siecią, ale usługami dla jej klientów.

– ***Czy może Pan powiedzieć coś więcej o nowej sieci. Dla jakich usług i dla jakiego klienta jest ona budowana?***

– Zwróćmy uwagę na kilka czynników. Po pierwsze, klienci wymagają obecnie coraz wyższego poziomu usług. Rozwija się biznes, który musi być obsługiwany profesjonalnie. Po drugie, rośnie liczba klientów. Można oczekiwać, że ten przyrost może być bardzo gwałtowny. W tej chwili zapotrzebowanie w dużej mierze przychodzi z zagranicy poprzez firmy, które mają tutaj swoje przedstawicielstwa. Trzeci element to konkurencja na rynku. Dotychczas Internet był postrzegany jako bardzo obiecujące medium komunikacyjne, jednak nie do końca nadające się do konkretnych zastosowań – zwłaszcza na polu biznesu. To się teraz gwałtownie zmienia, bo w ofercie producentów pojawia się nowa generacja technologii sieciowych adresowanych przede wszystkim do środowisk biznesowych. Są to wszystkie usługi spod znaku QoS (*Quality of Service*).

Przebudowa naszej sieci wiąże się z naszymi partnerami, z TBN (*Telia Business Network*) i Infonetem. Są to operatorzy globalni, bardzo cenieni na rynku, oferujący wysoką jakość usług. Musimy dopasować się technologią do ich poziomu i standardu. Wiele usług oferujemy wspólnie i nie może być tak, ze będziemy najsłabszym ogniwem całego łańcuszka. Jeśli klient ma do czynienia z usługą oferowaną przez Infonet czy TBN w Polsce, to musi ona mieć ten sam poziom, co usługa tych operatorów realizowana gdziekolwiek indziej na świecie.

Nasza nowa sieć powinna uzyskać zdolność operacyjną w połowie przyszłego roku. Powinna już za pół roku oferować nowe usługi i nową jakość na rynku. Musi być zdolna do obsługi znacznie większej liczby klientów niż to ma miejsce obecnie. Będziemy oferować usługi QoS na różnych poziomach dbając o dopasowanie ich do specyficznych potrzeb naszych klientów. Warto w tym miejscu dodać, że niezależnie od świadczenia usług we własnej sieci dołączamy klientów także przez Polpak-T, mamy operatorskie połączenia międzysieciowe (NNI) z innymi operatorami. Mam nadzieję, że ta współpraca międzyoperatorska będzie coraz intensywniejsza.

Naszymi klientami są coraz częściej duże firmy, dla których sieci stanowią podstawowe narzędzie działalności gospodarczej. Firmy te mają silne powiązania międzynarodowe, w związku z czym ich systemy, jako elementy międzynarodowej całości, nie mogą być tylko sieciami wewnętrznymi, lokalnymi. Muszą być trans-graniczne, globalne. Sądzę, że naszą zaletą jest to, że możemy elastycznie reagować na zapotrzebowanie klienta, nawet zupełnie nietypowe. Jesteśmy w stanie podjąć się bardzo różnych zadań, a w szczególności takich, które wymagają oryginalnego podejścia, oczywiście – w zakresie szeroko rozumianej transmisji danych.

– ***Ostatnio bardzo głośno jest w prasie o NASK-u w kwestii domen. Jak Pan skomentuje ostatnio pojawiające się artykuły i częste ataki?***

– Na to pytanie chciałbym odpowiedzieć cofając się do roku 1995. Wszyscy pamiętamy artykuły i temperaturę dyskusji, kiedy wprowadzany był nowy cennik. Historia rozpatrywana na spokojnie udowadnia, że mieliśmy racje. Stawiane nam zarzuty nie sprawdziły się. Powszechny był zarzut, ze jeżeli będziemy taryfikowali ruch przychodzący i wychodzący to ktoś będzie nam przysyłał pocztę, żebyśmy zbankrutowali. Owszem, taka możliwość teoretycznie istniała, ale takie zjawisko stanowi ten sam poziom zagrożenia jak to, że ktoś będzie nam przypadkowo lub celowo przysyłał faksy. Istota sprawy była jednak gdzie indziej. NASK był w owym czasie jedynym liczącym się operatorem Internetu w Polsce i tym samym przypadła mu niewdzięczna rola pioniera, także w zakresie taryfikacji. W tej dziedzinie w Polsce nie było wówczas żadnych sensownych doświadczeń. Z perspektywy lat widać, że nasza działalność przyczyniła się do zrozumienia, jakie są prawdziwe koszty Internetu, a pośrednio zmusiliśmy do działania konkurencję, przyczyniając się do rozbudowy i zintensyfikowania rynku usług internetowych.

Sprawa domen przedstawia się podobnie. Swego czasu zaczęliśmy ich rejestrację, bo ktoś to musiał robić. Potem stały się one istotnym narzędziem korzystania z sieci, a następnie ważnym elementem identyfikacji firm, ich działań rynkowych. Kwestia nazw i praw własności jest ważnym składnikiem marketingu, wymaga profesjonalnego, odpowiedzialnego podejścia, a to kosztuje, więc w pewnym momencie przestaliśmy to robić hobbystycznie, jak kiedyś. Ilość pracy związanej z domenami jest olbrzymia. Jej znaczna część wiąże się z windykacją zadłużeń, którą musimy robić pomimo tego, że kwoty są niewielkie, gdyż jeśli ktoś nie płaci, to jest szansa, że nie używa domeny i w takiej sytuacji ktoś inny może z niej zacząć korzystać. Nawet w tak uregulowanej prawnie dziedzinie jak znaki handlowe zdarzają się sytuacje, że jedne firmy wykupują znaki innych. W Internecie pod tym względem panuje wiele dowolności, nie ma żadnych jednolitych reguł. Są jedynie pewne zalecenia międzynarodowe. Staramy się je uwzględniać – co najmniej w 90 procentach. Dlatego, kiedy porównujemy nasze zasady przyznawania domen z tym, co się dzieje na świecie, okazuje się, że nasze reguły są bardzo zbliżone do światowych standardów.

– ***Na koniec pytanie związane z historią firmy. NASK został utworzony w zasadzie jako odpowiedź na potrzeby środowiska akademickiego. Jak ta "akademickość" wygląda dzisiaj i na ile pomaga w obecnej sytuacji firmy, a na ile przeszkadza?***

– NASK został powołany do tego, żeby dołączyć środowisko akademickie do międzynarodowej sieci Internet i z tego zadania się wywiązał. Nawet nasi najwięksi konkurenci i krytycy pomimo wielu zastrzeżeń i ataków nie zaprzeczają, że została tu wykonana wielka praca. Mamy przy tym równocześnie świadomość, że tamta rola się już skończyła, tym bardziej, że sam Internet przestał już być "własnością" środowiska akademickiego. To środowisko było kiedyś motorem rozwoju Internetu. Dziś, gdy Internet ma już inną jakość, środowisko to praktycznie nie uczestniczy w rozwoju Internetu, bo niezależnie od potrzeb, często nie ma na to pieniędzy. Z kolei NASK musi się samodzielnie utrzymać, nikt nas nie finansuje, działamy na rynku i musimy dostosować się do jego wymogów. Teraz często okazuje się, że ten akademicki rodowód nam przeszkadza. Klienci, którzy są przyzwyczajeni do obsługiwania przez prywatne firmy, zastanawiają się, co może im zaoferować akademicka sieć. Tak więc nie ukrywam, że obecnie dążymy do tego, by nie kojarzono nas wyłącznie z akademickością. Tak naprawdę w chwili obecnej „Naukowa i Akademicka..." w naszej nazwie ma wyłącznie charakter historyczny, co nie oznacza, że od środowiska naukowego chcielibyśmy się w jakiś sposób odciąć.

– ***Dziękuje za rozmowę.***

Międzynarodowe usługi INFONET

Piotr Łukawski

Od 1 listopada 1999 r. NASK wprowadza na rynek nową klasę usług międzynarodowych Infonet. Dzięki ich szerokiemu portfelowi NASK jest w stanie zapewnić – jako jedyna firma w Polsce – ogólnoświatową łączność przy zachowaniu wszelkich gwarancji wynikających ze spójności sieci.

Dewizą usług Infonet jest „seamless communication" – komunikacja pomiędzy sieciami bez względu na różnice wynikające z odmiennych technologii, sposobów zarządzania, systemów bilingu oraz „kultur wewnętrznych" kolejnych operatorów, przez których przechodzi połączenie. Zgodna z normami ISO 9000 sieć usług Infonet zapewnia wymagającemu klientowi międzynarodowemu użytkowanie systemu o zasięgu globalnym, w którym może on wymagać wyspecjalizowanych usług, takich jak np. ustalenie priorytetu przepływu danych w zależności od używanych aplikacji. Jest to istotne w obecnej sytuacji, kiedy coraz częściej prawdziwym systemem nerwowym przedsiębiorstwa staje się system komputerowy, łączący jego oddziały na całym świecie i wykorzystujący oprogramowanie działające w czasie rzeczywistym.

Pakiet usług Infonet zawiera w sobie wszystkie elementy potrzebne takiemu przedsiębiorstwu, zapewniając mu spokojny rozwój bez troski o rozwiązania sieciowe na świecie i problemy związane z utrudnieniami w globalnym przepływie informacji. Produkty takie jak Global Frame Relay, Global IP, Dial Express Remote Access Services, Global Connect wzajemnie się uzupełniają i umożliwiają stworzenie sieci dostosowanej do potrzeb i wymagań danej firmy. Towarzyszące temu usługi związane z dołączeniem sieci LAN bezpośrednio u klienta czy stworzeniem systemu bezpieczeństwa uzupełniają ten pakiet i zapewniają kompleksowe rozwiązania o światowym zasięgu.

Dla potrzeb tworzenia firmowych Intranetów o zasięgu globalnym Infonet oferuje klasę usług określanych wspólną nazwą Global IP. Sieć Global IP istnieje od 1991 r. i obecnie obejmuje swoim zasięgiem 43 kraje. Oferuje ona zarówno szerokie pasmo przesyłania danych, jak i krótkie czasy odpowiedzi, wykorzystując największą na świecie sieć opartą na switch'ach Nortel Magellan Passport. W ramach Global IP wyróżniamy usługi IP Plus oraz IP. Ta pierwsza jest przeznaczona dla aplikacji intranetowych o żywotnym znaczeniu, którym zapewnić trzeba minimalne opóźnienia, a które w typowej sieci IP są zagrożone przez „pasmożerne" aplikacje, takie jak np. FTP. Typową aplikacją wymagającą IP Plus jest np. przetwarzanie zleceń, dostęp do baz danych o użytkownikach używany przez biura obsługi użytkownika czy też inne aplikacje, dla których opóźnienia są krytyczne, np. *Voice over IP*.

Dla odmiany usługa IP jest dedykowana dla aplikacji, które wymagają szerokiego pasma, jednakże nie mają specjalnych wymagań, jeśli chodzi o opóźnienia. Typowymi aplikacjami o takich wymaganiach są systemy poczty elektronicznej, takie jak Lotus Notes™, Microsoft Exchange™, aplikacje biurowe czy operacje synchronizacji baz danych.

Zastosowanie powyższych klas usług oraz oferowanych w ich ramach usług związanych z bezpieczeństwem i monitoringiem sieci umożliwia stworzenie efektywnego rozwiązania Intranetu, opartego na IP.

W celu zapewnienia szybkiej i pewnej komunikacji pomiędzy oddziałami międzynarodowych przedsiębiorstw Infonet opracował także rozwiązanie Global Frame Relay. GFR dostosowuje i optymizuje połączenia w zależności od potrzeb używanych aplikacji poprzez „priorytaryzację" danych aplikacji i użytkowników. GFR jest w stanie przekazać także typowe protokoły LAN Digitala, Apple czy Novella. Za pomocą GFR można obsługiwać ruch zarówno bardzo wymagających aplikacji, takich jak SAP, Baan, PeopleSoft, Oracle, poprzez bardziej odporne na opóźnienia programy pocztowe, aż do aplikacji typu FTP. W typowym rozwiązaniu oferowanym na rynku dane z różnych aplikacji przesyłane są – poprzez stosowanie kolejnych NNI – z tym samym priorytetem. Natomiast Infonet rozwinął technologię zwaną „Customized Networking Options" – opcji dających efekty analogiczne do ATM. Tak zbudowana sieć umożliwia zapewnienie prawidłowego działania aplikacji nawet w momentach przeciążenia sieci. Użytkownik może kupić rozwiązanie, w którym ruch w sieci, tworzony przez aplikacje niskopriorytetowe, nie wpływa na działanie aplikacji czasu rzeczywistego. W ramach CNO zdefiniowano trzy klasy usług:

VC/Interactive *– zapewniające jakość porównywalną z linią dzierżawioną, potrzebną aplikacjom zarządzania zasobami, takimi jak SAP, Baan czy Oracle;*

VC/Lan2lan *– dedykowaną wieloprotokołowym aplikacjom wymagającym krótkiego czasu odpowiedzi, jak synchronizacja baz danych, drukowanie, przeszukiwanie Intranetu;*

VC/Access *dla aplikacji odpornych na opóźnienia, takich jak e-mail czy przeszukiwanie Internetu.*

GFR umożliwia dostosowanie struktury połączeń dokładnie do potrzeb przedsiębiorstwa przy zastosowaniu najlepszego stosunku jakości do ceny.

Ostatnimi w portfelu usług są wreszcie RAS – usługi zdalnego dostępu. Są nimi DialXpress Office i DialXpress Professional. Pierwszy, dedykowany dla małych oddziałów, umożliwia ich dołączenie do sieci IP bez dodatkowych kosztów związanych z linią dzierżawioną przy stałym adresie IP. Drugi, polecany dla klientów ruchomych, daje możliwość światowego dostępu do usług Infonet, gdziekolwiek na świecie znajdzie się ich użytkownik.

Wraz z otoczeniem wszelkich usług, jak *Managed Firewall*, Global-Web „hosting Infonet" stanowi pełną ofertę usług potrzebnych współczesnemu przedsiębiorstwu. □

Sieć optymistów

Maria Baranowska

Każdego roku jesienią piszemy w „Biuletynie NASK" o zmianach i ciekawych zjawiskach zachodzących w zbiorowości użytkowników polskiego Internetu. Przypomnijmy, że swego czasu NASK zainicjował te badania w Polsce realizując dwukrotnie ogólnopolskie sondaże – w latach 1995–1996. W ubiegłym roku pisaliśmy o wynikach ankiety polskiego WWW, które ujawniły intensywne zmiany dokonujące się w środowisku polskich internautów:

- rosnącą grupę ludzi młodych – uczniów i studentów;
- coraz liczniejszą kategorię osób łączących się z siecią z domowych komputerów – często z wykorzystaniem darmowego dostępu;
- coraz częstsze korzystanie sieci w celach komercyjnych.

Bardzo ciekawe wyniki przyniosły tegoroczne badania Katedry Marketingu Akademii Ekonomicznej z Krakowa – w sondażu przeprowadzonym w okresie od maja do lipca wzięło udział ponad 7 tys. osób.

Kilka słów o metodologii. Pewnym ograniczeniem ogólnodostępnej ankiety jest nie w pełni losowy dobór respondentów. W związku z tym odpowiedzi udzielonych na ankietę rozpropagowaną przez WWW nie możemy uznać za w pełni reprezentatywne, bo z reguły w badaniu takim biorą udział ludzie o określonej charakterystyce – bardziej aktywni, lepiej przygotowani do wykorzystania narzędzi internetowych, często ludzie „z branży".

Wielką zaletą badania krakowskiej Katedry Marketingu jest jego zasięg tematyczny. Autorzy ankiety wyszli daleko poza standardowe pytania, dzięki czemu otrzymaliśmy zróżnicowany opis grupy najbardziej dynamicznych użytkowników Internetu, których tygodnik „Wprost" określa nawet jako „nową elitę" (nr 37/99).

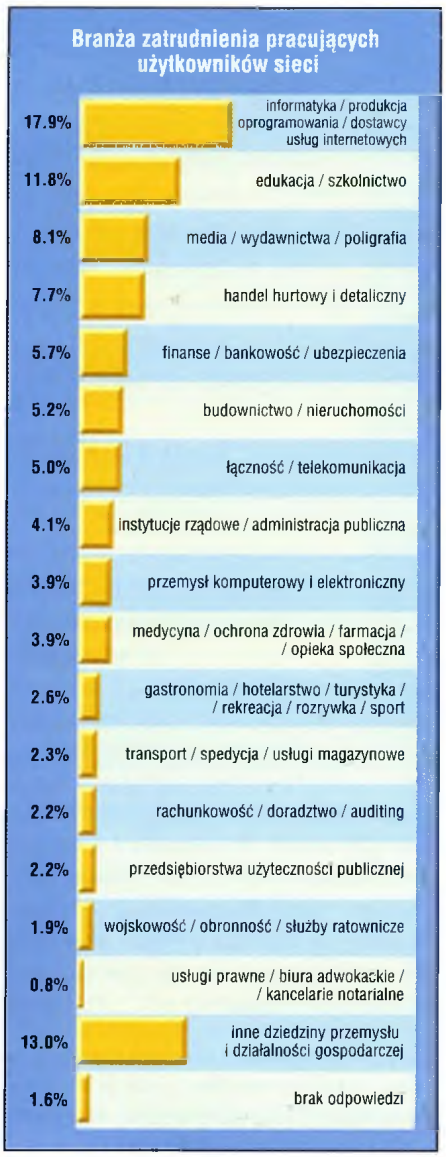
Dotychczas badania społeczności Internetu w Polsce ograniczały się do opisania głównych cech społeczno-demograficznych tej zbiorowości, takich jak płeć, wiek, wykształcenie. Badanie Katedry Marketingu AE potwierdza tu ubiegłoroczne tendencje, a więc:

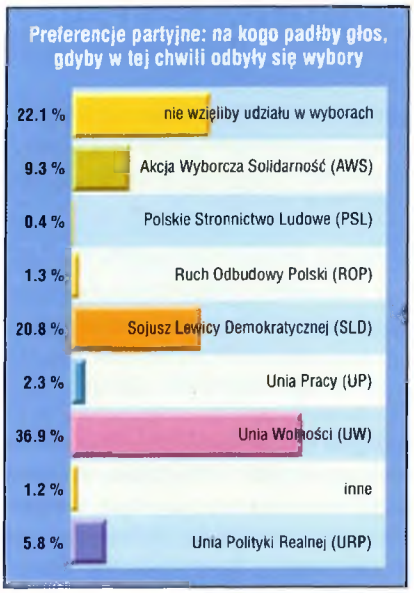
- polscy internauci pochodzą głównie z dużych miast (63 proc. mieszka w miastach powyżej 100 tys. mieszkańców, a tylko 6,7 proc. na wsi);
- coraz większą grupę stanowią ludzie młodzi (aż 57 proc. ma mniej niż 25 lat) i wykształceni (tylko 8,7 proc. użytkowników z podstawowym wykształceniem, ukończone studia wyższe lub przynajmniej licencjat ma blisko 40 proc. uczestników ankiety);
- jedyny wskaźnik, który nie zmienia się od dawna, to niski udział kobiet w zbiorowości polskich użytkowników Internetu – ciągle na poziomie 18-19 proc.

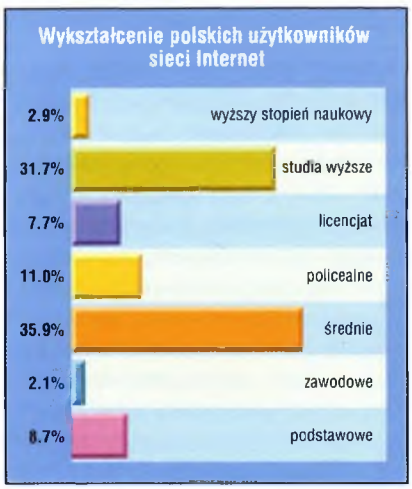
Internauci są mocno związani z technologiami informatycznymi (najwięcej – 18 proc. pracuje w informatyce, 12 proc. w edukacji, 8 – w mediach, natomiast handel, finanse i bankowość reprezentuje 13 proc. badanych).

Mniej więcej od 2 lat zwiększa się liczba osób korzystających z Internetu nie tylko w pracy, ale i w domu. Już ponad 45 proc.

> Wyniki ankiety Katedry Marketingu krakowskiej Akademii Ekonomicznej ukazują nam grupę wykształconych, aktywnych, dobrze zarabiających, przekonanych o własnej wartości, zadowolonych z życia młodych ludzi. Osobników takich często określa się jako *young urban (single) professionals* czyli młodych, wykształconych specjalistów wolnego stanu zamieszkujących miejskie aglomeracje. Niezależnie od tysięcy krążących po świecie anegdot na temat zachowania i stylu życia *yuppies* – Polska doczekała się własnej warstwy młodych wysoko kwalifikowanych profesjonalistów, którzy, jak wszędzie na świecie, i u nas stanowią awangardę przemian ekonomiczno-kulturowych. Ich znakiem szczególnym jest aktywne korzystanie z Internetu.



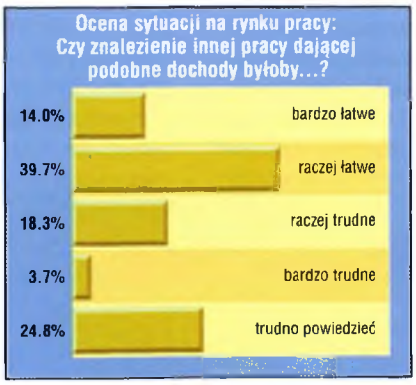


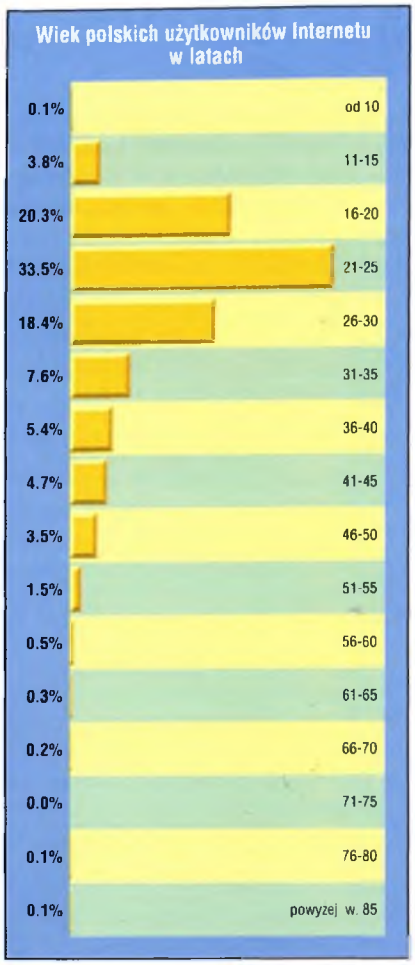


uczestników ankiety łączy się z siecią z domu. Ich korzystanie z Internetu jest dość intensywne – tylko 2 proc. uczestników ankiety robi to rzadziej niż raz w tygodniu. Ten ostatni wskaźnik wiąże się bezpośrednio z tym, o czym była mowa na początku – dobrowolna ankieta dostępna przez WWW przyciąga i skłania do udzielenia odpowiedzi przede wszystkim ludzi aktywnych.

Z tegorocznej ankiety wynika, że spośród narzędzi Internetu największą popularnością cieszą się WWW i poczta elektroniczna. Internet służy przede wszystkim do wyszukiwania informacji (80 proc. odpowiedzi) i komunikacji (75 proc.) Coraz więcej osób decyduje się na próbę nabycia czegoś w internetowym sklepie (dotychczas zrobiło to przynajmniej raz 23 proc. badanych – w ubiegłym roku było tylko 7 proc. takich odpowiedzi). Najciekawsze są dane przybliżające nam sytuację ekonomiczną, rodzinną oraz pewne preferencje (np. polityczne) użytkowników polskiego Internetu. Tego jeszcze w badaniach tego typu w Polsce nie było. Nasi internauci są młodzi, często jeszcze nie założyli rodziny (58,8 proc. to ludzie stanu wolnego, a 72,5 proc. nie ma jeszcze dzieci), są religijni, ale bez przesady – udział w praktykach religijnych przynajmniej raz w tygodniu deklaruje 31,6 proc. Zarabiają lepiej niż średnia krajowa (ponad 37 proc. ma zarobki od 2 tys. miesięcznie w górę). Ponad połowa nie obawia się bezrobocia ani poszukiwania innej pracy dającej podobne dochody. Zdecydowana większość używa telefonów komórkowych, korzysta z mediów, czyta gazety, przegląda tygodniki informacyjne, rzadziej ogląda telewizję (to także cecha ludzi intensywnie pochłoniętych pracą zawodową).

Uczestnicy ankiety są zwolennikami kapitalizmu i wolnego rynku (aż 89 proc. uważa, że przedsiębiorstwa powinny mieć pełną swobodę w działalności ekonomicznej).





W ocenie stanu polskiej gospodarki przeważa opinia, że mamy do czynienia z rozwojem (dynamiczny rozwój – 2 proc., powolny rozwój – 39,7 proc.) Są optymistami – 57 proc. stwierdza, że wszystko w Polsce posuwa się w dobrym kierunku, podczas gdy odmiennego zdania jest 19 proc.

Szerzej o korzystaniu z Internetu i opiniach na temat wykorzystania tego medium do celów komercyjnych i reklamowych napiszemy w następnym numerze biuletynu. □

Bezpieczna struktura informatyczna przedsiębiorstwa – systemy OTP (*one-time-password*) i SSO (*single-sign-on*)

Mirosław Maj, Krzysztof Silicki

Postępujący wzrost wymagań wobec bezpieczeństwa transakcji elektronicznych (*e-commerce*), dokonywanych w sieciach otwartych, jak również w ramach firmowych sieci lokalnych czy korporacyjnych (np. dostęp do sieciowych aplikacji bazodanowych), stymuluje rozwój technologii takich jak PKI (*Public Key Infrastructure* – infrastruktura klucza publicznego). Przy pomocy aplikacji wykorzystujących kryptografię zapewniają one w prosty i bezpieczny sposób bezpieczeństwo transakcji, rozumiane jako zapewnienie usług uwierzytelniania, poufności, niezaprzeczalności i podpisu cyfrowego.

Podstawowe warunki bezpieczeństwa

Korzyści i możliwości wynikające ze stosowania techniki kluczy publicznych, będącej podstawą PKI, są tak duże z punktu widzenia ochrony danych, że należy sobie zadać pytanie, jakie warunki muszą zaistnieć, aby stosowanie aplikacji wykorzystujących infrastrukturę klucza publicznego było pozbawione zagrożeń dla bezpieczeństwa.

Jednym z podstawowych warunków bezpieczeństwa użytkowania PKI jest zapewnienie ochrony dostępu do kluczy prywatnych użytkowników biorących udział w transakcjach elektronicznych. W tym znaczeniu dużej wagi nabiera na przykład zastosowanie różnych form kart inteligentnych (*smartcard*), sprzęgniętych z aplikacjami sterującymi dostępem do komputerów, sieci lokalnych, systemów bazodanowych w przedsiębiorstwie, które mogą zostać zastosowane dla realizacji bezpiecznego SSO (*single-sign-on*) w ramach danej sieci. Maksymalne bezpieczeństwo struktury informatycznej w przedsiębiorstwie uzyskuje się natomiast poprzez zaimplementowanie – wspólnie z technologiami wymienionymi powyżej – idei bezpiecznych, jednorazowych haseł dostępu do zasobów w oparciu o systemy typu OTP (*one-time-password*).

Inteligentne karty

W systemach klucza publicznego każdy użytkownik posiada parę kluczy kryptograficznych zwanych kluczem publicznym i kluczem prywatnym. Dodatkowo użytkownik legitymuje się cyfrowym certyfikatem potwierdzającym związek osoby z kluczami. Są to ciągi bitów, które powinny być przechowywane w określony sposób, aby zapewnić ich dostępność w czasie przeprowadzania bezpiecznej transakcji (np. szyfrowanego dostępu do firmowej aplikacji SAP). Klucze i certyfikaty mogą być przechowywane w różny sposób: na dysku komputera lokalnego, na dyskietce, na dysku serwera bądź na karcie inteligentnej. Dla użytkownika klucza prywatnego kluczową sprawą bezpieczeństwa jest właściwa ochrona dostępu do klucza. Chodzi o pewność, że nikt inny oprócz właściciela klucza nie jest w stanie się nim posłużyć – klucze są chronione przez hasło lub PIN. W przypadku kluczy składowanych na dyskach lokalnych czy dyskietkach – ich ochrona, realizowana poprzez statyczne hasło, z reguły jest nieskuteczna. Ta forma przechowywania kluczy jest też dość niewygodna.

Coraz częściej więc stosuje się do tego celu karty inteligentne, w których chipie zapisuje się klucze i certyfikaty (dostęp do nich jest chroniony poprzez PIN przesyłany z klawiatury do czytnika) lub karty inteligentne kryptograficzne, w których klucz prywatny w ogóle nie opuszcza karty, zapewniając tym samym maksymalne bezpieczeństwo. Karty inteligentne są bardzo wygodne w użyciu pod warunkiem, że komputer „desktop" jest wyposażony w odpowiedni czytnik.

Odmianą fizycznej karty inteligentnej jest tzw. wirtualna karta inteligentna, która jest niczym innym jak zestawem kluczy i certyfikatów użytkownika przechowywanych na serwerze sieciowym. W takim przypadku dostęp do klucza prywatnego nie może być chroniony za pomocą statycznego hasła, które można podsłuchać w sieci, stosuje się zatem systemy dynamicznych, jednorazowych haseł – czyli właśnie systemy OTP. Użytkownik jest wyposażony w token sprzętowy, który nie wymaga czytnika, a więc można zeń korzystać w każdych warunkach. Token ten generuje jednorazowe hasło, które umożliwia dostęp do klucza prywatnego i dalsze jego stosowanie – podobnie jak w każdym innym przypadku.

Więcej o systemach OTP

W każdym systemie wielodostępnym istnieje problem zapewnienia skutecznej identyfikacji i weryfikacji użytkownika na etapie zezwalania dostępu do określonych zasobów (np. logowanie do sieci, logowanie do systemu operacyjnego komputera, dostęp do aplikacji, dostęp do plików i katalogów np. WWW). Sieci lokalne, korporacyjne, intranety, extranety, VPN-y itp. obfitują w systemy o różnym przeznaczeniu, gdzie niezwykle istotne jest rozgraniczenie praw dostępu (np. blokowanie dostępu z zewnątrz do serwerów intranetowych, ograniczenie dostępu do niektórych aplikacji).

Tradycyjne systemy haseł nie są już obecnie traktowane jako wystarczające ze względu na powszechnie występujące przypadki podsłuchiwania, podpatrywania, wykradania czy łamania haseł. Coraz częściej wykorzystywane są metody typu OTP, w których w sposób programowy lub sprzętowy (użytkownik zostaje wyposażony w kartę/token generujący hasła ważne tylko jeden raz) realizowana jest zasada jednorazowego hasła dostępu: hasło raz użyte jest „zużyte". To, co pod względem bezpieczeństwa jest do zaakceptowania, ze względów użytkowych może posiadać pewne wady. W tym wypadku użytkownik, który miałby mieć precyzyjnie określone i egzekwowane prawa dostępu do wielu systemów i aplikacji w sieci, musiałby za każdym razem podawać hasło. Jeśli system haseł dostępu jest tradycyjny, użytkownika zmusza się do pamiętania kilku, kilkunastu czy kilkudziesięciu różnych haseł, co jest trudne i zazwyczaj powoduje zagrożenia bezpieczeństwa (jedno hasło do wszystkich zasobów, hasła zbyt proste, hasła zapisywane w widocznych miejscach). Jeśli system haseł dostępu jest dynamiczny (OTP), użytkownik haseł pamiętać nie musi, jednak częste wprowadzanie haseł w czasie pracy również może być uciążliwe.

Systemy SSO

Idea SSO (*single-sign-on*) polega na tym, aby w sposób bezpieczny zidentyfikować i zweryfikować użytkownika w pojedynczym procesie komunikacji z systemem w czasie pierwszego logowania do systemu w danej sesji, a następnie automatycznie zezwolić na jego dostęp do zasobów zdefiniowanych w centralnej bazie. W ten sposób użytkownik (w zakresie posiadanych praw dostępu, zdefiniowanych przez np. administratora bezpieczeństwa) po pozytywnym uwierzytelnieniu w czasie logowania do sieci uzyskuje w danej sesji dostęp do określonych komputerów, aplikacji, baz danych itp. W takim scenariuszu istotne jest dobranie mechanizmów bezpieczeństwa, które zapewnią, że uwierzytelnianie i autoryzacja – mimo, że dokonywane „w imieniu" użytkownika, będą odporne na rozmaite zagrożenia (np. podszywanie się, przechwytywanie sesji). Jest to możliwe tylko i wyłącznie przy zastosowaniu nowoczesnych i mocnych mechanizmów kryptograficznych oraz struktury PKI.

Niezawodność i bezpieczeństwo

W systemach SSO kluczową sprawą jest zapewnienie mocnego uwierzytelnienia na etapie dostępu do uprawnień. Hasło, które jest kluczem do wielu systemów i/lub aplikacji, nie może być statyczne, a sesja użytkownika z serwerem powinna być szyfrowana algorytmem o odpowiedniej mocy kryptograficznej. Centralny serwer uwierzytelniający jest w systemach SSO czułym miejscem. Może on stanowić obiekt ataków, a także nie byłoby dobrze, gdyby stał się pojedynczym punktem awarii (*single point of failure*). Serwery SSO muszą zapewniać redundancję.

Przykładowy system bezpiecznego dostępu do zasobów w ramach przedsiębiorstwa

Załóżywszy, że użytkownik jest wyposażony w kartę inteligentną rzeczywistą lub wirtualną, na której posiada swoje klucze i certyfikaty, możemy zaproponować bezpieczne rozwiązanie jego komunikacji z zasobami, do których dostęp musi być chroniony. Rozwiązanie omawiamy na przykładzie systemu Keon firmy Security Dynamics. Keon składa się z kilku elementów:

● Oprogramowanie na stację roboczą (Keon Desktop)

Oprogramowanie stacji użytkownika pozwala na bezpieczną komunikację i selektywne szyfrowanie zawartości dysków lokalnych. Zapewnia transparentne szyfrowanie sesji przy dostępie do serwerów i aplikacji, zabezpieczenie przed nieuprawnionym użyciem certyfikatów i kluczy prywatnych, wykorzystanie podpisu cyfrowego w celu uwierzytelnienia komunikujących się procesów. Podstawową funkcją jest zapewnienie dostępu do komputerów i aplikacji w rozproszonym, heterogenicznym środowisku teleinformatycznym przedsiębiorstwa czy organizacji.

● Oprogramowanie agenta (Keon Agent)

Aplikacje na serwerach objętych systemem bezpiecznego dostępu muszą zostać wyposażone w sprzężenie pozwalające na

komunikację z użytkownikiem posługującym się oprogramowaniem *Keon Desktop*. Możliwość praktycznego wdrożenia systemu tkwi w ilości standardowych modułów pozwalających na komunikację z wieloma systemami i aplikacjami różnych producentów (np. bazy danych Oracle, Informix, Sybase, SAP, protokoły HTTP, telnet, systemy operacyjne – np. rozmaite odmiany UNIX-a, NT). *Keon Agent* spełnia te warunki, a ponadto zapewnia też mocne uwierzytelnienie (OTP, *two factors authentication* itp.)

● Serwer Bezpieczeństwa (Keon Security Server)

Oprogramowanie *Keon Security Server* zapewnia centralną kontrolę nad procesami dostępu do zasobów w sieci. Serwer obsługuje zarządzanie strukturą klucza publicznego (PKI) w standardzie X.509, służącą do wykorzystania certyfikatów kluczy publicznych użytkowników jako informacji uwierzytelniającej (*credentials*) w procesie identyfikowania i uwierzytelniania użytkowników, a także w czasie szyfrowania sesji dostępu do zdalnych systemów i aplikacji.

Certyfikaty użytkowników mogą być przechowywane na dyskietkach bądź dyskach w postaci zaszyfrowanych plików, bądź na kartach inteligentnych. Dostęp do kluczy prywatnych użytkowników jest chroniony hasłem dynamicznym systemu OTP, sprzężonym z Serwerem Bezpieczeństwa.

Usługi katalogowe (LDAP) sprzężone z PKI zapewniają ułatwioną dystrybucję i zarządzanie certyfikatami. (Użytkownik może łatwo uzyskać swe „credentials" przy pomocy swojego komputera dostępowego do sieci (np. desktop PC), a administrator ma możliwość np. sprawnego centralnego unieważniania certyfikatów użytkowników.

Wbudowany w *Keon Security Server* serwer certyfikatów może współpracować z dowolnymi certyfikatami X.509, wydanymi przez inne Urzędy ds. Certyfikatów (*Certification Authority*).

Dodatkowo prawa dostępu dla użytkowników czy grup użytkowników są kontrolowane z jednego miejsca (konsola Serwera Bezpieczeństwa), podobnie jak poziom bezpieczeństwa komputerów w całej sieci. Serwer Bezpieczeństwa posiada swą replikę.

W środowisku Keon jest więc możliwe zapewnienie bezpiecznego dostępu do aplikacji, np. SAP, Oracle, Sybase, PeopleSoft, oraz wykorzystywanie wszelkich aplikacji opartych na idei otwartego PKI, jak np. poczta elektroniczna (SMIME), aplikacji opartych na WWW (SSL) czy wirtualnych sieci prywatnych (VPN), opartych o standard IPSec. W tym celu można wykorzystywać certyfikaty generowane przez system Keon lub dowolne certyfikaty wydawane na świecie (np. *VeriSign*). □

Usługi finansowe w polskim Internecie

Adam Kaliszewski [1]
Arthur Andersen Sp. z o.o.

Od trzech lat można już mówić o usługach finansowych w Polsce opartych o Internet. Na rynku działa kilka instytucji finansowych, które nie tylko reklamują swoje usługi w sieci, lecz świadczą je dla pewnego grona klientów. Obecnie inne podmioty rynków finansowych przymierzają się do wprowadzenia podobnych usług. Stoimy więc przed rewolucją jakościową w usługach finansowych.

Na czym to polega?

Internet jest dobrym medium wymiany informacji na odległość. Przy zapewnieniu odpowiedniego poziomu bezpieczeństwa przepływu informacji oraz zachowania procedur ostrożnościowych, można zawierać różnego rodzaju transakcje. Należą do nich usługi bankowe, np. zakładanie lokat, sprawdzanie salda rachunku, jak również handlowe, dotyczące zakupów hurtowych surowców i komponentów do produkcji.

Jakie korzyści oferuje Internet?

Przede wszystkim szybkość zawierania transakcji oraz precyzyjną wymianę informacji (znikomy ułamek przekłamań przesyłanych transakcji. Jest to wynik o klasę lepszy niż stosowanie faksu czy głosu). Dodatkowo czas zawierania transakcji oraz odległość geograficzna stron transakcji jest nieistotna. W efekcie możliwe jest całodobowe świadczenie usług, w miejscu pobytu klienta. W ten sposób otwiera się nowy sposób komunikacji z klientami, który umożliwi zarówno wyższą jakość usług jak również niższy koszt dla obu stron. Banki nie muszą posiadać gęstej sieci placówek, aby dotrzeć do klientów. Przeciwnie, klienci wyszukują bank poprzez Internet i korzystają z usług automatycznych, na zasadzie samoobsługowej. W rezultacie możliwe jest przeniesienie części korzyści dla klientów, np. w postaci niższych prowizji i lepszego oprocentowania.

Jakiego typu usługi świadczone są w Polsce?

Usługi dostępne w Polsce są jeszcze stosunkowo słabo rozwinięte i traktowane przez instytucje finansowe raczej na zasadzie eksperymentu niż jako podstawowy sposób sprzedaży usług. Tym niemniej usługi można podzielić na następujące grupy:

- bankowe,
- maklerskie,
- ubezpieczeniowe,
- pozostałe.

Banki dosyć szybko zorientowały się, że Internet może oznaczać coś więcej niż tylko ciekawostkę techniczną. Pierwszym bankiem w Polsce, który otworzył swoje podwoje w Internecie był Powszechny Bank Gospodarczy w Łodzi (obecnie PBG jest częścią Grupy Pekao S.A.)[2]. Niestety procedura zakładania rachunku jest czasochłonna i wynosi do 21 dni roboczych[3]. W ramach pakietu usług nazywanego „Oddziałem Elektronicznym" można sprawdzić saldo rachunku, zobaczyć ostatnie transakcje, założyć lokaty terminowe w złotych, a także dokonywać przelewów krajowych. W 1999 roku planowano rozszerzyć ofertę tak, aby przypominała ona znaną usługę Eurokonta. Chodzi przede wszystkim o karty bankomatowe, kredytowe, Euroczeki i inne usługi. Jednak nie jest znany ostateczny termin rozszerzenia oferty.

Usługi maklerskie reprezentuje Dom Maklerski Banku Ochrony Środowiska[4]. Po założeniu rachunku można składać zlecenia kupna, sprzedaży papierów wartościowych na giełdzie warszawskiej. Również możliwy jest udział w dogrywkach. Prowizje maklerskie kształtują się na niższym poziomie niż w pozostałych biurach. Co pewien czas DM BOŚ umożliwia zapisy na rynku pierwotnym, kiedy spółka dopiero wchodzi na giełdę i po raz pierwszy oferuję akcje. Przed dokonaniem zapisu należy przeczytać prospekt emisyjny (dostępny na stronach WWW banku). Dodatkowo można sprawdzić stan rachunku, a także przelać środki do innego banku. Jest to już całkiem spory pakiet usług. Być może za jakiś czas będzie możliwe wykorzystanie rachunku maklerskiego do kupna zagranicznych papierów wartościowych w Euro?

Ciekawym przykładem z **rynku ubezpieczeniowego** jest oferta Hestii Insurance[5] z Sopotu. Możliwe jest ubezpieczenie odpowiedzialności cywilnej w życiu prywatnym, a także indywidualne ubezpieczenie następstw nieszczęśliwych wypadków. Po przeczytaniu ogólnych warunków zawierania umów należy wybrać ten z wariantów ubezpieczenia, który najlepiej odpowiada indywidualnej sytuacji klienta. Ubezpieczyciel automatycznie obliczy składkę i poprosi o adres. Ochrona ubezpieczeniowa będzie skuteczna po około 14 dniach, kiedy klient ma czas na opłacenie składki. Już ponad 7000 osób odwiedziło strony Hestii.

Należy oczekiwać, że powyższe ubezpieczenia to dopiero wstęp do pełnego świadczenia usług poprzez sieć. Na przykład, wraz ze wzrostem liczby samochodów w Polsce coraz więcej zawiera się umów OC i AC. Kalkulując koszt świadczenia tego rodzaju usług bierze się pod uwagę wydatki na akwizytorów, punkty obsługi klienta itp. Jednak sprzedaż bezpośrednia poprzez Internet może radykalnie zmniejszyć ten koszt. Przenosząc oszczędności na klientów można obniżyć składki. Czy można zaoferować w Internecie ubezpieczenia tańsze np. o 30 proc. od tradycyjnych? Jeżeli tak, to można pokusić się o próbę zmiany układu sił na rynku ubezpieczeń komunikacyjnych w Polsce.

Do pozostałych usług należy zaliczyć oferty licznych funduszy powierniczych oraz Powszechnych Towarzystw Emerytalnych z drugiego filara. Jednakże nie sprzedają one pakietu usług poprzez sieć, tylko wykorzystują Internet jako medium reklamowe. Być może za jakiś czas będzie możliwy dostęp do konta inwestycyjnego i drugiego filaru. Również inne podmioty finansowe, np. oferujące kredyty ratalne czy usługi leasingowe są już obecne w sieci, lecz nie jest to jeszcze pełne świadczenie usług.

Jakie są największe przeszkody w świadczeniu usług poprzez Internet?

Do ważnych, otwartych problemów należy zachowanie bezpieczeństwa oraz pełne uregulowanie kwestii prawnych. Należy do nich między innymi wiarygodność podpisu elektronicznego zastępującego zwykły podpis i dowód osobisty w transakcjach finansowych. Jednak najważniejszą naturalną barierą rozwoju usług finansowych w Polsce są umiejętności potencjalnych użytkowników Internetu. Po pierwsze stanowią oni niewielką liczbą w społeczeństwie, nie przekraczającą 3 miliony osób. W dodatku są oni stosunkowo młodzi (uczniowie, studenci) i korzystają oni jeszcze w niewielkim zakresie z usług finansowych w ogóle. Należy oczekiwać, że w miarę rozpowszechniania się Internetu w całym społeczeństwie praktyczne wykorzystanie sieci jako medium świadczenia usług znacząco wzrośnie. □

---

[1] Artykuł zawiera wyłącznie poglądy autora.

[2] Por. www.pekao.com.pl

[3] Wg. informacji pochodzących z banku. Jest to potraktowane względami bezpieczeństwa oraz koniecznością wymiany dokumentacji papierowej pomiędzy jednostkami banku.

[4] Por. www.dmbos.pl

[5] Por. www.hestia.pl

W dniach 26 i 27 października odbyła się w Hotelu Europejskim w Warszawie kolejna edycja konferencji z cyklu SECURE, którą od trzech lat organizuje zespół CERT NASK.

SECURE '99

III KONFERENCJA CERT NASK

Aktywna ochrona systemów teleinformatycznych

pod patronatem Zarządu Łączności i Informatyki Sztabu Generalnego WP

CERT NASK, działający od roku 1996, jest pierwszym zespołem reagującym na incydenty związane z bezpieczeństwem systemów IT w naszym kraju. Jako jedyny zespół z Polski jest członkiem światowej organizacji FIRST (*Forum of Incident Response and Security Teams*) zrzeszającej ponad 80 zespołów typu IRT (*Incident Response Team*) z całego świata.

Trudno wymienić wszystkie prezentacje składające się na dwa ciągi tematyczne konferencji – ciąg TECHniczny i MANAGERski. Najwyższą ocenę w oczach uczestników uzyskał referat Krzysztofa Leszczyńskiego, reprezentującego PLUG (*Polish Linux Users Group*), na temat bezpieczeństwa systemu Linux oraz prezentacje Iana Cooka, pełniącego obwiązki kierownika zespołu oceny zagrożeń bezpieczeństwa w brytyjskim Citibanku. Te ostatnie dotyczyły aktywnej ochrony systemów teleinformatycznych ze szczególnym uwzględnieniem sieci NT.

Podobnie wysoko oceniono wystąpienia Grzegorza Pohoreckiego z firmy Safe Computing, prezentującego projekty norm i ustaw związanych z bezpieczeństwem (w tym projekt ustawy o podpisie elektronicznym). Dużym zainteresowaniem cieszył się przegląd metodologii i klasyfikacji incydentów przedstawiony przez CERT NASK, jak również wystąpienia przedstawicieli UOP. Wśród zagranicznych prelegentów byli przedstawiciele renomowanej firmy RSA Security, którzy przedstawili problematykę wdrażania Infrastruktury Klucza Publicznego w przedsiębiorstwie.

Obrońcy sieci: globalne zadania

Krzysztof Silicki

Sieci i systemy teleinformatyczne zostały gwałtownie zaadoptowane przez instytucje rządowe, administrację państwową oraz rynek komercyjny na całym świecie. Cel jest jasny: chodzi o zapewnienie lepszej komunikacji i podniesienie konkurencyjności. Coraz większa zależność rozwoju ekonomicznego od infrastruktury teleinformatycznej, a w szczególności od Internetu, jest faktem. W dodatku, dynamika wzrostu w tym zakresie jest coraz większa.

Bezpieczeństwo Internetu: stan dzisiejszy

Dzisiejszy Internet jest jednak narażony na ataki zagrażające bezpieczeństwu komputerów znajdujących się w sieci. Ataki te mają różną formę i siłę. Mogą to być np. włamania do systemów, ataki blokujące pracę komputerów lub bombardowanie przesyłkami poczty elektronicznej. Internet jest często miejscem nadużyć (fałszywe transakcje elektroniczne), przechwytywania informacji przez osoby niepowołane. Jest także narzędziem komunikacji używanym przez nielegalne organizacje.

Bez podjęcia kroków zmierzających do uczynienia z Internetu środowiska bardziej bezpiecznego i godnego zaufania, stworzona i rozwijana przez wiele krajów infrastruktura teleinformatyczna będzie w coraz większym stopniu zagrożona. Jest to tym bardziej prawdopodobne, że Internet jest konglomeratem sieci należących do poszczególnych operatorów oraz ich abonentów. Nie istnieje zatem żadna globalna instancja, mogąca narzucić użytkownikom sieci jakiekolwiek standardy bezpieczeństwa.

W środowisku organizacji zajmujących się problematyką ochrony i reagowania na incydenty pojawiające się w Internecie panuje przekonanie o konieczności podjęcia wysiłku na skalę międzynarodową celem podwyższenia ogólnego stanu bezpieczeństwa systemów teleinformatycznych. Przeprowadzenie skutecznego ataku na system włączony do Internetu nie wymaga fizycznego kontaktu z urządzeniem. Przeciwnie – atakujący może wybrać ofiarę z domeny znajdującej się geograficznie w dowolnym miejscu świata. Jeśli atak jest przeprowadzony grupowo, członkowie grupy mogą pochodzić z wielu krajów. Prawdopodobieństwo zaś, że atakujący zostanie zidentyfikowany, jest niewielkie.

Dodatkowo prawodawstwo, nawet w najbardziej rozwiniętych technologicznie krajach, nie nadąża za technologią. Nie istnieje także prawo międzynarodowe, pozwalające w skuteczny sposób ścigać przestępstwa komputerowe o charakterze trans-granicznym. W świecie wirtualnej informacji Internet stanowi poletko doświadczalne dla wielu dziedzin życia. Sieć ta rodzi nowe spojrzenie na media, rozrywkę, pracę, prawa jednostek i narodów. Najnowsze inicjatywy grupy G8 oraz organizacji OPEC idą w kierunku rozpoczęcia działań zmierzających do wypracowania skutecznej odpowiedzi na wyzwania wynikające ze specyfiki Internetu.

FIRST – reagowanie na incydenty

Potrzeba stworzenia międzynarodowego forum reagowania na incydenty naruszające bezpieczeństwo w Internecie doprowadziła do zorganizowania we wczesnych latach 90-tych *Forum of Incident Response and Security Teams* (FIRST), które zrzesza obecnie ponad 80 zespołów (z 19 krajów) zajmujących się bezpieczeństwem. FIRST stanowi forum wymiany doświadczeń i informacji związanej z zaistniałymi zdarzeniami zagrażającymi lub naruszającymi bezpieczeństwo, a także promuje działania prewencyjne. Chociaż liczba zespołów zrzeszonych w FIRST może wydawać się duża, to jednak przy istniejącej dynamice wzrostu liczby i wagi incydentów jest wielce prawdopodobne, że zespoły te nie będą w stanie ogarnąć wszystkich zadań, jakie przed nimi stoją. Obrazuje to tabela nr 1, przedstawiająca wzrost liczby zagrożeń i incydentów obsłużonych na przestrzeni ostatnich lat przez powszechnie znany zespół reagujący CERT/CC, działający na terenie USA.

Tabela 1. Incydenty i luki bezpieczeństwa zgłaszane do CERT/CC

Rok	Zgłoszone incydenty	Pojawiające się luki bezpieczeństwa
1988	6	
1989	132	
1990	252	
1991	406	
1992	773	
1993	1334	
1994	2340	
1995	2412	171
1996	2573	345
1997	2134	311
1998	3734	262
1999 (1 półrocze)	4398	163
Łącznie:	20494	1252

CERT NASK

W Polsce pierwszym zespołem powołanym (w 1996 roku) do reagowania na zdarzenia naruszające bezpieczeństwo w naszej części Internetu jest zespół CERT (*Computer Emergency Response Team*) NASK. Od 1997 roku CERT NASK jest także członkiem FIRST.

Do zadań tego zespołu należy:

- rejestrowanie zdarzeń naruszających oraz bezpośrednio zagrażających bezpieczeństwu sieci NASK, sieci abonentów NASK oraz sieci innych operatorów na terenie Polski,
- natychmiastowe podejmowanie czynności takich jak: diagnozowanie, analizowanie, znoszenie lub pomoc w znoszeniu skutków zdarzeń naruszających lub bezpośrednio zagrażających bezpieczeństwu sieci NASK i sieci abonentów NASK oraz czynności zapobiegających powstawaniu tych zdarzeń w przyszłości,
- alarmowanie użytkowników sieci o wystąpieniu bezpośrednich dla nich zagrożeń,
- współpraca z zespołami o podobnym charakterze, działającymi samodzielnie lub będącymi częścią innych podmiotów prawnych (krajowych i zagranicznych, w tym współpraca w ramach FIRST) oraz z osobami odpowiedzialnymi za bezpieczeństwo sieci w poszczególnych instytucjach dołączonych do sieci,
- prowadzenie działalności informacyjno-zapobiegawczej, mającej na celu podniesienie świadomości i troski użytkowników o właściwy stan bezpieczeństwa sieci.

Należy podkreślić, że działalność CERT NASK ma charakter dobrowolny i nie wiąże się z żadną odpłatnością ze strony zgłaszających. Praca zespołu, będąca swoistą służbą na rzecz całej społeczności internetowej w Polsce, jest finansowana ze środków NASK. Środki te są jednak na tyle szczupłe, że pozwalają jedynie na prowadzenie działalności w zakresie podstawowym.

Główne tendencje w dziedzinie bezpieczeństwa systemów teleinformatycznych można prześledzić analizując coroczne raporty publikowane przez CERT NASK (dostępne na stronach internetowych http://www.nask.pl/CERT). Prześledźmy je na podstawie danych roku 1998.

Statystyki krajowe

Podobnie jak w roku 1997, również w roku 1998 CERT NASK odnotował wzrost liczby zarejestrowanych incydentów naruszających bezpieczeństwo. Ich łączna liczba osiągnęła pułap ok. 100.

Rozkład czasowy

Ataki te odnotowywane były w przeciągu całego roku z nasileniem w takich miesiącach, jak marzec i październik. Szczególne nasilenie tego procesu w październiku może być spowodowane szczególną aktywnością środowiska akademickiego, z którego, jak wskazuje statystyka, wywodzi się najwięcej ataków.

Typ ataku

Wśród ataków prym wiodą te, które jako cel obrały sobie system poczty elektronicznej. Poważna część z tych ataków związana jest z popularnością i dużą ilością „dziur" w oprogramowaniu *sendmail*. Istotnym problemem okazały się też przypadki skanowania sieci w celu przygotowania ataku. Powszechna dostępność oprogramowania służącego do skanowania, często reklamowanego pod hasłem „sprawdź bezpieczeństwo swojego komputera", poważnie przyczyniła się do spopularyzowania tego typu ataku. Również niezwykle łatwy atak na serwer z wykorzystaniem oprogramowania typu *common gateway interface* (CGI) sprawił, że wśród zgłoszonych incydentów wiele było takich, które wskazywały na chęć przejęcia istotnych informacji przez intruza w ten właśnie sposób.

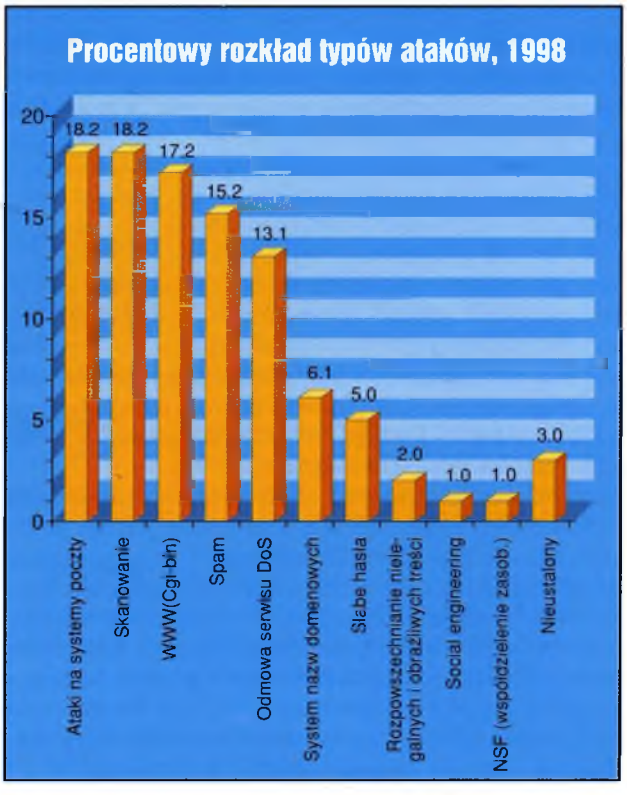
Źródło ataków

Tak jak już wspomniałem wcześniej, w tej kategorii pierwszeństwo ma środowisko akademickie. Nie jest to zjawisko nowe. Istotnym trendem okazał się natomiast poważny wzrost wykorzystania do przeprowadzania ataków darmowego (a wiec niekontrolowanego) dostępu do Internetu poprzez sieć TPNET. W strukturach TP S.A. powstał dedykowany zespół odpowiedzialny za tego typu przypadki, uruchomiono procedury organizacyjne i techniczne prowadzące do ograniczenia zjawiska. Współpraca z firmami udostępniającymi na swych serwerach darmowe konta dla internautów niewątpliwie przyniosła efekty, które widać w malejącej liczbie incydentów powiązanych właśnie z darmowymi kontami.

Efekt ataków

Wśród zarejestrowanych ataków więcej jest takich, które według zgłaszających zostały skutecznie odparte, niż tych, które skończyły się przejęciem przez intruza praw administratora systemu. Potwierdza to fakt, że tylko nieliczne incydenty zgłaszane są do oficjalnych statystyk i rzadko kto chce się przyznawać do tego, że jego sieć została skutecznie zaatakowana. Jest to zjawisko ogólnoświatowe.

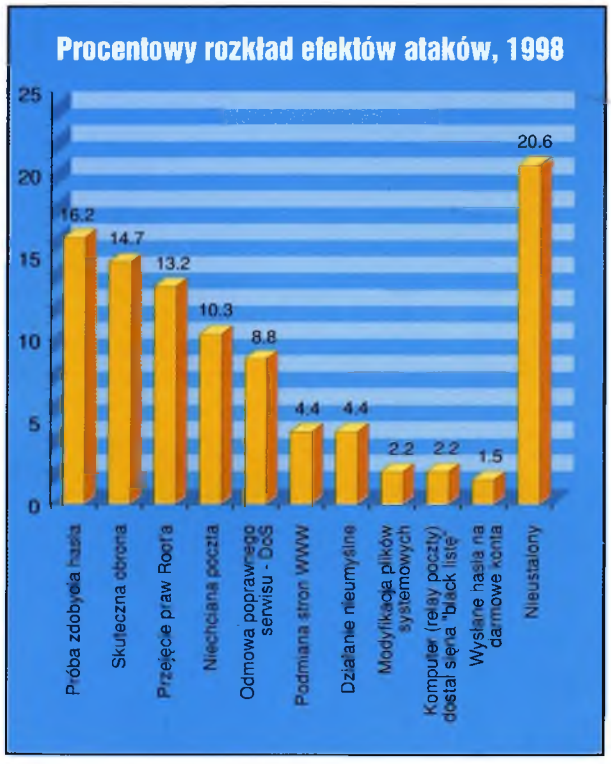
Niestety, największy procent incydentów odnosi się do sytuacji, w której poszkodowany nie jest w stanie ustalić poniesionych strat i często nie ma na to już szans, gdyż system, który musi działać w trybie ciągłym, jest dość szybko reinstalowany.



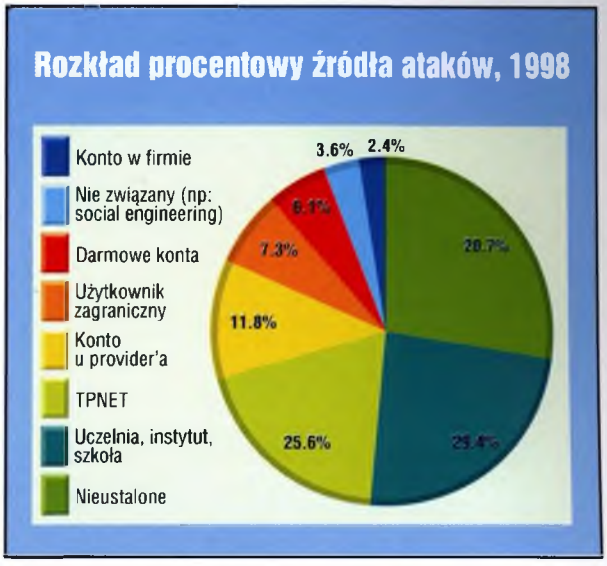
Cel ataku i źródło zgłoszenia

Większość, blisko 80 proc. zgłaszanych do CERT NASK incydentów, pochodzi od użytkowników sieci, głównie przedstawicieli firm i instytucji. Pozostałe, niewiele ponad 20 proc. zgłoszeń, pochodzi od instytucji, które w swojej działalności zajmują się walką z przestępczością komputerową, czyli innych zespołów reagujących IRT (*Incident Response Teams*) lub policji, ze zdecydowanym wskazaniem na te pierwsze.

Wśród poszkodowanych jest dokładnie 50 proc. użytkowników zagranicznych i 50 proc. użytkowników polskiej sieci Internet. Na negatywne oddziaływanie intruzów bardziej wyczuleni są użytkownicy zagraniczni. Przyczyną takiego stanu rzeczy jest – z jednej strony – większa wrażliwość użytkownika zagranicznego na nieuprawnioną działalność intruzów, zaś z drugiej – dotychczasowe przekonanie o bezkarności i często anonimowości intruza, jakie panuje wśród polskich internautów.



Wśród pozytywnych zmian, zaobserwowanych w trakcie działalności CERT NASK, należy wymienić powstawanie w ramach struktur firmowych zespołów lub grup osób odpowiedzialnych za sprawy bezpieczeństwa teleinformatycznego. Należy się spodziewać, że dodatkowym impulsem do powstawania takich zespołów będzie uchwalona z końcem ubiegłego roku ustawa o ochronie informacji niejawnej.



Globalna koordynacja zadań

FIRST w swej obecnej postaci jest organizacją o charakterze dobrowolnym i nie jest w stanie pełnić roli globalnej instancji, koordynującej działania zmierzające do poprawy bezpieczeństwa w Internecie.

Dotyczy to także samych zespołów reagujących IRT, zrzeszonych w FIRST. Składają się one z praktyków i specjalistów, którzy wprawdzie posiadają odpowiednią wiedzę i doświadczenie w dziedzinie ochrony systemów informatycznych, lecz nie mają żadnego tytułu do wpływania na poziom bezpieczeństwa systemów znajdujących się w sieci. Szczupłość środków, jakimi dysponują poszczególne zespoły, a FIRST w szczególności, objawia się w pewnych niekorzystnych zjawiskach, takich jak np. powolne powstawanie standardów, chociażby w sferze terminologii dotyczącej incydentów. Tak więc trudno jest np. porównywać ilościowo incydenty zarejestrowane w CERT/CC czy w CERT NASK, gdyż inne są kryteria rejestrowania otrzymanego zgłoszenia jako incydentu. Natomiast porównując tendencje można łatwo stwierdzić, że następuje stały wzrost ilości spraw rejestrowanych przez każdy z 80 zespołów należących do FIRST.

W związku z powyższymi trudnościami w ramach FIRST zrodziła się inicjatywa powołania międzynarodowej infrastruktury dla zapewnienia globalnej reakcji na wzrastające zagrożenie bezpieczeństwa systemów teleinformatycznych. Zarysy tej inicjatywy można ująć w następujących czterech niezależnych elementach:

– po pierwsze, infrastruktura dla koordynacji efektywnego reagowania na pojawiające się incydenty w skali globalnej celem

zapewnienia coraz efektywniejszych metod przeciwdziałania (wczesne ostrzeganie, analiza trendów, przewidywanie);

- po drugie, forum dyskusji i tworzenia międzynarodowych standardów czy polityki bezpieczeństwa, a także wypracowywania porozumień wspierających działanie infrastruktury zarysowanej w poprzednim punkcie;
- po trzecie, ciało koordynujące działania w zakresie podwyższania poziomu bezpieczeństwa technologii informacyjnych poprzez gromadzenie, analizę oraz rozpowszechnianie doświadczeń praktycznych, informacji i wniosków (zebranych w czasie obsługi incydentów przez zespoły reagujące na całym świecie);
- po czwarte, profesjonalna organizacja specjalizująca się w edukacji osób lub zespołów zajmujących się reagowaniem na incydenty naruszające bezpieczeństwo oraz ogólniej: działających w branży *IT security*.

Aby cele te zrealizować, konieczne jest nawiązanie szerokiej współpracy pomiędzy rządami poszczególnych krajów, instytucjami prawnymi, firmami komercyjnymi, nauką oraz praktykami mającymi doświadczenie w reagowaniu na incydenty.

Forum of Incident and Security Teams jest niewątpliwe organizacją, która może wcielać w życie tak zarysowaną misję. Z drugiej strony szczupłość środków, jakimi dysponują poszczególne zespoły oraz FIRST w obecnej formie, wydłuża chociażby procesy normowania nazewnictwa: obecnie trudno jest np. porównywać ilościowe dane podawane przez CERT/CC oraz CERT NASK, ponieważ rejestracja zgłoszenia jako incydentu przebiega podług innych kryteriów. Na pewno jednak można mówić o tendencji stałego, gwałtownego wzrostu liczby incydentów rejestrowanych przez wszystkie 80 zespołów zgrupowanych w FIRST.

Globalna koordynacja zadań w dziedzinie podwyższania bezpieczeństwa systemów teleinformatycznych jest odpowiedzią na wyzwanie, jakie stawia nam dzisiejszy Internet. Zbagatelizowanie tego wyzwania może być przykre w konsekwencjach dla światowych systemów komunikacji – i to w całkiem niedalekiej przyszłości. Dlatego już dziś w najbardziej uprzemysłowionych krajach świata na szczeblach rządowych pracuje się nad zjawiskiem, które coraz częściej określane jest jako „elektroniczny terroryzm". Można żywić nadzieję, że i w naszym kraju problematyka ta uzyska właściwą rangę na odpowiednich szczeblach władzy. □

NASK

Wydawca: NASK, ul. Bartycka 18, 00-716 Warszawa, tel. *Call Center* (022) 651 05 15
Sekretariat (022) 651 05 20, fax (022) 841 00 47, e-mail: contact@nask.pl, http://www.nask.pl
Redaguje: Maria Baranowska, e-mail: biuletyn@nask.pl
Przygotowanie do druku: DĄBROWA s.c.