

Dorota Górską
Papieska Akademia Teologiczna
Kraków

Sieć sieci komputerowych - czyli INTERNET

Komputery osobiste, zgodnie z sugestią zawartą w samej nazwie, zostały pomyślane jako niezależne narzędzia pracy, służące indywidualnym użytkownikom. Atrakcyjność tego narzędzia okazała się tak duża, że w krótkim czasie stało się ono podstawowym wyposażeniem wielu stanowisk pracy. Z chwilą, gdy liczba komputerów używanych w jakimkolwiek zakładzie pracy stała się większa niż jeden, pojawił się problem wymiany danych między poszczególnymi stanowiskami pracy. Oczywiście stało się to, że należy połączyć wszystkie komputery znajdujące się na poszczególnych stanowiskach pracy. Na terenie zakładów pracy, uczelniach oraz wszędzie tam, gdzie podczas pracy używa się większej ilości komputerów, pojawiły się *sieci komputerowe*.

Z punktu widzenia rozległości sieci komputerowe klasyfikuje się następująco:

- **LAN** (*ang. Local Area Network* - sieć o zasięgu lokalnym) są to sieci komputerowe z reguły znajdujące się w jednej instytucji (np. na uczelni). Zazwyczaj w sieciach lokalnych odległości pomiędzy poszczególnymi komputerami wynoszą od 10 metrów do kilkunastu kilometrów.
- **MAN** (*Metropolitan Area Network* - sieć o zasięgu wielkomiejskim) są to sieci obejmujące obszary wielkomiejskie. Sieci tego rodzaju są zazwyczaj wykorzystywane przez wielu użytkowników.
- **WAN** (*Wide Area Network* - sieć rozległa) są to sieci o zasięgu globalnym, używane zazwyczaj przez instytucje i organizacje międzynarodowe.

Pierwsza duża sieć komputerowa powstała w Stanach Zjednoczonych w roku 1996. Nazwano ją ARPANET- od *Advanced Research Project Agency* (agencja do spraw badań perspektywicznych). Drugi człon nazwy od *NET* - to wyraz, który w języku angielskim oznacza właśnie sieć. Zasadniczym celem, jaki przyświecał jej utworzeniu, było sprawdzenie nowych koncepcji przesyłania informacji zakodowanych cyfrowo. Do sieci tej zostały włączone komputery ośrodków badawczych i akademickich z terenu USA. Początkowo sieć była dostępna tylko dla instytucji i uczelni pracujących dla potrzeb obronności Stanów Zjednoczonych. Gdy okazało się, że eksperyment się powiódł, do sieci dołączano nowe ośrodki badawcze i sieć zatraciła swój, początkowo czysto wojskowy, charakter. W tym czasie na wielu uczelniach i w wielu instytucjach powstawały nowe sieci lokalne, a w końcu lat siedemdziesiątych zaczęto tworzyć sieci nadrzędne, których zadaniem było połączenie sieci lokalnych i ośrodków badawczych w jeden zespół umożliwiający wzajemną wymianę informacji; w ten sposób zrodziła się koncepcja sieci nadrzędnej, znanej obecnie jako **INTERNET**. Trudno jest wymienić konkretną datę, którą można uznać za dzień narodzin Internetu, gdyż jego powstanie było procesem ciągłym, polegającym na systematycznym wzroście liczby wzajemnie połączonych komputerów. W roku 1989 liczba komputerów włączonych do Internetu wynosiła 80 000, a w ciągu następnych pięciu lat zwiększyła się prawie 30-krotnie. W lipcu 1996 r. do Internetu włączonych było około 13 milionów komputerów w ponad 60 krajach, na wszystkich kontynentach. Polska dołączyła do Internetu w 1991 roku.¹

Współczesny Internet, nazywany także *Siecią Sieci*, zbudowany jest na zasadzie łączenia ze sobą poszczególnych sieci lokalnych. Sieci istniejące np. w jednej instytucji łączy się ze sobą (za pomocą tzw. routerów) tworząc dużą sieć danej instytucji. Takie sieci mogą być następnie przyłączane do sieci miejskich, ta zaś do sieci krajowej, łączącej poszczególne sieci

¹ Jarosław Rafa, *Internet od podstaw*, INTERNET-MAGAZYN UŻYTKOWNIKÓW SIECI, 1997 nr 3 s. 14-79

miejskie (jako łącza używane są najczęściej światłowody lub kable telefoniczne).

Z Internetu mogą korzystać także indywidualni użytkownicy. Aby włączyć się do Internetu, wystarczy zaopatrzyć się w komputer, homologowany modem i program komunikacyjny.

Modułowa budowa Internetu umożliwia jej dynamiczny rozwój, bowiem dołączenie nowego użytkownika nie zakłóca struktury i wymaga uzgodnień tylko z osobami zarządzającymi bezpośrednią podsicią, do której chce się dołączyć nowy klient.

Po przyłączeniu się do Internetu możemy korzystać z niego w bardzo różnorodny sposób. Szczególnie rozpowszechnione są trzy rodzaje wykorzystania sieci:

- Korzystanie z programów i danych znajdujących się na innym komputerze.
- Poczta elektroniczna.
- Przesyłanie listów.

Szczególnie atrakcyjna jest pierwsza z wymienionych możliwości. Dzięki niej stają się dostępne zasoby zgromadzone na bardzo dużych komputerach włączonych do Internetu. Oznacza to między innymi, że jest możliwe uruchomienie programów zainstalowanych na tych komputerach i używanie programów niemożliwych do zrealizowania na komputerach osobistych. Dostępne są również bazy danych z różnych dziedzin nauki, techniki i kultury gromadzone na innych komputerach.

Najbardziej popularnym sposobem wykorzystanie Internetu jest poczta elektroniczna. Za jej pomocą możliwe jest wysyłanie wiadomości do jednej osoby lub grupy osób. Ciekawe są również tzw. listy dyskusyjne służące do wymiany informacji na określone tematy. Możliwości porozumiewania się za pomocą Internetu są niemal nieograniczone.

Użytkownicy Internetu mogą również przysyłać różnego rodzaju pliki: teksty, obrazy, arkusze kalkulacyjne, a nawet pliki dźwiękowe.

Internet to międzynarodowa sieć komputerowa, która umożliwia komunikowanie się komputerów niezależnie od miejsca i rodzaju ich fizycznego połączenia. Korzystając ze wszystkich oferowanych przez Internet możliwości, użytkownicy najczęściej nie zdają sobie sprawy z tego na jakie narażeni są niebezpieczeństwa. Wiadomości przesyłane elektronicznie mogą zostać odczytane przez niewłaściwych odbiorców. Przesyłane teksty można przerobić lub też skierować do innego adresata. Elektroniczni fałszerze mogą popełniać oszustwa w czyimś imieniu lub podszywać się pod godne zaufania osoby, chcąc skłonić odbiorców do zaakceptowania podejrzanej wiadomości.

Pakiety danych są przesyłane po łączach sieciowych od jednego węzła do drugiego. Na każdym z takich łączy można odczytać zawartość przesyłanego pliku. Jedynie wzajemne zaufanie pozwala wierzyć, że przesłaną wiadomość odczyta tylko odbiorca. Każdy kto ma dostęp do Internetu może stać się ofiarą włamań lub też sam atakować innych.

Szczególnie niebezpieczne jest przyłączanie się do sieci dobrze skomputeryzowanych instytucji. Wewnętrzna sieć jest z reguły tak skonstruowana, że użytkownicy mogą bez przeszkód dzielić się danymi zapisanymi na swoich komputerach. Z chwilą włączenia się do Internetu wewnętrzna sieć staje się dostępna dla wszystkich osób korzystających z sieci.

W roku 1994 grupa informatyków z Carnegie Mellon University² odkryła, że wszystkie komputery z wbudowanymi głośnikami miały fabrycznie ustawione parametry na nieograniczony odczyt. Każdy, kto zdobył sieciowy dostęp do takiej stacji, mógł podsłuchiwać rozmowy prowadzone w pobliżu komputera. W parę miesięcy później zauważono, że bufony pamięci ekranu i bufony zapamiętujące znaki wystukiwane na klawiaturze były również ustawiane fabrycznie na nieograniczony odczyt. Informacje przesyłane z takich komputerów były bardzo łatwe do przechwycenia przez niepożądanych odbiorców. Mając dostęp do sieciowego komputera napastnicy mogli również instalować na nim własne

² Paul Wallich, *Sieciami piraci*, ŚWIAT NAUKI, 1994 nr 5(33) s.72-81

programy (także wirusowe), lub nawet zmieniać zapisy systemowe.

Dynamizmie rozwijająca się sieć komputerową, liczne ułatwienia pozwalające bez przeszkód przenieść się w dowolne miejsce na świecie spowodowały pominięcie etapów wzmacniających bezpieczeństwo. Powszechnie używany Gopher ma niedociągnięcia umożliwiając dostęp nie tylko do publicznych, ale i do prywatnych plików.

Coraz częściej duże i małe firmy, a nawet indywidualni użytkownicy prowadzą interesy za pomocą poczty elektronicznej. Zobowiązania pieniężne przechodzą z rąk do rąk na podstawie elektronicznych obietnic.

Aby uwierzytelnić tożsamość nadawcy informatycy starają się o to, aby każdy użytkownik „logujący” się w Internecie był sprawdzany przez system. Wprowadzono tzw. *demony identyfikacyjne*. Zadaniem demonów jest żądanie potwierdzenia tożsamości przy łączenie się z serwerem pocztowym. Tylko podanie właściwego identyfikatora pozwala na swobodne korzystanie z sieci. Demony to jednak tylko maszyny, które można skonfigurować tak, aby potwierdzały identyfikatory zgodnie z wolą autora.

Większość komputerów bazuje na serwerach nazw domen, które szybko tłumaczą *nazwę donmenową* np. xerox.com na nazwę zrozumiałą dla maszyny np. 148.22.371.86. Niestety takie serwery to przecież zwykłe komputery podatne na oszustwa i włamania. Oszuści komputerowi potrafią tak zmodyfikować bazę serwera, że mają swobodny dostęp do dowolnych baz. Żaden komputer nie potrafi sprawdzić, od kogo faktycznie pochodzi pakiet otrzymywany przez Internet, ani kto jest jego odbiorcą.

Użytkownicy Internetu ciągle lekceważą podstawowe zasady bezpieczeństwa i nie zabezpieczają dostępu do swoich stanowisk hasłami bądź naklejąją na swoje komputery karteczki z wypisanymi hasłami. Pięcioro z 80 użytkowników wybiera jako hasło swoje imię. Z tego powodu stworzono odpowiednie programy nie akceptujące jako hasła imion lub słów wziętych ze słownika.

Inną metodą uszczelnienia dostępu do Internetu jest tzw. *ściana ogniowa*. Jest to specjalny komputer przeznaczony do zabezpieczania wewnętrznej sieci przed włamaniem. Bada on wszystkie pakiety przybywające i opuszczające domeny. Ściany ogniowe ograniczają jednak znacznie ilość połączeń ze światem. Aby umożliwić mieć dostęp do wszystkich oferowanych przez Internet usług, a jednocześnie uszczelnić nieodporne na włamania programy (np. Gopher i Mosaic) zbudowano ścianę ogniową z dwóch wyspecjalizowanych komputerów. Jeden z nich jest podłączony do Internetu, a drugi do lokalnej sieci firmy. Zewnętrzny komputer bada wszystkie napływające informacje i do swojego wewnętrznego partnera dopuszcza jedynie „bezpieczne” informacje, które ponownie sprawdzane są przez wewnętrzny komputer.

Jako środek zabezpieczający przed niepożądanymi użytkownikami stosuje się również *hasła jednorazowe*, a także *hasło-odzew*. Metoda hasła jednorazowego polega na posiadaniu całej listy haseł i używaniu ich po kolei. Powtórzenie hasła powoduje rozpoznanie włamania. Zasada hasło-odzew rezygnuje z tradycyjnych haseł; zamiast tego użytkownik musi podać prawidłową odpowiedź na losowo zadane przez system pytanie. Najczęściej hasłem jest liczba, którą należy przekształcić według tajnego klucza.

Ponieważ największe niebezpieczeństwo włamania do sieci stwarza korzystanie z poczty elektronicznej wysunięto propozycję przesyłania zakodowanych informacji. Kodowanie mogłoby również służyć potwierdzeniu identyfikacji nadawcy.

W tym miejscu należałoby dodać, że włamanie się na cudze konto wymaga niemałych umiejętności. „Nieproszeni goście” Internetu to ludzie o ogromnych wiadomościach i doświadczeniu. Wciąż trwa rywalizacja między haker'ami, a ludźmi starającymi się zabezpieczyć nietykalność kont klientów sieci.

W ciągu ostatnich kilku lat Internet stał się miejscem wymiany informacji dla przedstawicieli wszystkich profesji - zaczynając od analityków finansowych, a na projektantach mody kończąc. Nadmiar krążących danych stał się przyczyną

przeciążenia sieci. Wyszukanie potrzebnych danych staje się coraz trudniejsze. Ostatnio mówi się o budowie Internetu II, odrębnego systemu, dzięki któremu naukowcy będą mogli znowu spokojnie pracować.

Komputery stają się powoli nieodwracalnym składnikiem prawie wszystkich dziedzin naszego życia, dając nam nowe, niespotykane dotąd możliwości. Jednak coraz częstsze są przypadki „niewłaściwego” użycia technologii komputerowej. Skłoniło to niektórych naukowców do zajęcia się analizą tego problemu. Podjęto próby sformułowania i uzasadnienia norm postępowania etycznego w dziedzinie użytkowania i wykorzystywania komputerów. W ten sposób powstała nawa dziedzina zwana *etyką komputerową*. Miejscem narodzin etyki komputerowej są Stany Zjednoczone. Właśnie tam z uwagi na ogromny rozwój komputeryzacji i wprowadzenie jej do wielu dziedzin życia, zanotowano najwięcej wypadków oszustw komputerowych. Pierwszy tekst poruszający problem etyki komputerowej został napisany przez Waltera Manera³. Rokiem przełomowym w historii komputerowej był rok 1985. Pojawiły się wtedy prace⁴, które stały się podstawą do zaakceptowania definicji etyki komputerowej wyrażającej wpływ technologii komputerowej na świat ludzkich wartości. Na liście wartości, którymi zajmuje się etyka komputerowa znajdujemy:⁵ wolność, odpowiedzialność, prywatność, własność prywatną, sprawiedliwość, samorealizację, wolność estetyczną. Pierwsze Europejskie spotkanie dotyczące etyki komputerowej odbyło się w marcu 1995 roku w Anglii na uniwersytecie De Montfort w Leicester. Europa Wschodnia reprezentowana była przez Polaków. Na konferencji postanowiono powołać centra badań etyki komputerowej w Europie. W Polsce miejscem takim stał

³ Walter Maner *Staeter Kit in Computer Ethics*, Helvetia Press. 1980

⁴ Deborach G. Johnson *Etyka komputerowa*,

Terrell W. Bynum *Komputery i etyka*

James H. Moor *Czym jest etyka komputerowa ?*

⁵ Andrzej Kocikowski *Wprowadzenie do problemu etyki komputerowej*, referat wygłoszony na VI Poskim Zjeździe Filozoficznym w Toruniu w październiku 1996 roku

się Poznań. W kwietniu 1995 roku w Instytucie Kulturoznawstwa UAM odbył się pierwszy wykład z dziedziny etyki komputerowej.

Internet jest zapowiedzią przyszłości, zwiastunem epoki informacji. Komputer, który do niedawna wiązał przy biurku pozwala obecnie na kontakt z całym światem. Każdy z nas powinien dążyć do tego aby praca w sieci była przyjemna i ciekawa. Dlatego też musimy przestrzegać wszystkich zasad chroniących dostęp do sieci „nieproszonych gości”.