Criminalitatea informatică poate cauza multe probleme în societatea modernă. Prin urmare, România a adoptat legislaţia privind criminalitatea informatică care corespunde pe deplin convenţiilor şi standardelor internaţionale. Totuşi, această legislaţie poate fi complexă din punctul de vedere al aplicării sale pentru autorităţile care o implementează, în special pentru aceia care sunt mai puţin familiarizaţi cu computerele şi serviciile electronice ca parte a vieţii de fiecare zi.

Portalul eFrauda a fost realizat de către Ministerul Comunicaţiilor şi Tehnologiei Informaţiei şi este gestionat împreună cu Serviciul de Combatere a Criminalităţii Informatice din cadrul Ministerului Administraţiei şi Internelor şi secţia specializată din Parchetul de pe lânga Înalta Curte de Casaţie şi Justiţie. Portalul dă oricui posibilitatea de a sesiza autorităţile cu privire la o posibilă fraudă sau alte activităţi ilegale pe Internet.
www.efrauda.ro

Acest *Ghid introductiv pentru aplicarea dispoziţiilor legale referitoare la criminalitatea informatică* a fost elaborat de către proiectul RITI dot-Gov, în cooperare cu Ministerul Comunicaţiilor şi Tehnologiei Informaţiei. *Ghidul* asigură asistenţă pentru autorităţile care aplică legea şi pentru toţi cei care sunt implicaţi în prevenirea criminalităţii informatice.

Proiectul RITI dot-Gov face parte din Iniţiativa pentru Tehnologia Informaţiei în România, RITI, a cărei implementare a fost începută în 2002 de către Misiunea din România a Agenţiei Statelor Unite pentru Dezvoltare Internaţională (USAID), în cooperare cu Ministerul Comunicaţiilor şi Tehnologiei Informaţiei. Proiectul RITI dot-Gov este implementat în România de Internews Network Inc, o organizaţie non-profit cu sediul în Statele Unite.

Pentru informaţii suplimentare:
www.usaid.gov/info_technology/dotcom
www.riti-internews.ro
www.internews.org
www.mcti.ro

GHID
INTRODUCTIV PENTRU APLICAREA DISPOZIŢIILOR LEGALE REFERITOARE LA CRIMINALITATEA INFORMATICĂ

INTERNEWS
RITI dot-Gov

MCTI

Bucureşti,
Mai 2004

Elaborarea acestui ghid a fost posibilă prin asistența asigurată de către Centrul de Servicii Regional Budapesta al Agenției Statelor Unite pentru Dezvoltare Internațională, USAID, în cadrul Acordului nr. CA # 186-A-00-02-00101-00; LA#GDG-A-00-01-00009-00; Internews Network/RITI dot-Gov Project.

Opiniile exprimate în cadrul acestui document aparțin autorilor şi nu reprezintă în mod necesar vederile Agenției Statelor Unite pentru Dezvoltare Internațională.

© Internews Network, Inc., 2004. Acest ghid poate fi utilizat şi copiat în scop ne-comercial atâta vreme cât “Internews Network, RITI dot-GOV" este creditat ca sursă şi “USAID” menționat ca finanțator.

Capitolul II – Rețele informatice

Sunt puţini utilizatori de calculatoare care nu au folosit niciodată o reţea. Fie pentru a trimite un mesaj, fie pentru a afla o anumită informaţie, din ce în ce mai mulţi oameni folosesc reţelele. Atât pentru persoane, dar mai ales pentru afaceri, în prezent a fi conectat la o reţea înseamnă a putea să comunici.

Calculatoarele pot realiza independent aproape orice, însă este mult mai eficient dacă resursele de care dispun sunt folosite în comun. Atunci când se doreşte ca toate persoanele dintr-un birou să poată tipări documentele pe care le redactează, i se poate cumpăra fiecărei persoane o imprimantă. Este o soluţie, însă cu siguranţă nu cea mai fericită. E mult mai simplu si mai ieftin să se cumpere o singură imprimantă, care se ataşează la un singur calculator şi care să fie folosită în comun de toţi ceilalţi ca şi cum ar fi conectată la calculatorul propriu.

Se poate spune că principalul scop al reţelelor de calculatoare este de a partaja resurse. Aceste resurse sunt foarte diverse, printre ele numărându-se modem-uri, imprimante, spaţii de stocare pentru fişiere, dar şi informaţii cum ar fi cele conţinute în baze de date. Din acest punct de vedere, calculatoarele dintr-o reţea se împart în **servere**, care oferă („servesc") resursele, respectiv **clienţi**, care le folosesc.

O reţea înseamnă mai mult decât două calculatoare legate între ele. Este vorba de echipamente, software şi oamenii care le-au creat. Principiile reţelelor sunt însă suficient de simple. Reţelele, sau *networks* în limba engleză, sunt clasificate în primul rând după întinderea geografică, care poate fi de la câţiva metri la câteva mii de kilometri.

Tipul de reţea cel mai uzual întâlnit este acela din birouri sau universităţi, numit **reţea locală** (**LAN** – *Local Area Network*). Aceasta poate să cuprindă calculatoarele unui departament sau ale unei întregi companii sau instituţii. Suprafaţa uzuală pe care o au astfel de reţele este de ordinul sutelor de metri pătraţi.

Pentru a putea conecta între ele sediile unei companii sau instituţii este necesară acoperirea unor distanţe mult mai mari. Reţelele mai mari, care realizează conectarea echipamentelor aflate la distanţe mari, se numesc **MAN** sau **WAN**, adică *reţele metropolitane* (*Metropolitan Area Network*), respectiv *reţele de mare întindere* (*Wide Area Networks*).

Tehnologia folosită pentru reţelele de calculatoare seamănă întrucâtva cu cea folosită pentru telefonie. Evoluţia tehnicii va face, cel mai probabil, ca într-un viitor apropiat cele două tehnologii să conveargă. Teoretic, telefoanele ar putea fi conectate direct fiecare cu fiecare, însă în practică acest lucru nu se întâmplă niciodată, pentru că ar fi imposibil. În loc să existe câte un cablu de legătură cu fiecare alt abonat, există unul singur, către centrală, aceasta având încapsulată funcţionalitatea de a pune în legătură oricare dintre doi (sau mai mulţi) utilizatori ai săi.

Acest lucru se întâmplă şi în cazul calculatoarelor. Există echipamente care au rolul de "centrale", coordonând grupuri de calculatoare şi fiind clasificate în general după funcţionalitatea pe care o oferă. Printre aceste echipamente se numără *router*-ele, *switch*-urile, *access point*-urile şi *hub*-urile, despre care vom vorbi în paragrafele ce urmează.

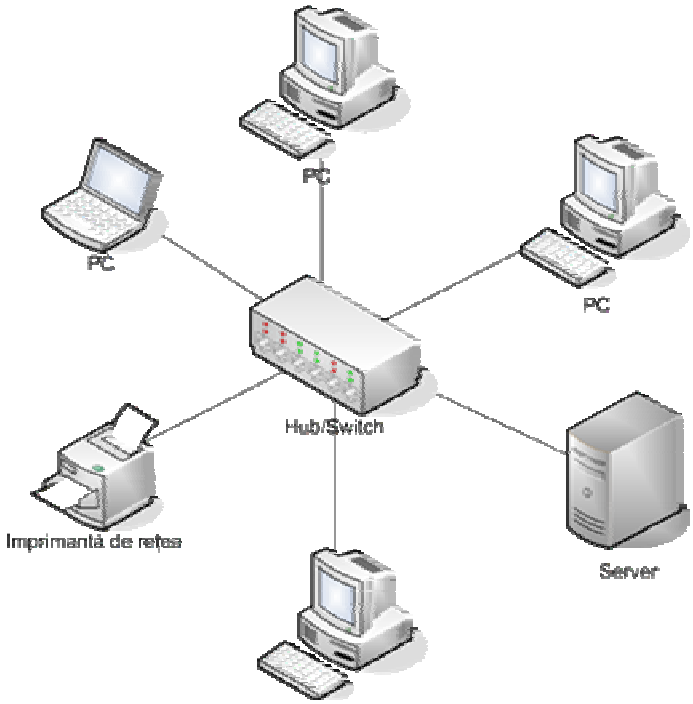
Conectarea la nivelul fizic – mufe, cabluri, etc. – se face în general prin 3 mijloace. Le vom descrie în continuare, împreună cu unele din caracteristicile lor:

A. Cablul de cupru

Este în prezent cel mai folosit mediu de conectare a calculatoarelor şi a echipamentelor de reţea. Printre avantajele sale se numără în primul rând preţul scăzut şi viteza destul de

mare pe care o poate asigura transmisiilor de date. În plus, materialul este suficient de flexibil pentru a fi montat în pereţi şi tras până la orice birou.

De-a lungul ultimelor decenii s-au folosit mai multe tipuri de cablu. În trecut cel mai folosit era cablul coaxial (foarte asemănător cu cel de la antena TV), însă în ultima vreme, standardul *de facto* a devenit cablul torsadat – UTP (*Unshielded Twisted Pairs*). Reţelele care folosesc acest tip de cablu au o arhitectură de *tip stea*, deoarece toate calculatoarele sunt legate la un singur echipament, numit **hub** sau **switch**.



Interceptarea comunicaţiilor prin cablurile de cupru nu prezintă dificultăţi deosebite pentru profesionişti, bazându-se pe aceleaşi principii cu telefonia fixă, necesitând însă acces fizic la cablu. Acest ultim fapt face interceptarea destul de rară, deoarece cablul de cupru este folosit în general în interiorul birourilor unde accesul este lesne controlat.

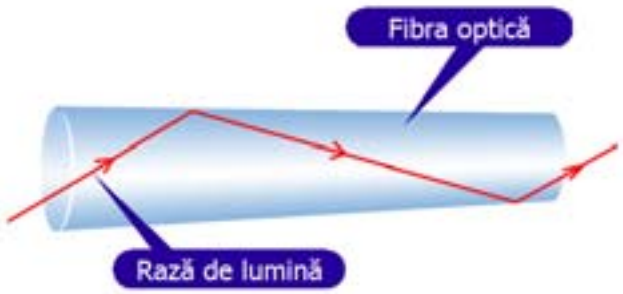
B. Fibra Optică

Este o tehnologie destul de recentă şi permite obţinerea unor capacităţi mult mai mari pentru transmiterea datelor informatice, fiind folosită în general între nodurile importante din reţea sau între reţele.

Fiind încă scumpă şi relativ dificil de manevrat şi conectat, fibra optică nu este folosită pentru conectarea echipamentelor din interiorul LAN-urilor, însă şi-a găsit aplicabilitatea perfectă ca parte a infrastructurilor furnizorilor de servicii, unde cerinţele de performanţă şi securitate sunt mai mari decât cele legate de preţ.

O conexiune pe fibră optică poate avea segmente de până la 4 kilometri, ceea ce reprezintă un alt avantaj faţă de cablurile de cupru care nu au acoperire mai mare de câteva sute de metri. Cablurile UTP si FTP au distanţa de acoperire de până în 100 de metri, distanţa pentru care sunt garantaţi parametrii de funcţionare a reţelei folosind acest tip de conexiune. Se foloseşte şi pe distanţe mai mari, însă garanţia funcţionării optime nu mai există. De asemenea, parametrii conexiunii pot fi dramatic perturbaţi de „zgomotul” pe care cablul îl percepe ca o antenă. Se pot folosi cabluri ecranate coaxiale de 75 ohmi, dar, şi în acest caz se întâlnesc aceleaşi limitări date de atenuarea de-a lungul cablului şi de zgomotul pe care cablul îl poate percepe.

Fibra optică are la bază un "fir", mai subţire decât cel de păr, fabricat dintr-o sticlă foarte pură. Datele sunt transmise sub forma unor impulsuri luminoase (raze de lumină), care se reflectă de pereţii interiori, ajungând ca atare în celălalt capăt.



Transmiterea informaţiilor cu ajutorul luminii

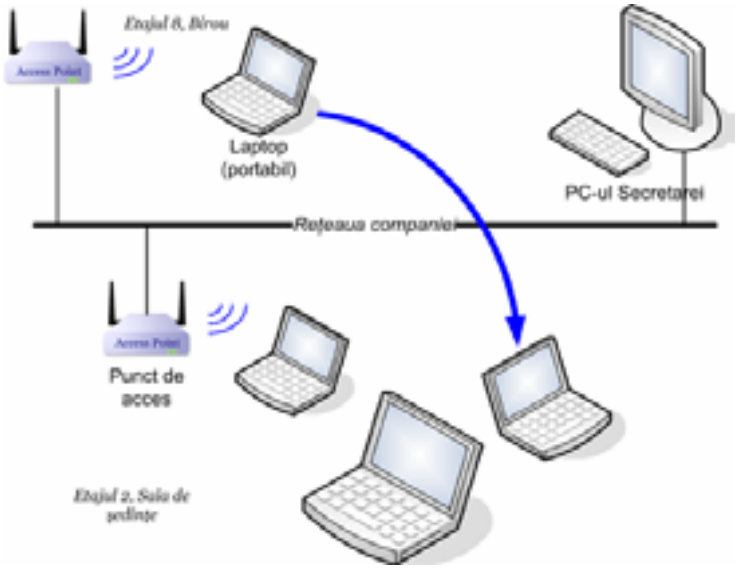
Tehnologia pe care am descris-o mai sus are un avantaj neaşteptat. Fibra optică pe toată lungimea ei nu poate fi interceptată, deoarece nu emite radiaţii electromagnetice (prin ea nu circulă curent electric, ci lumină) şi nu poate fi secţionată (în cazul în care fibra se rupe, comunicaţia se întrerupe în totalitate). Acest aspect o face ideală pentru reţelele (sau segmentele de reţea) în care confidenţialitatea transferului este esenţială. Comunicaţia se întrerupe pe perioada secţionării, dar se poate relua imediat ce ruptura fibrei se remediază, chiar utilizând un adaptor prin care se poate capta traficul prin fibră.

C. Wireless LAN (Reţea fără fir)

Wireless LAN, cunoscut şi sub denumirile de WLAN, 802.11 sau WiFi, deşi este cea mai recentă metodă de conectare, a cunoscut în ultimii ani o creştere fără precedent a popularităţii.

Această popularitate se datorează chiar principalei sale caracteristici: lipsa cablurilor. Calculatorul se află în reţea fără să aibă nevoie de cabluri sau conectori. Este un vis devenit realitate pentru cei care folosesc PC-uri mobile (laptop-uri sau *PDA*-uri) şi care obţin o libertate totală de mişcare în interiorul ariei acoperite de reţeaua fără fir.

Să luăm ca exemplu o firmă obişnuită, care are cabinetul Directorului la etajul 8 şi o Sală de Şedinţe la etajul 2 al unei clădiri de birouri.



Reţea fără fir

Reţeaua fără fir are drept componentă principală un echipament care se numeşte *Punct de Acces*. El este un releu care emite şi recepteaza unde radio către, respectiv de la dispozitivele din raza sa de acţiune.

În exemplul de mai sus am considerat că în reţea sunt două puncte de acces. Unul la etajul 8 al clădirii, în biroul directorului şi celălalt în Sala de Şedinţe de la etajul 2. Directorul poate să meargă la întâlniri luându-şi cu el laptop-ul şi deşi nu este în biroul său, poate să ceară informaţii secretarei sau poate să îşi cerceteze poşta electronică pentru a fi la curent cu ultimele noutăţi, toate acestea fără să conecteze vreun cablu.

Există însă şi un revers al medaliei în cazul reţelelor fără fir. Pe lângă cea mai uşoară utilizare şi cea mai mare flexibilitate, o reţea fără fir este totodată şi cea mai expusă din punct de vedere al vulnerabilităţii la interceptări neautorizate.

La nivelul fizic, oricine poate să acceseze o reţea fără fir. Nu este nevoie să tai cabluri, pentru că mediul de propagare al datelor este aerul. Ele pot trece prin ferestre, la fel de bine cum pot trece si prin pereţii subţiri din birourile obişnuite. Din fericire, nu este suficient în general sa ai acces la nivelul fizic pentru a obţine şi accesul efectiv la reţea, deoarece producătorii echipamentelor de comunicaţii au conceput modalităţi de criptare a informaţiilor, care să le facă inaccesibile intruşilor. Securitatea reţelelor *wireless* este un punct de discuţie foarte aprins, deoarece din motive de necunoştinţă a utilizatorilor sau de neprofesionalism al administratorilor, ori pentru a permite conectarea uşoară, aceste caracteristici de protecţie nu sunt întotdeauna activate.

Viitorul aparţine probabil unei combinaţii a tehnologiilor prezentate mai sus, la care se vor mai adăuga şi caracteristici venite din lumea telefoniei mobile.

Internet şi Intranet

Calculatoarele sunt, după cum am văzut, conectate în cadrul reţelele locale, metropolitane sau de mare întindere. La rândul lor, reţelele sunt legate între ele în ceea ce se numeşte **Internet**.

Internetul este o reţea globală de calculatoare. Orice calculator conectat la Internet poate să comunice cu orice alt calculator legat la Internet. Se poate face analogie cu reţeaua de străzi care permite unui autoturism ca plecând dintr-o localitate să ajungă în orice altă localitate. Sunt străzi mai mici sau mai mari, iar ruta folosită nu este neapărat cea directă.

Internetul este o reţea descentralizată, în sensul că nu există o instituţie sau un stat care să îl deţină sau să îi guverneze funcţionarea. Susţinerea financiară şi logistică se realizează de către companiile care îl accesează, iar administrarea sa este supravegheată de un comitet numit *ICANN (Internet Corporation For Assigned Names and Numbers)*.

Datorită faptului că oricine din lume se poate conecta la Internet fără restricţii, acesta este considerat ca fiind public. Ca orice entitate deschisă accesului public, prezenţa pe Internet implică un risc considerabil, atât pentru persoane, cât mai ales pentru companii. Fiind un spaţiu deschis, Internetul permite şi persoanelor sau organizaţiilor rău intenţionate să cauzeze daune celorlalţi membri mai mult decât orice altă reţea.

În contextul în care informaţia a devenit foarte valoroasă, tentaţiile de fraudare a sistemelor care o conţin au devenit din ce în ce mai mari. Având ca motiv fie interese financiare, fie pur si simplu distracţia, infracţionalitatea şi-a găsit un loc bun şi în reţelele de calculatoare.

Pentru a permite companiilor să se protejeze de ameninţările venite din Internet, putând totodată să folosească avantajele care îl fac atât de popular, se foloseşte o arhitectură care

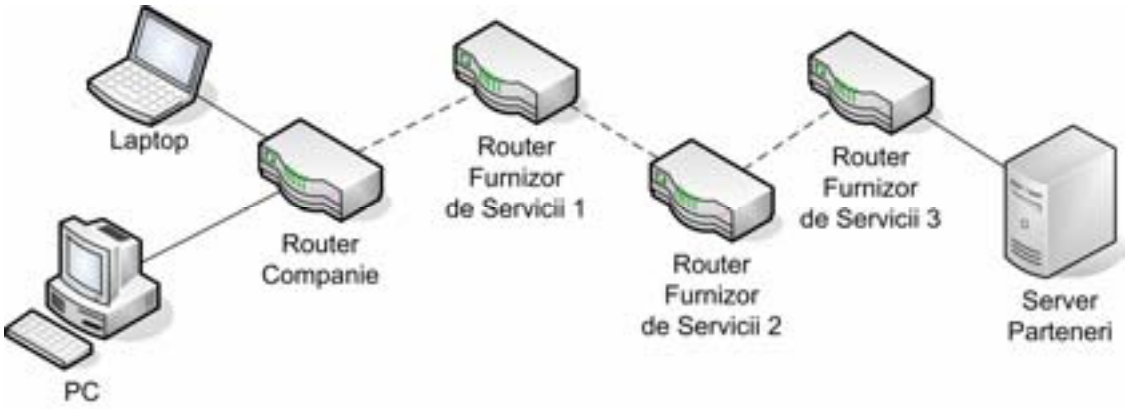
poartă numele de **Intranet**. Intranetul este o reţea privată (spre deosebire de Internet care este publică) din interiorul unei firme sau instituţii. Calculatoarele din interiorul Intranetului nu sunt accesibile din exterior, însă pot accesa atât resursele interne cât şi resursele oferite de serverele din Internet. Acest lucru este posibil cu ajutorul unui dispozitiv numit **firewall** (nu există o traducere exactă în limba română, în unele lucrări este menţionat cu termenul de *parafoc*). Acesta este de fapt un filtru care permite conexiunile doar într-un singur sens, interior către exterior. O analogie destul de bună pentru un *firewall* este centrala telefonică privată, PBX, întâlnită la majoritatea firmelor cu mai mult de două birouri. Un *firewall* nu închide complet accesul din exterior decât dacă este programat să facă acest lucru; conexiunile prin *firewall* sunt bidirecţionale. Un *firewall* nu blochează, în mod curent, decât acele conexiuni neautorizate din exterior, lăsând utilizatorii Intranet să acceseze resurse atât din Intranet cât şi din Internet. Utilizatorii din afara Intranetului nu pot accesa decât acele informaţii la care *firewall*-ul permite accesul şi pentru care este configurat sa le pună la dispoziţie.

La fel ca şi telefoanele, calculatoare folosesc numere pentru a fi identificate. Acestea sunt organizate în patru grupuri de cifre, despărţite de semnul „ . ” (punct), numite **adrese IP**. Spre exemplu *193.230.122.12* este adresa unui server din Ministerul de Interne. Calculatoarelor dintr-o reţea le sunt alocate grupuri consecutive de câte 256, 128, 64, 32, 16, 8 sau 4 adrese, în funcţie de numărul echipamentelor care trebuie conectate. Un tip special de adrese IP îl reprezintă **adresele private**. Acestea sunt similare numerelor de interior din centralele PBX de care am vorbit mai sus.

Adresele private se recunosc uşor datorită faptului ca au o formă standard, adică 10.xxx.xxx.xxx, 172.16.xxx.xxx, respectiv 192.168.x.x. Aceste adrese sunt folosite doar pentru calculatoarele din Intranet-uri.

Legătura între două reţele se face folosind un **router**. Acesta are câte o conexiune corespunzătoare fiecărei reţele din care face parte. În general, *router*-ul poate să fie un echipament dedicat, însă şi un PC obişnuit poate deservi acest rol.

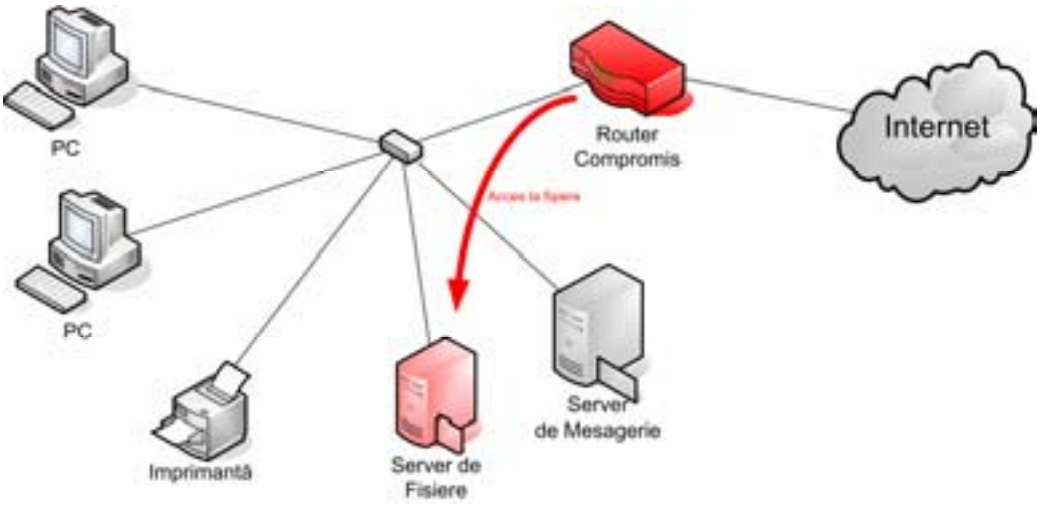
Router-ul are rolul unui dispecer, care decide cărei reţele îi este destinată o informaţie pe care o primeşte, având în plus de multe ori rolul de *firewall*. Este cel mai răspândit echipament al Internetului, după PC, fiind punctul de intrare, respectiv de ieşire al informaţiilor dintre reţele. Este un fapt uzual ca între două calculatoare din Internet să fie mai multe *router*-e (pot fi chiar câteva zeci) care sunt tranzitate.



Informaţiile primite de către utilizatorul PC-ului de la server-ul partenerilor tranzitează mai multe routere

Datorită acestui rol important pe care îl are, *router*-ul este cel mai delicat echipament al reţelelor. Fiind echipamentul prin care sunt tranzitate atât de multe informaţii, compromiterea lui este echivalentă cu accesul, de obicei neautorizat, la toate aceste

informaţii. În momentul în care controlezi accesul spre *router*-ul prin care o firmă se conectează la Internet, nu numai că ai acces la toate mesajele pe care firma le transmite partenerilor săi, dar obţii de asemenea o poartă deschisă către interiorul protejat al rețelei.



Atunci când o persoană compromite router-ul unei rețele, este foarte probabil să obțină controlul şi asupra altor resurse