VULNERABILITATEA SISTEMELOR ÎN CONTEXTUL INTERNET

dr. Vasile Baltac

Calea Floreasca Nr. 167, 72321 - Bucureşti, România
e-mail: Vasile.Baltac@softnet.ro

Rezumat: Internet este, în devenire, cel mai mare sistem creat de om, un fenomen global şi care accentuează globalizarea. Volumul de informaţie stocată şi accesibilă pe Internet creşte cu repeziciune. Aparent, rutările în acest ocean de informaţie ar apare dispersate. Cercetări recente arată, totuşi, că se manifestă o concentrare a conectivităţii, că există caracteristici independente de scară şi de autoorganizare. Ansamblul Internet fiind un sistem de sisteme care creşte rapid şi cu o infrastructură destul de puţin fiabilă cuprinde numeroase elemente de vulnerabilitate, care au generat preocupări pentru studierea acestora.
Elementele de vulnerabilitate pot fi evidenţiate la nivel de micro- şi macrosistem. La nivel de microsistem, complexitatea fiind suficient de mică, vulnerabilitatea este controlabilă. Vulnerabilitatea Internet la nivel macro este o consecinţă a arhitecturii sale ca reţea de elemente vulnerabile şi a perturbărilor induse prin incidente. Creşterea incidentelor este exponenţială. Principalul element actual de vulnerabilitate au devenit atacurile. Dezvoltarea afacerilor electronice de tip e-Business a introdus un nou nivel necesar de securitate, mult mai ridicat.
Din punct de vedere tehnic, viteza de creştere şi mai ales timpul scurt nu au permis contracararea eficientă a influenţei factorului uman în sporirea vulnerabilităţii Internet. Se pune justificat întrebarea dacă *studiul organizării societăţii umane nu este o sursă de soluţii pentru scăderea vulnerabilităţii?* Astfel de soluţii pot fi găsite prin analogia cu societatea umană. Aceasta a fost şi ea confruntată, încă din fazele incipiente, cu problema vulnerabilităţii. Soluţiile găsite au fost diverse, de la construcţii şi comunităţi fortificate la folosirea de sisteme de alarmare eficiente. Nu mai este de mult o dilemă să decizi dacă se pun uşi blindate la toate casele sau dacă se folosesc forţe de ordine eficiente. Societatea umană a optat de timpuriu pentru o organizare prin legi şi reguli şi instituţii de aplicare a acestora. *Lumea Internet va trebui să evolueze de la absenţa reglementării la reglementări naţionale şi globale.* Reglementările pot reduce vulnerabilitatea cu costuri mai mici decât măsurile tehnice. Lumea Internet poate deveni globală, democratică şi sigură şi prin măsuri tehnice, dar ,mai ales, prin reglementări naţionale şi globale.

Cuvinte cheie: Internet, vulnerabilitate, securitate sistem, reglementări.

Fenomenul Internet

Reţeaua de reţele Internet este în devenire cel mai mare sistem creat de om. Cu zeci de milioane servere, sute de milioane de utilizatori şi cu un trafic de date ce va depăşi traficul de voce în SUA încă din 2002, se poate vorbi de Internet ca un fenomen care reflectă în plan ştiinţific, tehnic şi comercial, evoluţia societăţii umane la sfârşitul secolului XX, începutul secolului XXI.

Este de remarcat că, în sistemul de telecomunicaţii mondial, s-a ajuns la o densitate de linii telefonice de 17% după peste 160 ani de evoluţie, în timp ce, numai după 20 ani, densitatea globală a utilizatorilor Internet este de 7%.

Se poate, deci, vorbi fără îndoială de Internet ca despre un fenomen global şi care accentuează globalizarea. Există numai accidental pete albe pe harta din figura 1 care arată răspândirea mondială a tehnologiilor informaţiei, comunicaţiilor şi Internet [1], pete albe care se datorează, în principal, unor considerente de natură politică şi socială, şi nu unor dificultăţi de natură tehnică [2], [3].

Cercetările privind Internet

Cu toată evoluţia rapidă a Internet, s-au abordat numeroase teme de cercetare, care se referă nu numai la noi tehnologii, soluţii arhitecturale, standarde şi interacţiune cu şi intrasistem(e), ci şi lucrări care se referă la aspecte vitale pentru viitorul Internet, în principal, topologii, stăpânirea complexităţii şi vulnerabilitate.

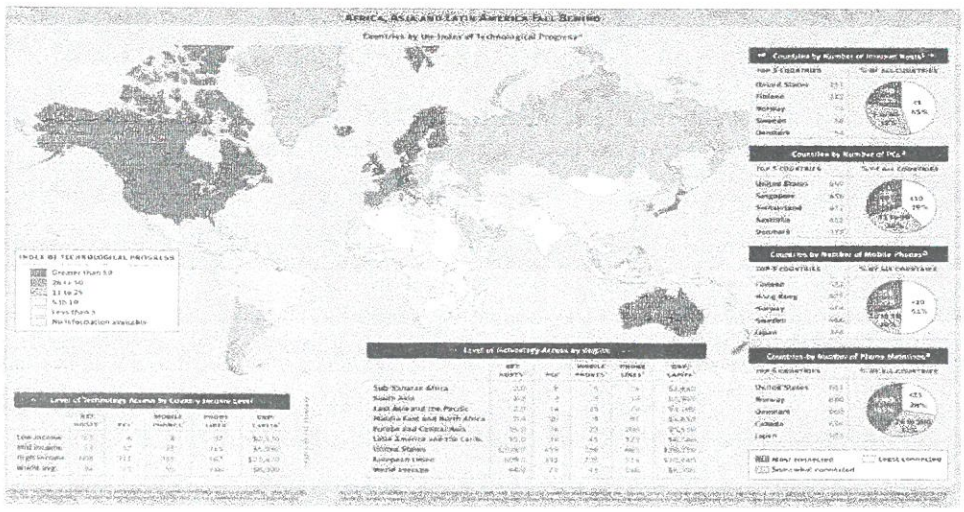

Figura 1. Ţările lumii şi dezvoltarea tehnologiilor Internet

Volumul de informaţie în Internet

Volumul de informaţie stocată şi accesibilă pe Internet creşte cu repeziciune. După calcule ale autorului, aceasta ar putea fi estimată la 10^{16}-10^{17} bytes. Din informaţie, circa 50% este în mişcare, din care 40% local şi 10% la distanţă în reţele de arie largă.

Aparent, rutările în acest ocean de informaţie ar fi dispersate. Cercetări recente arată, totuşi, că se manifestă o concentrare a conectivităţii. Centrul CAIDA de la University of California at San Diego a demonstrat o concentrare a conectivităţii providerilor Internet. Graficul experimental din figura 2 [4] reflectă orientarea spre alţi provideri a peste un milion de legături (*link-uri*) din sute de mii de adrese IP. Una din explicaţii este concentrarea în SUA a celor mai mari provideri, dar fenomenul va persista din motive legate de costurile realizării unor depozite de informaţie ce previn o fărâmiţare excesivă a acestora.

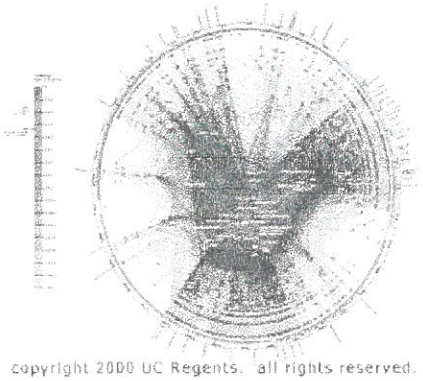

Figura 2. Concentrarea conectivităţii

Topologia Internet

Nodurile Internet nu sunt decât elemente de legătură între emiţătorii şi receptorii de informaţie. Probabilitatea ca un nod să fie legat cu k alte noduri este dată de o lege exponenţială

$$P(k) = \sim k^{-\lambda}$$

unde λ este aproximat la valoarea de 3.

Cercetări privind topologia Internet arată că, în aparenta dezordine din Internet, există astfel de caracteristici independente de scară şi de autoorganizare. Astfel, Barabasi ş.a. [5] demonstrează că diametrul *www*, definit ca fiind distanţa medie cea mai scurtă dintre două site-uri, nu era în anul 2000 mai mare de 19 legături. Din cauza dependenţei logaritmice de volumul Internet, chiar la o creştere de 1000% a *www* numărul de legături nu va creşte peste 21.

Legea lui Zipf

Descoperită pentru oraşe în 1949, legea lui Zipf arată că dimensiunea unui eveniment depinde de rangul său conform relaţiei:

$$P(r) = K * r^{-q}$$

unde r este rangul evenimentului, P este dimensiunea sa şi K este o constantă.

Valoarea lui q a fost determinată ca fiind 0,93.

Legea lui Zipf a fost demonstrată pentru corelaţia GDP cu dimensiunea *www* pentru o anumită ţară sau regiune [6] (figura 3).

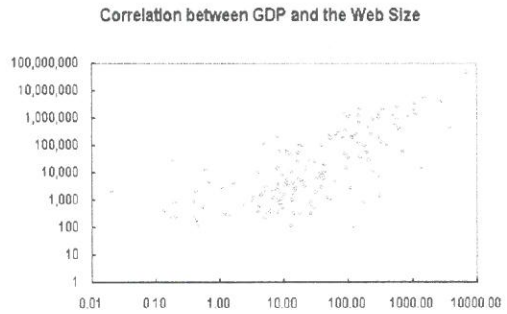

Figura 3
Corelaţia între PIB şi dimensiunile *www*

Preocupări pentru studiul vulnerabilităţii

Un sistem de tip Internet este vulnerabil. Ansamblul Internet este un sistem de sisteme, care creşte rapid şi cu o infrastructură destul de puţin fiabilă, în care există numeroase elemente de vulnerabilitate, care au generat preocupări pentru studierea acestora.

Vom evidenţia câteva dintre elementele de vulnerabilitate.

Elemente de vulnerabilitate

Vulnerabilitatea sistemelor Internet este mai mare decât cea a sistemelor care le-au precedat. Afirmaţia se justifică, în primul rând, deoarece volumul informaţiei este mult mai mare decât la celelalte sisteme. În al doilea rând, creşterea Internet a fost rapidă şi fără a fi însoţită de preocupări deosebite pentru asigurarea unei limitări a vulnerabilităţii. Important părea la un moment dat să fii prezent în Internet şi mai puţin să te asiguri.

În afara vulnerabilității clasice, în Internet a apărut atacul informatic ca element provocat sau declanșat întâmplător. Primul incident a avut loc în 1988 și anume așa numitul Morris Worm [7]. A urmat o creștere exponențială a incidentelor de acest tip și, ulterior, și a unei diversități de alte tipuri.

Este cunoscut că informația poate fi pierdută, furată, modificată, folosită necorespunzător și decriptată ilegal. Este posibilă pierderea integrității, confidențialității și a disponibilității datelor.

Elementele de vulnerabilitate pot fi evidențiate la nivel de micro- și macrosistem.

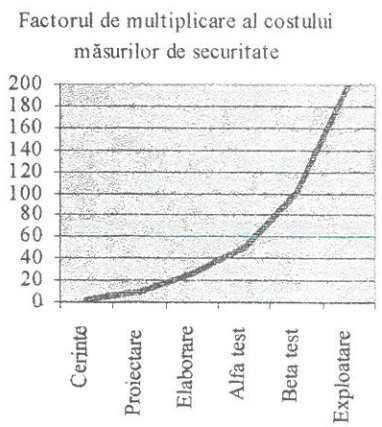

Figura 4

Elemente de vulnerabilitate la nivel de microsistem

Complexitatea fiind suficient de mică, vulnerabilitatea este controlabilă la nivel de microsistem. Sursele de risc sunt echipamentele, software-ul și bazele de date.

În cazul echipamentelor, principalii factori de vulnerabilitate, în afara problemelor normale generate de fiabilitatea intrinsecă a componentelor sistemului, sunt dezastrele naturale (furtuni, inundații, cutremure etc.), căderile sau întreruperile de alimentare cu energie și actele de vandalism.

În software, aplicații și date putem evidenția factorii furt, alterare/distrugere de date, virușii informatici și accidentele neintenționate.

Diminuarea vulnerabilității la nivel de microsistem se poate face prin măsuri de control al accesului și creșterea robusteței programelor. Toate acestea se fac cu un anumit cost care este cu atât mai mic, cu cât măsurile sunt luate mai din timp, în fazele de proiectare și de realizare a sistemului, așa cum se prezintă în figura 4.

Metode de creștere a securității

Există numeroase metode de reducere a vulnerabilității microsistemelor prin proiectare cu elemente de securitate, separarea funcțiilor, controale de rețea, criptare și creare de firewall-uri.

În bună măsură, folosirea acestor metode contribuie la creșterea rezistenței sistemelor la perturbații și atacuri.

Planuri de recuperare a daunelor

Problemele de vulnerabilitate fiind imposibil de eliminat, apare ca necesară adoptarea de planuri de recuperare a daunelor. Aceste planuri se pot dovedi extrem de eficace atunci când, din motive diverse, au loc căderi sau atacuri asupra sistemelor.

Din păcate, asemenea planuri se întocmesc foarte rar.

Costul măsurilor de securitate

Elementele rețelelor ce compun Internet-ul la nivel de microsistem sunt nesigure și vulnerabile. Costul măsurilor de securitate apare, de regulă, mare pentru beneficiarii sistemelor și chiar este mare în funcție de nivelul de securitate dorit, așa cum este ilustrat în figura 6.

Costul daunelor potențiale descrește, însă, funcție de nivelul de securitate. El poate fi exprimat prin formula:

$$C_t = \Sigma\ (C_1xP_1 + C_2xP_2 + ... + C_nxP_n)$$

unde Ct este costul daunelor potențiale, Ci costul și P_i probabilitatea de apariție a daunei i.

Un optim economic poate fi găsit prin calcularea costului combinat al asigurării securității microsistemului, conform celor reprezentate în figura 6.

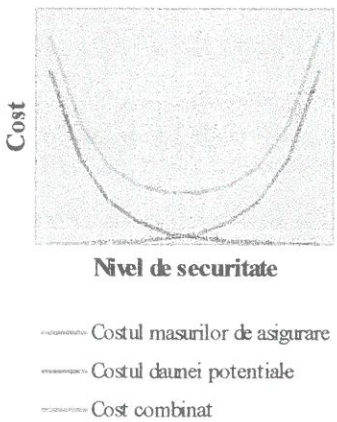

Figura 6 Costul măsurilor de securitate

Elemente de vulnerabilitate la nivelul canalelor de comunicație

Rețeaua Internet s-a dezvoltat, în principal, pe rețelele de comunicație existente. Canalele de comunicații tradiționale de dovedesc a fi cea mai vulnerabilă componentă a Internet. Fiabilitatea redusă este accentuată și de protocoalele nesigure de schimb de informație. În tabelul 1, se prezintă o comparație a diverselor medii folosite în rețelele de comunicații, inclusiv pentru Internet, din punct de vedere al capacității, vulnerabilității la perturbații electromagnetice și disponibilității.

Tabelul 1. Comparație a mediilor de comunicații

Mediu	Capacitate	Vulnerabilitate la interferență electromagnetică	Cost comparativ	Disponibilitate globală
Fire	mică	mare	mic	generală
Cablu coaxial	medie	mică	mediu	slabă
Microunde	mare	mică	mare	mare
Cablu optic	mare	zero	mare	limitată

Elemente de vulnerabilitate la nivel de macrosistem

Vulnerabilitatea Internet la nivel macro este o consecință a arhitecturii sale ca rețea de elemente vulnerabile la nivel microsistem și a perturbărilor prin incidente. Sursele de incidente sunt atacuri involuntare sau provocate.

Sunt cunoscute tipurile clasice de incidente: încercări, scanare, compromitere cont utilizator, compromitere rădăcină, captura de date din pachete, blocarea serviciului, înșelăciune, folosirea de coduri maligne, atacuri asupra infrastructurii.

Creșterea incidentelor este exponențială. Este adevărat că sistemele se caracterizează intrinsec prin robustețe [7]. În multe situații, funcționarea parțială reduce vulnerabilitatea.

Principalul element actual de vulnerabilitate au devenit atacurile. Numai în SUA, în anul 2000, s-au cheltuit 337 mil. $ pentru repararea daunelor produse de atacuri.

Factorii favorizanți ai acestui tip de vulnerabilitate sunt nodurile nesigure și folosirea comunicației necriptate. Este adevărat că, în fazele primare ale dezvoltării Internet, nu au existat aplicații majore, care să ceară vulnerabilitate redusă. Creșterea a fost rapidă, fără măsuri de securitate deosebite. Personalul de exploatare era și el insuficient instruit.

Dezvoltarea afacerilor electronice de tip e-Business a introdus un nou nivel necesar de securitate, mult mai ridicat. Criptarea a devenit instrumentul folosit de sute de milioane de utilizatori față de un număr restrâns în era pre-Internet.

Din punct de vedere tehnic viteza de creștere și, mai ales, timpul scurt nu au permis contracararea eficientă a influenței factorului uman în sporirea vulnerabilității Internet.

Interacțiunea umană în Internet ca factor de vulnerabilitate

Sistemele fără oameni se comportă diferit față de sistemele cu interacțiune umană puternică. În Internet, sunt peste 50 de milioane de servere și 410 milioane de oameni. Acțiunea umană devine, astfel, factorul principal de vulnerabilitate. Dimensiunea Internet devine comparabilă din punct de vedere al complexității interacțiunilor cu colectivitățile umane.

Se pune justificat întrebarea dacă *studiul organizării societății umane nu este o sursă de soluții pentru scăderea vulnerabilității ?*

Vulnerabilitatea societății umane este și ea foarte mare. Societatea reprezentată ca sistem are în noduri oamenii care sunt extrem de nefiabili. Societatea umană are multe asemănări cu sistemele din Internet și anume multă redundanță, comunicare vulnerabilă și vulnerabilitate a informației stocate în creștere în timp.

Globalizarea intensifică forța atacurilor și asupra societății, la fel cum, în mod pregnant, se manifestă și în Internet.

Un punct de vedere privind reducerea vulnerabilității sistemelor în contextul Internet

Este un fenomen necontestat că vulnerabilitatea sistemelor în contextul Internet este mare și în creștere. Soluții tehnice există, sunt însă scumpe, greu de generalizat și vor avea succes limitat.

Soluții pot fi, însă, găsite prin analogia cu societatea umană. Societatea a fost confruntată încă din fazele incipiente cu problema vulnerabilității ei. Soluțiile găsite au fost diverse, de la construcții și comunități fortificate la folosirea de sisteme de alarmare eficiente.

Nu este o dilemă să decizi dacă se pun uși blindate la toate casele dintr-o comunitate sau se folosesc forțe de ordine eficiente. Societatea umană a optat de timpuriu pentru o organizare prin legi și reguli și instituții de aplicare a acestora.

Lumea Internet va trebui să evolueze de la absența reglementării, la reglementări naționale și globale.

Reglementările pot reduce vulnerabilitatea cu costuri mai mici decât măsurile tehnice. Lumea Internet poate deveni globală, democratică și sigură și prin măsuri tehnice și prin reglementări internaționale.

Opozanții unei asemenea abordări pot invoca spiritul de liberă inițiativă (free enterprise), care a contribuit mult la creșterea Internet și piedicile pe care reglementările le-ar putea pune dezvoltării în continuare.

Trecerea la utilizarea Internet în ample aplicații economice, de învățământ, culturale, de administrație publică face ca ignorarea problematicii vulnerabilității să devină un factor de frânare chiar mai mare decât acela al unor reglementări insuficient fundamentate.

Prin caracterul său global, fenomenul Internet cere reglementări globale transfrontaliere.

Bibliografie

1. *** Nua Internet Surveys, How many on-line, http://www.nua.net
2. **COFFMAN, K. G., A.M. ODLYSKO**: The Size and Growth Rate of the Internet, FirstMonday Peer-Reviewed Jounal on the Internet, http://www.firstmonday.dk
3. *** Digital Planet 2000, The Global Information Economy, WITSA, November 2000.
4. *** CAIDA, Visualizing Internet Topologies at a Macroscopic Scale, http://www.caida.org/analysis/topology/as_core_network/
5. **BARABASI A. L.** e.a.: Scale free characteristics of random networks: the topology of the world-wide web, Physica A, Elsevier Science B.V., 2000.
6. **SHIODE, N.** e.a.: Power Law Distributions in Real and Virtual Worlds, Inet 2000 Proceedings, Internet Society, http://www.isoc.org/inet2000.
7. *** Carnegie Melon Software Engineering Institute, Security of the Internet, Froehlich/Kent Encyclopedia of Telecommunications, vol. 15.
8. **REKA A.** e.a.: The Internet Achilles' Heel: Error and attack tolerance of complex networks, Physica A, Elsevier Science B.V., 2000.