

Vulnerabilitatea sistemelor în contextul Internet

*Vasile Baltac**

VULNERABILITY OF SYSTEMS IN INTERNET RELATIONSHIP. Internet becomes the largest man-made system, a global event with direct implication on globalization. The information content of Internet rapidly grows. Despite of the fact that routings, apparently chaotic, show a certain degree of connectivity and some self-organizing features, numerous elements of vulnerability are present. The paper reviews some of the research directions in Internet studies and an approach to reduce vulnerability is proposed.

At Internet micro level vulnerability is mainly under control as the complexity is not too big. Vulnerability at macro level results from the architecture of Internet as a network of unreliable elements and from induced incidents. The latter grow exponentially and the attacks are in the forefront of vulnerability. The eBusiness development brought the necessity of a much higher level of security.

The quick development of Internet has not allowed countering the human factor in vulnerability. This is why the paper raises the question on *the study of human society as a source of solutions for vulnerability control*. Solutions may be found by analogy with human society confronted itself from the early stages with vulnerability. Various solutions have been found from fortified constructions to sophisticated alarm systems. But to the alternative to safe-proof every house the society opted for laws and law enforcement at community level. This is why the author considers that *the Internet has to go from almost an absence of regulations to local and global laws*. Regulations could reduce vulnerability at much lesser costs than the technical solutions. The Internet world will become global, democratic a safe through both technical approach and national and international laws.

The summary of the paper: The Internet phenomenon; Research studies on Internet; Elements of vulnerability; Human interaction as vulnerability element (**Abstract**)

World Wide Web: acest articol poate fi găsit pe web la <http://www.softnet.ro/vb/papers>

Cuprins

- Fenomenul Internet
- Cercetările privind Internet
 - Volumul de informație în Internet
 - Topologia Internet
 - Legea lui Zipf
 - Preocupări pentru studiul vulnerabilității
- Elemente de vulnerabilitate
 - Elemente de vulnerabilitate la nivel microsistem
 - Metode de creștere a securității
 - Planuri de recuperare a daunelor
 - Costul măsurilor de securitate
 - Elemente de vulnerabilitate la nivel canale de comunicație

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

Elemente de vulnerabilitate la nivel macrosistem
 Interacțiunea umană în Internet ca factor de vulnerabilitate
 Un punct de vedere privind reducerea vulnerabilității sistemelor în contextul Internet
 Bibliografie

1. Fenomenul Internet

Rețeaua de rețele Internet este în devenire cel mai mare sistem creat de om. Cu zeci de milioane servere, sute de milioane de utilizatori și cu un trafic de date ce va depăși traficul de voce în SUA încă din 2002 se poate vorbi de Internet ca un fenomen care reflectă în plan științific, tehnic și comercial evoluția societății umane la sfârșitul secolului XX, începutul secolului XXI.

Este de remarcat că în sistemul de telecomunicații mondial s-a ajuns la o densitate de linii telefonice de 17% după peste 160 ani de evoluție, 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 și care accentuează globalizarea. Există numai accidentale pete albe pe harta din figura 1 care arată răspândirea mondială a tehnologiilor informației, comunicațiilor și Internet (Nua /1/), pete albe care se datorează în principal unor considerente de natură politică și socială și nu unor dificultăți de natură tehnică (Coffman /2/, Digital Planet /3/).

2. Cercetările privind Internet

Cu toată evoluția rapidă a Internet s-au abordat numeroase teme de cercetare care se referă nu numai la noi tehnologii, soluții arhitecturale, standarde și interacțiuni cu și intra sistem(e), ci și lucrări care se referă la aspecte vitale pentru viitorul Internet, în principal topologii, stăpânirea complexității și vulnerabilitate.

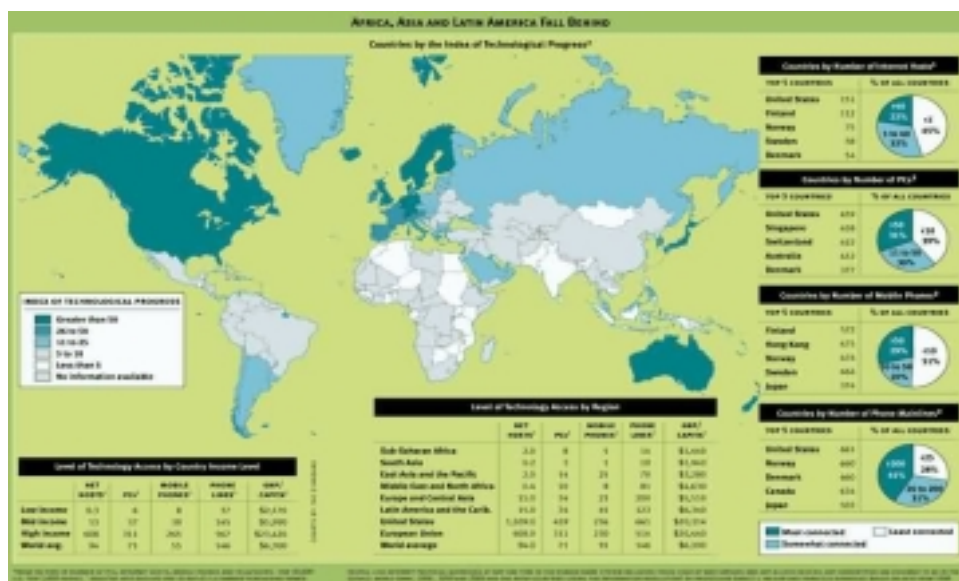


Figura 1 Țările lumii și dezvoltarea tehnologiilor Internet

2.1. Volumul de informație în Internet

Volumul de informație stocată și accesibilă pe Internet crește cu repeziciune. După calcule ale autorului aceasta ar putea fi estimată la 10^{16} - 10^{17} bytes. Din informație circa 50% este în mișcare, din care 40% local și 10% la distanță în rețele de arie largă. Aparent rutările în acest ocean de informație ar apare dispersate. Cercetări recente arată totuși că se manifestă o concentrare a conectivității. Centrul CAIDA de la University of California at San Diego a demonstrat o concentrare a conectivității providerilor Internet. Graficul experimental din figura 2 (Caida /4/) reflectă orientarea spre alți provideri a peste un milion de legături (*linkuri*) din sute de mii de adrese IP. Una din explicații este concentrarea în SUA celor mai mari provideri, dar fenomenul va persista din motive legate de costurile realizării unor depozite de informație ce previn o fărâmițare excesivă a acestora.

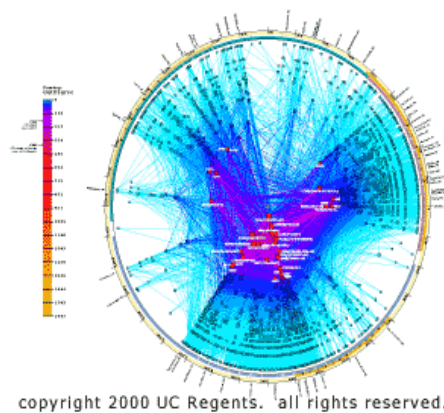


Figura 2. Concentrarea conectivității

2.2. Topologia Internet

Nodurile Internet nu sunt decât elemente de legătură între emițătorii și receptorii de informație. Probabilitatea ca un nod să fie legat cu k alte noduri este dată de o lege exponențială

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

unde λ este aproximat la valoarea de 3.

Cercetări privind topologia Internet arată că în aparenta dezordine din Internet există astfel caracteristici independente de scară și de autoorganizare. Astfel Barabasi s.a. /5/ demonstrează că diametrul www , definit ca distanța medie cea mai scurtă dintre două situri, nu era în anul 2000 mai mare de 19 legături. Din cauza dependenței logaritmice de volumul Internet, chiar la o creștere de 1000% a www numărul de legături nu va crește peste 21.

2.3. Legea lui Zipf

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

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

unde r este rangul evenimentului, P este dimensiunea sa și K este o constantă. Valoarea lui q a fost determinată ca 0,93

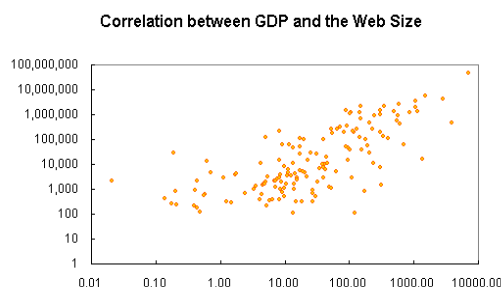


Figura 3

Legea lui Zipf a fost demonstrată pentru corelația GDP cu dimensiunea www pentru o anumită țară sau regiune (Shiode /6/ - figura 3).

2.4. Preocupări pentru studiul vulnerabilității

Un sistem de tip Internet este vulnerabil. Ansamblul Internet fiind un sistem de sisteme care crește rapid și cu o infrastructură destul de puțin fiabilă există numeroase elemente de vulnerabilitate care au generat preocupări pentru studierea acestora.

Vom evidenția câteva dintre elementele de vulnerabilitate.

3. Elemente de vulnerabilitate

Vulnerabilitatea sistemelor Internet este mai mare decât cea a sistemelor care le-au precedat. Afirmația se justifică în primul rând deoarece volumul informației este mult mai mare decât la celelalte sisteme. În al doilea rând creșterea Internet a fost rapidă și fără a fi însoțită de preocupări deosebite pentru asigurarea unei limitări a vulnerabilității. Important părea la un moment dat să fi prezent în Internet și mai puțin să te asiguri.

În afara vulnerabilității clasice în Internet a apărut atacul informatic ca element provocat sau declanșat întâmplător. Primul incident în 1988 și anume așa numitul Morris Worm (CMS /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 disponibilității datelor.

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

*Vulnerabilitatea Internet este de 100%,
nefiind posibil să se conceapă un sistem total nevulnerabil.*

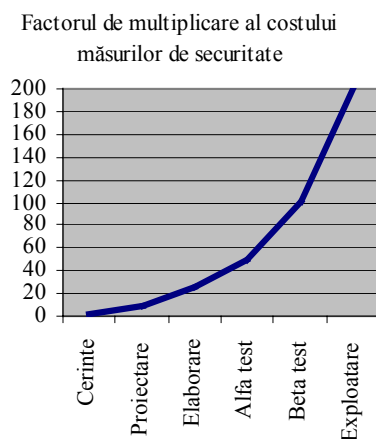


Figura 4

3.1 Elemente de vulnerabilitate la nivel 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, virusii informatici și accidentele neintenționate.

Diminuarea vulnerabilității la nivel microsistem se poate face prin măsuri de control al accesului și creșterea robusteții 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 realizare a sistemului așa cum se prezintă în figura 4.

3.1.1 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 la perturbații și atacuri a sistemelor.

3.1.2 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 eficiente atunci când din motive diverse au loc căderi sau atacuri asupra sistemelor.

Din păcate, asemenea planuri se întocmesc foarte rar

3.1.3 Costul măsurilor de securitate

Elementele rețelelor ce compun Internet 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 5.

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

$$C_t = \sum (C_1 \times P_1 + C_2 \times P_2 + \dots + C_n \times P_n)$$

unde C_t este costul daunelor potențiale, C_i 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 5.

3.1.4 Elemente de vulnerabilitate la nivel canale de comunicație

Rețeaua Internet s-a dezvoltat în principal pe rețelele de comunicație existente. Canalele de comunicații tradiționale de dovedesc 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.

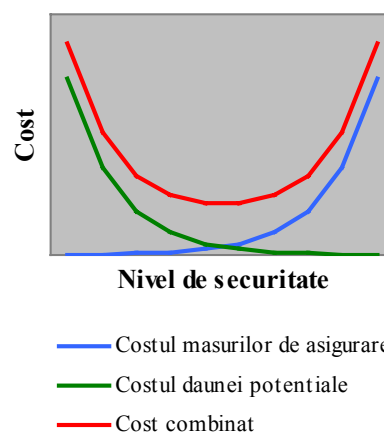


Figura 5 Costul măsurilor de securitate

3.2 Elemente de vulnerabilitate la nivel macrosistem

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

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 (Reka /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 eBusiness 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 eficienței a influenței factorului uman în sporirea vulnerabilității Internet.

4. Interacțiunea umană în Internet ca factor de vulnerabilitate

Sisteme fără oameni se comportă diferit față de sistemele cu interacțiune umană puternică. În Internet sunt peste 50 milioane servere și 410 milioane 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 nefiabli. 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.

4.1. 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. Soluții 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.

Referințe bibliografice

- [1] Nua Internet Surveys, How many on-line, <http://www.nua.net>.
- [2] Coffman, K. G., Odlysko, A.M. The Size and Growth Rate of the Internet, FirstMonday Peer-Reviewed Journal 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.