

Despre importanța tehnologiilor de securitate a informației

Lucian Vasiu

Concepte cheie: Societatea Informației; Economia Internet; tehnologiile de securitate a informației; confidențialitate, integritate și disponibilitate a informației.

1. Obiectul studiului

Acest studiu discută importanța tehnologiilor de securitate a informației în Societatea Informației. Sunt examinate cerințe legale și de afaceri și explicate avantajele adoptării tehnologiilor de securitate a informației (competitivitate și încredere, în principal). Informația reprezintă moneda Economiei Internet. Tehnologiile de securitate a informației au un imens impact asupra modului în care organizațiile conduc afaceri electronice și, implicit, își ating obiectivele strategice.

2. Societatea Informației¹

În mai puțin de o generație, revoluția informației și introducerea calculatoarelor în fiecare dimensiune a societății a schimbat lumea. Predicțiile unor futuriști ca Marshall McLuhan și Alvin Toffler se adeveresc și lumea se transformă într-un sat global, unde nu mai există granițe pentru afaceri, comunicații sau comerț.

Câteodată, o nouă tehnologie alterează profund peisajul și plantează semințele unei schimbări radicale. Astăzi este clar că Internet este o asemenea tehnologie: “În istoria comerțului, au existat puține salturi majore privind capacitatea companiilor de a schimba informații între ele – discutabil o cerință critică pentru conducerea afacerilor. Ultimul avans major a fost invenția telefonului, în 1885. Astăzi, facem un alt pas mare cu Internet. Transformarea nu a fost imediată – comerțul pe Internet reprezintă un factor minor în modelele majorității companiilor. Dar asta este pe cale de a se schimba. Stăm pe muchia unei explozii în comerțul electronic” [9].

“A spune că Internet este unul dintre cele mai uimitoare realizări tehnice ale revoluției informaționale este mult sub adevăr” [8]. Această masivă infrastructură de rețele schimbă modul în care lumea abordează educația, afacerile și alte activități. Internet este deja propriul său stat, cu propria sa economie și propria sa monedă (*digicash*); el modifică modul în care economia mondială funcționează.

¹ "Societatea informației" se referă la importanța rolului informației în societate, iar "societatea interconectată" se referă la logica interconectării existente în toate funcțiile societății.

În timp ce informația și transmiterea ei au fost întotdeauna importante - în toate societățile și timpurile – și nu este nimic nou în interconectare ca atare, impactul logicii interconectării în societate ca întreg ajutat de folosirea tehnologiilor informației și a rețelelor de calculatoare este un fenomen al timpurilor noastre [19]

Potrivit Control Objectives for Information and related Technology (COBIT), “extrem de important pentru supraviețuirea și succesul unei organizații este managementul eficient al informației și al tehnologiilor informației (IT). În această societate a informației globală – unde informația circulă prin cyberspațiu fără constrângeri de timp, distanță sau viteză – criticalitatea apare din:

- Dependența mărită de informație și de sistemele care o furnizează
- Vulnerabilitățile crescânde și un larg spectru de amenințări, cum ar fi războiul informațional sau alte amenințări din cyberspațiu
- Scara și costul investițiilor curente și viitoare în informație și sistemele informaționale
- Potențial pentru tehnologii să schimbe dramatic organizațiile și practicile de afaceri, să creeze noi oportunități și reduceri ale costurilor”.

În societățile din “al treilea val”, societăți postindustriale, materia primă este informația, produsul este cunoașterea, mașinăriile sunt calculatoarele iar munca manuală este înlocuită de efortul intelectual [10]. Importanța informației și a sistemelor de comunicații pentru societate și economia globală se intensifică odată cu valoarea și cantitatea informației transmisă și stocată pe aceste sisteme [12]. Pentru multe organizații, informația și tehnologiile care o fac posibilă reprezintă cele mai valoroase bunuri ale organizației.

Ca societate, devenim din ce în ce mai dependenți de accesul și procesarea rapidă a informației. Pe măsură ce această solicitare crește, tot mai multă informație este stocată și transmisă electronic², ceea ce cauzează schimbarea modului în care companiile abordează afacerile. Spre deosebire de informația imprimată pe hârtie, informația în formă electronică poate fi potențial furată de la distanță și este mult mai ușor să fie interceptată și modificată.

Deoarece predecesorul Internet-ului, ARPANET, nu a fost niciodată securizat cu adevărat – de fapt, a fost creat pentru a facilita schimbul de informații între oameni de știință și cercetători - comunicațiile via Internet sunt implicit deschise și necontrolate³. Aceasta intră în conflict cu nevoile afacerilor electronice (*e-business*), care solicită confidențialitate și integritatea pentru informațiile transmise. Creșterea exponențială a afacerilor pe Internet ridică serioase chestiuni de securitate în legătură cu asigurarea unui

² Conform CIO's Security Worksheet [5] 74% dintre respondenți au indicat că informațiile de afaceri critice sunt stocate electronic. În ceea ce privește locul stocării informațiilor critice, respondenții au indicat că aceste informații sunt pe un server central (95%), pe benzi back-up (84.7%), pe PC-urile utilizatorilor (68.3%), pe calculatoare portabile (61.9%) și pe servere back-up (54.5%).

³ Foarte cunoscutul sistem de operare UNIX a fost, de asemenea, realizat fără a acorda mare importanță securității. “De-a lungul istoriei, sistemele UNIX au fost constant penetrate, bătute, brutalizate, corupte, comandate, compromise și **fsck** ilegal” [11].

mediu de afaceri securizat via Internet [1]. Deschiderea face Internet-ul vulnerabil la amenințări (spre exemplu, atrage crackerii⁴). Chiar dacă numai o minoritate a utilizatorilor va crea probleme organizațiilor prin furtul, ștergerea sau alterarea informațiilor, aceste riscuri sunt reale și vor exista întotdeauna – iar pe măsură ce Internet crește, aceste riscuri vor crește și ele.

Internet deschide noi modalități pentru consumatori, firme și guverne. Comenzile și plățile electronice pot fi administrate eficient și facil; poșta electronică și paginile web au devenit resurse instituționale. Cu toate acestea, până când protecția și securitatea informațiilor nu vor fi asigurate, beneficiile comunicațiilor și afacerilor electronice nu vor fi depline [7].

3. Economia Internet

Sistemele de informații legate în rețele sunt rapid adoptate de organizații în întreaga lume pentru a îmbunătăți comunicațiile, eficiența, controlul operațional și – în final - competitivitatea. Realizarea afacerilor pe Internet este rapidă și la costuri relativ reduse⁵ - motive suficiente, irezistibile pentru ca firmele să considere afacerile electronice ca alternative viabile⁶.

Economia Internet a crescut mai rapid decât se întvedea acum câțiva ani⁷. Ceea ce a pornit ca un canal alternativ pentru marketing s-a transformat rapid într-un sistem economic complet [6] constând din:

- comunicații atot-cuprinzătoare, rețele de comunicații la prețuri scăzute, care folosesc tehnologiile și standardele Internet,
- aplicații și capital uman care permite conducerea afacerilor prin această infrastructură de rețele,
- piețe electronice interconectate care operează folosind infrastructura de rețele și aplicații existentă,
- producători și intermediari care furnizează o mare varietate de produse și servicii pentru a facilita eficiența și lichiditatea,
- un cadru legal, încă în formare, pentru conducerea afacerilor electronice.

⁴ Richard Stallman, fondatorul Free Software Foundation, care se autointitulează "hacker", recomandă numirea hackerilor care penetrează ilegal sistemele informatice "crackers" [16]

⁵ Spre exemplu, Office Depot, cu \$11.6 bilioane în vânzări în 2000, și-a pus catalogul pe Web pentru \$500,000, iar menținerea sistemului costă anual \$5 milioane [20]

⁶ În 1999, circa 23 milioane de persoane au cheltuit peste \$11 bilioane. Tranzacțiile business-to-business au fost chiar mai mari: \$671 bilioane au fost schimbate în 1998, \$92 bilioane în tranzacții Internet și \$579 bilioane folosind EDI.

Potrivit lui Gartner Group (January 2000), "piața globală B2B este așteptată să crească de la \$145 bilioane în 1999 la \$7.29 trilioane în 2004. Până în 2004, comerțul electronic B2B va reprezenta 7% din totalul de \$105 trilioane al tranzacțiilor globale totale."

The Forrester Report on e-Business, realizat în iunie 2001, raportează că 34% dintre firme consideră achizițiile pe Web ca foarte importante sau critice pentru strategiile lor de procurare.

⁷ Economia Internet suportă direct 3,088 milioane angajați, mai mult decât industriile de asigurări sau imobiliare; comerțul Internet a generat peste \$127 bilioane în prima parte a lui 2000 [6].

Folosirea Internet-ului și a altor mijloace de comunicare aduce numeroase beneficii și permite obținerea de avantaje concurențiale⁸. Internet permite firmelor să își lărgescă afacerile în moduri care nu ar fi fost posibile înainte. Este o nouă lume a afacerilor, una plină de posibilități, făcută posibilă de emergența mediilor de calcul distribuite, unde firmele pot beneficia de comunicații rapide, metode avansate de colectare a datelor, lanțuri de furnizori electronici și alte avantaje ale acestei noi ere a procesării informației. Aceste soluții au mărit – și vor mări în continuare – eficiența cu care firmele operează și rezultatele lor financiare – dar ele au mărit și riscul de securitate informatică [3].

Când firmele au automatizat pentru prima dată operațiile lor, informațiile erau stocate și procesate de către sisteme de tip mainframe, izolate și controlate fizic. Astăzi, adevăratele bunuri sunt stocate electronic, nu în Fort Knox, iar ținutele cyber-atacurilor sunt din ce în ce mai des rețelele de calculatoare. Aceste rețele locale sunt conectate la alte rețele, exterioare, în primul rând prin Internet [2].

Aceste conectări sunt nediscriminatorii; ele traversează frontiere și conectează firme, școli, cămine și guverne⁹. Cu această explozie în conexiuni vine accesul¹⁰. Întocmai cum un telefon poate accesa orice alt telefon pe glob, orice calculator poate, potențial, accesa și schimba informații cu alte calculatoare interconectate. Nu există nici un control al accesului în rețele precum Internet. Fiecare calculator individual trebuie să solicite autentificare și autorizare a accesului.

Proliferarea calculatoarelor la prețuri din ce în ce mai mici și dramatica expansiune a interconectivității au exacerbat problemele de acces neautorizat și alterare a informațiilor. Dezvoltările tehnologice au mărit mult securitatea sistemelor informatice, dar, în același timp, au dat potențialilor atacatori șansa unor penetrări mult mai rapide și adânci în sistemele informatice (fie ele personale, guvernamentale sau ale firmelor), aceasta cu efecte, în unele cazuri, foarte serioase. Conectivitatea permite acces la o mulțime de resurse, rapid și eficient, dar ea permite și o cale de acces [13] în care atacatorii pot surpasa sistemele de autentificare desemnate să protejeze sistemele¹¹.

Frecvența atacurilor care dăunează financiar sau în alte moduri organizațiile este în creștere¹². Bazat pe răspunsurile venite de la 538 persoane din domeniul securității

⁸ General Electric se așteaptă să economisească \$1.6 bilioane în acest an, înainte de taxe, prin digitizarea fluxurilor de producție de tip vechi și să realizeze aproape \$14 bilioane în licitații online. Sistemul electronic de introducere a ordinilor a micșorat rate de eroare pentru firmă de la 20% la 0,2%.

⁹ Se estimează că aceste conexiuni cresc cu 10% în fiecare lună [2]. Considerând implementarea și modernizarea sistemelor de telecomunicații în țările în curs de dezvoltare, această tendință va continua în viitorul apropiat.

¹⁰ În 30% dintre companiile chestionate de CIO, informațiile critice sunt accesibile direct de pe Internet. În 57.8% dintre companiile intervievate server-ele care stochează informații critice comunică direct cu alte sisteme care sunt accesibile de pe Internet [5].

¹¹ Exemplele sunt nenumărate; unul timpuriu a fost viermele Internet din 1988.

¹² Cazuri bine documentate includ:

- Un crack la Citibank în 1995 când \$10.4 milioane au fost furate;
- Expunerea informațiilor cardurilor de credit la dot-coms, cum ar fi Egghead.com, Inc., când baza de date conținând asemenea informații a fost compromisă.

informatică, CSI/FBI 2001 Computer Crime and Security Survey confirmă trendurile ultimilor ani:

- Organizațiile sunt atacate atât din interior cât și din exteriorul perimetrului lor electronic.
- Larga gamă de cyber atacuri a fost detectată.
- Cyber atacurile pot rezulta în pierderi financiare serioase.
- Protejarea împotriva unor asemenea atacuri solicită mai mult decât simpla folosire a tehnologiilor de securitate informatică.

Sofisticata societate a informației - “leagănul prosperității, expresia pură a capitalismului”, conform lui John Doerr – prezintă pericole semnificative, noi riscuri și o litanie de consecințe nedorite [4] care trebuiesc bine înțelese și administrate de către cei implicați.

Potrivit lui Dr. Paul Dorey, Director al Digital Business Security, “securitatea informatică furnizează procesele manageriale, tehnologia și asigurarea că se poate avea încredere în tranzacțiile de afaceri; asigură că serviciile informatice sunt utilizabile și pot rezista adecvat unor probleme cauzate de erori, atacuri deliberate sau dezastre; asigură că accesul la informație este permis numai celor care trebuie să aibă acces” [18].

Tehnologiile de securitate a informației bine folosite înseamnă pentru companii păstrarea reputației, a potențialului și evitarea unor pierderi financiare. Consecințele incidentelor de securitate informatică pot fi dezastruoase – dar ele pot fi evitate. Vechile metode de securitate informatică rămân importante, dar pe măsură ce firmele dobândesc o nouă identitate virtuală, acestea nu mai sunt suficiente.

4. Despre importanța tehnologiilor de securitate a informației

Informația, produsele informației, precum și costurile și beneficiile rezultate din informație devin din ce în ce mai mult transnaționale. Informația este “putere”, ea are o valoare, iar capacitatea de a stoca și procesa anumite informații poate furniza un important avantaj asupra competitorilor.

Informația este utilă doar atât timp cât rămâne validă, nealterată. Unul dintre modurile cele mai insidioase pentru un competitor de a obține avantaje constă în sabotarea bazelor de date ale rivalilor în moduri subtile [17]; impactul unor asemenea acțiuni poate fi devastator.

Informația este un bun foarte important, în consecință trebuie protejat adecvat pentru a asigura continuitate, a minimiza posibilele daune și a maximiza beneficiile și oportunitățile de afaceri¹³.

Cu toate că intruziunile informatice pot avea costuri foarte ridicate, multe firme nu au alocat resurse suficiente pentru a se proteja¹⁴. Situația este în schimbare¹⁵, iar ceea ce

● În 27 octombrie 2000 sistemele firmei Microsoft au fost penetrate iar codul sursă a fost compromis. Conform Reuters, Microsoft a caracterizat incidentul ca “un act deplorabil a de spionaj corporatist”.

¹³ În acest context, ne referim la informații înregistrate pe, procesate de, transmise sau accesate de pe un medium electronic.

odată a fost văzut doar ca o durere de cap, capătă o importanță din ce în ce mai mare – aceasta nu reprezintă o surpriză deoarece tehnologiile de securitate a informației sunt considerate astăzi un important factor, de care depinde succesul unei organizații.

E-business solicită “o abordare fundamental diferită în ceea ce privește securitatea informatică” spune Sunil Misra, șeful securității informatice la Unisys [15]. “În trecut singurele persoane care îți accesau rețelele erau angajații și unii parteneri. Aceștia erau persoane pe care le cunoșteai și în care aveai încredere. Cu e-business, nu știi cine îți accesează rețelele și nu știi dacă poți să ai încredere în ei. Așadar este necesar un set de principii diferite, procese și tehnologii care să asigure că rețelele rămân protejate”.

În mediul de afaceri electronice din zilele noastre, tehnologiile de securitate a informației pot servi la obținerea de profituri și noi oportunități de afaceri, nu numai să reducă riscurile. Tehnologiile de securitate a informației nu vizează doar prevenirea dezastrelor, ci ele reprezintă mijloace de realizare a obiectivelor de afaceri¹⁶. Tehnologiile de securitate a informației sunt absolut necesare pentru asigurarea succesului, prin urmare ele trebuie incluse în procesul de gândire strategică a firmelor. Securitatea informatică trebuie văzută ca un proces care este esențial în îndeplinirea nevoilor legitime ale partenerilor și clienților și nu ca ceva care “poate fi adăugat”. Pe de altă parte, companiile trebuie să se asigure că departamentele lor de marketing și relații cu publicul sunt versate în principiile tehnologiilor de securitate a informației pentru a putea comunica efectiv publicului măsurile care sunt luate pentru a proteja banii și intimitatea clienților [21.]. În afară de rațiuni comerciale, firmele au obligații legale să asigure protecția datelor personale ale clienților lor¹⁷.

“Tehnologiile de securitate a informației reprezintă o funcție care vizează un control complet și administrarea vulnerabilităților și riscurilor societății interconectate. Ele reprezintă o parte din siguranța în societate” [19]¹⁸; ele trebuie să asigure confidențialitatea, posesia (sau controlul), integritatea, autenticitatea, disponibilitatea și utilitatea informațiilor și sistemelor.

¹⁴ Potrivit DataMonitor (2000), costul total al violărilor de securitate informatică pentru corporații a fost de \$15 miliarde, în timp ce procentul companiilor care nu au implementat încă măsuri adecvate de securitate informatică a fost de 30%.

¹⁵ Un studiu al firmei John J. Davis & Associates arată că 92% dintre CIO consideră securitatea informatică drept cea mai presantă nevoie a companiilor lor (de la 59% în 1997 – [15]).

¹⁶ “Securitatea informatică trebuie să devină o decizie de afaceri. Trebuie să fie vorba despre ceea ce se dorește a se obține, nu despre ceea ce se dorește să fie evitat” (Frank Prince, analist senior, infrastructura e-business Forrester Research, Inc., citat în [15]).

¹⁷ Din punct de vedere al unui eventual litigiu, instalarea de mijloace adecvate de protecție informatică (cum ar fi firewalls, programe pentru detectarea intruziunilor, și politici pentru continuă evaluare a riscurilor și vulnerabilităților) va fi întotdeauna o bună apărare. Organizațiile care nu acordă atenția necesară pentru minimizarea expunerii la asemenea amenințări pot fi subiectul unor procese.

¹⁸ Netrex (http://netrex.actionwebservices.com/glossary_of_terms_h_l.html) definește “tehnologiile de securitate a informației” ca “rezultatul oricărui sistem de politici și/sau proceduri pentru identificare, controlarea și protejarea împotriva divulgării neautorizate a informațiilor a caror protecție este autorizată” – noi credem că această definiție este prea îngustă.

Tehnologiile de securitate a informației au mai multe componente și atribute care trebuie considerate când se analizează riscul potențial. În linii mari, acestea pot fi clasificate în trei mari categorii¹⁹:

● **Confidențialitatea** - protecția informațiilor în sistem astfel încât persoane neautorizate nu le pot accesa. Este vorba despre controlarea dreptului de a citi informațiile. Aproape fiecare organizație are informații care, dacă sunt divulgate sau furate, ar putea avea un impact semnificativ asupra avantajului competițional²⁰, valorii de piață sau a veniturilor. Adicional, o firmă poate fi făcută responsabilă pentru divulgarea de informații private. Aspecte cruciale ale confidențialității sunt indentificarea și autentificarea utilizatorilor.

● **Integritatea** - protecția informațiilor împotriva modificărilor intenționate sau accidentale neautorizate; condiția ca informația din sau produsă într-un mediu informatic reflectă sursa sau procesele pe care le reprezintă. Este vorba despre nevoia de a asigura că informația și programele sunt modificate numai în maniera specificată și autorizată și că datele prezente sunt originale, nealterate sau șterse în tranzit. Ca și în cazul confidențialității, identificarea și autentificarea utilizatorilor sunt elemente cheie ale unei politici de integritate a informațiilor.

● **Disponibilitatea** – se referă la asigurarea că sistemele de calcul sunt accesibile utilizatorilor autorizați când și unde aceștia au nevoie și în forma necesară (condiția ca informația stocată electronic este unde trebuie să fie, când trebuie să fie acolo și în forma necesară²¹).

Importanța pe care fiecare dintre aceste cerințe o joacă în cadrul operațiilor unei firme (și de aici nivelul de perturbare potențial) depinde de la industrie la industrie și de la firmă la firmă. Obiectivul tehnologiilor de securitate a informației constă în “protejarea intereselor celor care se bazează pe informații și sistemele și comunicațiile care livrează aceste informații împotriva daunelor care pot rezulta din incapacitatea de a se asigura disponibilitatea, confidențialitatea și integritatea informațiilor” [18].

¹⁹ [1] adauga alte doua categorii:

● **Folosire legitimă:** Sistemele și informațiile sunt folosite numai pentru scopuri legitime de catre indivizi autorizati.

● **Non-repudiare:** Caracteristica tranzactiilor in care partile intr-o tranzactie efectuata sunt atestate, astfel incat nici una dintre partile implicate nu poate tagadui participarea sau detaliile actiunilor sau deciziilor luate in timpul participarii [14].

²⁰ Un studiu publicat de revista Information Security (July 1999) arată că dintre companiile care conduc afaceri electronic sunt cu 57% mai probabil să sufere “scurgeri” de informații clasificate decât companiile care nu desfășoară afaceri pe Web.

"Trends in Intellectual Property Loss", un studiu al American Society for Industrial Security (ASIS) arată [2]:

"Potențialele pierderi datorate furtului de proprietate intelectuală pentru companiile din SUA sunt estimate la \$24 miliarde anual".

²¹ Joacă un rol critic în tranzacțiile electronice: clienții așteaptă să aibă acces și răspuns rapid. Aceasta constituie potențial un avantaj competitiv major: firmele pot opera 24 ore pe zi, furnizând servicii și informații clienților. De fapt, o rețea non-operațională poate costa organizațiile până la \$50,000 pe ora, în funcție de aplicație și de piață (conform studiului executat de The Yankee Group) - spre exemplu, un sistem de rezervare bilete de avion sau spectacol.

5. Probleme susceptibile să apară ca rezultat al studiului

Pentru prea multă vreme tehnologiile de securitate a informației au fost văzute ca un factor negativ, creând valoarea prin non-eveniment. Astăzi, ca rezultat al rețelelor globale și al extinderii firmelor dincolo de hotarele tradiționale apar ca facilitator de oportunități, ca un creator de valoare, în particular prin inducerea încrederii în cei implicați [18].

Pentru a asigura securitatea informațiilor care sunt critice pentru firme, fiecare companie trebuie să dezvolte o politică de securitate informatică, care să asigure că atunci când ceva se întâmplă, procesele care să rezolve situația există. Acesta este un proces fără sfârșit - un proces pentru dezvoltarea unei politici de securitate informatică este ca un cerc, care se întoarce întotdeauna la punctul de plecare pentru a mări siguranța: noi tehnologii și idei solicită o actualizare continuă a politicii de securitate informatică [1].

6. Costuri și consecințe ale inacțiunii sau acțiunii întârziate

România are pași importanți de făcut în direcția educării persoanelor implicate și a publicului larg pentru a înțelege necesitatea tehnologiilor de securitate a informației în Societatea Informației, mai ales în perspectiva integrării euro-atlantice. Considerăm că sunt necesare seminarii și broșuri care să explice clar beneficiile și (în multe situații) obligația legală de folosire a tehnologiilor de securitate a informației. Costurile și consecințele inacțiunii sau a acțiunii întârziate pot fi foarte însemnate.

Referințe bibliografice

- [1] Amor, D., The E-Business (R)evolution, Living and Working in an Interconnected World, Hewlett-Packard Professional Books, 2000, pp. 354-391.
- [2] Anderson, K., Criminal Threats to Business on the Internet, A White Paper, 1999, URL: http://www.aracnet.com/~kea/Papers/White_Paper.shtml (12 May 2001).
- [3] Axent Technologies, Information Security Begins with Sound Security Policies, 1998.
- [4] Cilluffo, F. J., "Cyber Attack: The National Protection Plan and its Privacy Implications" (Statement to the United States Senate Subcommittee on Technology, Terrorism, and Government Information Committee on the Judiciary, 2000, URL: <http://www.csis.org/goc/rc/cyber.html> (28 July 2001).
- [5] Cosgrove Ware, L., CIO Security Worksheet, August 8, 2001, www.cio.com/CIO (9 August 2001).
- [6] Internet Indicators, URL: www.internetindicators.com, 2001 (10 August 2001).
- [7] ITL Bulletin, advising users on information technology, cryptography standards and infrastructures for the twenty-first century, september 1998, URL: <http://www.itl.nist.gov/lab/bulletns/sep98.htm> (20 July 2001).
- [8] Krause, M. and Tipton, H. F., Information Security Management Handbook, Fourth Edition, CRC Press - Auerbach Publications, 1999.
- [9] Linder, J. C., URL: <http://www.se-com.com/wp/forrester.html>, (15 June 2001).
- [10] Mohrman, S. A., Galbraith, J. R., Lawler III, E. E., and Associates, Tomorrow's Organization – Crafting Winning Capabilities in a Dynamic World, Jossey-Bass Publishers, San Francisco, 1998.

- [11] Nemeth, E., Snyder, G., Seebass, S., Hein, T. R., UNIX System Administration Handbook, Second Edition, Prentice Hall, USA, 1995, pp. 539-558.
- [12] OECD, Report on background and issues of cryptography policy, 1997.
- [13] Power, R., Current and Future Danger, Computer Security Institute, San Francisco, California, 1995.
- [14] Schlumberger, Smartcards enhanced security for Microsoft Windows 2000 systems, White Paper, 2000.
- [15] Schoeniger, E., Security and the Internet Factor, Exec, November-December 2000.
- [16] Stallman, R. M., Letter to ACM Forum, Comm. ACM, Vol. 27, No. 1, Jan. 1984, pp. 8-9.
- [17] Stoll, C., The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, New York, Doubleday, 1989.
- [18] The IT Governance Institute, Information Security Governance: Guidance for Boards of Directors and Executive Management, 2001.
- [19] University of Lapland, Communication (2000) 890, Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime in the context of Information Security, Institute for Law and Informatics, Finland, 20 March 2001.
- [20] Varon, E., The ABCs of B2B Exchanges, 2001,
URL: <http://www.cio.com/ec/edit/b2babc.html> (20 August 2001).
- [21] Worstell, K., Gerdes, M. and Kabay M., Net Present Value of Information Security: Part I, URL: <http://securityportal.com/articles/npv20001102.html> (10 July 2001).