Analiza Sistemului Informatic din Punct de Vedere al Securităţii

Hlopeanicov C., Safonov Gh.
Academia Militară a Forţelor Armate „Alexandru cel Bun"
mun. Chișinău, Republica Moldova
claudia.hlopeanicov@academy.army.md

***Abstract* – Keeping organizational information assets secure in today's interconnected computing environment is a true challenge that becomes more difficult with each new "e" product and each new intruder tool. Most organizations realize that there is no one solution or panacea for securing systems and data; instead a multi-layered security strategy is required. One of the layers that many organizations are including in their strategy today is being proactive about security by being prepared about detecting and responding to incidents when they arise.**

***Termeni cheie* – securitate, informație, sistem informaţional, sistem informatic.**

I. Introducere

În viața noastră de zi cu zi, calculatoarele sunt ceva obișnuit, ba chiar necesar în unele cazuri. Putem spune, pe drept, că trăim într-o societate informatizată. În zilele noastre, întîlnim calculatoare peste tot, care-și ține evidențele sale cu ajutorul unui PC și pînă la ghișeul la care plătim telefonul. Peste tot sunt calculatoare, legate eventual între ele și formînd astfel rețele de calculatoare. Toate acestea se datorează faptului că ne dăm seama din ce în ce mai mult că PC-ul ne ușurează munca. Dar trebuie de subliniat faptul că un calculator este de fapt o „mașinărie" care prelucrează o serie de informații pe care i le dăm. Informația, este elementul esențial din acest întreg lanț. De fapt, în practică întîlnim, printre altele, două noțiuni legate de aceasta și anume sistemul informațional și sistemul informatic.

Sistemul informațional este ansamblul de elemente implicate în procesul de colectare, transmisie, prelucrare, etc. de informații.

Rolul sistemului informațional este de a transmite informația între diferite elemente. De exemplu, în cadrul unei instituții de învățămînt, rolulul sistemului informațional este de a asigura persoanele din conducere cu informații necesare pentru luarea diferitelor decizii importante sau de altă natură. În cadrul sistemului informațional, majoritatea activităților se pot desfășura cu ajutorul tehnicii de calcul.

În cadrul sistemului informațional, majoritatea activităților se pot desfășura cu ajutorul tehnicii de calcul.

Ansamblul de elemente implicate în tot acest proces de prelucrare și transmitere a datelor pe cale electronică alcătuiesc un ***sistem informatic***.[1]

Într-un sistem informatic pot intra: calculatoare, sisteme de transmisie a datelor, alte componente hardware, softwer-ul, datele prelucrate, personalul ce exploatează tehnica de calcul, teoriile ce stau la baza algoritmilor de prelucrare, etc.

Se poate spune deci, că sistemul informațional este inclus în sistemul informatic, acesta din urmă fiind o componență esențială a primului.

II. Abordarea Securității Informaționale

Datorită dezvoltării tehnologiei, sistemul informatic a devenit un instrument de comunicare obligatoriu. Dar orice mijloc de comunicare, mai ales când mediul de comunicare este un mediu nesigur, cum este Internetul, prezintă riscuri. Utilizarea sistemelor informatice conectate la Internet în domeniul militar sau domeniul comercial face ca acest risc să crească simțitor.

Sistemele informatice s-au dovedit vulnerabile în fața atacurilor de pe Internet, la accesările neautorizate a sistemului, la modificări sau distrugeri de informații, accidentale sau intenționate. Atenuarea și corectarea acestor vulnerabilități a devenit o obligație atît pentru organizațiile cît și pentru persoanele fizice pentru protejarea informațiilor.

Identificarea elementelor care să asigure un grad corespunzător de securitate presupune o planificare riguroasă și identificarea exactă a obiectivelor. Gradul de expunere a sistemelor informaționale variază în funcție de domeniul în care activează fiecare organizație. Cu cît acest risc este mai mare, atenția care trebuie acordată securității datelor ar trebui să fie mai mare. Instituțiile financiare, industria apărării, aerospațială, industria tehnologiei informației sau industria electronică sunt sectoarele cu cel mai mare grad de risc în ceea ce privește securitatea informațiilor.

Este important ca fiecare organizație/instituție să poată să-și identifice propriile cerințe de securitate. Pentru aceasta ea trebuie să facă apel la trei surse principale:

1) Evaluarea riscurilor: se identifică amenințările asupra resurselor, se evaluează vulnerabilitatea la aceste amenințări și probabilitatea de producere a lor și se estimează impactul potențial;

2) Legislația existentă pe care o organizație/instituție trebuie să o respecte;

3) Setul specific de principii, obiective și cerințe pentru

[1] Wikipedia Enciclopedia Liberă

procesarea informației, pe care organizația le dezvoltă pentru a-și susține activitățile.

Pentru a analiza riscurile o organizație/instituție își poate identifica propriile cerințe legate de securitate. Un astfel de proces presupune în general patru etape principale:

1) Identificare resurselor care trebuie protejate;
2) Identificarea riscurilor/amenințărilor specifice fiecărei resurse;
3) Ierarhizarea riscurilor;
4) Identificarea controalelor prin care vor fi eliminate/diminuate riscurile.

Pentru a-și defini politica de securitate trebuie să se decidă:

- care amenințări trebuie eliminate și care se pot tolera;
- care resurse trebuie protejate și la ce nivel;
- cu ce mijloace poate fi implementată securitatea;
- care este prețul (financiar, uman, social etc.) măsurilor de securitate care poate fi acceptat.

Un aspect important în stabilirea mecanismelor de securitate o constituie partea financiară. Un mecanism de control nu trebuie să depășească valoarea bunului ce trebuie protejat.

Odată stabilite obiectivele politicii de securitate, următoare etapa constă în selecția serviciilor de securitate – funcțiile individuale care sporesc securitatea. Fiecare serviciu poate fi implementat prin metode (mecanisme de securitate) variate pentru implementarea cărora este nevoie de așa-numitele funcții de gestiune a securității. Gestiunea securității constă în controlul și distribuția informațiilor către toate sistemele în scopul utilizării serviciilor și mecanismelor de securitate și al raportării evenimentelor de securitate ce pot apărea către administratorii de rețea.

Șablonul de securitate pentru un sistem informatic poate fi văzut ca avînd mai multe straturi ce reprezintă nivelurile de securitate ce înconjoară subiectul ce trebuie protejat. Fiecare nivel izolează subiectul și îl face mai dificil de accesat în alt mod decât cel în care a fost prevăzut.

Securitatea fizică reprezintă nivelul exterior al modelului de securitate și constă, în general, în închiderea echipamentelor informatice într-o altă incintă precum și asigurarea pazei și a controlului accesului. O problemă o constituie salvările sub forma de copii de rezervă ale datelor și programelor, precum și siguranța păstrării suporților de salvare (backup). Rețelele locale sunt, în acest caz, de mare ajutor, copiile de rezervă putându-se face prin rețea pe o singura mașina ce poate fi mai ușor securizată.

Securitatea fizică trebuie abordată foarte serios deoarece toate măsurile de securitate logice, cum ar fi stabilirea de parole pe sistemul respectiv, devin nesemnificative în cazul accesului neautorizat la echipamente. O altă, problemă importantă în securitatea fizică unui sistem informatic o constituie pur și simplu sustragerile de echipamente sau a suporților de backup.

Securitatea logică constă din acele metode logice (software) care asigură controlul accesului la resursele și serviciile sistemului. Ea are, la rîndul ei, mai multe niveluri impărțite în două grupe mari: niveluri de securitate a accesului și niveluri de securitate a serviciilor.

Securitatea accesului cuprinde:

- accesul la sistem, care este răspunzător de a determina în ce condiții și în ce moment este sistemul accesibil utilizatorilor. El poate fi răspunzător de asemenea și de gestionarea evidenței accesului. Accesul la sistem poate efectua și deconectarea forțată în anumite cazuri (ex. expirarea contului, ora de vîrf, …);
- accesul la cont care verifică dacă utilizatorul ce încearcă să se conecteze are un nume și o parolă validă;
- drepturile de acces (la fișiere, resurse, servicii etc.) care determină de ce privilegii dispune un utilizator (sau un grup de utilizatori) dat.

Securitatea serviciilor controlează accesul la serviciile unui sistem (calculator, rețea). Din acest nivel fac parte:

- controlul serviciilor care este responsabil cu funcțiile de avertizare și de raportare a stării serviciilor, precum și de activarea și dezactivarea diverselor servicii oferite de către sistemul respectiv;
- drepturile la servicii care determină exact cum folosește un anumit cont un serviciu dat (acces la fișiere, resurse, prioritate,…).

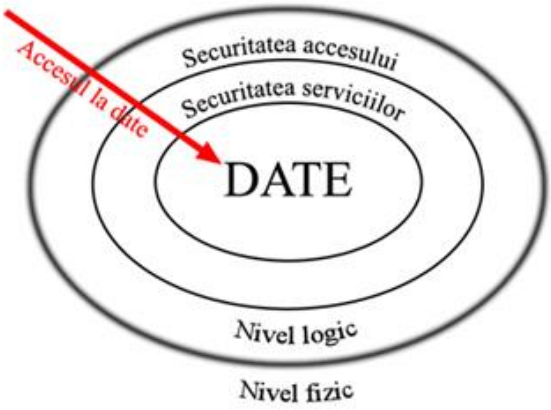

Fig. 1 Modelul de securitate.[2]

Odată stabilită conexiunea logică, subsistemul de securitate a accesului validează contul de acces. Subsistemul de securitate a serviciilor monitorizează activitatea utilizatorului și ia măsuri în cazurile în care cererile acestuia depășesc drepturile specificate în profilul utilizatorului (sau grupului de utilizatori) respectiv. Accesul într-un sistem sigur perfect ar trebui să se facă prin aceste niveluri de securitate descrise mai sus, de „sus" în „jos" fără să permită ocolirea vreunuia din ele.

Securitatea la nivel de gazdă urmează principiile enunțate mai sus. În cazul unui sistem conectat la Internet distingem:

- entitățile ce au acces local la acea mașină (utilizatori, programe server, agenți locali) precum și drepturile acestora (ce are voie să facă un anumit utilizator, cu ce privilegii

[2] Ioan-Cosmin Mihai, „Securitatea sistemului informatic", Editura Dunărea de Jos, Galați, 2007

rulează un anume proces, ce prioritate are un proces, ce drepturi are asupra fișierelor respective, asupra spațiului de stocare, ce resurse și între ce limite are voie să acceseze);

- serviciile oferite către exterior (publice sau pentru anumiți utilizatori; autentificare, monitorizare);
- sistemul de operare (tipul, distribuția, servicii implicite oferite – filtrarea sau dezactivarea celor de care nu e nevoie, bug-uri cunoscute, revizii etc.)

III. Importanța Securității Sistemului Informatic

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 atît timp cat rămîne validă, nealterata. Unul dintre modurile cele mai insidioase pentru un competitor de a obține avantaje constă în sabotarea bazelor de date ale rivalilor în moduri subtile. Impactul unor asemenea acțiuni poate fi devastator.

Informația este foarte importantă, în consecința trebuie protejată adecvat pentru a asigura continuitate, a minimiza posibile daune și a maximiza beneficiile și oportunitățile de afaceri[3].

Cu toate că intruziunile informatice pot avea costuri foarte ridicate, multe organizații/instituții nu au alocat resurse suficiente pentru a se proteja. Situația este în schimbare[4], iar ceea ce odată a fost văzut doar ca o durere de cap, căpăta 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/instituții.

E-business-ul solicită „o abordare fundamental diferită în ceea ce privește securitatea informatica" spune Sunil Misra, șeful securității informatice la Unisys [Schoeniger, 2000]. „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-ul, nu știi cine îți accesează rețelele și nu știi dacă poți să ai încredere în ei. Așadar este necesar un set de principii diferit, procese și tehnologii care să asigure ca rețelele să rămîn 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 afaceri. Tehnologiile de securitate a informației sunt absolut necesare pentru asigurarea succesului, prin urmare, ele trebuiesc incluse în procesul de gîndire strategică a organizațiilor/instituțiilor. 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, organizațiile/instituțiile trebuie să se asigure ca departamentele lor de marketing și relații cu publicul sunt competente în principiile tehnologiilor de securitate a informației pentru a putea comunica efectiv publicului măsurile care sunt luate pentru a proteja banii și intimitatea clienților. În afara de rațiuni comerciale, organizațiile/instituțiile au obligații legale să asigure protecția datelor personale ale clienților lor.

„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 siguranță în societate"[5]; ele trebuie să asigure confidențialitatea, posesia (sau controlul), integritatea, autenticitatea, disponibilitatea și utilitatea informațiilor și sistemelor.

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

1) Confidențialitatea – protecția informațiilor în sistem astfel încît persoane neautorizate nu le pot accesa. Este vorba despre controlarea dreptului de a citi informațiile. Aproape fiecare organizație/instituție are informații care, dacă sunt divulgate sau furate, ar putea avea un impact semnificativ asupra avantajului competițională, valorii de piață sau a veniturilor. Adițional, o organizație/instituție poate fi făcută responsabilă pentru divulgarea de informații private. Aspecte cruciale ale confidențialității sunt identificare și autentificarea utilizatorilor.

2) 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 ca informația și programele sunt modificate numai în maniera specificată și autorizată și ca 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 integritatea a informațiilor.

3) Disponibilitatea – se referă la asigurarea ca sistemele de calcul sunt accesibile utilizatorilor autorizați cînd și unde aceștia au nevoie și în forma necesară (condiția ca informația stocată electronic este unde trebuie sa fie, cînd trebuie să fie acolo și în forma necesara).

Importanța pe care fiecare dintre aceste cerințe joacă în cadrul operațiilor unei organizații/instituții (nivelul de perturbare potențial) depinde de la industrie la industrie și de la organizație/instituție la organizație/instituție. 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

[3] In acest context, ne referim la informații înregistrate pe, procesate de, transmise sau accesate de pe un medium electronic.

[4] Un studiu al firmei John J. Davis & Associates arată ca 92% dintre CIO consideră securitatea informatică drept cea mai presantă nevoie a companiilor lor (de la 59% in 1997 - Schoeniger, 2000).

[5] Netrex (*http://netrex.actionwebservices.com/glossary_of_terms_h_l.html*) definește "tehnologiile de securitate a informației" ca "rezultatul oricărui sistem de politici si/sau proceduri pentru identificare, controlarea si protejarea împotriva divulgării neautorizate a informațiilor a căror protecție este autorizata" – noi credem ca aceasta definiție este prea îngustă.

disponibilitatea, confidențialitatea și integritatea informațiilor"[6].

IV. Analiza Pierderilor în Sistemul Informatic

Analiza sistemului informaţional existent urmăreşte delimitarea ariei de cuprindere a sistemului şi formularea cerinţelor şi restricţiilor globale de realizare. Pentru a atinge acest scop, în această porţiune se face un studiu amănunţit al sistemului existent, se apreciază măsura în care sistemul existent este capabil să răspundă în continuare exigenţelor conducerii ştiinţifice, se apreciază oportunitatea realizării unui sistem informatic şi se formulează principalele restricţii şi cerinţe pentru viitorul sistem informatic.

Sistemele informatice sunt vulnerabile în primul rînd la atacurile clasice, atunci cînd un atacator reuşeşte să pătrundă în incinta sistemelor de calcul şi să sustragă informaţii confidenţiale. Pentru a preîntîmpina acest lucru, trebuie să se asigure securitatea fizică a echipamentelor de calcul prin plasarea acestora în zone sigure, restricţionate personalului neautorizat. Accesul la aceste zone trebuie făcut prin folosirea interfoanelor, cardurilor de acces sau dispozitivelor de scanare a datelor biometrice pentru autentificarea utilizatorilor cu permis de intrare. O altă vulnerabilitate a sistemelor informatice o reprezintă dezastrele naturale; cutremure, inundaţii, incendii sau accidentele precum căderile de tensiune sau supratensiunile ce pot duce la distrugerea fizică a echipamentelor de calcul. De aceea trebuie avute învedere şi amplasarea echipamentelor pentru reducerea riscului faţă de ameninţările mediului înconjurător. O atenţie deosebită trebuie acordată componentelor hardware pentru ca acestea să nu afecteze ulterior buna funcţionare a sistemelor informatice. În cazul serverelor ce furnizează servicii în Internet trebuie alese componente hardware tolerante la defectări pentru a oferi disponibilitate serviciilor şi datelor partajate în reţea şi pentru a reduce riscul vulnerabilităţilor de tip hardware. Aceste vulnerabilităţi sunt întîlnite cel mai des la sistemele de stocare a datelor, fiind cele mai sensibile componente hardware şi în cazul defectării lor pagubele fiind cele mai însemnate prin pierderea parţială sau totală a informaţiilor. Din acest punct de vedere se recomandă salvările de siguranţă atît la nivelul informaţiilor cît şi la nivelul sistemului de operare, pentru repunerea rapidă a acestuia şi a serviciilor configurate în caz de defecţiune. Comunicaţiile în Internet sunt de asemenea nesigure. Oricine se poate conecta la linia de comunicaţie şi poate intercepta, altera sau chiar devia traficul de date. Pentru a înlătura aceste vulnerabilităţi se recomandă folosirea metodelor de criptare a datelor, ca în cazul în care acestea sunt interceptate, ele să nu poată fi decriptate.

Cauzele apariţiei vulnerabilităţilor într-un sistem informatic sunt multiple, cîteva dintre acestea fiind:

- erorile existente la nivelul sistemelor de operare sau aplicaţiilor;
- configurarea necorespunzătoare a sistemului de operare sau a aplicaţiilor;
- cunoştinţele limitate ale administratorilor de sistem sau de reţea;
- lipsa suportului dezvoltatorilor de software în rezolvarea erorilor aplicaţiilor.

Nu în ultimul rînd, cele mai mari vulnerabilităţi sunt cele umane, date de personalul ce se ocupă de configurarea şi administrarea sistemelor informatice. Prin lipsa experienţei sau prin nedocumentare adecvată privind anumite configurări ale sistemului de operare sau ale aplicaţiilor instalate, securitatea informaţiilor poate fi total compromisă.

Deciziile relative la tratarea ameninţărilor trebuie să fie fundamentate pe o evaluare a riscurilor în cauză. Pentru aceasta, ameninţările trebuie să fie caracterizate, de fiecare dată cînd este posibil, printr-o categorie de gravitate şi printr-un nivel de probabilitate. Categoriile de gravitate furnizează o măsura calitativă, plecînd de la estimarea ce1ei mai grave consecinţe posibile a unui eveniment nedorit (ameninţare). Aceste categorii pot fi:

a) catastrofică (distrugerea totală a sistemului);
b) critică (distrugeri grave ale sistemului);
c) marginală (distrugeri reduse);
d) neglijabilă.

Probabilitatea unei ameninţări în cursul duratei de viaţă prevăzute a unui sistem poate fi definită ca fiind numărul de apariţii al evenimentului nedorit (ameninţării), raportat la o durata de timp.

Cuantificarea probabilităţii este în general imposibilă în faza de concepţie a sistemului, dar se poate da o apreciere calitativă bazată pe analize, cercetări, şi pe exploatarea experienţei acumulate în cadrul altor sisteme similare. O evaluare calitativă este de exemplu, *frecvența*: probabilă, ocazională, rară, improbabilă.

Plecînd de la gravitate și de la probabilitatea riscului asociat fiecărei ameninţări, se poate stabili o ordine de prioritate pentru tratarea lor. Deoarece măsurile de securitate și protecţie ce se aplică în cadrul unui sistem informaţional au întotdeauna un cost, și per ansamblul sistemului acesta poate să fie foarte important. De aceea, pentru a determina gradul în care aceste costuri se justifică, este necesară efectuarea unei proceduri numită „analiză a riscurilor". În cadrul ei sunt trecute în revistă diferitele ameninţări relevate, estimîndu-se frecvenţele de apariţie asociate precum și mărimile pierderilor corespondente ce le implică.

Plecînd de la aceste date, este previzionată „pierderea anuală" asociată fiecăreia dintre ameninţări. Ideea ce stă la baza evaluării respective este că, prin compararea pierderii anuale previzionate și a costului furnizării unei protecţii adecvate se vor putea determina care sunt aspectele de securitate ce trebuiesc tratate, adică se vor putea identifica punctele în care ameninţarea este cea mai mare și investiţia de securitate este cea mai potrivită în a produce rezultate.

Beneficiile unei analize a riscurilor sunt direct proporţionale cu gradul de credibilitate al măsurătorilor, și dacă acestea sunt efectuate la timp și pot fi cuantificate. Dar în practică riscul poate, de regulă, să fie cuantificat cu dificultate, iar analizele sunt costisitoare. Cuantificarea necesită statistici despre frecvenţa ameninţărilor și mărimea pierderilor inregistrate în sisteme similare. Asemenea statistici sunt, în

[6] The IT Governance Institute, 2001

general, dificil de obținut, iar frecvența pierderilor poate fi prea mică pentru a putea fi utilă sau nu poate fi aplicabilă unui sistem particular. În plus, incidentele privind pierderile din cadrul unui sistem sunt de obicei neraportate sau nedetectate.

CONCLUZII

Pe măsură ce organizaţiile devin din ce în ce mai dependente de buna funcţionare a sistemelor informaţionale, problema securităţii acestor sisteme devine din ce în ce mai importantă. Doar investind în securitate „cap-coadă" vom putea avea sisteme tehnologiilor informaționale mai sigure.

De multe ori vom constata că beneficiile vor fi mai mari, iar investiţiile şi eforturile făcute vor fi mai mici dacă vom avea o abordare pe ansamblu, decît dacă am trata problema punctual, sau, mai rău, vom acţiona pentru a înlătura efectele abia după producerea unui incident de securitate.

O bună practică ne învaţă că politicile de securitate trebuie aplicate la toate nivelurile ierarhice ale unei reţele de calculatore, nu doar la nivelul access, unde se regăsesc utilizatorii finali. De asemenea, utilizarea programelor de protecţie antivirus şi firewall pentru protejarea calculatoarelor şi serverelor este necesară la orice nivel al reţelei de date.

BIBLIOGRAFIE

[1] J. Habraken, „Reţele de calculatoare pentru începători", Editura BIC ALL, 2002.

[2] McClure Stuart, „Securitatea reţelelor", Editura Teora, 2002.

[3] E. Stancu, „Terorism şi Internet", revista „Pentru Patrie", nr. 12/2000, p. 26.

[4] D. Oprea, „ Sisteme informaţionale pentru afaceri", Editura Polirom, 2002.

[5] R. Daniel Zatu, „Reţele de calculatoare în era Internet", Editura Economică, 2002.

[6] D. Zaharie, „Proiectarea obiectuală a sistemelor informatice", Editura DualTech, 2003.

[7] http://www.securitatea-informatica.ro.

[8] http://ro.wikipedia.org/wiki/Sistem_informatic

[9] http://ro.wikipedia.org/wiki/Securitatatea_(calculatoare).

[10] www.scibd.com.

[11] www.bitdefender.ro