

# Protecția și securitatea informațiilor la nivelul autorităților publice naționale din România

Andreea-Maria TÎRZIU

Școala Națională de Studii Politice și Administrative  
Facultatea de Administrație Publică, Master Public Sector Management  
tirziu.andreea@yahoo.com

Anastasia CIUPERCA

Școala Națională de Studii Politice și Administrative  
Facultatea de Administrație Publică, Specializarea Administrație Europeană  
ciuperca.nastica@gmail.com

**Rezumat.** *Spațiul cibernetic se caracterizează prin anonimat, dinamism și lipsa frontierelor. Acest lucru generează atât oportunități de dezvoltare a societății informaționale, cât și riscuri la adresa funcționării acesteia la nivel individual, statal și interstatal. Asigurarea securității spațiului informatic devine o preocupare majoră a tuturor actorilor implicați, mai ales la nivel instituțional, unde se concentrează responsabilitatea elaborării și aplicării de politici coerente în domeniu, fapt care prevede necesitatea dezvoltării culturii de securitate cibernetică a utilizatorilor sistemelor informatice și de comunicații, utilizatori adesea insuficient informați în legătură cu potențialele riscuri, dar și cu soluțiile de contracarare a acestora. În consecință, una din premisele dezvoltării unei societăți sigure, sănătoase și puternice în România este prevenirea și combaterea riscurilor și amenințărilor la adresa securității cibernetice a țării. **Obiective:** Scopul acestei lucrări este acela de a oferi instituțiilor publice un exemplu de parcurs în vederea protecției și securității datelor de care dispun. **Metodologie:** Acest studiu se bazează pe literatura de specialitate în domeniul protecției și securității informatice. **Rezultate:** La final, reamintim faptul că securitatea informației distribuită în rețele de calculatoare nu este o problemă ce ține numai de tehnologie, aceasta constituind de asemenea o problemă umană și de management. **Valoare:** Cu cât autoritățile administrației publice vor pune mai mare accent pe securitatea informațiilor deținute, cu atât sistemele informatice utilizate de acestea vor fi mai sigure, în același timp asigurându-se și o protecție a funcționarilor instituțiilor respective.*

**Cuvinte-cheie:** protecția și securitatea informațiilor, confidențialitate, integritate, disponibilitate.

## 1. Introducere

*Pentru dezvoltarea planurilor operaționale, combinația de amenințări, vulnerabilități, precum și efectele acestora trebuie să fie evaluată pentru a identifica tendințe importante și a decide în cazul în care ar trebui să se depună eforturi în vederea eliminării sau a reducerii capacităților amenințărilor, a vulnerabilităților și trebuie să se evalueze, coordoneze și elimine conflictele tuturor operațiunilor spațiului cibernetic (The national strategy for cyberspace operations, citat de Locke, Gallagher, 2011, p. 1).*

În zilele noastre, societatea îmbrățișează din ce în ce mai mult tehnologia informației. Până nu demult, informația era transpusă pe hârtie, acum însă aceasta poate fi regăsită și sub formă electronică. Documentele oficiale se bazează încă pe informația pe suport de hârtie, în cazul în care este necesară o semnătură sau o stampilă. Adoptarea semnăturii electronice deschide însă perspectiva digitizării complete a documentelor, cel puțin din punct de vedere funcțional.

Calculatorul a devenit un instrument indispensabil și un mijloc de comunicare prin tehnologii precum poșta electronică sau rețelele de socializare, acest mod de lucru atrăgând după sine riscuri specifice. Pentru o gestiune corespunzătoare a documentelor în format electronic este necesară implementarea unor măsuri specifice de protecție și securitate a informațiilor. Aceste măsuri au menirea de a asigura protecția informațiilor împotriva pierderii, distrugerii sau divulgării către părți neautorizate. Cel mai sensibil aspect este cel care se referă la asigurarea securității informației gestionate de sistemele informatice în noul context tehnologic (Popa, 2007, pp. 5-6).

Securitatea informației este un concept de largă extindere și aplicabilitate care face referire la asigurarea integrității, confidențialității și a disponibilității informației. Datorită faptului că dinamica în domeniul IT induce noi riscuri, atât instituțiile publice, cât și organizațiile private trebuie să implementeze noi măsuri de control (Popa, 2007, pp. 5-6). De exemplu, popularizarea unităților de inscripționat CD-uri sau a memoriilor portabile de capacitate mare induce riscuri de copiere neautorizată sau furt de date. Conectarea la Internet și lucrul în rețea induc și acestea riscuri suplimentare, precum accesul neautorizat la date sau chiar fraudă.

Dezvoltarea tehnologică vine însoțită de soluții de securitate, producătorii de echipamente și aplicații incluzând metode tehnice de protecție din ce în ce mai performante. Totuși, în timp ce în domeniul tehnologiilor informaționale schimbarea este exponențială, componenta umană rămâne neschimbată. Asigurarea securității informațiilor nu se poate realiza exclusiv prin măsuri tehnice, fiind în principal o problemă umană. În acest scop, Parlamentul României a instituit o lege privind protecția informațiilor clasificate, prin intermediul căreia se atestă faptul că “protejarea acestor informații se face prin instituirea sistemului

național de protecție a informațiilor” (Legea nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate, publicată în M. Of. nr. 248/12 aprilie 2002, în vigoare din 11 iunie 2002; <http://www.sie.ro/>, accesat 6.11.2014). Despre cadrul legislativ privind securitatea informațiilor se va vorbi însă într-un alt capitol al acestei lucrări.

## 2. Noțiuni și concepte ale securității informațiilor

### 2.1. Definirea noțiunii de securitate informatică

Noțiunea de **securitate informatică** sau **cibernetică** este definită ca “starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic, a resurselor și serviciilor publice sau private din spațiul cibernetic” (*Strategia națională de dezvoltare a societății informaționale “Moldova Digitală 2020”*, pp. 23-24).

Acest concept al securității informaționale și-a făcut apariția simultan cu posibilitățile moderne prin care informația poate fi transferată și prelucrată. Instituțiile publice și companiile au ajuns la concluzia că acest bun virtual numit “informație” este, de multe ori, mai valoros decât bunurile materiale și că furtul, distrugerea, alterarea sau împiedicarea accesului la informație ar putea aduce prejudicii foarte mari. În prezent, din păcate, mediul informatic este încă unul în care atacuri de tipul celor enumerate anterior au loc destul de frecvent. Legislația în vigoare nu asigură o protecție prea mare împotriva unor astfel de atacuri, iar de multe ori atacatorii nu sunt prinși niciodată și prejudiciul provocat nu poate fi descoperit (*Conceptul de securitate*).

### 2.2. Structura conceptului de securitate

Conceptul de securitate are o întindere extinsă însă, pentru simplificarea lui, acesta poate fi structurat pe trei niveluri:

1) **Securitatea fizică** → reprezintă nivelul “exterior” al securității, ce constă în prevenirea, detectarea și limitarea accesului direct asupra bunurilor, valorilor și informațiilor. Pentru a da un exemplu, putem observa că într-un sistem distribuit, prima măsură de securitate care trebuie luată în considerare este chiar securitatea fizică, care se realizează prin prevenirea accesului fizic la echipamente: un anumit infractor care dorește să sustragă informații din sistem trebuie, mai întâi, să intre în contact fizic cu echipamentul. În afara acestor aspecte, securitatea fizică implică de asemenea și luarea măsurilor de protecție împotriva incendiilor, inundațiilor, scăpărilor de gaze și a calamităților naturale, toate aceste măsuri fiind în strânsă legătură cu protecția, în ansamblu, a clădirilor împotriva pericolelor potențiale. În momentul de față, distrugerile de informații datorate vulnerabilității nivelului de securitate fizică sunt considerate a reprezenta cel mai mare procent de insecuritate (Sebastiao, 2007).

2) **Securitatea logică** → este reprezentată de totalitatea metodelor ce asigură controlul asupra accesului la resursele și serviciile sistemului. Acest tip de securitate poate, la rândul lui, să fie împărțit în două mari niveluri (Sebastiao, 2007):

- a) nivelul de securitate a accesului;
- b) nivelul de securitate a serviciilor.

Securitatea accesului are ca principale componente (Sebastiao, 2007):

- accesul la sistem: care este răspunzător de gradul de accesibilitate al utilizatorilor în sistem, de cuplarea sau decuplarea unor stații;
- accesul la cont: care verifică dacă utilizatorul are un profil valid pentru sistem;
- drepturile de acces: după ce utilizatorul trece cu bine de cele două componente enunțate anterior, acesta va primi de la sistem anumite drepturi de conectare.

Securitatea serviciilor este alcătuită din următoarele elemente (Sebastiao, 2007):

- controlul serviciilor: control care este răspunzător de funcțiile de raportare a stării serviciilor și, respectiv, de avertizare;
- drepturile deținute la serviciu: care determină modul de utilizare a unui anumit cont de servicii.

3) **Securitatea juridică** → reprezintă nivelul constituit dintr-o colecție de legi naționale care au rolul de a reglementa actul de violare a primelor două niveluri de securitate menționate mai sus și de a stabili sancțiuni penale pentru aceste acte (*Conceptul de securitate*).

Sistemul de securitate fizică trebuie conceput în așa fel încât să permită o analiză posteveniment care să poată fi utilizată drept “martor” în procesul de realizare a obiectivului de securitate juridică. Cele trei niveluri de securitate determină, la un moment dat, securitatea în ansamblu a obiectivului protejat. Se poate constata așadar că între aceste niveluri de securitate există o puternică interconectare, acestea influențându-se reciproc, iar în anumite situații, determinându-și existența ca nivel de securitate valid (*conceptul de securitate*).

Cele menționate până acum în cadrul lucrării demonstrează faptul că cea mai eficientă soluție pentru asigurarea securității este reprezentată de analiza globală a gradului de securitate oferit de fiecare nivel în parte și compensarea acelui nivel care, la un moment dat, oferă un grad de securitate mai scăzut, aplicând măsuri ferme de creștere a securității celorlalte două niveluri sau numai a unuia dintre ele astfel încât protecția obiectivului să fie mai mare sau egală cu un grad minim necesar.

### 2.3. Concepte ale securității informatice: confidențialitate, integritate, disponibilitate

Securitatea referitoare la IT și la informație este, în mod normal, definită de trei aspecte, și anume: confidențialitatea, integritatea și disponibilitatea. Aceste concepte pot fi văzute ca obiective ale securității informatice și sunt adesea menționate ca *the CIA triad (Fundamental Security Concepts, pp. 4-6)*. Definiții ale acestei triadei pot diferi în funcție de activele pe care se concentrează. Drept exemplu, putem lua un calculator specific sau un sistem IT, un sistem de informații sau active de informare precum cele enunțate anterior.

În ceea ce privește obiectivele securității informatice, cele trei concepte pot fi definite după cum urmează:

1) **Confidențialitatea**, uneori numită secretizare, își propune să interzică accesul neautorizat al persoanelor la informația care nu le este destinată (Baltac, 2011, 129). Încă din cele mai vechi timpuri, omenirea a știut că informația înseamnă putere, iar în epoca informațională în care ne aflăm, accesul la informație este mai important decât oricând. Accesul neautorizat la informații confidențiale poate avea consecințe grave, nu numai în aplicațiile de securitate la nivel național, cât și în comerț și industrie. Principalele mecanisme de protecție a confidențialității în sistemele informatice sunt controalele criptografie și de acces (*Fundamental Security Concepts, p. 4*). Ca exemple de amenințări la adresa confidențialității, ne putem referi la următoarele: *malware*, intruși, inginerie socială, rețele nesigure, precum și sisteme administrate necorespunzător. Țări precum Statele Unite, Canada, Australia, Japonia și altele au reglementat prin lege controlul confidențialității.

2) **Integritatea**, numită uneori acuratețe, face referire la încrederea, originea, deplinătatea și corectitudinea informațiilor, precum și la prevenirea modificării necorespunzătoare sau neautorizate a datelor (Baltac, 2011, 129). În contextul securității informațiilor, integritatea se referă nu numai la integritatea informației în sine, ci și la originea acesteia, mai exact la integritatea sursei informației respective. Mecanismele de protecție a integrității pot fi grupate în două mari categorii (Oscarson, 2003, pp. 4-5):

a) mecanisme de prevenire → cum ar fi: controale de acces care să împiedice modificarea neautorizată de informații;

b) mecanisme de detectare → care au scopul de a detecta modificarea neautorizată, atunci când mecanismele de prevenire au eșuat în rolul lor.

3) **Disponibilitatea** reprezintă obiectivul care își propune ca datele stocate în calculatoare să poată fi accesate de persoanele autorizate. Utilizatorii trebuie să aibă acces doar la datele care le sunt destinate. Se pot distinge aici două categorii de utilizatori, cu drepturi de acces diferite: administratorii de sistem și utilizatorii generali, excepție făcând sistemele de operare care echipează calculatoarele desktop. Orice utilizator general este abilitat să schimbe configurările de securitate ale calculatorului sau chiar să le anuleze (*Fundamental Security Concepts, pp. 5-6*).

Pe lângă aceste trei obiective ale securității informațiilor, în literatura de specialitate se specifică și un al patrulea termen. Este vorba despre **nerepudiere**, care își propune să confirme destinatarului unui mesaj electronic faptul că acest mesaj este scris și trimis de persoana care pretinde că l-a trimis, asigurându-se astfel relația de încredere între părți. Expeditorul nu poate să nege că el este cel care a trimis mesajul (Baltac, 2011, p. 129). Nerepudierea stă la baza semnăturilor digitale, asigurând autenticitatea acestora, în noua piață a comerțului electronic – “E-Commerce” (*Techopedia dictionary*).

### 3. Cadrul legislativ privind protecția și securitatea informațiilor

Controalele interne pot fi considerate principiile care stau la baza implementării unui sistem de management al securității (Popa, 2007, p. 8). Chiar dacă astfel de măsuri pot avea surse variate, punctul de plecare într-un demers de acest gen este reprezentat de legislația aplicabilă. Este necesar și foarte important ca persoana care se ocupă de implementarea unui sistem de management al securității să aibă cunoștințe despre cerințele legislative în vigoare:

- Legea nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, publicată în M. Of. nr. 279/21 aprilie 2003 (actualizată la data de 22 aprilie 2011, cu modificări ulterioare);
- Legea nr. 506 din 17 noiembrie 2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, publicată în M. Of. nr. 1101/25 noiembrie 2004;
- Legea nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, publicată în M. Of., Partea I, nr. 790/12 decembrie 2001 (modificată prin Legea nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările și completările ulterioare, și OUG nr. 36/2007 pentru abrogarea Legii nr. 476/2003 privind aprobarea taxei de notificare a prelucrărilor de date cu caracter personal);
- Legea nr. 455 din 18 iulie 2001 privind semnătura electronică, publicată în M. Of. nr. 429/31 iulie 2001 și republicată în M. Of. nr. 316/30 aprilie 2014;
- Legea nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public, publicată în M. Of. nr. 663/23 octombrie 2001;
- Hotărârea nr. 1259 din 13 decembrie 2001 privind aprobarea normelor tehnice și metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronică, publicată în M. Of. nr. 847/28 decembrie 2001;
- Ordinul Avocatului Poporului nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal, publicat în M. Of. nr. 383/5 iunie 2002;

- Ordinul Avocatului Poporului nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, publicat în M. Of. nr. 383/5 iunie 2002;

- Ordinul Avocatului Poporului nr. 54 din 18 aprilie 2002 privind stabilirea unor situații în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidența Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, publicat în M. Of. nr. 383/5 iunie 2002;

- Hotărârea nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu, publicată în M. Of., Partea I, nr. 575/5 august 2002;

- Legea nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate, publicată în M. Of. nr. 248/12 aprilie 2002.

Pe lângă legislația internă, trebuie luate în considerare și convențiile internaționale și reglementările europene semnate de România sau la care aceasta este parte. Selectarea controalelor trebuie să țină cont de specificul instituției publice sau organizației. Nu toate recomandările pot fi aplicate, așa cum nu toate pot fi justificate din punct de vedere al costurilor. Eficacitatea sistemului de securitate depinde de următoarele elemente (Popa, 2007, pp. 8-9):

- stabilirea unor obiective de securitate care să reflecte cerințele instituției sau organizației;
- sprijinului conducerii;
- existența abilităților necesare realizării analizei riscurilor, a vulnerabilităților și a analizei de impact;
- instruirea angajaților;
- monitorizarea controalelor implementate.

#### **4. Cadrul instituțional privind protecția și securitatea informațiilor**

Atât instituțiile publice, cât și organizațiile private trebuie să conștientizeze riscurile asociate cu utilizarea tehnologiei și gestionarea informațiilor și să abordeze pozitiv acest subiect printr-o conștientizare, în rândul angajaților, a importanței securității informațiilor și a înțelegerii tipologiei amenințărilor, riscurilor și vulnerabilităților specifice mediilor informatizate și, nu în ultimul rând, a aplicării practicilor de control.

În perioada 14-26 octombrie 1946, în Londra a avut loc întrunirea de organizații naționale de norme din 25 de țări. Acesta a constituit momentul în care s-a luat decizia de a se înființa o nouă organizație, și anume ISO (*International Organization for Standardization*), care și-a început activitatea în data de 23 februarie 1947 (<http://www.certificareiso.ro/>, accesat 9.11.2014). Organizația Internațională de Standardizare – ISO este o confederație internațională care se

ocupă cu stabilirea normelor în toate domeniile, excepție făcând domeniul electricității și cel al electronicii – acestea fiind reprezentate de IEC (*International Electrotechnical Commission*), și de cel al telecomunicațiilor – reprezentat de ITU (*International Telecommunication Union*). Cele trei organizații menționate anterior sunt unite în WSC (*World Standards Cooperation*) (<http://www.iso.org/>, accesat 9.11.2014).

ISO cooperează în strânsă legătură cu Comisia Electrotehnică Internațională (IEC), care este responsabilă pentru standardizarea echipamentelor electrice și electronice, aceste două organizații alcătuind un forum specializat pentru standardizare. Organismele naționale care sunt membre ale ISO și IEC participă la dezvoltarea standardelor internaționale prin intermediul comitetelor tehnice. Statele Unite ale Americii, prin Institutul Național de Standardizare, ocupă poziția de Secretar, 24 de țări au statut de Participanți și alte 40 de țări au statut de Observatori (Popa, 2007, p. 5).

Ministerul pentru Societatea Informațională îndeplinește rolul de adoptare, la nivel național, a standardelor europene și internaționale recunoscute. Prin această activitate a ministerului, standardul ISO/IEC 17799: “Tehnologia Informației – Cod de bună practică pentru managementul securității informației” a fost adoptat și în România de către Asociația de Standardizare din România (ASRO, fostul IRS), în toamna anului 2004. Specialiștii ASRO participă în cadrul comitetelor tehnice internaționale ale Organizației Internaționale de Standardizare. Standardul ISO este recunoscut în rezoluțiile Consiliului Europei, implementarea acestuia la nivelul instituțiilor și al organizațiilor fiind însă opțională (Popa, 2007, p. 6).

#### **4.1. Organisme naționale cu atribuții în domeniul securității informatice**

Consiliul Suprem de Apărare a Țării reprezintă autoritatea care coordonează, la nivel strategic, activitatea Sistemului Național de Securitate Cibernetică (SNSC) (<http://csat.presidency.ro/>, accesat în data de 9.11.2014). Prin Ministerul pentru Societatea Informațională, Guvernul României este cel care asigură coordonarea celorlalte autorități publice în vederea realizării coerenței politicilor și a implementării strategiilor guvernamentale în domeniu.

Sistemul Național de Securitate Cibernetică include, pe lângă autoritățile publice cu competențe în materie (Serviciul Român de Informații, Ministerul Apărării Naționale, Ministerul Afacerilor Interne, Ministerul Afacerilor Externe, Ministerul pentru Societatea Informațională, Serviciul de Telecomunicații Speciale, Serviciul de Informații Externe, Serviciul de Protecție și Pază, Oficiul Registrului Național pentru Informații Secrete de Stat, precum și Secretarul Consiliului Suprem de Apărare a Țării), actori din mediul asociativ neguvernamental, profesional și de afaceri (*Legea privind securitatea cibernetică a României*, <http://www.cdep.ro/>, accesat 9.11.2014).



Mecanismul de implementare a strategiei de securitate cibernetică la nivel național este asigurat prin:

- Consiliul Operativ de Securitate Cibernetică (COSC), al cărui regulament de organizare și funcționare a fost aprobat prin Hotărârea CSAT nr. 17/2013. Acesta este format din reprezentanți la nivel de secretar de stat din cadrul instituțiilor sistemului de securitate națională, inclusiv ai MAE și care se ocupă de coordonarea unitară a SNSC. Funcția de coordonator tehnic al COSC este asigurată de către Serviciul Român de Informații în calitate de autoritate națională în domeniul securității cibernetice prin intermediul Centrului Național Cyberint (CNC), care informează operativ COSC cu privire la apariția incidentelor de tip cibernetic care pot aduce atingere securității naționale. Consiliul raportează către CSAT, anual sau când situația o impune, cu privire la acțiunile întreprinse, precum și la evoluțiile înregistrate în spațiul cibernetic, în special cu referire la incidente sau atacuri cibernetice (*Strategia de securitate cibernetică a României*).

- Grupul de Suport Tehnic (GST), care are în alcătuirea sa reprezentanți la nivel de expert din cadrul instituțiilor sistemului de securitate națională reprezentate în cadrul COSC (*Strategia de securitate cibernetică a României*).

SRI deține, în structura sa, Centrul Național de Securitate Cibernetică (CNSC) care, în cazul în care are loc un atac cibernetic asupra securității informatice a României, reprezintă punctul de contact pentru relaționarea cu organisme similare din străinătate (<http://www.sri.ro/>, accesat 9.11.2014).

Un alt suport în domeniul securității cibernetice este reprezentat de Sistemul Național de Alertă Cibernetică (SNAC), care instituie nivelurile de alertă cibernetică (NAC), pe baza evaluării procesului de management al riscurilor la adresa securității cibernetice a României. Coordonarea tehnică a activității SNAC și controlul măsurilor specifice fiecărui nivel de alertă, propuse în cadrul COSC și aprobate de CSAT, se realizează de către Centrul Național Cyberint (CNC) (*Legea securității cibernetice a României*, <http://www.mcsi.ro/>, accesat 9.11.2014).

Structura independentă de expertiză și cercetare-dezvoltare în domeniul protecției infrastructurilor cibernetice – CERT-RO, dispune de capacitatea necesară pentru prevenirea, analiza, identificarea și reacția la incidentele de securitate cibernetică ale sistemelor informatice ce asigură funcționalități de utilitate publică sau servicii ale societății informaționale (<http://www.cert-ro.eu/>, accesat 9.11.2014). CERT-RO este coordonat de Ministerul pentru Societatea Informațională, fiind finanțat integral de la bugetul de stat. Conform H.G. nr. 494/2011 publicată în M. Of. nr. 388/2 iunie 2011, act normativ ce reglementează activitatea structurii, acest centru putând emite alerte și atenționări cu privire la activități premergătoare atacurilor informatice.

## 5. Riscurile principale cu privire la server și la client/factor uman

### 5.1. Partea de server

Pentru nimeni nu mai este un mister care este sarcina de bază a unui răufăcător: aceea de a înfăptui, cu orice preț, operațiuni la distanță pe serverul atacat. Prima acțiune pe care o va întreprinde un agresor va fi aceea de a scana serverul pe porturi deschise\*. Acesta va introduce programul *Nmap*\* și astfel va putea vedea starea porturilor de pe server. Cu cât sunt deschise mai multe porturi, cu atât probabilitatea unui atac este mai mare. Deja în această etapă acțiunile sunt considerate a fi o încercare de acces neautorizat, filtrând fluxurile firewall\* cu ajutorul programelor specializate, un exemplu de astfel de program fiind *PortSentry*. Dacă serverul *DMVs*\* are acces la Internet și la rețeaua internă, și serverul *FTP*\* este folosit doar de utilizatori din rețeaua internă, atunci nu este nevoie să fi conectat și în afara rețelei, fiind suficient să programezi *firewall*-ul astfel încât accesul să fie disponibil doar pentru *IP*-uri interne (Tișinkov, <http://xn-b1afjrvh2f.xn--p1ai/attachments/article/63/NetworkSecurity.pdf>, accesat 9.11.2014).

\* Porturi deschise. Un sistem de operare poate să primească simultan sute, mii sau chiar zeci de mii de pachete TCP (Transmission Control Protocol) pe secundă și trebuie să stabilească rapid cărei conexiuni îi aparține fiecare pachet înainte de a face orice altceva. Porturile sunt necesare pentru a da posibilitatea sistemului de operare să deosebească conexiunile între ele. Orice port este deschis de către o aplicație care așteaptă cereri de la clienți.

\* Nmap. Nmap Network Scanning reprezintă o tehnică de scanare de porturi. Pentru mai multe informații, a se vizita <http://nmap.org/>, accesat în data de 9.11.2014.

\* Firewall este un soft sau un dispozitiv care funcționează ca barieră/filtru între calculatoare. Pentru o definiție mai detaliată, a se vizita <http://muntealb.orgfree.com/Traduceri/dictionar-traducere.htm#F>, accesat în data de 9.11.2014.

\* DMVs. Dynamic management views în SQL Server 2005 sunt concepute pentru a oferi transparență în ceea ce privește interiorul unui server SQL. Ele pot oferi informații cu privire la ceea ce se întâmplă în prezent în interiorul serverului, precum și la obiectele pe care le-a depozitat. Acestea sunt concepute pentru a fi folosite în loc de tabele de sistem și diferitele funcții prevăzute în SQL Server 2000. DMVs conțin de fapt ambele puncte de vedere și funcții de prim rang. Unele se aplică întregului server și sunt stocate într-o bază de date, altele sunt specifice fiecărei baze de date. Toate sunt stocate în schema *sys* și toate încep cu *dm\_* în nume.

\* FTP. File Transfer Protocol este un instrument important al Internetului. În rețelele de calculatoare și Internet, apare frecvent nevoia de a transfera fișiere de la un calculator la altul. FTP reprezintă un protocol care permite realizarea acestui lucru, deși fișierele se pot afla pe calculatoare ce folosesc alt tip de rețea decât cea a destinatarului sau chiar cu sisteme de operare diferite. Pentru mai multe informații, a se consulta Baltac, V., *Tehnologiile informației – noțiuni de bază*, Andreco Educațional, București, 2011, pp. 210-212.

Primind lista cu porturi deschise, agresorul va verifica versiunea serviciilor folosite de porturile respective, conectându-se pe rând la ele prin *telnet*. Acesta reprezintă un protocol de rețea care este folosit – în Internet, precum și în rețele de calculatoare de tip LAN (*Local Area Network* – rețea locală reprezentată de un

ansamblu de mijloace de transmisiune și de sisteme de calcul folosite pentru transportarea și prelucrarea informației) – la comunicarea textuală, bidirecțională și interactivă, bazată pe realizarea unei conexiuni virtuale cu stația de lucru destinată (http://www.eed.usv.ro/~mahalu/Curs/lectia06.html, accesat 9.11.2014; Baltac, 2011, p. 210).

Multe instituții publice și companii irosesc sume foarte mari pentru a asigura securitatea rețelelor informatice, însă nu acordă suficientă atenție accesului fizic al persoanelor. E posibil ca noul angajat să fie *hacker* sau angajat al unei instituții sau companii concurente. Astfel, având acces fizic la calculator și timp la dispoziție, acesta poate cu ușurință să ocolească programele de securitate.

## 5.2. Partea de client/factor uman

În ceea ce privește clientul/factorul uman, riscurile se pot constitui în două situații:

a) Utilizatorul singur se privează de confidențialitate, în urma instalării programelor “afectate” sau prin răspândirea informațiilor personale pe Internet. *Malware-ul\** activat de utilizator, cu ajutorul căruia răufăcătorul poate pătrunde de la distanță în calculator, se numește Trojan\*. În acest caz, putem considera drept exemplu programul *Back Orifice\**, a cărui instalare pe o platformă Windows se realizează după cum urmează:

- În registrul de system, la secțiunea HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\opțiune Run Services, subtitlul “(Implicit)” {"(Default)"} (uneori altul) apare fișierului *Back Orifice* care, de obicei, emite conținutul “.exe”;
- În directorul de sistem (C:\Windows\system), apare o copie a *Back Orifice* cu numele specificat în registru, de obicei “.exe” (http://web.archive.org/web/20100405225933/http://www.relcom.ru/Archive/2000/TechSupport/Advices/BO/, accesat 9.11.2014).

\* Malware este o categorie de programe care se instalează în calculatorul-țintă pentru a afla date despre posesor și preferințele acestuia (programe de spionare sau spyware) sau cu scopul de a afișa anumite mesaje de tip publicitar, în principal prin generarea de ferestre suplimentare pe ecran (pop-up), sau de tip virus informatic. Pentru mai multe informații despre această noțiune, a se vedea Baltac, V., *Tehnologiile informației – noțiuni de bază*, Andreco Educațional, București, 2011, p. 91, pp. 139-140.

\* Virusul de tip Trojan accesează fișierele calculatorului prin conexiunea la rețea. Acesta se mai numește și RAT (*Remote Administration Trojan*).

\* Back Orifice (BO) este un controversat program de calculator conceput pentru administrarea sistemului de la distanță. Acesta permite unui utilizator să controleze un calculator care rulează sistemul de operare Microsoft Windows de la o locație la distanță. Numele este un joc de cuvinte pe baza software-ului Microsoft BackOffice Server. Pentru mai multe informații, a se vizita http://searchmidmarketsecurity.techtarget.com/, accesat în data de 9.11.2014.

Calculatorul virusat poate fi ușor coordonat de răufăcător, astfel existând diferiți „cai troieni” pe domenii restrânse, de dimensiuni mici (6kb), utilizați pentru a paraliza clientul și a răspândi *spam*-ul. Trebuie deci avute în vedere căile de acces ale acestui virus prin directă participare a utilizatorului, acestea fiind de trei tipuri: ISQ (mesagerie instanță), prin intermediul poștei electronice sau prin directă descărcare a programelor virusate. În primul caz, descărcând o poză de pe Internet cu denumirea “foto.jpg”, poate fi de fapt descărcată o fotografie de tip “foto.jpg.exe”, aceasta reprezentând o fotografie care are “lipit” un program troian (această metodă este una arhaică, însă cu toate acestea nu trebuie scoasă din calcul). În al doilea caz, pe e-mail sunt trimise scrisori cu diverse conținuturi, sunt atașate link-uri unde, după cerința scrisorii, trebuie introduse date personale. În ultimul caz, sunt utile regulile elementare de descărcare de pe Internet: folosirea site-urilor cu un grad mare de protecție, citirea cu atenție a conținutului fișierelor etc.

Un exemplu de fraudă cibernetică este cea numită *phishing*. Scopul acestui tip de escrocherie este acela de a afla informații, cum ar fi: parole, carduri de credit, conturi bancare ș.a.m.d. Esența acestui tip de fraudă este următoarea: O scrisoare vine de la “furnizorul de banca” sau de la orice altă organizație în care se cere transmiterea de informații cu caracter personal, sub pretextul defectării sistemului, pierderii informațiilor etc. De cele mai multe ori, scrisoarea conține un link către un site similar (Mazanec, 2014, pp. 69-70).

b) Poate exista o eroare în structurile de bază, prin acest intermediu răufăcătorul având acces la informații. Principalul element vulnerabil al răspândirii erorii este *Microsoft Internet Explorer* și derivații săi. În acest caz, atacul începe cu primirea de e-mailuri care conțin link-uri către site-uri malițioase, pentru care *hackerii* folosesc *Active Scripting*\*. În popularele aplicații de e-mail, cum ar fi *Microsoft Outlook*, *Microsoft Outlook Express* și *Windows Mail*, nu se obișnuiește folosirea unor astfel de componente, dar în privința altor aplicații utilizatorul devine vulnerabil.

\* *Active Scripting* (cunoscut anterior ca *ActiveX Scripting*) este tehnologia utilizată în Windows în vederea punerii în aplicare a programării calculatoarelor bazată pe componente. Aceasta se bazează pe COM (Component Object Model – un standard de interfață binară pentru componente software introduse de Microsoft în 1993) și permite instalarea de motoare suplimentare de programare sub formă de module COM.

## 6. Studiu de caz: Consolidarea societății informaționale în România – cooperarea dintre sectorul public, mediul de afaceri și societatea civilă.

În anul 2008, fenomenul infraționalității informatice a cunoscut o evoluție extrem de puternică la nivel mondial. La nivel național, conform unei statistici întocmite de Direcția Generală de Combatere a Criminalității Organizate

(DGCCO) din cadrul Poliției Române, valoarea prejudiciilor cauzate de infracțiuni informatice s-a ridicat la cinci milioane de euro, cea mai mare parte aparținând fraudelor cu carduri. Previțiunile pentru anul 2009 nu au fost tocmai optimiste, pierderile fiind estimate la aproximativ 500 milioane de euro (<http://www.politiaromana.ro/>, accesat 9.11.2014).

„România are un nivel scăzut al managementului securității informatice” – așa începea, în 2009, un articol publicat pe site-ul Bursa On Line (<http://www.bursa.ro/>, accesat 9.11.2014). În perioada 25-26 mai a aceluiași an avea loc, la București, conferința *CyberSecurity*, în cadrul căreia specialistul în securitatea informației al Serviciului Român de Informații (SRI), Eduard Bîscanu, declara faptul că în România nu sunt operaționale organisme civile specializate pentru detectarea și analiza incidentelor sau atacurilor informatice, țara noastră având “un nivel scăzut de dezvoltare și interoperabilitate a sistemelor de management al incidentelor de securitate informatică”. Tot în cadrul evenimentului *CyberSecurity*, reprezentantul SRI a avansat ideea înființării unui nou birou, intitulat *Cyber Intelligence*, prin intermediul căruia să poată fi aflate date importante în vederea anticipării atacurilor de natură informatică (<http://www.immromania.ro/>, accesat 9.11.2014).

România este considerată, în principal, țară furnizoare de criminalitate informatică, aceasta amplificându-se și pe plan intern, în special prin operațiunile de fraudare a sistemului de achiziții online, a ATM-urilor\* și POS-urilor\*, precum și a aparatelor electronice de jocuri de noroc. Lupta împotriva criminalității informatice a dus la destructurarea, în anul 2012, a 35 de grupuri organizate cu preocupări infracționale în zona cyber-criminalității, 286 de persoane fiind trimise în judecată, dintre care 154 aflându-se în stare de reținere/arestare (*Evaluarea activității desfășurate de Ministerul Afacerilor Interne în anul 2012*).

\* Asynchronous Transmission Mode (ATM) este un protocol de transmisie și multiplexare a datelor de mare viteză.

\* Point of Sale (POS) reprezintă terminale de colectare a datelor folosite de personalul de execuție al unei instituții sau organizații.

În anul 2010, pe data de 4 noiembrie, România a participat la primul exercițiu paneuropean privind protecția infrastructurilor informatice critice, numit *Cyber Europe 2010*, experții europeni testând, cu această ocazie, sistemele de apărare împotriva atacurilor cibernetice (<http://www.enisa.europa.eu/>, accesat 9.11.2014). Acest exercițiu a constituit o parte a măsurilor prevăzute de Agenda Digitală pentru Europa (*Digital Agenda: cyber-security experts test defences in first pan-European simulation*, 2010), strategie lansată de Comisia Europeană în vederea creșterii încrederii în Internet și a îmbunătățirii securității rețelelor. Potrivit Ministerului pentru Societatea Informațională (MCSI), scenariul

exercițiului *Cyber Europe 2010* a prevăzut pierderea treptată sau reducerea considerabilă a conexiunilor Internet dintre țările europene și, în cel mai rău caz, anularea efectivă a principalelor conexiuni de tip transfrontalier din Europa. Această simulare a avut menirea de a testa capacitatea de răspuns a țărilor membre ale Uniunii Europene în fața unor incidente majore care pot afecta infrastructurile informatice critice (<http://www.mcsi.ro/>, accesat 9.11.2014), fiind organizată de statele membre ale UE, cu sprijinul Agenției Europene pentru Securitatea Rețelelor și a Informației (ENISA) și a Centrului Comun de Cercetare (JRC), la acest exercițiu de simulare participând și reprezentanți ai Centrului Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO), ai departamentului de specialitate din cadrul Institutului Național de Cercetare-Dezvoltare în Informatică (ICI), ai departamentelor de specialitate ale Ministerului Administrației și Internelor și ale Serviciului de Telecomunicații Speciale, precum și experți europeni în securitate informatică.

În 25 februarie 2014 a fost publicat un comunicat de presă privind finalizarea proiectului „Implementarea unui sistem de apărare cibernetică la nivelul Ministerului Afacerilor Interne prin Departamentul Informații și Protecție Internă (CERT-INT)”, acest proiect fiind cofinanțat din Fondul Social European prin Programul Operațional Dezvoltarea Capacității Administrative 2007-2013 și având ca obiectiv general îmbunătățirea capacității DIPI de a contribui la formularea politicilor în domeniul protecției informațiilor din spațiul cibernetic, prin asigurarea unui mecanism unitar de reacție și răspuns la incidente de securitate la sistemele informatice din cadrul Ministerului Afacerilor Interne (<http://www.dgipi.ro/>, accesat 9.11.2014). Dotarea cu echipamente informatice și pregătirea de specialiști care vor utiliza și administra sistemul integrat de management al infrastructurii, au reprezentat beneficii importante obținute în cadrul proiectului cu o durată de implementare de 27 de luni, având ca beneficiar personalul DIPI.

Departamentul Informații și Protecție Internă a mai implementat niște proiecte în scopul perfecționării și adaptării metodelor de lucru ale instituției pentru eficientizarea activităților desfășurate și pregătirea personalului, acestea fiind enumerate mai jos:

- Proiectul SIMITO (“Sistemul Național Integrat de Management al Informației și al Activității Tactico-Operative la nivelul Departamentului de Informații și Protecție Internă”) → care oferă instituției posibilitatea de a beneficia de sisteme informatice moderne, ce permit un proces de analiză și de coroborare a informațiilor primare, obținute la toate nivelurile, transformarea informațiilor singulare în produse analitice de calitate superioară, necesare pentru fundamentarea managementului decizional în domeniul politicilor și strategiilor naționale de securitate și ordine publică (<http://www.dgipi.ro/>, accesat 9.11.2014).

- Proiectul „Optimizarea activității de pregătire profesională în cadrul DIPI în sistem E-Educație” → care, la nivel operațional, reprezintă un sistem modern de îmbunătățire a pregătirii personalului. Acest proiect a obținut două nominalizări în finala European IT & Software Excellence Awards 2014, la categoriile dedicate proiectelor care au ca obiectiv eficientizarea activității derulate de instituțiile publice (<http://www.dgipi.ro/>, accesat 9.11.2014).
- Proiectul IMMEDIAT la DIPI („Instrumente moderne de management electronic al documentelor interne și activității din teritoriu la Departamentul de Informații și Protecție Internă”) → prin intermediul căruia a fost implementat un sistem informatic modern, la nivel național, ca suport de secretariat și gestiune a documentelor, având drept scop îmbunătățirea politicilor și a proceselor interne de lucru cu documentele (<http://www.dgipi.ro/>, accesat 9.11.2014).

România a fost, în perioada 21-22 mai 2013, gazda europeană în securitate informatică pentru desfășurarea unui *workshop* organizat de către Agenția ARNIEC/RoEduNet\*, în parteneriat cu ENISA\*. Peste 150 de experți în securitate informatică și oficiali guvernamentali din Uniunea Europeană și din SUA au venit la București pentru a dezbate cele mai noi soluții privind prevenirea și combaterea fenomenului de criminalitate informatică. România a ales să fie gazda evenimentului, în contextul dezvoltării din ultimii ani a relațiilor de cooperare între instituțiile de profil din țară și cele deja existente la nivel european. Printre participanții la aceste dezbateri s-au aflat oficiali din structurile naționale și guvernamentale (CERT – Computer Emergency Response Team), structuri care se ocupă de protecția instituțiilor conectate la rețelele naționale de comunicații și de asistență tehnică în tratarea incidentelor privind securitatea informatică (<https://www.csirt.ro/>, accesat 9.11.2014).

\* Agenția ARNIEC/RoEduNet (Agenția de Administrare a Rețelei Naționale de Informatică pentru Educație și Cercetare), aflată în subordinea Ministerului Educației Naționale, administrează și dezvoltă rețeaua RoEduNet care asigură servicii de comunicații de date pentru instituțiile de cercetare și academice de toate gradele din România. Agenția este membru al consorțiului european GEANT, rețeaua care interconectează toate rețelele pentru educație și cercetare din statele membre ale Uniunii Europene.

\* ENISA (The European Network and Information Security Agency) este agenția responsabilă de activitățile de securitate informatică din cadrul Uniunii Europene, deservind atât instituțiile Uniunii Europene, cât și pe cele ale statelor membre. ENISA este un centru de expertiză care definește și promovează standardele de securitate informatică în Europa.

În perioada 23-24 mai a aceluiași an a avut loc, la București, cea de-a 39-a întâlnire a TI\* și a TF-CSIRT\*, acestea reprezentând două grupuri de lucru constituite la nivel european, care au rolul de a susține și îmbunătăți colaborarea

în domeniul securității informatice, precum și de a combate incidentele de criminalitate în domeniul discutat (<https://www.csirt.ro/>, accesat 9.11.2014).

\* TI (Trusted Introducer) este un serviciu de cooperare, comunicare și recunoaștere a echipelor de tip CERT, fondat în anul 2000 de către membrii comunității CERT din Europa, care are ca scop dezvoltarea și facilitarea comunicării și cooperării membrilor săi.

\* TF-CSIRT este grupul de lucru pe probleme de securitate informatică a TERENA (The Trans-European Research and Education Networking Association), asociația rețelelor pentru educație și cercetare din Europa, ce oferă cadrul în care acestea inovază și schimbă cunoștințe menite să dezvolte tehnologiile, infrastructura și serviciile de acces la Internet folosite de comunitățile de cercetare și educație.

În ziua de 30 octombrie 2014 a fost realizat exercițiul *Cyber Europe 2014*, fiind considerat cel mai amplu și complex exercițiu de acest gen organizat în Europa. Peste 200 de organizații și 400 de specialiști în materie de securitate cibernetică din 29 de țări europene au verificat, în cadrul acestei simulări de o zi, organizată de Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA), cât de pregătite/pregătiți sunt să facă față atacurilor informatice. În cadrul scenariului de securitate cibernetică, experții din sectorul public și din cel privat (printre care agenții de securitate cibernetică, centre de răspuns la incidente de securitate cibernetică, ministere, societăți de telecomunicații, societăți energetice, instituții financiare și furnizori de servicii de Internet) au avut ocazia să-și testeze procedurile și capacitățile de a face față pericolelor în rețea (<http://ec.europa.eu/>, accesat 9.11.2014).

În vederea asigurării securității informațiilor, dezvoltarea cooperării dintre mediul public și cel privat reprezintă o direcție prioritară de acțiune la nivelul organismelor internaționale sau al alianțelor din care România face parte, luând în considerare faptul că spațiul cibernetic reunește deopotrivă infrastructuri cibernetică deținute și administrate de stat, precum și de entități private.

În ceea ce privește dinamismul evoluțiilor globale în spațiul cibernetic, precum și obiectivele României în procesul de dezvoltare a societății informaționale și implementare pe scară largă a serviciilor electronice, putem observa că, la nivel național, este necesară implementarea unor standarde minimale procedurale și de securitate pentru infrastructurile informatice, prin intermediul cărora să se fundamenteze eficiența demersurilor de protecție față de atacuri cibernetică și să se limiteze riscurile producerii unor incidente cu potențial impact semnificativ.

Autoritățile publice care au responsabilități în acest domeniu vor fi nevoite să aloce resursele financiare necesare asigurării protecției și securității informațiilor prin intermediul politicilor de planificare. Pentru asigurarea unei capacități sporite de identificare, evaluare și proiectare a măsurilor adecvate de management al riscului sau de răspuns la incidente și atacuri cibernetică, o



importanță majoră este reprezentată de dezvoltarea schimburilor de informații și a transferului de expertiză între autoritățile cu responsabilități în domeniu, dezvoltarea cooperării între sectorul public și cel privat și extinderea cooperării cu mediile neguvernamentale și comunitatea academică.

### Concluzii

Având în vedere faptul că tendințele economiei mondiale și naționale sunt îndreptate înspre gestionarea informației prin intermediul sistemelor informaționale, informația devine cel mai important activ, atât în cadrul instituțiilor publice, cât și în cel al organizațiilor private. Din această perspectivă, o atenție deosebită trebuie să fie acordată problemelor de securitate a informației.

În condițiile gestionării informației ce necesită protecție și securitate sporită, modul de gestionare și control al externalizării serviciilor este un factor determinant în organizarea activităților aferente IT. Din această perspectivă, lipsa unei abordări manageriale a problemelor de securitate informațională reprezintă un factor de risc pentru asigurarea confidențialității informației și a securității componentelor sistemului informațional al instituțiilor. Compromiterea securității informației poate afecta capacitatea de a oferi servicii, poate conduce la fraude sau distrugerea datelor, neonorarea clauzelor contractuale, divulgarea secretelor de stat și a informațiilor confidențiale, afectarea credibilității instituțiilor publice și a organizațiilor etc.

Metodele de protecție specifice tehnologiei informatice din ziua de astăzi sunt variate, depinzând de tipul de vulnerabilități pe care acestea le protejează. Soluțiile date de programele antivirus, *antispam*, *antispyware*, echipamentele sau programele de tip firewall, VPN (*Virtual Private Network* – o rețea privată într-o rețea publică, creată prin stabilirea unei conexiuni virtuale *point-to-point* prin intermediul utilizării de conexiuni dedicate, protocoale virtuale de tunneling, sau criptare de trafic), programele de detecție și prevenire a intruziunii (IDS – *Intrusion Detection System*, o aplicație de tip dispozitiv sau software care monitorizează activitățile legate de rețea sau de sistem pentru a identifica activitățile rău intenționate sau încălcările politicilor, și care produce rapoarte către o stație de management; IPS – *Intrusion Prevention Systems*, sistemele de prevenire a intruziunilor, cunoscute și sub denumirea de *Intrusion Detection and Prevention Systems* – IDPS) sau criptarea informației sunt metode folosite pe scară largă de toți cei care sunt conștienți de riscurile comunicațiilor în această eră intens bazată pe folosirea Internetului.

Securitatea informației este o componentă esențială a societății informaționale, din acest motiv creându-se standarde internaționale specifice, dintre care cele mai importante au fost enunțate în această lucrare, și anume ISO 17799, ISO 27001 și BS 7799 (<http://www.induction.to/>, accesat 9.11.2014).

Trebuie, de asemenea, amintit faptul că securitatea informației distribuită în rețele de calculatoare nu este o problemă ce ține numai de tehnologie, aceasta constituind și o problemă umană și de management. Lipsa de securitate și confidențialitate a informației are efecte nedorite asupra intimității vieții personale sau poate duce la producerea de pierderi materiale importante, răspândirea de conținut periculos la adresa moralei publice, a eticii sociale sau a securității individuale. Se dorește așadar realizarea unor tehnologii de securitate din ce în ce mai performante, făcând ca exploatarea vulnerabilităților de natură tehnologică să devină tot mai dificilă.

---

### **Bibliografie**

---

- Baltac, V., *Tehnologiile informației – noțiuni de bază*, Andreco Educațional, București, 2011.
- Bursa On Line, ediția din 26 mai 2009, <http://www.bursa.ro/>, accesat în data de 9.11.2014.
- <http://www.certificareiso.ro/>, accesat în data de 9.11.2014.
- Conceptul de securitate*, <http://www.securitatea-informatica.ro/> (site cu rol informativ în domeniul securității informatice), accesat în data de 7.11.2014.
- Digital Agenda: cyber-security experts test defences in first pan-European simulation*, European Commission Press Release Database, Brussels, 4 noiembrie 2010, <http://europa.eu/>, accesat în data de 9.11.2014.
- Evaluarea activității desfășurate de Ministerul Afacerilor Interne în anul 2012*, studiu accesibil pe pagina oficială a Instituției Prefectului Județului Bihor, <http://www.prefecturabihor.ro/>, accesat în data de 9.11.2014.
- Fundamental Security Concepts*, <http://cryptome.org/>, accesat în data de 8.11.2014.
- Mazanec, S., *Securitatea calculatorului: protecție împotriva eșecurilor și a virușilor*, Editura Эксмо, Moscova, 2014.
- <http://muntealb.orgfree.com/Traduceri/dictionar-traducere.htm#F>, accesat în data de 9.11.2014.
- <http://nmap.org/>, accesat în data de 9.11.2014.
- Oscarson, P., *Information security fundamentals – Graphical Conceptualisations for Understanding*, (Research Group VITS, Department of Business Administration, Economics, Statistics and Informatics, Örebro University, Sweden), published in “Security education and critical infrastructures”, Kluwer Academic Publishers Norwell, MA, USA, 2003.
- Pagina oficială a Camerei Deputaților, <http://www.cdep.ro/>, accesat în data de 7.11.2014.
- Pagina oficială a Centrului Național de Răspuns la Incidente de Securitate Cibernetică, <http://www.cert-ro.eu/>, accesat în data de 9.11.2014.
- Pagina oficială a Comisiei Europene, <http://ec.europa.eu/>, accesat în data de 9.11.2014.
- Pagina oficială a Consiliului Suprem de Apărare a Țării, <http://csat.presidency.ro/>, accesat în data de 9.11.2014.
- Pagina oficială a Departamentului de Informații și Protecție Internă, structura specializată a Ministerului Afacerilor Interne ce desfășoară activități de informare și protecție internă, în vederea asigurării ordinii publice, prevenirii și combaterii amenințărilor la adresa siguranței naționale privind misiunile, personalul și informațiile clasificate în cadrul ministerului, <http://www.dgipi.ro/>, accesat în data de 9.11.2014.

- Pagina oficială a Departamentului Portal de soluții și servicii pentru IMM-uri, din cadrul Consiliului Național al Întreprinderilor Private Mici și Mijlocii din România, <http://www.immromania.ro/>, accesat în data de 9.11.2014.
- Pagina oficială a European Union Agency for Network and Information Security, <http://www.enisa.europa.eu/>, accesat în data de 9.11.2014.
- Pagina oficială a Facultății de Inginerie Electrică și Știința Calculatoarelor, <http://www.eed.usv.ro/~mahalu/Curs/lectia06.html>, accesat în data de 9.11.2014.
- Pagina oficială a Induction, Awareness and Training Zone, <http://www.induction.to/>, accesat în data de 9.11.2014.
- Pagina oficială a Ministerului pentru Societatea Informațională, <http://www.mcsi.ro/>, accesat în data de 9.11.2014.
- Pagina oficială a Organizației Internaționale de Standardizare (ISO), <http://www.iso.org/>, accesat în data de 9.11.2014.
- Pagina oficială a Poliției Române, <http://www.politiaromana.ro/>, accesat în data de 9.11.2014.
- Pagina oficială a RoCSIRT, serviciul CSIRT operat de către Agenția ARNIEC/RoEduNet, <https://www.csirt.ro/>, accesat în data de 9.11.2014.
- Pagina oficială a Serviciului de Informații Externe, <http://www.sie.ro/>, accesat în data de 6.11.2014.
- Pagina oficială a Serviciului Român de Informații (SRI), <http://www.sri.ro/>, accesat în data de 9.11.2014.
- Popa, S.E., *Securitatea sistemelor informatice*, note de curs și aplicații pentru studenții Facultății de Inginerie – Universitatea din Bacău, 2007.
- <http://searchmidmarketsecurity.techtarget.com/>, accesat în data de 9.11.2014.
- Sebastiao, J. (LOB Head Global Services at International Turnkey Systems Group – ITS, a leading integrated information technology solutions and software services provider), *Integrating Physical And Logical Security*, The Identity Summit – Security Convention, Dubai, 15-19 aprilie 2007.
- Strategia de securitate cibernetică a României*, articol accesibil pe pagina oficială a Ministerului Afacerilor Externe (MAE), <http://www.mae.ro/>, accesat în data de 9.11.2014.
- Strategia națională de dezvoltare a societății informaționale “Moldova Digitală 2020”*, articol accesibil pe pagina oficială a Registrului de stat al actelor juridice al Republicii Moldova, <http://lex.justice.md/>, accesat în data de 7.11.2014.
- Techopedia dictionary, <http://www.techopedia.com/>, accesat în data de 8.11.2014.
- The national strategy for cyberspace operations*, Office of the chairman, Joint chiefs of staff, U.S. Department of Defense, citat de Locke, G. (secretary of the U.S. Department of Commerce), Gallagher, P.D. (director of the National Institute of Standards and Technology), *Information security*, NIST Special Publication 800-39, U.S., Martie 2011.
- Tișinkov, S., *Securitatea rețelei. Riscurile și metodologia protecției*, <http://xn--b1afjrvh2f.xn--1ai/attachments/article/63/NetworkSecurity.pdf>, accesat în data de 9.11.2014.
- <http://web.archive.org/web/20100405225933/http://www.relcom.ru/Archive/2000/TechSupport/Advices/BO/>, accesat în data de 9.11.2014.
- Vrabie Catalin - *Elemente de IT pentru Administratia Publica*, (Vol. 1 și Vol. 2, 2013), ProUniversitaria, București.