Protection and security of information at the level of national public authorities from Romania

Tirziu, Andreea-Maria

National University of Political Studies and Public Administration (SNSPA)

2015

PROTECȚIA ȘI SECURITATEA INFORMAȚIILOR LA NIVELUL AUTORITĂȚILOR PUBLICE NAȚIONALE DIN ROMÂNIA

Andreea-Maria TÎRZIU[1], Anastasia CIUPERCA[2]

Abstract: 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 premizele dezvoltării unei societăți sigure, sănătoase și puternice în România este reprezentată de 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.

Keywords: 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[3].

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 ștampilă. 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.

[1] Masterand, Școala Națională de Studii Politice și Administrative (SNSPA) – Facultatea de Administrație Publică, Bd. Expoziției, Nr. 30 A, sector 1, București, România, adresa de e-mail: tirziu.andreea@yahoo.com.
[2] Student, Școala Națională de Studii Politice și Administrative (SNSPA) – Facultatea de Administrație Publică, Bd. Expoziției, Nr. 30 A, sector 1, București, România, adresa de e-mail: ciuperca.nastica@gmail.com.
[3] *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, p. 1.

Cel mai sensibil aspect este cel care se referă la asigurarea securității informației gestionate de sistemele informatice în noul context tehnologic[4].

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[5]. 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"[6]. 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"[7].

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[8].

2.2. Structura conceptului de securitate

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

---

[4] Popa, S.E., *Securitatea sistemelor informatice*, note de curs și aplicații pentru studenții Facultății de Inginerie – Universitatea din Bacău, 2007, pp. 5-6.

[5] *Ibidem*.

[6] Legea nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate a fost publicată în M.Of. nr. 248/12 aprilie 2002, intrând în vigoare în data de 11 iunie 2002. Forma actualizată a acestui act normativ până la data de 11 septembrie 2014, când legea în discuție a fost consolidată, include toate modificările și completările aduse de către: OUG nr. 16 din 9 martie 2005; Legea nr. 268 din 1 octombrie 2007; Legea nr. 255 din 19 iulie 2013. Pentru mai multe informații, a se vizita pagina oficială a Serviciului de Informații Externe, http://www.sie.ro/, accesat în data de 6.11.2014.

[7] *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/, pp. 23-24, accesat în data de 7.11.2014.

[8] *Conceptul de securitate*, http://www.securitatea-informatica.ro/ (site cu rol informativ în domeniul securității informatice), accesat în data de 7.11.2014.

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[9].

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[10]:

a) nivelul de securitate a accesului;

b) nivelul de securitate a serviciilor.

Securitatea accesului are ca principale componente[11]:

– accesul la sistem: care este răspunzător de gradul de accessibilitate 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[12]:

– 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[13].

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[14].

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,

[9] 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.
[10] *Ibidem.*
[11] *Ibidem.*
[12] *Ibidem.*
[13] *Conceptul de securitate*, http://www.securitatea-informatica.ro/ (site cu rol informativ în domeniul securității informatice), accesat în data de 7.11.2014.
[14] *Idem.*

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 conceptele pot fi văzute ca obiective ale securității informatice și sunt adesea menționate ca *the CIA triad*[15]. 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) **Confidenţialitatea**, uneori numită secretizare, își propune să interzică accesul neautorizat al persoanelor la informaţia care nu le este destinată[16]. 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[17]. 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 etc. au reglementat prin lege controlul confidenţialităţii.

2) **Integritatea**, numită uneori acuratețe, face referire la încrederea, originea, deplinătatea și corectitudinea informațiilor, precum și la prevenirea modificării necorespunzătoare sau neautorizate a datelor[18]. 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[19]:

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[20].

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,

---

[15] *Fundamental Security Concepts*, http://cryptome.org/, pp. 4-6, accesat în data de 8.11.2014.
[16] Baltac, V., *Tehnologiile informației – noțiuni de bază*, Andreco Educaţional, Bucureşti, 2011, p. 129.
[17] *Fundamental Security Concepts*, http://cryptome.org/, p. 4, accesat în data de 8.11.2014.
[18] Baltac, V., *op. cit.*, 2011, p. 129.
[19] 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, pp. 4-5.
[20] *Fundamental Security Concepts*, http://cryptome.org/, pp. 5-6, accesat în data de 8.11.2014.

asigurându-se astfel relația de încredere între părți. Expeditorul nu poate să nege că el este cel care a trimis mesajul[21]. Nerepudierea stă la baza semnăturilor digitale, asigurând autenticitatea acestora, în noua piaţă a comerţului electronic (E-Commerce)[22].

3. Cadrul legislativ privind protecția şi securitatea informațiilor

Controalele interne pot fi considerate principiile care stau la baza implementării unui sistem de management al securității[23]. 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 şi foarte important ca persoana care se ocupă de implementarea unui sistem de management al securităţii să aibă cunoştinţe despre cerinţe 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[24];

• Legea nr. 506 din 17 noiembrie 2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice, publicată în M.Of. nr. 1101/25 noiembrie 2004;

• Legea nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, publicată în M.Of., Partea I, nr. 790/12 decembrie 2001[25];

• 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 informaţiile de interes public, publicată în M.Of. nr. 663/23 octombrie 2001;

• Hotărârea nr. 1259 din 13 decembrie 2001 privind aprobarea normelor tehnice şi 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 Cerinţelor 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 protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, publicat în M.Of. nr. 383/5 iunie 2002;

---

[21] Baltac, V., *op. cit.*, 2011, p. 129.
[22] Pentru mai multe informații, a se vedea Techopedia dictionary, http://www.techopedia.com/, accesat în data de 8.11.2014.
[23] Popa, S.E., *op.cit.*, 2007, p. 8.
[24] 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, a fost actualizată la data de 22 aprilie 2011 și modificată prin OUG nr. 40/2003, OUG nr. 77/2003, OUG nr. 92/2004, Legea nr. 171/2004, Legea nr. 96/2006, OUG nr. 31/2006, Legea nr. 251/2006, Ordonanța nr. 2/2006, OUG nr. 119/2006, Legea nr. 144/2007, Legea nr. 359/2004, OUG nr. 14/2005, Legea nr. 330/2009, Legea nr. 284/2010 și OUG nr. 37/2011. Pentru mai multe informații, a se vizita pagina oficială a Camerei Deputaților, http://www.cdep.ro/, accesat în data de 7.11.2014.
[25] Această lege a fost 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, 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 și a alin. (7) al art. 22 din Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.

• Ordinul Avocatului Poporului nr. 54 din 18 aprilie 2002 privind stabilirea unor situaţii în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidenţa Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, publicat în M.Of. nr. 383/5 iunie 2002;

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

• Legea nr. 182 din 12 aprilie 2002 privind protecţia informaţiilor clasificate, publicată în M.Of. nr. 248/12 aprilie 2002.

Pe lângă legislaţia internă, trebuie luate în considerare şi convenţiile internaţionale şi reglementările europene semnate de România sau în care aceasta este parte. Selectarea controalelor trebuie să ţină cont de specificul instituţiei publice sau organizaţiei. Nu toate recomandările pot fi aplicate, asa cum nu toate pot fi justificate din punct de vedere al costurilor. Eficacitatea sistemului de securitate depinde de următoarele elemente[26]:

– stabilirea unor obiective de securitate care să reflecte cerinţele instituţiei sau organizaţiei;

– sprijinului conducerii;

– existenţa abilităţilor necesare realizării analizei riscurilor, a vulnerabilităţilor şi a analizei de impact;

– instruirea angajaţilor;

– monitorizarea controalelor implementate.

4. Cadrul instituţional privind protecţia şi securitatea informaţiilor

Atât instituţiile publice, cât şi organizaţiile private trebuie să conştientizeze riscurile asociate cu utilizarea tehnologiei şi gestionarea informaţiilor şi să abordeze pozitiv acest subiect printr-o conştientizare în rândul angajaţilor a importanţei securităţii informaţiilor şi a înţelegerii tipologiei ameninţărilor, riscurilor şi vulnerabilităţilor specifice mediilor informatizate şi, nu în ultimul rând, a aplicării practicilor de control.

În perioada 14-26 octombrie 1946, în Londra a avut loc întrunirea de organizaţii naţionale de norme din 25 de ţări. Acesta a constituit momentul în care s-a luat decizia de a se înfiinţa o nouă organizaţie, şi anume ISO (*International Organization for Standardization*), care şi-a început activitatea în data de 23 februarie 1947[27]. **Organizaţia Internaţională de Standardizare – ISO** este o confederaţie internaţională care se ocupă cu stabilirea normelor în toate domeniile, excepţie făcând domeniul electricităţii şi cel al electronicii – acestea fiind reprezentate de IEC (*International Electrotechnical Commission*), şi de cel al telecomunicaţiilor – reprezentat de ITU (*International Telecommunication Union*). Cele trei organizaţii menţionate anterior sunt unite în WSC (*World Standards Cooperation*)[28].

ISO cooperează în strânsă legătură cu **Comisia Electrotehnică Internaţională** (IEC), care este responsabilă pentru standardizarea echipamentelor electrice şi electronice, aceste două organizaţii alcătuind un forum specializat pentru standardizare. Organismele naţionale care sunt membre ale ISO şi IEC participă la dezvoltarea standardelor internaţionale prin intermediul comitetelor tehnice. Statele Unite

[26] Popa, S.E., *op.cit.*, 2007, pp. 8-9.
[27] Pentru mai multe informaţii, a se vizita http://www.certificareiso.ro/, accesat în data de 9.11.2014.
[28] Pagina oficială a Organizaţiei Internaţionale de Standardizare (ISO), http://www.iso.org/, accesat în data de 9.11.2014.

ale Americii, prin Institutul Naţional de Standardizare, ocupă poziţia de Secretar, 24 de ţări au statut de Participanţi şi alte 40 de ţări au statut de Observatori[29].

Ministerul pentru Societatea Informaţională îndeplineşte rolul de adoptare, la nivel naţional, a standardelor europene şi internaţionale recunoscute. Prin această activitate a ministerului, standardul ISO/IEC 17799 – "Tehnologia Informaţiei – Cod de bună practică pentru managementul securităţii informaţiei" a fost adoptat şi în România de către **Asociaţia de Standardizare din România** (ASRO), în toamna anului 2004. Specialiştii ASRO (fostul IRS) participă în cadrul comitetelor tehnice internaţionale ale Organizaţiei Internaţionale de Standardizare. Standardul ISO este recunoscut în rezoluţiile Consiliului Europei, implementarea acestuia la nivelul instituţiilor şi al organizaţiilor fiind însă opţională[30].

4.1. Organisme naţionale cu atribuţii în domeniul securităţii informatice

Consiliul Suprem de Apărare a Ţării[31] reprezintă autoritatea care coordonează, la nivel strategic, activitatea Sistemului Naţional de Securitate Cibernetică (SNSC). Prin **Ministerul pentru Societatea Informaţională**, Guvernul României este cel care asigură coordonarea celorlalte autorităţi publice în vederea realizării coerenţei politicilor şi a implementarii strategiilor guvernamentale în domeniu.

Sistemul Naţional de Securitate Cibernetică[32] include, pe lângă autorităţile publice cu competenţe în materie (Serviciul Român de Informaţii, Ministerul Apărării Naţionale, Ministerul Afacerilor Interne, Ministerul Afacerilor Externe, Ministerul pentru Societatea Informaţională, Serviciul de Telecomunicaţii Speciale, Serviciul de Informaţii Externe, Serviciul de Protecţie şi Pază, Oficiul Registrului Naţional pentru Informaţii Secrete de Stat, precum şi Secretarul Consiliului Suprem de Apărare a Ţării), actori din mediul asociativ neguvernamental, profesional şi de afaceri.

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

▪ **Consiliul Operativ de Securitate Cibernetică** (COSC), al cărui regulament de organizare şi funcţionare a fost aprobat prin Hotărârea CSAT nr. 17/2013. Acesta este format din reprezentanţi la nivel de secretar de stat din cadrul instituţiilor sistemului de securitate naţională, inclusiv ai MAE şi care se ocupă de coordonarea unitară a SNSC. Funcţia de coordonator tehnic al COSC este asigurată de către Serviciul Român de Informaţii în calitate de autoritate naţională în domeniul securităţii cibernetice prin intermediul Centrului Naţional Cyberint (CNC), care informează operativ COSC cu privire la apariţia incidentelor de tip cibernetic care pot aduce atingere securităţii naţionale. Consiliul raportează către CSAT, anual sau ori de câte ori situaţia o impune, cu privire la acţiunile întreprinse, precum şi la evoluţiile înregistrate în spaţiul cibernetic, în special cu referire la incidente sau atacuri cibernetice[33].

▪ **Grupul de Suport Tehnic** (GST), care are în alcătuirea sa reprezentanţi la nivel de expert din cadrul instituţiilor sistemului de securitate naţională reprezentate în cadrul COSC[34].

SRI deţine, în structura sa, **Centrul Naţional de Securitate Cibernetică** (CNSC) care, în cazul în care are loc un atac cibernetic asupra securităţii informatice a României, reprezintă punctul de contact pentru relaţionarea cu organismele similare din străinătate[35].

---

[29] Popa, S.E., *op.cit.*, 2007, p. 5.
[30] *Ibidem*, p. 6.
[31] Pagina oficială a Consiliului Suprem de Apărare a Ţării, http://csat.presidency.ro/, accesat în data de 9.11.2014.
[32] Legea privind securitatea cibernetică a României, accesibilă pe pagina oficială a Camerei Deputaţilor, http://www.cdep.ro/, accesat în data de 9.11.2014.
[33] *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.
[34] *Idem*.

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 şi controlul măsurilor specifice fiecărui nivel de alertă, propuse în cadrul COSC şi aprobate de CSAT, se realizează de către Centrul Naţional Cyberint (CNC)[36].

Structura independentă de expertiză şi cercetare-dezvoltare în domeniul protecției infrastructurilor cibernetice – **CERT-RO**[37], dispune de capacitatea necesară pentru prevenirea, analiza, identificarea şi reacția la incidentele de securitate cibernetică ale sistemelor informatice ce asigură funcționalități de utilitate publică sau servicii ale societății informaționale. CERT-RO este coordonat de Ministerul pentru Societatea Informațională, fiind finanțat integral de la bugetul de stat. Conform H.G. nr. 494/2011[38], act normativ ce reglementează activitatea structurii, acest centru poate emite alerte şi 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[39]. Acesta va introduce programul *Nmap*[40] şi 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*[41] cu ajutorul programelor specializate, un exemplu de astfel de program fiind PortSentry. Dacă serverul *DMVs*[42] are acces la Internet și la rețeaua internă, și serverul *FTP*[43] este folosit doar de utilizatori din rețeaua internă, atunci nu este nevoie să fii conectat și în afara

---

[35] Pentru mai multe informații, a se vizita pagina oficială a Serviciului Român de Informații (SRI), http://www.sri.ro/, accesat în data de 9.11.2014.

[36] Legea securității cibernetice a României, disponibilă pe pagina oficială a Ministerului pentru Societatea Informațională, http://www.mcsi.ro/, accesat în data de 9.11.2014.

[37] Pagina oficială a Centrului Național de Răspuns la Incidente de Securitate Cibernetică, http://www.cert-ro.eu/, accesat în data de 9.11.2014.

[38] Act publicat în M.Of. nr. 388/2 iunie 2011.

[39] 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.

[40] 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.

[41] 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.

[42] Dynamic management views (DMVs) 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.

[43] 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 destinatatului sau chiar cu sisteme de operare diferite. Pentru mai multe informații, a se consulta Baltac, V., *op. cit.*, 2011, pp. 210-212.

rețelei, fiind suficient să programezi *firewall*-ul astfel încât accesul să fie disponibil doar pentru *IP*-uri interne[44].

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[45] – la comunicarea textuală, bidirecțională și interactivă, bazată pe realizarea unei conexiuni virtuale cu stația de lucru destinatară[46].

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 confidenţialitate, în urma instalării programelor "afectate" sau prin răspândirea informațiilor personale pe Internet. *Malware*-ul[47] activat de utilizator, cu ajutorul căruia răufăcătorul poate pătrunde de la distanță în calculator, se numeste Troian[48]. În acest caz, putem considera drept exemplu programul *Back Orifice*[49], a cărui instalare pe o platformă Windows se realizează după cum urmează:

– În registrul de system, în secțiunea HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows\CurrentVersion\opțiune Run Services, sub titlul "(Implicit)" {"(Default)"} (uneori altul) apare fișierului *Back Orifice* care, de obicei, emite conținutul ".exe" (space punct exe);

– În directorul de sistem (C:\Windows\system), apare o copie a *Back Orifice* cu numele specificat în registru, de obicei ".exe"[50].

Calculatorul virusat poate fi ușor coordonat de răufăcător, astfel existând diferiți "cai troiani" 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 directa participare a utilizatorului, acestea fiind de trei tipuri: ISQ (mesagerie instantă), prin intermediul poștei electronice sau prin directa descărcare a programelor virusate.

---

[44] Tișinkov, S., *Securitatea rețelei. Riscurile și metodologia protecției*, http://xn--b1afjrvh2f.xn--p1ai/attachments/article/63/NetworkSecurity.pdf, accesat în data de 9.11.2014.

[45] Local Area Network este o rețea locală reprezentată de un ansamblu de mijloace de transmisiune și de sisteme de calcul folosite pentru transportarea și prelucrarea informației, frecvent utilizată pentru a conecta calculatoarele personale și stațiile de lucru din birourile instituțiilor și organizațțiilor, cu scopul de a partaja resurse și de a face schimb de informații.

[46] Pentru mai multe informații despre notiunea de telnet, a se vizita 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; a se vedea și Baltac, V., *op. cit.*., 2011, p. 210.

[47] 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., *op. cit.*., 2011, p. 91, pp. 139-140.

[48] Virusul de tip Troian accesează fișierele calculatorului prin conexiunea la rețea. Acesta se mai numește și RAT (Remote Administration Trojan).

[49] 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.

[50] Descrierea detaliată a procesului se poate găsi vizitând link-ul: http://web.archive.org/web/20100405225933/http:/www.relcom.ru/Archive/2000/TechSupport/Advices/BO/, accesat în data de 9.11.2014.

În primul caz, descărcând o poză de pe Internet cu denumirea "foto.jpg", poate de fapt fi descărcată o fotografie de tip "foto.jpg.exe", aceasta reprezentând o fotografie care are "lipit" un program troian[51]. 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 (de exemplu: pagina oficială a băncii, furnizorul de licitație etc.)[52].

b) Poate exista o eroare în structurile de bază, prin acest intermediu răufăcătorul având acces la informații. Elementul vulnerabil principal 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*[53]. 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 afara acestor aplicații utilizatorul devine vulnerabil.

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

În anul 2008, fenomenul infracţionalităţii informatice a cunoscut o evoluţie extrem de puternică la nivel mondial. La nivel naţional, conform unei statistici întocmite de Direcţia Generală de Combatere a Criminalităţii Organizate (DGCCO) din cadrul Poliţiei Române, valoarea prejudiciilor cauzate de infracţiuni informatice s-a ridicat la cinci milioane de euro, cea mai mare parte aparţinând fraudelor cu carduri. Previziunile pentru anul 2009 nu au fost cele mai optimiste, pierderile fiind estimate la aproximativ 500 milioane de euro[54].

"România are un nivel scăzut al managementului securităţii informatice[55]" – așa începea, în 2009, un articol publicat pe site-ul Bursa On Line. În perioada 25-26 mai a aceluiași an avea loc, la București, conferința *CyberSecurity*[56], în cadrul căreia specialistul în securitatea informaţiei al Serviciului Român de Informaţii (SRI), Eduard Bîsceanu, declara faptul că în România nu sunt operaţionale organisme civile specializate pentru detectarea şi analiza incidentelor sau atacurilor informatice, ţara noastră având "un nivel scăzut de dezvoltare şi 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.

---

[51] Această metodă este una arhaică, însă cu toate acestea nu trebuie scoasă din calcul.

[52] Mazanic, S., *Securitatea calculatorului: protecție împotriva eșecurilor și a virușilor,* Editura Эксмо, Moscova, 2014, pp. 69-70.

[53] 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.

[54] Pentru mai multe informații, a se vizita pagina oficială a Poliției Române, http://www.politiaromana.ro/, accesat în data de 9.11.2014.

[55] Articol publicat pe site-ul Bursa On Line, ediția din 26 mai 2009, http://www.bursa.ro/, accesat în data de 9.11.2014.

[56] Mai multe informații despre conferința CyberSecurity din 2009 se pot vedea pe 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.

România este considerată, în principal, ţară furnizoare de criminalitate informatică, aceasta amplificându-se şi pe plan intern, în special prin operaţiunile de fraudare a sistemului de achiziţii online, a ATM-urilor[57] şi POS-urilor[58], precum şi a aparatelor electronice de jocuri de noroc. Lupta împotriva criminalităţii informatice a dus la destructurarea, în anul 2012, a 35 de grupuri organizate cu preocupări infracţionale în zona cyber-criminalităţii, 286 de persoane fiind trimise în judecată, dintre care 154 aflându-se în stare de reţinere/arestare[59].

În anul 2010, pe data de 4 noiembrie, România a participat la primul exerciţiu paneuropean privind protecţia infrastructurilor informatice critice – numit *Cyber Europe 2010*[60] – experţii europeni testând, cu această ocazie, sistemele de apărare împotriva atacurilor cibernetice. Acest exerciţiu a constituit o parte a măsurilor prevăzute de Agenda Digitală pentru Europa[61], strategie lansată de Comisia Europeană în vederea creşterii încrederii în Internet şi a îmbunătăţirii securităţii reţelelor. Potrivit Ministerului pentru Societatea Informaţională (MCSI), scenariul exerciţiului *Cyber Europe 2010* a prevăzut pierderea treptată sau reducerea considerabilă a conexiunilor Internet dintre ţările europene şi, 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 ţărilor membre ale Uniunii Europene în faţa unor incidente majore care pot afecta infrastructurile informatice critice[62], fiind organizată de statele membre ale UE, cu sprijinul Agenţiei Europene pentru Securitatea Reţelelor şi a Informaţiei (ENISA) şi a Centrului Comun de Cercetare (JRC), la acest exerciţiu de simulare participând şi reprezentanţi ai Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică (CERT-RO), ai departamentului de specialitate din cadrul Institutului Naţional de Cercetare-Dezvoltare în Informatică (ICI), ai departamentelor de specialitate ale Ministerului Administraţiei şi Internelor şi ale Serviciului de Telecomunicaţii Speciale, precum şi experţi 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 Informaţii şi Protecţie Internă (CERT-INT)", acest proiect fiind cofinanţat din Fondul Social European prin Programul Operaţional Dezvoltarea Capacităţii Administrative 2007-2013 şi având ca obiectiv general îmbunătăţirea capacităţii DIPI de a contribui la formularea politicilor în domeniul protecţiei informaţiilor din spaţiul cibernetic, prin asigurarea unui mecanism unitar de reacţie şi răspuns la incidente de securitate la sistemele informatice din cadrul Ministerului Afacerilor Interne[63]. Dotarea cu echipamente informatice şi pregătirea de specialişti care vor utiliza şi administra sistemul integrat de management al infrastructurii, au reprezentat beneficii importante obţinute în cadrul proiectului cu o durată de implementare de 27 de luni, având ca beneficiar personalul DIPI.

Departamentul Informaţii şi Protecţie Internă a mai implementat nişte proiecte în scopul perfecţionării şi adaptării metodelor de lucru ale instituţiei pentru eficientizarea activităţilor desfăşurate şi pregătirea personalului, acestea fiind enumerate mai jos:

---

[57] Asynchronous Transmission Mode (ATM) este un protocol de transmisie şi multiplexare a datelor de mare viteză.

[58] Point of Sale (POS) reprezintă terminale de colectare a datelor folosite de personalul de execuţie al unei instituţii sau organizaţii.

[59] *Evaluarea activităţii desfăşurate de Ministerul Afacerilor Interne în anul 2012*, studiu accesibil pe pagina oficială a Instituţiei Prefectului Judeţului Bihor, http://www.prefecturabihor.ro/, accesat în data de 9.11.2014.

[60] Mai multe informaţii pot fi găsite pe pagina oficială a European Union Agency for Network and Information Security, http://www.enisa.europa.eu/, accesat în data de 9.11.2014.

[61] *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.

[62] Pagina oficială a Ministerului pentru Societatea Informaţională, http://www.mcsi.ro/, accesat în data de 9.11.2014.

[63] Pagina oficială a Departamentului de Informaţii şi Protecţie Internă, structura specializată a Ministerului Afacerilor Interne ce desfăşoară activităţi de informaţii şi protecţie internă, în vederea asigurării ordinii publice, prevenirii şi combaterii ameninţărilor la adresa siguranţei naţionale privind misiunile, personalul şi informaţiile clasificate în cadrul ministerului, http://www.dgipi.ro/, accesat în data de 9.11.2014.

▪ Proiectul SIMITO (”Sistemul Naţional Integrat de Management al Informaţiei şi al Activităţii Tactico-Operative la nivelul Departamentului de Informaţii şi Protecţie Internă”) → care oferă instituţiei posibilitatea de a beneficia de sisteme informatice moderne, ce permit un proces de analiză şi de coroborare a informaţiilor primare, obţinute la toate nivelurile, transformarea informaţiilor singulare în produse analitice de calitate superioară, necesare pentru fundamentarea managementului decizional în domeniul politicilor şi strategiilor naţionale de securitate şi ordine publică[64].

▪ Proiectul „Optimizarea activităţii de pregătire profesională în cadrul DIPI în sistem E-Educaţie” → care, la nivel operaţional, reprezintă un sistem modern de îmbunătăţire a pregătirii personalului. Acest proiect a obţinut două nominalizări în finala din acest an a premiilor European IT & Software Excellence Awards 2014, la categoriile dedicate proiectelor care au ca obiectiv eficientizarea activităţii derulate de instituţiile publice[65].

▪ Proiectul „Instrumente moderne de management electronic al documentelor interne si activităţii din teritoriu la Departamentul de Informaţii şi Protecţie Internă (IMMEDIAT la DIPI)” → prin intermediul căruia a fost implementat un sistem informatic modern, la nivel naţional, ca suport de secretariat şi gestiune a documentelor, având drept scop îmbunătăţirea politicilor şi a proceselor interne de lucru cu documentele[66].

România a fost, în perioada 21-22 mai 2013, gazda europeană în securitate informatică pentru desfăşurarea unui *workshop*[67] organizat de către Agenţia ARNIEC/RoEduNet[68], în parteneriat cu ENISA[69]. Peste 150 de experţi în securitate informatică şi oficiali guvernamentali din Uniunea Europeană şi din SUA au venit la Bucureşti pentru a dezbate cele mai noi soluţii privind prevenirea şi combaterea fenomenului de criminalitate informatică. România a ales să fie gazda evenimentului, în contextul dezvoltării din ultimii ani a relaţiilor de cooperare între instituţiile de profil din ţară şi cele deja existente la nivel european. Printre participanţii la aceste dezbateri s-au aflat oficiali din structurile naţionale şi guvernamentale (CERT – *Computer Emergency Response Team*), structuri care se ocupă de protecţia instituţiilor conectate la reţelele naţionale de comunicaţii şi de asistenţă tehnică în tratarea incidentelor privind securitatea informatică[70].

În perioada 23-24 mai a aceluiaşi an a avut loc, la Bucureşti, cea de-a 39-a întâlnire a TI (*Trusted Introducer*)[71] şi a TF-CSIRT[72], acestea reprezentând două grupuri de lucru constituite la nivel european,

---

[64] Pagina oficială a Departamentului de Informaţii şi Protecţie Internă, structura specializată a Ministerului Afacerilor Interne ce desfăşoară activităţi de informaţii şi protecţie internă, în vederea asigurării ordinii publice, prevenirii şi combaterii ameninţărilor la adresa siguranţei naţionale privind misiunile, personalul şi informaţiile clasificate în cadrul ministerului, http://www.dgipi.ro/, accesat în data de 9.11.2014.

[65] *Idem*.

[66] *Idem.*

[67] “CERTs in Europe” este cel de-al optulea workshop anual al ENISA – Partea I.

[68] Agenţia ARNIEC/RoEduNet (Agenţia de Administrare a Reţelei Naţionale de Informatică pentru Educaţie şi Cercetare) este aflată în subordinea Ministerului Educaţiei Naţionale, administrează şi dezvoltă reţeaua RoEduNet care asigură servicii de comunicaţii de date pentru instituţiile de cercetare şi academice de toate gradele din România. Agenţia este membru al consorţiului european GEANT, reţeaua care interconectează toate reţelele pentru educaţie şi cercetare din statele membre ale Uniunii Europene.

[69] ENISA (The European Network and Information Security Agency) este agenţia responsabilă de activităţile de securitate informatică din cadrul Uniunii Europene, deservind atât instituţiile Uniunii Europene, cât şi pe cele ale statelor membre. ENISA este un centru de expertiză care defineşte şi promovează standardele de securitate informatică în Europa.

[70] Pagina oficială a RoCSIRT, serviciul CSIRT operat de către Agenţia ARNIEC/RoEduNet, https://www.csirt.ro/, accesat în data de 9.11.2014.

[71] TI (Trusted Introducer) este un serviciu de cooperare, comunicare şi recunoaştere a echipelor de tip CERT, fondat în anul 2000 de către membrii comunităţii CERT din Europa care are ca scop dezvoltarea şi facilitarea comunicării şi cooperării membrilor săi.

[72] TF-CSIRT este grupul de lucru pe probleme de securitate informatică a TERENA (The Trans-European Research and Education Networking Association), asociaţia reţelelor pentru educaţie şi cercetare din Europa, ce oferă cadrul în care acestea inovează şi schimbă cunoştinţe menite să dezvolte tehnologiile, infrastructura şi serviciile de acces la Internet folosite de comunităţile de cercetare şi educaţie.

care au rolul de a susține și crește colaborarea în domeniul securității informatice, precum și de a combate incidentele de criminaliate în domeniul discutat[73].

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[74].

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 cibernetice deținute și administrate de stat, precum și de entități private.

În ceea ce privește dinamismul evoluțiilor globale în spațiul cibernetic, precum şi 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 eficienţa demersurilor de protejare faţă de atacuri cibernetice şi să se limiteze riscurile producerii unor incidente cu potenţial impact semnificativ.

Autorităţile publice care au responsabilităţi în acest domeniu vor fi nevoite să aloce resursele financiare necesare asigurării protecţiei şi securităţii informaţiilor prin intermediul politicilor de planificare. Pentru asigurarea unei capacităţi sporite de identificare, evaluare şi proiectare a măsurilor adecvate de management al riscului sau de răspuns la incidente şi atacuri cibernetice, are o importanţă majoră dezvoltarea schimburilor de informaţii şi a transferului de expertiză între autorităţile cu responsabilităţi în domeniu, dezvoltarea cooperării între sectorul public şi cel privat şi extinderea cooperării cu mediile neguvernamentale şi 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.

[73] Pagina oficială a RoCSIRT, serviciul CSIRT operat de către Agenția ARNIEC/RoEduNet, https://www.csirt.ro/, accesat în data de 9.11.2014.
[74] Pagina oficială a Comisiei Europene, http://ec.europa.eu/, accesat în data de 9.11.2014.

Metodele de protecţie specifice tehnologiei informatice din ziua de astăzi sunt variate, depinzând de tipul de vulnerabilităţi pe care acestea le protejează. Soluţiile date de programele antivirus, antispam, *antispyware*, echipamentele sau programele de tip *firewall*, VPN[75], programele de detecţie şi prevenire a intruziunii (IDS[76], IPS[77]) sau criptarea informaţiei sunt metode folosite pe scară largă de toţi cei care sunt conştienţi de riscurile comunicaţiilor în această eră intens bazată pe folosirea Internetului.

Securitatea informaţiei este o componentă esenţială a societăţii informaţionale, din acest motiv creându-se standarde internaţionale specifice, dintre care cele mai importante au fost enunţate în această lucrare, şi anume ISO 17799, ISO 27001 şi BS 7799[78].

Trebuie, de asemenea, amintit faptul că securitatea informaţiei distribuită în reţele de calculatoare nu este o problemă ce ţine numai de tehnologie, aceasta constituind şi o problemă umană şi de management. Lipsa de securitate şi confidenţialitate a informaţiei are efecte nedorite asupra intimităţii vieţii personale sau poate duce la producerea de pierderi materiale importante, răspândirea de conţinut periculos la adresa moralei publice, a eticii sociale sau a securităţii individuale. Se doreşte aşadar realizarea unor tehnologii de securitate din ce în ce mai performante, făcând ca exploatarea vulnerabilităților de natură tehnologică să devină tot mai dificilă.

Referințe

1. Baltac, V., *Tehnologiile informației – noțiuni de bază*, Andreco Educațional, București, 2011.
2. Bursa On Line, ediția din 26 mai 2009, http://www.bursa.ro/, accesat în data de 9.11.2014.
3. http://www.certificareiso.ro/, accesat în data de 9.11.2014.
4. *Conceptul de securitate*, http://www.securitatea-informatica.ro/ (site cu rol informativ în domeniul securității informatice), accesat în data de 7.11.2014.
5. *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.
6. *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.
7. *Fundamental Security Concepts*, http://cryptome.org/, accesat în data de 8.11.2014.
8. Mazanic, S.*, Securitatea calculatorului: protecție împotriva eșecurilor și a virușilor,* Editura Эксмо, Moscova, 2014.
9. http://muntealb.orgfree.com/Traduceri/dictionar-traducere.htm#F, accesat în data de 9.11.2014.
10. http://nmap.org/, accesat în data de 9.11.2014.
11. 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.
12. Pagina oficială a Camerei Deputaților, http://www.cdep.ro/, accesat în data de 7.11.2014.

[75] Virtual Private Network (VPN) reprezintă o rețea privată într-o rețea publică, cum ar fi Internetul. Aceasta permite unui calculator sau dispozitiv Wi-Fi să trimită și primească date din rețelele partajate sau publice, ca și cum ar fi direct conectate la rețeaua privată, în timp ce beneficiază de politicile de funcționare, securitate și gestionare a rețelei private. O astfel de rețea este creată prin stabilirea unei conexiuni virtuale point-to-point prin intermediul utilizării de conexiuni dedicate, protocoale virtuale de tunneling, sau criptare de trafic.

[76] Un sistem de detectare a intruziunilor (Intrusion Detection System) este 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 produce rapoarte către o stație de management. Acest sistem înregistrează informații referitoare la evenimente observate, notifică administratorii de securitate ai acelor evenimente importante și întocmește rapoarte; poate, de asemenea, răspunde la o amenințare detectată prin încercarea de a preveni reușita acesteia. Sunt folosite mai multe tehnici de răspuns, în care sunt implicate oprirea atacului de către IDS în sine, schimbarea mediului de securitate (de exemplu, reconfigurarea unui firewall) sau schimbarea conținutului atacului.

[77] Sistemele de prevenire a intruziunilor (Intrusion Prevention Systems), cunoscute și sub denumirea de Intrusion Detection and Prevention Systems (IDPS), sunt aparate de securitate a rețelei care monitorizează activitățile de rețea și/sau de sistem pentru activitatea malware. Principalele funcții ale acestor sisteme sunt acelea de identificare a activității malware, de înregistrare a informațiilor despre această activitate, de încercare în vederea blocării/opririi, și de raportare a sa.

[78] Pentru mai multe informații, a se vizita pagina oficială a al Induction, Awareness and Training Zone, http://www.induction.to/, accesat în data de 9.11.2014.

13. Pagina oficială a Centrului Național de Răspuns la Incidente de Securitate Cibernetică, http://www.cert-ro.eu/, accesat în data de 9.11.2014.
14. Pagina oficială a Comisiei Europene, http://ec.europa.eu/, accesat în data de 9.11.2014.
15. Pagina oficială a Consiliului Suprem de Apărare a Ţării, http://csat.presidency.ro/, accesat în data de 9.11.2014.
16. Pagina oficială a Departamentului de Informaţii şi Protecţie Internă, structura specializată a Ministerului Afacerilor Interne ce desfăşoară activităţi de informaţii şi protecţie internă, în vederea asigurării ordinii publice, prevenirii şi combaterii ameninţărilor la adresa siguranţei naţionale privind misiunile, personalul şi informaţiile clasificate în cadrul ministerului, http://www.dgipi.ro/, accesat în data de 9.11.2014.
17. Pagina oficială a Departamentului Portal de soluții și servicii pentru IMM-uri, din cadrul Consiliului Național al Întreprinderilor Private Mici şi Mijlocii din România, http://www.immromania.ro/, accesat în data de 9.11.2014.
18. Pagina oficială a European Union Agency for Network and Information Security, http://www.enisa.europa.eu/, accesat în data de 9.11.2014.
19. 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.
20. Pagina oficială a Induction, Awareness and Training Zone, http://www.induction.to/, accesat în data de 9.11.2014.
21. Pagina oficială a Ministerului pentru Societatea Informațională, http://www.mcsi.ro/, accesat în data de 9.11.2014.
22. Pagina oficială a Organizației Internaționale de Standardizare (ISO), http://www.iso.org/, accesat în data de 9.11.2014.
23. Pagina oficială a Poliției Române, http://www.politiaromana.ro/, accesat în data de 9.11.2014.
24. Pagina oficială a RoCSIRT, serviciul CSIRT operat de către Agenția ARNIEC/RoEduNet, https://www.csirt.ro/, accesat în data de 9.11.2014.
25. Pagina oficială a Serviciului de Informații Externe, http://www.sie.ro/, accesat în data de 6.11.2014.
26. Pagina oficială a Serviciului Român de Informații (SRI), http://www.sri.ro/, accesat în data de 9.11.2014.
27. Popa, S.E., *Securitatea sistemelor informatice*, note de curs şi aplicaţii pentru studenţii Facultăţii de Inginerie – Universitatea din Bacău, 2007.
28. http://searchmidmarketsecurity.techtarget.com/, accesat în data de 9.11.2014.
29. 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.
30. *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.
31. *Strategia naţională de dezvoltare a societăţii informaţionale "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.
32. Techopedia dictionary, http://www.techopedia.com/, accesat în data de 8.11.2014.
33. *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.
34. Tişinkov, S., *Securitatea reţelei. Riscurile şi metodologia protecţiei*, http://xn--b1afjrvh2f.xn--p1ai/attachments/article/63/NetworkSecurity.pdf, accesat în data de 9.11.2014.
35. http://web.archive.org/web/20100405225933/http:/www.relcom.ru/Archive/2000/TechSupport/Advices/BO/, accesat în data de 9.11.2014.