NOI CERINȚE PENTRU SISTEMELE INFORMAȚIONALE DIN INFRASTRUCTURA CRITICĂ ÎN CONDIȚIILE CONTEMPORANE

NEW REQUIREMENTS TO INFORMATION SYSTEMS FROM CRITICAL INFRASTRUCTURE IN CONTEMPORARY CONDITIONS

Prof. univ. dr. Gruia TIMOFTE*

Acest articol analizează vulnerabilitățile, riscurile şi amenințările la adresa sistemelor informaționale din compunerea infrastructurii critice, in era informațională, cu ample şi rapide evoluții in tehnologia informației şi comunicațiilor. Dimensiunea virtuală este foarte importantă pentru sistemele informatice, rețelele de comunicații, sistemele de supraveghere, control şi avertizare şi fluxurile informaționale critice aferente pentru managementul infrastructurii critice globale şi naționale. Aceste sisteme sunt considerate ca fundamentale pentru infrastructura critică şi necesare pentru continuitatea managementului informațiilor şi cunoştințelor în scopul asigurării serviciilor specifice. De aceea, sistemele care integrează tehnologia informației şi comunicațiilor trebuie să fie robuste, fiabile, sustenabile, sigure, redundante, adaptive etc. pentru a rezista la amenințările şi riscurile cibernetice.

Cuvinte cheie: *infrastructură informațională critică; sisteme informaționale; managementul informațiilor şi cunoştințelor; amenințări cibernetice; securitate cibernetică.*

This paper analyzes the cyber vulnerabilities, threats and risks to critical information infrastructure in the information age with large and intensive developments in information and communications technology. This virtual dimension is very important for information systems, communications networks, surveillance, control and warning systems and their critical information flows which ensure the management of the global and national critical infrastructure. These systems are regarded the backbone of critical infrastructures and very necessary to the continuity for the information and knowledge

* gruia.timofte@gmail.com

management for providing specific services. Therefore, the information and communications technology systems must be robust, reliable, sustainable, secure, redundant, adaptive etc. to meet the cyber threats and risks challenges.

Keywords: *critical information infrastructure; information systems; information and knowledge management; cyber threats; cyber security.*

Dicţionarul *Wikipedia* defineşte *spaţiul cibernetic* ca un mediu electronic compus din reţele de calculatoare în care se desfăşoară comunicaţii on-line. În utilizarea uzuală termenul de „spaţiu cibernetic" reprezintă reţeaua cu infrastructuri independente de tehnologia informaţiei, reţele de telecomunicaţii şi sisteme de prelucrare informaţională computerizate. Din punct de vedere social, indivizii pot interacţiona, schimba idei, partaja informaţii, asigura sprijin social, conduce afaceri, crea canale de comunicaţii în masă, participa la jocuri, angaja în discuţii politice etc. prin utilizarea reţelei globale. Termenul a devenit unul convenţional pentru a descrie orice activitate asociată cu Internetul şi diversitatea de culturi care se manifestă în această reţea de reţele [1].

În S.U.A., *spaţiul cibernetic* este definit ca o reţea independentă de infrastructuri de tehnologia informaţiei care cuprinde Internetul, reţelele de telecomunicaţii, sistemele de calculatoare, procesoarele şi dispozitivele de control electronic din ramurile industriale critice. În sens uzual, termenul desemnează mediul informaţional virtual şi interacţiunile dintre oameni care au loc prin intermediul acestuia [2].

Spaţiul cibernetic este înţeles mai corect ca un mediu de comunicare şi informare, în care tehnologia nu reprezintă numai un vector pentru dezbatere ci şi unul important pentru schimbare [3]. Acesta reprezintă un ansamblu tehnologii, produse, medii şi aplicaţii de colaborare. Aceste elemente interacţionează permanent într-un sistem evolutiv, dinamic şi impredictibil. Mai mult decât atât, sistemul este populat de o gamă vastă şi diversă de actori cuprinzând utilizatori individuali, din comunităţi ad-hoc, sectorul privat şi public, comunităţi ale securităţii naţionale etc. În mod evident, odată cu evoluţia tehnologiei şi spaţiului cibernetic este de aşteptat ca şi ameninţările şi provocările care derivă din aceasta să devină tot mai sofisticate.

1. Spaţiul cibernetic şi infrastructura informaţională critică

Cele mai elocvente preocupări privind protecţia infrastructurilor critice în corelaţie ce dezvoltarea spaţiului cibernetic se manifestă în ţările dezvoltate şi, în mod deosebit, în S.U.A.

La scurt timp după preluarea funcţiei, preşedintele Obama a dispus o revedere riguroasă a eforturilor federale pentru apărarea infrastructurii

informaţionale şi de comunicaţii a S.U.A. şi dezvoltarea unei abordări comprehensive pentru securizarea activităţilor digitale ale Americii în spaţiul cibernetic care cuprinde o gamă de măsuri privind reducerea vulnerabilităţilor şi ameninţărilor, descurajarea, angajarea internaţională, răspunsul la incidente, activităţile de restabilire şi recuperare incluzând operaţiile în reţelele de calculatoare, asigurarea informaţională, impunerea legii, misiunile diplomatice, militare şi de informaţii referitoare la securitatea şi stabilitatea infrastructurii globale informaţionale şi de comunicaţii. Scopul urmărit nu cuprinde şi alte politici informaţionale şi de comunicaţii care nu au conexiune directă cu securitatea naţională sau protecţia infrastructurii [4].

Acţiunile pe termen scurt recomandate sunt menţionate în continuare:

•Elaborarea unei politici oficiale de securitate cibernetică pentru coordonarea strategiilor şi activităţilor din acest domeniu la nivel naţional.

•Pregătirea şi aprobarea de către Preşedinte a unei strategii naţionale actualizate privind securizarea infrastructurii informaţionale şi de comunicaţii.

•Desemnarea securităţii cibernetice ca una din priorităţile esenţiale de management ale Preşedintelui şi stabilirea criteriilor de evaluare a acesteia.

•Desemnarea privaţiunilor şi libertăţilor civile pentru directoratul securităţii cibernetice.

•Stabilirea mecanismelor potrivite între agenţii privind realizarea analizelor legale referitoare la prioritățile securităţii cibernetice şi formularea unei politici unitare coerente care să clarifice rolurile, responsabilităţile şi modul de aplicare a autorităţii agenţiilor privind activităţile de securitate cibernetică.

•Iniţierea unei campanii naţionale publice de cunoaştere a situaţiei şi educaţie pentru promovarea securităţii cibernetice.

•Îmbunătăţirea punctelor de vedere ale guvernului S.U.A. privind cadrul politic internaţional referitor la securitatea cibernetică şi întărirea parteneriatelor internaţionale pentru dezvoltarea iniţiativelor care vizează întreaga gamă de activităţi, politici şi oportunităţi conexe securităţii cibernetice.

•Pregătirea unui plan de răspuns la incidentele de securitate cibernetică, iniţierea unui dialog pentru îmbunătăţirea parteneriatului public-privat şi asigurarea resurselor necesare pentru optimizarea contribuţiei şi angajamentului acestor sectoare.

•Colaborarea cu alte entităţi şi elaborarea unui cadru pentru cercetarea şi dezvoltarea strategiilor ce se concentrează pe tehnologiile de vârf care au potenţialul să îmbunătăţească securitatea, fiabilitatea, flexibilitatea şi încrederea în infrastructura digitală.

•Crearea unei viziuni şi strategii de management bazate pe securitatea cibernetică care vizează păstrarea confidenţialităţii şi libertăţilor civile, precum şi îmbunătăţirea tehnologiilor pentru naţiune.

În mai 2009, Preşedintele a acceptat recomandările rezultate din Politica Revizuită privind Spaţiul Cibernetic şi a apreciat că iniţiativele vor juca un rol esenţial în îmbunătăţirea multor prevederi din acest document [5].

Iniţiativele privind Securitatea Cibernetică Naţională Comprehensivă constau într-un număr de propuneri cu următoarele obiective privind îmbunătăţirea securităţii SUA în spaţiul cibernetic: *stabilirea unui front comun pentru apărarea împotriva ameninţărilor imediate, apărarea împotriva întregului spectru de ameninţări şi întărirea mediului de securitate cibernetică viitor*.

Aceste iniţiative vizează următoarele aspecte:

▪Gestionarea reţelei informaţionale naţionale ca un tot unitar cu conexiuni de încredere la Internet.

▪Realizarea unui sistem de senzori pentru detectarea intruziunilor la nivelul reţelei naţionale.

▪Continuarea implementării sistemului de prevenire a intruziunilor la nivelul întregii ţări.

▪Coordonarea şi reorientarea eforturilor de cercetare şi dezvoltare.

▪Interconectarea centrelor pentru operaţiile cibernetice existente pentru a îmbunătăţi cunoaşterea situaţiei.

▪Elaborarea şi implementarea unui plan guvernamental amplu de contrainformaţii în domeniul cibernetic.

▪Creşterea nivelului securităţii în reţelele cu informaţii clasificate.

▪Extinderea activităţii de educaţie cibernetică.

▪Definirea şi dezvoltarea strategiilor şi programelor privind tehnologiile avansate durabile.

▪Definirea şi dezvoltarea strategiilor şi programelor de descurajare.

▪Dezvoltarea unei abordări multilaterale pentru managementul riscurilor privind sistemul de aprovizionare global.

▪Definirea rolului statului federal privind extinderea securităţii cibernetice în domeniile infrastructurii critice.

Securitatea şi performanţele efective ale infrastructurii critice din S.U.A. şi alte ţări se bazează pe spaţiul cibernetic, sistemele de control industrial şi tehnologia informaţiei care sunt vulnerabile la întreruperi sau în exploatare. Împreună cu Guvernul, Departamentul Apărării depinde în funcţionarea sa de spaţiul cibernetic. Acesta utilizează peste 15.000 de reţele şi 7 milioane de dispozitive de prelucrare computerizată în cadrul sutelor de instalaţii dispuse într-o serie de ţări de pe tot globul pământesc. Departamentul utilizează spaţiul cibernetic

pentru activităţi militare, de informaţii şi afaceri, deplasarea personalului şi materialelor, comanda şi controlul întregului spectru de operaţii militare. În acest scop sunt stabilite 5 iniţiative strategice, după cum urmează [6]:

(1). *Departamentul Apărării va trata spaţiul cibernetic ca un domeniu operaţional şi se va organiza, instrui şi dota astfel încât să utilizeze întregul potenţial oferit de acesta.*

•Managementul riscurilor din spaţiul cibernetic prin eforturi de intensificare a instruirii, asigurare informaţională, cunoaşterea mai detaliată a situaţiei şi realizarea unei infrastructuri de reţea sigure şi fiabile;

•Asigurarea integrităţii şi disponibilităţii prin angajarea în parteneriate eficiente, realizarea apărării colective şi menţinerea unei imagini operaţionale comune;

•Realizarea capabilităţilor integrate de deplasare şi desfăşurare în zonele cele mai importante.

(2). *Departamentul Apărării va întrebuinţa noi concepte de apărare pentru a-şi proteja propriile sisteme şi reţele.*

În prima etapă, Departamentul îşi va perfecţiona metodele pentru a îmbunătăţi securitatea cibernetică proprie. În al doilea rând, pentru a descuraja şi diminua ameninţările din interiorul sistemului, va perfecţiona personalul din comunicaţii, cel cu responsabilităţi în domeniul resurselor umane, capabilităţile de monitorizare internă şi management informaţional. În al treilea rând, va întrebuinţa capacităţi active de apărare cibernetică pentru a preveni intruziunile în reţelele şi sistemele proprii. În al patrulea rând, Departamentul dezvoltă noi concepte operaţionale de apărare şi arhitecturi de prelucrare computerizată a informaţiilor.

(3). *Departamentul Apărării va colabora cu celelalte departamente şi agenţii, precum şi cu sectorul privat pentru aplicarea strategiei de securitate cibernetică.*

(4). *Departamentul Apărării va întreţine relaţii puternice cu aliaţii S.U.A. şi partenerii internaţionali pentru a întări securitatea cibernetică comună.*

(5). *Departamentul Apărării va contribui la ingeniozitatea naţiunii printr-un personal cu pregătire cibernetică superioară şi o inovaţie tehnologică rapidă.*

Cele 5 iniţiative strategice ale Departamentului îi oferă posibilitatea de a acţiona eficient în spaţiul cibernetic, a apăra interesele naţionale şi a îndeplini obiectivele securităţii naţionale.

În documentele oficiale, termenul de *protecţie a infrastructurii critice* (PIC) este utilizat în mod frecvent chiar dacă documentul se referă doar la aspectele informaţionale. Din acest motiv cele două aspecte nu pot şi nu trebuie să fie discutate ca şi concepte separate. PIC este un concept mai larg decât PIIC (*protecţia infrastructurii informaţionale critice*), dar PIIC este o componentă

esenţială a primului concept. O concentrare exclusivă pe ameninţările cibernetice care ignoră ameninţările fizice tradiţionale importante este la fel de periculoasă ca şi neglijarea dimensiunii virtuale şi, de aceea, acestea trebuie abordate într-o strânsă corelaţie [7]. În timp ce PIC cuprinde toate sectoarele infrastructurii critice naţionale, PIIC este un subset al efortului de protecţie comprehensivă care se focalizează pe măsurile pentru securizarea infrastructurii informaţionale critice (IIC). În general, IIC reprezintă o parte a infrastructurii informaţionale naţionale sau globale esenţial necesară pentru asigurarea continuităţii serviciilor furnizate de către infrastructura critică. IIC, în sens larg, constă în sectorul de telecomunicaţii şi informaţional, cuprinzând mijloacele de telecomunicaţii, calculatoarele şi software-ul, sistemele de control, supraveghere şi alarmare, Internetul etc. Termenul este utilizat, de asemenea, pentru a desemna totalitatea reţelelor de calculatoare şi comunicaţii interconectate, precum şi fluxurile de informaţii critice aferente. Datorită rolului lor de interconectare a diferitelor alte sectoare din infrastructură, precum şi datorită pericolelor care se aduc prin faptul că devin ţinte, aceste tipuri de infrastructură au un rol special care trebuie analizat ca atare. Ele sunt privite ca esenţiale pentru infrastructurile critice, datorită faptului că schimbul neîntrerupt de informaţii este foarte important pentru activităţile desfăşurate în cadrul infrastructurilor şi serviciile pe care acestea le oferă.

2. Sistemele informatice şi spaţiul cibernetic

Un sistem informatic reprezintă o combinaţie de personal, mijloace tehnice, software, reţele de comunicaţii, resurse de date, politici şi proceduri care stochează, regăsesc, transformă şi diseminează informaţii într-o organizaţie. Oamenii se bazează pe sistemele informatice moderne pentru a comunica unii cu alţii utilizând o varietate de mijloace tehnice, proceduri de prelucrare a informaţiei, canale de comunicaţii şi datele stocate [8].

Din punct de vedere conceptual, aplicaţiile sistemelor informatice implementate în infrastructura critică pot fi clasificate în diferite moduri. De exemplu, *câteva tipuri de sisteme informatice* pot fi clasificate ca operaţionale sau de management al informaţiei.

a. Asemenea *sisteme de sprijin operaţional* realizează o varietate de produse informaţionale pentru uz intern sau extern. Oricum, acestea nu evidenţiază produsele informaţionale specifice pentru uzul managerilor. De aceea, este necesară o prelucrare suplimentară de către sistemele de management al informaţiilor. Rolul sistemelor de sprijin operaţional al organizaţiei este de a procesa tranzacţiile, controla procesele industriale, sprijini comunicaţiile şi colaborarea organizaţiei şi actualiza bazele de date. Principalele sisteme de sprijin operaţional sunt următoarele:

•*Sisteme de procesare a tranzacţiilor* – prelucrează datele rezultate din tranzacţii, actualizează bazele de date şi produc documente.

•*Sisteme de control al proceselor* – monitorizează şi controlează procesele industriale.

•*Sisteme de colaborare a organizaţiilor* – sprijină echipele, grupurile de lucru, comunicaţiile şi colaborarea organizaţiei.

b. Când aplicaţiile sistemelor informaţionale se concentrează pe asigurarea informaţiilor şi sprijinul efectiv al deciziilor managerilor, acestea se numesc *sisteme de sprijin al managementului.* Din punct de vedere conceptual, câteva tipuri de sisteme informatice sprijină elaborarea deciziilor: (1) sistemele de management informaţional, (2) sistemele de sprijin decizional, (3) sisteme informatice de execuţie.

•*Sistemele de management informaţional* – asigură informaţii în rapoarte pre-definite şi le afişează pentru sprijin în elaborarea deciziilor.

•*Sistemele de sprijin decizional* – asigură sprijin interactiv ad-hoc pentru elaborarea deciziilor de către manageri şi alţi specialişti.

•*Sisteme informatice de execuţie* – asigură informaţii critice de la sistemele de management informaţional, cele de sprijin al deciziei şi alte surse adecvate pentru personalul de execuţie.

c. Alte câteva categorii de sisteme informatice pot sprijini activităţile şi aplicaţiile de management. De exemplu, *sistemele expert* pot asigura informaţii specializate pentru activităţi şi decizii manageriale. *Sistemele de management al cunoştinţelor* sprijină crearea, organizarea şi diseminarea cunoştinţelor pentru managerii şi angajaţii unei organizaţii. Sistemele informatice care sprijină funcţii de bază precum contabilitatea sau marketingul sunt cunoscute ca *sisteme funcţionale pentru afaceri*.

Sistemele informatice strategice aplică tehnologia informaţiei pentru realizarea unor produse, servicii sau afaceri ale organizaţiei pentru a obţine un avantaj strategic faţă de alţi competitori.

Este important de remarcat că aplicaţiile sistemelor informatice sunt integrate în câteva tipuri de asemenea sisteme, în funcţie de rolul îndeplinit de acestea. În practică, aceste roluri sunt combinate în *sisteme integrate sau trans-funcţionale* care oferă o varietate de funcţii. Atunci când este analizat un sistem informatic se poate observa că acesta asigură o varietate de informaţii şi funcţii pentru mai multe niveluri manageriale.

Un model de sistem informatic constă din cinci resurse majore: personal, mijloace tehnice, software, date şi reţele:

▪*Personalul* cuprinde specialişti (analişti de sistem, programatori, operatori), utilizatori finali, precum şi alţi beneficiari ai sistemelor informatice.

▪*Mijloace tehnice* – echipamente (calculatoare, monitoare, discuri magnetice, imprimante, scannere) şi suporţi media (discuri optice, benzi magnetice, card-uri din plastic, formulare din hârtie).

▪*Resursele de date* – descrierea produselor, înregistrări privind clienţii, fişierele angajaţilor, catalogul bazelor de date.

▪*Resursele de reţea* – mediile de comunicaţii, procesoare, software de acces şi control al reţelei.

▪*Produse informaţionale* – rapoarte de management şi afaceri, documente în format text şi grafic, înregistrări audio, documente scrise.

Odată cu dezvoltarea tehnologiei informaţiei şi infrastructura critică devine tot mai dependentă de sistemele computerizate pentru controlul activităţilor, prelucrarea, înregistrarea şi raportarea informaţiilor esenţiale. Organizaţiile publice şi private se bazează pe sistemele computerizate pentru transferul unor sume mari de bani şi a unor informaţii importante, conducerea activităţilor şi livrarea serviciilor către beneficiari. Securitatea acestor sisteme şi date este esenţială pentru securitatea naţională şi economică, sănătatea şi siguranţa publică. În mod contrar, mijloacele de securitate ineficientă pot conduce la riscuri semnificative: pierderi de resurse (colectări de fonduri şi taxe naţionale); acces inadecvat la informaţii senzitive (securitate naţională, personal, plătitorii de taxe); perturbarea activităţilor care sprijină infrastructura critică, apărarea naţională sau serviciile de urgenţă etc. [9]. Ameninţările la adresa sistemelor informaţionale care sprijină infrastructura critică devin tot mai numeroase şi sofisticate. Conectivitatea dintre sistemele informatice, Internet şi alte infrastructuri creează de asemenea oportunităţi pentru atacatori pentru întreruperea telecomunicaţiilor, alimentării cu energie electrică şi a altor servicii critice.

O activitate foarte importantă pentru protecţia infrastructurii informaţionale critice constă în verificare modului în care sunt implementate standardele şi recomandările specifice. În acest sens, se evidenţiază câteva direcţii de acţiune care vizează: standardele privind securitatea cibernetică; eforturile naţionale pentru recrutarea, instruirea şi profesionalizarea specialiştilor în securitate cibernetică; eforturile naţionale pentru asigurarea tehnologiei informaţiei în sistemele de aprovizionare etc. În plus, pentru îmbunătăţirea capabilităţilor naţionale privind securitatea cibernetică organizaţiile trebuie să-şi perfecţioneze capacităţile de analiză cibernetică şi avertizare şi să întărească parteneriatul dintre sectoarele public şi privat în securizarea cibernetică a infrastructurii critice.

Un apreciat om de ştiinţă american prezintă, într-o lucrare tipărită recent, o nouă metodologie de analiză şi protecţie a infrastructurii critice împotriva atacurilor cibernetice utilizând 10 principii de bază[10]:

a. *Inducerea în eroare* care implică introducerea deliberată a funcţionalităţii eronate sau a informaţiilor false în cadrul infrastructurii informaţionale critice în scopul de a dezinforma un adversar. Anunţul public privind utilizarea inducerii în eroare creează pentru adversari incertitudini deoarece ei nu-şi dau seama dacă problema descoperită este reală sau o capcană. Această metodă este utilă pentru analiza comportamentului, în timp real, în cazul în care un intrus din reţea este prins în capcană.

b. S*epararea* care implică întărirea restricţiilor în politicile de acces ale utilizatorilor şi resurselor într-un mediu computerizat. Separarea reţelei este realizată prin utilizarea de *firewalls*, dar programele de protecţie a infrastructurii informaţionale critice solicită trei modificări specifice: *firewalls* pentru reţele de infrastructură de mare capacitate, interne şi pentru aplicaţii şi protocoale specifice.

c. *Diversitatea* cere selectarea şi utilizarea tehnologiei şi sistemelor care au în mod intenţionat funcţionare diferită. Diversitatea produselor, serviciilor şi tehnologiilor care sprijină infrastructura naţională reduce şansele ca o deficienţă comună să poată fi exploatată pentru producerea unui atac în cascadă. De aceea, este necesar un program de coordonare a achiziţiilor şi management al furnizorilor pentru a obţine un nivel dorit al diversităţii naţionale pentru toate categoriile de mijloace.

d. *Caracteristicile comune* care necesită aceeaşi atenţie privind cele mai bune măsuri de securitate în toate sectoarele infrastructurii critice. Această metodă utilizată în managementul infrastructurii critice determină ca nici una din componente nu este mai puţin gestionată sau lăsată complet fără protecţie. În acest scop sunt necesare programe de selecţie a standardelor şi validarea acestora.

e. *Profunzimea* care implică utilizarea nivelurilor multiple de securitate pentru mijloacele din infrastructura critică. Utilizarea apărării în profunzime în infrastructura critică determină ca nici un mijloc important să se bazeze pe un singur nivel de securitate. La nivel naţional este necesară o analiză care să asigure că toate mijloacele critice sunt protejate cel puţin prin două niveluri.

f. *Discreţia* care implică indivizii şi grupurile ce iau decizii de a nu divulga informaţii senzitive privind infrastructura critică. Protecţia infrastructurii la scară largă nu poate fi corectă până ce nu este promovată o cultură naţională privind discreţia şi păstrarea secretului.

g. *Colectarea* care implică obţinerea automată a informaţiilor din sistemele interconectate despre infrastructura naţională care să permită analiza securităţii acesteia. Protecţia infrastructurii naţionale solicită o abordare privind colectarea datelor acceptabilă pentru cetăţeni şi care să asigure nivelul de detaliere cerut pentru analiza securităţii.

h. *Corelarea* care implică un mod specific de analiză ce poate fi realizată asupra factorilor privitori la protecţia infrastructurii critice. Acest principiu este cel mai important pentru toate tehnicile de analiză a securităţii cibernetice. Corelarea la nivel naţional trebuie realizată prin utilizarea tuturor surselor disponibile şi a celei mai bune tehnologii.

i. *Cunoaşterea situaţiei* care solicită unei organizaţii să observe diferenţele în timp real şi să le sesizeze pe cele anormale în infrastructura critică. Un program de cunoaştere a situaţiei trebuie implementat pentru a se asigura managementul decizional corect al mijloacelor naţionale.

j. *Răspunsul* care implică asigurarea ca procesele în desfăşurare să răspundă la orice indiciu disponibil referitor la securitate. Răspunsul la incidentele privind protecţia infrastructurilor critice este dificil de perceput datorită dependenţelor şi interacţiunilor dintre organizaţiile dispuse disparat. De aceea, acesta este realizat cel mai bine la nivel naţional pe baza indiciilor timpurii, decât pe baza incidentelor care deja au produs daune la nivelul mijloacelor naţionale.

Pentru utilizatorii individuali, securitatea cibernetică este mai bine înţeleasă ca o combinaţie între securitatea calculatoarelor şi securitatea reţelei. *Securitatea calculatoarelor* reprezintă protecţia sistemului (hardware şi software) şi a informaţiilor pe care transportă de sustragere, denaturare sau interzicere a accesului la acestea. Aceasta implică atât măsuri fizice privind limitarea accesului la sistemele de tehnologia informaţiei şi comunicaţiilor (TIC) şi controlul numărului de utilizatori, precum şi digitale care vizează crearea unei arhitecturi TIC şi a unui sistem de operare sigure, utilizarea unui software de securizare şi împotriva viruşilor. Într-o singură exprimare, scopul securităţii calculatoarelor este de a realiza securizarea la nivelul fiecărei părţi a unui sistem [11].

Securitatea calculatoarelor este completată de **securitatea reţelei**. Când vulnerabilităţile pleacă de la o conexiune în reţea este necesară securizarea reţelei de calculatoare şi a informaţiilor conţinute împotriva distrugerii sau perturbării. Securitatea reţelei cuprinde o gamă largă de instrumente de control fizic şi administrativ, precum şi electronice (firewalls, criptare, software de autentificare şi antivirus, sistem de detectare a intruziunilor).

La un anumit nivel, atât sectorul comercial privat cât şi guvernele naţionale au adoptat o abordare tehnologică privind securitatea cibernetică, de obicei exprimată sintetic prin terminologia de *securitate a informaţiei*. Termenul de securitate a informaţiei exprimă protecţia informaţiei şi a sistemelor informatice împotriva accesului neautorizat, utilizării, divulgării, întreruperii, modificării sau distrugerii în scopul de a asigura *integritatea* (protecţia împotriva modificării sau distrugerii prin non-repudiere şi autentificare), confidenţialitatea (prezervarea prin

acces autorizat, păstrarea secretului şi a posesiei informaţiei) şi disponibilitatea (asigurarea accesului oportun şi sigur la informaţie, precum şi utilizarea acesteia).

Asigurarea informaţională este definită drept încrederea că sistemele informatice vor proteja informaţiile pe care le deţin şi vor fi utilizate când este necesar în locul şi la momentul solicitate, sub controlul utilizatorilor legitimi.

3. Sisteme de control şi avertizare sigure

Interconectarea extinsă a sistemelor informatice conduce la serioase riscuri pentru organizaţii, naţiuni şi infrastructurile lor critice pe care le sprijină [12].

Sistemele de control se bazează pe computere şi sunt utilizate în cadrul infrastructurilor critice pentru monitorizarea şi controlul proceselor senzitive, precum şi a funcţiilor fizice. Sistemele de control colectează datele operaţionale de la senzorii distribuiţi, prelucrează şi afişează aceste informaţii şi le retransmit la echipamentele de control locale sau distante. Există două tipuri de sisteme de control: (1) *sisteme de control distribuite* utilizate în cadrul unei uzine de prelucrare sau generare sau la nivelul unei zone geografice mici; (2) *sistemele de control de supervizare şi achiziţie a datelor* (SCADA) utilizate pentru activităţi desfăşurate pe zone geografice întinse.

Din punct de vedere istoric, *securitatea privind controlul* se referea, în primul rând, la protecţia împotriva atacurilor fizice şi prevenirea utilizării abuzive a locaţiilor de filtrare şi prelucrare sau a mijloacelor de distribuţie şi păstrare. Oricum, se recunoaşte că sistemele de control sunt vulnerabile la atacuri cibernetice. Câţiva factori au contribuit la creşterea riscurilor la adresa sistemelor de control: adoptarea tehnologiilor standardizate cu vulnerabilităţile cunoscute; conectarea sistemelor de control la alte reţele; conexiuni la distanţă nesigure; larga disponibilitate a informaţiilor tehnice despre sistemele de control.

a. În prezent, pentru a reduce costurile şi îmbunătăţi performanţele, organizaţiile trec de la *sistemele proprietare* la *tehnologiile standardizate*, mai puţin costisitoare, care utilizează protocoale de reţea tip Internet. Acestea sunt utilizate pe scară largă, dispun de tehnologie standardizată cu vulnerabilităţi bine cunoscute, au dispozitive sofisticate şi uşor de exploatat, sunt disponibile pe scară largă. Ca urmare, atât numărul persoanelor cu cunoştinţe pentru a desfăşura atacuri cât şi cel al sistemelor de control care pot fi subiect de atac au crescut considerabil. De asemenea, protocoalele şi standardele comune de comunicaţii fac ca informaţiile transmise prin sistemele de control să fie uşor de interpretat de către un *hacker*.

b. Organizaţiile integrează deseori sistemele lor de control cu reţelele proprii. Această conectivitate crescută are avantaje semnificative: asigurarea factorilor de decizie cu informaţii în timp real; facilitatea oferită personalului tehnic de a monitoriza şi controla procesele din cadrul sistemelor de control din

diferite puncte ale reţelei organizaţiei. În plus, reţelele organizaţiei sunt adesea conectate cu reţelele partenerilor strategici şi la Internet. Această convergenţă a reţelelor de control cu cele de întreprindere şi publice creează potenţiale vulnerabilităţi privind securitatea sistemelor de control.

c. Vulnerabilităţile din sistemele de control sunt amplificate de conexiunile nesecurizate. Organizaţiile permit adesea accesul la conexiuni pentru diagnosticarea defecţiunilor de la distanţă, mentenanţă şi examinarea stării sistemului de control. Dacă asemenea conexiuni nu sunt protejate prin autentificare sau criptare, creşte riscul de penetrare în sistem şi punctele controlate de la distanţă a persoanelor neautorizate. De asemenea, sistemele de control pot utiliza mijloace de comunicaţii radio (*wireless*) vulnerabile la atacuri electronice sau linii comerciale care pot fi accesate fizic foarte uşor.

d. *Informaţii publice despre infrastructuri şi sistemele de control sunt disponibile pentru potenţialii hackeri şi persoanele rău intenţionate*. Informaţii semnificative despre sistemele de control (documentele de proiectare şi mentenanţă, standardele tehnice privind interconectarea, protocoalele de comunicaţie între echipamente) sunt disponibile cu mare uşurinţă, fapt ce determină ca *hackerii* să intre în posesia lor, să le utilizeze şi să provoace serioase daune sistemelor din infrastructură şi celor de control. De asemenea, există numeroşi foşti angajaţi, distribuitori, contractori, utilizatori finali ai acestor sisteme care posedă cunoştinţe despre funcţionarea şi utilizarea echipamentelor şi sistemelor de control.

Sistemele de control pot fi vulnerabile la atacuri cibernetice. Entităţile sau indivizii cu intenţii rele pot desfăşura una sau mai multe din următoarele acţiuni pentru a ataca cu succes sistemele de control [13]:

• întreruperea funcţionării sistemelor de control prin întârzierea sau blocarea fluxului de informaţii în reţelele de control, prin negarea disponibilităţii reţelelor pentru operatorii sistemelor de control;

• efectuarea de modificări neautorizate în instrucţiunile de programare ale echipamentelor, modificarea intrărilor în sistemele de alarmă sau emiterea unor comenzi neautorizate pentru controlul echipamentelor care pot conduce la distrugerea acestora, întreruperea prematură a proceselor sau chiar deconectarea echipamentelor de control;

• transmiterea de informaţii false către operatorii sistemelor de control în scopul de a ascunde schimbările neautorizate sau să determine unele acţiuni inadecvate ale operatorilor sistemului;

• modificarea software-ului sistemului de control conducând la rezultate impredictibile;

• producerea de interferenţe pentru operaţiunile de siguranţă ale sistemului.

Specialiştii din sistemele de control se confruntă cu câteva provocări privind securizarea sistemelor de control împotriva atacurilor cibernetice. Aceste provocări cuprind: limitările tehnologiilor actuale pentru securizarea sistemelor de control; percepţia că sistemele de securizare a controlului nu sunt justificate din punct de vedere economic; priorităţile contradictorii în cadrul organizaţiilor privind securitatea sistemelor de control.

Eforturile pentru întărirea securităţii cibernetice a sistemelor de control sunt orientate în următoarele direcţii:

• cercetarea şi dezvoltarea unor noi tehnologii pentru protecţia sistemelor de control;

• dezvoltarea cerinţelor şi standardelor pentru securitatea sistemelor de control;

• creşterea nivelului de cunoaştere a situaţiei şi partajarea informaţiilor privind implementarea unor arhitecturi de securitate mult mai sigure şi a tehnologiilor de securitate existente;

• implementarea programelor de management eficient al securităţii, inclusiv a politicilor şi instrucţiunilor care vizează securitatea sistemelor de control.

În concluzie, sistemele informatice au un rol important în protecţia infrastructurilor critice împotriva atacurilor cibernetice. De aceea, în fiecare organizaţie trebuie dezvoltate, testate şi implementate programe pentru asigurarea securităţii informaţiei şi a sistemelor informatice prin următoarele măsuri: analiza periodică a riscurilor şi dimensiunilor distrugerilor privind informaţiile şi sistemele informaţionale; politici şi proceduri bazate pe analiza riscurilor pentru reducerea riscurilor securităţii informaţionale la un nivel acceptabil şi asigurarea că aceasta se realizează pe întreaga durată a ciclului de viaţă a fiecărui sistem informatic; coordonarea planurilor pentru asigurarea securităţii informaţionale adecvate pentru reţele, mijloace şi sisteme sau grupuri de sisteme informatice; instruirea privind modul de analiză a securităţii a personalului organizaţiei, contractorilor şi utilizatorilor din sistemele informatice; testarea periodică şi evaluarea eficienţei politicilor, procedurilor şi metodelor practice de asigurare a securităţii informaţiei, a managementului operaţional şi tehnic pentru sistemele informatice importante; un proces pentru planificarea, implementarea, evaluarea şi verificarea acţiunilor de remediere a deficienţelor din politicile, procedurile şi practicile de asigurare a securităţii informaţiei la nivelul organizaţiei; proceduri pentru detectarea, raportarea şi răspunsul la incidentele de securitate; planuri şi proceduri care să asigure funcţionarea continuă a sistemelor informatice care sprijină activităţile şi mijloacele organizaţiei.

NOTE BIBLIOGRAFICE

[1] http://en.wikipedia.org/wiki/Cyberspace/

[2] The White House, *The Comprehensive National Cybersecurity Initiative* (Washington, D.C.: March 2, 2010).

[3] Paul Cornish, Rex Hughes and David Livingstone, *Cyberspace and the National Security of the United Kingdom Threats and Responses* (A Chatham House Report, London, March 2009).

[4] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: June 19, 2009).

[5] *The Comprehensive National Cybersecurity Initiative*.

[6] U.S. Department of Defense, *DoD Strategy for Operating in Cyberspace* (Washington, D.C.: July 20, 2011).

[7] Elgin M. Brunner and Manuel Suter, *International CIIP Handbook: An Inventory of 25 National and 7 International Critical Infrastructure Protection* (Center for Security Studies, Zurich, 2008).

[8] James A. O'Brien, George M. Marakos, *Introduction to Information Systems* (McGraw Hill, New York, 2007).

[9] U.S. General Accounting Office, *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems,* GAO-11-463T (Washington, D.C.: March 16, 2011).

[10] Edward G. Amoroso, *Cyber Attacks: Protecting National Infrastructure* (Elsevier Inc., New York, 2011).

[11] *Cyberspace and the National Security of the United Kingdom Threats and Responses*.

[12] U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems,* GAO-04-628T (Washington, D.C.: March 30, 2004).

[13] U.S. General Accounting Office, *Federal Information Systems Controls Audit Manual*, GAO-09-232G (Washington, D.C.: February 12, 2009).