RISCURI DE SECURITATE ÎN SPAȚIUL CIBERNETIC

SECURITY RISKS IN CYBER SPACE

Col.drd. Cătălin-Iulian BALOG *

Spațiul cibernetic – o schimbare de paradigmă în conceptul de securitate. Atacurile teroriste din 11 septembrie 2001 au avut un impact global profund, forțând guvernele statelor şi societatea, în ansamblu, să reexamineze conceptele de securitate națională şi să includă posibilitatea unor atacuri neconvenționale, desfăşurate în spațiul cibernetic.

Cyber space – a shift of paradigm in the security concept. The terrorist attacks on September 11, 2001 had a profound global impact, forcing governments and society, as a whole, to review the national security concepts and include the possibility of unconventional attacks carried out in cyber space.

Cuvinte-cheie: spațiu cibernetic; securitate; riscuri; infrastructuri critice; vulnerabilități; amenințări.
Keywords: *cyber space; security; risks; critical infrastructures; vulnerabilities; threats*

„Somewhere in the world someone is training
when you are not. When you race him, he will win”.
Tom FLEMING[1]

O lume dependentă de spațiul cibernetic

Pentru toate statele occidentale dezvoltate, dar şi pentru cele care aspiră la modul de viață occidental, revoluția în domeniul tehnologiei informației şi comunicațiilor a schimbat aproape imperceptibil modul în care funcționează mediul economic şi cel politic. Lipsite de o gândire profundă cu privire la modul de asigurare a securității, lumea modernă a pierdut controlul, concentrându-şi atenția asupra proceselor esențiale de producție, asigurarea de servicii financiar-bancare, comunicații şi telecomunicații. Ca urmare, atât costurile de producție, cât şi productivitatea au cunoscut evoluții semnificative, cele dintâi în scădere şi cele din urmă în creştere. În context, trebuie menționată tendința continuă spre o mai mare utilizare a sistemelor de calcul interconectate.

Începând cu noul mileniu, economia mondială şi securitatea națiunilor dezvoltate au devenit dependente complet de tehnologia informației şi a infrastructurii de comunicații. Un număr impresionant de rețele de calculatoare şi sisteme de comunicații asigură în mod direct funcționarea tuturor sectoarelor de activitate din sfera publică şi privată fie că este vorba despre sectorul energetic (energie electrică, petrol şi gaze), transport (feroviar, maritim şi aerian), financiar-bancar, comunicații şi telecomunicații, servicii de urgență şi utilitate publică, apărare națională etc. Prin intermediul acestora se controlează, de asemenea, obiecte fizice, cum ar fi, transformatoare electrice, sisteme de pompare, instalații chimice, sisteme de dirijare a traficului (terestru, maritim şi aerian), trenuri, vapoare, avioane şi sateliți artificiali.

Raza de acțiune a acestor rețele de calculatoare şi sisteme de comunicații care formează infrastructura critică de comunicații depăşeşte limitele spațiului cibernetic, punându-şi amprenta asupra existenței umane, în ansamblu.

Vulnerabilități şi amenințări în spațiul cibernetic

În spațiul cibernetic există o serie de indivizi sau entități rău intenționate care pot iniția atacuri împotriva infrastructurii critice de comunicații. În acest sens, o preocupare majoră a autorităților guvernamentale, precum şi a unor entități private, o reprezintă posibilitatea ca un atac cibernetic organizat să fie capabil să provoace daune majore infrastructurii critice de comunicații, economiei sau chiar să afecteze securitatea națională a unui stat.

Universitatea Națională de Apărare „Carol I”
e-mail: *catalin.balog@gmail.com*

Însă, cunoştinţele teoretice şi capacităţile tehnice necesare pentru a efectua un astfel de atac sunt deosebit de complexe – ceea ce ar putea explica parţial lipsa unui atac cu astfel de efecte, până în prezent. Pe lângă acestea există şi riscul exploatării unor vulnerabilităţi care să implice efecte încă ignorate sau chiar negândite.

În prezent, încă există incertitudini referitoare la intenţiile sau capacităţile distructive ale unora dintre atacurile înregistrate în spaţiul cibernetic, ştiut fiind faptul că efectul acestora nu este întotdeauna unul vădit. De aceea este necesară o analiză îmbunătăţită pentru a identifica vulnerabilităţile, tendinţele ameninţărilor şi evaluarea efectelor atacurilor cibernetice, pe termen lung. Ceea ce se ştie este faptul că metodologiile şi instrumentele de atac devin disponibile pe scară largă, iar cunoştinţele teoretice şi capacităţile tehnice ale utilizatorilor cu astfel de preocupări se îmbunătăţesc permanent.

Din cauza perfecţionării metodologiilor şi instrumentelor de atac, un număr tot mai mare de indivizi sau entităţi sunt capabile să lanseze atacuri cibernetice semnificative la nivel naţional, iar frecvenţa acestora este în continuă creştere.

În timp de pace, adversarii sau inamicii unei naţiuni pot desfăşura acţiuni de spionaj care vizează activitatea instituţiilor guvernamentale, centrelor de cercetare şi companiilor naţionale sau multinaţionale. De asemenea, pot să se pregătească pentru executarea unor atacuri cibernetice ulterioare prin cartografierea infrastructurilor critice naţionale, identificarea obiectivelor cheie, generând breşe de securitate controlate prin programe specializate *(back doors)* sau prin alte mijloace (infiltrarea de agenţi).

În timp de criză sau război, aceştia pot încerca intimidarea liderilor politici şi a formatorilor de opinie prin atacarea infrastructurilor critice de comunicaţii şi alterarea funcţiilor economice cheie sau prin erodarea încrederii populaţiei în sistemele de informare publică.

Astfel de atacuri cibernetice pot avea consecinţe deosebit de grave, iar contracararea lor necesită dezvoltarea unor capacităţi de apărare extrem de rapide şi robuste. Doar astfel pot fi reduse vulnerabilităţile şi pot fi descurajaţi indivizii sau entităţile rău intenţionate.

Spaţiul cibernetic permite un atac organizat asupra infrastructurii critice a unei naţiuni, de la distanţă. Iniţiatorii unui asemenea demers au nevoie doar de tehnologia adecvată care le va permite ascunderea identităţii, dispunerea fizică şi breşele de securitate. Nu numai că spaţiul cibernetic oferă posibilitatea de a exploata punctele slabe ale infrastructurilor critice, dar oferă, de asemenea, un sprijin semnificativ pentru executarea unor atacuri fizice, permiţând perturbarea comunicaţiilor, întârzierea unei intervenţii de urgenţă şi împiedicând un răspuns adecvat (defensiv sau ofensiv) – elemente esenţiale în urma unui atac fizic.

Se poate aprecia că în trecut (secolul XX), izolarea geografică a constituit o piedică în calea unei invazii fizice directe a unor state, precum Statele Unite. În prezent, din perspectiva spaţiului cibernetic, graniţele naţionale nu mai au acelaşi sens, acestea diluându-se într-o foarte mare măsură. Chiar şi infrastructura – *software* şi *hardware* – care alcătuieşte spaţiul cibernetic devine globală, dacă avem în vedere proiectarea şi dezvoltarea sa. Din această cauză, a globalizării spaţiului cibernetic, orice potenţială vulnerabilitate poate fi exploatată de către oricine, oriunde s-ar afla, cu condiţia să dispună de suficiente cunoştinţe teoretice şi capacităţi tehnice pentru a o „valorifica”, transformând-o într-o ameninţare reală.

Reducerea vulnerabilităţilor în absenţa ameninţărilor

Infrastructurile critice naţionale trebuie să facă faţă unor ameninţări specifice, imediat ce acestea apar. Din acest motiv, încercarea de depistare a unui atac iminent asupra infrastructurii critice înainte de eliminarea vulnerabilităţilor semnificative reprezintă o strategie riscantă şi chiar contraindicată. Un atac cibernetic se poate declanşa printr-o reţea naţională şi se poate răspândi rapid şi fără avertisment, la nivel internaţional, astfel încât numeroase victime nu vor avea timp să afle ce s-a întâmplat. Chiar şi în situaţia unei avertizări prealabile, un mare număr de presupuse victime nu dispun de cunoştinţele teoretice şi capacităţile tehnice minime pentru a se proteja.

Un lucru deosebit de important pentru organizaţiile a căror activitate principală presupune utilizarea unei infrastructuri de comunicaţii îl reprezintă necesitatea aplicării unor măsuri proactive de identificare şi de remediere a vulnerabilităţilor, în mod continuu şi în ritm permanent. Un audit de securitate realizat de către profesionişti pentru evaluarea vulnerabilităţilor unei infrastructuri de comunicaţii poate dura chiar şi câteva luni de zile. Ulterior, procesul de dezvoltare şi de implementare

a unei strategii de apărare structurată pe niveluri şi a unei infrastructuri rezistente pentru a permite remedierea celor mai grave vulnerabilități ar mai putea dura alte luni. Iar acest proces trebuie repetat, cu regularitate.

Amenințări şi vulnerabilități: o problemă cu cinci niveluri

Datorită numărului şi diversității utilizatorilor prezenți în spațiul cibernetic, gestionarea amenințărilor şi reducerea vulnerabilităților în acest domeniu reprezintă o provocare extrem de complexă. De asemenea, având în vedere numărul calculatoarelor şi al sistemelor de comunicații existente în spațiul cibernetic, asigurarea securității necesită acțiuni desfăşurate pe mai multe niveluri, de către grupuri diferite de utilizatori. Problema securității în spațiul cibernetic poate fi cel mai bine abordată ca o problemă cu cinci niveluri.

• **Nivelul 1**, *Home Users / Small Business*

Deşi nu fac parte dintr-o infrastructură critică, calculatoarele utilizatorilor individuali şi întreprinderilor mici şi mijlocii pot deveni parte a rețelelor de calculatoare controlate de la distanță, folosite ulterior pentru atacarea infrastructurilor critice. Calculatoarele lipsite de apărare ale utilizatorilor individuali şi întreprinderilor mici şi mijlocii, în special cele care folosesc conexiuni de tip DSL *(Digital Subscriber Line)* sau conexiuni prin cablu sunt vulnerabile la atacuri care pot angaja utilizarea acestora fără ştirea proprietarului. Grupuri astfel constituite de calculatoare „zombie” pot fi apoi utilizate de către terți actori pentru a lansa atacuri de tip DoS *(Denial of Service)* asupra nodurilor cheie de *Internet*, companiilor importante sau chiar asupra infrastructurilor critice.

• **Nivelul 2,** *Large Enterprises*

Întreprinderile mari (societăți comerciale, agenții guvernamentale şi universități) reprezintă obiective obişnuite ale atacurilor cibernetice. Multe dintre acestea sunt parte a infrastructurilor critice. Întreprinderile mari necesită în mod clar politici active şi articulate de securitate a informațiilor şi programe de supraveghere, în conformitate cu cele mai bune practici în domeniu. Se poate aprecia că rețelele de calculatoare ale acestor întreprinderi se vor confrunta cu o creştere a atacurilor inițiate de indivizi sau entități rău intenționate, având în vedere datele şi informațiile, dar şi puterea de calcul de care acestea dispun.

• **Nivelul 3,** *Critical Sectors / Infrastructures*

Atunci când organizații din sectorul economic, guvernamental sau academic îşi unesc eforturile pentru abordarea unor probleme comune de natură cibernetică, se pot reduce sarcinile individuale ale unei întreprinderi. De foarte multe ori, astfel de colaborări pot da naştere unor instituții şi mecanisme comune, care prezintă, la rândul lor, anumite vulnerabilități a căror exploatare afectează în mod direct activitatea organizațiilor partenere şi a sectorului, în ansamblu. Totodată, întreprinderile pot contribui la reducea riscurilor din spațiul cibernetic prin participarea la grupuri de lucru care elaborează recomandări de specialitate, evaluări tehnologice, certificări de produse şi servicii şi distribuie informații.

Ca şi în alte domenii, nevoia de a reacționa rapid cu specialişti care înțeleg complexitatea unor astfel de amenințări a dus la apariția echipelor de răspuns la incidente de securitate informatică, cunoscute sub denumirea de echipe de tip CERT sau CSIRT[2]. Acestea reprezintă, de asemenea, un instrument pentru schimbul de informații cu privire la tendințele de atac, amenințări şi vulnerabilități, precum şi cele mai bune practici în spațiul cibernetic.

• **Nivelul 4,** *National Issues and Vulnerabilities*

Unele probleme din spațiul cibernetic au implicații majore, la nivel național şi nu pot fi rezolvate de către o întreprindere sau un sector, în mod singular. Toate sectoarele de activitate la nivel național utilizează Internetul. În consecință, toate acestea sunt expuse aceluiaşi risc în cazul în care unele dispozitive, la nivel național, nu prezintă siguranță. De asemenea, anumite deficiențe – *software* sau *hardware* – utilizate pe scară largă pot genera probleme, la nivel național, care necesită activități coordonate pentru cercetarea şi dezvoltarea unor tehnologii îmbunătățite. Totodată, şi numărul insuficient al profesioniştilor certificați în domeniul securității cibernetice reprezintă o problemă de nivel național.

• **Nivelul 5**, *Global*

Sistemul WWW *(World Wide Web)* este o rețea de informații globală. Existența standardelor comune la nivel internațional permite interconectarea şi interoperabilitatea sistemelor de calculatoare şi comunicații din lumea întreagă. Acest fapt creează premisele extinderii unor probleme de pe un continent pe altul. Prin urmare, este esențială cooperarea internațională pentru distribuirea

informațiilor referitoare la problemele din spațiul cibernetic, precum şi pentru urmărirea infractorilor cibernetici. În lipsa acestei forme de cooperare, capacitatea colectivă de a detecta, a descuraja şi a reduce efectele atacurilor din spațiul cibernetic ar fi mult diminuată.

Noile vulnerabilități necesită răspuns continuu

Noi vulnerabilități sunt create sau descoperite în ritm permanent. Prin urmare, procesul de securizare a rețelelor şi a sistemelor trebuie să se desfăşoare în mod continuu. Statisticile elaborate de organismele de tip CERT indică faptul că numărul incidentelor şi atacurilor cibernetice este în creştere, într-un ritm alarmant. De asemenea, numărul vulnerabilităților pe care un posibil agresor le-ar putea exploata. Se apreciază că, începând cu anul 2000, vulnerabilitățile identificate în sistemele de securitate ale rețelelor de calculatoare şi sistemelor de comunicații – defecte de natură *software* şi *hardware*, care ar putea permite accesul neautorizat sau provoca daune – au cunoscut o creştere semnificativă.

Simpla instalare a unor programe de securitate (de exemplu, antivirus, *firewall*) nu poate fi un substitut pentru menținerea şi actualizarea elementelor de apărare într-o rețea de calculatoare sau într-un sistem de comunicații. Vulnerabilitățile, în marea lor majoritate, pot fi reduse prin cunoaşterea şi implementarea bunelor practici de securitate (de exemplu, actualizări periodice permanente).

Securitatea cibernetică şi oportunități de cost

În sectoarele economice, în general, şi în industria tehnologiei informației şi comunicațiilor, în particular, lipsa unor sisteme de informații sigure şi fiabile reprezintă un obstacol pentru creşterea economică. O mare parte din potențialul de creştere economică datorat evoluției din acest domeniu nu este atins din cauza riscurilor de securitate din spațiul cibernetic, riscuri care se extind asupra tranzacțiilor economice. Aceste riscuri de securitate pot afecta proprietatea intelectuală, operațiunile de afaceri, serviciile de infrastructură şi încrederea consumatorilor etc.

Atât pentru întreprinderile mici, mijlocii şi mari, cât şi pentru organizațiile din sectorul economic, guvernamental sau academic, în ansamblu, îmbunătățirea securității necesită investiții majore de atenție, timp şi bani. Însă, costurile acestor investiții se pot ameliora prin implementarea unor soluții de electronice de bună guvernare, management modern, controlul pierderilor şi reducerea fraudelor.

Deşi investițiile în infrastructura de comunicații generează cheltuieli de regie suplimentare, ele produc, în schimb, o rentabilitate a investiției. Astfel, se pot face următoarele aprecieri:

• cu toate că estimarea consecințelor unui atac cibernetic grav este operațiune destul de dificilă, costurile asociate cu investiția într-un program de securitate cibernetică pentru prevenirea şi evitarea unui astfel de atac sunt mult mai mici;

• proiectarea şi implementarea unor protocoale de securitate puternice în arhitectura rețelelor şi a sistemelor unei întreprinderi poate avea ca efect reducerea costurilor operaționale totale, prin dezvoltarea unor procese suplimentare care să urmărească reducerea costurilor (de exemplu, accesul la distanță şi interacțiuni cu clienții sau lanțurile de aprovizionare), lucru imposibil în lipsa de măsuri de securitate adecvate.

Aceste rezultate sugerează faptul că o întreprindere care conştientizează riscurile de securitate din spațiul cibernetic poate beneficia de creşterea nivelului său de securitate cibernetică.

Concluzii

Elemente de management al riscului

Până de curând, grupuri şi rețele de crimă organizată au produs doar daune limitate, în lumea întreagă. În prezent, utilizatori individuali şi întreprinderi mici şi mijlocii suferă prejudicii semnificative, aproape zilnic. Deşi există condiții favorabile pentru aplicarea unor măsuri relative de limitare a pierderilor, acestea sunt afectate de existența simultană a unor elemente nefavorabile:

- indivizi sau entități cu potențial de rele intenții;
- metodologii şi instrumente de atac care proliferează;
- vulnerabilități ale infrastructurilor critice de comunicații.

În spațiul cibernetic, nicio strategie izolată/singulară nu poate elimina complet vulnerabilitățile şi amenințările asociate acestora. Iată de ce, organismele naționale şi internaționale trebuie să acționeze în mod responsabil pentru gestionarea riscurilor şi extinderea capacităților de reducere şi eliminare a daunelor produse de atacurile cibernetice. Reexaminarea conceptelor

de securitate națională şi apariția strategiilor de securitate cibernetică impune o prioritate sporită acordată apărării cibernetice, alături de celelalte componente ale apărării naționale.

Asigurarea securității cibernetice

Nici un stat nu poate asigura securitatea spațiului cibernetic național, de unul singur. Nici un stat nu ar putea – şi, poate, nu ar trebui – să asigure securitatea rețelelor de calculatoare şi a sistemelor de comunicații din sectorul privat. De asemenea, „statul” nu trebuie să pătrundă în casele oamenilor şi în întreprinderi – fie că este vorba despre întreprinderi mici şi mijlocii sau întreprinderi mari (societăți comerciale, agenții guvernamentale şi universități) – pentru a crea rețele de calculatoare şi sisteme de comunicații sigure. Fiecare cetățean care depinde de spațiul cibernetic trebuie să-şi asigure securitatea în partea pe care o deține sau pentru care este responsabil.

În pofida atenției care se acordă asigurării securității cibernetice şi a măsurilor luate până în prezent pentru îmbunătățirea şi creşterea capacității de apărare şi reacție, riscurile de securitate în spațiul cibernetic constituie o preocupare continuă a tuturor organismelor de profil şi a factorilor decidenți. Reducerea acestor riscuri necesită realizarea unor parteneriate active, fără precedent, între componentele apărării cibernetice naționale şi cu partenerii noştri, la nivel internațional.

NOTE:

1 Tom Fleming (născut la 23.07.1951) este atlet american, câştigător al maratonului din New York, în anii 1973 şi 1975.

2 CERT reprezintă un acronim pentru *Computer Emergency Response Team*, deşi mult mai potrivit ar fi *Cyber Security Incident Response Team* – CSIRT.

BIBLIOGRAFIE

Strategia de Securitate Cibernetică a României şi *Planul de acțiune la nivel național privind implementarea Sistemului Național de Securitate Cibernetică* (în M.O. nr. 296 din 23 mai 2013, H.G. nr. 271/2013).

Dunnigan F. James, *Noua amenințare mondială: cyber-terorismul*, Editura Curtea Veche, Bucureşti, 2010.

McLuhan Marshall, *Mass-media sau mediul invizibil*, Editura Nemira, Bucureşti, 1997.

Gordon A. Lawrence, *Cybersecurity risk management: an economics perspective*, http://www.rhsmith.umd.edu/faculty/lgordon

FFIEC Handbook Definition of Reputation Risk, http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-riskmanagement/reputation-risk.aspx

Governing for Enterprise Security, http://www.cert.org/governance/

Socializing Securely: Using Social Networking Services, http://www.us-cert.gov/reading_room/safe_social_networking.pdf

US-CERT's Protect Your Workplace Posters & Brochure, http://www.us-cert.gov/reading_room/distributable.html

What Businesses can do to help with cyber security, http://www.staysafeonline.org/sites/default/files/resource_documents/What%20Businesses%20Can%20Do%202011%20Final_0.pdf

http://news.bbc.co.uk/2/hi/technology/6653119.stm

http://www.securitatea-informatiilor.ro

http://www.sri.ro