CULTURA DE SECURITATE – PRIMA LINIE A APĂRĂRII CIBERNETICE

SECURITY CULTURE – THE FIRST LINE OF CYBER DEFENSE

COLONEL (R) PROF.UNIV.DR. GHEORGHE BOARU*
DRD. BENEDICTOS IORGA**

Rezumat: *Dezvoltarea şi accesibilitatea aproape universală a mediului Internet, explozia tehnologică accelerată şi accesul facil la înalta tehnologie au generat condiţiile prielnice pentru apariţia unui nou mediu de manifestare a vieţii sociale, sub toate aspectele ei, pe care toţi îl conştientizăm sub denumirea de spaţiu cibernetic. În mod implicit, criminalitatea informatică, ameninţările din mediul digital precum şi atacurile şi agresiunile cibernetice, ca părţi inevitabile ale vieţii sociale virtuale s-au manifestat în mod agresiv încă de la început şi au creat cel de-al V-lea spaţiu al confruntărilor sociale.*

Raportându-ne la dezvoltarea elementelor ce definesc spaţiul cibernetic ca spaţiu de luptă, putem observa că, în ceea ce priveşte cultura de securitate, aceasta a evoluat mult prea lent şi nu are o contribuţie semnificativă în acţiunile de prevenire a criminalităţii, agresiunilor şi provocărilor din mediul online. Justificările teoretice şi tehnice ale acestei evoluţii lente se bazează, în mare parte, pe ipoteza potrivit căreia spaţiul cibernetic este mediul dinamic şi fluid de manifestare a milioane de utilizatori noi, care iau contact în premieră cu tehnologiile digitale şi implicit, nivelul de conştientizare şi de pregătire al acestora se află la un nivel iniţial de „default" ce va fi în permanenţă exploatat. Cu toate acestea, eforturile de îmbogăţire a culturii de securitate în mediul cibernetic precum şi de accelerare a ritmului de progres cultural vor trebui să devină în curând parte componentă a politicilor de stat.

Cuvinte-cheie*: spaţiu cibernetic, atac cibernetic, apărare cibernetică, securitate informaţională, cultură de securitate, ţintă,reţea, sistem informatic.*

Abstract: *The development and universal accessibility of Internet environment, accelerated technological explosion and easy access to high technology have generated favorable conditions for the emergence of a new environment for social life expression under all its aspects, which we all acknowledge it as the cyber space. By default, cybercrime, threats and attacks in the digital environment and cyber aggressions treated as unavoidable parts of virtual life, have come forward aggressively from the beginning and have created the fifth space of social confrontation .*

* Universitatea Naţională de Apărare „Carol I", Bucureşti, telefon: 0744359483, email: boarugheorghe@yahoo.com.
** Doctorand Universitatea Naţională de Apărare „Carol I", Bucureşti, email: iorgaben@yahoo.com.

Relating to the development of the elements that define cyberspace as a new combat area, we can notice that security culture evolved too slow and does not have a significant contribution to prevention of crime actions, cyber frauds and challenges from online environment. Theoretical and technical justifications of this slow evolution is largely based on the assumption that cyberspace is a dynamic and fluid environment for manifestation of millions of new users. These new users get the first contact with digital technologies and their level of awareness and training it is at initial level of "default", fact that will be permanently exploited. However, the efforts to enrich the cyber security culture and to accelerate the rhythm of cultural progress should become soon a part of state policies for World Wide Web.

***Keywords**: cyber space, cyber attack, cyber defense, information security, security culture,target, network, computer system.*

Deşi poate fi considerată o utopie, realitatea actuală ne demonstrează că trăim în două medii paralele, fiecare mediu cu legile şi regulile lui, dar care coexistă şi se dezvoltă simultan – mediul social sau „viaţa reală” şi mediul digital sau „realitatea virtuală”. Respirăm – navigăm, vorbim – socializăm online, ne hrănim – simulăm, mergem la şcoală – suntem clienţi e-learning, compunem o scrisoare – transmitem un mail, facem investiţii – tranzacţionăm on-line, toate acestea sunt doar câteva elemente ce coexistă în cele două spaţii total diferite ca mod de manifestare, dar care sunt legate de componenta umană ca fiind acea componentă care le-a generat, le dezvoltă şi exploatează.

Realitatea virtuală, ca parte componentă a vieţii sociale, a apărut încă din anul 1982 odată cu definirea protocolului TCP - IP[1] şi cu apariţia noţiunii de INTERNET[2] şi s-a dezvoltat accelerat până la stadiul actual, când putem afirma că la o populaţie a globului de 7, 262 miliarde de locuitori, avem peste 2,9 miliarde de utilizatori ai reţelei globale INTERNET[3]. Desigur, ritmul accelerat de dezvoltare al mediului de reţea şi dependenţa funcţionării societăţii umane de tot ceea ce înseamnă informaţie şi mediul de reţea ca mijloc de procesare a datelor, va conduce într-o foarte scurtă perioadă de timp la egalizarea cifrelor de mai sus sau la inversarea raportului. Nu sunt puţine vocile care susţin că dependenţa de tot ceea ce înseamnă spaţiul cibernetic şi mediul online, în ansamblul său, nu reprezintă altceva decât o schimbare a regulilor vieţii umane şi un nou pas al evoluţiei societăţii, caracterizat, în principal, prin lipsa frontierelor, accesul la resurse informaţionale impresionante, dinamism permanent şi, nu în ultimul rând, anonimat.

---

[1] Modelul **TCP/IP** (**Protocol de control al transmisiei/Protocol Internet**, în engleză *Transmission Control Protocol/Internet Protocol*) a fost creat de US DoD (US Department of Defence - Ministerul Apărării al Statelor Unite) din necesitatea unei reţele care ar putea supravieţui în orice condiţii.

[2] Termenul **Internet** provine din împreunarea artificială şi parţială a două cuvinte englezeşti: interconnected = interconectat şi network = reţea.

[3] http://www.worldometers.info/ro/, accesat la 22.04.2015, ora 16.00.

Aceste caracteristici, deşi extrem de benefice, pot fi distructive şi ne pot trimite cu gândul la faptul că o societate sau o structură organizaţională de tip statal, indiferent de mărimea ei fizică şi caracteristicile existenţiale pe care le deţine ca entitate (teritoriu, mărime, frontiere, populaţie, resurse, dezvoltare economică etc.) este cu atât mai vulnerabilă cu cât gradul de informatizare deţinut este mai ridicat. Analizând istoria recentă a atacurilor şi ameninţărilor cibernetice, un exemplu relevant ce poate servi drept argument pentru susţinerea afirmaţiei anterioare, demn de teoria haosului, poate fi considerat incidentul din anul 2004 la nivelul aviaţiei civile americane, în care a fost implicată compania Delta Air Lines cu sediul în Texas. Incidentul a fost generat de o eroare de programare la nivelul tehnicii de calcul echipată cu sistemele de operare Windows XP sau Windows 2000 care a permis exploatarea unei vulnerabilităţi de sistem de tip "buffer overflow"[4] de către un student german[5] prin introducerea de la distanţă, în infrastructura informatică a companiei, a unei secvenţe de cod de tip worm, intrată în istorie sub denumirea de „Sasser worm". Incidentul, pe lângă panica şi paguba financiară creată la nivel mondial (peste 500 milioane de dolari), a pus în pericol siguranţa a milioane de pasageri şi a periclitat întreaga activitate a aviaţie civile americane, pazei de coastă britanice, sistemului de comunicaţii satelitar al agenţiei de presă France-Presse (AFP), a afectat compania de asigurări finlandeză IF şi sucursalele bancare SAMPO BANK, Universitatea din Missouri, precum şi secţia de radiologie a spitalului Lund University Hospital din Germania.

Incidentul prezentat nu îşi propune să expună în principal vulnerabilităţile din mediul online ci doreşte să exemplifice interdependenţele la nivel global existente în spaţiul cibernetic, fapt pentru care este denumit, în lumea virtuală, drept „zborul fluturelui", deoarece prin modul de desfăşurare, propagare şi evoluţie în spaţiul cibernetic, poate fi asociat cu modul în care „zborul unui fluture" (spre exemplu în Germania) poate produce o tornadă în Texas, iar efectele tornadei din Texas vor fi resimţite în Japonia. Din acest punct de vedere, spaţiul cibernetic poate fi definit ca acel mediu virtual global, generat de totalitatea infrastructurilor cibernetice existente care includ informaţiile procesate, stocate şi/sau transmise, acţiunile utilizatorilor virtuali, politicile şi procedurile de securitate aplicate la

[4] Un *buffer overflow* apare atunci când un program sau proces încearcă să stocheze mai multe date într-un tampon (zona de stocare temporară a datelor) decât a fost destinat să deţină.

[5] Sven Jaschan s-a născut în localitatea Waffensen, Germania şi a studiat informatica în cadrul liceului din localitatea Rotenburg. A fost arestat la data de 7 mai 2004 de către poliţia germană în urma unei anchete internaţionale, fiind acuzat de atacuri informatice ce au generat pagube de aproximativ 500 milioane de dolari.

nivelul întregului mediu de reţea. Conceptul de spaţiu cibernetic (cyberspace[6]) este un termen polisemantic, fiind în plin proces de fundamentare teoretică dar care poate fi explicat prin prisma interacţiunii om-tehnologie.

Noutatea conceptului şi inexistenţa unei hărţi complete şi descriptive a acestui spaţiu a generat polemici, abordări şi interpretări diferite şi aprinse care au tratat această noţiune ca putând fi o filozofie în dezvoltare, o realitate virtuală, un produs al interacţiunii sociale sau o altă dimensiune umană. Din această perspectivă, din punct de vedere tehnic, „spaţiul cibernetic poate fi abordat prin prisma a trei curente cunoscute”[7]: **spaţiul cibernetic gibsonian**[8] - utilizatorul, tehnologia si mediul de transmisie sunt considerate a fi o singura entitate, **realitatea virtuală** - un mediu multidimensional în care oamenii pot circula liberi şi pot să interacţioneze atât cu computerul cât si cu alte fiinţe umane şi **ciberspaţiul barlovian**[9] - văzut ca un mediu de transmisie electronic, digital, în care utilizatorul este situat într-o reţea comunicaţională de computere.

Indiferent de modul de definire şi de abordările teoretice şi tehnice prezentate, la nivelul spaţiului cibernetic şi implicit la nivelul fiecărui mediu de reţea component, putem identifica 5 caracteristici de bază, reprezentate de:

- *existenţa* unei platforme hardware *şi software* flexibile şi deschise, la baza oricărei infrastructuri cibernetice - orice mediu de reţea închis nu poate supravieţui în timp;

- *existenţa a 4 niveluri componente*: **infrastructura fizică** (baza de dezvoltare a spaţiului cibernetic, reprezentată de calculatoare interconectate, servere, senzori, medii de transmisie etc.**), nivelul logic**, (totalitatea protocoalelor logice ce permit iniţierea şi realizarea comunicaţiilor, aplicaţii şi servicii informatice în mediul de reţea), **nivelul informaţional** (totalitatea datelor, metadatelor şi informaţiilor procesate, stocate şi transmise de infrastructura fizică) şi **nivelul uman** (totalitatea utilizatorilor activi şi pasivi ce activează în mediul cibernetic);

- *dependenţa de acţiunea şi interacţiunea umană,* reliefată de faptul că omul este cel care, prin acţiunea sa, menţine în viaţă mediul de reţea şi de aceea, nu

---

[6] Conceptul provine din limba engleză - „cyberspace”, iar termenul se datorează lui William Gibson care l-a folosit în premieră în romanul SF „Neuromancer”, apărut în anul 1984, pentru a descrie o lume a calculatoarelor, în cadrul societăţii reale.

[7] Featherstone, Mike&Burrows, Roger, 1996, Cyberspace/Cyberbodies/Cyberpunk. Cultures of Technological Embodiment, Sage, London: 5-7.

[8] William GIBSON „Ciberspaţiul: o halucinaţie consensuala, trăită zilnic de miliarde de operatori legitimi, în fiecare naţiune, de copii care sunt învăţaţi concepte matematice … O reprezentare grafica a datelor extrase din băncile fiecărui computer ale societarii omeneşti. Complexitate de neconceput..”.

[9] Concepţia lui John Barlow, fondatorul grupului de acţiune Electronic Frontier Foundation, Revista *Informatica Economica*, nr. 3(27)/2003.

calculatorul este cel care defineşte azi noţiunea de spaţiu cibernetic, ci interacţiunea utilizator – sisteme de calcul.

- *există şi evoluează pe baza modelelor comportamentale umane şi a cerinţelor societăţii,* transpuse virtual din viaţa reală. Această afirmaţie poate fi exemplificată prin modul în care caracteristica unui segment de reţea, spre exemplu din reţeaua INTERNET dintr-o anumită regiune, va fi generată de caracteristicile socio-comportamentale şi cerinţele specifice utilizatorilor din acea regiune. Concret, dacă într-o anumită zonă mediul infracţional este ridicat, atacurile şi agresiunile realizate în mediul online pe acel segment de reţea din acea regiune vor fi mai ridicate şi vor purta amprenta sau modul de operare specific acelor utilizatori.

- *existenţa unui grad ridicat de insecuritate*, generat de anonimatul utilizatorilor şi de lipsa frontierelor de manifestare şi dezvoltare a elementelor componente.

Fiecare din caracteristicele menţionate anterior sunt definitorii pentru tot ceea ce reprezintă spaţiul cibernetic în ansamblu său ori chiar un mediu de reţea local. Indiferent că vorbim de infrastructura fizică, infrastructura logică sau platformele şi tehnologiile software şi hardware utilizate ca temelie a dezvoltării acestui spaţiu, caracteristica de securitate rămâne poate cea mai stringentă problematică a societăţii informaţionale în care trăim şi, totodată, cea mai semnificativă caracteristică ce poate genera involuţie în spaţiul virtual.

Plecând de la dihotomia **spaţiul cibernetic - realitate virtuală**, problematica securităţii în mediul online nu poate fi mai redusă decât cea din mediul social. Cumulativ, totalitatea riscurilor, ameninţărilor şi vulnerabilităţilor din viaţa de zi cu zi atât la nivelul siguranţei indivizilor cât şi la nivelul siguranţei comunităţii cunosc un factor de amplificare exponenţial, generat în principal de caracteristicile spaţiului cibernetic enumerate anterior. Anonimatul, accesul la tehnologie, lipsa barierelor de dezvoltare, inteligenţa artificială, volumul imens de resursă informaţională, capacităţile rapide de procesare a datelor, ingeniozitatea utilizatorilor şi nu în ultimul rând costurile relativ reduse de transpunere în mediul virtual a voinţei acestora, fac ca noţiunea de securitate în spaţiul cibernetic să devină de multe ori hilară. Întrebat, în cadrul unui interviu, despre securitatea în mediul cibernetic, generalul american KEITH B. Alexander, comandatul „US Cyber Command/NSA" susţinea faptul că „securitatea în mediul cibernetic dinamic eşuează deoarece adversarii schimbă regulile jocului prin simpla exploatare a unor facilităţi şi vulnerabilităţi noi"[10]. De asemenea, Richard Thieme, consultant

[10] The next wave, vol.19, nr.4, 2012, p.1 - Building a national program for cyber security science / NSA - Central security agency.

guvernamental american pe probleme de tehnologie, în cadrul conferinţei internaţionale de securitate - BLACK HAT din LAS Vegas (2011), a evidenţiat faptul că „securitatea în mediul cibernetic este un mit sau, în cel mai bun caz, o glumă", iar acest lucru este o axiomă prin însuşi modul de construcţie a mediului cibernetic, ca sumă de realităţi virtuale care nu pot fi niciodată sigure sau, de cele mai multe ori fără corespondent în realitate.

Starea de insecuritate din mediul online este rezultanta riscurilor, ameninţărilor şi vulnerabilităţilor din mediu de reţea generată de indivizi, grupuri de interese, organizaţii statale şi non-statale capabile să desfăşoare atacuri şi agresiuni cibernetice care să depăşească rezilienţa infrastructurilor cibernetice. Din acest punct de vedere securitatea cibernetică poate fi definită ca acea stare de normalitate din mediu de reţea, obţinută ca efect al aplicării unor măsuri tehnice de protecţie şi a unor politici de securitate proactive, prin care se asigură permanent confidenţialitatea, disponibilitatea, integritatea şi autenticitatea datelor şi informaţiilor din mediu precum şi accesul continuu şi sigur la resursele şi serviciile reţelei. La baza securităţii cibernetice se află, asemenea securităţii sociale sau militare, apărarea cibernetică, definită ca totalitatea acţiunilor executate pentru protejarea mediului cibernetic prin detectarea, stoparea şi contracararea oricărei agresiuni cibernetice. Securitatea în mediul online nu este o problemă nouă, ceea ce este nou însă, sunt efectele pe care le generează mediul de insecuritate din spaţiul cibernetic actual.

Dacă în urmă cu aproximativ 30 de ani un virus sau o secvenţă distructivă de cod putea afecta un computer şi poate cel mult un segment de reţea, la momentul actual efectele pot fi devastatoare atât prin amplitudine cât şi prin implicaţiile economice şi sociale. Istoria spionajului cibernetic recentă a evidenţiat faptul că atacurile cibernetice deja celebre precum „Stuxnet", „Flame", „Gauss", „Operaţiunea Tallinn", „Octombrie roşu", „epic-turla" au avut efectul unor arme de distrugere în masă asupra infrastructurilor informatice, fiind definită astfel o nouă categorie de armament denumită armament cibernetic. În mediul civil, lucrurile nu par nici pe departe mai simple, iar interdependenţa dintre societate şi mediul informaţional face ca atacurile asupra unei infrastructuri informatice civile a unui stat să genereze panică şi haos la nivelul întregii societăţii. Un exemplu relevant în acest sens este reprezentat de operaţiunea denumită „Dragonfly" sau „ Energetic Bar RAT", prin care, încă din anul 2009 parte din infrastructura energetică a SUA a fost controlată de la distanţă prin aplicaţii de tip malware implementate în sistemele de management şi distribuţie ale reţelei electrice naţionale. Printre ţintele grupului Dragonfly s-au numărat operatori ai reţelelor de distribuţie energetică, mari firme generatoare de electricitate, operatori ai conductelor de petrol, precum şi furnizori de echipamente industriale din domeniul energetic. Majoritatea companiilor care au

fost vizate sunt localizate în Statele Unite, Spania, Franţa, Italia, Germania, Turcia şi Polonia, iar efectele şi potenţialul distructiv al acestor tipuri de atacuri cibernetice asupra unei infrastructuri civile ne fac să conştientizăm pericolele societăţii informaţionale în care trăim.

Pornind de la aceste exemple, limitate ca număr, şi făcând apel la răsunătoarele operaţiuni de spionaj în mediul de reţea şi de infracţiuni informatice zilnice din mediul Internet, putem constata că, la o simplă accesare a unui motor de căutare online prin introducerea termenului de „atac cibernetic", paginile indexate vor fi de ordinul sutelor de mii, toate exemplificând sau documentând diverse acţiuni şi operaţiuni în mediul virtual. Toate acestea ne fac să afirmăm că securitatea cibernetică a devenit treptat, dar sigur, o a doua mare preocupare a structurilor de securitate şi a organismelor naţionale şi internaţionale, după terorism. Realitatea de azi confirmă că, în fiecare zi, învăţăm despre un alt atac cibernetic, efectuat undeva în lume asupra instalaţiilor militare, website-urilor oficiale, reţelelor electrice, băncilor şi instituţiilor financiare, cardurilor de credit devenite astfel ţinte ale agresiunilor cibernetice susţinute. Autorii de azi ai atacurilor sunt diferiţi de cei de ieri, ne mai fiind un grup renegat sau un hacker singular orientat spre profit, ci, mai degrabă, guverne şi grupuri de crimă organizată, terorism şi carteluri infracţionale. Valenţele securităţii cibernetice au căpătat în ultimii ani o importanţă strategică la nivelul statelor lumii, în contextul în care conflictele militare au depăşit cu mult folosirea arsenalului clasic, desfăşurându-se în mare parte în zona cibernetică, cu un potenţial impact devastator într-un timp foarte scurt. Practic, prin mediul de reţea poate fi dus un război permanent fără ca acest lucru să fie declarat în conformitate cu legile luptei armate. Cele mai cunoscute ameninţări de natură cibernetică precum reţele de calculatoare infectate, software-ul nociv, hacktivismul, ca formă de protest online, şi ameninţările avansate persistente, pentru a fi eliminate sau limitate, au nevoie de sisteme de protecţie bazate pe înalta tehnologie traduse în principal prin bugete şi resurse financiare consistente.

Toate aceste elemente nasc în mintea fiecăruia dintre noi fireasca întrebare „care este soluţia de securitate în mediul cibernetic?". Adresând întrebarea experţilor din diverse domenii, cu preponderenţă tehnice, se poate constata că răspunsurile sunt diferite şi generate în principal de experienţa individuală a fiecăruia. Un inginer hardware din domeniul IT a răspuns că cea mai bună soluţie de securizare a unui mediu de reţea sau subspaţiu cibernetic este reprezentată de ultima soluţie de firewall ce implementează tehnologia Advanced Firewall Protection cunoscută sub denumirea de Next Generation Firewalls (NGFW). Din punct de vedere tehnic, răspunsul poate fi cu greu contestat, ţinând cont de faptul că soluţia aleasă este vârful de gamă în ceea ce priveşte soluţiile de securizare

hardware dedicate ce asigură funcţionalităţi de tip QoS (quality of service), sisteme de prevenire a intruziunilor şi tehnologii de filtrare malware, pentru care au fost investite, numai în cercetare, aproximativ 100 milioane de dolari.

Un specialist în domeniul comunicaţiilor va recomanda în permanenţă utilizarea unor sisteme de legătură pentru asigurarea schimbului de date, ce folosesc soluţii hardware tip concentratoare de flux în tehnologie VPN cu facilităţi IP Security (IPsec), Secure Sockets Layer (SSL) şi criptare în tunel folosind tehnologia de criptare software în standard AES 512 biţi sau hardware.

Un developer de produse software va recomanda cu precădere actualizarea tuturor add-on-urilor şi update-urilor de securitate la nivelul sistemelor de operare şi al aplicaţiilor utilizate, precum şi instalarea şi actualizarea permanentă a unei soluţii antivirus cu facilităţi extinse, de tipul software „firewall protection" şi „advanced malware detection".

Nu în ultimul rând, un administrator de securitate la nivelul unei reţele, probabil, va solicita impetuos bugetarea şi, ulterior, aplicarea tuturor soluţiilor recomandate anterior. Suplimentar, va implementa o politică de securitate adecvată mediului de reţea deservit şi organizaţiei din care face parte, care să reducă vulnerabilităţile din sistemele de operare, să limiteze accesul la porturile inutile, să controleze auditul de securitate la nivelul reţelei şi, nu în ultimul rând, să asigure doar acele resurse necesare funcţionării sistemului în ansamblul său.

Toate aceste soluţii ipotetice şi răspunsuri sunt adevărate şi pot, cu siguranţă, creşte semnificativ nivelul de securitate al unei reţele în mediul cibernetic global. În plus, vor asigura, cu certitudine, un grad ridicat de disponibilitate al serviciilor şi aplicaţiilor coroborat cu păstrarea confidenţialităţii datelor procesate în mediul de reţea, chiar dacă costurile unei astfel de soluţii sunt considerabile. De exemplu, costul anual la nivelul economiei globale pentru contracararea efectelor criminalităţii informatice este estimat la „peste 400 de bilioane de dolari". Cea mai optimistă estimare „a fost de peste 375 de bilioane de dolari"[11], dar, şi aşa această sumă reprezintă mult mai mult decât produsul intern brut al multor ţări sau mult peste venitul cumulat al multor companii multinaţionale. Suplimentar, costurile în acest caz sunt cumulate cu efectele induse de compromiterea a milioane de zetabiţi de informaţii confidenţiale ce aparţin utilizatorilor atacaţi din mediul online, aproximativ 40 de milioane de persoane din SUA, 14 milioane în Turcia, 20 de milioane în Coreea, 16 milioane în Germania, şi mai mult de 30 de milioane în China, pe baza raportului din anul 2013 al Centrului pentru Studii Strategice Internaţionale. Desigur, în accepţiunea aceluiaşi administrator de securitate, atunci

[11] http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf, accesat la 22.03.2015, ora 20.00.

când vorbim despre asigurarea securităţii unui mediu de reţea în spaţiul cibernetic, cu atât mai mult cu nivelul de confidenţialitate al informaţiei protejate este unul ridicat, factorul sau resursa financiară trebuie să conteze cel mai puţin, iar elementul care primează să fie însăşi siguranţa datelor.

Deşi aşa cum am menţionat, soluţiile tehnice propuse sunt fundamentate şi susţinute de argumente solide, la baza implementării şi a utilizării lor se regăseşte omul sau mai bine spus utilizatorul virtual. Din această perspectivă, utilizatorul reprezintă veriga cea mai slabă a întregului angrenaj al securităţii în spaţiul cibernetic, fapt ce face ca succesul atacurilor şi agresiunilor cibernetice să se bazeze şi să exploateze, în principal, această verigă. Utilizatorul, aşa cum am afirmat în partea anterioară, este un angrenaj în cadrul celui de al IV-lea nivel definit, ce deţine o experienţă personală limitată în ceea ce priveşte comportamentul virtual, urmare a pregătirii personale a acestuia şi în mod special a culturii de securitate deţinute.

Cultura de securitate poate fi definită ca prima linie a apărării cibernetice şi reprezintă suma valorilor, normelor, atitudinilor sau acţiunilor întreprinse în mediul virtual, care determină înţelegerea şi asimilarea conceptului de securitate cibernetică şi a celorlalte concepte derivate: securitatea informatică, securitate fizică, securitatea documentelor, securitatea personalului, securitatea comunicaţiilor, politică de securitate, insecuritate etc.

Din punct de vedere fizic, cultura de securitate nu este ceva palpabil ce poate fi achiziţionat sau implementat asemenea unei componente hardware, ci este rezultanta unui cumul de factori ce îmbină experienţa individuală a fiecărui utilizator cu cunoştinţele tehnice şi teoretice deţinute, cu valorile organizaţiei din care face parte şi nu în ultimul rând cu procedurile de securitate aplicate la nivelul acelei organizaţii. Toate aceste elemente definesc cultura de securitate la nivelul fiecărui individ, iar cultura de securitate la nivelul organizaţiei este imaginea însumată a nivelului de cultură de securitate a membrilor acelei organizaţii.

Cea mai bună soluţie de securitate hardware implementată la nivelul unui nod de reţea sau chiar la nivelul întregului mediu cibernetic, este penetrabilă, în faţa atacurilor combinate bazate, de exemplu, pe tehnici de inginerie socială sau pe exploatarea necunoaşterii de către personal a procedurilor interne de securitate, aplicabile la nivelul unei organizaţii. În conformitate cu ultimele raportări referitoare la atacurile cibernetice asupra utilizatorilor serviciilor de email publice, peste 60% din atacurile încheiate cu compromiterea corespondenţei şi a căsuţelor de email aparţinând utilizatorilor s-au datorat slabei pregătiri a acestora în ceea ce priveşte cultura de securitate minimală ce trebuie deţinută pentru folosirea corespondenţei electronice. Plecând de la o greşeală comună, spre exemplu, generarea unei parole de acces la un sistem ce conţine combinaţii simpliste şi uzuale de caractere (p@ssw0rd, nume de persoană, ani de naştere) şi ajungând la

încălcarea unor norme de securitate prin forţarea unor politici interne de securitate definite în cadrul unei organizaţii (utilizarea unor medii de stocare neautorizate, accesul folosind credenţialele unui alt utilizator), toate aceste elemente au în comun cultura de securitate precară la nivelul utilizatorilor.

Gândind din perspectiva unui atacator, va fi tot timpul mai simplu să obţii o informaţie confidenţială atacând un utilizator acolo unde el este mai vulnerabil, folosind limitările generate de lipsa pregătirii, neglijenţă în manipularea informaţiilor şi a mijloacelor tehnice, preocuparea pentru îndeplinirea unei sarcini rapid prin realizarea de compromisuri în detrimentul menţinerii securităţii, decât să îţi propui atacarea unui server de email sau a unui controler de domeniu ce gestionează o reţea închisă, deoarece aceasta presupune pe lângă consumul de resurse tehnice, timp şi un grad de risc ce nu poate fi estimat. Penetrarea unei reţele în scopul obţinerii unor informaţii confidenţiale se realizează în urma unor acţiuni combinate ce presupun suprapunerea mai multor metode şi tehnici de atac[12], plecând de la documentarea infrastructurii de reţea, a soluţiilor de firewall, a traficului de date, a metodelor de securizare aplicate la nivelul reţelei.

Toate acestea pot fi sortite eşecului în situaţia în care, în spatele acelei infrastructuri cibernetice, managementul este realizat de personal de securitate care deţine cunoştinţele necesare şi echipamentele tehnice apte să asigure detecţia intruziunii şi protecţia specifică respingerii atacului. În detrimentul tuturor eforturilor de securizare a unei reţele, spre exemplu în cadrul unei organizaţii, experienţa şi realitatea ultimilor ani au dovedit că vulnerabilităţile cele mari nu se regăsesc în mediul de securitate local specific acelei reţele sau la nivelul configurărilor şi infrastructurii de reţea, ci în mediul de securitate global, acolo unde utilizatorii îşi desfăşoară activitatea în mod liber nefiind constrânşi de regulile specifice de protecţie proxime de securitate aplicate la nivelul acelei organizaţii.

Spre exemplu, la nivelul marilor corporaţii, dar şi la nivelul organizaţiilor guvernamentale închise, se consideră de multe ori că un utilizator, tradus în fapt printr-o persoană ce deţine calitatea de angajat, este liber să se manifeste în mediul social aşa cum doreşte, fără să fie constrâns de aplicarea unor reguli de autoprotecţie şi securitate la nivel personal, atunci când nu se regăseşte în perimetrul organizaţiei. Acest aspect poate fi dovedit ca fiind greşit şi este de multe ori o vulnerabilitate intens exploatată de atacatori, deoarece este mult mai simplu să accesezi şi să penetrezi un sistem de calcul sau o reţea personală wirreles a unui utilizator, în mediul său familiar, decât să îţi propui să obţii aceleaşi rezultate

[12] Pentru exploatare - ameninţările avansate persistente, pentru spionaj economic şi politic - operaţiunea GhostNet, tehnici de infestare malware, pentru furtul de identitate - tehnici de spam, phishing şi pharming, pentru sabotaj - atacurile de tip Distributed Denial of Service sau spamurile generate prin bootneturi (reţeaua Conficker şi reţeaua Mariposa), pentru distrugere -Stuxnet.

atacându-i echipamentele informatice pe care operează în interiorul organizaţiei. De la atacarea calculatorului personal sau a smartphone-ului unui utilizator, până la aflarea datelor confidenţiale pe care acesta le deţine în interiorul organizaţiei nu este de multe ori decât un pas cu direcţie sigură spre succes, ce ţine în principal de ingeniozitatea şi experienţa atacatorului coroborate cu cultura de securitate şi tertipurile utilizatorilor (folosirea aceloraşi credenţiale de securitate, deţinerea de informaţii pe calculatoarele personale care pot ajuta la documentarea activităţii desfăşurate în organizaţie etc.).

În ceea ce priveşte tehnicile de exploatare a utilizatorului, cele mai recente atacuri (spre exemplu atacul „epic-turla" sau „turla-carbon") au folosit metode de inginerie socială combinate cu soluţiile tehnice de atac de tip malware (70% din penetrări se bazează pe soluţii de infestare de acest tip), profitând de naivitatea utilizatorilor şi de slaba cunoaştere a regulilor minimale de securitate, în special aplicabile la nivelul reţelelor guvernamentale închise, unde teoretic, nivelul de control şi de aplicare a managementului de securitate este mai ridicat. Tehnicile de inginerie socială, coroborate cu posibilităţile oferite de reţelele de socializare prin exploatarea şi documentarea aproape în timp real a comportamentului unui utilizator în mediul virtual sunt o adevărată armă cibernetică, la care soluţiile de securitate hardware şi software nu pot să reziste, ci pot cel mult să încetinească sau să limiteze efectele unor atacuri. Atunci când un atacator îşi propune exploatarea unui mediu de reţea chiar şi închis, aparţinând unei organizaţii, inclusiv prin exploatarea vulnerabilităţilor de tip „zero-days", este foarte utilă cunoaşterea comportamentului online al utilizatorilor şi al personalului administrativ de securitate, din mediul public. Informaţiile obţinute prin documentarea online, folosind reţelele de socializare şi ingineria socială, pot duce la stabilirea modului de reacţie, a modului de gândire şi a atitudinilor comportamentale şi abilităţilor tehnice ale utilizatorilor şi personalului administrativ. Practic, un atacator află ce ştie, ce poate, cât poate, cum poate şi cum reacţionează acel utilizator sau administrator de securitate, facilitându-şi astfel acţiunile tehnice ulterioare sau comercializând bazele de date comportamentale către alte grupuri de atacatori sau structuri organizaţionale interesate.

Singura linie de apărare care poate limita sau elimina aceste riscuri şi vulnerabilităţi nu este, din păcate, o soluţie tehnică, ci este reprezentată de cultura de securitate a fiecărei entităţi ce intră în contact cu mediul cibernetic.

Atingerea stării de securitate la nivelul unei reţele presupune în primul rând un demers intelectual creativ, fiind importante educaţia, cercetarea şi cultura de securitate a fiecărui utilizator în parte. O structură nu poate fi competitivă şi nu îşi poate utiliza resursele, tehnologia şi potenţialul de care dispune, fiind doar un consumator de securitate. Pentru aceasta, fiecare organizaţie (în mediul Internet

acest aspect este poate cel mai vizibil) trebuie să fie un generator de securitate în zona sa de acţiune, deoarece mediul cibernetic este dependent de fiecare mediu de reţea care îl alcătuieşte.

Apare, astfel, problematica a ceea ce este de făcut pentru îmbunătăţirea culturii de securitate la nivelul personalului organizaţiilor, în scopul creşterii protecţiei în mediul cibernetic. Această problemă nu este una simplă ce poate fi realizată instantaneu, ci presupune un cumul de acţiuni desfăşurate permanent şi poate chiar integrate intr-o politică de stat legislativă şi aplicativă.

Un prim pas ar putea fi reprezentat de asigurarea unui cadru legal, prin aprobarea şi implementarea unei legi a securităţii cibernetice care să reglementeze cadrul normativ, precum şi responsabilităţile deţinătorilor de infrastructuri cibernetice. La momentul actual, majoritatea atacurilor din mediul Internet la nivelul utilizatorului sunt pasate în responsabilitatea acestuia, ca fiind răspunzător de propria securitate a sistemului de calcul terminal, fără ca furnizorul de servicii de Internet să fie obligat la asigurarea calităţii serviciului, inclusiv la nivelul securităţii infrastructurii terminale.

În acest fel, un atac asupra unui sistem de calcul se propagă rapid în mediul de reţea, iar furnizorul de servicii nu are în responsabilitate decât asigurarea efectivă a liniei de comunicaţie, a activelor şi pasivelor de reţea şi a menţinerii nivelului de trafic. În ceea ce priveşte pregătirea de securitate privind accesul la serviciile din Internet, aceasta nu se realizează, fiind responsabilitatea exclusivă a utilizatorului. În cazul contractării unui serviciu electronic din mediul Internet (iar uneori şi în cazul reţelelor guvernamentale), pregătirea de securitate pentru utilizarea acelui serviciu presupune acceptarea tacită, printr-o bifă, a unui memorandum (agreement, terms of use, EULA) care descrie în termeni generali politica acceptată de utilizare a serviciului şi exonerează generatorul de servicii de responsabilitatea apariţiei incidentelor de securitate din mediul online.

Un al doilea pas este reprezentat de apariţia formelor organizate de educaţie cibernetică la nivelul instituţiilor de învăţământ, argumentul solid fiind reprezentat de faptul că noţiunea şi domeniul „cyber” are aproape 35 de ani de apariţie, iar dependenţa vieţii sociale de acest domeniu este covârşitoare, înlocuind domenii precum „artele” şi „sportul” în ceea ce priveşte impactul asupra vieţii sociale. Educaţia cibernetică poate fi primul pilon al culturii de securitate, care va permite subdomeniului securitate cibernetică să se adapteze pentru a răspunde noilor provocări din mediul de reţea, aceasta cu atât mai mult cu cât securitatea în mediul online a devenit o adevărată industrie generatoare de profit. Strâns legat de educaţia cibernetică se află cercetarea în domeniul „cyber” care poate fi cel de al II-lea pilon al culturii de securitate, în scopul înţelegerii ameninţărilor actuale, studierii implicaţiilor şi efectelor acestora, precum şi a documentării şi elaborării a

unor noi soluţii de securitate hardware şi software şi a unor noi proceduri de securitate la nivel instituţional şi guvernamental.

Un al treilea pas poate fi reprezentat de dezvoltarea unui parteneriat guvernamental inter- instituţional sau între instituţii guvernamentale şi societatea civilă, care să genereze proiecte comune de îmbunătăţire a culturii de securitate cibernetică la nivelul utilizatorilor şi consumatorilor, având în vedere că personalul are atât calitatea de utilizator al reţelelor private, guvernamentale, cât şi utilizatori ai mediului Internet.

Obiectivele comune în cadrul proiectelor pot fi reprezentate de acţiuni de promovare a culturii de securitate prin mass-media, organizarea de cursuri, simpozioane, training-uri şi seminarii, work-shopuri şi conferinţe în instituţiile de învăţământ publice care să abordeze problematica culturii de securitate din mediul cibernetic, stabilirea de contacte şi colaborarea permanentă cu instituţiile ştiinţifice internaţionale, cu experţii în domeniu, sprijinirea prin finanţare a persoanelor fizice sau juridice care doresc să se iniţieze şi să se perfecţioneze în domeniul culturii de securitate cibernetică, atragerea autorităţilor publice locale în acţiunile de editare, publicare şi difuzare a materialelor informatice, materialelor tipărite şi audio-vizuale specifice, precum şi elaborarea de platforme online bazate pe tehnologia e-learning care să abordeze problematica pregătirii de securitate şi care să certifice un nivel minim acceptat de instruire pentru utilizatorii mediului online, ai reţelelor private şi guvernamentale.

Ultimul pas îl reprezintă schimbarea mentalităţii actuale privind cultura de securitate cibernetică, în special la nivelul organizaţiilor guvernamentale, autorităţilor publice locale şi al instituţiilor din sistemul naţional de apărare şi ordine publică. Aceasta se poate realiza prin adoptarea şi implementarea unor strategii pro-active bazate pe conştientizare, prevenire, protecţie şi reacţie, în mediile de reţea deţinute şi părăsirea concepţiei actuale privind dezvoltarea culturii de securitate prin mijloace statice reprezentate în principal de parcurgerea de către fiecare utilizator a unui documentar (ce prezintă riscurile, drepturi şi obligaţii în mediul de reţea) care se încheie prin asumare responsabilităţii utilizatorului asupra propriilor acţiuni în mediul cibernetic.

Deşi practica actuală poate fi acoperitoare din punct de vedere legal la nivel instituţional şi guvernamental, ea nu te protejează şi nu limitează efectele unui atac cibernetic asupra infrastructurilor critice, aşa cum se poate realiza în situaţia în care nivelul de cultură de securitate al utilizatorilor este ridicat şi adaptat palierului la care aceştia activează în organizaţii. De multe ori, a şti ce trebuie făcut, când trebuie făcut, cum trebuie făcut şi a pune în practică acţiuni specifice de protecţie în mediul de reţea cât mai rapid, poate duce la salvarea întregii organizaţii sau a întregii infrastructuri critice a statului.

Indiferent de capacitatea de analiză sau de previziune asupra evoluţiei mediului cibernetic, cultura de securitate trebuie să evolueze concomitent, sau pe cât posibil, anticipativ, pe baza experienţelor sociale umane şi să fie în concordanţă cu cerinţele de protecţie a infrastructurilor critice şi a informaţiilor procesate în mediile de reţea. Realizarea protecţiei cibernetice la nivelul unei întregi infrastructuri prin mijloace coercitive individuale sau restrictive la nivelul tuturor mediilor de reţea nu poate fi o soluţie a progresului societăţii bazată pe cunoaştere, cu toate că diverse forme de organizare statală aplică aceste metode. Conceptele precum „open-security", „open-society" sau organizaţii virtuale (Anonymus) sunt din ce în ce mai vehiculate şi atrag numeroşi susţinători care se manifestă activ în mediul online chiar prin agresiuni cibernetice împotriva organismelor de securitate. Din acest punct de vedere, tendinţa de îmbunătăţire a culturii de securitate cibernetică trebuie să devină firească în societate, să pornească de la utilizatorul obişnuit, ca urmare a progresului tehnico-ştiinţific şi a apariţiei unor noi valori sociale şi nu trebuie să se transforme într-un mijloc rigid de stopare a evoluţiei şi extinderii spaţiului cibernetic.

Un vechi proverb biblic ne sfătuieşte: „Cel prevăzător ia aminte la paşii lui"[13], iar acest sfat înţelept poate fi aplicat cu succes activităţii din spaţiul cibernetic indiferent că suntem în mediul Internet sau gestionăm o infrastructură de reţea critică pentru securitatea statului.

Această lucrare a fost posibilă prin sprijinul financiar oferit prin Programul Operaţional Sectorial Dezvoltarea Resurselor Umane 2007-2013, cofinanţat prin Fondul Social European, în cadrul proiectului ***POSDRU/159/1.5/S/138822****, cu titlul* ***„Reţea Transnaţională de Management Integrat al Cercetării Doctorale şi Postdoctorale Inteligente în Domeniile „Ştiinţe Militare", „Securitate şi Informaţii" şi „Ordine Publică şi Siguranţă Naţională" - Program de Formare Continuă a Cercetătorilor de Elită –„SmartSPODAS".***

BIBLIOGRAFIE

*** *Legea privind securitatea cibernetică a României*, 2014.
*** *Strategia de securitate cibernetică a României,* 2013.
*** *The next wave*, *Building a national program for cyber security science* , Central security agency, vol.19, nr.4, 2012.

[13] Biblia, Geneza / Proverbele 14:15, p.47.

***, *Twenty Critical Controls for Effective Cyber Defense:Consensus Audit Guidelines*, 2009.

FEATHERSTONE, Mike&Burrows, Roger, *Cyberspace, Cyberbodies, Cyberpunk. Cultures of Technological Embodiment*, Editura Sage, Londra, 1996.

RODOSEK Gabi Dreo, *Challenges of cyber defence in future internet*, Universitatea din Munchen, 2011.

http://www.mcafee.com.

http://www.worldometers.info/ro/.

http://www.securelist.com/en/analysis/204792238/Gauss_Abnormal_Distribution.

http://rt.com/news/iran-us-israel-cyberwar-virus-weapon-770/.

http://news.yahoo.com/report-secret-u-cyberwar-against-iranian-nukes-began-065204641.html