ATACURILE CIBERNETICE ÎN TOPUL AMENINŢĂRILOR ŞI VULNERABILITĂŢILOR LA ADRESA STATELOR, ORGANIZAŢIILOR ŞI CETĂŢENILOR, ÎN PREZENT ŞI ÎN VIITOR

CYBER ATTACKS TOP THREATS AND VULNERABILITIES AGAINST STATES, ORGANIZATIONS AND CITIZENS, AT PRESENT AND IN THE FUTURE

Gl. mr. (r) prof. asoc. dr. Constantin MINCU*

Rezumat*: Autorul încearcă, pe scurt, să readucă în atenţia celor interesaţi problema complexă, cu dezvoltare la nivel global, privind riscurile, ameninţările şi vulnerabilităţile cibernetice, mergând până la nivelul de „război cibernetic" cu implicarea directă a unor actori statali.*

Sunt prezentate unele mijloace şi vectori de atac, precum şi măsurile ce se impun pentru a proteja utilizatorii individuali, companiile, structurile guvernamentale şi militare.

În final, este adusă în atenţie situaţia din România, privind unele măsuri deja luate şi altele care, probabil, se vor lua în viitor, mai ales în plan legislativ şi administrativ, în problematica protecţiei cibernetice.

Cuvinte cheie*: atacuri cibernetice, război cibernetic, scurt istoric, vulnerabilităţi şi ameninţări cibernetice, NATO, UE.*

Abstract*: The author briefly tries to draw the attention of those interested in this topic on the complex issue developed globally with respect to cyber risks, threats and vulnerabilities, reaching up to the level of „cyber warfare" with the direct involvement of some state actors.*

Some means and vectors of attack are presented, as well as the countermeasures to be taken in order to protect the individual users, companies, governmental and military structures.

In the end, the author outlines the situation in Romania regarding some measures already taken and others that will be probably taken in the future, particularly in the legislative and administrative sectors aiming at ensuring cyber protection.

* Membru titular al Academiei Oamenilor de Ştiinţă din România, membru al Consiliului Onorific al Academiei Oamenilor de Ştiinţă din România, secretar ştiinţific al Secţiei de Ştiinţe Militare, Telefon 0722.303.015, E-mail: mincu-constantin@yahoo.com.

Key words: *cyber attacks, cyber warfare, brief history, cyber vulnerabilities and threats, NATO, EU*

Numeroşi autori români şi străini au abordat şi abordează, îndeosebi după anul 2005, problematica complexă a atacurilor cibernetice efectuate de actori individuali şi, mai nou, de actori statali interesaţi, din raţiuni diferite, să dezorganizeze sistemele informaţionale ale adversarilor, să fure informaţii sensibile, să obţină beneficii materiale importante, să afecteze grav funcţionarea unor sisteme publice vitale cum sunt: sistemele medicale, sistemele financiar-bancare, comunicaţiile civile şi militare, sistemele militare de comandă şi control, precum şi cele de arme complexe, utilităţile (energie electrică, gazele naturale, reţelele de apă, reţelele de transport) precum şi vectorii mass-media şi instituţiile culturale.

Mai nou, un nou tip de război îşi face simţită prezenţa din ce în ce mai mult în ultimul timp, unul purtat în faţa calculatorului, iar câmpul de luptă este internetul. Studierea, cu atenţie sporită, a tuturor aspectelor războiului informaţional şi cibernetic, precum şi a efectelor sale asupra civilizaţiei umane cade în sarcina tuturor serviciilor şi instituţiilor specializate, dar şi în sarcina fiecărui utilizator de bună credinţă, conectat la internet.

În acest articol nu putem epuiza această temă complexă, dar vom încerca să punctăm câteva aspecte, care, să arate importanţa dezvoltării unor sisteme solide de protecţie prin acţiuni ale factorului politic (legislaţie adecvată), instituţiilor statului cu atribuţii în domeniu, corporaţiilor şi societăţilor comerciale şi nu în ultimul rând a fiecărui cetăţean conectat la internet şi reţelele sociale.

Scurt istoric al comunicaţiilor electrice şi electronice, precum şi a sistemelor informatice

Deşi foarte mulţi oameni cunosc, fie şi secvenţial, dezvoltarea sistemelor de comunicaţii şi informatice, puţini se mai apleacă asupra unor momente cruciale în dezvoltarea, cu rapiditate, a comunicării la distanţă. Contează acum doar efectul reţelelor de azi şi de mâine care să ne facă interconectabili, în timp real, la nivel global.

Să revedem, totuşi, câteva repere şi realizări istorice, care au făcut posibile progresele de astăzi:

- 1837 – apare telegraful electric pe fir;
- 1854 – se inventează telefonul;
- 1865 – începe construirea de cabluri terestre şi subacvatice;
- 1930 – apare telexul (se renunţă la el abia în 1990);
- 1872 – importante cercetări ale telegrafiei fără fir (Loomis - SUA);
- 1888 – savantul Hertz – descoperă existenţa undelor electromagnetice;

- 1894 – se fac primele experimente ale transmiterii unor mesaje prin radio;
- 1901 – românul Dragomir Hurmuzescu face cercetări, cu rezultate importante, ale transmisiunilor radio;
- 1902 – prima transmisiune radio a vocii umane;
- 1917 – prima legătură radio avion-sol;
- 1917 – 1960: dezvoltarea comunicaţiilor radio în domeniile militar, guvernamental şi comercial;
- 1962 – SUA lansează primul satelit comercial de comunicaţii;
- 1964 – Organizaţia „INTELSAT" ia decizia să lanseze sateliţi de comunicaţii;
- 1965 – este lansat primul satelit de comunicaţii „INTELSAT-1". După acest eveniment au apărut şi alte reţele cu destinaţii comerciale dar şi guvernamentale: INMARSAT, EUTELSAT, IRIDIUM, INTERSPUTNIK;
- După anul 1965 se accentuează relaţia biunivocă globalizare - comunicaţii;
- **1967 – Momentul zero al viitorului INTERNET. Pentagonul în cooperare cu câteva universităţi de prestigiu din SUA începe realizarea unei reţele complexe numită ARPANET;**
- 1967 – apare compania INTEL care se specializează în producţia de microprocesoare (moment crucial în accelerarea dezvoltărilor ulterioare în domeniul sistemelor de calcul);
- 1970 – apare banala dischetă, care uşurează în mod substanţial dialogul om-maşină;
- 1971 – ARPANETUL (SUA) ajunge la 15 noduri şi 23 de hosturi. Este vorba de o reţea distribuită în teritoriu, care să poată asigura continuitatea conducerii de către structurile guvernamentale şi militare, în situaţia unui conflict militar major;
- 1971 – apare primul procesor INTEL cunoscut ca ***„chip"***;
- 1972 – se introduce **e-mailul** pe ARPANET;
- 1972 – apare prima reţea locală (LAN) numită ETHERNET;
- 1973 – **vorbim deja de INTERNET**;
- 1981 – „IBM" – realizează primul *„personal computer"* (PC);
- 1982 – în lume sunt 5,5 milioane PC-uri, iar acum în 2016 – 4,5 miliarde;
- 1982 – apare utilul „MOUSE", care uşurează interacţiunea cu computerul;
- 1985 – MICROSOFT lansează *„Windows 1.0"*;

- 1991 – primele conexiuni INTERNET în România, pentru unele universităţi;
- 1992 – în lume sunt 65 milioane de PC-uri şi un milion de hosturi;
- 1992 – **INTERNETUL este globalizat**;
- 1993 – apare domeniul „.ro”;
- 1996 – cetăţenii şi instituţiile din peste 100 de ţări sunt conectate la internet;
- 1997 – apare conceptul de EXTRANET;
- 1998 – apare conceptul de „GRID”, o reţea extinsă cu conexiuni puternice;
- 2000 – 100 de milioane de sisteme de calcul sunt în INTERNET;
- 2007 – se poate afirma că societatea este dominată de puterea şi facilităţile internetului (politică-alegeri, afaceri-finanţe, sisteme bancare, apărare, securitate, mass-media, cetăţeni etc.).
- 2007 – apar şi se extind reţelele şi site-urile populare de socializare şi comunicare (My SPACE, FACEBOOK, YOU TUBE etc.);
- După 2007 şi până astăzi (2016) reţelele s-au dezvoltat exponenţial, astfel că putem consemna[1]:

	POPULAŢIE	**Conectaţi la internet**	**Grad de penetrare**	**% din conexiunile totale în lume**
ÎN LUME	TOTAL ÎN LUME 7,3 mld. oameni	3,367 mld. oameni	46,4%	100%
EU	ÎN EUROPA 822 milioane	604,2 milioane	73,5%	18%
AMERICA DE NORD	AMERICA DE NORD 358 milioane	314 milioane	87,9%	9,3%

- **Situaţia din România în noiembrie 2015**
  -Populaţie: 19.861.408;
  -Conectaţi la internet: 11.178.477 (56,3% penetrare);
  -Conectaţi la FACEBOOK: 8.100.000

[1] www.internetworldstats.com/stats.html

- **Gradul de penetrare în unele ţări europene**

-Danemarca: 96%;
-Franţa: 84%;
-Germania: 88,4%;
-Ungaria: 76%;
-Bulgaria: 56,7%
-Rusia: 70,5%;
-Serbia: 66,2%;
-Ucraina: 43,4%.

Toate datele menţionate mai sus demonstrează, din plin globalizarea sistemelor informaţionale, în general, şi a INTERNETULUI, în special, cu utilizări în toate domeniile de activitate umană.

Vulnerabilităţi şi ameninţări cibernetice

Între autorii care au analizat, utilizând un limbaj accesibil marelui public, problematica complexă a sistemelor informaţionale actuale şi ale atacurilor cibernetice venite din surse diferite, se află şi specialistul american James F. Dunnigan[2], care pe lângă descrierea evoluţiei sistemelor de comunicaţii şi informatice, prezintă, în oglindă, partea neplăcută a proceselor, prin dezvoltarea atacurilor şi înmulţirea atacatorilor fie ei indivizi, grupuri sau unele state.

Specialistul afirmă că cyber-războiului este lupta pentru supremaţia asupra internetului şi a marelui segment din economie care acum depinde de această reţea de computere. Vulnerabile sunt şi structurile guvernamentale şi cele militare, atât în faţa atacatorilor individuali cât şi a atacatorilor state.

Hackerii civili, fie ei individuali sau grupuri, atacă pentru a da lovituri financiare şi de imagine, pe când războinicii militari o fac pentru a ajuta la câştigarea războiului, pentru a produce pagube maxime economiei şi forţelor armate ale adversarului.

Pentru a înţelege mai bine ce distrugeri pot face atacatorii cibernetici este necesar să reamintim câteva elemente ale vocabularului specific acestui gen de acţiuni:

- **Caii troieni** sunt programe deghizate în programe legale. La început, caii troieni au fost folosiţi în scop de farse şi realizau doar nişte glume inofensive. Dar pe parcursul anilor ’80 aceştia au devenit periculoşi, unii dintre ei fiind capabili să distrugă date şi programe. Alţii, odată rulaţi, se răspândeau prin modificarea altui software cu ajutorul propriilor rutine.

[2] James F. Dunnigan, *Noua ameninţare mondială – Cyber-Terorismul*, Editura Curtea Veche, Bucureşti, 2010.

• **Viruşii** sunt ceea ce au devenit caii troieni. Virusul se ataşează de un program sau document autentic. În anii ’90 când caii troieni au început să se răspândească rapid pe internet, au fost numiţi viruşi informatici.

• **Viermii** sunt viruşi care se ataşează de alte programe. De exemplu *„Logic Bomb”*. Acesta este un program ascuns din sistemul Computerului care devine activ numai când sunt îndeplinite anumite condiţii.

• **Zombie** (uneori numiţi boţi, de la roboţi) sunt o variantă a calului troian. Spre deosebire de adevăratele programe cal troian, zombie sunt mai degrabă controlaţi (pe internet) de către persoane care i-a inserat, decât să fie lăsaţi să acţioneze automat.

• **Vampirii** sunt viermi sau viruşi al căror unic scop este să pătrundă atât de adânc în sistem, încât calculatorul infestat să nu mai poată face nimic altceva.

• **Adulmecătorii** sunt instrumente de hacking care colectează informaţiile ce intră sau ies dintr-un computer (de obicei în server). Informaţia este apoi trimisă către cel care a implantat adulmecătorul. Adulmecătorii sunt utili pentru colectarea parolelor sau ID-urilor utilizatorilor.

• **Buffer Overflow Exploitation** este o tehnică prin care se trimite un anumit tip de date către un server web şi se declanşează manifestarea unei deficienţe a software-lui (comună multor produse Microsoft), lucru care permite strecurarea un virus sau un program zombie şi astfel se pătrunde în server, în ciuda apărării.

• **Există** şi alte instrumente de hacking şi arme sofisticate, în permanentă dezvoltare cantitativă şi perfecţionare calitativă care pot aduce multe necazuri utilizatorilor individuali şi celor din corporaţii şi structuri guvernamentale.

Să rememorăm câteva elemente ale evoluţiei ameninţărilor cibernetice resimţite de NATO, Uniunea Europeană şi majoritatea ţărilor membre ale acestor organizaţii, precum şi de către alte state aflate în vizorul unor atacatori[3]:

• **Atacurile executate** cu implicarea unui grup numeros de calculatoare care generează refuzul de a presta serviciile solicitate (distributed denial of service - DDOS), privite până acum ca, de fapt nimic mai mult decât nişte *„blocaje de protest”*, au devenit un instrument în războiul informaţional.

• **În anul 2007** a fost lansat de către un actor statal virusul *„Octombrie Roşu.”* Cele mai multe victime au fost instituţii diplomatice, guvernamentale, companii de energie, inclusiv energie nucleară, instituţii de cercetare ştiinţifică, contractori militari şi firme care se ocupă de industria petrolieră şi de gaze. Atacurile au fost axate pe extragerea de informaţii de la victime, informaţii care

[3] http://www.nato.int/dom/review/2011/11-september/Cyber-Threads

puteau oferi avantaje geostrategice. Instituţii importante din România au fost, la rândul lor, afectate de acest virus.

• **În anul 2008,** unul din cele mai serioase atacuri de până în prezent a fost lansat împotriva sistemelor americane de computere. Prin intermediul unui singur memory-stick conectat la un laptop al armatei, la o bază militară din Orientul Mijlociu, un program spion s-a răspândit nedetectat, atât în sisteme clasificate, cât şi în cele neclasificate. Acest eveniment a realizat ceea ce a echivalat cu un *„cap de pod digital”*, prin care mii de dosare cu date au fost transferate în servere aflate sub control străin. Începând de atunci, spionajul cibernetic a devenit o ameninţare constantă. Incidente similare s-au produs în toate ţările membre NATO.

• **În iunie 2010,** softul maliţios *„Stuxnet”* a devenit public, ceva ca o *„bombă de penetrare a ţintelor blindate digitale”* care a atacat programul nuclear iranian. Prin aceasta, avertizările timpurii transmise de experţi începând din 2001, au devenit realitate, sugerând că dimensiunea cibernetică ar putea fi folosită mai devreme sau mai târziu pentru executarea unor atacuri serioase care vor avea consecinţe letale în lumea reală.

• **În timpul conflictului Georgia - Rusia** s-au produs atacuri masive împotriva website-urilor şi serverelor guvernamentale din Georgia, oferind termenului de război cibernetic o formă mai concretă.

• **În vara lui 2010** s-a răspândit vestea că aproximativ 45 000 de sisteme de control industrial **Siemens** din întreaga lume au fost infectate cu un virus troian special conceput, care putea manipula procesele tehnice de o importanţă crucială pentru controalele nucleare din Iran. Deşi evaluarea avariilor este în continuare neclară, acest lucru a evidenţiat riscul softului maliţios care afectează sisteme de computere de o importanţă crucială în managementul aprovizionării cu energie sau al reţelelor de trafic. Pentru prima dată, aici a existat dovada existenţei atacurilor cibernetice care pot cauza avarii fizice reale şi generează riscul pierderii de vieţi umane.

• **În februarie 2013**[4] se înregistrează un atac puternic prin programul *„Adobe Reader”*. Acesta nu este un atac obişnuit, e un atac extraordinar de sofisticat care apare cam o dată pe an. O vulnerabilitate le permite hackerilor să copieze nişte fişiere pe sistem şi o a doua le permite să scape din sandbox. Cine a făcut atacul este extraordinar (funcţionează pe sisteme Adobe Reader în limba arabă, ebraică, engleză şi greacă).

Concluzia specialiştilor este că avem de a face cu un atac sponsorizat de un stat, de cel mai înalt nivel, atac care a necesitat resurse enorme.

[4] Costin Raiu, *Laboratoarele Kaspersky*, Interviu acordat Ziarului Adevărul, 19 februarie 2013.

• **După debutul crizei**, dintre Ucraina şi Rusia (2014), s-au amplificat atacurile cibernetice împotriva Ucrainei, dar şi împotriva statelor membre NATO şi UE.

• **Este de remarcat** că în 1996 apărea câte un virus nou pe săptămână sau pe lună, acum apar peste 200 000 de viruşi noi pe zi.

• **România**, fiind la ora actuală, puternic conectată la Internet este afectată, mai ales după 2010 de atacurile cibernetice asupra utilizatorilor individuali şi mai nou, ţinte au devenit instituţiile guvernamentale, cele militare şi companiile.

O evaluare echilibrată a ameninţărilor demonstrează clar două lucruri:

• **Până în prezent**, cei mai periculoşi actori în domeniul cibernetic sunt tot statele-naţiuni. În pofida unor capabilităţi ofensive aflate din ce în ce mai mult la dispoziţia reţelelor de criminalitate, care ar putea fi folosite de actori non-statali precum teroriştii, spionajul şi sabotajul de înaltă sofisticare în domeniul cibernetic, aceste grupări au nevoie, în continuare, de capabilităţile, hotărârea şi raţiunea cost-beneficii ale unui stat-naţiune.

• **Pagubele fizice** şi terorismul cibernetic în lumea reală nu s-au produs încă. Este clar că tehnologia atacurilor evoluează de la câteva probleme agasante la o ameninţare serioasă la adresa securităţii informaţiilor şi chiar la adresa infrastructurilor naţionale de o importanţă majoră.

Nu există nici o îndoială că unele ţări investesc deja masiv în capabilităţi cibernetice care pot fi folosite în scopuri militare. La prima vedere, cursa digitală a momentului se bazează pe o logică clară şi implacabilă, deoarece domeniul războiului cibernetic oferă numeroase avantaje: este asimetric, atrăgător prin costurile scăzute, iar atacatorul deţine în faza iniţială toate avantajele.

Mai mult decât atât, nu există practic nicio formă reală de descurajare în cadrul războiului cibernetic, deoarece până şi identificarea atacatorului este extrem de dificilă şi, respectând dreptul internaţional, probabil, aproape imposibil.

Este însă de remarcat că cele mai multe state membre NATO şi UE dezvoltă, în ritm accelerat, capabilităţi de apărare în domeniul cibernetic, mergând de la crearea unui cadru legal şi până la constituirea unor puternice capabilităţi tehnice şi asigurarea cu specialişti de cea mai înaltă clasă în domeniu.

Aflat în faţa provocărilor, în domeniul securităţii cibernetice, NATO încearcă să se adapteze la acest tip de ameninţări şi vulnerabilităţi:

• În 2002 a adresat statelor membre o solicitare vizând îmbunătăţirea *„capabilităţilor acestora de a se apăra împotriva atacurilor cibernetice”*, ca parte a angajamentelor de la Praga privind capabilităţile (noiembrie 2002).

• **Totuşi, în anii de după 2002,** Alianţa s-a concentrat, în primul rând, asupra reglementării unor măsuri pasive de protecţie, care fuseseră solicitate de partea militară.

• **Evenimentele din Estonia** din primăvara lui 2007 au impulsionat Alianţa să-şi regândească în mod radical nevoia de o politică în domeniul apărării cibernetice şi să-şi ridice contra-măsurile la un nou nivel. De aceea, organizaţia a elaborat pentru prima dată o *„Politica NATO privind Apărarea Cibernetică”*, adoptată în ianuarie 2008, document în care au fost stabiliţi trei piloni centrali ai politicii în spaţiul cibernetic:

- **subsidiaritatea** – asistenţa este furnizată numai la cerere, altfel se aplică principiul responsabilităţii proprii purtate de statele suverane.
- **Neduplicarea**, de exemplu, prin evitarea unei duplicări inutile la nivelul structurilor sau au capabilităţilor – la nivel internaţional, regional şi naţional.
- **Securitatea** – cooperarea bazată pe încredere, luând în considerare sensibilitatea informaţiilor legate de sisteme care trebuie puse la dispoziţie şi posibilele vulnerabilităţi.

• **La Summitul de la Lisabona** (noiembrie 2010) Alianţa a pus, cu succes, bazele unei examinări factuale autogestionate a problematicii, din ce în ce mai complexe, a războiului cibernetic.

• **În conformitate cu Noul Concept Strategic al NATO,** politica Alianţei privind Apărarea Cibernetică revăzută defineşte ameninţările cibernetice drept o sursă potenţială care face obiectul apărării colective în concordanţă cu Articolul 5 al NATO. Mai mult decât atât, noua politică şi *„Planul de Acţiune”* pentru implementarea sa – oferă NATO linii directoare clare şi o listă de priorităţi agreată în privinţa modului în care să avanseze apărarea cibernetică a Alianţei.

Securitatea cibernetică – o dimensiune importantă a securităţii naţionale a României

Toate statele lumii resimt efectele pozitive ale evoluţiilor din domeniul tehnologiei informaţiilor şi comunicaţiilor, dar aşa cum am arătat anterior, acestea vin la pachet cu riscuri şi ameninţări şi vulnerabilităţi în domeniul atacurilor cibernetice şi chiar a războiului cibernetic. *„Aceste fenomene implică crearea şi finanţarea unor instituţii care să se ocupe doar de securitatea cibernetică, realizând planuri pentru prevenirea atacurilor cibernetice, pentru posibilitatea de a avea un răspuns rapid în cazul în care asemenea evenimente au loc, pentru abilitatea de a descoperi persoanele sau organizaţiile responsabile pentru acestea astfel încât să fie aduse în faţa justiţiei, şi nu în ultimul rând, pentru abilitatea de a*

înlocui sau repara în cel mai scurt timp componentele afectate ale reţelei digitale."[5]

Securitatea cibernetică reprezintă o provocare ce trebuie abordată prin cooperare între diverşi actori naţionali, precum instituţii, companii private sau organizaţii nonguvernamentale, dar şi la nivel internaţional prin cooperarea între state, organizaţii regionale şi globale, având în vedere faptul că securitatea cibernetică este o problemă globală. Şi România a recunoscut securitatea cibernetică drept o dimensiune importantă pentru securitatea sa naţională în anul 2010, atunci când a fost inclusă în „**Strategia Naţională de Apărare**". Acest document politico-militar include, în ceea ce priveşte securitatea cibernetică, obiective pe termen scurt şi pe termen lung, deoarece menţionează că ţara depinde de buna funcţionare a multiplelor reţele de care depind vieţile cetăţenilor români şi economia naţională. În Strategie se recunoaşte de asemenea, faptul că România are vulnerabilităţi în a asigura securitatea spaţiului cibernetic naţional, deoarece prezintă deficienţe în ceea ce priveşte protecţia şi funcţionarea infrastructurii digitale şi a celei critice.

Totodată, Strategia evidenţiază că un nivel mai ridicat de securitate a infrastructurii digitale este necesară, deoarece la un nivel mondial atacurile cibernetice sunt din ce în ce mai frecvente şi mai complexe. De aceea, România a avut în vedere anumite obiective care între timp au fost îndeplinite, precum înfiinţarea unei comunităţi de experţi în domeniul informaticii şi a securităţii reţelelor digitale, **CERT-RO** (Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică).

CERT-RO este acum un centru funcţional responsabil pentru *„Prevenirea, analiza, identificarea şi reacţia la incidentele cibernetice"* şi pentru dezvoltarea de politici publice în domeniu.

Există, de asemenea, instituţii naţionale implicate în activităţi specifice securităţii cibernetice, precum Ministerul Comunicaţiilor şi Societăţii Informaţionale, Direcţia de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism (DIICOT), Serviciul Român de Informaţii, Ministerul Apărării Naţionale, Ministerul Afacerilor Interne, Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal şi alte câteva având capabilităţi limitate.

Cu toate acestea, nu există încă o instituţie centrală care să se ocupe în mod direct şi cuprinzător de riscuri cibernetice la nivel naţional, având ca fundament o strategie de securitate cibernetică.

[5] http://www.caleaeuropeana.ro/securitate-securitate-cibernetica-national-romania-cepe/ (Autor: Andra Alexandru)

De menţionat că Ministerul Comunicaţiilor şi Societăţii Informaţionale a lansat în iunie 2011 un document de lucru numit *„Strategia de Securitate Cibernetică a României”*, care, întro formă mai complexă a fost aprobat de către CSAT, în februarie 2013.

A fost lansat în dezbatere publică, la începutul acestui an proiectul *„Legea privind Securitatea Cibernetică a României”*. Acesta nu a ajuns în dezbaterea Parlamentului din cauza numeroaselor critici şi rezerve privind viaţa privată a cetăţenilor şi confidenţialitatea necesară pentru mediul de afaceri. Este însă, un document mult aşteptat şi necesar în această fază a atacurilor cibernetice. Să sperăm că până la 31 decembrie 2016 se va găsi o soluţie de compromis şi legea va fi votată şi promulgată.

Trebuie să arătăm că problema securităţii cibernetice este tratată în mod corespunzător şi în *„Ghidul Strategiei Naţionale de Apărare pentru perioada 2015-2019”*, document aprobat prin Hotărârea CSAT nr. 128, din 10 decembrie 2015.

După câte se observă documente sunt şi vor mai fi, dar noi credem că se impun măsuri practice mai hotărâte pentru a răspunde eficient riscurilor, ameninţărilor şi vulnerabilităţilor cibernetice.

Sunt numeroşi specialişti, români şi străini, în domeniul ITC, care propun soluţii de securitate pentru utilizatorii individuali, companii şi structuri guvernamentale, între care menţionăm:

- Să fie folosită o soluţie de securitate actualizată constant;
- Să se remedieze şi să se actualizeze toate programele software care rulează pe terminale şi servere web;
- Să fie instalate soluţii de backup;
- Să se administreze fişierele care rulează în calea de director, *„AppData/Local AppData”* şi să se asigure politici care împiedică utilizatorii să execute aplicaţii sau fişiere;
- Să fie limitată utilizarea de către unele persoane a accesării unor destinaţii din reţea;
- Să se aplice soluţii performante de protecţie a serverelor de e-mail, prin filtrarea conţinutului;
- Să se asigure că angajaţii pot identifica e-mailuri care răspândesc viruşi şi să evite accesarea acestora provenite de la expeditori necunoscuţi;
- Mai sunt şi alte măsuri care privesc alegerea şi protejarea parolei, protecţia împotriva programelor spyware, protecţia atunci când utilizăm reţelele publice folosind şi conexiunile Wi-Fi (cu laptop, telefoane sau tablete).

De la început am menţionat că problematica complexă, de mare actualitate, a atacurilor cibernetice nu poate fi clarificată întrun simplu articol dintr-o revistă.

Scopul este doar ridicarea, în faţa celor interesaţi, a acestor probleme şi descoperirea celor mai bune soluţii de protecţie.

Pentru un studiu mai complet este necesară parcurgerea a zeci de cărţi, studii şi articole activitate care intră în fişa postului administratorilor de reţea şi responsabililor din instituţiile statului cu atribuţii directe în securitatea cibernetică a României.

BIBLIOGRAFIE

Strategia Naţională de Apărare, bucureşti, 2010;

Strategia de Securitate Cibernetică a României, aprobată de CSAT, în luna februarie 2013;

Proiect de Lege privind Securitatea Cibernetică a României", lansat în dezbatere publică de către MCTI, în luna Ianuarie 2016;

Ghidul Strategiei Naţionale de Apărare a ţării pentru perioada 2015-2019, aprobat prin Hotărârea CSAT nr. 128, din 10 decembrie 2015;

DUNNIGAN F.J., *Noua ameninţare mondială – Cyber-Terorismul*, Editura Curtea Veche, Bucureşti, 2010.

RAIU C., *Laboratoarele Kaspersky*, Interviu acordat Ziarului Adevărul, 19 februarie 2013.

www.internetworldstats.com/stats.html

http://www.nato.int/dom/review/2011/11-september/Cyber-Threads/RO/index.htm

http://www.caleaeuropeana.ro/securitate-securitate-cibernetica-national-romania-cepe/

Alte site-uri de profil utilizând căutarea cu „atacuri cibernetice".