ROMÂNIA ÎN SPAȚIUL CIBERNETIC

Victor Adrian Vevera

victor.vevera@gmail.com

Academia Națională de Informații „Mihai Viteazul" Bucureşti

Rezumat: Spațiul cibernetic s-a dovedit per ansamblu rezistent la atacuri şi alte distrugeri, dinamica sa a evoluat în aşa fel încât, atacatorilor le-a fost mai uşor decât apărătorilor. În România, un computer din patru e virusat. Asta înseamnă 1,5 milioane de calculatoare. Cifrele anului trecut arată o creştere cu 70% a numărului atacurilor cibernetice. Specialiştii au avut de analizat 78 de milioane de alerte de securitate. România resimte foarte mult lipsa unei legislații specializate în domeniul securității cibernetice. Oricum ar arăta ea, ar reuși să impună o normă națională care să determine o acțiune coerentă şi susținută a tuturor instituțiilor publice sau private din România. Este un lucru pe care l-au descoperit foarte multe țări europene, care sunt la a doua sau a treia ediție a legislației de securitate cibernetică națională.

Cuvinte cheie: Spațiul cibernetic**,** vulnerabilitate, Securitate cibernetică, spionajul cibernetic, criminalitatea cibernetică.

Abstract: cyberspace has proved resilient to overall attacks and other damage, dynamics evolved in such a way that for attackers have been easier than for defenders. In Romania one in four computers is infected with some kind of virus. That is 1,5 millions computers. The last year figures show an increase with 70% of the number of cybernetic attacks. The specialists had to analyze over 78 millions security alerts. Romania suffers from the lack of specialized cyber security legislation. Good or bad it would be able to determine a national rule that would determine in return a coherent and sustained action of all public or private institutions in Romania. It's something that many European countries discovered, and they are to the second or third edition of national cyber security legislation.

Keywords: Cyberspace , vulnerability, cyber security , cyber espionage , cyber crime.

Spațiul cibernetic este mediul virtual, generat de infrastructurile cibernetice, care include conținutul informațional procesat, stocat sau transmis, precum şi acțiunile derulate de utilizatori în acesta.

Securitate cibernetică este starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea şi nonrepudierea informațiilor în format electronic, a resurselor şi serviciilor publice sau private, din spațiul cibernetic. Măsurile proactive şi reactive pot include: politici, concepte, standarde şi ghiduri de securitate, managementul riscului, activități de instruire şi conştientizare, implementarea de soluții tehnice de protejare a infrastructurilor cibernetice, managementul identității, managementul consecințelor.

Până acum spațiul cibernetic s-a dovedit per ansamblu rezistent la atacuri şi alte distrugeri, dinamica sa a evoluat în aşa fel încât, atacatorilor le-a fost mai uşor decât apărătorilor. Sunt motive care ne duc cu gândul că rezistența este încet subminată, permițând ca dinamica vulnerabilității să aibă un impact mai mare.

În primul rând, creşterea "bunurilor Internetului" înseamnă că din ce în ce mai multe dispozitive sunt conectate online, atingând mult mai multe aspecte ale vieții şi lărgind atât potențialele puncte de intrare cât şi punctele de impact. În al doilea rând, există o adâncire din ce în ce mai mare a complexității interacțiunilor între multele aspecte ale vieții care sunt dependente de dispozitivele conectate, făcând acele impacturi potențial mai greu de prevăzut.

La nivel mondial sunt trei miliarde de utilizatori de internet, adică 40% din populația lumii. În România există şase milioane de computere cu acces la internet.

În România, un computer din patru e virusat. Asta înseamnă 1,5 milioane de calculatoare. Cifrele anului trecut arată o creştere cu 70% a numărului atacurilor cibernetice. Specialiştii au avut de analizat 78 de milioane de alerte de securitate. Toate aceste date se traduc în pierderi de bani şi de informații prețioase. În vremurile noastre, spionajul se duce online, aşa că instituții precum Ministerul de Externe, cel al Apărării sau al Economiei sunt aproape zilnic ținta unor atacuri informatice.

Există patru tipuri de agresori: actorii statali, actorii provenind din mediul crimei organizate, extremiştii şi teroriştii, grupările teroriste. Ameninţarea reprezentată de actorii statali are cel mai ridicat nivel de impact asupra securităţii naţionale, în raport cu celelalte trei tipuri de actori. Actorii statali afectează cel mai mult securitatea naţională a României. Pe locul doi sunt actorii din mediile criminalităţii organizate. Agresiunea cibernetică derulată de extremişti şi terorişti, în acest moment are un nivel scăzut, în raport cu securitatea naţională a României.

Tocmai pentru a putea fi în măsură să înţeleagă evoluţia fenomenului şi să poată anticipa momentul în care vor reprezenta o ameninţare semnificativă pentru securitatea naţională, România acordă o atenţie dedicată acestor două fenomene, acestor două tipuri de actori. Nivelul lor tehnologic este, în acest moment, scăzut şi reuşesc totuşi să fie vizibili în special în media, prin faptul că înlocuiesc conţinutul legitim al site-urilor, fie al instituţiilor, fie al firmelor private, fie al comunicaţiilor, în general al media, cu mesaje, de regulă, de factură religioasă. În esenţă, extremismul este un fenomen pe care îl monitorizăm cu atenţie, dar, pe de altă parte, modul în care se manifestă prin afectarea conţinutului, disponibilităţii şi integrităţii informaţiilor din infrastructurile cibernetice este o altă dimensiune care preocupă Serviciul Român de Informaţii.

În era informaţională, atacatorii din spaţiul virtual sunt cu ochii pe noi, România, ţară membră a NATO şi a Uniunii Europene. Caută la noi tot felul de date, mai ales cele secrete, aflate în posesia Ministerului de Exerne, celui al Apărării sau la Ministerul Economiei.

Practic, se încearcă extragerea de informaţii strategice din reţelele acestor ministere sau ale unor companii private pentru promovarea intereselor statelor care le obţin. România nu face o excepţie şi este ţinta unor asemenea atacuri.

Vorbim aici de spionaj la nivel guvernamental, în care instituţii de stat au fost infectate şi de unde se extrăgeau documente confidenţiale, dar asta nu se întâmplă numai în România. Este noul teren de luptă.

Una dintre cele mai importante operaţiuni de acest gen a fost Octombrie Roşu. Atacul s-a întâmplat în 2013. Specialiştii l-au clasificat drept cel mai grav atac cibernetic la adresa României postdecembriste.

Atacatorii căutau informaţii secrete şi sensibile. În plus, acest tip de atacuri sunt considerate din ce în ce mai mult comandate sau sponsorizate la nivel statal.

În ultimii ani, odată cu dezvoltarea şi dependenţa tot mai mare a proceselor care au loc la nivelul societăţii, au apărut şi ameninţările faţă de infrastructurile care prelucrează şi stochează informaţii. Au fost identificate mai multe tipologii de atacuri. Atacurile statale, atacuri sponsorizate de diverse state care vizează informaţii strategice ale unei ţări, atacuri de tip criminal care vizează obţinerea de foloase financiare şi atacurile de tip terrorist, care sunt într-o fază de început, dar evoluţiile s-ar putea să ajungă la un nivel îngrijorător într-un timp nu foarte îndepărtat.

Multe dintre instituţiile publice din România sunt vulnerabile în faţa unor atacuri de acest fel pentru că folosesc computere învechite şi sisteme de operare care nu sunt aduse la zi.

Aici vulnerabilitatea cea mai mare a administraţiei este scandalul Microsoft. Să nu uităm că licenţele de pe aproape toate aceste calculatoare sunt expirate, prin urmare şi toate licenţele programelor care ofereau o apărare a sistemelor informatice, sunt la rândul lor expirate, sau numai pot fi actualizate, oferind astfel încă o portiţă de invazie pentru eventualii atacatori.

Acestea de regulă se produc prin metoda spear phishing, practic prin transmiterea unor e-mailuri cu ataşamente malitioase, iar deschiderea acestor ataşamente produce practic infectarea calculatorului pe care un utilizator îl foloseşte.

Un virus te poate surprinde în orice moment, în fiecare zi apar pe piaţă foarte multe tipuri de viruşi care au diverse capabilităţi, cum ar fi extragerea credenţialelor pentru conectarea la contul bancar, extragerea credenţialelor pentru diverse site-uri pe care te conectezi, extragerea de informaţii din calculator în cazul în care te afli într-o instituţie. Aceşti viruşi sunt suficient de inteligenţi şi sunt creaţi pentru a extrage ceea ce doreşte creatorul lor.

Pentru că este un domeniu în care urmele sunt mai greu de descoperit, organizațiile teroriste din întreaga lume se apleacă cu tot mai mare interes asupra internetului. Specialiştii susțin că ciber-terorismul este noua provocare de securitate.

Perspectivele sunt ca cei care vor să facă cu adevărat rău să înceapă să recruteze specialişti cu o expertiză mai înaltă, iar obiectivul lor, cel de a crea panică, poate să vizeze infrastructuri cibernetice critice cum ar fi: domeniul transporturilor, domeniul energiei, domeniul energiei nucleare, ceea ce ar fi şi mai grav.

După spionajul cibernetic, criminalitatea cibernetică a avut un impact major asupra securității naționale a României.

În România nivelul amenințării cibernetice a crescut de la an la an, începând din 2008, anul în care s-a început în mod instituțional evaluarea nivelului amenințării cibernetice, an în care a fost constituit Centrul Național CYBERINT în interiorul SRI. Practic, constatăm că, în fiecare an, nivelul amenințării cibernetice creşte. Această creştere este una semnificativă şi calitativă.

România are deja la activ cel puțin trei botneți de concepție proprie, națională. Hackerii români sunt foarte imaginativi şi foarte ingenioşi şi au o adaptabilitate singulară pe piață. Cu caracter de noutate, există forumuri de hackeri în lume care au diverse reputații. În cel mai apreciat şi cel mai important forum de criminalitate cibernetică, în top 10 utilizatori sunt trei români, adică în primii 10 din lume trei sunt români.

Statutul României de membru NATO a dus la creşterea atacurilor cibernetice asupra țării noastre.

Atât direct cât şi indirect, România a fost țintă a acestor atacuri, pentru că ştim foarte bine că au fost atacuri care au vizat Alianța. Este evident că toate evenimentele care au implicat NATO în ultimii ani au constituit subiect de interes pentru agresori, încercând să înțeleagă, să culeagă informații despre intențiile, deciziile şi resursele pe care le are NATO pentru a gestiona diferite crize sau situații la nivel global, având în vedere rolul defensiv al Alianței. Din acest punct de vedere, România şi-a adus contribuția la securitatea Alianței în întregimea ei, ca şi organizație.

România, datorită poziționării pe care o are, şi aici mă refer la sistemul de alianțe din care facem parte, calitatea de membru al Uniunii Europene, poziția geostrategică în care suntem, toate evenimentele în care suntem parte sunt factori care determină creşterea nivelului amenințării cibernetice. Din acest punct de vedere, România nu este o victimă colaterală, ci este, alături de celelalte state europene, o țintă explicită a acestor atacuri.

Resimțim foarte mult lipsa unei legislații specializate în domeniul securității cibernetice. Oricum ar arăta ea, ar reuşi să impună o normă națională care să determine o acțiune coerentă şi susținută a tuturor instituțiilor publice sau private din România. Este un lucru pe care l-au descoperit foarte multe țări europene, care sunt la a doua sau a treia ediție a legislației de securitate cibernetică națională.

Plenul Camerei Deputaților a aprobat în septembrie 2015 proiectul de lege pentru modificarea legii privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul comunicațiilor electronice. Proiectul a fost adoptat cu 187 voturi pentru, 12 împotrivă şi 22 de abțineri.

Potrivit actului normativ, accesul la datele personale se poate face numai cu autorizarea prealabilă a judecătorului.

„La solicitarea instanțelor de judecată sau la solicitarea organelor de urmărire penală ori a organelor de stat cu atribuții în domeniul apărării şi securității naționale, cu autorizarea prealabilă a judecătorului stabilit potrivit legii, furnizorii de servicii de comunicații electronice destinate publicului şi furnizorii de rețele publice de comunicații electronice pun la dispoziția acestora, de îndată, dar nu mai târziu de 48 de ore, datele de trafic, datele de identificare a echipamentului şi datele de localizare, în conformitate cu prevederile referitoare la protecția datelor cu caracter personal”, se prevede în proiect.

BIBLIOGRAFIE

1. *** Legea nr. 235/2015 pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice.
2. *** Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice.
3. *** Strategia de Securitate Cibernetică a României.
4. www.securitatea-cibernetica.ro
5. www.cert.org
6. www.europa.eu