Agresiunile în spațiul cibernetic

Dumitru DUMBRAVĂ
Serviciul Român de Informații
e-mail: **dumbrava_dumitru@dcti.ro**

Abstract

Since the advent of Internet in the 1990s, not all users have acted in cyberspace for peaceful purposes. In fact the threat and impact of attacks in and through cyberspace have continously grown to the extent that cyberspace has emerged as a setting for war, with increasing potential to damage the national security of states. Because of this reason, the international community has to come up with a body of norms, or regulations that must be established in order to deter agression in cyberspace.

As cyberspace matures, the international system faces a new challenge in confronting the use of force. Non-state actors continue to grow in importance, acquiring the skill and expertise necessary to wage asymmetric warfare using non-traditional weaponry that can create devastating real world consequences. These actors involved with various types of crimes also vary in their skill sets, interests and motivations. Some are identified as internal threats, while others are external – encompassing national as well as international players. All actors vary in age, education, gender, ethnicity, as well as their skills, professional status and social relationships. Since it is nearly impossible to identify the plethora of actors according to physical discriminating factors, elements of skills, motivation and social relationships within the community of hackers can successfully be used to differentiate and categorize their threat potential. The international legal system must adapt to this battleground and provide workable mechanisms to hold aggressive actors accountable for their actions. The very nature of cyberspace: its lack of territorial definability; its organisational capacities; and its decentralised structure plays an important role in cyberspace governance.

Keywords: cyberspace, cyber agressions, cyber security, cyber intelligence.

Aprecieri preliminare

Apariția şi dezvoltarea calculatoarelor electronice a reprezentat o adevărată revoluție în societatea umană, având ca principală consecință tranziția de la societatea industrială la societatea informațională.

Calculatorul a devenit o componentă normală a activității noastre zilnice, iar tehnologia comunicațiilor şi posibilitățile oferite de Internet au produs transformări în întreaga societate, pătrunzând în toate aspectele vieții economice, sociale şi culturale.

Istoria Internetului este o lectură fascinantă, plină de paradoxuri, originile sale putând explica pe deplin configurația sa actuală. Ca în orice domeniu în care inovația joacă un rol deosebit, în Internet există etape precursoare, acumulări anterioare mai importante sau mai puțin importante. Dezvoltarea Internetului a depins, în mod evident, de tehnologie, dar în egală măsură şi de factori sociali care s-au îmbinat pentru ca acesta să ajungă ceea ce este astăzi. Iar o dată instaurat în fibrele societății, Internetul a produs şi produce consecințe noi pentru societate, cel mai important dintre acestea fiind procesul de globalizare.

În anul 1990, Internetul cuprindea aproximativ 3000 de rețele şi 200.000 de calculatoare, în 1992, existau peste 1 milion de gazde, iar în anul 1995 existau mai multe coloane vertebrale (rețele principale), sute de rețele de nivel mediu (regionale), zeci de mii de LAN-uri, milioane de gazde şi zeci de milioane de utilizatori. Mărimea Internet-ului se dublează aproximativ la fiecare an, iar creşterea lui este datorată şi conectării unor rețele existente, precum rețeaua de fizică spațială NASA.

Caracterul academic, guvernamental şi industrial pe care l-a avut Internetul până în anul 1990 s-a transformat, însă, odată cu apariția noii aplicații WWW (World Wide Web), care a adus în rețea milioane de utilizatori neprofesionişti. În zilele noastre, mediul Internet poate fi privit ca o rețea de rețele, un mediu informațional şi de calcul cu resurse şi servicii extrem de bogate, biblioteci şi baze de date, el reunind, prin facilitățile de informare şi comunicare oferite, o comunitate de persoane din toate domeniile vieții economico-sociale şi răspunzând la solicitări diverse.

Astfel, dacă în anii 1970 sintagma predominantă era aceea de Societate informatică, treptat conceptul de Societate informațională a câştigat tot mai mult teren şi a devenit o realitate din momentul exploziei Internetului, cu accente deosebite în ultimul deceniu al secolului XX, pentru prima parte a secolul XXI urmând a se pune problema Societății Cunoaşterii.

În acest context, Societatea Cunoaşterii depinde, cu siguranță, de performanțele şi securitatea infrastructurilor critice, precum: sistemele de producere, transport şi distribuție ale energiei, sistemele de telecomunicație, bănci, sistemele de transport aerian, naval, rutier şi feroviar.

„Cunoaşterea", ca atare, a devenit o „armă" de apărare împotriva

ameninţărilor cu care se confruntă un mediu popular, uşor de utilizat şi care, în acelaşi timp, oferă o cantitate imensă de informaţie despre orice subiect posibil.

Spaţiul cibernetic

Noţiunea a fost lansată pentru prima dată de către William Gibson – scriitor canadian de science fiction – în anul 1982, prin nuvela „*Burning Crome*", apărută în revista *Omni*, care a fost ulterior popularizată în romanul său – „*Neuromancer*". Aceasta a devenit o sursă de inspiraţie artistică care a generat cybercultura şi, datorită importanţei şi relevanţei ei psiho-sociologice, un obiect de studiu pentru ştiinţele sociale, determinând apariţia unor areale teoretice şi de cercetare, precum psihologia şi sociologia cyberspaţiului, informatica socială etc.

Spaţiul cibernetic este corelat cu o serie de termeni înrudiţi, precum cei de realitate virtuală, mediu *online*, spaţiu digital, care alcătuiesc împreună un aparat conceptual, încă destul de tânăr şi, prin urmare, disputat, ce s-a conglomerat în jurul noului domeniu. Asupra noţiunii de spaţiu cibernetic s-au adunat, în timp, mai multe perspective, pe măsură ce acest fenomen s-a dezvoltat în extensie, profunzime şi nuanţe prin răspândirea şi popularizarea reţelei mondiale de computere şi telecomunicaţii (ce include Internetul, Usenetul şi alte reţele mai mici ca importanţă) şi, prin varierea instrumentelor şi aplicaţiilor (domeniul de *software*), varietate la fel de exponenţială ca şi globalizarea infrastructurii sale (*hardware şi netware*).

În principiu, spaţiul cibernetic nu trebuie confundat cu Internetul real (ca reţea), ci trebuie privit ca însumând aspectele psihologice şi sociale pe care i le conferă, prin utilizare, psihicul uman individual şi societatea în ansamblu. Acesta cuprinde, prin urmare, identităţile şi obiectele care există în reţele de computere folosite de indivizii umani în diverse scopuri.

Multitudinea perspectivelor de analiză a generat numeroase teorii şi definiţii acordate spaţiului cibernetic.

În prezent, spaţiul cibernetic a devenit coloana vertebrală a ceea ce numim Societatea Cunoaşterii, concepută ca un mediu foarte diferit, fără precedent, în care implementarea ultimelor realizări tehnice trebuie să meargă în paralel cu adoptarea de noi soluţii juridice menite să monitorizeze efectele negative ale impactului utilizării tehnologiei informaţiei şi comunicaţiilor şi ameninţările în mediul informaţional.

Ameninţări

Contrar convingerii larg răspândite, preocupările legate de securitatea cibernetică nu sunt un fenomen al anilor 1990. Viruşii şi viermii informatici au fost o parte din zgomotul de fundal al spațiului cibernetic, chiar dintr-o perioadă timpurie. Astfel, în filmul „War Games", produs în anul 1986, un tânăr adolescent hacker reuşeşte ca, prin intermediul computerului personal, să dețină comanda şi controlul asupra arsenalului nuclear american. De asemenea, celebrul incident „Cuckoo's Egg", de la mijlocul anilor '80, a atras atenția că organizațiile de spionaj au descoperit noi modalități de a obține informații clasificate, prin intermediul rețelelor de calculatoare.

În acest context, dezbaterile pe teme cibernetice, îşi au originea în Statele Unite la mijlocul anilor '90, de unde s-au răspândit ulterior în alte țări dezvoltate şi sunt trecute într-o varietate de forme pe ordinea de zi a politicilor de securitate.

Comparativ cu analiza amenințărilor tradiționale, care constă în analize ale actorilor, intențiilor şi capacităților lor, amenințările în mediul informațional au caracteristici diferite care fac atacurile dificil de monitorizat, analizat şi contracarat. Aceste caracteristici se încadrează în tipologii care pot fi regăsite în toate țările, deşi accentul pus pe una sau mai multe dintre ele conduce la diferențe considerabile.

În prezent, amenințările la adresele utilizatorilor variază de la accidente, căderi de sistem, programări greşite şi eşecuri umane, la atacuri ale hackerilor. Totodată, securitatea cibernetică este o şi problemă economică, iar acest concept este definitoriu pentru continuitatea afacerilor, în special a afacerilor on-line, care, pentru performanță, necesită acces permanent la infrastructurile de comunicații.

Şi, deşi multe organizații au investit în mod semnificativ în obținerea de informații în acest domeniu, majoritatea experților în securitatea rețelelor de calculatoare cred că un adversar bine echipat din punct de vedere tehnologic va avea mai mult succes în derularea unor agresiuni cibernetice cu impact semnificativ atât din punct de vedere distructiv cât şi al complexității tehnice, mai ales dacă dezvoltarea mecanismelor de protecție a sistemelor de calcul este singurul răspuns la un atac.

Deci, ne aflăm în fața unei mari probleme, foarte greu de rezolvat, deoarece în interiorul arhitecturii Internet actuale este aproape imposibil să se identifice sursa atacurilor cibernetice, iar capacitățile de investigație din lumea fizică sunt mult mai avansate decât sunt cele din domeniul cibernetic.

Datorită structurii globale a rețelelor de informații, atacurile pot fi

lansate de oriunde din lume, iar descoperirea originii atacurilor rămâne o dificultate majoră, în cazul în care acestea sunt într-adevăr detectate.

De asemenea, nu există statistici exacte referitor la agresiunile cibernetice care au loc anual, însă majoritatea experților consideră că numărul celor derulate în zilele noastre este atât de mare încât cifrele par irelevante. Cu titlu de exemplu, menționez că numărul lor este atât de mare încât, în anul 2004, guvernul american a oprit raportarea agresiunilor cibernetice în acel an, în condițiile în care în anul 2003 acestea depășiseră 100.000.

Taxonomia amenințărilor

Într-un interviu cu Information Security Media Group, Dmitri Alperovitch (McAfee Labs) vorbeşte despre provocările amenințărilor prezente din mediul informațional şi face referiri la modul în care le pot contracara persoanele fizice şi juridice.

Astfel, acestea sunt principalele riscuri şi vulnerabilități identificate de McAfee Labs pentru anul 2011[1]:

Exploatarea rețelelor de socializare

Rețelele de socializare ocupă locul principal în furtul de identitate, precum şi ca distribuitor de malware pe e-mail. În mod similar, se constată, de asemenea, creşterea abuzurilor prin scurtarea URL-ului şi prin dezvoltarea serviciilor locative.

Telefoane mobile inteligente (smartphones)

Accesarea internetului de pe telefoanele mobile inteligente pentru îndeplinirea unor atribuții de serviciu are drept urmare creşterea amenințărilor cibernetice nu numai pentru indivizi, dar şi pentru angajatorii lor.

Apple

Din punct de vedere istoric, sistemele de operare Apple nu au fost direcționate pentru abuz, dar popularitatea iPad-urilor şi iPhone-urilor în afaceri şi portabilitatea uşoară de cod malițios ar putea schimba acest lucru, în anii următori.

Aplicații

[1] http://www.bankinfosecurity.asia/podcasts.php?podcastID=908

Fie la domiciliu, fie la locul de muncă, aplicațiile pe dispozitive, cum ar fi iPhone şi Androids devin din ce în ce mai populare şi vor deveni din ce în ce mai mult obiective-țintă, întrucât au un istoric slab de codare şi practici de securitate primitive, astfel încât infractorii din spațiul cibernetic vor încerca să manipuleze o varietate de dispozitive fizice prin aplicații compromise sau controlate, precum şi prin creşterea eficienței botnets la un nou nivel.

Rafinamentul imită legitimitatea

În anul 2010, s-a observat o creştere a gradului de sofisticare al unor amenințări, cum ar fi malware disimulat în fişiere normale. Deoarece această tendință s-a intensificat în anul 2011, s-a putut observa o creştere a tehnicilor şi echipamentelor destinate să creeze chei false.

Supraviețuirea Botnet

În anul următor, McAfee Labs se aşteaptă mai degrabă la o creştere a botnet-urilor care elimina datele din sistemele orientate, decât trimiterea de spam. Botnet-urile se vor angaja în colectarea de date rezultate din exploatarea rețelelor sociale.

Activismul cibernetic (Hacktivism)

În ceea ce demonstrează episodul WikiLeaks, hacktiviştii vor creşte utilizarea de crowdsourcing pentru a recruta o armată de hackeri motivați să urmeze o agendă politică. Aceste atacuri nu sunt sofisticate şi organizațiile ar trebui să poată să se apere cu succes împotriva lor în cazul în care iau măsurile corespunzătoare.

Avansarea de amenințări persistente

Aceste atacuri, efectuate fie de către statele națiune sau garantate în mod direct sau indirect, de către guverne străine, nu au fost extrem de sofisticate, dar după cum spune si numele, ele sunt persistente. Se aşteaptă intensificarea acestora în anul următor, fiind vizate arhivele e-mail, documentele şi bazele de date ale arhivelor de proprietate intelectuală.

De asemenea, în ultimele luni, o atenție deosebită a fost acordată unor evenimente de un nivel mai modest, deşi supărătoare, cum ar fi

agresiunile suportate de către RSA, Sony şi Epsilon.

În acelaşi registru, Joe Gottlieb, directorul executiv al riscului şi securităţii, furnizor de software de management SenSage, compară publicitatea agresivă promovată de hactivişti cu operaţiunile efectuate pe furiş de către actorii din operaţiunea RAT Shady[2]: „Aceste hackeri s-au implicat în colectarea de informaţii fără a trebui să trâmbiţeze atacurile lor cu succes, aceştia au rămas tăcuţi pentru a acumula în linişte IP valoroase şi alte produse digitale de contrabandă". Aceasta este cheia, respectiv actele ascunse ale agresiunilor cibernetice, pe care le vom vedea tot mai mult începând de astăzi.

Abilitatea de a automatiza colectarea datelor, eforturile tenace de folosire a Cyber-crawlerelor, crearea de spaţii tot mai largi în acelaşi timp cu transmiterea datelor recoltate înapoi la o imensă bază de date de informaţii, în vederea acumulării sunt principalele atuuri dar şi principalii factori de vulnerabilitate

Din acest punct de vedere, ameninţările cibernetice, adevărate ameninţări la adresa securităţii naţionale, ca şi atacurile împotriva infrastructurii informatice a altui stat sau oponent, sunt percepute în general ca instrumente de coerciţie strategică.

În timp ce atacurile care încalcă confidenţialitatea, integritatea sau disponibilitatea sistemelor de informaţii ar putea, cel puţin teoretic, să fie tratate ca acte de război şi să fie introduse în domeniul de aplicare al controlului armamentului, ori să fie supuse dispoziţiilor care reglementează dreptul războiului.

Aşadar, într-un mediu în care actorii şi motivele sunt necunoscuţi, iar consecinţele potenţiale pot fi de amploare, este uşor de înţeles de ce există o mare îngrijorare.

Iar în cazul în care există atât de mulţi actori, cu atât de multe motive, iar activităţile desfăşurate de aceştia ar putea fi inofensive şi chiar protejate prin Constituţie, este uşor de înţeles de ce persoanelor responsabile pentru implementarea măsurilor strategice şi tactice le vine atât de greu.

Într-o lume plină de diverse ameninţări, precum şi de acuzaţii referitoare la creşterea criminalităţii cibernetice, spionajul economic, spionajul militar şi războiul informatic, este extrem de important ca guvernele şi profesioniştii din domeniul securităţii sistemelor informatice să gândească diferenţiat despre evenimentele cibernetice de tip malware şi despre

[2] http://blogs.mcafee.com/mcafee-labs/revealed-operation-shady-rat

modalitatea de a răspunde la ele.

Punctul de pornire este acela de fracturare a agresiunilor prin sistematizare şi clasare. Cu privire la „cine" (şi în mod implicit „de ce"), poate exista o puternică atribuire, o oarecare probabilitate de atribuire (mai ridicată sau mai scăzută) sau nici o atribuire.

În aceşti parametrii, mai pragmatici, principalele ameninţări cibernetice pot fi definite pe următoarele coordonate:

Spionajul cibernetic, în care cel mai mare pericol îl reprezintă serviciile de informaţii, civile şi militare. Anumite ţări utilizează grupările de hackeri şi criminalitate organizată informatică drept forţe cu rol de proxy – în spatele cărora se ascund pentru a putea nega implicarea lor, ca actor statal.

Spionajul cibernetic are 3 dimensiuni:

a) Spionajul economic – produce prejudiciul cel mai grav, deoarece instituţii guvernamentale, companii şi cetăţeni străini sunt angrenate în operaţiuni de furt al proprietăţii intelectuale şi al informaţiilor de afaceri confidenţiale. Fiecare euro investit de statul ţintit şi fiecare an de cercetare-dezvoltare a tehnologiilor de vârf se transformă în cenţi cheltuiţi şi zile consumate de statul agresor pentru a obţine prin spionaj economic acelaşi avantaj tehnologic şi economic.

b) Spionajul politic.

c) Spionajul militar.

Datorită unui nivel scăzut al securităţii cibernetice, spionajul cibernetic oferă posibilităţi de neimaginat în culegerea de informaţii, atât în volum cât şi în sensibilitate, greu de atins prin spionajul clasic.

În acelaşi timp, constituie un nou instrument pentru acţiunea politică statală: în loc să controleze crima organizată sau să creeze diversiuni prin relatări false în ziare, un serviciu de informaţii poate influenţa decizii prin atacuri DDoS, efectuează demascări prin Internet a documentelor obţinute prin hacking sau poate utiliza viruşi sofisticaţi în încercarea de a manipula politica statului agresat.

Criminalitatea organizată cibernetică, al cărui scop este mai degrabă patrimonial, să obţină bani de la instituţii financiar-bancare, decât să sustragă proprietatea intelectuală a unor ţinte. Criminalitatea organizată cibernetică nu va urmări să atace Infrastructura Critică Informaţională a unui stat, atât timp cât infractorii sunt ocupaţi să producă prejudicii financiare, însă în anumite condiţii, aceste prejudicii pot atinge o dimensiune care să afecteze stabilitatea a unor pieţe financiare sau a unor economii, context în care devine de interes pentru securitatea naţională a unui stat.

Se consideră că, în anumite țări, criminalitatea organizată cibernetică poate juca un rol important de forță proxy, atât timp cât oferă unor state capacitatea de a nega implicarea în operațiuni de spionaj sau acțiuni politice.

Activismul cibernetic (hactivismul) – în prezent nu reprezintă un risc acut pentru securitatea națională, însă va continua să-şi mențină tendința atât de intensificare, motivat de un spectru din ce în ce mai larg de motivații pentru sancționarea unor atitudini politice, sociale, ecologice, religioase şi militare, cât şi de radicalizare a impactului acestor atacuri.

Terorismul cibernetic – acesta nu este un risc în acest moment. Teroriştii nu au lansat, până în prezent, nici un atac cibernetic şi ca atare, se consideră că nu sunt întrunite condițiile ca aceste grupări să asimileze cunoştințele tehnologice necesare astfel încât, pe termen scurt şi mediu (3-5 ani) să realizeze un atac de complexitate mare la adresa ICI ale unui stat.

Pe termen lung, nu este, totuşi, exclusă o astfel de evoluție, având în vedere tocmai asimetria amenințărilor cibernetice.

Riscul unui război cibernetic a apărut pe harta de riscuri ale unui stat modern, odată cu apariția virusului Stuxnet, şi deşi este în prezent într-o fază incipientă, evoluția va fi extrem de dinamică. Pe termen scurt, atacurile militare cibernetice vor fi utilizate doar într-un context mai larg al unui conflict militar convențional.

De asemenea, o amploare deosebită a luat în ultimii ani şi **agresarea comunicațiilor electronice.** Astfel, în primul trimestru al anului 2011, a fost semnalată intruziunea în comunicațiile electronice provenite din 199 de țări de pe mapamond. Myanmar a fost în topul surselor de atac al comunicațiilor, reprezentând 13% din totalul agresiunilor observate.

În acest domeniu, Statele Unite ale Americii şi Taiwan ocupă cea de a doua şi, respectiv, cea de a treia poziție, acumulând împreună aproape 20% din totalul atacurilor[3]. Concentrația agresiunilor a fost mai mică cu 10 porturi decât în al patrulea trimestru din anul 2010, reprezentând 65% din totalul agresiunilor observate, fiind remarcat inclusiv un set de atacuri care au urmărit au căutat să utilizeze instrumentele de confidențialitate TOR de pe Internet ca modalități de a-şi ascunde urmele.

Securitatea cibernetică

Protejarea spațiul cibernetic este o responsabilitate comună, nicio entitate individuală sau grup de persoane interesate neputând rezolva singuri

[3] http://www.akamai.com/stateoftheinternet/

problemele în acest domeniu.

Cei implicați în industrie, consumatorii, marile companii şi guvernele trebuie să ia toate măsurile pentru a-şi asigura propriile sisteme informatice, fiind nevoie să colaboreze unii cu alții pentru a defini şi a pune în aplicare politici din domeniul securității cibernetice şi al tehnologiei.

Securitatea cibernetică nu presupune doar protejarea împotriva amenințărilor actuale. Ea permite, de asemenea, creşterea randamentului şi beneficiul de a permite utilizări extinse şi mai sofisticate în mediul digital.

Totodată, securitatea cibernetică oferă persoanelor fizice, companiilor şi guvernelor mai multă încredere că pot opera în acest mediu, şi îi pot încredința bunuri de valoare şi informații.

În lumina celor de mai sus, putem concluziona că elementele de referință pentru asigurarea securității spațiului cibernetic trebuie orientate pe următoarele coordonate:

- Securitatea din spațiul cibernetic nu este o problemă opțională, ci o necesitate imperioasă, având în vedere impactul acesteia asupra securității naționale, siguranței publice şi bunăstării economice.
- Problema securității cibernetice trebuie să treacă dincolo de măsurile tradiționale, tehnologice, cum ar fi programele anti-virus si firewall-uri.
- Securitatea cibernetică trebuie să fie dinamică în structura sa, şi să aibă profunzimea necesară pentru a identifica, opri şi preveni atacurile.
- Securitatea informațiilor trebuie să constituie o componentă integrantă a securității în spațiul cibernetic, pentru a fi în măsură să anticipeze atacuri, să adopte măsuri adecvate de combatere şi să-şi însuşească atributele de acțiune împotriva posibilelor atacuri.

Cu alte cuvinte, trebuie urmărită corelarea eficientă a informațiilor recepționate din surse multiple şi monitorizarea în timp real a bunurilor care au nevoie de protecție, prin asigurarea expertizei corespunzătoare pentru a face față situațiilor de criză.

Apărarea cibernetică

În timp ce securitatea cibernetică este activitatea de protecție a informațiilor şi a sistemelor informatice (rețele, calculatoare, baze de date, centre de date şi aplicații), cu măsuri de securitate adecvate din punctul de vedere procedural şi tehnologic şi are un caracter generic, incluzând toate activitățile de protecție, apărarea cibernetică se referă la o activitate mult mai specializată, legată de aspecte particulare şi de organizare.

În general, apărarea cibernetică este determinată de informațiile obținute cu privire la amenințările îndreptate contra sistemului de apărare, care conduce, colectează, analizează şi difuzează informații relevante şi secrete utilizabile pentru părțile interesate de inițierea unor demersuri proactive necesare, în vederea întreprinderii măsurilor de prevenire şi protecție, termenul specific acesteia fiind acela de „cyber intelligence". Acesta este un termen despre care nu auzi prea multe, dar care ar putea reține o atenție mult mai mare în perioada următoare.

Cu privire la acesta, Chuck Alsup, vice-preşedintele desemnat cu politica Alianței Nord-Atlantice a declarat că „Noi nu sunt încă pregătiți să propunem o definiție definitivă". „În acest moment, vorbim despre amenințările neidentificate din domeniul cibernetic, cu potențiale consecințe enorme, de la distrugerea fizică la haosul economic. Oamenii care monitorizează şi răspund de aceste amenințări formează o singură organizație constituită cu ajutorul guvernului, zonei de afaceri şi mediului academic, precum şi al partenerilor străini"[4].

Principiile directoare ale securității cibernetice

Standardele internaționale stabilite de către industrie şi acceptate pe plan internațional, stau la baza tehnologiei informației de la nivel mondial (IT), fiind menite să impulsioneze dezvoltarea şi utilizarea unor tehnologii inovatoare şi sigure. Politica securității cibernetice ar trebui să mențină rolul standardelor internaționale.

Politicile de securitate cibernetică trebuie să recunoască natura fără margini a Internetului, a economiei globale şi a amenințărilor cibernetice şi, drept urmare, este indicat ca guvernele să coopereze pentru a asigura cadrul legislativ național de politică cibernetică integrată în abordările şi practicile globale.

Regimurile sunt de obicei definite drept „seturi de principii implicite sau explicite, norme, reguli, şi procese de luare a deciziilor în jurul unor valori determinate", elemente care converg spre domeniul relațiilor internaționale.

În ultimele două decenii, o serie de inițiative au fost întreprinse pe plan internațional în vederea îmbunătățirii securității şi fiabilității sistemelor, a practicilor de management, precum şi a cooperării polițieneşti internaționale.

Astfel, pentru a ajuta guvernele să construiască şi să implementeze planuri cuprinzătoare şi viabile, care să funcționeze la nivel național şi mondial,

[4] http://blogs.govinfosecurity.com/posts.php?postID=1061

Business Software Alliance BSA a stabilit următorul set de principii directoare[5]:

1. Politica marilor trusturi cibernetice ar trebui să sporească încrederea consumatorilor, întreprinderilor şi guvernelor cu privire la confidențialitatea, integritatea şi disponibilitatea mediului on-line.

2. Inovația în mediul cibernetic este o cursă extrem de rapidă, în care ne lovim de acțiunea infractorilor cibernetici, care se adaptează în mod constant.

3. Politica în domeniul securității cibernetice ar trebui să maximizeze capacitatea organizațiilor de a dezvolta şi adopta cea mai recentă gamă posibilă de soluții cibernetice.

4. În cadrul unei abordări bazate pe riscuri, consumatorii, întreprinderile şi agențiile guvernamentale încearcă să protejeze un spectru extins de obiective împotriva unei game largi de amenințări cibernetice.

5. Mecanismele securității cibernetice permit punerea în aplicare a măsurilor de prevenire care sunt cele mai potrivite pentru a atenua riscurile specifice cu care se confruntă.

Posibile soluții

Peisajul amenințărilor cibernetice a evoluat semnificativ în ultimii ani, în primul rând de la contestarea serviciilor şi vandalism pe site-urile web în ultimii ani, la adversarii din prezent bine echipați din punctul de vedere tehnologic, care utilizează tehnologii complexe pentru a obține beneficii financiare şi politice.

Privind în urmă, anii 2010-2011 par să fi fost dominați de rapoarte pe o singură problemă de securitate analizată într-un mod special: amenințările cibernetice. Prejudiciul provocat de atacurile cibernetice este din ce în ce mai frecvent, mai organizat şi mai costisitor, iar percepția asupra acestui fenomen s-a schimbat.

Rezultatul este clar: atacurile cibernetice sunt considerate unele dintre amenințările de securitate de top şi au fost reglementate în documentele naționale de strategie peste tot în lume.

Astfel, descoperirea Stuxnet, super-viermele sabotor al industriei, care a speriat politicienii din toată lumea, poveştile despre spionajul chinez în mai multe variante, creşterea nivelului de specializare al infractorilor cibernetici aşa cum reiese din escrocheriile lor impresionante, precum si documentele Wikileaks despre canalele diplomatice şi acțiunile ulterioare ale grupului de hackeri Anonim, toate acestea au catapultat subiectele

[5] http://www.bsa.org/~/media/Files/Policy/Security/CyberSecure/Cybersecurity_Framework.ashx

cibernetice din domeniul excentricilor experţi IT şi al strategilor militari într-o fobie publică.

Devine clar pentru toată lumea că securitatea cibernetică este tot mai pregnant o problemă de securitate naţională, societatea aşa cum o ştim, precum şi valorile sale de bază fiind pe cale de dispariţie, din cauza dependenţei lor de domeniul informaţiei şi tehnologiei comunicaţiilor.

Acţiunea împotriva acestei ameninţări se desfăşoară, atât la nivel naţional cât şi în plan internaţional, pe mai multe niveluri tehnice, legislative sau organizatorice, iar actorii sunt specialiştii în securitatea informatică.

Având în vedere această stare de spirit generală, menţiunile NATO se referă în documentul „Noul Concept Strategic”[6] din noiembrie 2010 la atacurile cibernetice ca fiind unele dintre problemele esenţiale pentru viitorul său de securitate.

Dar pentru NATO acest fapt nu a reprezentat doar o potenţială strategie, el este totodată un element de referinţă prin care marchează un punct culminant în politica de securitate a Alianţei care se ocupă cu analiza ameninţării.

Pornind de la aceeaşi concluzie evidentă că nici o naţiune din zilele noastre nu poate face faţă ameninţărilor cibernetice pentru a gestiona pe cont propriu arhitectura globală de reţele, deoarece natura acesteia, împreună cu numărul semnificativ de agenţi implicaţi în administrarea sistemelor, face imposibilă identificarea unei limite de aplicare în cadrul jurisdicţiilor stabilite sau definite teritorial, Consiliul Europei a elaborat în anul 2001, Convenţiei privind Criminalitatea Cibernetică.

Păstrând aceleaşi coordonate, în ultimii ani, instituţiile UE au făcut un pas important pentru a contracara ameninţările atacurilor cibernetice îndreptate împotriva lor, a organismelor şi agenţiilor, prin înfiinţarea unui Computer Emergency Response pre-configuration TEAM (CERT)[7]. Echipa astfel formată reuneşte experţi în securitate IT de la toate instituţiile UE. La terminarea stagiului de un an pregătitor în echipă, va fi făcută o evaluare menită să conducă la o decizie cu privire la condiţiile de stabilire a unui CERT pe scară largă pentru instituţiile UE.

În ultimii ani, CERT au fost dezvoltate în sectoarele privat şi public, atât în echipe mici de cyber-experţi conectaţi la Internet, care pot în mod eficient să răspundă la incidentele de securitate a informaţiilor şi la ameninţările cibernetice, de multe ori pe o durată de 24 de ore pe zi, timp de şapte zile

[6] http://www.nato.int/strategic-concept/index.html
[7] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/694

pe săptămână.

În Agenda digitală pentru Europa[8], adoptată în luna mai 2010 (a se vedea IP/10/581, MEMO/10/199 şi MEMO/10/200), Comisia s-a angajat să stabilească un CERT pentru instituțiile UE, ca parte a angajamentului asumat, într-o rețea consolidată la nivelul UE si a politicii de informații pentru securitate în Europa.

În luna august 2010, Comisia a solicitat unui număr de patru experți în securitatea cibernetică, cunoscuți sub numele de „Rat der IT Weisen"[9], să facă recomandări cu privire la modul de a înființa un astfel de CERT.

Raportul lor a fost finalizat în luna noiembrie 2010. Agenda digitală, de asemenea, invită toate statele membre să stabilească propriile lor CERT-uri, deschizând calea către o rețea de echipe naționale şi guvernamentale Computer Emergency Response, la nivelul UE, până în anul 2012 (a se vedea IP/11/395).

Concluziile adoptate pe data de 27 mai de către Consiliul UE al miniştrilor telecomunicațiilor au confirmat acest obiectiv.

Neelie Kroes, vicepreşedinte al Comisiei Europene pentru Agenda digitală, a declarat că „cyber-atacurile sunt o amenințare foarte reală şi în continuă creştere, fie împotriva unor entități statale, a companiilor sau cel mai recent împotriva Comisiei Europene, acestea putând paraliza cheile de infrastructură şi cauza daune imense pe termen lung".

Implementarea acestui CERT pre-configurare în echipă este o demonstrație a modului în care instituțiile UE iau în serios amenințările la adresa securității informatice.

În loc de concluzii

Din cele prezentate un fapt devine evident, acela că securitatea informațiilor se referă atât la oameni cât şi la tehnologii şi, ca atare, există o nevoie clară de concentrare atât asupra activității oamenilor şi a proceselor tehnologice. Este nevoie de timp pentru a identifica cele mai bune soluții, dar acestea trebuie să aibă în vedere că cele mai bune soluții tehnologice disponibile s-ar putea dovedi ineficiente fără o utilizare a forței de muncă într-un mod adecvat, instruit şi calificat, pentru obținerea unor rezultate eficiente într-un domeniu extrem de specializat, reprezentat de securitatea cibernetică.

Astfel, apărarea are nevoie să fie construită încă din faza de proiectare conceptuală, atunci când vine vorba despre dezvoltarea şi implementarea infrastructurilor critice de informație, spre deosebire de mecanismele de protecție care au ca obiectiv implementarea după un proiect ulterior.

Planificarea strategică a securității cibernetice este, în prezent,

[8] http://ec.europa.eu/information_society/digital-agenda/index_en.htm

[9] http://www.enisa.europa.eu/media/news-items/speech-on-european-and-international-cooperation-on-incident-response

în plină dezvoltare şi trebuie concentrată pe dezvoltarea la scară largă a serviciilor, pentru realizarea acestui deziderat fiind necesar ca toți actorii implicați să acționeze în mod concertat.

Din punctul de vedere istoric, majoritatea națiunilor au elaborat versiuni originale ale Strategiilor societății informaționale, cu o elementară atenție acordată criminalității cibernetice în cadrul politicii naționale de securitate cibernetică reflectată la dimensiunea securității naționale.

Astfel, Guvernele din întreaga lume îşi recunosc atribuții multiple în asigurarea securității cibernetice, incluzând:

1. Protecția sistemelor informatice.
2. Colaborarea cu sectorul privat pentru a proteja infrastructura digitală.
3. Investigarea, cercetarea şi urmărirea penală a infractorilor cibernetici.

Însă, într-un mediu în care există atât de mulți actori, cu atât de multe motive, în care consecințele potențiale pot fi de amploare, iar activitățile desfăşurate de actori sunt uneori la limita legalității şi chiar protejate prin Constituție, este uşor de înțeles de ce există o mare îngrijorare şi de ce, mai mult ca oricând, este extrem de important ca guvernele şi profesioniştii din domeniul securității sistemelor informatice să-şi conjuge eforturile pentru a putea asigura protecția unui spațiu precum cel cibernetic.

Bibliografie selectivă

Resurse Internet

1. http://www.bankinfosecurity.asia
2. http://blogs.mcafee.com
3. http://www.akamai.com
4. http://blogs.govinfosecurity.com
5. http://www.bsa.org
6. http://www.nato.int
7. http://europa.eu
8. http://ec.europa.eu
9. http://www.enisa.europa.eu