De la amenințarea cibernetică la acțiunea ostilă în spațiul cibernetic

Adrian Victor VEVERA
Institutul Naţional de Cercetare-Dezvoltare în Informatică, ICI Bucureşti
victor.vevera@ici.ro

Rezumat: În contextul agresiunilor cibernetice de dată recentă putem spune că acestea reprezintă pentru societatea informaţională cea mai mare provocare. Din acest motiv, o componentă fundamentală a securităţii naţionale a oricărui stat modern o reprezintă asigurarea securităţii cibernetice. Întrucât spațiul cibernetic al unui stat capătă din ce în ce mai mult o valoare critică pentru efectiv orice aspect al societății moderne, riscurile și amenințările la adresa Securității Naționale vor continua să crească pe măsură ce instituțiile guvernamentale și sectorul privat vor continua să se dezvolte sub forma unor rețele; cetățenii se vor baza tot mai des pe serviciile societății informaționale şi vor utiliza spațiul cibernetic în activitățile zilnice; sistemele digitale vor dispune la intervale de timp tot mai scurte de noi resurse tehnice, iar proiectarea, producerea şi furnizarea de servicii din domeniul tehnologiei informațiilor vor deveni tot mai accesibile. Sistemele informatice şi de comunicaţii ale unui stat, precum şi datele gestionate de acestea, tind să constituie, pe măsură ce progresul tehnologic estompează și chiar șterge granițe între domenii complementare, un singur mediu, „spațiul cibernetic”. Această evoluție a spațiului cibernetic determină un fenomen fără precedent care răspândește idei ce influențează comunități masive de oameni, determină evenimente regionale și continentale, schimbă strategii globale și trasează noi granițe, statale sau ale zonelor de influență. Astfel, statele-națiune și actorii non-statali au un interes crescând în rolul pe care spațiul cibernetic îl are în formarea și susținerea opiniilor ce depășesc frontierele unui stat, în apariția și propagarea ideologiilor ce schimbă sau pun sub semnul întrebării relația cetățeanului cu valorile fundamentale ale statului, precum identitatea națională, unitatea, independența sau suveranitatea statală.

Cuvinte cheie: atac cibernetic, reţea informaţională, ameninţare cibernetică, securitate informaţională.

From cyber threat to hostile action in cyberspace

Abstract: In the context of recent cyber-aggressions, we can say that they represent the greatest challenge for the information society. For this reason, a fundamental part of the national security of any modern state is to ensure cyber security. Since a state's cyber space is gaining an increasingly critical value for almost any aspect of modern society, the risks and threats to the National Security will continue to grow as government and private sector institutions continue to develop themselves in the shape of networks; citizens will rely more and more on information society services and use cyber space in daily activities; digital systems will have new technical resources at shorter time spans, while the design, production and provision of information technology services will become more and more accessible. The information and communications systems of a state, as well as the data managed by them, tend to build, as technological progress blurs and even clears borders between complementary domains, a single environment, the „cyberspace.” This evolution of cyberspace causes an unprecedented phenomenon that spreads ideas that influence massive communities of people, determines regional and continental events, changes global strategies and draws new borders, state or influence zones. Thus, nation states and non-state actors have an increasing interest in the role that cyberspace has in forming and sustaining opinions that transcend the borders of a state, in the emergence and propagation of ideologies that change or question the citizen's relationship with fundamental values of the state, such as national identity, state unity, independence or sovereignty.

Keywords: cyber attack, information network, cyber threat, information security.

1. Introducere

Creşterea conectivităţii între sistemele informatice, ce compun Internetul, şi alte infrastructuri creează oportunităţi pentru agresorii ce urmăresc să distrugă sistemele de comunicaţii, infrastructura naţională energetică, reţelele financiare sau alte infrastructuri critice ale unui stat.

Un atac cibernetic de succes derulat împotriva principalilor operatori de servicii financiare din stat poate avea un impact sever asupra monedei naţionale şi implicit asupra economiei naţionale, în timp ce un atac cibernetic asupra reţelei de calculatoare ce gestionează fie furnizarea de energie electrică, fie transportul de resurse energetice, are capacitatea de a întrerupe activitatea industriei naţionale pentru ore sau săptămâni, toate acestea putând induce intrarea în colaps a unui stat dacă atacul are o durată mai mare.

Estimările arată că din ce în ce mai mulţi actori statali dispun şi îşi perfecţionează capabilităţile tehnice de a ţinti şi penetra informativ infrastructura critică a altor state a căror existenţă şi funcţionare poate determina chiar existenţa statului, inclusiv din domeniul securităţii şi apărării naţionale. Se anticipează că agresiunile informatice vor deveni un standard minimal în culegerea de informaţii prin mijloace tehnice secrete, dar şi în viitoarele conflicte politice şi militare.

Pe de altă parte, grupările criminale continuă să-şi dezvolte nivelul de complexitate şi sofisticare a capabilităţilor tehnice deţinute, dar şi a ţintelor pe care au început să le vizeze.

Astăzi, crima organizată transfrontalieră operează prin intermediul unei adevărate economii cibernetice infracţionale, în care victimele sunt dintr-un spectru din ce în ce mai larg de entităţi ce utilizează tranzacţiile electronice, începând de la persoane private până la instituţii financiar-bancare.

2. Amenințările cibernetice - caracteristici

Dacă în cazurile mai sus-menţionate, spaţiul cibernetic al unui stat este un mediu de propagare şi amplificare a ameninţărilor (asimetrice şi transfrontaliere, dar de acum, convenţionale) la adresa securităţii naţionale, ultimii ani au demonstrat că a apărut o nouă tipologie de ameninţare la adresa securităţii naţionale a unui stat: ameninţările cibernetice.

În cazul acestor ameninţări, spaţiul cibernetic al unui stat este chiar ţinta unui atac cibernetic, iar adeseori agresiunea la adresa sistemelor naţionale informatice şi de comunicaţii este un scop în sine.

Agresiunile cibernetice vizează însă cu predilecţie sistemele TIC (tehnologia informaţiei şi comunicaţii) ce reprezintă Infrastructuri Critice în sine denumite şi Infrastructuri Critice Informaţionale (ICI), dar şi sistemele TIC ce sunt esenţiale pentru funcţionarea celorlalte Infrastructuri Critice Naţionale ale statului, a căror disfuncţionalitate, chiar şi temporară, are efecte destabilizatoare asupra Securităţii Naţionale (telecomunicaţiile şi reţeaua Internet, infrastructura de transport aerian, feroviar şi rutier, sistemele de aprovizionare cu energie, gaze, petrol şi apă, serviciile medicale, sistemul financiar-bancar etc.).

2.1. Caracteristicile ameninţărilor cibernetice

Amenințările cibernetice se caracterizează prin câteva aspecte:

- caracter asimetric – capacitatea atacatorului de a cauza pierderi substanţiale, chiar critice, cu investiţii şi riscuri reduse;
- dificultate în atribuire – presupune eforturi semnificative pentru a stabili identitatea agresorului şi este un proces cronofag, în detrimentul vitezei cu care se derulează atacul;
- predictibilitate redusă – numărul mare de domenii vizate şi ritmul accelerat de evoluţie tehnologică;
- dinamism extrem – procesele au loc cu o viteză care fac dificil de constatat şi stopat un atac cibernetic, fapt pentru care un rol însemnat îl are limitarea consecinţelor unui astfel de atac.

Datorită acestor caracteristici, spaţiul cibernetic este deja considerat un nou domeniu de confruntare (desfăşurată preponderent pe timp de pace!), alături de cel terestru, maritim, aerian şi spaţial.

2.2. Tipologia agresorilor cibernetici

În contextul unei diversităţi atât de mari a scopurilor şi motivaţiilor care determină manifestarea ameninţării cibernetice, este cu atât mai dificil de cunoscut, prevenit şi contracarat un atac cibernetic cu cât profilul agresorilor cibernetici, ce pot fi actori statali sau non-statali, implică de regulă un nivel tehnologic mult superior sistemelor atacate. Din acest punct de vedere, literatura de specialitate distinge două tipuri de agresori (activităţile ambelor categorii fiind considerate infracţiuni): hackeri „white-hat" – sunt cei care identifică vulnerabilităţile unui sistem informatic şi de comunicaţii, fără însă să întreprindă agresiuni, care eventual aduc la cunoştinţa sistemelor vizate acele vulnerabilităţi, şi hackeri „black-hat" (crakeri) – sunt cei care identifică vulnerabilităţile unui sistem informatic şi de comunicaţii, dar care însă întreprind agresiuni asupra acestora sau fac publice aceste vulnerabilităţi unor grupuri ce au ca obiectiv desfăşurarea unor astfel de agresiuni.

Pentru a înţelege mai bine actorii ameninţărilor, vom realiza o prezentare a acestora în raport cu următoarele caracteristici: **experienţă, resurse, organizare, ţinte vizate, mod de acţiune, motivaţii, nivel de pericol.**

Ţinând cont de aceste şapte caracteristici, s-au identificat trei tipuri de agresori:

- Amatori;
- Profesionişti;
- Actori statali.

Tipul de agresor	Experienţă	Resurse	Organizare	Ţinte vizate	Mod de acţiune	Motivaţii	Nivel de pericol
AMATORI	lipsă de experienţă	fonduri limitate	comportament oportunist	ţintesc vulnerabilităţi cunoscute	utilizează viruşi, viermi, troieni rudimentari, reţele de boţi	motivaţi de ego şi vanitate, protest ideologic* (hacktivismul), accederea şi obţinerea unui statut într-un grup meritocratic, şi, nu în ultimul rând, banii**	uşor de detectat
PROFESIONIŞTI	experienţă de nivel înalt	bine finanţaţi	activitate focalizată şi organizată	ţintesc şi exploatează date a căror compromitere produce consecinţe semnificative	utilizează viruşi, viermi, troieni rudimentari, reţele de boţi ca mijloc pentru introducerea unor programe informatice mult mai sofisticate	preponderent financiare şi apartenenţa la un grup	detectabili, dar greu de atribuit unui anumit atac cibernetic
ACTORI STATALI	experienţă de nivel foarte înalt	extrem de bine finanţaţi	de regulă, sunt structuri ale serviciilor de informaţii	urmăresc obţinerea de tehnologii şi accesează disimulat reţele cu informaţii sensibile	folosesc aplicaţii maliţioase foarte sofisticate, dintr-o gamă foarte diversificată, disimulate inclusiv în componentele hard ale echipamentelor	evidente (prin apartenenţa la un stat)	dificil de detectat

* Determinat de o paletă largă de motivaţii, plecând de la promovarea ideii liberului acces la informaţii, până la sancţionarea unor atitudini politice, militare, sociale, ştiinţifice, ecologice etc.

** Bani obţinuţi nu prin furtul de date personale şi bancare, ci de exemplu, prin şantajarea unor mari companii pentru a nu compromite datele confidenţiale ale clienţilor lor, pentru a nu declanşa atacuri DDOS asupra site-urilor lor sau pentru a nu face publice anumite vulnerabilităţi ale unor programe informatice cu valoare comercială.

2.3. Activități ostile în spațiul cibernetic

Putem descrie etapa actuală printr-o varietate de oferte atractive, servicii şi produse, dezvoltate pentru confortul utilizatorilor și accesul rapid la informaţii. Situația duplicitară apare în momentul în care acestea, găsindu-se pe internet, devin unelte şi resurse pentru un atac cibernetic. Mai mult decât atât, se creează mediul propice pentru valorificarea de noi puncte vulnerabile ale reţelelor.

În acest context, atacul cibernetic ia forma unei arme care poate fi susţinută cu resurse financiare, umane și temporale minimale, în comparaţie cu alte moduri de acţiuni cu caracter agresiv. Consecinţa este de moment, iar efectele se menţin de-a lungul timpului, situaţie la care contribuie şi faptul că acela care atacă își păstrează anonimatul.

Caracterul deliberat sau gradul în care este afectat(ă) o persoană sau un obiectiv (prin aceasta fiind atinsă economia sau securitatea unui stat) poartă în subsidiar amprenta acţiunilor teroriste sau ale terorismului cibernetic. Aceasta se compune din două elemente de bază: dispozitivul electronic și rețeaua care provoacă prejudicii de proporţii, scopul fiind de a înlătura sau intimida adversarul.

Raportându-ne la reţelele publice, Internetul este cel mai mare mijloc de informare în masă care dispune de date confidenţiale, conectează telefoane mobile, computere, rețele, servere, precum și alte dispozitive și asigură mentenanța de domenii variate: administraţie publică, comerţ, afaceri, bănci.

Ingineria Socială

Aceasta reprezintă una din cele mai accesibile şi mai eficace forme de atac, deși nu necesită cunoștințe în câmpul tehnologiilor informatice. Prin aceasta se reușește manipularea persoanelor cheie din structura care urmează să fie atacată pentru a întreprinde anumite acțiuni care îl pot ajuta pe atacator să inițieze un atac.

Pentru că ingineria socială nu este foarte complicată, deseori nu se iau în considerare astfel de atacuri şi drept urmare pot atrage daune uriaşe într-o întreprindere. Motivul pentru care ingineria socială devine o armă puternică în mâna atacatorului îl constituie faptul că de foarte multe ori sunt asociate şi alte tipuri de atac.

Această strategie de atac poate fi evitată prin introducerea şi implementarea de tehnici de protecție care apără accesul liber la date în incinta unei companii de persoanele care nu sunt autorizate, pregătirea şi instruirea personalului, înștiințarea persoanelor care lucrează temporar în cazul în care apare o nouă persoană autorizată etc.

O tehnică asemănătoare cu cea descrisă mai sus şi care este folosită de atacatori o reprezintă *Dumpster Diving*, care presupune aflarea codului de programe, a parolelor, dar şi resursele neutilizate. Din acest motiv, este importantă şi necesară distrugerea datelor confidențiale, iar nu aruncarea lor.

În gama metodelor de atac cu această structură se regăsesc: *phishing-ul, vishing-ul şi baiting-ul.* Prin realizarea unor site-uri de *phishing* este simulată o organizație legitimă şi sunt cerute date cu caracter confidenţial de la un utilizator (de pildă, victima primește pe e-mail un mesaj ce conține site-ul simulat al unei instituţii adevărate, având logo-ul acesteia, iar în cazul în care un utilizator iniţiază logarea, acesta trimite parola sa hackerului. Vishing-ul este o metodă de phishing prin intermediul apelurilor telefonice. Riscul expunerii la astfel de atacuri poate fi limitat prin educarea permanentă cu privire la cele mai bune practici de securitate cibernetică.

Atunci când cel atacat adaugă un cod toxic în propriul computer, doar din curiozitate, vorbim despre atacul de tip *baiting*. Putem descrie aceasta metodă astfel: hackerul lăsa la îndemâna victimei un dispozitiv de stocare – unitate de stocare USB, disc –, care, la momentul introducerii în

computer, instalează automat codul dăunător. Din curiozitate, victima poate introduce acel dispozitiv de stocare cu scopul vizualizării datelor pe care le poate conţine, infectând astfel computerul şi oferind hackerului o fereastră de intrare.

Atacuri SMTP

Bazat, de regulă, pe vulnerabilitatea buffer overflow, acest tip de atac presupune inserarea în textul mesajului a unui conținut prea mare, iar în componenta care nu intră în e-mail sunt conţinute comenzi pentru serverul e-mail, prin urmare, după ce mesajul este trimis, comenzile ascunse vor aplica codul dăunător din structura mesajului, oferind hackerului posibilitatea de a sparge serverul.

O modalitate de apărare împotriva acestui tip de atac o reprezintă actualizarea regulată a software-ului şi sistemului de operare al serverului, în scopul evitării punctelor vulnerabile.

Spargerea parolelor

Acest tip de atac se produce atunci când hackerul efectuează operațiuni pentru a realiza autorizarea şi autentificarea într-o structură informatică, scopul final fiind acela de a-i dobândi resursele. În cele mai multe dintre situații, hackerul nu obține parolele, ci hash-ul acestora. Întrucât funcția de codificare a parolelor nu este una interșanjabilă, iar parola nu poate fi calculată cunoscând hash-ul, ea este de obicei găsită printr-un proces de selecție al tuturor opțiunilor fezabile, sau cu ajutorul unui dicționar, până în momentul în care coincide parola criptată cu hash-ul obținut. Există o paletă variată de metode de criptare, însă cele mai sigure şi cele mai des utilizate în momentul de față sunt md5 şi sha. *Salting*-ul este o tehnică de codificare a parolelor, în funcție de numele de utilizator, complicându-se astfel considerabil spargerea lor.

Pentru evitarea riscului de decodificare a parolelor este necesar ca acestea să îndeplinească câteva criterii care să-i asigure un grad mare de dificultate – să includă majuscule, litere mici, semne de punctuație, cifre. În plus, parolele trebuie să fie modificate regulat, argumentul fiind acela de a nu da atacatorului ocazia de a reuși să le decodifice în această perioadă de timp.

Flooding

Flooding-ul reflectă situația în care un server sau host este inundat de un volum neobișnuit de pachete, scopul fiind supraîncărcarea serverului. Există două moduri:

SYN Flood – când inundarea se produce cu pachete speciale SYN, fără trimiterea pachetelor ACK ca răspuns înapoi. Această operațiune se traduce prin faptul că un computer recepționează pachete SYN peste cât este capabil să proceseze, lăsând multe conexiuni semideschise simultan.

O soluție de apărare contra acestui tip de atac este serviciul denumit SYNcookie. Acesta prelucrează în altă manieră stabilirea legăturii dintre computere prin intermediul handshaking-ului. Fără această componentă, legătura s-ar putea face astfel: Subiectul solicită o conexiune, trimițând către server un pachet SYN. Serverul notifică faptul că solicitarea a fost recepționată, şi transmite la rândul său un pachet SYN-ACK subiectului. Ultimul pas, prin care acesta îi trimite pachetul ACK, confirmă conexiunea. Prin SYNcookie, legătura se face după cum urmează: Computerul α transmite numărul λ computerului β pentru a solicita conexiunea. Acesta generează numărul λ, reprezentând o modificare criptată a lui λ. Dacă computerul β acceptă, conexiunea are loc. Acest proces face să nu fie nevoie să fie salvate toate pachetele SYN deschise pe jumătate, pe cale de consecință aceste atacuri nu îşi vor mai produce efectele.

Crearea unor programe care, după un anumit timp, vor şterge automat pachetele SYN, reprezintă o altă metodă de protecție. Regula ce se impune este foarte simplă: dacă receptorul nu solicită răspuns, pachetul urmează să fie şters.

Întrucât metodele de apărare împotriva SYN Flood sunt utilizate frecvent, rețelele nu sunt vulnerabile în momentul de față.

ICMP ping Flood, este un atac care se realizează prin inundarea cu pinguri. Această metodă prezintă un pericol numai atunci când lăţimea de bandă a sistemului este considerabil mai mică decât a sursei atacului. În situaţia în care atacul se produce, computerul atacat va folosi un volum mare din lățimea sa de bandă, iar operaţiuni adiţionale nu vor mai putea fi derulate.

Momentan, genul acesta de atacuri nu reprezintă o amenințare, întrucât lățimile de bandă sunt de regulă suficiente pentru a susţine volumul de cereri ICMP.

Spoofing

Nu întotdeauna un atac, spoofingul este, de regulă, însoțit de un atac. Ca particularitate, avem ascunderea informației despre computerul atacator (de pildă, adresa IP, adresa MAC, serverul DHCP, DNS, User-ul agentului etc.). Spoofing-ul este folosit la ascunderea identităţii atacatorului și a complica aflarea computerului care atacă, putându-se realiza prin serviciile anonime de pe internet, punctele slabe din protocoalele TCP/IP, serverele proxy, etc.

Prin utilizarea Spoofingului pentru IP, atacatorul are posibilitatea de a trimite pachete dăunătoare unui computer din rețea, iar acela îi va răspunde computerului cu adresa IP sub care s-a ascuns atacatorul. Pentru acest motiv IP Spoofingul este utilizat adesea în atacuri de tip smurf, MITM, DoS, pentru redirecționarea traficului sau pentru accesarea rețelei protejate de un firewall, dacă se cunoaşte un IP ce poate accesa rețeaua.

O tehnică eficace de atac este Spoofingul Numerelor Secvențiale întrucât rețelele TCP/IP folosesc numere secvențiale pentru a stabili conexiuni, prin intermediul procesului de handshaking. Acestea se bazează pe ceasul intern al computerului respectiv, calculat după un algoritm.

Prin urmărirea numerelor secvențiale transmise între două computere se pot efectua calcule cu privire la valorile următoare ale acestor numere, iar prin trimiterea acelor numere calculate se permite intrarea într-o rețea de încredere cu computerele victime.

Asemănător cu acesta este Session Highjacking, numai aici este însușită ilicit sesiunea unui client, prin substituirea adresei IP sau MAC reale, cu adresele clientului deja conectat la rețea, astfel obținând privilegiile acelui client în rețeaua dată.

Codificarea datelor între routere şi hosturi externe este cea mai des întâlnită tehnică de apărare împotriva Spoofingului deoarece reduce riscul ca atacatorul să intre în timp util în posesia datelor despre computerul respectiv. O altă modalitate ar fi filtrarea în firewall a traficului extern ce vine de la un host de încredere din interiorul rețelei, ce ar evita IP Spoofingul.

Sniffing

Sniffingul este un proces de capturare şi de interpretare a traficului. Utilitarele folosite pentru sniffing poartă denumirea de sniffere sau analizatoare de protocoale. Acestea analizează pachetele transmise în rețea, capturând parolele, sau alte date confidențiale transmise în formă de text simplu. Deseori, analizatoarele de protocoale sunt folosite în rețele locale, dar pot fi întâlnite, de asemenea, în rețelele WAN. Sniffingul este simplu de utilizat în LAN în cazul în care placa de rețea a victimei e setată în modul „promiscuous”, fapt ce asigură că informația poate fi citită indiferent de IP-ul sursei.

Pentru protecția împotriva acestui tip de atac, se utilizează IPSec, care codifică traficul din rețea, astfel încât informațiile strânse de atacator să nu fie simplu de descifrat. Programele anti-sniffer sunt o altă metodă de protejare întrucât acestea verifică dacă rețeaua este monitorizată sau nu.

De asemenea, folosirea *switch*-urilor în loc de *hub*-uri face posibilă segmentarea subrețelelor. Pe cale de consecință, hackerul dintr-un segment de subrețea nu va putea analiza traficul dintre computerele unei alte subrețele.

Denial of Service (DoS)

Prin acest tip de atac schimbăm un pic paradigma în sensul că ținta atacurilor DoS nu constă în colectarea informațiilor sau a parolelor, ci în împiedicarea utilizatorilor legitimi de a se folosi de anumite resurse ale rețelei. Sunt cunoscute două moduri de manifestare ale atacurilor DoS: prin inundarea serverului cu informație invalidă sau prin scoaterea lui din funcțiune. Drept urmare, orice atac care are ca scop limitarea disponibilității unui host poate fi catalogat ca atac DoS. Cele mai întâlnite atacuri DoS sunt bazate pe protocoalele TCP/IP. Acestea se manifestă prin una din următoarele metode: împiedicarea comunicării dintre două calculatoare, prin aceasta ele nemaiputând comunica adecvat, distrugerea fizică a componentelor rețelei, consumul resurselor computaționale (de exemplu, lățimea benzii de transfer, spațiul pe hard, puterea procesorului etc.), coruperea configurațiilor informației sau coruperea stării informației (de exemplu, întreruperea nesolicitată a conexiunilor TCP/IP).

Sunt cunoscute diferite tipuri de atacuri DoS, printre care:

Ping of Death

Prin intermediul unui astfel de atac sunt trimise pinguri într-un volum care depășește maximul de 65535 B, astfel că pachetul ICMP ajunge fragmentat, iar stația victimă trebuie să îl reasambleze, timp în care mai primeşte pinguri, iar sistemul se supraîncarcă.

Atacuri Teardrop

Deşi are la bază un principiu similar cu cel din cazul Ping of Death, acest tip de atac foloseşte defectele în protocoalele TCP/IP. Reasamblarea devine imposibilă după ce pachetele au fost trimise în rețea din cauza unei valori eronate a *offset*-ului introdus în traficul IP. Acest aspect este un punct vulnerabil critic în codul de reasamblare a pachetelor invalide din TCP/IP. Computerul ajunge să se supraîncarce, urmare a prelucrării multor pachete invalide.

Atacuri peer-to-peer

Atacatorii au aflat punctele vulnerabile ale rețelelor peer-to-peer, fapt care le-a permis să pornească atacuri DDoS prin intermediul computerelor zombie din rețeaua p2p. Specificitatea acestui tip de atac față de atacurile DDoS simple constă în faptul că hackerul nu are nevoie să comunice cu computerele zombie pentru a iniția un atac. Acestea se vor deconecta automat de la rețeaua p2p, începând astfel atacul asupra serverului web victimă. În situația atacurilor cu un număr mare de computere, serverul se supraîncarcă. Chiar dacă îşi închide conexiunile, tot va cheltui multe resurse.

Prin menționarea explicită a porturilor permise, şi a celor care nu sunt permise, în protocolul p2p această situație poate fi ocolită. De exemplu, blocând portul 80, condițiile optime de atac al serverului web prin această metodă devin foarte mici.

Permanent Denial of Service (PDoS)

Acest tip de atac este cunoscut ca şi Phlashing şi reprezintă atacul care afectează sistemul într-o proporție atât de mare încât este nevoie de schimbarea de componente hardware, sau chiar a întregului sistem. Hackerul reușește astfel să obțină acces la un router, printre sau alte componente din rețea, prin intermediul cărora poate schimba *firmware*-ul cu o imagine invalidă, coruptă sau modificată, distrugând astfel acea componentă.

Flood la nivelul de aplicație

Flood-ul pe Internet Relay Chat (IRC), este o armă de atac utilizată frecvent. Ea are ca scop excluderea unui utilizator din conversație, sau chiar închiderea conversației, prin intermediului *Flood*-ului. Întâlnim metode variate de astfel de atacuri, printre care conectarea/deconectarea foarte rapidă și repetată, schimbarea *nick*-ului, trimiterea unui număr enorm de notificări, invitații, mesaje victimei într-un timp scurt, trimiterea unor mesaje extrem de lungi.

SPAM-ul poate fi, de asemenea, un atac DoS. Utilizatorii unui server e-mail pot recepționa mesaje cu caracter neplăcut sau pe care nu le-au solicitat, mesaje care fac reclamă la produse variate inutile etc. Acestea reprezintă *SPAM*-ul, care nu are ca scop deranjarea utilizatorului, ci atacul serverului, prin transmiterea a numeroase e-mailuri, pe care unii utilizatori le trimit altora. Ceea ce își doresc *SPAM*-erii este supraîncărcarea serverului, care poate conduce la folosirea în întregime a lățimii de bandă, a spațiului de pe hard sau a puterii de procesare. *SPAM*-ul poate include o adresă de returnare falsificată, sub numele unui utilizator adevărat. Drept urmare, e-mailul acestuia va fi invadat de răspunsuri la mesaj. Programele anti-spam pot filtra mesajele nesolicitate, însă deseori acestea interpretează ca SPAM şi mesajele legitime.

Diferite utilizări care exploatează punctele vulnerabile buffer overflow pot folosi întreg spațiul de pe disc, sau puterea de procesare, făcând astfel serverul ineficient. Un alt tip de atac DoS poate fi aplicat prin bruteforce, adică prin transmiterea de numere mari de pachete victimei, saturând lățimea de bandă a victimei, astfel încât alți utilizatori legitimi nu o pot folosi. O astfel de metodă este folosită de regulă în atacurile DDoS. Un alt exemplu este atunci când se supraîncarcă un anumit serviciu al serverului, ocupând tot spațiul de pe hard cu fișierele de înregistrare log. Un mod deosebit de atac DoS îl reprezintă „Banana attack”, prin care sunt redirecționate toate pachetele transmise de client serverului înapoi clientului, inundând-ul cu aceleași pachete trimise.

Întrucât are acces la computerul afectat, hackerul îi poate încetini activitatea într-atât de mult încât să devină inutilizabil. În acest scop este folosit Fork Bomb, o operaţiune care se lansează pe sine însăși de atâtea ori, atât cât permite numărul maxim de sloturi de proces al sistemului de operare. Mai mult, în cazul în care se închide un proces, acesta se deschide automat din nou şi nu îngăduie computerului să facă alte operaţii, sistemul devenind astfel inutilizabil.

DdoS

Distributed Denial of Service este o tehnică prin care un singur server este atacat de multe computere zombie. Particularitatea o constituie faptul că atacatorul le infectează prin tehnici variate, cel mai adesea prin programele malware, în care este înscrisă adresa IP a victimei, ca atare nu este necesară implicarea atacatorului pentru inițierea atacului. Totuși, în unele cazuri acesta poate prelua controlul asupra computerelor infectate. Această tehnică este folosită în atacurile Smurf şi Fraggle, pe care le vom detalia mai jos.

Momentan, nu există metode eficiente de evitare a atacurilor DdoS. Mai mult, nu poate fi aflată uşor proveniența atacului.

Distributed Reflected Denial of Service Attack (DRDoS)

Acest atac presupune trimiterea de cereri false către un număr mare de computere, iar cu ajutorul IP Spoofing, se redirecționează toate răspunsurile către hostul cu IP-ul emulat. Atacul Smurf reprezintă un tip de atac DRDoS şi se referă la generarea unui trafic enorm în interiorul unei rețele, prin intermediul pachetelor ICMP cu o adresă IP modificată a sursei. În cazul în care routerul transmite pachetele spre toate calculatoarele din rețea, atunci pingurile se vor transmite spre calculatorul victimă în număr foarte mare, multiplicând traficul proporţional cu numărul de hosturi din rețea. În această situație, rețeaua care transmite pingurile calculatorului victimă este numită amplificator Smurf.

Tehnicile de apărare contra unui astfel de atac nu au ca scop apărarea victimei, ci a rețelei, ca aceasta să nu fie implicată în atacul Smurf. În acest sens este interzisă transmiterea pachetelor ICMP în afara rețelei, sau se configurează routerele ca să nu permită trecerea pachetelor ICMP.

Similar cu Smurf este atacul Fraggle, care este doar o simplă modificarea a primului menționat, pachetele de date fiind de tip UDP, iar atacul se bazează pe porturile 7 şi 19.

Degradation of Service

Această tehnică folosește computerele Zombie pulsatoare, mai exact acestea transmit Flooduri în anumite intervale de timp, dar nu pentru timp îndelungat. O astfel de metodă este greu de identificat, deoarece este similară cu un trafic mărit. Ceea ce o diferențiază este că ea degradează treptat serverul și poate avea urmări mai grave decât în cazul Flood-ul simplu, conducând la întreruperea conexiunilor cu serverul pe perioade lungi de timp.

Man-in-the-Middle attack (MITM)

În cazul unui atac MITM, hackerul interceptează şi, dacă are nevoie, modifică conținutul mesajelor dintre două computere, determinând cele două victime să considere autentic modul lor de comunicare, în vreme ce întreaga comunicare este dirijată de hacker.

Procedeul este următorul: o victimă îi solicită alteia codul de acces cu care vor codifica comunicările următoare. Hackerul primește codul de acces al celei de-a doua victime, dar celei dintâi îi transmite altceva. În acest fel, cele două victime nu își vor putea transmite, respectiv primi, mesajele reale. Atunci când cele două victime consideră că comunică între ele, în fapt hackerul transformă mesajele dintr-un cod de acces în altul, şi, dacă se impune, schimbă înțelesul mesajului.

Modalitatea prin care se face acest atac este Spoofingului DHCP, și anume: un computer din rețea pretinde că el este serverul DHCP, luând informația despre hosturi de la serverul DHCP real. Dacă hackerul indică computerelor din rețea date greșite, acestea vor avea erori la conectare, iar în cazul în care ca default gateway este indicat un computer al atacatorului din rețea, acel computer poate aplica sniffingul pentru a colecta informații confidențiale transmise de computerele din rețea altor rețele externe. Putem descoperi acest tip de atac folosind programele special realizate pentru aceasta.

Atacul Replay

Prin acest atac sunt trimise mesaje fraudate către o victimă, sub aparenta că ar fi din partea altei persoane. Cel care atacă se poate afla în situația de a intercepta informații confidențiale din rețeaua vizată ca urmare a unui atac de tip sniffing.

De pildă, computerul Alfa dorește să comunice cu computerul Beta, acesta solicitându-i o cale de acces pentru a-i verifica identitatea. Conexiunea poate avea loc numai în cazul în care hashul parolei este același cu cel pe care îl știe computerul Beta. În acest interval de timp, hackerul a colectat acest hash, îl va putea utiliza în viitor cu scopul ca acel computer Beta să considere că în realitate transmite mesaje către computerul Alfa.

Astfel de atacuri pot fi evitate prin utilizarea de jetoane de sesiune, de care se anexează hashul parolei, care depinde de acest jeton, la verificarea identității. Pentru fiecare sesiune, este utilizat alt jeton, care este generat de numere aleatoare.

Cu toate acestea, poate interveni un obstacol, întrucât numerele aleatoare sunt calculate după unele valori care se schimbă în timp, cum ar fi, de pildă, timpul de când e pornit computerul. Prin monitorizarea mai multor legături ale victimelor, hackerul ar putea descoperi algoritmul şi care ar putea fi următoarea valoare la momentul începerii atacului.

DNS Rebiding

DNS Rebiding este întâlnit atunci când victima accesează o pagină web care modifică felul în care browserul accesează siteul folosind serverul DNS. Cu ajutorul codului web java, javascript sau flash atacatorul este în poziţia de a manevra browserul victimei. Această metodă este utilizată frecvent în cazul atacurilor DDoS, mai exact atunci când browserul computerului atacat primește comanda de a ataca un server Web. În acest fel, cei care vor deschide din pură întâmplare pagină web vizată, nu numai că își vor infecta browserul, dar vor ajuta hackerul să atace acel server. Putem evita astfel de atacuri utilizând metode diverse. DNS Pinning, de pildă, este o tehnică prin care se verifică dacă adresa DNS inițială este aceeași ca şi la moment, doar că această metodă produce erori în cazul serverelor DNS dinamice. O altă metodă implică negarea tuturor cererilor HTTP care nu au un header cunoscut al hostului.

DNS cache poisoning

Această tehnică se referă la schimbarea bazei de date cache a serverului DNS, astfel încât acesta va asocia adrese ale siteurilor Web cu IP eronat, redirecționând spre alt site. Hackerul poate redirecționa, de exemplu, către o pagină web ce conține un cal troian, vierme sau un virus, infectând astfel computerul victimei prin intermediul punctelor vulnerabile din serverul DNS. Infectarea serverului DNS are loc cel mai des cu ajutorul exploatărilor sau a utilitarelor special scrise pentru aceasta. De asemenea, există numeroase utilitare, sau implementarea serviciilor Network Address Translation (NAT) şi Port Address Translation (PAT) pentru a preveni astfel de atacuri.

ARP Poisoning

Acest tip de atac este întâlnit în literatura de specialitate ca ARP Flooding sau ARP Poisning Routing (APR). Mecanismul este următorul: hackerul transmite pachete ARP (Address Resolution Protocol) falsificate către utilizatorii rețelei. Pachetul asociază adresa MAC a hackerului cu o adresă IP străină din rețea (de exemplu, a gatewayului).

În aceste condiții, întregul trafic care pretinde să iasă în exteriorul rețelei, va trece nu prin gateway, ci prin computerul hackerului, oferindu-i posibilitatea să inițieze tehnici de atac precum sniffingul rețelei sau Man-in-the-Middle.

DHCP snopping constituie un mod de a ne proteja de acest gen de atac. Prin această modalitate putem afla că este într-adevăr real serverul DHCP prin verificarea adresei MAC.

Atacuri Wireless

Aşa cum undele radio sunt greu de controlat, rețelele Wi-Fi sunt supuse frecvent atacurilor de securitate. Trebuie menționat că atacurile în rețea prin cablu se aplică și în cazul wireless. Diferența constă în faptul că ne confruntăm cu o gamă variată de tehnici a căror particularitate este legată în majoritatea cazurilor de punctele de acces.

Orice computer cu conexiune wireless, va putea intercepta toate pachetele care se transmit în radiusul în care funcționează punctul de acces wireless. Din acest motiv, securitatea în rețele Wi-Fi este extrem de sensibilă, iar prin intermediul tehnicilor de acest tip rețeaua prin cablu poate fi atacată în continuare.

Metoda cea mai simplă de atac wireless este reprezentată de Wireless DeAuth, care nu are ca scop modificarea sau furtul datelor, ci doar delogarea tuturor utilizatorilor din rețea, fără a cunoaşte codul de acces.

Odată cu valorificarea rețelelor wireless de către atacatori, au apărut tehnici de securitate bazate pe coduri de acces. O primă modalitate de împiedicare a accesului neautorizat a fost WEP, dar implica o serie de puncte atacabile folosite de hackeri pentru a exploata rețeaua. WPA este o metodă de apărare mai sigură, pe baza căreia a fost dezvoltat ulterior WPA-2, însă puncte vulnerabile ale acestor metode au fost aflate în cele din urmă de către atacatori. Cisco LEAP este în momentul de față, unul dintre cele mai sigure moduri de apărare a rețelei wireless. Această metodă a corectat punctele slabe ale celorlalte tehnici. Atacurile MITM, DoS sau Replay sunt destul de frecvente pentru rețelele Wi-Fi.

Filtrarea adreselor MAC reprezintă o metodă suplimentară de securitate întrucât doar computerul cu o adresă specifică va putea folosi punctul de acces. Deoarece utilizarea Spoofingului MAC este destul de simplă, astfel e posibil de utilizat aceasta pentru a obține acces neautorizat la rețea. Putem utiliza Spoofingul MAC în Session HighJacking. Aceasta implică Sniffingul rețelei wireless pentru a găsi adresele MAC ale utilizatorilor deja autorizați, şi transformarea adresei proprii în conformitate cu adresa utilizatorului, iar atacatorul se poate folosi de rețea, fiind socotit deja logat la punctul de acces.

Network Injection este o metodă prin care hackerul folosește un punct de acces care nu triază traficul, pentru a reconfigura routerele, switchurile şi huburile inteligente. Astfel, o întreagă rețea poate să cadă, impunându-se repornirea, sau chiar reconfigurarea lor.

Un alt mod de exploatare a rețelei WEP este atacul de tip Caffe Latte. Pentru a-l pune în practică, atacatorul nu trebuie să fie în aria de acoperire a rețelei. El exploatează sistemele Windows, captând informația din stivă şi aflând astfel codul de acces al rețelei wireless. Ceea ce urmează este uşor de intuit: hackerul trimite multe solicitări ARP codificate, şi va putea procura codul de acces folosind inundarea cu aceste pachete.

Scopul final al tehnicilor de securitate a informației constă în apărarea intereselor celor care folosesc şi depind de informații, sisteme şi comunicații care furnizează aceste informații împotriva prejudiciilor apărute ca urmare a imposibilității garantării accesului, confidențialității și integrității datelor.

Ceea ce își propune securitatea informațională să realizeze trebuie hotărât pe baza priorităților constante ale securității naționale care corespund cerințelor de lungă durată ale dezvoltării mediului informațional al societății, incluzând:

- apărarea intereselor naționale ale statului în condițiile globalizării proceselor informaționale şi formării rețelelor informaționale globale;
- asigurarea organelor puterii şi conducerii de stat, persoanelor fizice şi juridice cu informație reală, completă și adecvată, necesară pentru luarea deciziilor;
- prevenirea încălcării integrității resurselor informaționale de stat, utilizării lor ilegitime şi neproductive;
- conştientizarea drepturilor cetățenilor, organizațiilor şi statului în vederea obținerii, propagării și utilizării informației;
- promovarea normelor democratice, în special a principiilor de interacțiune a statului, societății şi persoanei în mediul informațional, în calitate de agenți egali în mod real ai relațiilor democratice; apărarea informațională a cetățenilor.

Trebuie menționat faptul că spațiul cibernetic este într-o continuă creştere şi evoluție, însă odată cu dezvoltarea acestuia se dezvoltă şi pericolele. O preocupare importantă trebuie să fie contracararea atacurilor cibernetice organizate, dispuse să creeze o destabilizare critică a infrastructurii naționale, a apărării sau a economiei naționale. Este cunoscut că disponibilitățile tehnice şi numărul utilizatorilor capabili de provocarea unui adevărat dezastru este în creştere, iar instrumentele şi metodele de realizare a atacurilor sunt tot mai răspândite.

Atacurile cibernetice asupra rețelelor informaționale ale oricărei țări pot avea urmări grave, precum discontinuitatea desfășurării unor procese-cheie, provocarea pierderilor de venituri şi proprietăți intelectuale sau chiar pierderea vieților omenești.

Anihilarea unor astfel de atacuri implică impunerea unor componente stricte, care nu există la momentul actual, dacă se dorește reducerea punctelor vulnerabile şi prevenirea sau diminuarea forței capacităților îndreptate împotriva infrastructurilor critice.

Metodele tradiționale de protecție a informațiilor nu mai sunt eficiente în contextul actual de dezvoltare a sistemelor informaționale, odată cu creşterea cantității de informații vehiculate prin rețelele informaționale, evoluția rapidă a tehnologiilor, şi sporirea numărului de specialişti în domeniul tehnologiilor informaționale, precum şi accesibilitatea echipamentelor performante.

În acest sens observăm în ultimii ani o creştere semnificativă a investițiilor în securitatea cibernetică. Acest lucru se datorează nu numai înmulțirii numărului de atacuri cibernetice asupra instituțiilor, organizațiilor, companiilor atât civile, cât şi a celor din sectorul de apărare, ci şi creşterii considerabile a „calității" atacurilor şi pagubelor materiale şi morale cauzate de către acestea.

Pe cale de consecință, cursa după digitizarea serviciilor publice, automatizarea proceselor, fluxurilor şi informatizarea, fără o atenție adecvată apărării cibernetice, conduce în cele din urmă la expunerea considerabilă a societății informaționale la punctele vulnerabile şi amenințările cibernetice.

În ziua de astăzi, sectorul public este dependent de spațiul cibernetic prin:

- Mpay (sistem de plăți electronice);
- Mpass (platforma ca serviciu);
- MCloud (infrastructura Cloud Computing);
- Semnătura digitală;
- Guvern fără hîrtie -E-government Platforma de registre;
- Portaluri de date guvernamentale (servicii, date) etc.

Potrivit statisticilor pentru anii 2014 și 2015, o parte considerabilă a atacurilor automate au fost lansate din rețelele furnizorilor de servicii tip Cloud.

Cu alte cuvinte, odată cu dezvoltarea rețelelor de acest tip, fără concentrarea atenției asupra problemelor securității acestora, infrastructura Cloud Computing poate deveni o sursă pentru atacuri dacă se află în mâinile persoanelor rău intenționate.

În plus, accesul în masă la Internetul de bandă largă, utilizarea omniprezentă a rețelelor virtuale de socializare, a mijloacelor mobile de bandă largă și accesibilitatea conținutului digital împreună cu o lipsă acută a culturii de securitate cibernetică și utilizarea preponderent a softului piratat (90% din softul instalat) reprezintă o sursă ideală pentru crearea rețelelor botnet.

În anii care vor urma, importanța spațiului cibernetic va determina conștientizarea protecției lui nu numai de către guverne, dar și de către firme private și persoane particulare.

Aceasta va conduce la asocierea utilizatorilor în scopul reducerii vulnerabilităților, combaterii și eradicării amenințărilor îndreptate împotriva spațiului cibernetic. Statul în acest efort trebuie să joace rolul cel mai important.

Avem astfel o viziune puternică a statului în dezvoltarea tehnologiilor informaționale și a comunicațiilor ca unul dintre domeniile critice pentru economia locală, care continuă a produce efecte bune, atât din punct de vedere economic și social, cât și în domeniile unde țara înregistrează cele mai remarcabile succese de pe glob.

Mergând mai departe, țara ar putea beneficia mai mult de consolidarea sistemului de inovare, care, la acest moment, suferă de o serie de deficiențe ce limitează capacitatea de inovare a sectorului privat și de a beneficia, astfel, de întregul potențial pe care tehnologiile informaționale și comunicațiile îl pot oferi.

BIBLIOGRAFIE

1. 2013-2014 DDoS Threat Landscape Report, Incapsula, p. 12;
2. Alyson Bailes Europe's Defense Challenge: Reinventing the Atlantic Alliance;
3. Apărarea cibernetică DELEGAŢIA PERMANENTĂ A ROMÂNIEI la NATO;
4. Christopher Leidigh; Fundamental Principles of Network Security; American Power Conversion, 2005;
5. Cisco 2014. Annual Security Report, p. 80;
6. Detection and Risk Mitigation, TIZOR Mantra, 2007;
7. Detection: A Survey, White Paper, http://www.cs.virginia;
8. ENISA Threat Landscape 2013, Overview of current and emerging cyber-threats, 11 December 2013, p. 70;
9. Florent Parent, Managing Cisco Network Security: Building Rock-Solid Networks, Syngress Publishing, 2000;
10. http://assets.aarp.org/rgcenter/consume/dd142_security_breach.pdf;
11. http://hosteddocs.ittoolbox.com/Tizor021507b.pdf;
12. http://offensive-security.com/metasploit-unleashed;
13. http://www.cert.org/encyc_article/tocencyc.html;
14. http://www.educause.edu/ir/library/pdf/erm05413.pdf;
15. http://www.interhack.net/pubs/network-security/;
16. http://www.sans.org/reading_room/whitepapers/case studies/1103.php
17. https://cybermap.kaspersky.com/;
18. Internet Security Threat Report 2014, Volume 19, Symantec Corporation, p. 24;
19. John E. Canavan; Fundamentals of Network Security; ARTECH HOUSE, 2001;

Adrian Victor VEVERA – este Director Tehnic, Cercetător Științific gradul II și membru în Consiliul Științific al Institutului Național de Cercetare-Dezvoltare în Informatică. Doctor în științe militare și informații, fiind la bază atât jurist cât și inginer specializat în fizică nucleară, deține o vastă experiență în ceea ce înseamnă securitatea națională, ocupând, de-a lungul timpului, numeroase poziții manageriale și de consiliere în diverse organisme ale statului. A publicat numeroase articole și lucrări pe teme de securitate națională și internațională, securitate energetică, criminalitate informatică, protecția infrastructurilor critice și a fost coordonatorul a numeroase proiecte de interes național.

Adrian Victor VEVERA – is a Senior Researcher II, the Technical Director and a member of the Scientific Council of the National Institute for Research and Development in Informatics. Doctor of Military Sciences and Information, being both a lawyer and a nuclear physics engineer, Mr. Vevera has extensive experience in the field of national security, fulfilling various positions, over time, in numerous managerial and counseling positions in different state organisms. He has published numerous articles and papers on national and international security issues, energy security, cybercrime, critical infrastructure protection, and has been the coordinator of numerous projects of national interest.