CAPITOLUL 2

ATACURI ASUPRA DATELOR DIN SISTEMELE INFORMATICE

2.1. Tipologia atacurilor asupra informației din rețelele de calculatoare

Atacurile asupra informației din sistemele de calcul pot lua diferite forme.

O primă clasificare a atacurilor poate fi făcută ținând cont de locul de unde se execută atacul. Distingem două categorii de atacuri: **locale** şi **la distanță** [PATR94].

O a două clasificare poate fi făcută după modul de interacțiune a atacatorului cu informația rezultată în urma unui atac reuşit. Aici se disting două categorii de atacuri: **pasive** şi **active** [PATR94].

2.1.1. Atacuri locale

Atacurile locale urmăresc spargerea securității unei rețele de calculatoare de către o persoană care face parte din personalul angajat al unei firme - *utilizator local*. Aceasta dispune de un cont şi de o parolă care-i dau acces la o parte din resursele sistemului. De asemenea, persoana respectivă poate să aibă cunoştințe despre arhitectura de securitate a firmei şi în acest fel să-i fie mai uşor să lanseze atacuri.

Atacatorul, de la calculatorul propriu, va putea să-şi sporească privilegiile şi în acest fel să acceseze informații la care nu are drept de acces. De pe calculatorul propriu va putea să încarce programe care să scaneze rețeaua şi să găsească punctele vulnerabile. Dacă local îi sunt limitate drepturile de configurare a modului de BOOT-are a sistemului de operare, pentru a nu se putea face încărcarea sistemului de operare de pe dischetă, utilizatorul va putea trece peste aceasta dacă ştie combinațiile secrete de parole CMOS de la producător sau cu ajutorul a patru linii de program scrise în QBASIC care vor reinițializa CMOS-ul, anulând parola:

FOR i=1 to 128; OUT &H 70, 1; OUT &H 71, 0; NEXT i.

Lipsa discului flexibil sau unității CD-ROM cu ajutorul cărora să se poată introduce programe va fi suplinită de programele pe care utilizatorul le va putea procura din Internet. Obținerea de drepturi de *root*, adică drepturile de administrator reprezintă țelul atacatorilor.

2.1.2. Atacuri la distanță

Atacul **la distanță** (remote attack) este un atac lansat împotriva unui calculator despre care atacatorul nu deține nici un fel de control, calculatorul aflându-se la distanță. Calculator la distanță (sau maşină la distanță – remote machine) este orice calculator care poate fi accesat în rețeaua locală sau în Internet – altul decât cel de la care se inițiază atacul.

Prima etapă este una de tatonare. Atacatorul va trebui să identifice:

- cine este administratorul;
- calculatoarele (maşinile din rețea), funcțiile acestora şi serverul de domeniu;
- sistemele de operare folosite;
- punctele de vulnerabilitate;
- diverse informații despre topologia rețelei, construcția şi administrarea acesteia, politici de securitate etc.

Atunci când calculatorul-țintă nu se află în spatele unui firewall, eforturile de atac sunt diminuate.

În funcție de dimensiunea şi arhitectura rețelei în care se află calculatorul-țintă, folosind programe de scanare se pot obține informații despre numele şi adresele IP ale calculatoarelor din domeniu. O interogare *host* va produce un volum foarte mare de informații despre domeniu cu multe calculatoare. O interogare WHOIS va determina dacă ținta este o maşină reală, un nod sau un domeniu virtual. În cazul unor interogări se poate determina şi sistemul de operare de pe calculatorul-țintă, aceasta uşurând considerabil munca.

Dar cea mai mare importanță o are colectarea informației despre administratorul de sistem din care provine ținta. Aceasta va aduce cele mai multe informații utile atacatorului. Dacă se determină când, cum şi cât îi ia administratorului de sistem, sau persoanei însărcinate cu securitatea, să verifice existența eventualelor atacuri, atacatorul va iniția atacurile în afara acestor perioade.

A două etapă este una de testare. Uneori, din nerăbdarea de a obține informația cât mai repede cu putință, această etapă este omisă.

Ea presupune crearea unei clone a țintei şi testarea asupra atacului pentru a se vedea comportamentul. În acest fel, se fac experimente pe un calculator-clonă care nu va atrage atenția. Dacă aceste experimente se fac pe ținta reală, atunci acest lucru poate fi sesizat atacul să eşueze şi atacatorul să fie prins. Răbdarea îşi va arăta roadele.

Etapa a treia presupune efectuarea atacului real asupra țintei. Atacul trebuie să dureze foarte puțin şi să fie efectuat atunci când ținta este mai puțin supravegheată. În urma acestui atac trebuie să se obțină informațiile scontate.

O categorie aparte o reprezintă atacurile care sunt o combinație a celor două. În această situație atacatorul cunoaşte date despre sistemul țintă. Atacantul este ori un fost angajat, ori a intrat în posesia informațiilor referitoare la țintă de la un fost sau actual angajat al firmei. În această situație atacurile au foarte mari sorți de izbândă.

Atacurile pasive au ca scop mai degrabă „vizualizarea“ informației şi mai puțin alterarea şi distrugerea acesteia.

Atacurile active au ca scop furtul, inserarea, alterarea sau distrugerea informației.

2.1.3. Niveluri de atac şi niveluri de răspuns

Securitatea este relativă. Deşi sunt implementate ultimele tehnologii de securitate în cadrul firmei, atacurile pot surveni în orice moment. Dacă atacurile locale pot surveni atunci când atacatorul-angajat al firmei este la serviciu, atacurile la distanță pot să survină în orice moment. Atacurile sunt lansate în aşa fel încât să nu fie detectate. Pentru ca un atac să aibă succes, acesta trebuie să fie eficient, executat cu mare viteză şi în deplină clandestinitate.

Pentru a putea să fie eficient, atacatorul trebuie să folosească instrumente şi tehnici verificate de atac. Folosirea haotică a acestora se poate concretiza în prinderea şi pedepsirea atacatorului.

Viteza este esențială. Atacatorul trebuie să acceseze, să penetreze, să culeagă şi să iasă din calculatorul-țintă, fără să lase urme, în timpul cel mai scurt posibil. Orice fracțiune de secundă în plus pierdută în sistemul-țintă poate fi fatală. Pentru a se asigura o viteză mare, atacatorul va folosi rețeaua atunci când traficul în rețea (inclusiv Internet) este mai scăzut. Sunt şi cazuri când atacurile se execută atunci când calculatorul (serverul) este foarte solicitat, pentru a se masca atacul.

Dacă atacatorul face o greşeală sau personalul însărcinat cu securitatea este foarte bine pregătit, atunci nu numai că atacul eşuează, dar sunt dezvăluite chiar identitatea şi localizarea sursei atacului.

Nivelurile de atac pot fi clasificate în şase mari categorii exemplificate în figura 9 [SECU99].

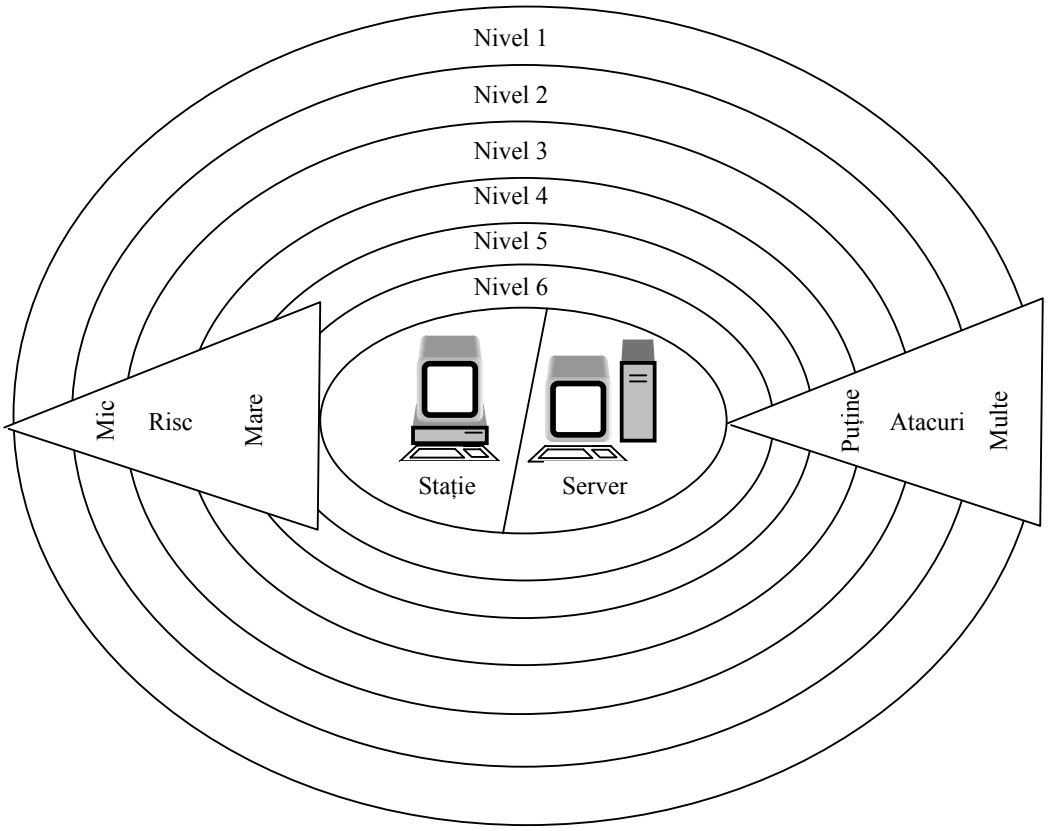


Figura 9. Nivelul de atac.

Nivelul 1:
- atac prin bombe e-mail;
- atac de refuz al serviciului.

Nivelul 2:
- atac prin care utilizatorii locali obțin acces neautorizat pentru citire.

Nivelul 3:
- atac prin care utilizatorii locali obțin acces neautorizat pentru scriere în fişiere în care nu au dreptul;
- utilizatorii de la distanță pot să deschidă sesiuni de lucru neautorizate (login).

Nivelul 4:
- utilizatorii de la distanță pot avea acces la fişiere privilegiate (care conțin conturi şi parole).

Nivelul 5:
- utilizatorii de la distanță pot scrie în fişiere privilegiate – pot crea conturi.

Nivelul 6:
- utilizatorii de la distanță au drepturi de administrator (root) asupra sistemului.

Atacurile de **nivel 1** sunt cele mai dese şi mai lipsite de pericol atacuri. Acestea constau, în principal, din atacuri de refuz al serviciului (denial of service) şi din bombardare cu mesaje e-mail. De regulă produc mai multă enervare decât dezastre.

Dacă atacul este de tip *syn_flood* (inundare cu pachete SYN), se pot lua măsuri de stopare a acestuia. O parte din programele care sunt folosite pentru „inundare“ dezvăluie identitatea atacatorului. Codul acestor programe au la bază instrucțiuni PING care poartă cu ele şi adresa IP a calculatorului care a lansat-o. În acest fel, identitatea atacatorului este dezvăluită. Sau se poate folosi comanda *traceroute* pentru a putea vedea adresa de unde vine atacul. De regulă, aceasta este penultima din lista afişată.

Majoritatea acestor atacuri au un grad redus de risc, dar nu trebuie totuşi ignorate. Ele pot duce la paralizarea traficului din rețea şi chiar stopa funcționarea anumitor calculatoare/ servere.

Atacurile de **nivel 2** şi **nivel 3** sunt efectuate de către utilizatori locali care obțin acces de citire şi scriere în fişiere şi foldere (directoare) unde nu au acces. Nivelul 2 poate fi atins de utilizatorul local dacă acesta are acces la fişiere sau foldere. Dacă reuşeşte să-şi creeze drepturi şi de scriere atunci atinge nivelul 3. Aceste situații apar cu precădere la sistemele de operare UNIX, Linux, Windows. Problemele cele mai mari le are sistemul de operare Windows la versiunile 95, 98, Me. Atacurile de nivel 2 sunt foarte dese la acestea, ele putând uşor să ajungă până la nivelurile 6. Acest lucru poate fi suplinit prin programe suplimentare de control al accesului. Chiar şi la sistemele de operare unde accesul este controlat pot să apară probleme cauzate de configurările greşite din partea administratorului de sistem sau de vulnerabilitățile interne ale programelor utilizate. O configurare optimă, cu şanse foarte mici de vulnerabilitate, va putea fi făcută numai de persoane specializate pe domeniu.

Atacurile de **nivel 4** sunt executate de persoane din exteriorul firmei care au acces la informația din interiorul firmei. Aceşti utilizatori pot să citească atât existența unor fişiere, cât şi să citească conținutul acestora. În acest fel atacatorul va putea avea acces limitat la anumite informații de pe serverul sau serverele firmei, chiar dacă nu are conturi valide. Acest lucru este posibil din cauza configurării greşite a serverelor, a unor programe CGI slab concepute sau a unor probleme de depăşire (overflow).

Atacurile de **nivel 5** şi **nivel 6** sunt cele mai grave, uneori aceste atacuri devenind fatale. Aceste atacuri sunt posibile doar dacă nu au fost luate măsuri pentru stoparea atacurilor de niveluri inferioare sau din erori de programare.

Răspunsurile la atacurile de nivel 1 sunt relativ simple şi uşor de implementat. Bombardarea e-mail poate fi uşor contracarată prin configurarea de filtre de exclusivitate care fac ca atacurile să fie fără succes. Atacurile de refuz al serviciului vor putea fi contracarate prin blocarea traficului acestuia. Dacă atacurile continuă sau sunt doar o parte a unui atac combinat, atunci se poate merge până la contactarea furnizorului de servicii al atacatorului sau la alertarea autorităților.

Răspunsurile la atacurile de nivel 2 se pot rezolva prin acoperirea golurilor de securitate în sistemele de operare şi prin configurarea optimă, de către specialişti, a sistemului. De asemenea, se pot lua şi măsuri administrative împotriva celor care îşi depăşesc atribuțiile.

Răspunsurile la atacurile care depăşesc nivelul 2 sunt mult mai complexe şi trebuie tratate cu foarte mare responsabilitate. Dacă celelalte atacuri erau, poate, întâmplătoare sau erau opera unor începători în domeniu, acestea sunt executate de specialişti şi pot produce consecințe grave.

În cazul unor astfel de atacuri trebuie luate următoarele măsuri:

- restrângerea ariei de desfăşurare a atacului prin izolarea porțiunii de rețea supusă atacului;
- urmărirea evoluției atacului;
- înregistrarea evidențelor referitoare la atac;

- identificarea sursei atacului;
- identificarea utilizatorului.

Pentru a se realiza aceste măsuri se poate cere ajutorul unor firme specializate în domeniu. De asemenea, se poate cere şi sprijinul autorităţilor în prinderea autorului care de multe ori este foarte laborioasă sau, deşi se identifică autorul, să nu poate să fie pus sub acuzare pentru că se află în altă ţară, unde nu există legi care să pedepsească astfel de activităţi.

2.2. Tehnici şi instrumente de atac asupra datelor

2.2.1. O posibilă tipologie a programelor malițioase

Viruşii informatici reprezintă una dintre cele mai evidente şi mai prezente ameninţări la adresa securităţii datelor din cadrul firmelor şi care necesită luarea de măsuri imediate. Detectarea viruşilor informatici şi anihilarea acestora reprezintă prima cerinţă în asigurarea securităţii calculatoarelor. Termenul de virus informatic este atât de bine cunoscut ca termen încât atunci când se face referire la acesta se foloseşte doar denumirea de **virus**. În multe cazuri se face însă confuzie între diferitele tipuri de programe malițioase, numindu-le pe toate virus.

Pe ansamblu, numai în anul 2001, rata infecţiilor cu viruşi, conform ICSA Labs[38] (www.icslabs.com), a fost de 113 infecţii la 1000 de calculatoare. Aceasta înseamnă că cel puţin 10% din calculatoare au fost infectate cu viruşi. Conform aceleiaşi surse, rata de infectare s-a dublat la fiecare an în ultimii cinci ani. Sondajele făcute de ICSA Labs pe un număr de 300 de firme arătau că dacă la sfârşitul anului 2002 fuseseră afectate serios de viruşi 80 de firme, în anul 2003 numărul acestora a crescut la 90. Cheltuielile pentru refacere au crescut de la 81.000 dolari în anul 2002 la 100.000 dolari în anul 2003. Acelaşi raport arăta că în anul 2003 viermele MSBlast (cunoscut şi sub denumirea de Blaster) a afectat 130.000 de calculatoare dintr-un număr de 960.000 supuse testului. Mai mult de 80% din daunele provocate de viruşi au implicat şi serverele firmelor. Viruşii au reuşit să scoată din funcţiune serverele pentru o perioadă de 17 ore. Firma McAffee (www.mcafee.com), specializată în produse antivirus, estimează că două treimi din companiile americane au fost afectate de viruşi în fiecare an. Viruşii au reuşit să scoată din funcţiune serverele pentru o medie de 5,8 ore pentru fiecare infecţie. Refacerea sistemelor a necesitat pentru 45% din companii o perioadă de cel puţin 19 zile.

Refacerea sistemelor în urma incidentelor a creat cheltuieli uriaşe. Computer Economics (www.computereconomics.com) estimează că s-au cheltuit numai în anul 2001 10,7 miliarde de dolari pentru repunerea sistemelor în funcţiune. Alte surse – revista The Industry Standard (www.thestandard.com) – estimează cheltuielile la 266 miliarde dolari. Indiferent care ar fi datele exacte, este clar că este nevoie să se cheltuiască bani şi timp pentru detectarea, eliminarea viruşilor, precum şi pentru refacerea datelor afectate.

Individual, fiecare virus a adus aportul său la aceste sume. Dacă primul virus, Giant Worm, producea, la 2 noiembrie 1988, pagube estimate între un milion şi 100 milioane de dolari, urmaşii acestuia făceau ca aceste sume să crească. Conform cu Computer Economics, virusul Nimda a costat firmele 590 milioane de dolari; viruşii CodeReed şi LoveLetter au costat fiecare în jur de 2,6 miliarde dolari. La nivelul firmelor mari s-au cheltuit sume între 100 mii şi un milion de dolari pe an pentru fiecare infecţie cu viruşi. În februarie 2004 se raportau 65.000 de viruşi. Cu alte cuvinte, o firmă poate fi atacată de 65.000 de ori.

[38] *ICSA Labs* este subsidiară a firmei *TruSecure*.

Noţiunea de virus informatic este generală. Aceasta descrie un număr de diferite tipuri de atac asupra calculatoarelor. **Un virus reprezintă un cod maliţios de program care se autocopiază în alte programe şi pe care le modifică**. Un cod maliţios va lansa în execuţie operaţii care vor avea efect asupra securităţii datelor din calculator. Un cod maliţios mai este întâlnit şi sub denumirea de *cale de atac*, *program vagabond*, *vandalizator*. Codul maliţios va contribui la identificarea virusului creând aşa-numita „semnătură" a virusului.

→ *Pentru că existenţa unui cod maliţios în sistemele de calcul are acţiune diferită prin însăşi construcţia codului, este de preferat ca atunci când facem referire la aceste „programe" maliţioase să se ţină cont de gruparea acestora în următoarele categorii:*

- *viruşi;*
- *viermi;*
- *Cai Troieni;*
- *bombe;*
- *căi ascunse (Trap Doors / Back Doors);*
- *spoofer-e;*
- *hoax (păcăleli);*
- *alte tipuri de programe maliţioase.*

Un program maliţios poate să aibă, şi sunt foarte multe astfel de cazuri, comportamentul mai multor programe maliţioase (viruşi). În această categorie se înscriu viruşii *hibrizi.* Datorită acestui comportament este greu de definit cărei categorii îi aparţin aceştia. În lucrare o să întâlnim acelaşi program maliţios care are comportamente multiple.

Un **virus** este un fragment de cod program care se autocopiază într-un mare număr de programe şi pe care le modifică. Un virus nu este un program independent. Un virus îşi execută codul program numai atunci când programul gazdă, în care se depune, este lansat în execuţie. Virusul se poate reproduce imediat, infectând alte programe, sau poate aştepta, în funcţie de cum a fost programat, o anumită dată sau un eveniment la care să se multiplice. Virusul Vineri 13 (Friday 13th virus) se lansa în execuţie la orice zi din an care era vineri şi avea numărul 13.

Un virus va infecta discul flexibil, discul dur, CD-ROM-ul, casetele şi benzile magnetice şi memoria internă. De aici se poate răspândi cu ajutorul suporturilor de memorie portabile (disc flexibil, CD-ROM, casete şi benzi magnetice, pen sau flash drive-uri), conexiune la reţea şi modem. Foarte mulţi viruşi s-au răspândit cu ajutorul discurilor flexibile.

Între viruşi şi viermi (alt program maliţios) se nasc uneori confuzii. Viruşii sunt consideraţi distructivi, iar viermii nedistructivi. Un virus alterează sau distruge datele din calculatorul infectat, în timp ce un vierme afectează buna funcţionare a calculatorului.

Un **vierme** este un program independent. El se reproduce prin autocopierea de la un calculator la altul prin intermediul reţelei în cele mai multe cazuri. Spre deosebire de virus, un vierme nu alterează sau distruge datele din calculator, dar poate crea disfuncţionalităţi în reţea prin utilizarea resurselor acesteia pentru autoreproducere.

Noţiunea de vierme informatic a fost introdusă pentru prima dată în anul 1975 de către scriitorul de literatură science fiction John Brunner în cartea The Shockwave Rider. Autorul descrie un program cu numele „tapeworm" care „trăieşte" în interiorul computerelor, se multiplică de la calculator la calculator atâta timp cât există o conexiune la reţea[39].

John Schoch şi Joh Hupp, cercetători la Xerox Palo Alto Research Center, dezvoltă la începutul anilor '80 primul program experimental de tip vierme. Acest program era destinat să se multiplice de la un calculator la altul. Cei doi cercetători descriau viermele în felul următor: „Un vierme este un program care se găseşte într-unul sau mai multe calculatoare... Programul dintr-un calculator poate fi descris ca un segment al viermelui... Segmentele viermelui rămân

[39] John Brunner*, The Shockwave Rider*, Ballantine, New York (NY), 1975.

în comunicare unele cu altele; dacă un segment al viermelui moare, segmentele rămase trebuie să găsească un alt calculator, să-l iniţializeze şi să-i ataşeze un vierme. Pe măsură ce segmentele se unesc şi apoi părăsesc calculatorul, viermele pare că se mută prin reţea".

Un **Cal Troian** (uneori se foloseşte denumirea de **troian**) este un fragment de cod care se ascunde în interiorul unui program şi care va executa o operaţie ascunsă. Un Cal Troian reprezintă cel mai utilizat mecanism pentru a disimula un virus sau un vierme.

Ideea folosirii de astfel de programe vine din mitologie. În timpul războiului Troian, grecii, sub conducerea lui Odiseu, au atacat fără succes cetatea Troia. Atunci, aceştia au construit un cal mare din lemn în care au introdus soldaţi greci şi pe care l-au lăsat în dar la poarta cetăţii. Troienii au adus „darul" în cetate. Noaptea grecii au ieşit din cal şi au deschis porţile pentru ceilalţi soldaţi care au cucerit cetatea.

Un Cal Troian se va ascunde într-un program cunoscut sau o funcţie apelabilă, care nu creează suspiciuni utilizatorului, dar care va lansa alte operaţii ilegale. Utilizatorul poate să lanseze în execuţie un program aparent inofensiv, dar care are încorporat în el un cod neautorizat. Funcţiile neautorizate realizate de codul program inclus pot să lanseze un virus sau un vierme.

Termenul de „Cal Troian"(Troian Horse)[40] a fost folosit pentru prima dată de Dan Eduards de la NSA.

Cazul clasic de atac cu un Cal Troian este descris de Dennis M. Ritchie[41]. Un atacator va crea un program care capturează parolele (password grabber). Acesta va afişa pe ecranul terminalului prompterul: **login:.** O dată introduse contul şi parola, acestea sunt preluate de programul care conţine Calul Troian şi copiate sau trimise la o destinaţie de unde vor putea fi citite. Pe ecran se afişează mesajul **login incorrect**. În timp ce utilizatorul, crezând că a introdus greşit contul sau parola, reintroduce combinaţia ştiută, programul care conţine calul Troian se opreşte din execuţie şi urmele sunt şterse. În acest fel au fost capturate contul şi parola utilizatorului fără ca acesta să bănuiască ceva.

Există o categorie specială de troieni care sunt creaţi ca instrumente de distrugere. În această categorie se include Calul Troian PC Cyborg. Acesta se disimulează într-un program care oferă informaţii despre virusul informatic AIDS. După ce se instalează în sistem, modifică fişierul AUTOEXEC.BAT şi va contoriza de câte ori se porneşte sistemul infectat. După un număr predefinit de porniri, de regulă 90, troianul ascunde directoarele şi criptează numele fişierelor de pe disc. Un alt tip de troian, distribuit prin reţeaua Usenet şi prin e-mail, denumit AOLGOLD, va instala dintr-o arhivă un program care se vrea o îmbunătăţire a Usenet, dar care de fapt va şterge de pe discul dur o serie de directoare, printre care:
C:\dos; C:\windows; C:\windows\system.

Există cai troieni care nu lasă urme ale prezenţei lor, nu creează distrugeri detectabile, pot să stea nelimitat în programe şi pot să se autodistrugă înainte de a fi detectaţi.

O **bombă** este un tip de Cal Troian folosit cu scopul de a lansa un virus, un vierme sau un alt tip de atac. O bombă poate fi un program independent sau o bucată de cod care va fi instalată de un programator. O bombă se va activa la o anumită dată sau atunci când anumite condiţii sunt îndeplinite.

Tehnic, există două tipuri de bombe: *de timp* şi *logice*. O bombă de timp se va activa atunci când se scurge o anumită perioada de timp de la instalare sau când se atinge o anumită dată calendaristică. O bombă logică va acţiona atunci când se îndeplinesc anumite condiţii impuse de cel care a creat-o.

---

[40] Morie Gasser, *„Building a Secure Computer System"*, New York (NY), Van Nostrand Reinold, 1988. Donn B. Parker, *„The Troian Horse Virus and Other Crimoids"*, ACM Press, Adisson Wesley, Reading (MA), 1990.
[41] Denis M. Ritchie, *„On the Security of UNIX"*, *UNIX Manager Manual*, 4.3 BSD, University of California, Berkeley (CA), 1986.

Căile ascunse (Trap Doors) sunt mecanisme care sunt create de către proiectanții de software pentru a putea să pătrundă în sistemul de calcul ocolind sistemele de protecție. Aceste puncte de intrare în sistem sunt lăsate intenționat de proiectanți pentru a putea să testeze şi monitorizeze programele sau în caz de refuz al accesului să poată să depaneze subrutina de acces. Trap doors-urile sunt folosite în perioada de testare şi apoi sunt eliminate când programul este livrat către utilizator. Acestea sunt eliminate în totalitate sau parțial, după caz.

În mod normal, un punct de intrare de tip Trap Door este activat de către persoana care l-a creat. Sunt însă şi cazuri când aceste puncte sunt descoperite şi exploatate de persoane răuvoitoare.

Căi ascunse (Back Doors) se pot crea cu ajutorul cailor Troieni. Mecanismul presupune introducerea în calculatorul-țintă a unui program care ulterior să deschidă căi de acces către resursele acestuia. Caii Troieni sunt cei mai folosiți pentru atingerea acestor scopuri.

Spoofer-ele reprezintă un nume generic dat unor programe care permit unui utilizator, folosind anumite şiretlicuri, să aibă acces la informațiile din sistem. De regulă, spoofer-ele, sunt posibile cu ajutorul mecanismelor Cal Troian care vor activa programe care dau acces la informații.

Hoax (păcălelile) sunt mesaje trimise prin e-mail care conțin avertizări false despre un virus existent şi care cer să fie avertizate toate persoanele cunoscute. Uneori aceste avertizări conțin şi fişiere ataşate care sunt menite, chipurile, să stopeze sau să elimine presupusul virus. Retrimiterea mesajului la alte destinații face ca virusul să se multiplice fără ca cel care l-a creat să-l proiecteze să se multiplice.

După cum se constată, nu orice program malițios este virus. Dacă vrem să fim riguroşi nu trebuie să mai punem laolaltă toate programele, sau codurile de program, care produc pagube.

Pe lângă aceste secvențe de cod malițios care pot afecta securitatea sistemelor de calcul se mai întâlnesc şi:

- bacterii;
- şobolani;
- crabi;
- târâtoare;
- feliatoare de salam.

Bacteriile sunt programe care nu creează daune, dar care prin simplă copiere a lor pot să încetinească performanțele sistemului. Acesta se pot multiplică în memoria internă sau externă şi să se ajungă la o limitare a spațiului.

Şobolanii reprezintă o categorie aparte de programe care se reproduc foarte repede.

Crabii atacă cu predilecție monitoarele sistemelor de calcul. Imaginile pe ecranul monitorului vor fi trunchiate sau ilizibile. Acestea nu produc distrugeri. Se cunosc însă şi situații când aceste programe distrug fizic echipamentele de calcul.

Târâtoarele au aceiaşi structură şi acelaşi comportament ca şi viermii.

Feliatoarele „taie“ porțiuni mici din date. Un atac de tip *salami slice* va altera una sau două poziții zecimale dintr-un fişier. De exemplu, un astfel de atac va trunchia prin rotunjire în minus un număr de poziții zecimale din suma salarială a unui angajat. Diferența, ca sumă, va fi depusă într-un cont al intruderului.

Pentru că toate aceste „programe“ se comportă aparent ca un virus biologic, au primit denumirea generică de virus informatic.

Ca şi virusul biologic, virusul informatic are nevoie de o gazdă pentru a putea să infecteze, să se reproducă, să se răspândească. Aceasta gazdă este formată din informația stocată pe suporturile de memorie. Majoritatea viruşilor infectează fişiere program, din această cauză poartă şi denumirea de *virus de fişiere*. Atunci când acest fişier, purtător de virus, este lansat în execuție de un utilizator care nu ştie de existența infecției, codul malițios

este autoîncărcat în memoria internă a calculatorului, este executat codul, se caută apoi un alt fişier care să fie infectat şi se autocopiază în acesta. Acţiunea unui virus informatic este reprezentată schematic în figura următoare (figura 10).

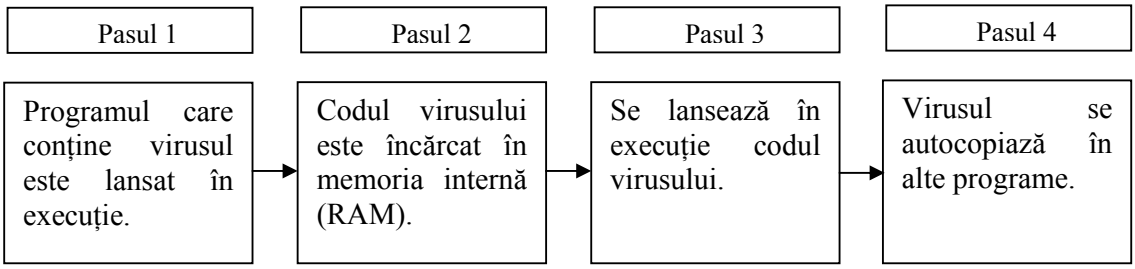


Figura 10. Modul de acţiune al unui virus informatic.

Conceptul de **virus informatic** a fost introdus pentru prima dată în anul 1949 de către pionierul calculatoarelor John von Newmann în articolul „Theory and Organization of Complicated Automata". Conform articolului respectiv, autorul iniţia ideea de program auto-multiplicator. Ulterior, ideea a fost preluată, în anul 1950, la Bell Labs, care a fost încorporată în jocul pe calculator denumit „Core War". În acest joc, participanţii lansau „organisme" în calculatorul mainframe şi încercau să preia controlul acestuia.

Definiţia de *virus informatic* avea să fie dată mai târziu, în anul 1983, de către programatorul Len Adleman, care a făcut un experiment pe un calculator VAX 11/750 demonstrând funcţionarea unui virus.

Ca şi omologul său biologic, virusul informatic are şi el un ciclu de viaţă. Acest ciclu de viaţă depinde de mai mulţi factori, printre care: agresivitatea virusului, modalitatea de disimulare a acestuia, detectarea acestuia, conceperea antidotului şi acţiunea acestuia. Ca şi în viaţă reală, informarea corectă a populaţiei are un mare aport la eradicarea acestuia şi limitarea dezastrelor.

Ciclul de viaţă al unui virus este exemplificat în figura 11:

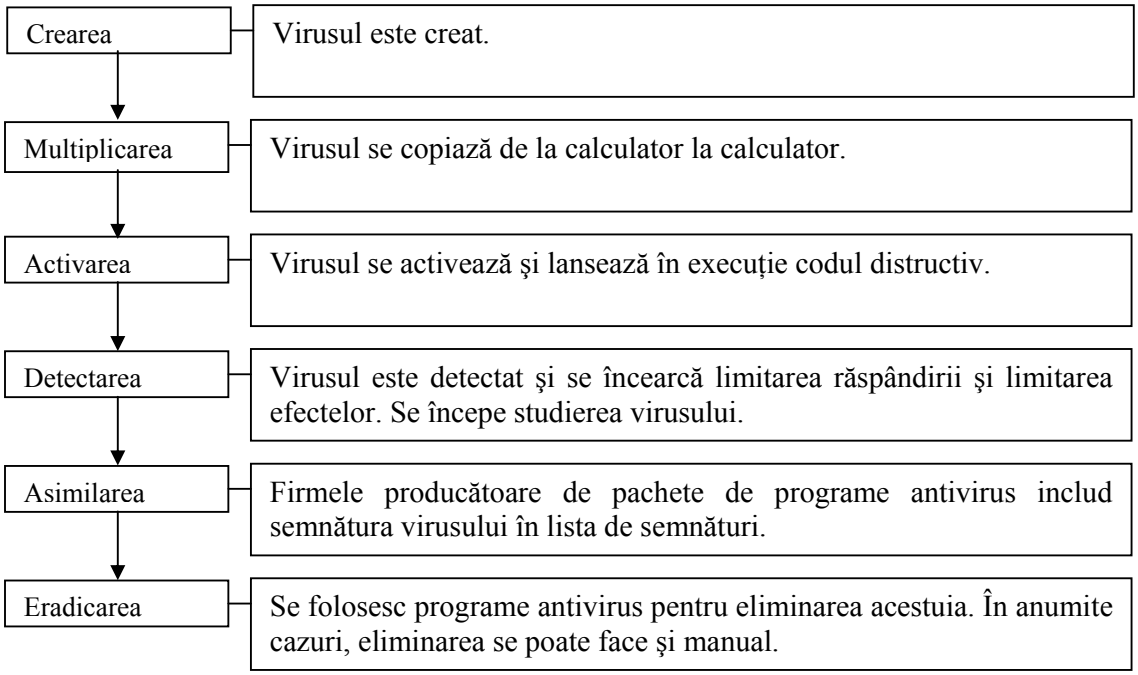


Figura 11. Ciclul de viaţă al unui virus.

Eforturile depuse pentru detectare, documentare şi eradicare se concretizează în cheltuieli financiare care uneori pot fi foarte mari pentru anumite firme. În anumite cazuri nu se mai poate face nimic. Virusul şi-a lansat codul distructiv şi s-a multiplicat fără să fie detectat, iar datele nu mai pot fi recuperate. Fiecare virus poate să creeze un număr mai mare sau mai mic de incidente. De asemenea, un virus, poate să creeze pagube mai mari sau mai mici. De regulă, cu cât sunt infectate mai multe calculatoare, cu atât pagubele sunt mai mari. Există viruşi care au un grad de apariţie mic, dar care produc dezastre mari, precum şi viruşi care au un grad de apariţie mare, dar produc dezastre mici.

Firma TrueSecure (www.trusecure.com) raporta o creştere cu 24% a numărului de viruşi la sfârşitul anului 2003 faţă de începutul aceluiaşi an. Apariţia de noi viruşi la începutul şi sfârşitul anului 2003, precum şi evoluţia acestora pe tipuri este exemplificata în tabelul 5.

Tabelul 5. Evoluţia numărului de viruşi nou-apăruţi în anul 2003.

Tip	Număr de viruşi nou-apăruţi				Schimbări
	Început 2003		Sfârşit 2003		
	Număr	%	Număr	%	%
Boot sector	10	5	9	4	-10
Script	16	8	14	5	-13
Win32(PE)	101	49	157	62	+55
Win95	11	5	12	5	+09
Macro	67	33	63	24	-6
Total	**205**	**100**	**255**	**100**	**24**

Sursa: TruSecure ICSA Labs

Ca mod de propagare (vector de propagare), studiul TruSecure ICSA Labs evidenţiază următoarele (tabelul 6):

Tabelul 6. Moduri de propagare şi evoluţia răspândirii viruşilor în anul 2003.

Mod de propagare	Număr de viruşi nou-apăruţi		Schimbări
	Început 2003	Sfârşit 2003	%
Internet worms	10	30	+200
Mass-mailers	80	98	+23
Mailers	9	17	+89
Network Shares	41	79	+93
P2P (KaZaA)	9	21	+133
AVKill	20	35	+75
DDOS	3	15	+400
Bot-Net	2	9	+350
Self Updating	11	25	+127
Spoofed email	10	18	+80
BackDoor	18	38	+111
Instant Messenger	7	12	+71

Sursa: TruSecure ICSA Labs

Viermii internet (Internet Worms) în mod uzual caută o nouă gazdă şi exploatează golurile de securitate cunoscute. Exemplele cele mai cunoscute de acest tip de viermi sunt variante de Blaster, Nachi (Welchia), şi variante de OpaServ.

Viruşii de e-mail care exploatează vulnerabilităţile programelor de poştă electronică cum ar fi Outlook şi Outlook Express, permiţând culegerea de adrese şi trimiterea de mesaje

virusate la aceste adrese, formează acea categorie de e-mail-uri numite **mass-mailers**. În ultima vreme, aceste mesaje care par a veni de la un prieten continuau să atace cu precădere utilizatorii individuali mai mult decât firmele.

Se observă o creştere a numărului viruşilor de e-mail în ultimul an. Viruşii de e-mail standard diferă de cei mass-mail prin faptul că nu provin dintr-o sursă „cunoscută", nu includ propriul motor de mail şi nu îngreunează traficul de e-mail aşa de mult.

Cea mai comună cale de propagare a unui virus în cadrul firmei este aceea prin partajarea (share) reţelei. O persoană cu drepturi de administrator va putea să iniţieze un atac foarte virulent folosind opţiunea share a reţelei.

Conexiunile de tip P2P (point to point), care numără 3 milioane de utilizatori, fac să se răspândească foarte mult numărul de viruşi prin schimburile de fişiere virusate între utilizatori.

În ultima vreme se observă o creştere a numărului viruşilor care au posibilitatea de a dezafecta şi chiar de a şterge din calculator programele antivirus. Aceste programe, purtătoare de viruşi, poartă denumirea de AVKill (distrugătoare de antiviruşi). Trebuie amintit aici efectul distrugător al diferitelor variante ale virusului W32/Yaha.

Distributed Denial of Service (DDoS) se folosea de tehnologia client-server pentru a concentra atacul asupra anumitor puncte. Firma Microsoft a fost în ultimul timp ţinta unor astfel de atacuri.

Bot-Net se foloseşte de canale IRC pentru a accesa şi a prelua controlul asupra calculatorului ţintă de unde se pot iniţia atacuri şi de unde se pot prelua informaţii.

Viruşii care se autoactualizează (self-updating) dispun de instrucţiuni care verifică site-urile Web sau grupurile usenet pentru a instala noi facilităţi sau pentru a evita detectarea acestora de către programele antivirus.

Tehnica spoofed-email imită adresa de e-mail a unei persoane şi trimite mesaje virusate ca şi cum ar fi de la acea persoană. Mesajele trimise sunt interceptate de programele antivirus care vor trimite mesaje de avertizare periodice către destinatarul real. Acest lucru va avea ca efect aglomerarea cu mesaje inutile şi alarmarea fără motiv a destinatarului care crede că are un virus pe calculator. Un exemplu de acest fel este W32/SoBig.

Numărul de viruşi care include şi Back Door a crescut semnificativ în anul 2003. Unii dintre aceştia permit ca atacatorul să aibă control total asupra calculatorului virusat.

Folosirea largă a programelor de IM fac ca viruşii să se folosească de acestea pentru o răpândire rapidă.

Cele mai exploatate vulnerabilităţi de către viruşi pe parcursul anului 2003 sunt exemplificate în tabelul următor (tabelul 7):

Tabelul 7. Cele mai exploatate vulnerabilităţi în anul 2003.

Numărul de viruşi	**Codul vulnerabilităţii exploatate**	**Numele vulnerabilităţii exploatate**
28	MS01-020	Header MIME incorect poate cauza ca Internet Explorer să execute ataşamentul de e-mail
16	MS00-072	Share Level Passord
6	MS03-026	Eroarea de tip Buffer Overrun în interfaţă RPC poate activa lansarea codului
3	MS99-032	Scriptlet.typelib/eyedog
2	MS00-075	Microsoft VM ActiveX Component
1	MS99-042	IFRAME ExecCommand
1	MS00-043	Header e-mail trunchiat
1	MS00-046	Cache Bypass
1	MS03-007	Uncheched Buffer în Windows Component

Sursa: TruSecure ICSA Labs.

MS01-020: Header MIME incorect poate cauza ca Internet Explorer să execute ataşamentul de e-mail. Viruşii utilizează această vulnerabilitate deoarece Internet Explorer va lansa în execuție automat ataşamentele de e-mail atunci când sunt afişate mesajele. Virusul W32/Klez.H-mm, care exploatează această vulnerabilitate, a fost cel mai raportat în anul 2003.

MS00-072: Share Level Passord. Este o vulnerabilitate prezentă în sistemele de operare Microsoft Windows 9x/Me care permite viermilor să se autocopieze în toată rețeaua la calculatoarele care nu au această vulnerabilitate acoperită.

MS03-026: eroarea de tip Buffer Overrun în interfață RPC poate activa lansarea codului. Această eroare este exploatată de Blaster şi Nachi, care vor rula propriul cod cu facilități privilegiate pe calculatorul infectat.

Se observă că cele mai exploatate vulnerabilități în anul 2003 aparțin producătorului Microsoft. De unde şi codul vulnerabilității – MSxx-xxx.

Pierderile anuale cauzate de viruşi ating valori de ordinul zecilor de milioane de dolari. Conform cu Computer Security Institute, CSI/FBI Computer Crime and Security Survey, pierderile anuale din cauza viruşilor informaticii se ridică în anul 2003 la 27 milioane de dolari, în scădere cu 45% (1,8 ori) față de anul precedent şi la un nivel mai scăzut chiar şi decât anul 2000 (tabelul 8).

Tabelul 8. Pierderile anuale cauzate de viruşi pe ultimii patru ani.

	Valoare pierderi anuale (milioane de dolari)			
Anul	2000	2001	2002	2003
Valoare pierdere	29	45	50	27

2.2.2. Categorii de viruşi informatici şi modul lor de acțiune

Programele malițioase (coduri malițioase) cu comportament de **viruşi** „standard“ pot fi grupate în mai multe categorii, în funcție de „gazda“ purtătoare. Întâlnim viruşii de:

- fişier;
- boot;
- macro;
- script;
- e-mail;
- Chat şi Instant Messaging;
- Hoax (păcăleală).

Viruşii de fişier reprezintă cea mai răspândită categorie de viruşi. Aceştia sunt şi cei mai distructivi. Viruşii de fişier, numiți uneori şi viruşi de program, îşi depun codul malițios într-un fişier program. Când programul respectiv este lansat în execuție virusul se copiază în memoria internă a sistemului de calcul şi îşi lansează în execuție propriul program de distrugere şi de autocopiere. Trebuie să facem o distincție între viruşii de fişier care afectează fişierele executabile şi viruşii de macro care afectează fişierele de tip document. Viruşii de fişiere şi-au făcut apariția în anul 1987, o dată cu descoperirea la Universitatea Ebraică din Israel a virusului Jerusalem (Ierusalim).

Funcţionarea unui virus de fişier este exemplificată în figura 12:

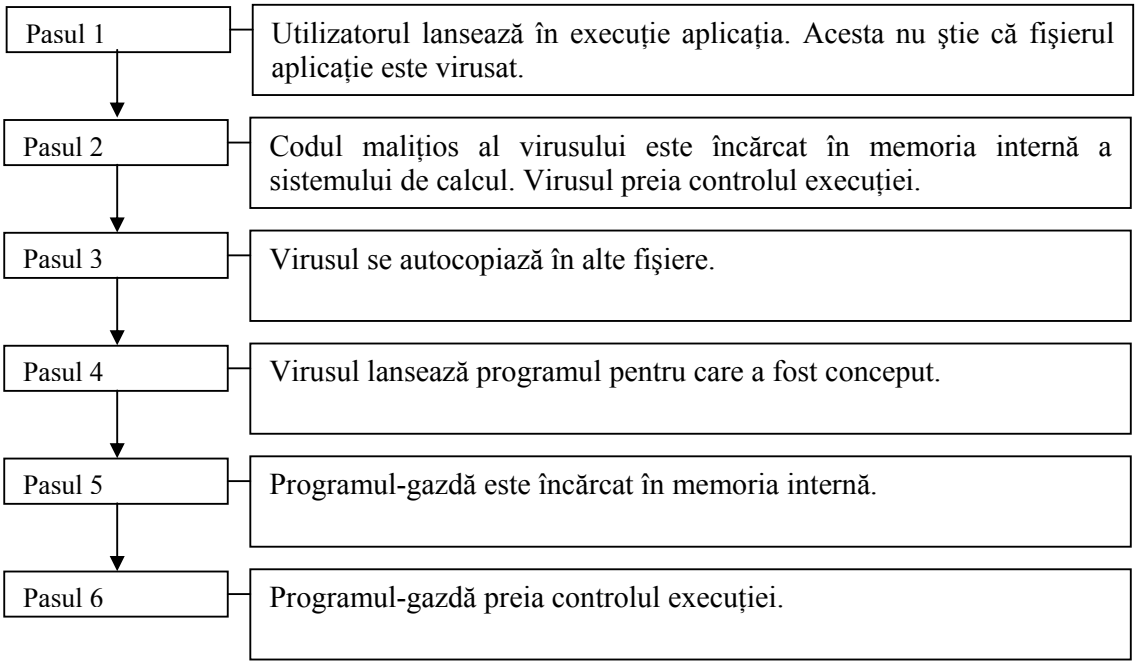


Figura 12. Modul de funcţionare al unui virus de fişier.

Infectarea fişierului-gazdă cu virus poate fi făcută în trei moduri distincte:

- prin suprascrierea la începutul programului-gazdă;
- prin salt la sfârşitul programului-gazdă;
- prin suprascrierea datelor rezultate în urma execuţiei programului-gazdă.

Virusarea prin suprascrierea la începutul programului-gazdă nu este prea des folosită deoarece, în acest fel, programul-gazdă va funcţiona anormal pentru că, după ce se termină secvenţa de cod a virusului inserat, se va trece la execuţia programului-gazdă dintr-o secvenţă care poate să ducă la blocarea execuţiei şi la crearea de suspiciuni referitoare la buna funcţionare a calculatorului.

Acest mod de infectare este exemplificat în figura 13.

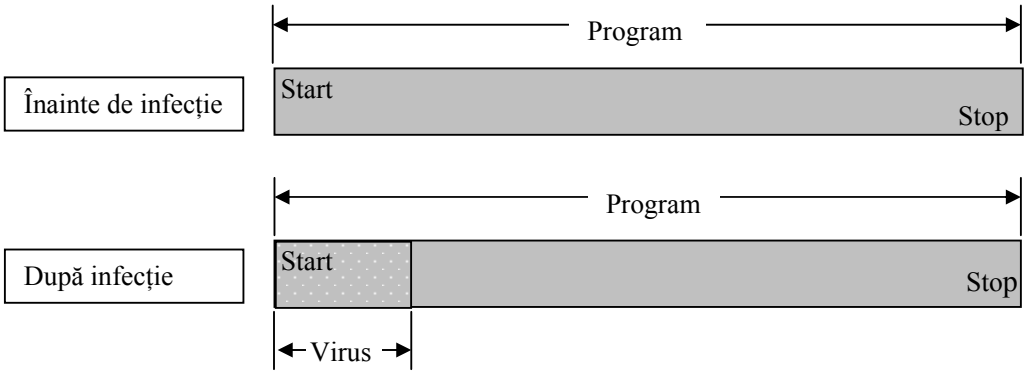


Figura 13. Virusarea prin suprascrierea la începutul programului-gazdă.

Virusarea prin salt la sfârşitul programului-gazdă presupune ca la începutul fişierului-gazdă să existe o instrucţiune de salt necondiţionat la sfârşitul fişierului unde este ataşat codul maliţios al virusului. După ce se execută codul virusului se face un salt înapoi la începutul

programului-gazdă. În acest fel, programul-gazdă va funcţiona fără să se blocheze. Se observă însă, în acest caz, o mărire a dimensiunii fişierului-gazdă (figura 14).

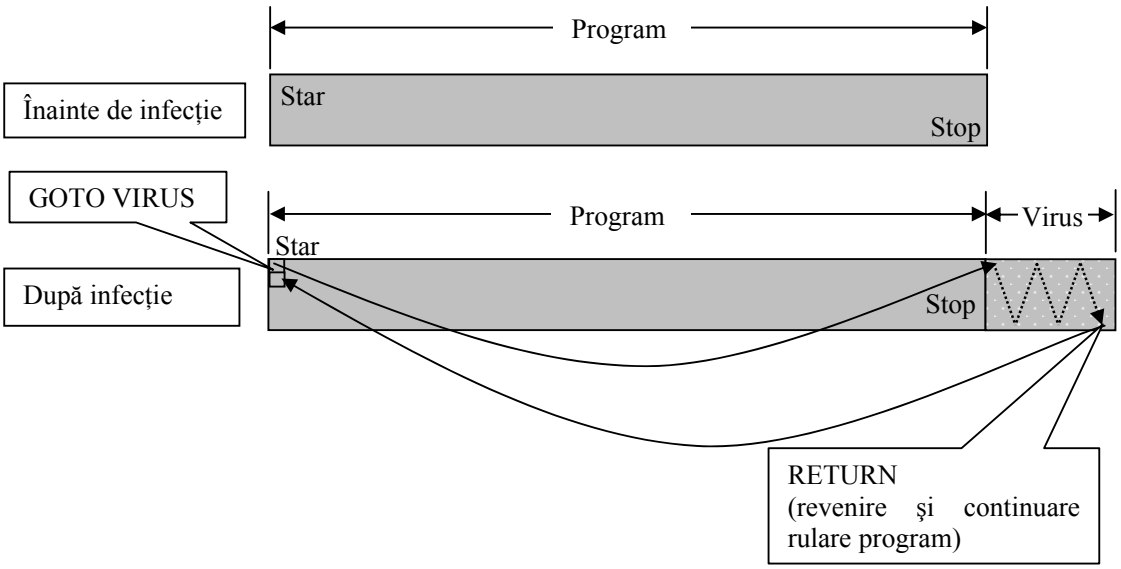


Figura 14. Virusarea prin salt la sfârşitul programului-gazdă.

Virusarea prin suprascrierea datelor rezultate în urma execuţiei programului-gazdă se face prin inserarea codului malițios a virusului în zona rezervată datelor fără să se afecteze în acest fel funcţionarea programului. Acest mod de virusare este cel mai greu de detectat, deoarece nu afectează în dimensiune sau conținut programul-gazdă (figura 15).

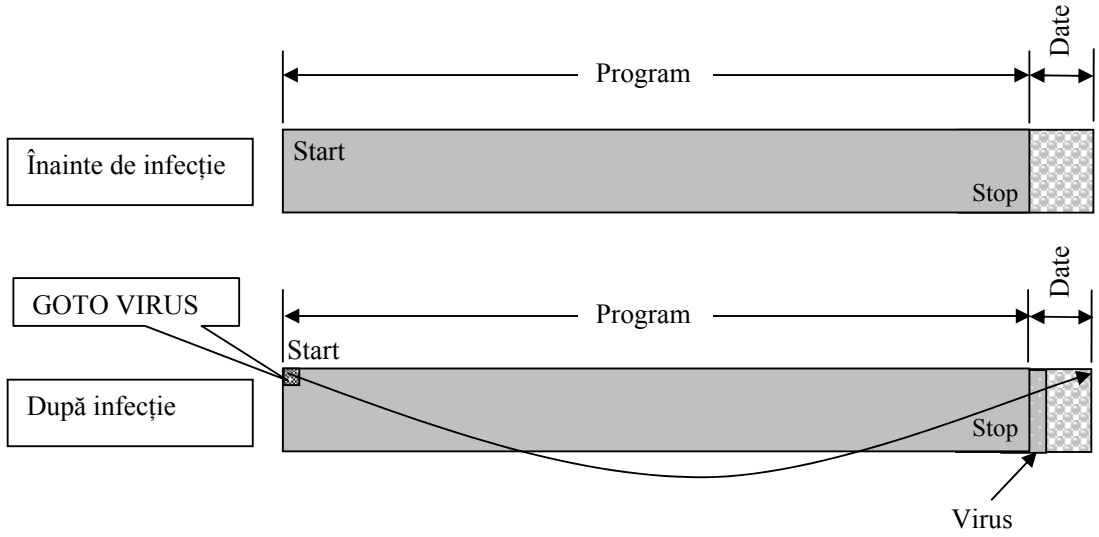


Figura 15. Virusarea datelor.

Un virus de fişier mai poate fi descris ca fiind *static* sau *polimorfic*. Un virus se poate „adapta“ la anumite condiţii oferite de sistemul de calcul sau de fişierul-gazdă. Acest virus poartă denumirea de virus adaptabil.

Un virus de fişier este considerat ca fiind *static* dacă, pe parcursul existenţei acestuia, nu-şi schimbă structura codului malițios. Codul rămâne intact indiferent de numărul şi de amploarea infecţiei create.

Viruşii de fişier polimorfici sunt capabili să-şi schimbe „semnătura“ atunci când se multiplică de la un sistem de calcul la altul. Din această cauză, aceşti viruşi sunt foarte greu de detectat, producând, de aceea, cele mai mari dezastre.

Modul de infectare cu viruşi a fişierelor poate fi diferit de la virus la virus. O clasificare a viruşilor de fişier ţinând cont de modul de infectare este următoarea:

- paraziţi;
- suprascriere;
- Entry-Point Obscuring;
- de companie;
- de legătură;
- OBJ, LIB şi viruşi cod sursă.

Viruşii paraziţi modifică conţinutul programului-gazdă, dar lasă cea mai mare parte din el intactă. Aceşti viruşi se ataşează la începutul sau la sfârşitul programului-gazdă. În anumite situaţii, codul virusului se poate instala în zone nefolosite din fişier.

Viruşii de suprascriere rescriu (suprascriu) programul-gazdă cu propriul lor program. În acest mod, programul-gazdă nu mai este funcţional.

Viruşii de tip Entry-Point Obscuring folosesc o metodă ingenioasă de infectare a programului-gazdă. În programul-gazdă se va introduce doar o mică secvenţă de program care, la îndeplinirea anumitor condiţii, va lansa în execuţie codul malitios al virusului aflat la o altă locaţie. Lansarea în execuţie a programului-gazdă nu va presupune şi lansarea în execuţie a virusului, acesta aşteptând condiţiile pentru a putea să-şi lanseze programul distructiv.

Viruşii de companie nu atacă în mod direct fişierul gazdă, dar creează o copie a acestuia care va fi lansată în execuţie în locul originalului. În acest fel, fişierul original care execută operaţia de formatare a suporturilor de memorie *format.com* va fi clonat şi redenumit *format.exe.* Acest din urmă fişier va conţine de fapt virusul. Viruşii de companie pot să modifice şi căile (paths) de acces în aşa fel încât să se dea trimitere la fişierele clonate.

Viruşii de legătură nu modifică decât în mică măsură conţinutul programului-gazdă. La începutul programului-gazdă se va inocula o instrucţiune de salt (GOTO, JUMP) la o locaţie din afara gazdei care va conţine codul virusului. Acţiunea este similară cu cea descrisă în modurile de infectare prin salt la sfârşitul programului gazdă sau prin suprascrierea datelor rezultate în urma execuţiei programului-gazdă.

Viruşii OBJ, LIB şi cod sursă nu au o răspândire aşa de mare. Aceştia infectează modulele obiect (OBJ), bibliotecile compilatoare (LIB), precum şi codurile sursă ale programelor-gazdă.

În cea mai mare măsură însă, viruşii de fişiere afectează fişierele executabile (cu extensiile EXE, COM etc.).

Cei mai cunoscuţi viruşi de fişier sunt: **CASPER**, **Chernobyl**, **CRUNCHER**, **Die-Hard2**, **Fun Love**, **Jerusalem**, **Junkie**, **Magistr**, **Natas**, **Nimda**, **OneHalf**, **Plagiarist**, **Vienna.**

Viruşii de boot pot să infecteze sectorul de boot de pe discurile flexibile sau dure. Pe discurile dure infectează de regulă zona de MBR[42]. Pot fi foarte distructivi, putând bloca sistemul de calcul în timpul operaţiei de boot-are. De asemenea, pot să distrugă întreaga informaţie de pe discuri, de regulă de pe discul dur. Apariţia şi recrudescenţa acestor viruşi îşi face simţită prezenţa încă de la apariţia primelor suporturi de memorie de tip disc flexibil pe care le infectau şi pe care le foloseau ca purtătoare pentru răspândirea lor. La ora actuală sunt cunoscuţi peste 1000 (1025) de viruşi sau variante de viruşi de boot. Faţă de alte tipuri de viruşi, aceştia şi-au limitat acţiunea datorită limitării folosirii din ce în ce mai puţin a discurilor flexibile. Nu înseamnă însă că au dispărut în totalitate.

[42] *MBR – Master Boot Record* – Zonă de pe discul dur rezidentă în cilindrul 0, capul 0, sectorul 1.

Singurul mod de infectare cu un virus de boot este de a se încărca sistemul de operare de pe o dischetă care conține un virus de boot. Aceasta dischetă, la rândul ei, a fost infectată de pe un calculator care conținea un virus de boot.

La punerea sub tensiune a sistemului de calcul – pornirea acestuia, se execută în mod normal următoarele acțiuni în procesul de încărcare (boot-are) (figura 16).

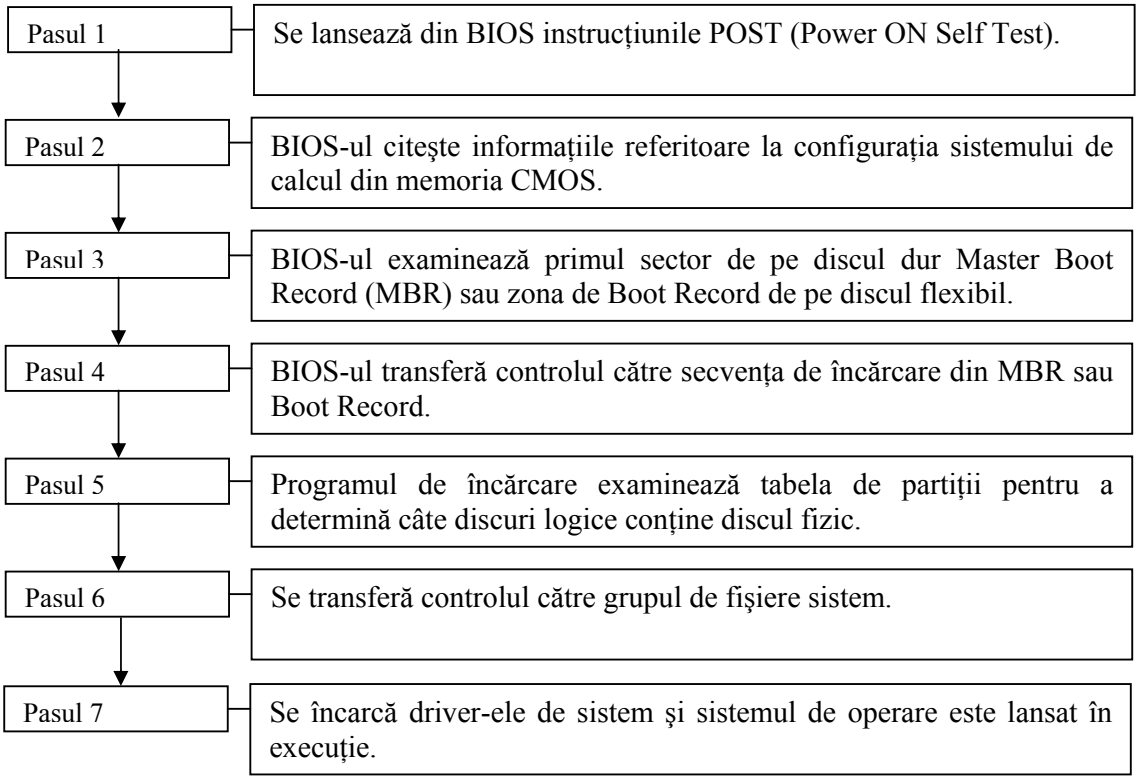


Figura 16. Procesul normal de boot-are.

Procesul de boot-are este modificat considerabil atunci când sistemul este infectat cu un virus de boot (figura 17).

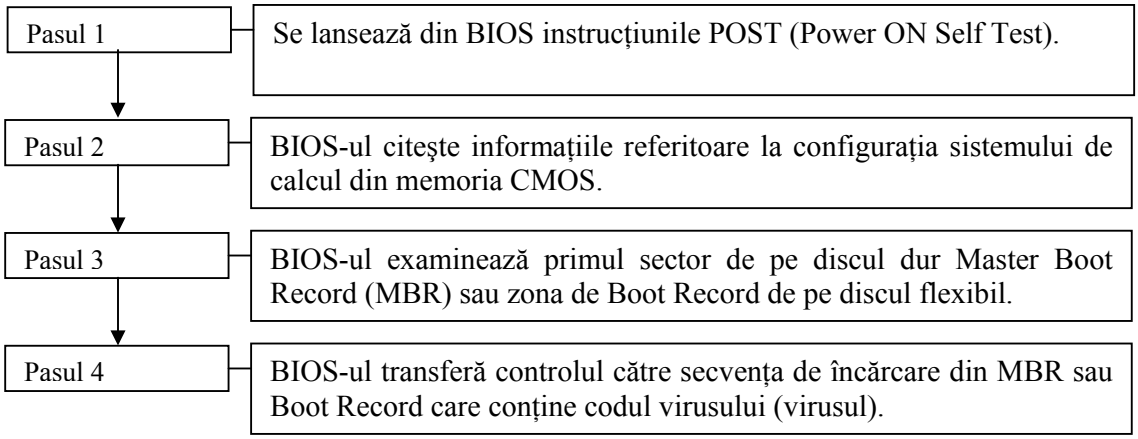


Figura 17. Procesul de boot-are de pe un disc virusat cu virus de boot.

Virusarea discurilor flexibile cu viruşi de boot se face prin suprascrierea codului existent în zona sectorului de boot cu cel al virusului.

Virusarea discurilor dure cu viruşi de boot se poate face în trei moduri:

- virusul va suprascrie codul MBR;
- virusul va suprascrie sectorul de boot;
- virusul va modifică adresa sectorului de boot către o adresă care va conține codul virusului.

Virusul va muta, în majoritatea cazurilor, sectorul original de boot într-o altă zonă liberă de pe disc. Din aceasta cauză, eliminarea virusului şi a efectelor acestuia de pe discurile dure pot fi realizate prin comanda ascunsă DOS *FDISK/MBR* executată de pe un disc flexibil boot-abil nevirusat care va conține şi această comandă.

O dată lansat în execuție, virusul rămâne rezident în memorie şi va infecta discurile flexibile folosite.

Interesant de remarcat la această categorie de viruşi este modul lor de acțiune față de alți viruşi de acelaşi tip. Pentru că acest tip de viruşi ocupă aceeaşi zonă de pe disc, MBR sau sectorul de boot, nu pot exista mai mulți viruşi de boot pe un disc. Ultimul virus instalat îl va şterge pe cel existent pe disc.

Cei mai cunoscuți viruşi de boot sunt: **Frankenstein**, **KULROY-B**, **Matthew**, **Michelangelo**, **PARITY**, **Stoned**.

Viruşi de macro, sau macro viruşi, infectează fişierele de tip document. Nu trebuie confundați cu viruşii de fişier care afectează fişierele executabile. Viruşii de macro tind să ia locul, ca modalitate de răspândire fizică, viruşilor de boot. Dacă viruşii de boot se răspândesc cu ajutorul dischetelor purtate de la un utilizator la altul, viruşii de macro se răspândesc cu ajutorul documentelor transmise între utilizatori. Față de viruşii de boot, viruşii de macro sunt mult mai numeroşi, atingând un număr de aproape 5000. Pentru că infectează fişiere de tip document, care sunt portabile pe diferite platforme, pot afecta atât sistemele Windows, cât şi Macintosh.

Primele manifestări ale macro viruşilor au apărut în anul 1995. Paradoxal, primul virus de macro, numit Concept, a fost conținut în CD-ROM-urile cu documentații şi programe de aplicații oferite de firma Microsoft, „Microsoft Windows 95 Software Compatibility Test", „Microsoft Office 95 and Windows 95 Business Guide" şi „Snap-On Tools for Windows NT CD". Deşi a fost repede descoperit şi discurile au fost retrase de pe piață, răul fusese făcut şi ideea de virus de macro fusese lansată neintenționat.

Un virus de macro se va folosi de facilitatea de a crea macro comenzi oferită de unele programe cum ar fi Microsoft Office 95/97/2000 şi Lotus Ami Pro. Dacă utilizatorul va folosi facilitățile oferite prin crearea de comenzi macro pentru a-şi uşura munca, virusul va folosi această facilitate pentru a se răspândi şi a-şi îndeplini scopul distructiv.

Virusul exploatează o aplicație *auto-execution macro* care este lansată automat în execuție când documentul este deschis. Lansată în execuție, comanda macro care conține codul malițios al virusului va putea să şteargă sau să modifice porțiuni de text, să şteargă sau să redenumească fişiere, să se multiplice şi să creeze alte tipuri de distrugeri. Mulți viruşi de macro se autocopiază în fişierul *normal.dot* care este lansat în execuție (în Microsoft Word) ori de câte ori este deschis un document. În acest fel, noul document deschis va fi infectat.

Viruşii de macro afectează fişierele cu extensiile: DOC şi DOT – create cu Microsoft Word; XLS şi XLW – create cu Microsoft Excel; ADE, ADP, MDB şi MDE – create cu Microsoft Access; PPT – create cu Microsoft Access; SAM – create cu Lotus Ami Pro; CSC – create cu Corel Draw şi Corel Photo-Paint.

Cei mai răspândiți viruşi de macro sunt cei care afectează platformele Microsoft. Şi aceasta nu din cauză că această platformă este mai vulnerabilă ca altele, ci din cauză că cele mai multe documente sunt create cu aceasta.

Funcţionarea unui virus de macro este exemplificată în figura 18.

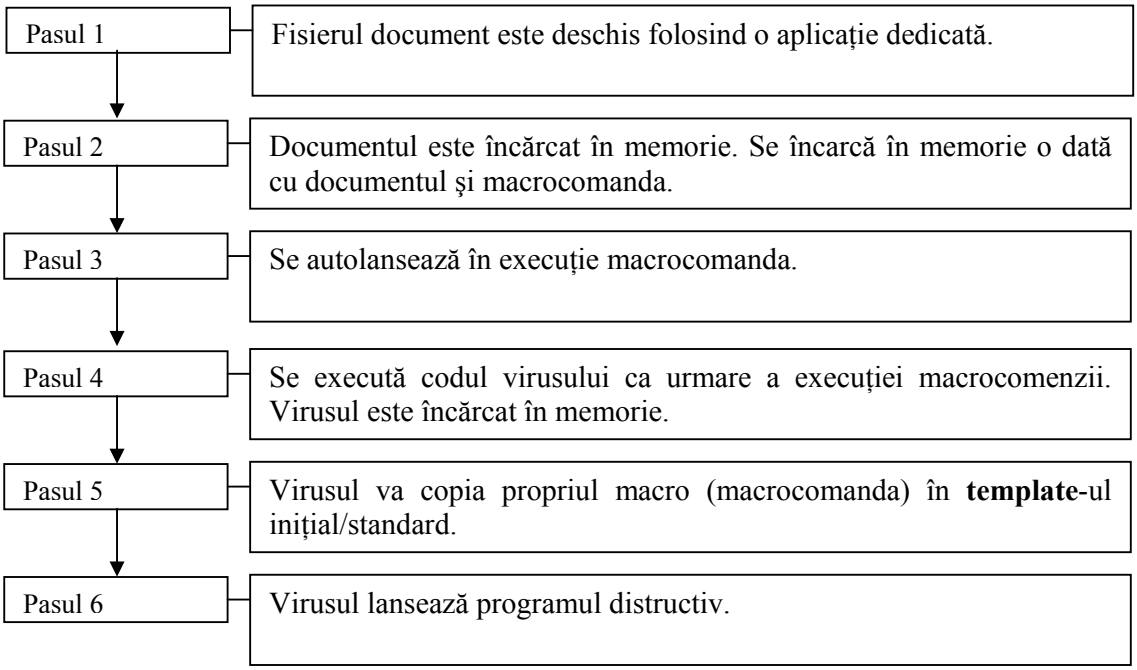


Figura 18. Funcţionarea unui virus de macro.

Cei mai cunoscuţi viruşi de macro sunt: **Atom**, **Colors**, **Concept**, **DMV**, **FormatC**, **Gala**, **Hot**, **Melissa**, **Nuclear**, **PPoint.Attach**.

Viruşii de script sunt creaţi cu ajutorul unor limbaje numite limbaje script sau scripturi. Există mai multe limbaje script care sunt folosite de la scrierea de programe pentru sistemele de operare şi până la crearea paginilor Web. Deosebirea dintre limbajele script şi limbajele tradiţionale este aceea că, faţă de limbajele de programare ca C sau Visual Basic, scripturile sunt mai puţin complexe. Scriptul reprezintă de fapt un cod de program scris cu un limbaj script. Instrucţiunile script sunt executate pe rând în mod secvenţial. Un fişier script este similar cu un fişier de comenzi BATCH din vechile sisteme de operare de tip DOS[43].

Un avantaj al acestor limbaje este acela că sunt uşor de învăţat, din această cauză sunt creaţi din ce în ce mai mulţi viruşi cu ajutorul acestora.

Un fişier VBS va conţine de fapt instrucţiuni scrise în mod text. Este suficient să se folosească un editor de texte la îndemână, un Windows Notepad sau Word Pad, să se scrie instrucţiunile şi în final să se salveze fişierul cu extensia VBS. Lansat în execuţie, fişierul îşi lansează codul distructiv. Un virus de script va putea fi modificat cu uşurinţă folosind aceste unelte. Rezultatul va fi o nouă variantă de virus.

Se poate face observaţia că un virus de macro reprezintă de fapt un tip de virus de script deoarece un limbaj macro este la ora actuală un limbaj script.

Cele mai cunoscute limbaje script sunt: Visual Basic Script (VBS), JavaScript (JS) şi ActiveX.

Activarea acestor viruşi se face prin intermediul lui Microsoft Windows Scripting Host la sistemele de operare Windows sau atunci când un document care conţine virusul este deschis sau vizualizat. Viruşii VBS sau JavaScript se vor activa atunci când fişierele respective vor fi lansate în execuţie. Dacă o pagina HTML[44] conţine un virus de script, simpla

[43] *DOS – Disk Operating System* – Sistem de operare de tip MS DOS, DR DOS, PTS DOS.
[44] *HTML – Hyper Text Markup Language* – Limbaj hipertext.

vizualizare a acesteia va lansa în execuţie codul virusului. Un mesaj de poştă electronică ce conţine un virus de script va duce, prin deschiderea acestuia, la execuţia virusului.

Propagarea acestor viruşi se face prin pagini Web infectate, mesaje de poştă electronică (e-mail), prin fişiere ataşate mesajelor de poştă electronică, sesiuni IRC[45] sau documente.

În cazul în care se infectează documente aceşti viruşi sunt de fapt viruşi de macro.

O clasificare a acestor viruşi poate fi făcută după limbajele care sunt folosite pentru crearea acestora. Cele mai cunoscute sunt: **Visual Basic Script**, **Windows Script**, **ActiveX**, **JavaScript**, **HTML**, **MIME**, **PHP**.

Visual Basic Script este cel mai popular în crearea acestor viruşi. Visual Basic Script este o versiune script a limbajului de programare Visual Basic. Un VBS va conţine linii de comandă care vor fi executate secvenţial la lansarea în execuţie a fişierului care le conţine.

Windows Script permite sistemelor de operare Windows, prin intermediul lui Windows Script Host (WSH), lansarea în execuţie a diferitelor fişiere create cu ajutorul unui limbaj script. Fişierele create cu ajutorul unor limbaje script – VBS, ActiveX sau JavaScript – au extensia VHS şi pot să modifice funcţiile sistemului de operare.

ActiveX reprezintă o tehnologie folosită de către Microsoft pentru vizualizarea paginilor Web. Controalele ActiveX sunt folosite pentru gestionarea paginilor Web atunci când sunt încărcate într-un browser de Web şi pot include contoare de vizitatori, butoane etc. ActiveX este creat folosind limbajul ActiveX script. Modificarea acestuia poate duce la deteriorarea sau pierderea datelor din calculator. Browser-ul Internet Explorer de la Microsoft (la versiunile mai vechi de sisteme de operare) avea o serie de goluri de securitate în această privinţă. În unele cazuri, utilizatorul recurgea la dezactivarea controalelor ActiveX pentru a putea să-şi asigure securitatea.

JavaScript este un limbaj script derivat din Java şi are foarte multe asemănări cu ActiveX. A fost creat pentru a fi încorporat în codul standard HTML la crearea paginilor Web. Poate fi lansat de către Windows Scripting Host şi este încorporat în paginile Web şi poştă electronică.

HTML reprezintă un cod folosit pentru crearea paginilor WEB. Un cod simplu HTML nu poate conţine un virus, dar o pagină Web creată cu acesta poate conţine virusul prin încorporarea VBS, JavaScript sau ActiveX.

MIME face posibilă exploatarea unui gol de securitate din Outlook sau Outlook Express care permite vizualizarea automată a unui mesaj. Dacă acest mesaj va conţine virusul, acesta îşi va lansa codul distructiv.

PHP este un limbaj script folosit la nivel de server pentru crearea paginilor Web dinamice.

Pe lângă aceste modalităţi de creare, lansare şi multiplicare a viruşilor de script se mai întâlnesc şi cele care acţionează la nivelul fişierelor cu extensia INF şi REG din sistemele de operare Windows. Modificarea neautorizată a acestor fişiere va duce la disfuncţionalităţi ale sistemului.

Cei mai cunoscuţi viruşi de script sunt: **666test**, **777**, **BeanHive**, **Exploit-MIME.gen**, **FreeLink**, **Hard**, **HTML.Internal**, **KakWorm**, **LoveLetter**, **Monopoly**, **NewWorld**, **Rabbit**, **Regbomb**, **Script.Inf**, **Strange Brew**, **VBS/SST**, **Win95.SK**.

Viruşii de e-mail se folosesc de faptul că e-mail-ul reprezintă cea mai utilizată aplicaţie Internet din zilele noastre. Zilnic fiecare utilizator transmite şi recepţionează mesaje în format electronic. Beneficiile sunt evidente în acest caz. Reversul este că tot prin e-mail se transmit şi coduri malitioase – viruşi informatici.

Posibilitatea de a folosi poşta electronică pentru transmiterea de viruşi a fost făcută posibilă datorită evoluţiei tehnicii. Primele mesaje de e-mail erau trimise şi recepţionate în text clar (plain text) fără posibilitatea de a se putea insera un virus în acest mesaj. Numai că

[45] *IRC – Internet Relay Chat.*

utilizatorul nu avea posibilitatea de formatare a textului. Nu se putea scrie cu litere groase, înclinate, colorate, de diferite mărimi etc. Şi nici nu era nevoie. Conta doar informaţia transmisă de textul în sine şi nu de artificiile pe marginea textului. Numai că tehnica a evoluat şi s-a făcut trecerea de la Plain Text e-mail la HTML e-mail. Şi o dată cu acesta a apărut şi posibilitatea de a se transporta viruşi cu ajutorul e-mail-ului.

Un e-mail în format HTML este ca o pagină Web HTML. Iar o pagina Web HTML are încorporate controale ActiveX şi applet-uri JavaScript care pot să conţină şi să lanseze coduri maliţioase. Viruşii care se transmit prin e-mail sunt de fapt viruşi de script şi nu viruşi de e-mail în accepţiunea standard. O altă modalitate de transmitere a unui virus este de a-l ataşa ca fişier de mesajul scris în mod plain text.

Pentru răspândirea viruşilor cu ajutorul poştei electronice se folosesc în principal trei modalităţi:

- prin ataşamente, utilizând tehnica de Cal Troian;
- prin exploatarea golurilor de securitate, MIME exploit;
- prin încorporarea codului maliţios în mesaje HTML.

Răspândirea viruşilor prin fişiere infectate ataşate la mesajul text este cea mai comună cale şi cea mai utilizată. Dacă destinatarul nu lansează în execuţie fişierul care conţine virusul nu se întâmplă nimic. Dacă însă se trece la execuţia acestuia atunci codul maliţios al virusului este executat şi virusul va executa operaţiile pentru care a fost proiectat şi se va multiplica şi răspândi.

De regulă utilizatorii, care dispun de un minim de cunoştinţe despre viruşi, nu vor deschide un fişier nesolicitat sau trimis de o persoană necunoscută. Dar sunt situaţii când virusul a luat adresa utilizatorului din Address Book-ul unui alt utilizator cunoscut, dar care a are calculatorul virusat. Şi dacă mesajul care conţine un fişier infectat vine de la un prieten s-ar putea ca utilizatorul să-l deschidă şi infecţia să se producă.

Tehnica de Cal Troian este folosită pentru a disimula fişiere infectate în fişiere inofensive. Marea majoritate a utilizatorilor de e-mail nu deschid fişierele care au extensia EXE sau COM chiar dacă vin dintr-o sursă sigură. Şi atunci virusul vine sub forma de Cal Troian, schimbându-şi extensia pentru a păcăli victima. Extensiile TXT şi JPG sunt cele mai de încredere în acest caz. Fişierele cu aceste extensii nu pot conţine viruşi. Un fişier Foto.exe.jpg (se observă două extensii) va putea să fie deschis de către un utilizator neatent sau neavizat şi virusul să se execute.

Golurile de securitate exploatate de către viruşi pentru a se multiplica sunt prezente cu precădere la programele de poştă electronică de la Microsoft – Outlook Express şi Microsoft Outlook, precum şi la browser-ul Internet Explorer. Standardul creat pentru transmisia fişierelor ataşate la mesajele de poştă electronică, Multipurpose Internet Mail Extension (MIME), reprezintă punctul slab exploatat de către viruşi. Versiunile mai vechi de Internet Explorer, precum şi vechile programe de poştă electronică deschideau automat mesajele ataşate. Acest fapt permitea crearea de e-mail-uri în format HTML care conţineau un ataşament executabil cu conţinut maliţios. Atacatorul nu trebuia decât să modifice header-ul MIME al fişierului ataşat. Internet Explorer citea ataşamentul ca fiind unul în regulă şi-l deschidea automat.

Acest tip de atac se numeşte MIME exploit (exploatare MIME). Microsoft a umplut acest gol de securitate şi versiunile Internet Explorer şi programele de poştă electronică nu mai permit astfel de atacuri.

Încorporarea codului maliţios în mesaje e-mail HTML se face scriind coduri JavaScript. Aceste coduri vor rula automat când mesajul va fi vizualizat fără să mai fie nevoie ca infecţia să se producă prin ataşamente virusate. Faţă de infecţia prin fişiere ataşate, când utilizatorul poate să nu deschidă fişierul ataşat şi infecţia să nu se producă, aici infecţia se produce automat la vizualizarea mesajului. Această modalitate de răspândire are cele mai mari şanse

de reuşită, dar necesită şi cunoştinţe avansate pentru încorporarea codului în e-mail. Din această cauză, infectarea în acest mod este destul de rară.

Din categoria viruşilor de e-mail se remarcă: **666test**, **Babylonia**, **Badtrans**, **BubbleBoy**, **FreeLink**, **Hard**, **Hybrys**, **KakWorm**, **Kletz**, **LoveLetter**, **Melissa**, **Monopoly**, **MyLife**, **NakedWife**, **Nimda**, **VBS/SST**.

Viruşi de Chat şi Instant Messaging

Serviciul de Chat este asigurat de servere specializate dintr-o subreţea Internet numită Internet Relay Chat (IRC). Aceasta permite ca doi sau mai mulţi utilizatori să poarte discuţii (chat[46]) individuale sau de grup şi să schimbe între ei fişiere folosind un canal de comunicaţie. Utilizatorii unui canal se numesc membri ai acelui canal. Protocolul folosit în transmisie este DCC[47].

Utilizatorul va putea cu ajutorul unui program, cum ar fi mIRC[48], să se conecteze la un server de chat şi să iniţieze un grup de discuţii.

Folosind acest mediu creat, un virus se va putea multiplica şi va putea infecta calculatoarele din reţea în două moduri distincte:

- prin transferul de fişiere infectate între utilizatori;
- prin folosirea scripturilor IRC.

Infectarea prin transferul de fişiere infectate între utilizatori este destul de simplu de realizat. Atacatorul va trimite către ţintă un fişier care se vrea să fie util destinatarului. Acesta poate să fie un fişier de ajutor, un program utilitar, un mic joc, un fişier cu documentaţii sau o imagine. O dată ce destinatarul va deschide fişierul trimis, virusul se va activa şi-şi va lansa programul distructiv.

Infectarea prin folosirea scripturilor IRC presupune scrierea de scripturi care vor conţine instrucţiuni care se vor executa secvenţial. O dată acceptate de către destinatar sau destinatari, aceste scripturi se vor substitui automat în fişierele similare din calculatorul-ţintă şi vor iniţia atacul.

Majoritatea infecţiilor se întâmplă atunci când, în urma atacului, se va crea fişierul **script.ini** sau **mirc.ini** în folderul curent mIRC. Acestea conţin scripturi şi se vor executa comenzile pentru care au fost proiectate. Instalarea acestor scripturi este posibilă dacă opţiunea Auto-DCC-Get este configurată pe activ. Fiind activă, se vor accepta toate fişierele trimise de către utilizatorii din canalul respectiv de chat. Pentru o mai mare siguranţă, această opţiune va fi setată pe inactiv.

Cei mai cunoscuţi viruşi de IRC sunt: **Acoragil**, **Back Orifice**, **Bat**, **Dmsetup**, **Flood**, **Fono**, **Goner**, **Links**, **Millenium**, **pIRCH.Events**, **Script.ini**, **Simpsalapim**, **Stages**.

Programele de Instant Messaging folosite la ora actuala, AOL Instant Messenger (AIM), MSN Messenger, Windows Messenger, ICQ şi Yahoo! Messenger, sunt şi ele supuse atacurilor. Folosind aceste programe, utilizatorii pot să transmită mesaje instant şi de asemenea şi fişiere. În acest mod se pot transmite şi viruşii. Numai că, spre deosebire de alte programe care permit recepţionarea de fişiere prin Internet fără acceptul utilizatorului, aici utilizatorul poate să accepte sau nu un fişier care-i este destinat. Un calculator care participă la transmiterea de mesaje instant nu va putea să fie virusat decât dacă utilizatorul a dat accept pentru descărcarea şi rularea sau vizualizarea unui fişier care-i era destinat şi care conţinea virusul.

Programele de instant messaging sunt de regulă folosite de persoane care au într-adevăr nevoie de acest serviciu şi pentru care timpul nu le permite să stea la conversaţii inutile (chat). Mesajele se transmit între utilizatori de încredere (trust), mare parte a acestora cunoscându-se fizic, faţă de serviciul de chat, unde de multe ori utilizatorii dintr-un canal nu se cunosc şi, mai mult, au identităţi dubioase.

[46] *Chat* – conversaţie, taifas, pălăvrăgeală, şuetă, flecăreală.
[47] *DCC – Direct Client to Client Protocol*.
[48] *mIRC – Microsoft Internet Relay Chat*.

Chiar dacă numărul de viruşi care se poate transmite este mai mic, totuşi aceştia se pot transmite. Un mare aport în limitarea numărului de viruşi îl au companiile proprietare ale acestor servicii.

Viruşii din această categorie au ca particularitate faptul că sunt dedicaţi pe reţeua/serviciul respectiv de IM. Dacă un virus este făcut să lucreze într-o reţea Yahoo! Messenger, acesta nu va funcţiona într-o reţea MSN Messenger.

Cei mai importanţi viruşi din această categorie sunt: **Choke**, **Goner**, **Hello**, **Reeezak**, **Stages**. Cu observaţia că doar doi dintre aceştia se regăsesc şi în lista de viruşi care afectează reţelele de chat, ceilalţi sunt viruşi dedicaţi numai anumitor reţele/servicii.

Viruşi păcăleală (Hoax)

Aceştia reprezintă o categorie specială de viruşi care se bazează pe credulitatea aceluia care poate să devină ţinta unui atac. Mesaje de e-mail sau ferestre apărute în timp ce faci browsing de genul „**Ai câştigat o excursie în…**“, „**Ai câştigat o sumă de…**“, „**Calculatorul tău are un virus…**“, „**Trimite acest mesaj la toţi cunoscuţii tăi şi vei avea noroc…**“, cu invitaţia de a trimite sau de a confirma cu **opţiunea Yes**, sunt destul de frecvente în Internet. Uneori, acest tip de viruşi, mai ales cei care apar în ferestre browsing, acţionează chiar şi atunci când se alege **opţiunea No** (Nu). Din aceasta cauză, este indicat să se închidă fereastra din **opţiunea Close** (**X**), din **Taskbar → Close**, sau apăsând perechea de taste **Alt+F4**.

Cei mai importanţi viruşi din această categorie sunt: **Blue Mountain Card**, **Goood Times**, **Help**, **Rit Takes Guts to Say** „**Jesus**“, **MusicPanel(MP3)**, **New Pictures of Family**, **New Ice Age**, **Pretty Park**, **Sulfnbk.exe**, **VeryBad**, **WOBBLER**, **WTC Survivor Virus.**

2.2.3. Modalităţi de acţiune a programelor independente de tip vierme

Un **vierme** este un program independent. El se reproduce prin autocopierea de la un calculator la altul prin intermediul reţelei în cele mai multe cazuri şi fără acceptul utilizatorului. Spre deosebire de virus, un vierme nu alterează sau distruge datele din calculator, dar poate crea disfuncţionalităţi în reţea prin utilizarea resurselor acestuia pentru autoreproducere.

Viermele se foloseşte de mecanismele de transmisie de fişiere care se regăsesc în majoritatea programelor care folosesc Internetul. Cu ajutorul acestora, viermele se va multiplica către alte calculatoare.

În majoritatea cazurilor, viermii se propagă cu ajutorul poştei electronice. Alte modalităţi de propagare mai sunt prin IRC şi IM.

O categorie aparte de viermi o reprezintă **viermii de reţea**. Aceştia exploatează golurile de securitate din serverele sau browser-ele Web şi infectează, fără ca să poată fi detectaţi, serverele respective. De aici vor lansa atacuri pentru a infecta toate calculatoarele care se leagă la acestea. Fiind foarte greu de detectat şi urmărit, aceşti viermi de reţea creează cele mai multe inconveniente. Pentru a se răspândi la alte locaţii din Internet, viermele va culege datele despre alţi utilizatori din Address Book şi se va copia la aceste adrese. Cu cât numărul persoanelor de contact de aici este mai mare, cu atât infecţia se va răspândi la mai multe locaţii. Viermele va culege un număr predefinit de adrese de aici. Numărul de adrese culese diferă de la vierme la vierme. De regulă, aceştia culeg până la 50 de adrese. Dar sunt şi situaţii când se culeg şi mai multe adrese. Melissa – care a fost considerat la vremea când au apărut primele lui atacuri ca fiind foarte distructiv – culegea 50 de adrese de e-mail. Efectele lui LoveLetter au fost însă şi mai mari, deoarece acesta culegea primele 300 de adrese de e-mail şi în plus mai distrugea şi fişiere. Adică aproape toate adresele din Address Book (nu multă lume are peste 100 de adrese). MyLife se retransmitea la toate contactele din Address Book.

Multiplicarea acestora la alte adrese şi de aici la altele culese din calculator va avea ca efect paralizarea traficului şi într-un final serverul/serviciul respectiv de poştă electronică, IRC sau IM, va fi paralizat şi în final oprit. Acesta este modul de acţiune al unui vierme. El nu cauzează distrugeri directe. Nu va altera sau şterge fişiere. El doar se va multiplica. Dar cheltuielile şi timpul pierdut pentru depistarea acestuia şi refacerea serviciilor sunt foarte mari.

Viermii sunt consideraţi ca fiind cele mai distrugătoare programe maliţioase din ultimii ani. Jumătate din primele zece programe maliţioase apărute în această perioadă sunt viermi.

Cei mai cunoscuţi viermi sunt: **Badtrans**, **BubbleBoy**, **CodeRed**, **Hybris**, **Klez**, **LoveLetter**, **MyLife**, **Nimda**, **SirCam**.

2.2.2. Instrumente de atac de tip Cai Troieni, Back Doors-uri şi bombe

CAI TROIENI

Un **Cal Troian** este un fragment de cod care se ascunde în interiorul unui program şi care va executa o operaţie ascunsă. Acesta reprezintă cel mai utilizat mecanism pentru a disimula un virus sau un vierme.

Un Cal Troian se va disimula în fişiere executabile, fişiere imagine, fişiere screen saver etc. În anumite situaţii se ascunde în programe care se vor a fi aplicaţii antivirus.

Pentru a putea să lanseze codul distructiv, un Cal Troian trebuie să convingă utilizatorul ca fişierul ataşat este „**curat**“, dar mai ales că **„trebuie**“ deschis.

Pentru a putea realiza aceasta, proiectanţii de Cai Troieni folosesc următoarele tehnici menite să păcălească destinatarul:

- trimiterea de fişiere ataşate care vin dintr-o sursă de încredere;
- denumirea fişierelor ataşate cu nume care să determine utilizatorul să le deschidă;
- ascunderea tipului de fişier.

Trimiterea de fişiere care vin dintr-o sursă de încredere se face prin colectarea datelor din Address Book, de pe calculatorul virusat, şi trimiterea de e-mail-uri care conţin Calul Troian la aceste adrese. Când utilizatorul calculatorului-ţintă va deschide spre vizualizare mesajul, la From: va apărea numele cunoscut al unui prieten, coleg de serviciu, rudă şi va avea încredere să deschidă fişierul ataşat şi astfel infecţia să se producă.

Denumirea fişierelor ataşate cu nume care să determine utilizatorul să le deschidă se foloseşte de slăbiciunile umane. Un utilizator va fi tentat să deschidă un fişier care conţine o declaraţie de dragoste de la un admirator (cazul LoveLetter), să vizualizeze o caricatură cu preşedintele ţării (cazul MyLife), să vadă o imagine cu nudul unei actriţe sau vecine (cazul Naked Wife) sau să primească un program antivirus.

Ascunderea tipului de fişier se face pentru ca utilizatorul să nu vadă extensia executabilă a fişierului ataşat. Pentru aceasta se folosesc două metode.

Prima presupune ca fişierele executabile care conţin Calul Troian, şi care au extensiile EXE, COM, SCR, PIF, VBS, să fie dublate de extensii „inofensive“ care să „adoarmă“ vigilenţa utilizatorului care ştie că nu trebuie lansate în execuţie fişierele executabile fără o verificare prealabilă. Un fişier **fiser.exe** va avea ataşată una dintre extensiile JPG, GIF sau TXT. În acest fel, acesta devine **fiser.jpg.exe.**

A două metodă este foarte ingenioasă şi presupune interpunerea între extensia reală şi denumirea rămasă a unui număr foarte mare de spaţii în aşa fel încât la o vizualizare pe ecran extensia să nu fie afişată. Spre exemplu, fişierul anterior va apărea afişat pe ecran în forma:

fiser.jpg **.exe**

(cu **.exe** care nu va fi afişată, deoarece depăşeşte spaţiul de afişare al ecranului).

În acest fel, utilizatorul crede că este un fişier „inofensiv“ şi-l va deschide.

O mare parte din Caii Troieni au caracteristica de vierme, ei răspândindu-se cu ajutorul poştei electronice către alţi utilizatori. Adresa utilizatorilor este culeasă din Address Book.

Cei mai cunoscuţi Cai Troieni sunt: **Dmsetup**, **Flood**, **LoveLetter**, **MyLife**, **Naked Wife.**

CĂI ASCUNSE – TRAP DOORS / BACK DOORS

Căi ascunse (Trap Doors) sunt mecanisme care sunt create de către proiectanţii de software pentru a putea să pătrundă în sistemul de calcul ocolind sistemele de protecţie.

Căi ascunse (Back Doors) se pot crea cu ajutorul Cailor Troieni. Mecanismul presupune introducerea în calculatorul-ţintă a unui program care ulterior să deschidă căi de acces către resursele acestuia. Programele din această categorie poartă chiar denumiri generice gen **BackDoor. Subseven**, **BackDoor.Troian** şi **BackOriffice**[49].

BOMBE

O **bombă** reprezintă un tip de Cal Troian, care va lansa un program distructiv la o anumită dată sau atunci când anumite condiţii impuse sunt îndeplinite.

Tehnic, există două tipuri de bombe: *de timp* şi *logice*. O bombă de timp se va activa atunci când se scurge o anumită perioadă de timp de la instalare sau când se atinge o anumită dată calendaristică. O bombă logică va acţiona atunci când se îndeplinesc anumite condiţii impuse de cel care a creat-o. Avantajul acţiunii unei bombe este acela că dă posibilitatea celui care a trimis-o să-şi şteargă urmele în intervalul de timp până la activare.

→ *Am făcut această prezentare a programelor maliţioase şi am încercat să le grupez după modul lor de acţiune pentru a da o viziune de ansamblu corectă asupra acţiunii acestora, dar şi ca o informare a utilizatorului despre acest pericol.* ***Nu cred că există utilizator de calculatoare care să nu fi avut de-a face cel puţin o dată cu acţiunea unor astfel de programe.***

Marii producători de programe antivirus oferă şi alte clasificări. Firma Symantec, liderul în materie de programe antivirus, grupează programele maliţioase în următoarele categorii: comuni, de program, de boot, Stealt, polimorfici, multipartiţie, de macro, de windows şi programe maliţioase. Alte firme oferă alte tipuri de clasificări. Am întâlnit şi situaţii amuzante referitoare la „viruşi". Erorile datorate instalărilor defectuoase a programelor sau driverelor de periferice au fost puse pe seama acţiunii viruşilor. O altă situaţie este aceea generată de „faimosul" virus Y2K[50]*. O simplă scriere a anului calendaristic pe două cifre şi nu pe patru a dat naştere la o adevărată psihoză la sfârşitul anului 1999. Această „scăpare" (în anii de început ai erei informatice nevoia de spaţiu era stringentă) a fost impropriu numită bug, apoi virus informatic, pentru ca în final să ajungă sub denumirea de virus (de orice natură) în ştirile sistemului mass-media care preziceau Apocalipsa şi din această cauză. S-au livrat numeroase programe care să testeze compatibilitatea calculatorului cu anul 2000 şi eventual să stopeze „virusul". Un manager de la o firmă mi-a spus la vremea respectivă că-şi va reînnoi parcul de calculatoare după 1 ianuarie 2000 ca să fie sigur „că merg". Cunoscătorii în domeniu au făcut mare haz de această situaţie propunând tastaturi, mouse şi alte echipamente „compatibile cu anul 2000". A trecut şi fatidica dată şi Apocalipsa nu s-a produs. Un utilizator al programului Ciel Contab se plângea chiar de faptul că, după ce programul a fost făcut „compatibil cu anul 2000", trebuia să tasteze în loc de două cifre patru pentru an, deşi în programele de contabilitate data calendaristică nu este supusă operaţiilor aritmetice ca să fie nevoie de patru cifre pentru an.*

[49] BackOriffice a fost creat ca o parodiere a programului Microsoft BackOffice.
[50] Întâlnit şi sub denumirea de „Virusul anului 2000".

2.2.3. Spărgătoare de parole şi utilizarea lor în testarea securității firmei

Protejarea prin parole a accesului la resursele sistemului de calcul sau protejarea în acelaşi mod a accesului la fişiere reprezintă cea mai des utilizată şi mai la îndemână metodă de protecție a datelor din calculatoare.

În majoritatea cazurilor sistemul de parole este folosit pentru autentificare şi identificare în limitarea accesului, dar poate fi folosit şi pentru protecție la nivel de fişier sau folder.

Un spărgător de parole este un program care poate determina parolele sau care poate evita sau dezactiva protecția prin parole. În literatura de specialitate termenul poate fi întâlnit sub denumirile de „password cracker" sau „password recovery". Programele din această categorie îşi bazează succesul pe folosirea algoritmilor care prezintă slăbiciuni, implementări greşite ale acestora şi factorul uman. Un spărgător de parole este cu atât mai eficient cu cât parola folosită este mai simplă de găsit şi cu cât programul de spart parole rulează pe un calculator performant.

Ca tehnici de atac pentru „ghicirea" parolei se folosesc următoarele:

- atac prin „forța brută";
- atac folosind dicționare.

Atacul folosind ca tehnică „forța brută" este un program care încearcă să găsească, încercare după încercare, parola corectă. Aceasta presupune generarea, după un anume algoritm, de cuvinte care sunt apoi testate ca parolă. Folosirea combinațiilor de 10 cifre, 26 de litere şi alte simboluri existente pe tastatură fac ca procesul să fie de lungă durată. Folosirea unui calculator performant reduce considerabil timpul. De asemenea, dacă parola este scurtă sau foloseşte combinații doar de cifre sau de litere, timpul este redus.

Atacul folosind dicționare presupune existența unui fişier dicționar (dictionary file) care conține o listă de cuvinte folosite în algoritmul de generare a parolei. Programul va folosi datele din acest dicționar pentru a încerca spargerea parolei.

→ *În cadrul firmei este indicat ca periodic să se facă o testare a parolelor. Aceasta se impune mai ales atunci când acestea sunt alese de către utilizator atunci când îşi protejează prin parole, într-un fel sau altul, accesul la fişiere.*

→ *Folosirea parolelor pentru limitarea accesului se impune în două situații:*

- *pentru limitarea accesului persoanelor neautorizate la resursele calculatorului;*
- *atunci când calculatorul este folosit de mai mulți utilizatori.*

→ *Prezența parolelor care să permită accesul la resursele calculatorului se face simțită în patru cazuri, şi anume:*

- *la pornirea calculatorului;*
- *la încărcarea sistemului de operare;*
- *la accesarea resurselor rețelei;*
- *la accesarea fişierelor.*

Pornirea calculatorului este marcată, dacă este configurată din CMOS această opțiune, de cererea introducerii unei parole de acces. Necunoaşterea acestei parole va bloca calculatorul în faza de preîncărcare a sistemului de operare. Metoda a funcționat şi funcționează cu condiția ca intruderul să fie un novice. Există parole universale, create de proiectanții de calculatoare, care permit depăşirea acestui obstacol. Faimoasa combinație 589589 făcea ca parola de CMOS să fie inutilă la calculatoarele echipate cu microprocesoare din generația 486. Complementar sau în paralel cu această metodă există programe care se instalează în CMOS şi care asigură un grad sporit de securitate şi care realizează aceeaşi funcție.

Majoritatea sistemelor de operare pot fi configurate, mai ales în cazul folosirii de către mai mulți utilizatori a calculatorului, să nu permită încărcarea sistemului de operare dacă nu este introdusă corect parola.

Accesul la resursele rețelei poate fi de asemenea blocat de cunoaşterea unei parole. Acest lucru poate fi asigurat de către sistemul de operare sau de către software-ul rețelei. Ca software de rețea, Novell Netware se achită foarte bine de această sarcină.

Determinarea modului de acces la un fişier, grup de fişiere sau foldere poate fi limitat tot cu ajutorul folosirii parolelor. Aceasta operație poate fi realizată de către sistemul de operare sau de alte programe. Ca exemplu, accesul la o bază de date poate fi limitat de către sistemul de operare sau de către SGBD[51].

Dacă primele sisteme de operare nu aveau implementată această facilitate, sistemele de operare UNIX şi apoi cele de tip DOS au implementat-o. Primele sisteme de operare DOS care au implementat folosirea parolelor au fost cele livrate de firma Digital Research Inc. la versiunile DR-DOS 6.0 şi ulterioare. Acest sistem de operare permitea o protecție ridicată, la acea vreme (1990-1995), prin limitarea modului de acces la fişiere sau directoare. Protecția era efectivă numai pe calculatorul pe care funcționa sistemul de operare DR-DOS. Securitatea nu era însă totală. Printre golurile de securitate ale acestui sistem de operare se pot enumera două mai importante:

- *fişierele protejate de parole puteau fi citite pe alte calculatoare pe care rula un alt sistem de operare;*
- *folosirea unui editor de disc elimina protecția. Câtă lume se pricepea însă la acea dată să folosească un editor de disc?*

Sistemele de operare de la Microsoft au introdus folosirea parolelor de abia la sistemul de operare Windows. Şi atunci când au fost implementate au constituit deliciul crackerilor prin modurile uşoare prin care puteau fi ocolite sau sparte. Sunt bine cunoscute golurile de securitate ale sistemelor de operare de tip Windows 9x. Dar firma Microsoft a introdus şi protecția la nivel de fişier. Suita de aplicații MS Office permite protejarea cu ajutorul parolelor la nivel de fişier. Mai nou, MS Office System permite chiar protecția la nivel de porțiune de text în MS Word sau celulă MS Excel.

Soluția folosirii parolelor pare simplă. Oricine a auzit şi ştie de parole. Orice utilizator va putea, beneficiind de facilitățile sistemului de operare sau de alte programe specializate, să-şi protejeze datele. Numai că trebuie luate în considerare anumite cerințe. De exemplu, nu trebuie protejate prin parole, fără ca ceilalți utilizatori să cunoască parola, fişierele partajate din rețea.

→ *Cea mai importantă problemă o reprezintă, însă, alegerea parolei. O parolă scurtă şi intuitivă va fi uşor de ocolit. Crackerii se bazează în principiu, la inițierea unui atac, pe existența unor parole greşit alese sau slab protejate. Utilizatorii nu ştiu cum să-şi aleagă parolele sau nu sunt educați cum să-şi aleagă aceste parole. O parte din responsabilitate cade în sarcina angajatorului, iar o altă parte în cea a personalului însărcinat cu asigurarea securității. Alegerea parolei va fi detaliată în paragraful 4.5.2.*

Folosirea optimă a parolelor pentru asigurarea securității presupune alegerea adecvată a acestora sau generarea acestora cu ajutorul generatoarelor de parole.

În marea majoritate a lor, generatoarele de parole folosesc metode criptografice pentru a genera parole.

→ *Am testat „soliditatea" parolelor pe un număr de 20 de calculatoare care erau stații de lucru la firmă (firma supusă testului este o firmă de construcții – S.C. Apartamentul S.A. – şi dispune de 22 de calculatoare, din care două sunt servere). Testarea a fost efectuată înainte de implementarea măsurilor de securitate. După ce au fost implementate măsurile de securitate am procedat la o nouă testare.*

[51] SGBD – Sistemul de Gestiune al Bazelor de Date.

Direcţiile pe care am mers au fost pentru aflarea parolelor de:

- *Windows;*
- *screensavers;*
- *fişiere.*

Aflarea parolelor de Windows logon a fost posibilă doar atunci când utilizatorul este conectat, pentru versiunile de Windows 95/98/Me, şi atunci când utilizatorul este conectat şi are privilegii de Administrator, la versiunile de Windows NT 4/2000. La versiunea de Windows XP a fost posibilă descoperirea parolelor tuturor utilizatorilor. Comportamentul cel mai slab a fost al sistemelor de operare Windows 95, 98 şi Me. Ulterior, aceste sisteme de operare au şi fost înlocuite în cadrul firmei.

Aflarea parolelor de screensaver a constituit un obiectiv deoarece mulţi utilizatori folosesc parole destul de uşor de ghicit sau, şi mai rău, nu folosesc deloc parole, iar dacă le folosesc, perioada de timp de autoactivare a protecţiei ecranului este aşa de mare configurată încât facilitează folosirea calculatorului de către alte persoane în intervalul când utilizatorul de drept nu se află la post.

Aflarea parolelor de fişiere a vizat în special aflarea parolelor programelor de arhivare (ZIP, RAR, ACE, ARJ), dar şi a parolelor pentru aplicaţiile de birou MS Office (Word, Excel).

→ *Obiectivele fiind alese, mai rămânea să aleg uneltele de testare. Iniţial am testat cu mai vechile programe cunoscute de mine. Apoi am căutat „noutăţile" în domeniu. Surprinderea a fost mare să constat că spărgătoarele de parole au evoluat în acelaşi ritm (dacă nu chiar mai mult) cu tehnologia. O parte din programele de spart parole au fost dezvoltate cu scopul nobil de a reuşi să se recupereze datele dintr-un fişier protejat prin parolă de către un angajat uituc. O altă serie de programe au fost dezvoltate şi mai apoi răspândite cu ajutorul Internetului de către persoane răuvoitoare. Unele dintre aceste site-uri au chiar denumiri sugestive, cum ar fi http://www.password-cracker.com. Două au fost programele care mi-au captat atenţia: Advanced Windows Password Recovery (AWPR) şi Brutus. Versiuni gratuite ale acestora pot fi găsite la adresele din Internet http://www.elcomsoft.com/awpr.html pentru AWPR şi la http://www.hoobie.net/brutus pentru Brutus. Există şi versiuni pentru uzul personal sau versiuni mai complexe la care preţul variază între 50 de dolari şi 150 de dolari. Acestea au însă, faţă de versiunile gratuite, facilităţi suplimentare şi algoritmi mai rapizi pentru găsirea parolelor. Nu am folosit pentru testare dicţionare, ci numai „forţa brută" din cauza lipsei unor dicţionare de limba română.*

Aflarea parolelor de Windows 95/98/Me de pe calculatoarele locale a fost făcută instantaneu. Există programe (destul de multe) care încap pe o dischetă şi care introduse într-un calculator nesupravegheat pot dezvălui date importante despre cont si parolă. O perioadă mai mare de timp a necesitat aflarea parolelor de fişiere şi a parolelor de utilizatori din reţea. În funcţie de lungimea parolelor şi de complexitatea acestora, intervalele de timp au fost de la câteva secunde şi până la zeci de minute pentru fişiere, şi de la zeci de minute până la ore pentru utilizatorii din reţea. Pentru aflarea unei parole a unui utilizator din reţea, în condiţiile în care nu se face o testare, ci se efectuează o primă fază a unui atac, intervalul de timp total poate să ajungă la zile având în vedere că ţinta va opri calculatorul în afara orelor de program. Dar programele de spargere a parolelor au posibilitatea de a relua de unde au rămas.

→ *La finalul testului au rezultat următoarele concluzii:*

- *Trebuie schimbate sistemele de operare din cadrul firmei, deoarece nu oferă suficientă protecţie. Concluzie de aşteptat datorită folosirii sistemelor de operare Windows 95/98/Me care sunt cunoscute ca vulnerabile.*

- *Folosirea neadecvată a parolelor. Acestea nu numai ca sunt greşit alese, dar sunt folosite şi o perioadă mare de timp. În majoritatea cazurilor, parolele erau foarte scurte şi uşor de ghicit sau nu foloseau decât cifre şi litere.*
- *Schimbarea politicii în ceea ce priveşte folosirea parolelor. Parolele de utilizator erau alese de către acesta şi erau schimbate aleator. Parolele de screensaver erau scurte şi uşor de „citit" urmărind ce taste se apasă la introducerea acestora.*

→ *Implementarea unei politici de folosire adecvată a parolelor a generat discuții. Unii angajați s-au plâns de „complexitatea" parolei, de faptul că trebuie să o memoreze şi nu să o scrie şi de faptul că periodic trebuie să memoreze alta.*

2.2.4. Scanere şi utilizarea lor în testarea securității firmei

Scanerul este un program utilitar folosit pentru detectarea automată a punctelor slabe în securitatea unui sistem. Cu ajutorul scanerului, un utilizator va putea să verifice, local sau la distanță, punctele prin care se poate pătrunde într-un sistem şi ulterior să acopere aceste goluri de securitate. Dacă acest instrument este utilizat însă de o persoană răuvoitoare, care posedă cunoştințe avansate în domeniu, securitatea calculatorului țintă sau a sistemului va fi serios afectată. Construite inițial pentru a creşte securitatea, scanerele, ajunse de cealaltă parte a baricadei, pot crea serioase probleme în asigurarea securității.

Nu trebuie făcută însă confuzie între utilitarele de rețea şi scanere. **Un utilitar de rețea este un program folosit pentru investigarea unei singure ținte.** Un scaner va efectua automat operațiile pentru care a fost proiectat, în timp ce un utilitar de rețea va efectua numai operațiile dictate de un utilizator. O altă deosebire este aceea ca un scaner lasă de multe ori urme ale acțiunii lui, în timp ce un utilitar nu lasă urme.

Traceroute, **showmount**, **host**, **rusers** şi **finger** de pe platformele UNIX precum şi **Netscan Tools**, **Network Toolbox**, **TCP/IP Surveyor** de pe platformele Windows sunt utilitare de rețea.

Majoritatea scanerelor sunt folosite pentru a testa porturile TCP, adică acele porturi care folosesc serviciile TCP/IP.

Un scaner va trimite către țintă o serie de pachete şi va testa răspunsul la acestea. În funcție de răspuns se va alege o cale de atac.

Principalele atribute ale unui scaner sunt:

- capacitatea de a găsi un server, o rețea sau un calculator partajat în rețea;
- capacitatea de a determina ce servicii rulează pe acesta;
- capacitatea de a testa serviciile pentru a se determina eventualele vulnerabilități.

Un atac cu ajutorul scanerelor va avea mari şanse de reuşită dacă:

- este executat cu mare viteză;
- nu poate fi detectată locația atacatorului;
- programul de scanare este performant;
- este executat la momente de timp bine alese.

O scanare de porturi va trebui să fie executată cu mare viteză deoarece alocarea unui timp prea mare va putea fi sesizată. Pentru atacul la distanță, folosind rețeaua Internet, atacatorul trebuie să dispună de puternice resurse hardware şi de o lățime de bandă suficientă mai ales dacă se inițiază un atac asupra mai multor locații.

Atacatorul va trebui ca înainte de inițierea unui atac să-şi mascheze propria poziție. În caz contrar, va putea fi detectat. Pentru aceasta se folosesc programe de ascundere a identității. Aceste programe ascund adresa IP.

Un program performant folosit pentru scanare va aloca şi foarte puțin timp operației, va ascunde identitatea IP a atacatorului şi va culege rapid informațiile necesare unei intruziuni.

Momentele de timp bine alese pot să asigure o plajă mai mare de timp necesară efectuării uneia sau mai multor scanări. Aceste momente se aleg pe baza presupunerilor referitoare la personalul care deserveşte calculatorul țintă vizat. Momentele în care personalul este în pauza de masă sau la începerea şi terminarea lucrului, la început sau sfârşit de săptămână pot fi alese ca moment de scanare ştiut fiind că la acele momente atenția este mai redusă.

Atacul cu ajutorul scanerelor poate fi detectat uşor dacă calculatorul țintă dispune de capacitatea de înregistrare a activităților. Stoparea unui scaner poate fi făcută uşor cu ajutorul unui dispozitiv firewall.

Cele mai utilizate scanere sunt **NSS (Network Security Scanner)**, **Strobe**, **SATAN (Security Administrator's Tools for Analyzing Networks)**, **Jakal**, **IndentTCPscan**, **Xscan**, **Xsharez, Advanced Port Scanner, Super Scan, Angry IP Scanner.**

→ *În cadrul aceleiaşi firme am folosit scanerele pentru a detecta eventualele puncte slabe în securitate rețelei acesteia. O analiză detaliată este prezentată în paragraful 4.4. Testările au fost făcute pe situația existentă şi, ulterior, pe noua arhitectură. Arhitectura inițială era cea care genera cele mai mari probleme datorită blocajelor frecvente care se datorau resurselor partajate din rețea.*

→ *Ca obiectiv principal am dorit să găsesc resursele partajate în rețea. Ca obiectiv secundar am căutat să descopăr posibilele echipamente care generau blocajele. Programele de scanare cel mai uşor de folosit şi care au dat rezultatele cele mai concludente au fost Xscan, Super Scan si Xsharez. Combinația ideală este Xscan şi Xsharez. Aceste programe se găsesc sporadic la adresa de Internet http://www.tool-for.net. Xscan va determina adresa din rețea a resursei partajate, iar Xsharez va găsi parola de acces a acesteia. Ce este foarte interesant de remarcat e faptul că timpul necesar aflării parolei cu ajutorul programului Xsharez este cu mult mai mic decât cel necesar unui atac cu „forță brută".*

→ *În urma testelor au rezultat foarte multe calculatoare care aveau partajate foldere sau fişiere fără vreun rost anume decât acela de a schimba informații, iar unele dintre acestea nu aveau nici o legătură cu activitatea firmei. Utilizatorii, care aveau drepturi depline, partajau resursele locale după bunul-plac. În această situație am decis trecerea la un sistem de operare restrictiv. După această operație şi după schimbarea arhitecturii rețelei am testat periodic rețeaua şi calculatoarele. O analiză a conexiunilor a evidențiat faptul că blocajele care apăreau se datorau atât traficului generat de resurse partajate, cât şi folosirii unor echipamente cu probleme. Înlocuirea acestora a eliminat neajunsurile.*

2.2.5. Folosirea interceptoarelor de trafic pentru accesul la datele firmei

Interceptarea traficului dintr-o rețea constituie o altă cale de a sustrage informația.

Un interceptor (sniffer[52]) este o componentă, software sau hardware, proiectată să „asculte" şi să „captureze" informațiile vehiculate în rețea.

Nu trebuie să se facă confuzie între interceptoare de trafic (sniffer-e) şi programe utilitare de capturare a tastelor (key strokes). Utilitarele de captură a tastelor vor culege şi stoca toate tastele şi combinațiile de taste apăsate, ulterior urmând să fie analizate în vederea căutării de informații. Sunt folosite de regulă pentru capturarea parolelor. În schimb, interceptoarele vor captura traficul din rețea indiferent de protocolul folosit.

Un interceptor reprezintă o amenințare serioasă la adresa securității deoarece cu ajutorul acestuia se pot efectua următoarele operații:

- capturarea parolelor;
- capturarea informațiilor secrete;

[52] *Sniffer* – Interceptor.

- testarea vulnerabilității în alte rețele.

Pentru capturarea traficului trebuie îndeplinite anumite condiții:

- arhitectura rețelei să permită acest lucru;
- configurarea plăcii de rețea în mod neselectiv (promiscuous[53]).

Cel mai cunoscut mod de interconectare a calculatoarelor în rețea se realizează cu ajutorul tehnologiei Ethernet. Tehnologia Ethernet permite interconectarea calculatoarelor cu condiția ca acestea să posede componente hardware, cât şi software care să permită transportul pachetelor Ethernet. Cerințele hardware presupun existența unei placi de rețea (NIC[54]), a unui cablu de interconectare (sau altă modalitate) şi, evident, a unui calculator. Software-ul minim necesar se compune dintr-un driver pentru pachete Ethernet şi un driver pentru placa de rețea. Driverul de pachete Ethernet va asigura transportul informației în ambele sensuri şi are rol de legătura între placa de rețea şi protocolul Ethernet.

Setul de protocoale folosit poate fi TCP/IP, IPX/SPX sau alte protocoale.

Acestea funcționează pe o configurație de rețea uzuală (figura 19) întâlnită la majoritatea firmelor.

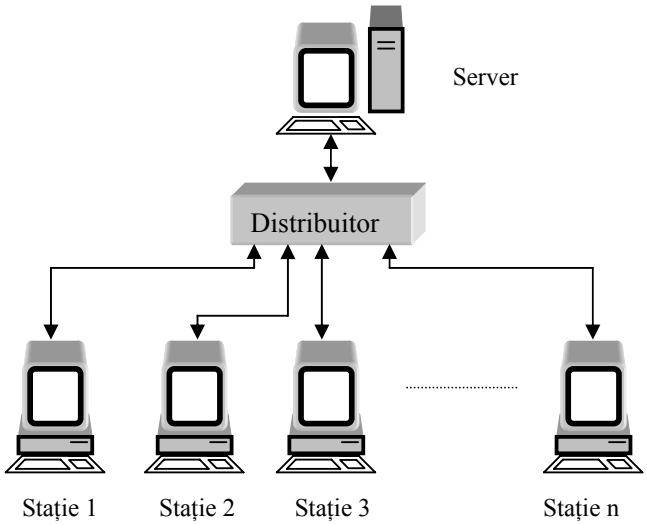


Figura 19. Configurație de rețea uzuală.

Atunci când trebuie trimis un mesaj către o anumită destinație din rețea, cererea este transmisă către toate interfețele, în căutarea destinației corecte. Dacă Stație 1 doreşte să trimită un mesaj la Stație 3, sau Stație 1 a emis o cerere către Server, atunci cererea Stației 1 şi răspunsul Serverului vor putea fi recepționate şi de celelalte stații, chiar dacă nu le sunt destinate. Acest mod de difuzare (broadband) este posibil doar în segmente de rețea şi nu este de dorit. Configurarea optimă a rețelelor şi subrețelelor poate ridica gradul de securitate prin interzicerea sau limitarea accesului interceptoarelor.

Ca şi în cazul scanerelor, interceptoarele au fost inițial proiectate ca dispozitive pentru diagnosticarea conexiunilor din rețea.

Amplasarea unui interceptor se face de regulă în următoarele puncte:

- în fluxul de date care provine de la un server;
- într-o rețea care are legătură cu altă rețea vizată.

[53] În rețelele locale (LAN), modul promiscuous este un mod de lucru în care fiecare pachet de date transmis de-a lungul rețelei va putea fi recepționat şi citit de oricare dintre adaptoarele de rețea. Acest mod este folosit pentru o mai bună monitorizare a activităților din rețea. Modul promiscuous este opus modului non-promiscuous. Când pachetul de date este transmis în mod non-promiscuous, toate adaptoarele de rețea pot „asculta" datele pentru a determina dacă adresa de rețea inclusă este identică cu cea proprie. Dacă este, atunci pachetul este recepționat.

[54] *NIC – Network Interface Card* – Placă de rețea.

În multe cazuri birourile firmei sunt amplasate în clădiri separate aflate la distanţă unele de altele. Interconectarea reţelelor din aceste clădiri presupune existenţa unor cabluri de legătură şi distribuitoare (hub, switch sau splitter) sau amplificatoare de semnal. Amplificatoarele de semnal pot fi eliminate dacă se foloseşte ca mediu de transmisie fibra optică în locul cablului standard de comunicaţie[55]. Pe aceste linii de comunicaţie şi dispozitive auxiliare se poate insera un interceptor (figura 20).

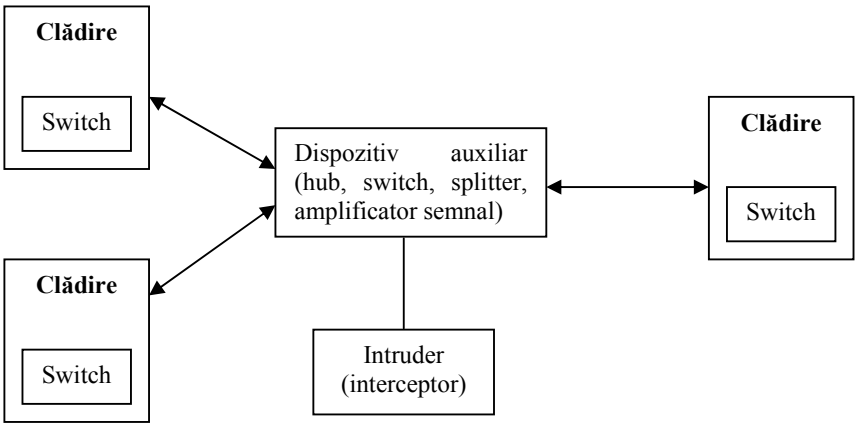


Figura 20. Amplasarea unui interceptor.

Plasarea unui interceptor într-o reţea este posibilă doar dacă:

- atacatorul a găsit un gol în sistemul de securitate;
- atacatorul este un angajat al firmei care doreşte să sustragă informaţie privată.

O dată pătruns printr-un punct în sistem, după ce a capturat parolele de acces, atacatorul va putea să sustragă, distrugă sau modifice date importante ale firmei, baze de date cu clienţi, furnizori, stocuri şi liste de preţuri, adrese şi conturi de e-mail etc.

Se consideră că atacul cu interceptoare este un atac de nivel doi.

Cele mai cunoscute programe interceptoare sunt: **Gobbler**, **ETHLOAD**, **Netman**.

Acţiunea unui interceptor nu poate fi evidenţiată.

Printre metodele folosite împotriva interceptoarelor se pot enumera:

- criptarea comunicaţiilor;
- folosirea unei topologii sigure.

→ *În cadrul firmei am încercat să găsesc un punct în care să pot plasa un interceptor. Cum toate calculatoarele se aflau în aceeaşi clădire, posibilitatea de a insera un interceptor era minimă. Am întâlnit însă şi firme care aveau clădirile separate, iar pe exteriorul unei clădiri se afla amplasat un hub care avea şi conexiuni libere. Singura posibilitate rămânea ca un eventual interceptor să fie amplasat undeva în interior. Verificarea traseelor cablurilor de legătură şi a dispozitivelor de conexiune a eliminat această variantă. O dată cu instalarea altor sisteme de operare, plăcile de reţea au fost configurate pe modul selectiv şi posibilitatea ca un atacator să poată captura traficul a fost eliminată. Toate aceste operaţii nu au implicat cu nimic personalul angajat.*

[55] Cablu BNC sau cablu torsadat.

2.2.6. Tehnica „Social Engineering" şi impactul acesteia asupra securităţii datelor firmei

Atacurile de tip social engineering folosesc natura umană pentru a putea să aibă acces la informaţii secrete. Ţintele acestor atacuri sunt de regulă oamenii creduli care fac parte din personalul angajat al firmei. Folosind liniile telefonice, e-mail-ul, Instant messaging sau Internet Relay Chat (IRC), atacatorul se va da drept membru al personalului IT&C din firmă sau din afară însărcinat cu întreţinerea echipamentelor de tehnică de calcul şi va cere de la un angajat al firmei contul şi parola pentru a face „diferite teste şi verificări". Sunt şi situaţii în care atacatorul se poate da drept un angajat care şi-a uitat contul şi parola personală şi „are nevoie urgent de date pentru şefu'". O dată trimise contul şi parola, atacatorul va avea drepturi de acces în sistem. Aceste tipuri de atacuri au mari şanse de reuşită în firmele care au personal numeros deoarece ţintele supuse atacului – angajaţii – sunt mai mulţi (posibilităţi mai multe) şi pentru că angajaţii nu cunosc personalul IT&C căruia îi pot furniza detalii. Într-o firmă mică sau medie, unde personalul are legături directe, aceste tipuri de atacuri, mai ales dacă se foloseşte linia telefonică, sunt mai greu de realizat, deoarece se poate ca angajatul să nu recunoască vocea celui care solicită datele referitoare la cont şi parola (atacatorul).

În majoritatea cazurilor, atacurile de tip social engineering folosesc o legătură directă – telefonul – pentru atingerea scopului propus.

Celelalte medii folosite în acest scop – e-mail, Instant messaging sau IRC – pot fi deghizate în viruşi hoax. De regulă, se primeşte un mesaj care conţine cod maliţios şi care solicită (re)verificarea contului şi a parolei pentru diferite aplicaţii sau cele de logare. O dată efectuate acestea, programul maliţios va trimite datele către atacator şi în acest fel contul şi parola au fost compromise. În alte situaţii pot fi primite mesaje sau se pot afişa ferestre ecran care să avertizeze că trebuie schimbate contul şi parola deoarece sunt „slabe".

Aceste atacuri nu au ca scop aflarea doar a contului şi a parolei de log-are în sistem, ci se adresează şi aflării datelor de acces la conturile bancare sau cărţile de credit.

În anumite situaţii, efortul depus de atacatori pentru furtul informaţiilor ajunge până acolo încât folosesc metode tradiţionale pentru a afla conturi şi parole. Una dintre metode presupune consultarea documentelor aruncate la coşul de gunoi. Este bine ştiut că angajaţii îşi notează contul şi parola pe hârtii sau bilețele, după care le memorează şi aruncă hârtiile la coş fără să le distrugă. Mai gravă este situaţia în care contul şi parola sunt scrise pe bilețele şi lipite la vedere sau sunt direct scrise pe monitor sau pe birou.

Studiile făcute arată că, în cadrul firmelor mari, sunt necesare 5 (cinci) zile pentru ca un atac de tip social engineering să aibă succes. Tot aceste studii arată că este practic imposibil de protejat împotriva atacurilor de tip social engineering. Cele mai eficiente măsuri privesc educarea personalului şi stabilirea unor reguli stricte de comunicare.

→ *În cadrul firmei studiate, tehnica „Social Engineering" a fost aplicată iniţial pentru a se vedea cum răspund angajaţii la acest tip de atac. S-a vizat cu precădere aflarea contului şi a parolelor de log-are la server, a parolelor utilizator din programele Ciel, dar şi a unor parole personale folosite în documentele de birou şi care se aflau pe server. În toate cazurile, pentru cele 20 de posturi de lucru cu calculatoare ale firmei, au fost parţial dezvăluite majoritatea parolelor. Pentru a avea succes cu acest tip de atac, dar şi pentru a testa credulitatea unora dintre angajaţi, m-am prelevat de faptul că am fost „trimis de director să repar calculatoarele". Ulterior, după implementarea măsurilor de securitate, acest lucru nu a mai fost posibil. Aceasta nu înseamnă că nu mai poate fi iniţiat un astfel de atac. Cu trecerea timpului, angajatul mai uită din rigorile impuse şi devine mai permisiv cu acestea.*

2.3. Atacuri asupra bazelor de date

2.3.1. Particularități ale securității bazelor de date

O bază de date poate fi definită ca o colecție partajată de date, între care există relații logice, precum şi o descriere a acestor date, proiectată pentru a satisface necesitățile informaționale ale unei organizații.

Informațiile conținute în baza de date vor putea fi accesate de o mulțime de utilizatori. Accesul necontrolat al utilizatorilor poate crea neajunsuri în funcționarea sistemului. Aceste neajunsuri pot fi de la cele mai nesemnificative şi până la blocări ale accesului sau, mai grav, chiar pierderi de date uneori irecuperabile.

→ *Consider că atacurile asupra bazelor de date prezintă câteva particularități față de restul informațiilor din firmă, şi anume:*

- *bazele de date reprezintă marea masă a informațiilor cu care firma lucrează;*
- *bazele de date pot dezvălui informații private prin prelucrarea datelor publice.*

Firmele îşi stochează datele referitoare la activitățile lor economice în fişiere baze de date. Accesul neautorizat la datele din aceste fişiere poate compromite activitatea firmei. Persoanele sau firmele concurente interesate de activitatea firmei vor face tot posibilul să intre în posesia acestor informații. Vor merge până acolo încât acțiunile lor pot fi categorisite ca acțiuni de spionaj. Pentru a se evita asemenea riscuri, firma trebuie să ia o serie de măsuri.

Asigurarea securității bazei de date presupune interzicerea accesului neautorizat la date. Aceasta se realizează cu ajutorul unui set de măsuri de securitate umane, software şi hardware.

Ca primă măsură de securitate umană se poate constitui izolarea sistemului de calcul în încăperi în care accesul să fie permis după trecerea de niveluri de securitate cum ar fi legitimarea sau alte forme de identificare.

Securitatea software presupune ca, într-o primă fază, accesul atât la sistemul de calcul, cât şi la bazele de date să se facă numai pe baza unor parole de identificare şi a drepturilor utilizatorului respectiv. Se poate ține un jurnal al accesului la bazele de date, pe baza acestuia detectându-se încercările de acces neautorizat.

Accesul la înregistrările din baza de date se va face sub controlul strict al câtorva elemente care să prevină funcționarea defectuoasă a sistemului.

Administratorul bazei de date (**DBA**[56]) are în principal două sarcini în asigurarea securității bazei de date:

- defineşte regulile de acces la date;
- determină accesul la date.

Sistemul de gestiune al bazelor de date (**SGBD**) reprezintă un program care va interacționa cu baza de date, acesta având rolul de menținere a integrității elementelor bazei de date.

Nerespectarea cerințelor minime de securitate poate reduce la minimum avantajul lucrului cu baze de date, şi anume:

- partajarea accesului la informații;
- redundanță minimă şi controlată a datelor în sistem;
- consistența datelor;
- controlul accesului.

Dintre cerințele minime de securitate a bazelor de date se pot enumera:

- integritatea fizică a bazelor de date;
- integritatea logică a bazelor de date;
- integritatea fiecărui element care compune baza de date;

[56] *DBA – Data Base Administrator.*

- controlul accesului;
- identificarea utilizatorului;
- disponibilitatea.

Integritatea fizică a bazei de date presupune prevenirea distrugerii fizice a întregii baze de date. Integritatea logică a bazei de date impune ca fiecare element al bazei de date să fie protejat. Dintre formele de protecție cele mai sigure şi mai utilizate se numără operația de salvare periodică a datelor (backup).

Integritatea fiecărui element care formează baza de date este asigurată de sistemul de gestiune al bazelor de date în următoarele trei moduri [HSST95]:

- verificarea câmpurilor;
- controlul accesului;
- schimbarea „log"-ului.

Valoarea fiecărui câmp va putea fi scrisă sau schimbată numai de utilizatorii autorizați şi numai dacă sunt valori corecte.

Integritatea fiecărui element este foarte importantă de asigurat mai ales atunci când sistemul de calcul eşuează la o operație de modificare a datelor. Atunci pot apărea două situații:

- numai o porțiune din câmp a fost modificată, restul rămânând nemodificat;
- la actualizarea mai multor câmpuri când erorile de actualizare sunt prezente la mai mult de un câmp.

Pentru a se preîntâmpina aceasta, modificarea/actualizarea se va face în două faze:

- faza de intenție;
- faza de înregistrare.

Faza de intenție presupune ca SGBD-ul să culeagă informațiile şi resursele necesare pentru actualizare. Nu se face nici o modificare în baza de date.

Faza de înregistrare se face modificând mai întâi indicatorul (flag) de scriere după care SGBD-ul face modificările permanente.

Dacă sistemul eşuează în timpul fazei a doua, baza de date va conține date incomplete, dar acest lucru poate fi remediat prin reluarea fazei a doua.

Controlul accesului se face ținând cont de restricțiile administratorului bazei de date. SGBD-ul va aplica politica se securitate a administratorului bazei de date (ABD). De asemenea, controlul accesului se va face ținând cont de accesul asupra datelor care vine din partea sistemului de operare sau din partea aplicației care lucrează cu baza de date.

Sistemul de operare lucrează cu fişiere, şi nu cu înregistrări din acestea, care la o primă vedere par să nu aibă nici o legătură între ele. Din acest punct de vedere, dezvăluirea de date senzitive este mai puțin probabilă.

Spre deosebire de sistemul de operare, programul care interacționează cu înregistrările din baza de date, cu valorile de câmpuri din anumite înregistrări poate dezvălui date senzitive.

Este mai uşor de implementat o listă de acces pentru un număr foarte mare de fişiere decât o listă de acces la elementele unei baze de date.

Identificarea utilizatorului va permite în orice moment să se ştie cine ce face în sistem. Toate operațiile efectuate de utilizatori vor fi stocate şi vor forma un istoric al accesului. Verificarea istoricului tuturor accesărilor este uneori greoaie şi necesită un volum de muncă considerabil. De asemenea, pot apărea şi raportări false ca în cazul în care s-a accesat un câmp, dar valoarea acestuia nu a fost afişată.

Regulile de autentificare ale SGBD-ului rulează peste cele ale sistemului de operare.

Un principiu de bază al securității datelor spune că trebuie să fim suspicioşi la orice informație primită.

Disponibilitatea va permite arbitrarea unei cereri în care doi sau mai mulți utilizatori solicită accesarea aceleiaşi înregistrări.

2.3.2. Senzitivitate şi afişări senzitive în cadrul datelor firmei

Datele care nu pot fi făcute publice poartă denumirea de date senzitive. O dată senzitivă va fi disponibilă numai persoanelor autorizate.

Factorii care fac ca o dată să fie senzitivă sunt [HSST95]:

- sunt date inerent senzitive;
- provin dintr-o sursă senzitivă;
- sunt declarate senzitive;
- atribute sau înregistrări senzitive;
- sunt senzitive în relație cu datele anterioare.

Dintre tipurile de afişări ale unor date senzitive avem:

- date exacte;
- date aproximative;
- date negative;
- date existente;
- date probabile.

Afişările datelor exacte permit chiar afişarea datelor cerute. Şi aceasta în condițiile în care datele respective trebuiau să fie ascunse unei cereri neautorizate.

O altă situație este aceea în care se afişează o valoare apropiată de valoarea exactă a datei. Afişarea acestor date depinde de context. Datele afişate pot fi benefice sau, în funcție de context, răufăcătoare.

Rezultatele negative apar în urma unor cereri deghizate în cereri inocente.

Dezvăluirea existenței unei date (a existenței unui câmp într-o tabelă) poate fi senzitivă.

În anumite situații se pot determina rezultate senzitive prin combinarea sau aplicarea de relații între datele afişate.

→ *În cadrul firmei supuse testului am încercat să obțin date senzitive din baza de date cu salariați. Am avut la dispoziție date parțiale din programul de salarii folosit la firmă. De asemenea, datele nu au fost actuale, motivându-se faptul că salariile sunt secrete. Structura tabelei este următoarea* (figura 21):

```
Structure for database: C:\SALA\SALA.DBF
Number of data records:        11
Date of last update    : 10/02/02
Field  Field Name  Type        Width    Dec
    1  NUME        Character      30
    2  SEX         Character       1
    3  STUD        Character       1
    4  SALB        Numeric         8
    5  SANC        Numeric         1
    6  COMP        Character       1
** Total **                       43
```

Figura 21. Structura bazei de date de personal supusă testului.

Legenda:

Denumire câmp		**Explicație**
NUME	-	Denumire persoană
SEX	-	Sex
STUD	-	Studii (**L**-liceu, **P**-postliceale, **S**-superioare)
SALB	-	Salariu brut
SANC	-	Sancțiuni (0-Nu, 3-Da, multe)
COMP	-	Compartiment lucru (**C**-comercial, **F**-financiar, **P**-producție)

Cele mai puțin senzitive date sunt: ***NUME.*** *Cele mai senzitive date sunt:* ***SALB***, ***SANC.*** *În anumite situații şi câmpul* ***NUME*** *poate să fie o dată senzitivă dacă cineva caută o anumită persoană.*

Popularea tabelei cu înregistrări este următoarea (figura 22):

Figura 22. Popularea cu înregistrări a tabelei SALA.DBF.

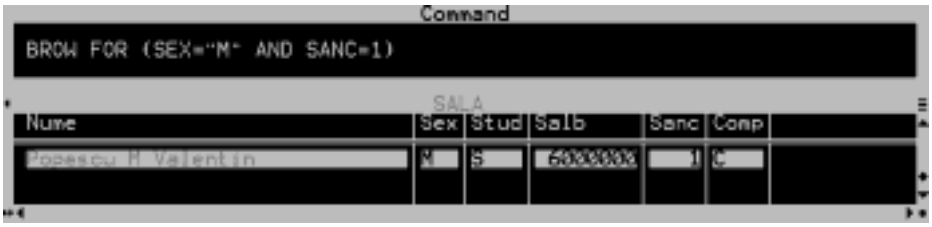
Vom exemplifica pe tabela anterioară câteva tipuri de atacuri.

Atacul direct

→ *Aplicăm un atac direct asupra tabelei de mai sus.*

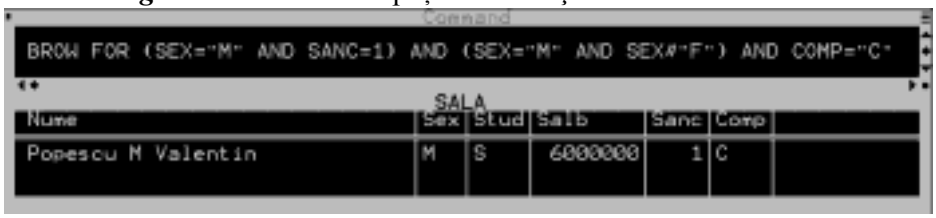
Vom folosi pentru început un atac evident de forma şi rezultatul acestuia exemplificate în figura următoare (figura 23):

Figura 23. Atacul direct şi rezultatul acestuia.



Vom folosi acum un atac mai puțin evident de forma şi rezultatul acestuia exemplificate în figura următoare (figura 24):

Figura 24. Atacul mai puțin evident şi rezultatul acestuia.



Se observă că doar condiția (**SEX**=„**M**“ AND **SANC=1**) *este cea reală după care se face sortarea, celelalte fiind puse pentru derutare.*

Acest tip de atac este posibil datorită faptului că atacatorul vede toate câmpurile din baza de date. O modalitate de a preîntâmpina acest tip de atac este ca atacatorul să nu vadă decât porțiunile nesenzitive din baza de date. Acest lucru se poate face prin aplicarea de vederi ale bazei de date.

Atacul indirect

→ *Acest tip de atac se execută atunci când nu se afişează decât date sumare despre angajaţi (în cazul de faţă doar numele şi compartimentul la care lucrează). Căutăm să determinăm numărul de persoane de la fiecare compartiment şi eventual salariile unora dintre aceştia.*

Aplicăm acum un atac indirect cu funcţii de următoarea formă (figura 25).

Figura 25. Atacul indirect folosind funcţia SUM condiţionat.

Rezultatele centralizate sunt următoarele:

	C (comercial)	**F** (financiar)	**P** (producţie)	**Total**
M	6.000.000	14.800.000	5.500.000	26.300.000
F	11.500.000	6.400.000	15.600.000	33.500.000
Total	17.500.000	21.200.000	21.100.000	59.800.000

A ieşit în evidenţă faptul ca la compartimentul Comercial şi la compartimentul Producţie să lucreze o singură persoană de gen masculin care să aibă salariile respective[57]*. De asemenea, la compartimentul Financiar există o singură persoană de genul feminin care are salariul de 6.400.000 lei. Analizând în continuare, se poate trage concluzia că la toate cele trei compartimente este posibil să existe două situaţii, şi anume* (tabelul 9):

- *să existe o singură persoană de gen masculin, respectiv feminin, care să aibă un salariu mare;*
- *să existe cel puţin două persoane care să aibă salariile mici în aşa fel încât suma lor să fie cea indicată.*

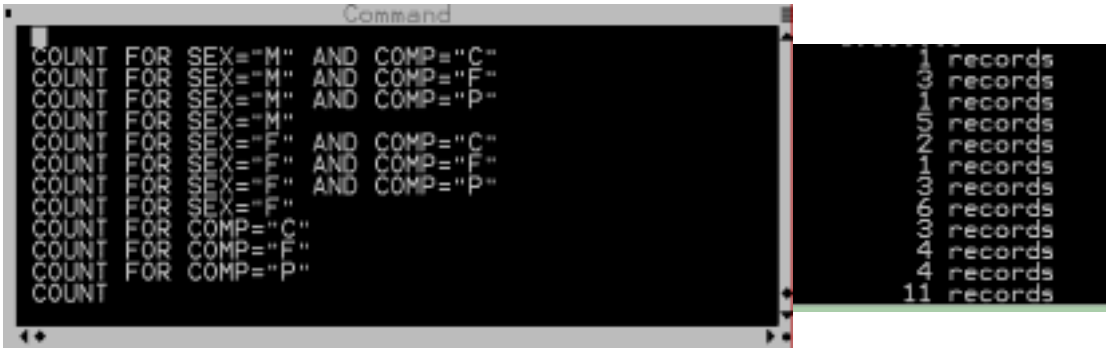
Tabelul 9. Evidenţierea rezultatelor la un atac indirect.

NUME	SEX	STUD	SALB	SANC	COMP
Popescu M Valentin	M	S	6000000	1	C
Ionescu A Stelian	M	P	5500000	0	F
Grigore A Marcela	F	L	3500000	0	P
Georgescu P Ion	M	P	3900000	3	F
Simion I Janina	F	S	5100000	1	C
Tanase A Loredana	F	S	6000000	0	P
Alexe A Virgil	M	S	5500000	3	P
Gherase I Mihaela	F	P	6400000	2	C
Constantin I Iulia	F	S	6100000	1	P
Ilie G Ioana	F	L	6400000	2	F
Alexandru A Silviu	M	S	5400000	1	F

[57] S-a luat în considerare nivelul salariilor din anul 2002.

Continuăm atacul şi încercăm să determinăm numărul de persoane de la aceste compartimente. Aplicăm funcţia COUNT condiţionat care are ca afect afişarea numărului de persoane de la compartimentele respective (figura 26). *Aceleaşi date au fost generate şi la folosirea funcţiei SUM care afişează atât suma cerută, cât şi numărul de înregistrări din care a fost calculată aceasta.*

Figura 26. Atacul indirect folosind funcţia COUNT condiţionat.



Rezultatele centralizate sunt următoarele:

	C (comercial)	**F** (financiar)	**P** (producţie)	**Total**
M	1	3	1	5
F	2	1	3	6
Total	3	4	4	11

Rezultatul afişat este de fapt cel intuit. Aceste atacuri destul de simple nu au făcut decât să evidenţieze cât de repede se pot determina anumite date senzitive din interiorul firmei doar pe baza datelor publice. Aceste tipuri de atacuri au mai mari sorţi de reuşită dacă numărul de înregistrări este redus. În cazul tabelelor complexe în care numărul de înregistrări este mare ne putem folosi de mai multe câmpuri pentru a extrage date senzitive.

În anumite situaţii mai complexe se pot folosi interogări cu ajutorul funcţiilor statistice implementate de SGBD-uri mai performante.

La acest tip de atacuri se poate răspunde cu una dintre metodele de aproximare a rezultatelor sau combinarea rezultatelor. Se poate de asemenea aplica şi metoda de suprimare a cererilor care se bazează pe situaţii când rezultatul la o cerere senzitivă este 1 (unu) (Capitolul 4).

Atacul prin urmărire

→ *Aplicăm un atac asupra unei baze de date care are implementat un mecanism de suprimare a cererilor care au rezultate dominante. Vom interoga baza de date cu un set de cereri şi vom studia răspunsul la aceste cereri, urmând ca din acestea să vedem unde sunt datele senzitive. Acest tip de atac este folosit împotriva bazelor de date care au răspunsuri scurte la interogări. Atacul se bazează pe principiul conform căruia dacă o interogare directă are ca rezultat un număr mic de răspunsuri, negarea cereri iniţiale va avea rezultat zero.*

Aplicăm un atac de acest tip asupra aceleiaşi tabele.

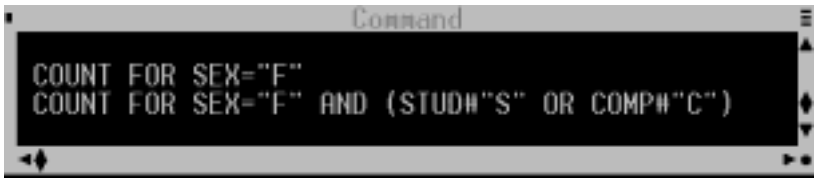
Vom interoga tabela cu următoarea expresie:

Interogarea va fi refuzată deoarece o înregistrare (a cincea) este dominantă.

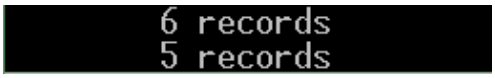
Împărțim interogarea în două părți care vor avea două rezultate la aceste cereri. Apoi vom extrage datele senzitive din cele două interogări:

Q = count (**a** and **b** and **c**) care este echivalent cu:
Q = count (**a**) – count (**a** and not (**b** and **c**)), unde:
a → SEX=F
b → STUD=S
c → COMP=C

Interogarea Q va putea fi împărțită în două interogări q_1 *şi* q_2 *de următoarea formă:*



şi are ca rezultate:



$$Q = q_1 – q_2 = 6 – 5 = 1$$

Concluzia este că există o singură persoană de sex feminin cu studii superioare care lucrează la compartimentul Contabilitate. Deci pe baza datelor nesenzitive am putut determina o dată senzitivă (tabelul 10).

Tabelul 10. Răspunsul la atacul prin urmărire.

NUME	SEX	STUD	SALB	SANC	COMP
Popescu M Valentin	M	S	6000000	1	C
Ionescu A Stelian	M	P	5500000	0	F
Grigore A Marcela	F	L	3500000	0	P
Georgescu P Ion	M	P	3900000	3	F
Simion I Janina	F	S	5100000	1	C
Tanase A Loredana	F	S	6000000	0	P
Alexe A Virgil	M	S	5500000	3	P
Gherase I Mihaela	F	P	6400000	2	C
Constantin I Iulia	F	S	6100000	1	P
Ilie G Ioana	F	L	6400000	2	F
Alexandru A Silviu	M	S	5400000	1	F

Pe această bază se pot determina sisteme de ecuații liniare pentru determinarea datelor senzitive.

$$\begin{aligned}
q_1 &= c_1 + c_2 + c_3 + c_4 + c_5 \\
q_2 &= c_1 + c_2 + c_4 \\
q_3 &= c_3 + c_4 \\
q_4 &= c_4 + c_5 \\
q_5 &= c_2 + c_5
\end{aligned}$$

În majoritatea cazurilor de atac studiate am observat dezvăluiri senzitive atunci când în urma unei cereri se obțin rezultate singulare (o singură înregistrare). Se impune deci restricționarea cererilor care au ca efect rezultate singulare (Capitolul 4).