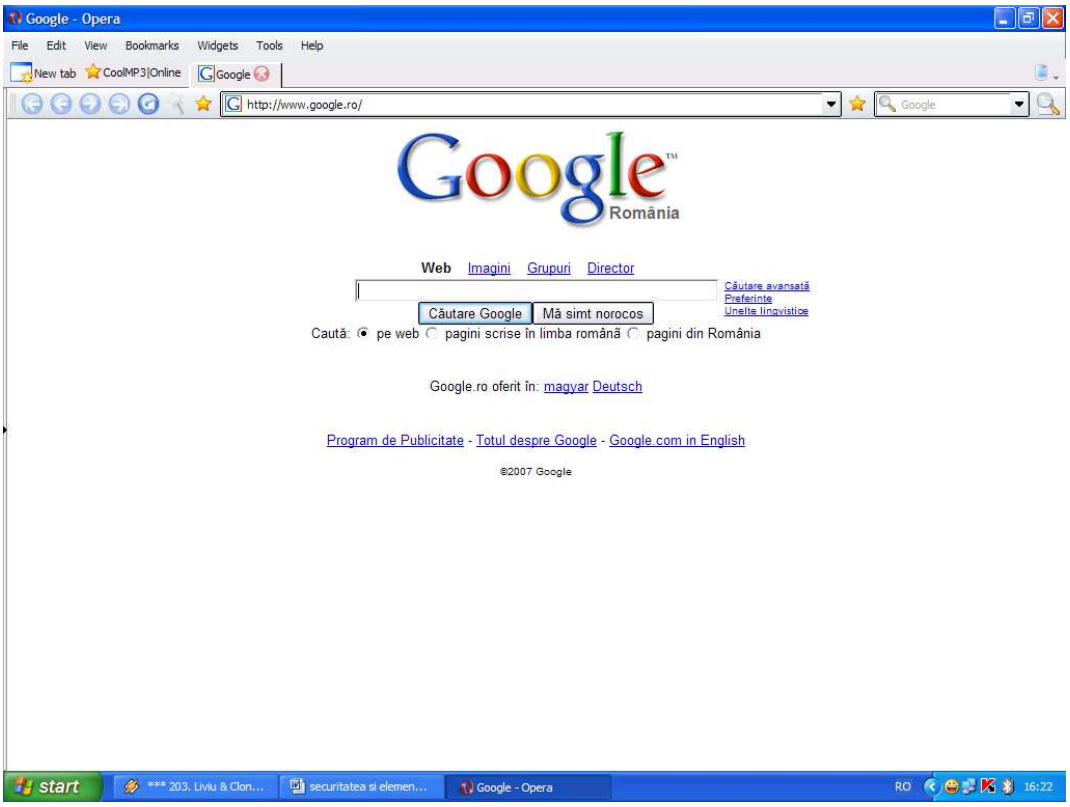
CUPRINS

INTRODUCERE

În perioada anilor'60, Departamentul de Apărare a Statelor Unite avea nevoie de o reţea de comunicare în cazul unui atac nuclear. RAND o corporaţie militară a propus centralizarea comunicaţiilor într-o reţea. Această reţea conţinea noduri capabile să transmită şi să primească mesaje. Fiecare nod îşi avea propria adresă astfel încât mesajul putea transmite un anumit nod.



Departamentul apărării pentru proiecte avansate (The Defense Department's Advanced Research Projects Agency) cunoscut sub numele de ARPA sau DARPA a decis să extindă această reţea. În anul 1969 primul "Interface Message Processor", predecesorul router-ului de azi a fost instalat la UCLA (University of California in Los Angeles) încât ARPANET-ul a început să se extindă. ARPANETUL include câteva servicii care sunt foarte importante în Internetul de azi, cum ar fi FTP-ul (File Transfer Protocol), remote login (TELNET) şi E-mail (electronic mail). În timp ce ARPANET-ul începe să crească, companii ca Xerox dezvoltă tehnologia reţelelor locale (LAN).

Reţeaua cu cel mai mult impact a fost Ethernet-ul, reţea ce permitea conectarea mai multor calculatoare impreună. Prima versiune avea teoretic o rată de transfer de 3 Mbps şi mai târziu 10 Mbps. Cercetatorii de la ARPANET au început să creadă că ar fi folositor să conecteze LAN-urile la ARPANET. Pentru a putea realiza acest lucru a fost dezvoltat un protocol pentru a putea conecta tipuri diferite de echipamente, TCP-ul (Transmission Control Protocol) şi Internet Protocol (IP). În 1983 creşterea Internetului a fost impulsionată de apariţia versiunii 4.2 BSD UNIX care conţinea si protocolul TCP/IP.

Internetul este o comunitate globală de reţele de calculatoare cu resurse informatice imense şi o gamă largă de servicii. În Internet sunt interconectate sute de mii de reţele, circa 130 mil. staţii de pe toate continentele. De serviciile acestuia se folosesc circa 400 mil.utilizatori.

Resursele Internet sunt constituite din:

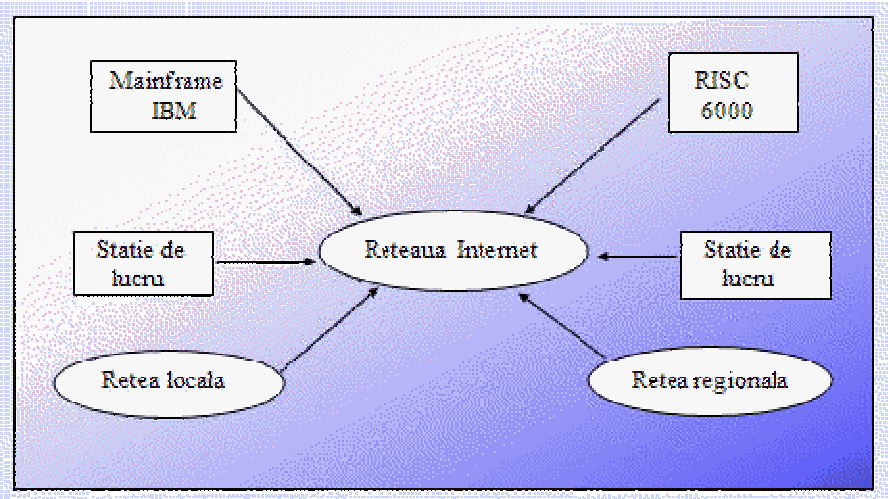
- servere-calculatoare-gazdă la care se stochează informaţii şi care prestează diverse informatice;
- sute de mil. de fişiere baze de date în cadrul serverelor cu informaţii din cele mai diverse domenii;
- Sub-sistemul de comunicaţii, ce asigură intercomunicarea şi transferul de date intre staţii.
- Accesul la resursele Internet se efectuează de la terminale sau calculatoare, conectate în reţea.Gama de servicii Internet se dezvoltă continuu, perfecţionându-se cele existente şi fiind împlementate altele noi.

La ele se referă:

- Teleconectarea, accesul la baze de date şi execuţia de programe la alte calculatoare;
- Teletransferul de fişiere dintre calculatare;
- Poşta electronică;
- Teleconversaţia în timp real, inclusiv teleconferinţa electronică;
- Difuzarea de ştiri;
- Insrumentare şi sisteme de căutare a informaţiilor.

Bogăţia informaţiilor, gama largă şi calitatea înaltă a serviciilor, simplitatea utilizării au atras atenţia savanţilor, profesorilor şi studenţilor, o poeticenilor, fabrcanţilor şi

furnizorilor de produse şi servicii a oamenilor de cultură.Internet a devenit un mediu puternic de instruire, cercetare şi activitattea de afaceri.



CAPITOULUL I

1.1.Internetul

Internetul, în cea mai simplă definiţie a sa, este o faimoasă reţea la scară mondială, alcătuită din milioane de calculatoare interconectate prin intermendiul unor standarde şi protocoale comune. Aceste protocoale şi standarde comune perimit utilizatorilor de pe tot globul să realizeze schimburi de informaţii, mesaje si programe, toate prin intermediul calculatorelor personale.

Conceptual vorbind, internetul este “o reţea a reţelelor”. Aceasta include un mare număr de reţele locale (LAN) aflate in cadrul unor instituţii comerciale, academice sau guvernamentale. O LAN este un grup de calculatoare fie interconectate unele cu altele, fie conectatae la un calculator central (server) fiecare calculator fiind amplasat în imediata vecinătate a celorlante calculatoare din reţea. Exemple de LAN sunt implementate în majoritatea firmelor de pe glob. În cadrul unei LAN, fiecare utilizator conectat la reţea dispune de un calculator de birou sau de un laptop.

Fiecare calculator din reţea are o placă de reţea care în funcţie de timeconfiguraţia calculatorului poate fi o componentă internă a sistemului sau este conectată la aceasta printr-un port de date de un anumit tip. Prin intermediul cablurilor sau a altor componente electronice, fiecare placă de reţea se conectează la un “server de reţea” care gestionează datele şi programele.

Pentru a întelege cum funcţionează Internetul, trebuie să inţelegeţi că Internetul nu este o entitate omogenă. Într-adevăr este un mare miracol că totuşi funcţionează. Internetul are o structură, astfel încât dacă vrei să trimiţi un E-mail la calculatorul vecinului mesajul trebuie să strabată sute de mile. Mai mult chiar, maşinile care sunt conectate nu au fost construite să comunice direct între ele. Şi totuşi Internetul funcţionează.

Internetul este un fel de bază de date gigantică, răspânditã la nivelul întregii lumi, în care poţi gãsi informaţii şi servicii de toate tipurile, accesabile de la orice calculator conectat la reţea. De acasã sau de la serviciu, de la liceu sau de la facultate, pornind un

calculator şi formând doar un număr local de telefon ne putem conecta la cel mai mare sistem informatic din lume.

Datoritã Internetului utilizatorul are acces la urmãtoarele servicii:

-Comunicare**.** Utilizatorii pot comunica între ei prin scris sau chiar prin vorbit. Pot trimite mesaje sau participa la dezbateri care îi interesează.

-Informare**.** Utilizatorul are acces la fişierele cu informaţii stocate pe serverele din reţea (informaţii despre artă, galerii, muzee…).

-Transfer de fişiere. Utilizatorul poate copia pe calculator fişiere de pe alte calculatoare. Aceste fişiere pot conţine programe pentru jocuri, muzicã, pentru utilizarea mai eficientã a Internetului, copierea fãcându-se gratuit sau contra cost.

-Acces la distanţã. Utilizatorul are acces la un alt calculator de la distanţã şi îl poate utiliza ca pe propriul calculator.

-Servicii comerciale**.** Utilizatorul poate folosi unele calculatoare din reţea pentru a face cumpărături, pentru a afla diferite informaţii utile (orarul trenurilor, al avioanelor), pentru rezervarea biletelor, pentru a primi diverse sfaturi (economice, medicale…).

-Poşta electronicã**.** E-mail. Utilizatorul poate folosi reţeaua Internet pentru a coresponda prin mail-uri (scrisori electronice)

1.2.Parafocuri(firewall)– descriere si mod de utilizare

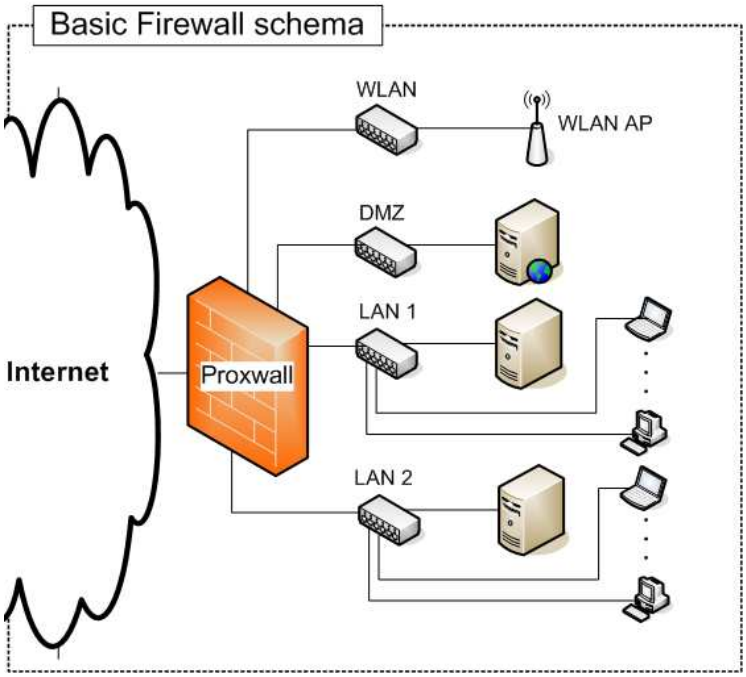
La conectarea reţelei la Internet, fundaţia sistemului de securitate trebuie să fie asigurată de un parafoc (firewall). Un parafoc este un instrument care face diferenţa dintre reţele protejate şi cele neprotejate şi in mai multe cazuri dintre regiunea protejată a unei reţele si o altă regiune (neprotejată) a aceleiaşi retele.

- Un parafoc combină elemente hard şi soft pentru protejarea reţelei împotriva accesului neautorizat.
- Parafocurile se folosesc în cadrul unei reţele pentru a aplica măsurile de securitate între departamenetele unei firme sau oraganizaţii.
- Un parafoc nu poate preveni pătrunderea viruşilor în reţea.

- Înainte de a proiecta un parafoc, este necesară dezvoltarea unui plan de asigurare a securităţii care să stabilească gradul de acces al angajaţilor şi al persoanelor din afara firmei.
- Cele trei tipuri principale de parafocuri sunt de nivel de retea, de nivel de aplicaţie şi si de nivel de circuit.
- Cele mai populare arhitecturi de parafocuri sunt: parafoc de host dual (dual-homed host firewall), parafoc de host ecranat şi parafoc de subreţea ecranată.
- Un ruter de ecranare poate filtra şi elimina pachetele care ajung într-o reţea.

Ruterele de ecranare în sine nu reprezintă o măsura de protecţie suficient de sigură.

Termenul *firewall* (zid de foc, zid de protecţie) are mai multe sensuri în funcţie de implementare şi scop. Firewall-ul e o maşină conectată la Internet pe care vor fi implementate politicile de securitate. Va avea două conexiuni la două reţele diferite. O placă de reţea este conectată la Internet, iar cealaltă placă la reţeaua locală. Orice pachet de informaţie care vine din Internet şi vrea să ajungă în reţeaua locală trebuie întâi să treacă prin firewall. Astfel că firewall-ul devine locul ideal pentru implementarea politicilor de securitate de reţea şi pentru controlul accesului din exterior.



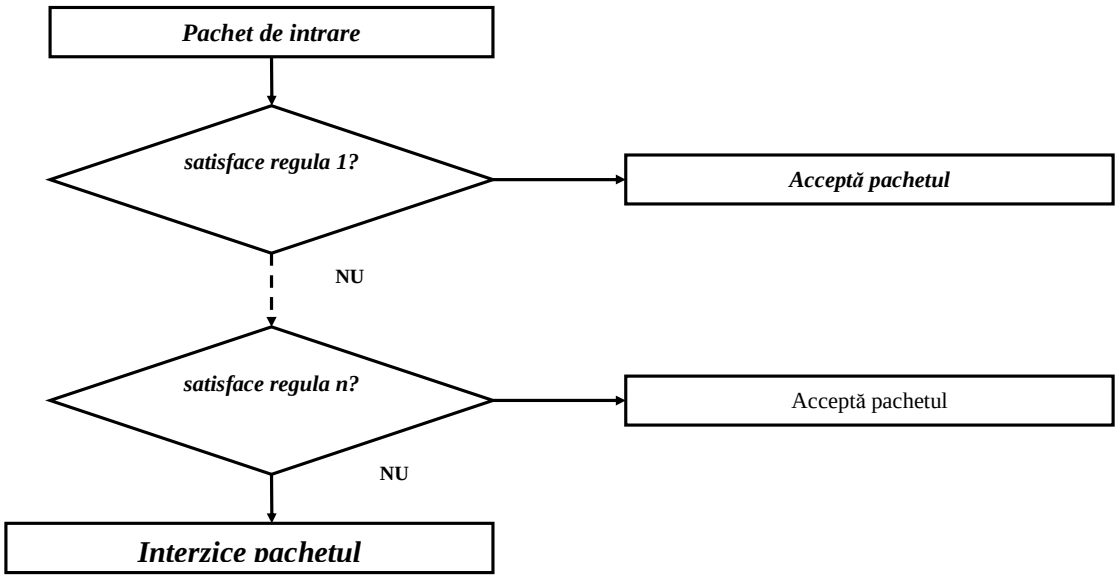
Politici firewall

O maşină firewall nu înseamnă nimic dacă nu sunt definite politici firewall. În genere, firewall-urile au două scopuri:

1. să ţină persoane (viermi/hackeri/crackeri) afară.
2. să ţină persoane (angajaţi/copii) înnăuntru.

Pentru un firewall există două moduri principale de abordare:

- Interzice totul in mod prestabilit şi permite explicit trecerea anumitor pachete .



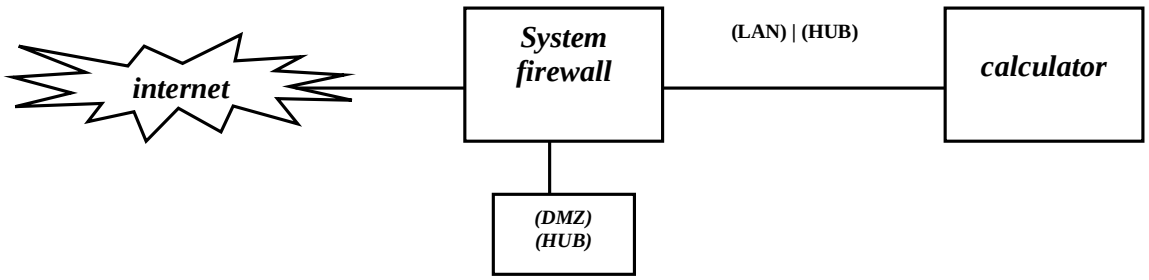
Crearea unei politici firewall este, în esenţă, destul de simplă:

- trebuie stabilit ce este permis să iesă din reţeaua locală, dar mai ales ce este permis să intre în ea (ce tipuri de pachete ?)
- trebuie stabilite serviciile pe care o să le ofere firewall şi la cine o să ofere aceste servicii
- trebuie descrise tipurile de atacuri potenţiale pe care firewall-ul trebuie să le oprească.

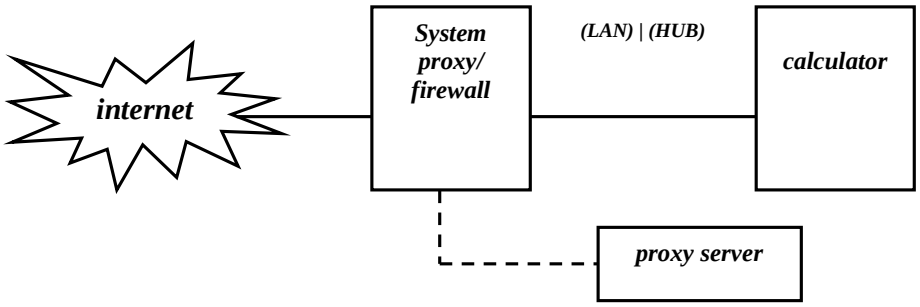
Tipuri de firewall-uri

Există două tipuri de firewall-uri:

1. Firewall-uri de filtrare – care blochează anumite pachete specifice



2. Servere Proxy – care stabilesc conexiuni de reţea în exterior pentru calculatoarele din interiorul LAN-ului

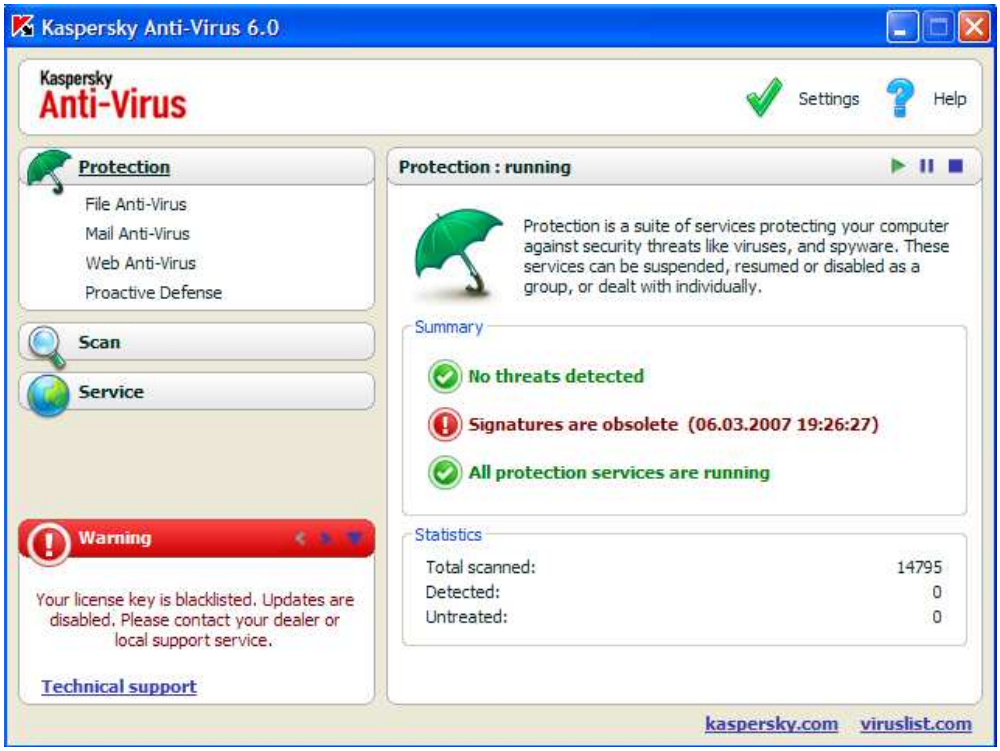


Un firewall de filtrare lucrează la nivelul reţea. Informaţia poate părăsi sistemul doar dacă regulile firewall-ului o permit. Când pachetele ajung la firewall ele sunt filtrate după tip, adresa sursă, adresa destinaţie şi număr de port, informaţii care sunt conţinute în orice pachet IP. Majoritatea routerelor de reţea oferă servicii de filtrare

De fapt firewall-ul este un fel de router. Pentru că foarte puţine date sunt analizate şi logate, firewall-urile de filtrare consumă mai puţin timp CPU şi creează mai puţine întârzieri pe reţea decât alte servicii de acest gen. Firewall-urile de filtrare nu suportă autentificarea prin parole. Un firewall identifică un utilizator doar după adresa IP de la care lucrează.

Printre avantajele firewall-urilor cu filtrare de pachete se numară şi următoarele: controlul traficului (dacă firewall-ul rulează pe gateway-ul spre alta reţea atunci acesta poate să permită (să lase să treacă) un anumit tip de trafic, pe când alt tip de trafic poate să-l oprească – se poate restricţiona, astfel traficul spre o anumită parte a Internetului sau a altei reţele exterioare), securitate sporită (când linux box-ul dumneavoastră este singurul paravan care stă între reţeaua dumneavoastră locală şi haosul din Internet, este o idee bună aceea de a restricţiona accesul din exterior la porturile dumneavoastră deschise – astfel, se poate permite accesul la reţeaua dumneavoastră locală numai din anumite locuri considerate sigure) ăi supravegherea reţelei (dacă o maşină prost configurată sau virusată din reţeaua dumneavostră locală începe să transmită la întamplare pachete în lumea exterioară este bine să ştiţi acest lucru şi să remediaţi situaţia).

CAPITOLUL II



2.1.Securitatea conexiunii la internet

Datele existente pe hard-discul unui calculator sunt de multe ori mai valoroase decât calculatorul însuşi, de aceea păstrarea lor în siguranţă trebuie să fie foarte serios avută în vedere. Pe de altă parte chiar dacă nu avem date importante pe harddisc infectarea calculatorului cu un virus informatic sau alt program de tip "malware" (prescurtare de la "malicious software", programe care fac rău, nocive) duce de cel mai multe ori la scăderea performanţei sistemului şi chiar la imposibilitatea de a rula unele programe.

2.1.1. VIRUŞII INFORMATICI

Internetul a devenit în ultimii ani mediul cel mai folosit pentru răspândirea de viruşi informatici. Cele mai multe contaminări ale calculatoarelor personale au loc prin ataşamente infectate ale unor mesaje de poştă electronică şi prin fişiere infectate descărcate de pe Internet.

Un virus informatic este un program care se caracterizează prin faptul că are un potenţial distructiv asupra calculatorului infectat. La fel ca şi viruşii biologici (gripă, etc.), cei informatici se pot "înmulţi" creând copii ale lor care pot infecta alte calculatoare. Contaminarea cu un virus informatic se face dacă lansăm în execuţie un fişier infectat (facem dublu click pe el). În acest fel virusul este activat şi işi va incepe acţiunea distructivă care poate varia foarte mult din punct de vedere al nocivităţii.

Unii viruşi folosesc calculatorul infectat doar pentru a se multiplica în vederea infectării altor calculatoare. Aceştia sunt de obicei numiţi "viermi" (worms) şi în această categorie se încadrează mulţi dintre viruşii care se transmit prin ataşamentele infectate ale unor mesaje de poştă electronică.

Cei mai mulţi viruşi au o acţiune nocivă care se declanşează instantaneu la deschiderea unui program infectat sau într-o anumită zi a anului. Acţiunea nocivă este variabilă, mergând de la modificarea sau ştergerea unor fişiere până la suprascrierea biosului calculatorului. Fişierele modificate sau şterse sunt alese cu grijă de autorul virusului în aşa fel încât calculatorul infectat să fie incapabil să îşi îndeplinească funcţiile într-o mai mică sau mai mare măsură. În general aceşti viruşi, infectează fişierele

executabile (cu extensia EXE, COM, BAT, PIF) dar există şi viruşi care infectează fişierele cu extensia DOC sau XLS create de aplicaţiile Word sau Excel ale suitei MS Office.

O categorie cu totul aparte sunt programele de tip "troian". Acestea funcţionează la fel ca un "cal troian" oferind acces la calculatorul infectat unei persoane care nu se află fizic lângă calculator. Astfel un calculator infectat cu un troian poate fi manipulat foarte uşor prin Internet putându-se face cu el toate operaţiile obişnuite (deschidere de programe, ştergere de fişiere, etc.) care însă se pot transforma în acţiuni distructive dacă se şterg fişiere de sistem sau fişiere importante depozitate pe calculatorul respectiv.

Înmulţirea cazurilor de infectare cu viruşi pe scară largă (adevarate "epidemii") a făcut să fie folosite din ce în ce mai mult mijloacele de contracarare a viruşilor. Şi în domeniul viruşilor informatici este valabilă afirmaţia că este mai bine să previi infecţia decât să o tratezi. La ora actuală există cel puţin o duzină de programe antivirus foarte bune care ne permit să evităm infectarea calculatorului nostru. Toate aceste programe sunt actualizate periodic pentru a ţine pasul cu viruşii nou creaţi. Multe plăci de bază cumpărate din magazin au pe CD un program antivirus (de ex. Trend PC Cillin) care este inclus în preţul plăcii. Există şi programe gratuite, de exemplu AntiVir PE sau AVG Free Edition . Cele mai bune programe antivirus sunt însă cu plată, exemple fiind Kaspersky Anti-Virus, McAfee Anti-Virus, Norton Anti-Virus sau BitDefender Anti-Virus (românesc). Alt antivirus românesc şi anume RAV a fost cumpărat de Microsoft şi va fi probabil inclus în viitoarele sisteme de operare Windows. Dacă vrem să comparăm antiviruşii existenţi putem să îi instalăm pe rând (de ex. de pe CD-urile unor reviste cu tematică IT) şi să ii punem la încercare.

Pentru a vedea dacă avem calculatorul infectat scanăm harddiscul cu ajutorul programului antivirus. Acesta conţine "semnăturile" (modificările specifice produse în fişierele infectate) celor mai răspândiţi viruşi într-o bază de date şi dacă pe parcursul scanării întâlneşte un fişier modificat de un virus ne atenţionează. La sfârşitul scanării vedem care sunt fişierele infectate şi putem lua măsuri de a eradica infecţia prin ştergerea sau "repararea" fişierelor afectate, ambele acţiuni putând fi făcute de soft-ul antivirus. De multe ori însă este imposibil ca fişierele afectate să poată fi "dezinfectate" corespunzator şi de aceea singura soluţie rămâne ştergerea. Cum viruşii pot afecta fişiere a căror ştergere poate duce la o funcţionare defectuoasă a sistemului de operare, uneori nu avem

altă soluţie decât să aplicăm măsura radicală de formatare a harddiscului. De altfel cea mai sigură metodă de a ne debarasa de un virus informatic este sa formatăm hardiscul şi să instalăm din nou sistemul de operare. Cum această operaţie ia destul de mult timp şi nu poate fi făcută de cei nefamiliarizaţi cu procedeul, cea mai bună metodă de a contracara acţiunea unui virus este să evităm cu orice preţ infectarea calculatorului.

Prevenirea unei infecţii se face din două direcţii :

Prima, şi cea mai importantă, este educarea utilizatorului unui calculator cu privire la viruşii informatici. Utilizatorul trebuie să scaneze cu un antivirus actualizat toate CD-urile sau dischetele pe care le foloseşte înainte de a lansa vreun program de pe acestea. De asemenea trebuie scanate toate fişierele descărcate de pe Internet sau ataşamentele primite prin poşta electronică.

A doua direcţie este instalarea unui program antivirus care să fie în funcţiune pe toată durata folosirii calculatorului. În acest fel ne asigurăm ca protecţia se păstrează chiar dacă alţi utilizatori ai calculatorului (de ex. copii) uită sa scaneze un CD sau o dischetă. Toate programele antivirus au un modul de scanare automată a fişierelor deschise în timpul unei sesiuni de lucru cu calculatorul. Dacă antivirusul detectează că un fişier infectat este pe cale de a fi deschis, fişierul respectiv nu va putea fi lansat în execuţie. Acest modul nu ocupă multe resurse ale calculatorului şi de aceea el nu deranjează funcţionarea altor programe. Foarte importantă este actualizarea "semnăturilor" virale din baza de date a programului antivirus care trebuie să se facă săptămânal sau lunar. Toţi antiviruşii moderni includ capacitatea de actualizare automată prin Internet.

2.1.2. PROGRAMELE SPION

Internetul a produs apariţia şi a unor programe care nu sunt viruşi informatici propriu-zişi, dar activitatea lor se desfăşoară fără cunostinţă utilizatorului calculatorului infectat şi este de cele mai multe ori de o nocivitate redusă. Aceste programe sunt denumite "spioni" (spyware) şi funcţia lor este aşa cum le-o arată şi numele să spioneze obiceiurile celor care utilizează calculatorul infectat. De exemplu, unele programe spion înregistrează într-o bază de date site-urile web vizitate şi apoi transmit prin Internet o listă cu adresele acestora.

Programele spion sunt de multe ori asociate cu unele programe gratuite (şi utile) care pot fi descărcate de pe Internet. Atunci când instalăm un program gratuit care ne trebuie este posibil să instalăm şi un program spion. Cei care beneficiază de pe urma programelor spion sunt de cele mai multe ori marile companii de publicitate prin Internet care culeg date despre internauţi, date pe care le folosesc pentru a-şi ajusta ofertele publicitare. Pentru ca aceste programe nu sunt de tip virus ele se află la limita legalităţii. Multe programe gratuite care au inclus în ele şi un program spion fac cunoscut acest lucru în termenii contractuali (licenţa de folosire a soft-ului) care apar la instalarea programului. Cum cei mai mulţi dintre utilizatori nu citesc acest text scris în jargon juridic programul spion este instalat alături de programul util. Programul spion rămâne de obicei pe calculator şi îşi indeplineşte funcţia chiar dacă dezinstalăm programul util pentru ca nu il mai folosim.

Pentru a vedea dacă avem pe calculator programe spion trebuie să instalăm soft-urile gratuite Ad-Aware sau SpyBot Search&Destroy. Acestea ne scanează calculatorul (fişiere şi registrul Windows) şi ne atrag atenţia dacă avem programe spion aflate în funcţiune, oferindu-ne şi posibilitatea să le ştergem. Trebuie să fim însă atenţi la faptul că

unele programe utile încetează să funcţioneze dacă este şters programul spion cu care sunt asociate.

2.1.3.PROGRAMELE CARE "DETURNEAZĂ" EXPLORATORUL

Ultimele programe apărute în lista de soft-uri "malware" sunt programele care "deturnează" exploratorul ("browser") . Numele acestor programe vine de la acţiunea de deturnare ("hijacking") a unui obiect de la scopul pe care trebuie să îl îndeplinească. Acţiunile acestor soft-uri nu sunt extrem de nocive însă sunt foarte supărătoare. Ele se instalează automat atunci când vizităm anumite pagini web şi nu devenim conştienţi de faptul că exploratorul a fost deturnat decât atunci când observăm ca pagina gazdă (principală) şi cea de căutare au fost modificate. Un alt semn clar al prezentei unui soft "malware" este faptul că exploratorul funcţionează foarte lent şi derularea paginilor mai mari se face sacadat.

Cele mai comune deturnări ale exploratorului sunt modificarea paginii principale ("home page") şi a paginii de căutare. În varianta obişnuită (imediat după instalarea IE) aceste două pagini se găsesc pe site-ul MSN al companiei Microsoft. Atunci când vizităm pagini web aflate în zone "mai intunecate" ale Internetului (de ex. site-uri pornografice sau cu soft piratat) este posibil ca unele din pagini să conţină nişte scripturi care modifică

automat configuraţia IE. Pagina principală a exploratorului şi cea de căutare sunt astfel schimbate cu alte pagini, de obicei publicitare.

Soluţia pentru situaţia de mai sus este la prima vedere foarte simplă. În prima etapă facem click pe meniul "Tools" în IE şi apoi pe comanda "Internet Options". Va apărea multifereastra cu acelaşi nume. Scriem din nou adresa paginii principale dorite de noi (ştergând-o evident pe cea apărută fără voia noastră) sau facem click pe butonul "Use Blank" şi apoi apăsăm butonul OK pentru a închide fereastra.

În a două etapa trebuie să reparăm toate modificările făcute de fişierele "malware" de pe calculatorul nostru cu ajutorul soft-ului gratuit "HijackThis". Îl lansăm pe acesta după instalare şi apăsăm pe butonul "Scan". Programul ne va afişa toate fişierele suspecte şi toate modificările suspecte făcute în registrul Windows. Modificările din registrul Windows care sunt responsabile de problemele apărute sunt dispuse de obicei în primele cinci rânduri din partea de sus a ferestrei programului.

Bifăm valorile din registru denumite HKCU...Search URL, HKCU...Search Bar, HKCU...Search Page, HKCU...Search Assisstant şi HKCU...Home OldISP care indică nişte adrese de pagini web publicitare (de ex. http://www.search-2005.com , http://sharempeg.com/find) şi apoi facem click pe butonul "Fix Checked". Va apărea o minifereastră de confirmare în care va trebui să apăsăm butonul "Yes". Dacă după terminarea operaţiei facem din nou click pe butonul "Scan" vom vedea că programul "Hijack This" a şters valorile din registru falsificate şi le-a restaurat pe cele corecte care indică nişte adrese de pe site-ul Microsoft (http://www.microsoft.com).

Cei care se ocupă cu soft-urile "malware" au găsit însa o variantă prin care acţiunea de mai sus nu mai este încununată de succes complet pentru ca de exemplu funcţia de căutare folosind bara de adrese a exploratorului este in continuare inutilizabilă. Aceasta se întimplă pentru ca a fost instalat pe calculator un fişier numit "hosts" în dosarul C:\Windows. Dacă il deschidem cu Notepad observăm că în el este scris de exemplu "66.250.171.136 auto.search.msn.com". Cu alte cuvinte în fişier se specifică o adresă IP greşită pentru pagina de căutare de la MSN. De câte ori vom încerca să căutăm ceva pe internet cu ajutorul motorului MSN (scriem un cuvânt în bara de adrese şi apăsăm tasta Enter) vom vedea că în loc de pagina cu rezultate de pe MSN va apărea o pagină web publicitară (de ex. http://www.martfinder.com). Va trebui să ştergem rindul "66.250.171.136 auto.search.msn.com" din fişierul "hosts" şi în acest fel motorul de

căutare MSN va putea fi folosit din nou direct din explorator. Fişierul însuşi poate fi şters de pe harddisc dacă el conţine doar rândul specificat mai sus iar acest lucru nu va cauza nici o problema în funcţionarea exploratorului, pentru că fişierul în cauză nu a fost instalat de Windows.

Un alt program foarte bun care ne ajută să prevenim deturnarea exploratorului este "Browser Hijack Blaster". Acesta trebuie lansat ori de cite ori explorăm Internetul şi el va rula în fundal împiedicând modificarea adreselor paginii principale şi a celei de căutare.

Mai multe informatii despre viruşii informatici pot fi găsite pe site-urile producătorilor de antiviruşi iar informaţii despre programele spion sau cele care deturnează exploratorul pot fi găsite pe site-ul SpywareInfo pe care se afla de asemenea şi un forum foarte util.

2.1.4.REALIZAREA DE COPII DE SIGURANŢĂ

Cea mai bună metodă de a ne pune datele importante la adăpost este crearea de copii de siguranţă, ceea ce ne permite recuperarea integrală a datelor chiar şi în situaţia în care o parte dintre ele au fost şterse sau corupte de acţiunea unui virus informatic.

Datele importante de pe harddisc trebuie arhivate periodic (şi eventual criptate) iar arhivele rezultate trebuie transferate pe medii de stocare pe care să le păstrăm la loc sigur. Cea mai indicată metodă este folosirea unităţilor de inscripţionare de tip CD-RW pentru crearea de discuri care să conţină datele pe care vrem să le punem în siguranţă. Evident, pentru stocarea unor cantităţi mici de date pot fi folosite şi dischetele.

O altă metodă sigură în cazul în care vrem să depozităm cantităţi importante de date este stocarea datelor pe Internet folosind un serviciu cu plată. Dacă avem doar câţiva MB de date importante putem folosi pentru stocarea pe Internet serviciile de tipul Yahoo Briefcase sau o parte din spaţiul oferit gratuit de serviciile de găzduire de site-uri web.

Este recomandat să stocăm datele importante în mai multe locuri, de exemplu stocare pe CD-ROM dar şi stocare pe Internet şi să le actualizăm regulat.

CAPITOLUL III

3.1.Prevenirea retelei cu virusi din internet

Pentru a preveni infectarea reţelei cu viruşi este necesară aplicarea a trei etape simple la toate informaţiile sosite din exterior.

Mai intâi se va folosi un program antivirus pentru a scana toate dischetele, fişierele, programele executabile şi anexele e-mail inainte de a le deschide pe un calculator din reţea.

În al doilea rand se va include protecţia antivirus ca o componentă a parafocului astfel incât fişierele infectate să nu poată intra in reţea. După cum s-a discutat în capitolul referitor la parafocuri practic toate produsele parafoc comerciale includ facilitatea de filtrare antivirus. Majoritatea parafocurilor include instrumente de detecţie a viruşilor, integrate şi complet adaptabile care pot preveni infectarea şi distrugerea datelor din calculator. În plus, conţin sisteme de asigurare a integrităţii care permit monitorizarea în timp real a modificărilor survenite în fişiere sau in sistem ca ansamblu. Informaţiile în timp real privind modificările pot contribui la stoparea imediată a oricaror viruşi care incearcă să infecteze sistemul. De asemenea, cele mai multe parafocuri furnizează protecţie care se extinde şi asupra sesiunilor DOS, astfel că utilizatorul nu poate fi luat niciodată prin surprindere.

În al treilea rând, se va instala un program de protecţie antivirus pe fiecare sistem de reţea, pentru a preveni transmiterea viruşilor de la un calculator infectat.

3.2.Elemente de etică, politica de securitate a Internetului

- fiecare configuraţie care include o reţea trebuie să-şi aibă propria politică de securitate;
- politica de securitate a fiecărei reţele trebuie să fie unică;
- pentru crearea unei politici de securitate este necesară interacţiunea între mai multe departamente şi personae individuale inclusiv factori de decizie, specialişti în domeniul informaţiei sau utilizatori obisnuiţi;

- o estimare a riscului implică determinarea proprietarilor sistemului şi a pericolelor potenţiale la care sunt expuse acestea.

- scopul de bază al unei politici de securitate îl constituie specificarea obiectului protecţiei şi mai puţin a modului de exercitare a protectiei.

3.3.Metoda de bază pentru dezvoltarea unei politici de securitate

Creearea unei politici de securitate se traduce prin dezvoltarea unui plan pentru rezolvarea aspectelor privind securitatea reţelei. Cu alte cuvinte se încearcă protecţia utilizatorului şi a reţelei inainte ca un haker sa reuşească să compromită sistemul.

1.Determinarea obiectivelor care urmează a fi protejate şi a caracteristicilor acestora. De exemplu, să presupunem că serverul de reţea conţine baze de date ale firmei. Prin determinarea modului de accesare a bazei de date, se poate lua decizia de protecţie a acesteia cu măsuri de securitate de nivel redus şi protecţie a întregistrărilor individuale cu măsuri de protecţie de nivel mai ridicat.

2.Determinarea factorilor umani si tehnici carora trebuie protejata reţeaua. Folosind exemplul anterior se poate opta pentru protecţia integrală a bazei de date împotriva furtului. De aseamenea, în funcţie de conţinutul bazei de date se pot proteja de exemplu, înregistrările fiecarui agent de vânzări împotriva accesului tuturor celorlalti agenţi de vânzari din cadrul firmei;

3.Determinare gradului de probabilitate a pericolelor. Dacă firma are caracter local şi zona de piaţă acoperită este redusă agenţii de vânzări neatenţi reprezintă un pericol mai mare decat hakeri externi.

4.Implementarea măsurilor de protecţie a reţelei într-o manieră eficientă. Securitatea parolelor înregistrările criptate şi parafocurile reprezintă exemple de măsuri de securitate eficiente.

5.Monitorizarea continuă a procesului şi îmbunătăţirea tuturor componeneteleor de asigurare a securităţii reţelei la fiecare aparaiţie a unui punct slab.

3.4.Stabilirea unei politici oficiale de securitate a calculatoarelor

Scopul urmărit în dezvoltarea unei politici oficiale de securitate a calculatoarelor este de a defini dezideratele firmei în ceea ce priveşte utilizarea corectă a calculatoarelor şi reţelei. De asemenea, politica de securitate trebuie să definească proceduri de prevenirea a indicelor de securitate şi proceduri care să specifice modul de reacţie la asemenea incidente, pentru a rezolva cele două aspecte, trebuie luate in considerare anumite caracteristici ale firmei atât înainte cât şi in timpul dezvoltării unei politici de securitate. La dezvoltarea politicii în sine se vor parcurge următoarele trei etape :

- Examinarea scopurilor şi direcţiei organizatiei. De exemplu, o bază militară va prezenta probleme de securitate sensibil diferite de ale unei universităţi, iar preocupările de securitate ale unei configuraţii comerciale diferă, de asemenea, atât de cele ale bazei miliare cât şi de cele ale universităţii.

- Dezvoltarea unei politici de securitate conforme cu regulile politice, regulamentele şi legile pe care le respectă organizaţia şi membrii acesteia. Pentru a asigura o conformitate completă cu regulile existente se impune identificarea acestora şi luarea în considerare a fiecărei în momentul dezvoltării politicii de securitate.

- Dacă reţeaua locală nu este complet izolată şi de sine stătătoare este necesară luarea în considerare a implicaţiilor securităţii într-un context global. Politica de securitate trebuie să conţină referinţe la probleme privind utilizarea de la distanţă a calculatoarelor. În această categorie de probleme intră modul de rezolvare a problemelor locale de securitate generate de un site îndepărtat, modul de rezolvare a problemelor care survin pe sisteme îndepartate ca rezultat al acţiunii unui host sau utilizator local, precum şi modul de a reacţiona la o pătrundere neautorizată a unui utilizator îndepartat. Crearea unei politici de securitate a reţelei nu este o problemă care să poată rezolva într-o dupa-amiază de sâmbătă. În realitate, la dezvoltarea unei politici de securitate se doreşte implicarea mai multor persoane cu diferite funcţii şi care lucrează în diferite departamente. Cu toate acestea, răspunderea finală privind crearea politcii de securitate trebuie să revină unei persoane sau a unui grup.

3.5.Securizarea si protejarea informatiilor normale si sensibile.

Înainte de acorda utilizatorilor acces la servicii, trebuie determinat nivelul securităţii datelor din sistem. Prin aceasta se determină nivelul de sensibilitate al datelor stocate de utilizatori. Nu este recomandată stocarea de informaţii sensibile pe un sistem care nu urmează a fi securizat corespunzator. Utilizatorii care pot stoca informaţii sensibile trebuie să ştie care sunt serviciile (dacă acestea există), corespunzatoare pentru stocarea acestor informaţii. Această componentă a politicii de securitate include stocarea datelor în diferite moduri (pe disc, pe bandă maganetică, pe servere de fişiere, etc). Politica aferentă acestei regiuni trebuie corelată cu politica referitoare la drepturile administratorilor de sistem şi ale utilizatorilor.

3.6.Stabilirea procedurilor de prevenire a problemelor de securitate

Politica de securitate defineşte ce anume trebuie protejat: ce este mai important, care sunt proprietăţile şi care este metoda generală de tratare a problemelor de securitate. Politica de securitate în sine nu indică *modul* de protecţie al elementelor; acesta este rolul procedurilor de securitate. Politica de securitate trebuie să fie un document de nivel înalt care trasează strategia generală. Procedurile de securitate trebuie să stabilească ăn detaliu măsurile exacte de protecţie a site-ului.

Politica de securitate trebuie să includă o estimare generală a riscului privind cele mai comune tipuri de pericole pentru site şi consecinţele acestuia (după cum s-a arătat în secţiunea “identificarea pericolelor“). Această informaţie este esenţială pentru conceperea unor proceduri eficiente sub aspectul costului.

Există tentaţia de a începe crearea procedurilor de securitate ale site-ului prin luarea de decizii referitoare la diferite mecanisme; de exemplu, afirmaţii gen “acest site va avea login pe toate hosturile, modemuri call-back şi plăci inteligente pentru toti utilizatorii”. Prin aceasta metodă se ajunge la diferite zone ca un volum exagerat de protecţie faţă de potenţiale riscuri şi la alte zone cu o protectie insuficientă. Politica de securitate şi riscurile pe care le descrie trebuie să asigure un nivel corect de protecţie pentru toate elementele reţelei.

3.7.Selectarea sistemelor de control pentru protejarea eficientă a componentelor

Dupa stabilirea componentelor care urmează a fi protejate şi estimarea riscurilor cu care se confruntă acestea, trebuie luată o decizie cu privire la implementarea sistemelor de control care protejează aceste componente. Este necesară selectarea mecanismelor de control şi protecţie care să contracareze în mod adecvat pericolele indentificate la evaluare riscurilor şi implementarea acestor mecanisme într-un mod eficient sub aspectul costului. Investiţiile excesive şi restrângerea bazei de utilizatori nu-şi au rostul în cazul unor riscuri foarte reduse. Următoarea listă prezintă unele aspecte care trebuie luate in considerare la selectarea sistemelor de control pentru reţea:

- **Setul de sisteme de control adecvat:** Sistemele de control selectate asigură prima şi principala linie de apărare pentru protecţia componenetelor sistemelor. Ca atare, trebuie să existe certitudinea că şi elementele de control selectate sunt potrivite pentru sistem. Dacă pericolul principal pentru sistem îl reprezintă pătrunderile din exterior, probabil că utilizarea de dispozitive biometrice pentru autentificarea utilizatorilor obişnuiţi ai sistemului nu are sens. Pe de alta parte, dacă pericolul esenţial este exploatarea neautorizată a resurselor sistemului de către utilizatorii obişnuiţi, este de dorit utilizarea unor proceduri automate de stabilire a conturilor extrem de riguroase.
- **Securitatea fizică:** În cadrul securităţii calculatoarelor, dacă un sistem nu este sigur sub aspect fizic, atunci nimic relativ la sistem nu mai este sigur; un intrus cu acces fizic la sistem îl poate opri, îl poate readuce în mod privilegiat, poate inlocui sau modifica discul. Este necesară amplasarea conexiunilor de comunicatie esenţiale, a serverelor importante şi a altor sisteme cheie în zone sigure din punct de vedere fizic. Unele sisteme de securitate (gen Kerberos) impun ca sistemul să dispună de siguranţa fizică. Dacă nu există posibilitatea de securizare fizica a sistemelor, se impune o atenţie sporită la credibilitatea acestor sisteme. Site-urile vor avea în vedere limitarea accesului de la sistemele nesigure la sisteme mai sigure. În particular, accesul credibil (realizat cu comenzile distante din UNIX,gen *rsh*) de la aceste categorii de host-uri este deosebit de riscant. Este necesară o grijă deosebită privind accesul la sistemele

pentru care se va asigura securitatea fizică sau care par sigure sub acest aspect. Se reţine că personalul de întreţinere are deseori cheile de la birouri.

3.8.Resurse internet referitoare la politicile de securitate

Ca şi pentru majoritatea subiectelor tratate în aceasta lucrare, există câteva site-uri Web excelente, referitoare la dezvoltarea şi implementarea unei politici de securitate în cadrul unei organizaţii.Aceste site-uri pot fi consultate, suplimentar faţă de RFC 1244, la dezvoltarea politicii de securitate a unei organizaţii.

CAPITOLUL IV

4.1.Protecţia transmisiunilor prin criptare

Până în acest moment, au fost prezentate elemmentele de bază privind proiectarea şi implementarea unei reţele, precum şi unele probleme esenţiale legate de securitatea reţelelor. După cum s-a aratat, calculatoarele trimit mesaje e-mail (majoritatea transmisiunilor TCP/IP) prin Internet sub forma de pachete. Într-o reţea interceptarea transmisiunilor repezintă unul dintre cele mai mari riscuri de securitate la adresa persoanelor fizice şi a firmelor. Pentru protecţia împotriva atacurilor prin interceptarea pachetelor, toate transmisiunile efectuate trebuie *criptate*. O transmisiune criptată este o transmisiune ce conţine date aşezate dezordonat, care pot fi reordonate numai prin aplicarea cheii criptografice corecte.

- Modul de realizare a unei criptări singulare folosind glisări alfabetice.
- Calculatoarele realizează criptarea prin multimplicarea şi împărţirea valorilor transmise cu numere mari, decriptarea fiind efectuată prin aplicarea unui număr mare corelat datelor transmise.
- Cele două tipuri esenţiale de criptare sunt *criptarea cu cheie unică,* cunoscută sub numele de *criptare cu cheie simetrică,* şi *criptare cu cheie publică,* sau *criptare cu cheie asimetrică.* Criptarea cu cheie unică foloseşte o singură cheie, partajată de ambele părţi şi folosită la criptare şi decriptare .Criptarea cu cheie publică foloseşte pentru criptarea şi decriptarea o cheie cunoscută disponibilă pe scară largă (cheia publică) şi o cheie pe care nu o cunoaşte nimeni cu excepţia utilizatorului (cheia privată).
- Două organisme de control al Internetului definesc regulile de bază ale criptării mesajelor în cadrul standardului Privacy Enhanced Mail (PEM)
- Majoritatea programelor de criptare folosite inclusiv popularul PGP (pretty Good Privacy-confidenţialitate acceptabilă) se conformează standardului PEM.
- La criptarea unui document, în mod obişnuit se criptează numai o porţiune a acestuia, cunoscută sub numele de esenţa mesajului.

- Hackerii pot descifra multe scheme de criptare moderne prin măsurarea timpului necesar pentru criptarea unui document
- Anumite locaţii WEB, cunoscute sub numele de inele de chei publice, conţin multe asemenea chei.

4.2.Utilizarea şi verificarea pistelor pentru detectarea şi anihilarea intruşilor

După cum s-a arăta în capitolele anterioare, hackeri pot folosi mai multe metode pentru a se infiltra în sistem şi a compromite date importante ale utilizatorului. Pistele de verificare (audit trails) asigură una dintre cele mai bune modalităţi de detecţie a unei posibile infiltrări a heckerilor. O pistă de verificare este o înregistrare semi-permanentă a sistemului de operare a unui calculator, referitoare la activităţile efectuate de utilizatori de acel calculator. Pistele de verificare sunt utile nu numai dupa apariţia infiltrării dar şi în timpul atacului. Vom discuta în detaliu despre diverse piste de verificare utile pentru îmbunătăţirea securităţii :

- O *pistă de verificare* (audit-trail) este o înregistrare a tuturor activităţilor, sau a unei submulţimi a acestora care survin de pe calculator.
- În general, pistele de verificare se vor concentra pe informaîii referitoare la accesul obiectelor interzise.
- Pistele de verificare pot fi folosite la nivelele ruter de ecranare sau parafoc pentru a alerta utilizatorul cu privire la potentiale atacuri.
- În funcţie de informaţia stocată de pe server, se pot folosi nivele diferite de verificare, cum ar fi verificarea la nivelul calculatorului (precizie redusă), verificare la nivel de director (precizie medie) s-au verificare la nivel de obiect (precizie ridicată).
- Pistele de verificare se pot folosi în urma unui atac pentru a determina pagubele potenţiale aduse sistemului de un hacker sau datele furate de acesta.
- Politica de securitate a unei organizaţii trebuie să includă întreţinerea, analiza şi efectuarea de copii de siguranţă pentru pistele de verificare.
- Chiar şi cele mai sigure sisteme sunt vulnerabile la utilizări eroante (pistele de verificare pot construi unica modalitate de detectare a unei activităţi autorizate, dar abuzive).

- Uneori, utilizatorii neautorizaţi determină căderea unui sistem, iar pistele de verificare vor determina identitatea întruşilor şi modul în care au procedat aceştia.
- Înlocuirea unor sisteme nesigure existente cu sisteme sigure este uneori prohibitivă sub aspectul costului. Cu toate acestea, urmăriea informaţiei de pe pistele de verificare este în general o metodă puţin costisitoare de asigurare a securităţii.

4.3.Securizarea reţelelor împotriva atacurilor antihacker

Datorită popularităţii crescânde a sistemului Windows NT, vom trata mai întâi problemele de securitate legate de acesta. Windows NT, chiar dacă a facut progrese semnificative în direcţia imbunătăţirii securităţii de la prima lansare, mai are încă breşe de securitate semnificative, pe care heckerii le pot exploata.

- Windows NT foloseşte un model de securitate bazat pe obiect, ceea ce înseamna că sistemul furnizează capacitatea de securizare a fiecărui fişier stocat in server
- Modelul de securitate Windows NT constă în patru componente*: autoritatea de securitate locală(Local Security Authority), managerul de securitate a conturilor (Security Account Manager-SAN), monitorul de referintă a securităţii (Security Reference Monitor-SRM) şi interfaţa utilizator (User Interface-UI).*
- Windows NT foloseşte protocolul Server Message Block (SMB) pentru gestiunea transmisiunilor.
- Sistemul de operare Windows NT are un nivel de interfaţă de securitate folosit pentru includerea de interfeţe de securitate multiple.
- Printre altele o reţea sigură impune prezenţa unui server singur din punct de vedere fizic.
- Pentru securizarea unei reţele Windows NT se vor folosi în primul rând strategii elementare de apărare anti-hacker.
- Multe atacuri hacker exploatează breşe ale serviciilor Windows NT.

4.4.Utilizarea de indentificatori de administrare a Securităţii

Deseori este necesară creearea unor utilizatori speciali care să poată acorda drepturi de acces altor utilizatori fără a avea drepturi complete în reţea. De exemplu, un manager de proiect are nevoie de un număr suplimentar de ingineri. În loc de a atribui managerului

de proiect un identificator de *administrator* pentru a gestiona privilegii de acces în interiorul zonei de reţea proprii , mangaerul de proiect va primi drepturile *Account Operations.* Ulterior, *administratorul* trebuie să se asigure ca *Account Opperators* au drepturi la toate directoarele situate în regiunea de reţea a managerului de proiect. Dacă se creează *Account Operators* pentru fiecare departament sau regiune aceasta va reduce volumul de muncă al personalului de administrare a reţelei. De aseamenea, deoarece un *Account Operator* este responsabil pentru întregul acces din regiunea sa, dacă acesta acordă acidental accesul la un anumit director sau fişier, administratorul îl poate face cu uşurinţă răspunzator pe *Account Opperator* în loc de a determina care membru al persoanalului de administrare a acordat acele drepturi.

4.5.Securitatea Grupului Administrator

Deoarece utilizatorii cu privilegii grupului *Administrators* au acces la întregul server sau domeniu, un hacker va încerca să ajungă mai întâi la un calculator, folosit un cont cu privilegii de *administrator*. Dacă toate conturile care aparţin grupului *Administrators* au fost suficient de asigurate, hackerul nu poate intra în niciunul din acestea. Al doilea scop al hakerului, va fi de a intra în sistem cu un cont de nivel mai redus şi a-şi acorda statutul de membru al grupului *administrators*. Trecerea de la un cont cu privilegii mai reduse la unul cu privilegii mai înalte se numeşte *atac progresiv de securitate* (security step-up attack).

BIBLIOGRAFIE

1. SamsNet - "Securitatea în intemet, Editura Teora, 2000

2. Oprea D. - "Protecţia şi securitatea sistemelor informaţionale", Editura Polirom, 2002

3. Munteanu A., Greavu Ş.V. - "Reţele locale de calculatoare, Editura Karnyanszky T.M

4.Reţele de calculatoare si comunicatii de date, Editura Augusta Timisoara, 2001

5. Tannenbaum A.S. - "Reţele de calculatoare", Computer Press Agora, 1996

6. Peterson L., Davie B. - "Reţele de calculatoare", Editura All Education

7. Alina Andreica – Information and Communication Facilities in Internet, "Babeş Bolyai" Univ., Studia Europaea, XLIII, 1-2, 1998, p. 105-131.

8. Alina Andreica, Florin Bota – Informare şi comunicare in reţele de calculatoare, Ed.EFES, 2001.

9. Larry Schumer, Chris Negus, Utilizare Unix, Ed. Teora, 1995

10. Jason J. Manger, Netscape Navigator, Ed. Teora, 1995

11. Şerban Dronca, Windows NT 4.0, Ed. Promedia Plus, 1997