PETRE RÃU

INFRACTIONALITATEA PE CALCULATOR

- 2001 -

CUPRINS

INTRODUCERE

Infractiunea informaticã înseamnã folosirea calculatorului ca obiect prin intermediul cãruia se sãvârseste o faptã care prezintã un pericol social, faptã sãvârsitã cu vinovãtie si prevãzutã de legea penalã.

Nu existã un catalog complet al infractiunilor informatice, ele fiind foarte diverse. În plus, domeniul însusi se aflã într-o continuã efervescentã, îmbogãtindu-se permanent cu tipuri noi de infractiuni.

Chiar si în acest context, se poate vorbi totusi de o listã a principalelor tipuri de infractiuni, incluzând: frauda, falsul, sabotajul sau spionajul informatic, prejudiciile aduse datelor si/sau programelor de calculator, accesul sau interceptarea neautorizatã, reproducerea neautorizatã a programelor protejate, alterarea datelor si/ sau a programelor de calculator, utilizarea neautorizatã a unui calculator sau a unui program de calculator etc.

Multe delicte informatice nu au însã nici la aceastã orã un corespondent în legislatia românească. De exemplu, infestarea, intentionatã sau nu, a unor calculatoare sau retele de calculatoare, cu virusi informatici, care, se stie, pot provoca uneori pagube imense. Stergerea sau alterarea datelor sau programelor de calculator, intruziunea în sistemele de calcul a unor persoane neautorizate, sunt de asemenea fapte încã neprevãzute în legislatie.

Aceste fapte de naturã infractionalã pot aduce prejudicii importante persoanelor fizice sau juridice, institutiilor de stat sau particulare, reprezentând un real pericol social. Unele delicte care caracterizează

criminalitatea prin computer pot merge până la amenintări militare, acte teroriste si chiar distrugeri la scară planetară. Pentru a ne convinge că pot exista si astfel de pericole este suficient să reamintim despre Y2K - problema anului 2000, pentru care s-a consumat multă cernealã si energie ca lumea să ia în serios amenintările concrete. Desigur, multe lucruri au fost atunci exagerate, ajungând să se vorbească de o presupusă apocalipsă inevitabilă la sfârsit de mileniu. Dar pericolele prevăzute atunci, dacă ar fi fost acte criminale asistate de calculator, ar fi putut cu adevărat să devină reale. După cum stim bine, acestea au fost depăsite cu brio, pentru că omenirea a înteles la timp că trebuie să actioneze, să depună eforturi si să cheltuiască sume importante pentru ca amenintările să nu se transforme în realitate.

Cartea de fată nu este un manual pentru informaticieni si nici un ghid pentru hackeri. Ea se adresează acelora, multi, care încă nu stiu nimic sau aproape nimic despre atât de controversatul subiect al infractionalitătii prin intermediul calculatorului. Nu există nici un argument pentru a pretinde că manualul ar acoperi întreaga problematică a acestui subiect. El a apărut din necesitatea acoperirii unei lipse de informatii accesibile si pe întelesul tuturor pe acest subiect de pe piata românească. Manualul se doreste a fi un material informativ si un documentar pentru toti cititori interesati doar să afle câte ceva despre ce înseamnă acest pericol la care si ei pot cădea victime, acum sau într-un viitor apropiat.

Prima parte a acestei cărti este alcătuită dintr-o serie de articole publicate de autor în cotidianul gălătean "Viata Liberă" în perioada martie-mai, 2001. Ele reprezintă o expunere mai simplă a subiectului, concepută pentru o

accesibilitate mai largã, asa încât, chiar si un nespecialist poate întelege fenomenul tratat.

Celelalte patru pãrti ale manualului este posibil sã nu fie asimilate usor de un cititor nespecialist, ele abordând subiecte mai speciale, uneori chiar dificile. În fine, manualul este completat si cu un dictionar de specialitate, ce poate veni în sprijinul acelora pentru care unele notiuni tratate nu sunt bine cunoscute.

Cea mai mare sperantã pe care si-a pus-o autorul atunci când s-a gândit sã publice acest manual a fost accea de a furniza o imagine de ansamblu cu privire la problema infractionalitãtii prin intermediul calculatorului si, în special, de a convinge cititorul de necesitatea întelegerii si combaterii acestui fenomen îngrijorãtor la scarã mondialã.

Autorul

Partea I

CALCULATORUL SI DELICTUL

1. Infractiunea informaticã

Deschidem aici o serie de articole care vizeazã principalele aspecte ale delincventei prin intermediul calculatorului. Dupã cum se stie, fenomenul a cãpãtat astãzi o amploare deosebitã. În ultimii ani calculatorul a devenit deja principalul corp delict al infractiunilor moderne.

Vom avea ocazia, pe parcursul a mai multor seriale, atât cât ne permite spatiul pus la dispozitie, sã vorbim despre tehnologia informatiei din punct de vedere infractional si juridic, despre frauda informaticã si implicatiile ei, despre pirateria software, securitatea sistemelor de calcul de acasã sau de la birou, despre ce înseamnã comertul electronic, semnãtura digitalã si riscurile pe care le comportã acestea, despre criptãri si decriptãri, virusi si tehnicile de protectie împotriva lor, despre cine si ce poate ameninta un sistem informatic, despre metode elementare de protectie împotriva atacurilor persoanelor neautorizate, despre hackeri sau spãrgãtorii de coduri. Cu alte cuvinte, vom face cunostintã cu cele mai noi aspecte ale fenomenelor de delincventã pe calculator, cu stiri proaspete si sentinte penale, cu legea copyrightului, a protectiei dreptului de autor si cum se aplicã toate acestea, atât în tara noastrã cât si în strãinãtate, cu referire la programele informatice. Vom încerca sã pãtrundem, atât cât ne putem permite, în "etica" si "psihologia" spãrgãtorilor de coduri si vom aborda si alte probleme din acest domeniu atât de fascinant si controversat al informaticii moderne.

Din cauzã cã unii termeni pot pãrea "prea tehnici" pentru multi dintre cititori, ei vor fi explicati pe mãsurã ce

se va considera necesar. Pentru început vom încerca să explicăm ce semnifică si ce uprinde infractionalitatea informatică.

În termeni juridici, infractiunea informatică înseamnă folosirea calculatorului ca obiect prin intermediul căruia se săvârseste o infractiune, deci o faptă care prezintă un pericol social, săvârsită cu vinovătie si prevăzută de legea penală. Simpla sustragere de componente de comunicatie sau de calculatoare electronice nu reprezintă o infractiune de natură informatică, ea fiind calificată drept un furt obisnuit.

Infractiunile informatice sunt multiple si diverse. Un catalog al acestora poate fi incomplet deoarece, domeniul fiind în continuă efervescentă, se îmbogăteste permanent cu tipuri noi de infractiuni. Există totusi o listă al principalelor tipuri de infractiuni. Aceasta include pe cele care sunt cunoscute astăzi si catalogate, precum: frauda informatică, falsul informatic, prejudiciile aduse datelor si programelor de calculator, sabotajul informatic, accesul neautorizat, interceptarea neautorizată, reproducerea neautorizată de programe protejate, alterarea datelor sau a programelor de calculator, spionajul informatic, utilizarea neautorizată a unui calculator sau a unui program de calculator.

Tara noastră nu dispune nici la această oră de o legislatie care să combată infractionalitatea săvârsită prin intermediul calculatorului. Majoritatea tărilor dezvoltate din lume si-au rezolvat de multă vreme această problemă, desi nu în toate cazurile la modul ideal. Există si o recomandare a Consiliului Europei, R(89)9, atât pentru statele membre cât si pentru cele aspirante la statutul de tară comunitară, deci inclusiv pentru România, recomandare care califică toate aceste aspecte ale

delincventei prin intermediul calculatorului. Aceasta ar putea fi folositã cu usurintã pentru armonizarea legislatiilor interne cu cele comunitare. Si mai mult ca sigur cã acest lucru se va întâmpla în viitorul foarte apropiat. Altfel riscãm sã rãmânem acolo unde ne situãm astãzi si în acest domeniu în care - sunt argumente suficiente sã credem asta - am putea avea ceva sanse de a ne demostra capacitatea de popor inteligent si capabil sã se adapteze rapid la tehnologiile de vârf ale lumii.

2. Legislatia pentru delicte informatice

Cu toate cã tara noastrã nu dispune de o legislatie adecvatã în acest domeniu (nici mãcar un singur cuvânt din Codul Penal nu pomeneste de infractiunea de naturã informaticã, desi acesta a fost modificat recent, ca sã nu mai vorbim de Codul Civil care este de pe vremea lui Cuza), totusi anumite fapte sãvârsite prin intermediul calculatorului, pot fi echivalate cu unele prevederi din Codul Penal. Dintre acestea am putea exemplifica urmãtoarele: falsificarea de monedã sau de alte valori cu scannere performante, imprimante laser, fabricarea intrumentelor proprii de falsificare. Chiar si omorul sãvârsit prin intermediul calculatorului (pentru cã, desi nu la noi, asemenea lucruri s-au întâmplat prin modificarea premeditatã a unor diagnostice în SUA), poate fi pedepsit de legea penalã. Însã existã multe alte delicte informatice care nu au nici un corespondent în legislatia românească. De exemplu, infestarea, intentionatã sau nu, a unor calculatoare sau retele de calculatoare, cu virusi informatici, care, se stie, pot provoca uneori pagube

imense. Stergerea sau alterarea datelor sau programelor de calculator, intruziunea în sistemele de calcul a unor persoane neautorizate, sunt de asemenea fapte încã neprevãzute de legislatia noastrã. Si ca ele sunt multe alte fapte de acest gen, care pot aduce prejudicii importante persoanelor fizice sau juridice, institutiilor de stat sau particulate, reprezentând totodatã si un real pericol social.

Din punct de vedere istoric, cu mai bine de cincisprezece ani în urmã, pe plan mondial a existat o încercare de catalogare a pericolelor sociale de naturã informaticã, fiind grupate în categoria "Computer Aided ..." din care fac parte cunoscutele acronime informatice CAD, CAM, CAE, CASE etc. S-a propus atunci ca faptele criminale sãvârsite prin intermediul calculatorului sã se numeascã "Computer Aided Crime". Din motive usor sesizabile, un român a venit cu o contrapropunere de denumire autohtonã, abreviatã prin DAC - "Delincventa Asistatã de Calculator". Indiferent de denumirea acestor fapte, un lucru este sigur, ele nu mai pot fi neglijate deloc astãzi, când este evident cã în viata noastrã de zi cu zi, calculatoarele ocupã un loc din ce în ce mai important si, din nefericire, în paralel cu spectaculoasa evolutie a acestora, ia amploare si o infractionalitate specificã.

Prin *pirateria software* se întelege folosirea nepermisã si utilizarea fãrã drept de autor a software. Se spune cã rata pirateriei soft din tara noastrã este una dintre cele mai ridicate din lume. Dacã facem abstractie de Rusia, în topul european al pirateriei programelor de calculator tara noastrã ocupã de multã vreme primul loc.

Acum cinci ani a apãrut si la noi prima lege care face referire la anumite delicte de naturã informaticã. Este

vorba despre Legea nr.8/1996, cunoscutã si sub numele de legea copyright-ului, care prevede, printre altele, protectia drepturilor de autor pentru programele de calculator (software). Desi au fost descoperite destule imperfectiuni ale acestei legi care, coroborate cu imperfectiunile legii vamale, au contribuit decisiv pânã în prezent la lipsa unei finalitãti a actiunilor judecãtoresti, totusi poate fi considerat cã a fost fãcut primul pas pe drumul alinierii legislatiei românesti la cele ale tãrilor avansate.

Dar despre pirateria software vom mai avea ocazia sã discutãm într-un capitol special.

3. PC-ul (c)are minte

Pe lângã numeroasele aplicatii pe care le are în aproape toate domeniile activitãtilor umane, PC-urile pot fi folosite si pentru spargerea bazelor de date si a programelor, pentru falsificarea de înscrisuri valorice si de dovezi, pentru cifrãrile spargerilor de tip mafiot, pentru transferul sau alterarea datelor în scop de tãinuire, pentru distribuirea pornografiei de orice fel, inclusiv cea infantilã, pentru comenzi de organe pentru transplant si comert cu carne vie, pentru înselãtorii si sabotaje, pentru spionaj computerizat, pentru manipularea sistemelor de pazã si protectie si pentru multe altele.

Manipulãrile si abuzurile din acest domeniu pot aduce mari prejudicii, pot afecta libertatea individualã si de grup si - de ce nu ? - pot ameninta chiar si statul de drept.

Delictele care caracterizează criminalitatea prin computer pot merge până la amenintări militare si la posibile distrugeri la scară planetară. Pentru a ne convinge că pot exista si astfel de pericole este suficient să reamintim despre Y2K - problema anului 2000, pentru care s-a consumat multă cernealã pentru ca lumea să ia în serios amenintările concrete. Desigur, multe lucruri au fost exagerate, ajungând să se vorbească de o presupusă apocalipsă inevitabilă la sfârsit de mileniu. Dar pericolele iminente prevăzute atunci, dacă ar fi fost însotite de acte criminale asistate de computer, ar fi putut cu adevărat să devină reale. După cum stim bine, acestea au fost depăsite cu brio, tocmai pentru că omenirea a înteles la timp în primul rând că trebuie să actioneze, dar si să depună eforturi si să cheltuiască sume importante pentru ca aceste pericole să nu se transforme în realitate.

Cum de este PC-ul un calculator atât de vulnerabil? În primul rând trebuie spus că nu numai calculatoarele de tip personal sunt vulnerabile. Sub incidenta actelor infractionale se găsesc toate calculatoarele, inclusiv mainframe-urile, desi nu în aceeasi măsură. PC-ul este astăzi cel mai răspândit calculator din lume. El se află pe toate birourile importante ale societatilor comerciale si institutiilor de stat si particulare si, în plus, lucru care aproape că nu putea fi prevăzut în urmă cu trei decenii, el a pătruns din ce în ce mai mult în casele oamenilor. Dar asta încă nu e suficient ca el să poată deveni un adevărat instrument de propagare a minciunii si fraudelor, desi se cunoaste foarte bine că falsificarea monedelor si a înscrisurilor valorice, a documentelor, dovezilor si multe altele se petrec cel mai adesea pe calculatoarele si anexele acestora de acasă.

Numărul fenomenelor infractionale este cu mult mai ridicat însă pe calculatoarele ce sunt legate într-o retea si, cu preponderentă, cele legate la reteaua globală Internet.

Cu un PC performant, dotat cu o imprimantă de tip laser sau cu alte dispozitive periferice din ce în ce mai numeroase si performante astăzi, se pot face o groază de lucruri care contravin oricăror reguli de convietuire socială.

PC-ul poate fi transformat cu usurintă într-o sursă de produs minciuni. De aceea justitia trebuie să lupte neîncetat, cu arme noi, împotriva abuzurilor prin computer. Este nevoie de legi noi, adecvate si pe măsura noilor infractori, pentru că - se întelege - acestia sunt, de regulă, "specialisti" cu un coeficient de inteligentă peste medie.

Nu se poate rămâne însă doar la stadiul că "există o lege si de acum înainte infractiunile prin computer, precum pirateria software, vor putea fi pedepsite". Politiei îi va fi imposibil să aplice legile dacă nu este bine pregătită si nu este solicitată. Organele de cercetare penală, functionarii criminalisti, trebuie să se pregătească si în domeniul informaticii, deoarece din acest domeniu au izvorât noile tipuri de infractiuni. Legea trebuie să se impună cu oameni pregătiti.

Asa cum sustinea cu mai bine de un deceniu în urmă un cunoscut specialist în informatică, profesorul Klaus Brunnstein de la Universitatea din Hamburg, informatica ar trebui să devină materie de examen la facultătile care pregătesc cadre pentru politie.

4. Ce este un hacker

Între două calculatoare care comunică printr-o retea un intrus oarecare se poate interpune prin intermediul porturilor calculatorului sursă sau destinatie, prin elementele active si dispozitivele de comunicatie asamblate între cele două calculatoare (modemuri, router-e etc.) sau chiar direct prin legare la linia de comunicatie dintre cele două sisteme de calcul. În acest scop există dispozitive hardware dar si programe special concepute, care permit scanarea la distantă.

Oricât de bună ar fi protectia asigurată pentru prelucrarea automată a datelor, oricâte instrumente de securitate s-ar inventa si implementa, trebuie să fim convinsi de faptul că, printr-o cale sau alta, mai devreme sau mai târziu, protectiile acestea vor fi sparte si efractia se va produce. Din acest punct de vedere putem compara fenomenul cu ceea ce se întâmplă în lume cu sistemele de avertizare pentru usi, case de bani, automobile etc. Nu sunt infailibile. Infractorii găsesc mereu brese în sistemele noastre, ei dovedind un interes mai mare pentru problemele de securitate decât noi, cei care încercăm să le protejăm. Acest lucru se întâmplă si din motivul că un responsabil cu prelucrarea automată a datelor care neglijează securitatea datelor riscă, în cel mai rău caz, o sanctiune profesională. Dimpotrivă, un infractor poate manifesta destulă grijă să-si ascundă dovezile de ochii politiei.

Cu problemele de intrare prin efractie, bazate în principal pe "ocolirea" codurilor de protectie existente în sistemele de computere sau în bazele de date, se ocupă asa-numitii "spărgători" de coduri sau *hackerii*. Fiindcă

vom utiliza des acest termen, vom începe prin a lămuri această notiune. Deci, ce este un hacker?

Desi traducerea directă a acestui cuvânt de origine englezească are un înteles putin ciudat (hack = a ciopârti), în lumea informaticii acesta nu reprezintă altceva decât actiunea unui individ care utilizează cunostintele sale despre calculatoare, retele de comunicatie, lumea Internet s.a., cunostinte nu neapărat extraordinare, cu scopul de a pătrunde în locuri nepermise dintr-o retea de calculatoare, de a sustrage informatii confidentiale sau pur si simplu de a distruge, de cele mai multe ori cu bună stiintă, tot ceea ce s-ar putea distruge într-un calculator sau în mai multe deodată.

Hackerii nu se aseamănă între ei. Fiecare are un stil propriu de actiune. Unii actionează doar sub impulsul curiozitătii, vrând să afle cum functionează un anumit program sau, pur si simplu, dorind să arunce o privire indiscretă asupra anumitor lucruri din "bucătăria" altuia. Acestea ar putea reprezinta cel mai mic "rău" pe care îl pot provoca, desi uneori, involuntar sau nu, hackerii pot chiar ajuta, contribuind la descoperirea unor bug-uri (erori) ale programelor.

Din nefericire, multi hackeri actionează ca niste criminali, pătrunzând prin efractie în locuri nepermise si provocând în mod constient pagube însemnate.

Iată câteva exemple mai vechi. Pe data de 6 ianuarie 1993, câtiva hackeri din Marea Britanie au pătruns în banca de date a unei companii comerciale din Londra, operând un transfer de 10 milioane de lire sterline. Tot în aceeasi perioadă câteva site-uri oficiale americane au fost "ocupate" de o actiune spectaculoasă a unor chinezi. Acestia au introdus în locul mesajelor standard existente, propriile lor texte de protest,

provocând un fel de mini-războiu psihologic. Primul exemplu se referă la o infractiune concretă, fâcând parte din categoria "campaniilor active" care lasă prejudicii ce pot fi imediat cuantificate. Al doilea exemplu este doar o "campanie pasivă", cu implicatii de natură psihologică în primul rând, dar si de natură politică, fiind mai degrabă o dovadă că războiul informational este o realitate cu care trebuie să ne obisnuim.

5. Statistici despre hackeri

Din unele statistici oficiale se apreciază că există cel putin un hacker pentru fiecare sută de utilizatori. Din fericire, doar câtiva dintre acestia urmăresc un scop precis.

Toti cei care sunt conectati la Internet, de acasă sau de la birou, este foarte probabil să fi fost vizitati de un hacker cel putin odată.

Evident, aceste fenomene se petrec în special în tările dezvoltate, si cu prisosintă în SUA, unde informatica este cu adevărat un fenomen de masă si unde interesele hackerilor sunt mai largi. În astfel de tări tranzactiile bancare sunt aproape în totalitate pe calculator, comertul electronic de asemenea, iar institutiile militare si guvernamentale sunt de mare interes în lumea spionajului. Nu sunt lipsite de interes nici marile firme de hardware si software care, prin evolutia lor concurentială de mare spectaculozitate, contribuie permanent si decisiv la dezvoltarea instrumentelor noi în domeniu. Din asta nu

trebuie să credem că firmele mici si persoanele particulare ar fi evitate de hackeri.

Mai mult de 40% dintre americani au fost vizitati de către persoane neautorizate în decurs de un an, spune un studiu-sondaj efectuat de Computer Security Institute Of San Francisco si de FBI's International Computer Crime Squard. În acelasi timp peste 50% au raportat că au sesizat încercări de acces nepermis, atât din exterior, cât si din interior.

Un raport recent al acelorasi institutii redă următoarele cifre: 90% dintre organizatii au detectat probleme de securitate în ultimile 12 luni; 70% au raportat probleme neimportante, altele decât virusi, furturi de laptop-uri sau abuzuri în folosirea legăturii la Internet; trei ani la rând s-a constatat cresterea numărului de accesări neautorizate prin Internet (59%) fată de 38% din reteaua internă; 74% au recunoscut că au avut pierderi financiare; 273 de institutii au raportat pierderi de aproape 266 milioane USD (media anuală fiind 120 milioane USD).

Asadar, nu este corectă o atitudine de genul: "nu am nimic deosebit în calculatorul meu, care poate să prezinte interes pentru cineva". Nu este corect să credem că un hacker îsi alege "victima" numai pe criteriul importantei datelor si programelor continute într-un calculator. Unii cad victime tocmai datoritã acestei naivităti.

Atacurile persoanelor neautorizate într-o retea nu pot fi întotdeauna distinse cu usurintă de comunicările legitime. De cele mai multe ori atacatorii dispar fără să lase vreo urmă care să poată sprijini identificarea.

Statistica infractionalitătii pe calculator nu redă decât o parte a realitătii. De exemplu, unii apreciază că, în domeniul pirateriei software, datele statistice oferite

publicitãtii nu reflectã decât în proportie de 50-60% din ceea ce se întâmplã în realitate.

Aproape în fiecare an autoritãtile federale din SUA anuntã cã a fost atins un numãr record de cazuri de infractiuni electronice. De la un an la altul rata criminalitãtii în acest domeniu creste cu câteva zeci de procente. În plus, mai bine de jumãtate din cazurile semnalate sunt respinse de procurori. Din investigatiile FBI si ale altor agentii specializate doar un numãr foarte mic al actiunilor judecãtoresti privind infractiunile electronice au o finalitate, deoarece acestea sunt foarte greu de dovedit si majoritatea lor sunt respinse din lipsã de probe. Sentintele date pentru cei care au fost gãsiti vinovati sunt, în medie, de 5 luni de închisoare.

În tara noastrã, în domeniul informatic, cea mai frecventã încãlcare a legii o reprezintã copierea si difuzarea ilegalã a unui produs informatic, care este sanctionatã conform Legii 8/1996 cu închisoare de la trei luni la trei ani sau cu amendã de la 700.000 la 7.000.000 lei.

6. Hackerii în actiune

Internetul nu mai e de mult ce a fost odatã, o retea preponderent stiintificã cu legãturi mai mult în mediile universitare. Practic, în Internet are acces astãzi orice individ, reteaua fiind "populatã" de cele mai diverse personaje, multe din ele de origine incertã. Lumea business-ului, supusã unei competitii acerbe, a schimbat fata Internetului în teatrul unor rãzboaie dure.

În urma infiltrării unui hacker într-un computer sau o retea pot apărea următoarele categorii de probleme: a) cu efecte imediate si cu urmări grave, precum blocarea serviciilor ("total denial of service") b) cu efecte pe termen lung, cu schimbări subtile dar importante în bazele de date (de exemplu, cele financiare) pentru a submina integritatea sistemelor.

Prezentăm în continuare câteva dintre cele mai iminente pericole care pot fi întâlnite în lumea calculatoarelor.

Multi probabil că nu stiu - sau nu bănuiesc - că, de când cu Internetul, un hacker poate să-ti acceseze, în anumite conditii, calculatorul de acasă sau de la serviciu, îsi poate instala pe acest calculator un program special care inspectează si controlează calculatorul si să fure date importante sau să steargă anumite informatii de pe hard disk-uri.

Sunt multi care nici nu bănuie că este posibil să ai un spion în casă fără să-l vezi sau să-l simti, fără să fie un microfon bine ascuns (procedeu deja devenit clasic), o ureche sau altceva uman. Totul e să ai un calculator, iar acesta să fie conectat într-o retea sau, foarte la modă în ultimii ani, să fie conectat în reteaua internationalã de calculatoare Internet.

Cum pătrunde un hacker la tine "în casă"? Trebuie să stiti că nu-i mare lucru să ajungi pe PC-ul alctuiva. Ati auzit, desigur, despre cât de tineri sunt - uneori chiar copii - majoritatea celor care îndrăznesc si reusesc acest lucru. Important este să găsesti o asa-numită poartă de intrare, aceasta nefiind altceva decât un număr de telefon sau o adresă de comunicatie. Odată stabilită această legătură, uneori nici nu-ti mai trebuie altceva. Dificultăti mai mari sunt întâlnite doar atunci când, prevăzător, proprietarul si-

a pus o parolã pe care, desigur, nu a divulgat-o nimãnui. Dar si peste acest lucru se poate trece. Cum? Hackerul, care, desigur, ati înteles cã este un "bãiat" inteligent, pune la bãtaie un program special, care nu face altceva decât sã bombardeze respectivul calculator cu parole generate aleator, în speranta cã va nimeri peste combinatia corectã. Unora nu le scapã din vedere sã încerce mai întâi numele proprietarului sau diferite combinatii ale acestuia, data nasterii sau tot ce s-ar putea presupune cã i-a putut trece prin cap aceluia care si-a ales buclucasa parolã. Pentru cã - trebuie sã stiti - atunci când ne alegem o parolã pentru a avea numai noi acces la un calculator, la o retea de calculatoare sau pur si simplu doar la niste fisiere de date sau programe, trebuie sã o si tinem minte o perioadã de timp, pânã o vom schimba. Altfel putem risca sã nu mai putem avea chiar noi acces acolo unde am avut pânã atunci. Uneori nu este un risc prea mare sã-ti uiti propria parolã, însã cine îsi doreste chiar si niste mici necazuri? Si, asa cum am vãzut, hackerul poate avea noroc sã nimereascã parola noastrã si sã pãtrundã în sistem ca si cum am fi noi însine acolo. Si, evident, cam tot ce-am fi putut face noi, va putea face si el, numai cã intentiile nu coincid. Dacã noi puteam vedea niste date, le va putea vedea si el, dacã noi puteam sterge un fisier îl poate sterge si el s.a.m.d. Dar, fiti convins cã intentiile lui nu sunt deloc "curate".

Chiar si atunci când nu reuseste "din prima" sã descifreze o parolã, hackerul nu va renunta usor. Trebuie sã stiti cã multi dintre ei dispun de programe foarte bine puse la punct, care pot "încerca" milioane de combinatii într-un interval relativ scurt de timp. Ca orice infractor care actioneazã cu premeditare, ei sunt bine "înarmati",

cu instrumente informatice, dar si cu multă abilitate si răbdare, si vor insista până când li se deschide "poarta de acces".

7. Tipuri de amenintări si metode de atac

Cine sunt cei care ne "vizitează"? Într-o statistică de dată recentă, prezentată într-un raport al FBI în fata Comisiei Juridice a Senatului American, sunt mentionati pe primul loc angajatii sau fostii angajati ca principală sursă a infractiunilor pe calculator. Acestia au adesea ca mobil răzbunarea sau dorinta de a obtine unele venituri. Pagubele pe care le produc sunt de regulă foarte mari. În raport se mentionează exemplul unui fost inginer soft al unei companii care, plasând bine doar sase linii de cod undeva anume, acestea au produs pagube companiei evaluate la 10 milioane dolari.

După fostii angajati, hackerii ocupă locul doi în topul spărgătorilor de coduri. Ei penetrează calculatoarele si retelele din diverse motive, cele mai multe fiind de ordin financiar. Alteori însă acestia manifestă pur si simplu dorinta de a distruge. În urma pătrunderii neutorizate pe un calculator se pot fura informatii pretioase si/sau se pot sterge date importante.

Locul trei este ocupat de autorii de virusi, în timp ce pe locul patru apar grupurile criminale, care au ca obiectiv obtinerea de bani prin vânzarea informatiilor furate sau prin realizarea de tranzactii bancare ilegale.

Nu trebuie să ne mire faptul că si teroristii au trecut în ultimul timp la utilizarea noilor tehnologii de transmitere

a informatiei prin Internet, pentru a face planuri, pentru a obtine fonduri si pentru a comunica în siguranţă. Acestia ocupă abia pozitia a cincea în ierarhia tipurilor de amenintări asupra sistemelor informatice. Simplul fapt că organizatiile teroriste încep să se bazeze din ce în ce mai mult pe tehnologia informatiei constituie un real avertisment.

În fine, ultimul loc în acest original clasament îl ocupă serviciile secrete ce au început să folosească canalele de comunicatii si Internetul ca mijloace de obtinere a informatiei.

După cum s-a mentionat, se pare că furtul de informatii este cel mai putin interesant pentru "spărgătorii" de coduri. De aceea, o politică de genul "nu am informatii vitale în calculatorul meu, deci nu trebuie să mă tem de hackeri" nu este tocmai potrivită.

Să vedem acum care sunt principalele metodele de atac ale hackerilor. Pe primul loc se situează încercările acestora de obtinere a acceselor pe sistemele existente în retea.

Multi hackeri doresc să iasă în evidentă, ei lăsând mesaje care dovedesc aceasta. De cele mai multe ori ei doresc doar să citească ce informatii se găsesc pe sistemele "sparte", provocând stricăciuni nu neapărat dorite, ci doar făcute inconstient atunci când doresc să-si steargă urmele.

O categorie specială de atac o constituie vandalismele, care lasă amprente serioase din punct de vedere a distrugerilor cauzate. Hackerii din această categorie sunt persoane răuvoitoare, sau cel atacat este un "dusman" cert al atacatorului. Spărgătorii încearcă să steargă complet datele din calculator, situatie care conduce, de cele mai multe ori, la declansarea

procedurilor de recuperare bazate pe back-up. Unii hackeri mai subtili, pot provoca un rău mai mare, prin încercarea de a modifica unele date importante din sistem, de pildă cele de natură financiar-contabilă, care pot avea implicatii foarte grave asupra activitătii firmei atacate.

O altă metodă de atac are la bază utilizarea sistemelor atacate pentru a distribui materiale ilegale (pornografie, materiale propagandist-teroriste etc.) sau software nelicentiat.

Există si metode de spionare, de exemplu cele de preluare a datelor interesante pentru avantaje economice sau militare evidente. Aceste atacuri sunt foarte greu de detectat deoarece, de regulă, atacatorul nu are ca scop modificarea în vreun fel sau altul a continutului informatiilor din sistemul accesat, deci nu lasă urme.

8. Cum actionează un hacker

În lupta împotriva delincventei asistate de calculator se petrece un fenomen paradoxal: în timp ce se depun eforturi sustinute pentru cresterea securitătii sistemelor informatice si pentru descoperirea solutiilor de preîntâmpinare a atacurilor persoanelor neautorizate, "maniacii" computerelor descoperă permanent metode si tehnici noi de atac.

Atacul unui hacker nu se rezumă doar la calculatoarele conectate la Internet. Acesta actionează asupra oricărui calculator conectat într-o retea care nu detine un sistem de securitate bine implementat. Hackerul stie să-si fabrice singur, dacă e nevoie, sau să

mânuiascã, "instrumente" special concepute pentru a descoperi slãbiciunile unui calculator dintr-o retea.

Un prim "instrument" la îndemâna acestora este cunoscut sub numele Host Scans. De fapt, Host Scans nu este decât o metodã de identificare a calculatoarelor din retea. Ea constã în scanarea unui numãr de adrese de Internet si, în cazul în care de la una din masini se primeste un rãspuns, confirmându-se faptul cã existã un sistem care are adresa respectivã configuratã, se va putea trece cu încredere la faza urmãtoare, adicã la atacul propriu-zis.

Un alt pas îl constituie scanarea pentru identificarea porturilor deschise ale aplicatiilor pentru a fi utilizate în scopul obtinerii accesului în sistem.

Cea mai cunoscutã formã de actiune si totodatã, cea mai "spectaculoasã" prin efect, este cunoscutã sub numele Denial of Service (DoS). Efectul constã în blocarea serviciilor existente pe computerul respectiv; de fapt, este o încercare de a bloca accesul la calculator a acelora care aveau acest drept, deci chiar a persoanelor autorizate. Realizarea acestui scop se face de obicei prin schimbarea parametrilor sau configuratiei sistemului sau, adesea, prin instalarea unui program propriu care are ca scop generarea unui trafic foarte mare în sistemul vizat.

Atacurile de tip DoS sunt numeroase. Nu vom face aici un inventar sau o enumerare a acestora care, desigur, nu ar avea sanse niciodatã sã fie exhaustivã, tinând seamã de faptul cã inventivitatea atacatorilor este permanentã si nelimitatã. Vom prezenta doar câteva exemple, din care cititorul si-ar putea face o imagine mai clarã despre câte resurse se pot investi chiar si în domeniul infractionalitãtii.

Se stie cã protocolul Internet TCP/IP gestioneazã mesajele foarte mari prin fragmentarea lor, pentru a putea fi trimise prin retea în pachete optime, urmând ca la destinatie sã fie asamblate la loc. Una dintre metodele rãufãcãtorilor constã chiar în aceea de a exploata aceastã slãbiciune, trimitând suficient de multe fragmente foarte mici care simuleazã un pachet foarte mare, imposibil de asamblat.

În contextul aceleiasi metode, unii procedeazã la "stârnirea" tutoror calculatoarelor active dintr-o retea, pentru a trimite, într-un trafic foarte mare, rãspunsuri pe adresa unei victime alese în prealabil, pânã la obtinerea unei blocãri complete.

Blocarea unor servere care oferã servicii importante, de exemplu cele de Web, este o altã tehnicã utilizatã frecvent. Ea constã în simularea unei sesiuni TCP, odatã cu expedierea unui numãr foarte mare de mesaje, la care nu se mai generează rãspunsurile la informatiile de confirmare, paralizând astfel activitatea calculatorului destinatie care nu mai poate deschide nici o conexiune legitimã.

9. Ce urmãreste un hacker

De cele mai multe ori, pentru a-si atinge scopurile, hackerii încearcã obtinerea accesului direct, precum drepturi de administrare, de root sau drepturile unui alt utilizator (user) pe masinile atacate. Unele obiective de acest gen pot fi atinse fãrã a executa comenzi pe calculatorul server.

Sunt însă si alte obiective, precum cele de modificare a configuratiei masinilor ce oferă anumite servicii, care pot fi atinse fie cu acces direct la masină, în general prin obtinerea de drepturi de administrator sau root, fie fără acces direct, adică exploatând bug-uri (erori) în servicii care rulează cu drepturi mari pe masina respectivă.

În general se poate spune că atingerea obiectivelor presupune de obicei acces direct la masină, dar nu neapărat.

Prezentăm mai jos o inventariere a scopurilor pe care le urmăreste un atacator, asa cum sunt ele văzute si publicate în revista PC Report nr.11/2000, cu mentiunea că acestea nu epuizează toate cazurilor întâlnite în practică:

1) îngreunarea sau încetinirea activitătii normale a unui serviciu prin mărirea timpilor de răspuns la cereri sau prin perturbarea accesului la resurse, mergând până la blocarea completă a activitătii

2) inserarea de secvente denaturate în datele trimise de un serviciu către utilizatori, mergând până la deturnarea completă a serviciului către o resursă controlată de atacator

3) obtinerea de acces nelegitim la servicii private sau cu acces limitat

4) capturarea informatiilor vehiculate de servicii cu caracter privat sau secret

5) modificarea configuratiei masinilor care oferă anumite servicii

6) instalarea de programe speciale, care execută pe serverele atacate diverse actiuni în interesul atacatorului, cum ar fi colectarea de parole etc.

7) înlocuirea unor programe ce fac parte din instalarea masinii atacate, cu altele care par a executa aceleasi actiuni ca si cele originale, dar de fapt lucrează pentru atacator

8) stergerea pur si simplu a unor programe si/sau informatii pe serverele atacate, mergând până la distrugerea completă din punct de vedere software a masinilor atacate, sau chiar până la distrugeri hardware (improbabil, dar nu imposibil).

După cum s-a putut întelege până acum, toate sistemele de calcul cu deschidere spre lumea exterioară nu sunt si nu pot fi în deplină siguranță. De aceea, măsurile de protectie sunt o practică obisnuită în lumea tehnologiei informatiei, si este de la sine înteles că, acolo unde protectia sistemelor este maximă si numărul atacurilor sunt minime.

Spărgătorii de coduri care atacă sistemele tocmai din cauza unor imperfectiuni ale acestora, sunt uneori priviti ca eroi, deoarece ne arată că sistemele noastre nu sunt sigure.

În serialul următor vom vedea cum putem să ne apărăm împotriva atacurilor de orice fel, deoarece, trebuie să stiti, aproape ca în medicină pentru orice boală descoperită specialistii găsesc, de regulă, si un remediu pe măsură.

10. Cum ne apărăm împotriva atacurilor

În locul denumirii de hacker s-ar putea folosi mai exact numele de cracker, care înseamnă, în traducere din

limba englezã, spãrgãtor. Însã termenul de hacker este mai simpatic si se pare cã defineste mai bine modul de actiune al infractorilor de acest gen. De aceea el a pãtruns cu usurintã în limbajul informatic comun si astãzi este atât de la modã.

Indiferent de numele care li se atribuie trebuie sã recunoastem însã cã acesti infractori au devenit o adevãratã sursã de pericole. Paradoxal însã, existã si motive ca hackerii sã fie apreciati, de exemplu cei care descoperã bug-uri sau cei care aduc un serviciu în interes national, precum spionii care sparg codurile de acces ale calculatoarelor unor institutii apartinând altor state. Cu toate acestea, nimeni nu îndrãzneste sã le recunoascã vreun merit. Sau, asa cum spune John C. Dvorak, simpatia pentru hackeri este în continuã descrestere.

În crâncena luptã dusã împotriva hackerilor, respingerea atacurilor succesive este neeconomicoasã si deranjeazã. Cea mai bunã politicã este aceea de protejare a sistemelor importante pentru care trebuie rezolvate toate problemele de securitate ale acestora.

Din fericire, ca si în medicinã unde aproape pentru toate bolile existã tratamente adecvate, desi zilnic se concep modalitãti noi de atac, sunt descoperite destul de repede si cele de protectie. Astfel, s-a ajuns sã se dezvolte o diversitate de solutii de apãrare.

Una dintre cele mai vechi metode de protectie are la bazã tehnica utilizãrii parolei la intrarea în sistem, într-o aplicatie, sau pur si simplu pentru vizualizarea unor informatii importante. Parola, ca metodã de acces limitat la fisiere si aplicatii, este des utilizatã pentru securitatea informatiilor. Dar nu este un instrument infailibil. Am mai vorbit despre unele tehnici aplicate de hackeri pentru a "sparge" o parolã de acces. În practicã, ele sunt cu mult

mai multe, ingeniozitarea "spărgătorilor" dovedindu-se a fi nelimitată.

Un alt instrument de protectie, utilizat în anumite cazuri speciale de aplicatii si acces la informatii, este cel referitor la criptarea comunicatiilor în retea. Despre această metodă vom mai discuta. Ceea ce este important să retinem este faptul că nu există metode de criptare perfecte, pentru care să nu existe solutii de decriptare, la fel de ingenioase. Acest lucru a fost demonstrat matematic în urmă cu câteva decenii de mai multi oameni de stiintă. Cu toate acestea, sistemul de criptare a informatiilor în sistemele de comunicatie este o practică pe care se bazează toate sistemele complexe de tranzactii bancare, militare, servicii secrete etc.

Autentificarea si criptarea sunt metode des folosite pentru asigurarea integrităti informatiilor în sesiunile de comunicatie care folosesc Internetul ca suport de transport pentru transferul de date.

Una din cele mai cunoscute metode, numită Firewall în literatura de specialitate, are la bază implementarea unor politici de securitate. Ea constă în solutii hardware si/sau software, concepute special pentru conectarea în siguranță la retelele partajate de date, deci inclusiv la Internet. Metoda are în vedere primul nivel de protectie împotriva accesului neautorizat si utilizează, de regulă, tehnici de permisiuni sau blocări ale accesului pe baza unor reguli prestabilite, urmărind permanent evenimentele care apar la interfata cu reteaua publică.

Există multe alte metode de protectie împotriva atacurilor de orice fel. Unele sunt specifice si abordează doar rezolvarea anumitor categorii de probleme, altele încearcă să generalizeze mecanismele de apărare si, în bună parte, reusesc.

Iatã doar câteva metode de apãrare împotriva accesului neautorizat: deschiderea conexiunii pe baza numãrului apelantului sau prin autentificarea utilizatorului, atunci când soseste un apel, dupã care se procedeazã la închiderea canalului de comunicatie si se sunã înapoi apelantul; utilizarea unor protocoale de identificare specialã prin combinatia utilizator/parolã; validarea utilizatorilor sau sesiunilor de comunicatie utilizând o bazã de date, utilizarea solutiilor speciale de protectie în retele conectate permanent la Internet; folosirea de sesiuni criptate pentru administrarea sistemelor de la distantã etc.

11. Cum protejãm programele

Unii specialisti sustin cã ar exista suficiente "retete" pentru rezolvarea completã a problemelor legate de protectia împotriva accesului neautorizat, atât în sistemele de comunicatie cât si în programele de calculator, numai cã acestea nu sunt aplicate. De-a lungul timpului au fost concepute numeroase reguli speciale, care s-au constituit în principii generale si alãturi de care s-au dezvoltat tehnici adecvate de protectie, tehnici care sunt astãzi la îndemâna oricui.

Altii invocã, deseori pe bunã dreptate, cã implementarea unei politici adevãrate de securitate este foarte costisitoare. Indiferent cine are dreptate, cert este faptul cã la aceastã orã nu avem motive suficiente sã credem cã suntem protejati împotriva atacurilor constiente sau inconstiente ale "musafirilor nepoftiti".

Dupã cum se stie, Internetul abundã în solutii (crackuri, utilitare, tutoriale etc.) care prezintã tot felul de metode privind spargerea protectiilor programelor de calculator. Ele oferã detalii suficiente pentru ca un program care interesează sã devinã, practic fãrã nici un cost, accesibil oricui.

În acelasi timp, există si o întreagã colectie de sfaturi, multe dintre ele publicate în diverse reviste de specialitate sau pe Internet, vizând unul si acelasi aspect: cum sã ne apãrãm împotriva infractiunilor pe calculator. În general, tehnicile particulare urmãresc sã îngreuneze viata spãrgãtorilor de coduri. Unele sunt simple, altele sunt mai greu de aplicat.

Este bine cunoscut faptul cã, de regulã, un programator nu-si alocã prea mult timp pentru a-si proteja programele. Acesta poate fi considerat un prim motiv pentru care programele cele mai "cãutate" ajung, "pe gratis", pe mâna oricui, si circulã astfel în mod ilegal prin diverse canale de distributie (CD-uri, Internet etc).

Pentru protectia aplicatiilor programatorii folosesc atât solutii proprii, concepute special în acest scop si care pot constitui o amprentã personalã din acest punct de vedere, cât si diverse variante bazate pe reguli generale, cunoscute si implementate în numeroase sisteme. Prezentãm în continuare câteva dintre acestea, care sunt cel mai des utilizate astãzi pe piata software.

Deseori se obisnuieste lansarea pe piata utilizatorilor a unei versiuni demonstrative pentru o aplicatie sau un program. Aceasta se caracterizează prin aceea cã este lipsitã de unele functionalitãti vitale. Accesul la toate functiile programului se face numai dupã cumpãrarea licentei de utilizare în varianta sa completã.

Se întelege cã varianta demo nu oferã nici o posibilitate de reconstituire a versiunii complete.

Practica produselor din categoria shareware foloseste o idee asemãnãtoare. Programele cuprind unele limitări functionale si sunt distribuite într-un numãr mare. Eliminarea constrângerilor de functionare se face dupã ce are loc înregistrarea produsului, moment în care se practicã si plata unor sume modice. Programele din aceastã categorie trebuie sã fie atrãgãtoare, sã facã o impresie bunã, încât sã ofere sansa cã vor fi cumpãrate de multi dintre cei care intrã în contact cu ele. Functionalitãtile care lipsesc nu trebuie sã fie esentiale în utilizarea programului, iar cele existente trebuie sã asigure utilizatorul cã are de-a face cu un produs serios.

Introducerea unor executii care iritã utilizatorul în cazul utilizării neautorizate, este o altã practicã cunoscutã pe piata software. Programele din aceastã categorie au toate functiunile de bazã, însã contin unele întârzieri în executie sau dialoguri care deranjeazã, de obicei amintind cã versiunea utilizatã nu este înregistratã oficial. Alte programe abundã în informatii care definesc aproape obsesiv termenii de înregistrare.

O metodã foarte popularã este cea bazatã pe un numãr limitat de executii. Si în acest caz functiunile programului pot fi complete, dar dupã un anumit numãr de lansări în executie sau dupã expirarea unui termen prestabilit programul refuzã orice functionare.

O categorie specialã de programe utilizeazã tehnica upgrade-ului. Asta înseamnã cã, fatã de versiunea initialã, furnizorul vine periodic cu adaosuri si dezvoltări de functii noi, totdeauna mai performante.

12. Alte recomandări privind protectia programelor

Programatorii se pot lãuda, pe bunã dreptate, cã au la îndemânã diverse metode si tehnici pentru a-si proteja propriile programe de pericolul "spargerii" acestora de cãtre hackeri. Multe dintre ele sunt descrise, uneori cu lux de amãnunte, în diverse documentatii, specificatii si metodologii, în standarde, sunt publicate în diverse reviste de specialitate. Si din acest punct de vedere Internetul abundã în informatii despre acest subiect. Existã grupuri de discutii pe aceastã temã foarte bine organizate, întretinute si "vizitate" de multi dintre cei cu o mare experientã, ca si de cei care doresc sã învete câte ceva din acest domeniu.

Primul sfat important pentru protectia programelor, recunoscut ca atare de toti cei implicati în dezvoltarea de software, se referã la acoperirea punctelor slabe dintr-o aplicatie. Aceasta înseamnã ca elementele precum denumirea functiilor utilizate în validarea înregistrãrii, localizarea datelor de licentiere etc., sã fie acoperite suficient de bine, pentru ca utilitarele de detectare folosite de hackeri în scopul "spargerii" protectiei existente sã nu poatã sã le depisteze usor.

Se mai recomandã sã nu se foloseascã nume sugestive de functii pentru numãrul serial sau de fisiere de licentiere. Înaintea operatiilor de autentificare este bine sã se foloseascã niste pauze scurte si totodatã sã se evite folosirea sirurilor de caractere pentru autentificarea în resurse. Tot în aceeasi idee se recomandã si salvarea în mai multe locuri a respectivelor date de autentificare.

Multi programatori utilizeazã o verificare a consistentei fisierelor executabile, utilizând cunoscutele

sume de control si, tot pentru aceste fisiere, aplicã autocorectii în cazul în care sunt. Nu este indicat sã se punã bazã pe diversele sisteme de compresie a executabilelor.

Se recomandã cu acelasi interes si evitarea folosirii dialogurilor de atentionare, care pot fi un indiciu uneori suficient pentru unii hackeri "experimentati".

Pentru criptarea datelor este indicat sã se foloseascã metode proprii sau metode verificate în practicã, pentru a da cât mai multã bãtaie de cap "spãrgãtorilor" de coduri.

Nu se recomandã folosirea datei sistemului de operare în tratarea protectiei, deoarece aceasta poate fi usor "ocolitã" de un hacker, uneori doar prin simpla dare înapoi a ceasului sistemului.

Între douã versiuni consecutive este indicat sã fie modificat codul de protectie pentru a nu da prilejul rãufãcãtorilor sã "recunoascã" usor metoda de protectie folositã. Metodele de upgrade sunt, desigur, cele mai indicate, întrucât ele vin numai cu adaosuri, nu cu întreaga aplicatie.

Alte metode ar putea avea în vedere anumite "siretlicuri" inventate de programator, de exemplu: folosirea cheilor de validare de dimensiune mare, folosirea codurilor de eroare false pentru a semnala o aplicatie spartã, salvarea ultimei date de rulare etc.

De asemenea, este indicat sã se foloseascã, acolo unde este posibil, cuvinte rezervate si coduri numerice accesibile din limbajul respectiv. Ele sunt cu mult mai greu de recunoscut de cãtre "spãrgãtori". Se recomandã sã fie detectate, pe cât posibil, utilitarele folosite de hackeri. Acestea ar trebui sã fie cunoscute pentru a sti cum sã se facã protectia cea mai bunã.

Este bine să se stie că diverse categorii de aplicatii pot utiliza diverse solutii de protectie, unele puse la dispozitie chiar prin instrumentele de dezvoltare.

Un ultim sfat pe care, desigur, îl puteti intui, recomandă să nu fie dezvăluite niciodată altor persoane tehnicile proprii de protectie folosite.

13. Pirateria software

O stire proaspătă anuntă că un studiu recent al FBI plasează România pe locul patru în lume în privinta fraudelor pe Internet. Fraudele în cauză nu sunt altceva decât furturi. Însă, stiind că de curând Ucraina a fost sanctionată de Statele Unite pentru pirateria software si adăugând faptul că în recentul clasament această tară ocupă "fruntasul" loc trei, adică doar un singur loc înaintea noastră, nu este exclus să ne trezim în viitorul apropiat si cu o surpriză de acest gen: România să fie sanctionată pentru fraude comise prin intermediul Internetului, fraude care au atins proportii de-a dreptul îngrijorătoare.

Ca piraterie software se consideră folosirea nepermisă si utilizarea fără drept de autor a software. Plângerile despre pagubele enorme provocate prin copierea ilegală a programelor de calculator sunt în continuă crestere, desi datele statistice redau, si în acest domeniu ca si în altele, numai o parte a realitătii.

Asadar, pirateria software se referă la lezarea drepturilor de autor pentru programe de calculator, drepturi consfintite prin lege. Prin Legea 8/1996 cu privire

la drepturile de autor, denumitã impropriu si legea copyrightului, tara noastrã se pare cã a luat în serios problema protectiei drepturilor de autor si conexe, pentru capitolul privind produsele informatice ea inspirându-se direct din Directiva Comunitarã 91/250 din 14 mai 1991 care este aplicabilã la nivelul Comunit?tii Europene.

Legea 8/1996 defineste autorul unui produs informatic ca fiind o persoanã fizicã sau juridicã, care realizeazã (creeazã) produsul software respectiv. Aceastã persoanã are urmãtoarele prerogative exclusive: reproducerea unui program, traducerea, adaptarea, aranjarea si orice alte transformãri aduse unui program, precum si difuzarea originalului sau a copiilor sub orice formã, inclusiv prin închiriere. Persoana în cauzã, fizicã sau juridicã, detine astfel toate drepturile de autor asupra produsului sãu. Nerespectarea acestor drepturi de cãtre orice altã persoanã fizicã sau juridicã, mai precis folosirea produsului în orice scop fãrã autorizarea expresã a autorului, reprezintã o încãlcare gravã a drepturilor de autor si se pedepseste conform legii.

Legea drepturilor de autor este adaptatã la realitatea românească si, bunã sau rea, trebuie sã recunoastem, ea existã si se cere a fi respectatã.

Pot fi invocate suficiente motive pentru care România se situeazã pe un rusinos loc de frunte în pirateria software. Unul dintre acestea incrimineazã "cultura" insuficientã din acest domeniu a românilor. Practic, românii încã nu s-au obisnuit sã priveascã softul din punct de vedere comercial ca pe un produs oarecare, ce presupune cheltuieli de cercetare, productie si distributie, incluse în pretul produsului.
Pe de altã parte, softul are un pret prea ridicat iar cumpãrãtorii români, pe bunã dreptate, au de ce sã se

plângã.

Tot la fel de adevărat este însă si faptul cã existã o oarecare indiferentã si uneori chiar lipsã de respect, care până la urmã nu înseamnã altceva decât probleme de mentalitate. De aceea, s-ar impune cu necesitate un efort sustinut de educare a celor ce folosesc programe de calculator, implicând pe toti cei implicati în domeniul IT (Information Technology): scoli, facultãti, institutii de stat si particulare, asociatii, mass-media, inclusiv producãtorii de soft.

14. Lupta împotriva pirateriei software

Cea mai frecventã încãlcare a legii în domeniul informatic o reprezintã copierea si difuzarea ilegalã a unui produs informatic, care este sanctionatã conform Legii 8/1996, cu închisoare de la trei luni la trei ani sau cu amendã de la 700.000 la 7.000.000 lei.

Din punct de vedere legal un produs soft contine patru elemente de bazã: materialul de conceptie, programul-sursã (codul sursã), codul obiect (traducerea codului sursã în cod înteles de calculator) si manualul de utilizare, adicã documentatia conexã si cea auxiliarã.

Lipsa unei finalitãti a actiunilor judecãtoresti privind pirateria software este pusã pe seama unor imperfectiuni ale legii copyright-ului si o parte din legislatia vamalã. Dar si lipsa de decizii guvernamentale referitoare la respectarea legii privind protectia drepturilor de autor, coroboratã cu inexistenta unor politici serioase de informatizare a societãtii românesti, sunt cauze care au

condus ca tara noastrã sã ocupe un atât de dezonorant loc în clasamentul mondial al pirateriei software. De ce este dezonorant acest locã Pentru cã, am mai spus-o, pirateria software nu este altceva decât un furt.

La nivel mondial existã o organizatie specializatã OMPI - Organizatia Mondialã a Proprietãtii Intelectuale, care a propus o lege tip în domeniul protectiei produselor informatice, lege care, la nivel european, a fost corelatã cu Directiva CEE - Comunitatea Economicã Europeanã 91/250 din 14 mai 1991 si care este aplicabilã la nivelul Comunitãtii Europene si în acest moment.

În SUA produsele software sunt apãrate printr-o lege intratã în vigoare încã din data de 1 ianuarie 1978, practic aceasta fiind prima lege care a asimilat programul de calculator cu opera literarã.

În Europa, desi existã directiva comunitarã mentionatã mai sus, fiecare tarã, fie membrã sau doar aspirantã la Comunitatea Economicã Europeanã, are propriile legi interne adaptate realitãtilor sociale ale acelei tãri, dar care sunt armonizate cu cele comunitare.

Organizatia guvernamentalã care se ocupã la noi cu protectia drepturilor de autor se numeste ORDA - Oficiul Român pentru Drepturile de Autor. În ultimul trimestru al anului 2000 a fost emisã o ordonantã guvernamentalã si o metodologie de înregistrare oficialã a programelor de calculator în scopul protectiei, RPC - Registrul pentru Programele de Calculator. Cu numai câteva sãptãmâni în urmã i-am vizitat, în scopul clarificãrii modului de înregistrare oficialã a software-ului apartinând Directiei Informatice din Sidex. Nu micã a fost surprinderea când am aflat cã suntem primii care batem la aceastã usã cu asemenea pretentii. Cu alte cuvinte, activitatea privind protectia programelor de calculator lipseste cu

desãvârsire. În schimb este în plinã efervescentã cea din domeniul fonogramelor si a muzicii în general.

Pe lângã ORDA, în tara noastrã îsi mai desfãsoarã activitatea încã o organizatie specializatã si autorizatã international pentru investigarea în domeniul respectãrii drepturilor de autor pentru programele de calculator. Ea se numeste BSA - Business Software Alliance si a desfãsurat în ultimii ani o activitate intensã, dar mai au multe de fãcut în directia informãrii marii mase a utilizatorilor. BSA nu prea verificã marile firme (de stat sau private), ministerele, bãncile, Parlamentul sau Guvernul care, trebuie sã recunoastem, sunt primele institutii cãrora ar trebui sã li se cearã sã respecte legea.

Chiar si unii producãtori de calculatoare au de suferit din cauza pirateriei soft, acestia vânzând calculatorul cu tot soiul de sisteme de operare si produse software preinstalate, dar fãrã licentele corespunzãtoare.

Pe 6 octombrie 1999 s-a pronuntat si prima sentintã penalã din România împotriva unui pirat. La Judecãtoria Ploiesti un administrator al firmei Andantino SRL a fost condamnat la sase luni închisoare, cu suspendarea pedepsei si la plata a 26 milioane lei organizatiei BSA, pentru cã a fost surprins de politie si inspectorii ORDA în timp ce comercializa CD-uri cu programe de calculator la punctul de lucru al societãtii sale.

15. Statistici despre pirateria software

Asa cum s-a mai spus, pirateria software reprezintă folosirea nepermisă si utilizarea fără drept de autor a programelor de calculator.

Legea copyrightului din tara noastră, care reglemetează pirateria software, are în vedere si sanctionarea unor fapte de genul publicării unor programe existente sub un alt nume sau a publicării unui program de asemeni existent, însusindu-si pe nedrept calitatea de autor. Pedeapsa pentru aceste fapte este închisoare de la trei luni la cinci ani sau amendă de la 500.000 la 10.000.000 lei.

Se spune că (si vom vedea mai departe că aproape toate statisticile o confirmă) rata piraterieiei soft din tara noastră este cea mai ridicată: ocupăm, si în acest domeniu, ca în multe altele, primul loc în Europa (fără Rusia).

Conform unor studii efectuate de BSA (Business Software Alliance) si SIIA (Software & Information Industry Association), România ocupă locuri fruntase nu numai în Europa, ci si în lume.

Din punct de vedere istoric, rata piraterieiei din tara noastră a scăzut de la 93% în 1994, la 81% în 1999 si putin sub 80% în anul 2000. Desi în continuă scădere, procentul rămâne totusi îngrijorător si este cel mai ridicat din Europa (în 1999 Rusia detinea 89%).

Statisticile mentionau în urmă cu doi ani că media pentru Europa răsăriteană era de 70%, în timp ce Europa de Vest avea o medie de numai 34% (sub 30% situându-se Marea Britanie cu 26%, Germania cu 27% si Danemarca cu 29%). Este cunoscută si media mondială

de 36%, cu extremele în Vietnam care detine recordul absolut de 98% si SUA care are doar 25%.

Tot în urmã cu doi ani pierderile estimate datorate achizitionării pe cãi ilegale a produselor software au fost de peste 15 milioane dolari. În acelasi an doar 17 cazuri s-au aflat în investigarea organelor de politie din Bucuresti si judetele Constanta, Vâlcea si Cluj, desi numãrul celor depistati si prinsi în flagrant în raidurile efectuate de BSA sunt de 10 ori mai mare.

SIIA a inclus România pe lista tãrilor care trebuie supravegheate de cãtre US Trade Representative. Pe aceeasi listã mai apar: Arabia Saudita, Argentina, Brazilia, Irlanda, Korea, Malaezia, Mexic, Polonia, Singapore, Tailanda, Taiwan si Uruguay.

Pentru cei interesati în a da o mânã de ajutor în lupta împotriva pirateriei software BSA a pus la dispozitie o linie telefonicã Hot Line 01-210.41.54. Ea poate fi folositã pentru cazuri de furturi de programe sau utilizări ilegale din cadrul companiilor, institutiilor financiare, colegii si universitãti, autoritãti locale sau a organizatiilor non-profit.

Un alt top în care România detine tot un loc "fruntas" este cel al tãrilor de provenientã a infractorilor. Din acest punct de vedere România ocupã locul patru în lume, dupã Ucraina.

Societatea, economia si statul se bazează din ce în ce mai mult pe integrarea tehnicii de calcul în aplicatii importante, dar fãrã a analiza riscurile. În acelasi timp, prosperitatea sau ruina firmelor de stat sau particulare au devenit dependente si ele de tehnica de calcul. Promisiunile guvernantilor privind noua Românie conectatã online par si mai îndepãrtate de realitate, dacã avem în vedere cel mai recent sondaj care mentionează

cã tara noastrã alocã cele mai mici sume pentru dezvoltarea IT (Information Technology). Si din acest punct de vedere ocupãm tot primul loc în Europa. Mai precis, într-un an, pe un locuitor se investesc doar 12 dolari. În timp ce Bulgaria se aflã înaintea noastrã, cu 15 dolari/locuitor/an, ca sã nu mai vorbim de Polonia cu 60, Ungaria cu 100 si Cehia cu 140 dolari/locuitor/an.

16. Pirateria software - cauze posibile

În fata dezvoltãrii extraordinare a lumii computerului suntem nevoiti sã recunoastem cã acesta a devenit un instrument autentic de falsificare. Experienta ne aratã cã infractorii se inspirã fãrã reticentã din orice nouã dezvoltare hardware sau software. Rãufãcãtorul care "opera", pânã nu demult, la automatele de jocuri cu sârme, surubelnite, magneti si burghie, astãzi îsi poate permite sã cumpere, contra unor sume relativ mici, un laptop si programe specializate de manipulare.

Încã de acum zece ani au fost identificate si catalogate principalele cauze ale infractiunilor din lumea calculatoarelor. Iatã, într-o prezentare succintã, doar câteva dintre acestea.

Aproape toate activitãtile umane sunt din ce în ce mai dependente de tehnica de calcul. Societatea, economia si statul se bazeazã tot mai mult pe integrarea tehnicii de calcul în aplicatii importante, însã fãrã o analizã serioasã a riscurilor.

Sistemele de calcul dezvoltate în ultimile douã decenii, si cu precãdere calculatoarele de tip IBM-PC, au

fost concepute si proiectate fără să asigure suficient de bine securitatea si controlul. De aceea, chiar si cei neinitiati pot introduce în acestea, constient sau nu, erori prin virusi sau alte programe. Cu probleme asemănătoare se confruntă însă si sistemele de tip Mac-Intosh sau Unix. Practic, s-ar putea spune că nu avem de-a face cu o criminalitate asistată de calculator, ci doar cu existenta unor pericole iminente si posibilităti de abuz, prin însăsi lipsa de securitate a calculatoarelor si retelelor.

În fapt, multi dintre spărgătorii si autorii de virusi nu au motive criminale atunci când "atacă" un calculator străin. Lipsa de etică si/sau de cunostinte privind legislatia si interdictiile, pot determina să nu-si considere preocupările lor ca fiind "criminale".

În plus, se stie că sistemele de calcul foarte răspândite astăzi, precum PC-urile, retele s.a., nu contin componente pentru păstrarea urmelor sau, în cazul mainframe-urilor, acestea sunt deseori neutilizate.

În acelasi timp, organele de cercetare (politie, procuratură) ca si expertii în drept (judecători, avocati) înteleg cu destulă dificultate elementele criminale din domeniul utilizării sistemelor de calcul. Mai sunt si astăzi situatii în care unele procese împotriva spărgătorilor de coduri sunt bazate pe expertize neconvingătoare pentru completul de judecată. Uneori sunt necesare informatii suplimentare pentru ca judecătorul să înteleagă bine natura, obiectul juridic, obiectul material si celelalte elemente care definesc infractiunea. Este bine cunoscut cazul din procesul KGB-ului în care chiar spărgătorii au fost nevoiti să explice judecătorului ce înseamnă “E-mail”.

Statul si economia, societatea în general, au devenit dependente de o tehnică de calcul nesigură. De aceea,

unele abuzuri comise pot fi cu greu considerate drept criminale. În plus, multe din ele nu pot fi urmărite cu eficientă.

Nu în ultimul rând se apreciază că nu există legi sau cele care există au multe "scăpări" si nu sunt suficient de clare. Totodată, o bună parte a delictelor comise cu calculatorul nu sunt si nu pot fi încă descoperite. Nu trebuie să uităm însă că mafia este mai interesată decât societatea si statul să speculeze avantajele extraordinare pe care le oferă tehnica de calcul. Si dacă până acum acest lucru nu pare a fi evident, sunt semne clare că afacerile cu droguri si arme devin mai putin "rentabile" decât afacerile mafiote prin intermediul computerului. Mai mult ca sigur, într-o bună zi mafiotii vor pătrunde si vor încerca să domine această piată inimaginabilă de resurse din domeniul tehnologiei informatiei.

17. Despre furtul de carduri

În bună măsură datorită multiplelor facilităti oferite de reteaua globală Internet, infractionalitatea prin intermediul calculatorului din ultimii ani s-a extins si diversificat. Au apărut astfel câteva noi tipuri de infractori.

Dacă o bună parte din asa-numitii hackeri obisnuiesc doar să-si bage nasul peste tot, din curiozitate sau nu, fără să urmărească neapărat un câstig material, o nouă categorie de ilegalisti, cunoscută în lumea informaticii sub denumirea de *crackeri*, au ca scop bine definit câstigul în bani sau obiecte, obtinut prin spargerea

unor site-uri care contin în bazele de date numere de cărti de credit.

Carderii, asa cum mai sunt numiti acesti infractori, sunt cei care valorificã numerele unor cărti de credite, de la distanta si adăpostul oferite de un fotoliu comod în care stau ceasuri întregi în fata unui computer conectat la Internet. Informatiile pe care le obtin după o muncă deseori istovitoare, sunt folosite pentru a cumpăra de la magazinele on-line diferite produse, pe care le vând apoi la preturi mai mici.

Există multe metode de actiune la îndemâna infractorilor din această categorie. Câteva dintre ele sunt bine-cunoscute, fiind publicate chiar si pe unele site-uri, sau "discutate" în unele grupuri de discutii pe Internet. Altele însă, nu pot fi decât imaginate, rămânând necunoscute, deoarece poartă amprenta inventivitătii "operatorului" însusi care, cel mai probabil, nu si-ar vinde "arta" pentru nimic în lume.

Internetul oferă anumite posibilitãti de accesare a informatiilor utile pentru acest scop. Ajungând la ele, răufăcătorul pune în functiune un program special conceput pentru a genera aleator numere pe structura unor coduri de carduri si, cu putin noroc, poate "nimeri" un număr valid, cu care apoi comandă cu succes diferite obiecte din magazinul on-line vizat. Desigur, totul merge foarte bine, mai ales dacă magazinul respectiv nu are prevăzut un sistem sigur de verificare a cardurilor.

Anumite numere de cărti de credit pot fi aflate uneori si prin intermediul unor persoane "binevoitoare" care, desigur, trebuie plătite pentru serviciile lor. Aceasta este însă o variantă "costisitoare" si nu este preferată de carderi.

Pentru ca operatiunea să se deruleze în bune

conditii până la capăt mai este necesar să se stabilească si o adresă la care marfa comandată să fie expediată. Se întelege, nu acasă trebuie primit acest gen de marfă, pentru că riscul este prea mare. Dar solutii se găsesc întotdeauna, mai ales de către cei ingeniosi.

O regulă bine cunoscută în lumea carderilor este aceea că nu de pe calculatorul de acasă se comandă marfa si nici de pe unul pe care se stie că are acces. Iar solutii pentru această categorie de probleme există suficiente. De exemplu, se poate apela cu usurintă si fără a da nimic de bănuit, la serviciile oferite contra unui cost banal de un Internet Café.

O altă regulă folosită de carderi constă în aceea că o comandă trebuie să se limiteze, de la câteva sute la câteva mii de dolari. Altfel bate la ochi.

Valorificarea mărfii după primire este si ea o treabă care necesită destulă atentie. Regula de aur este să nu vinzi la oricine, iar pretul trebuie să ofere satisfactie si clientului. Se poate apela uneori si la intermediari în scopul pierderii urmei, însă acestia vor dori si ei un comision.

În tara noastră riscurile unei astfel de infractiuni sunt minore, mai ales în conditiile în care nu există nici măcar un cadru legislativ adecvat, cu referiri la acest tip de infractionalitate.

18. Securitatea retelelor

Dupã cum stim, primele retelele de calculatoare au fost folosite în principal de cercetãtorii din universitãti pentru trimiterea postei electronice. Astãzi, milioane de cetãteni din toate colturile lumii folosesc retelele pentru diferite categorii de operatiuni bancare, pentru a face cumpãrãturi, pentru plata unor taxe etc. De aceea, problema securitãtii a devenit una foarte importantã pentru multe din aplicatii. Existã numeroase pericole privind securitatea unei retele. În acelasi timp, existã si multe tehnici pentru a face retelele mai sigure.

Securitatea nu înseamnã altceva decât asigurarea cã persoane neautorizate sau pur si simplu curioase, nu pot avea acces sã citeascã sau, si mai rãu, sã modifice mesajele apartinând altora. Ea vizeazã pe cei care încearcã sã apeleze servicii la distantã pe care nu sunt autorizati sã le foloseascã. În acelasi timp securitatea mai poate implica si verificarea dacã un mesaj provine de acolo de unde trebuie sau vine din altã parte.

Altfel spus, securitatea sistemelor de calculatoare are ca obiect problemele legate de capturarea si falsificarea mesajelor autorizate, ocupându-se totodatã si de cei care nu recunosc faptul cã au trimis anumite mesaje.

Majoritatea problemelor de securitate sunt cauzate în mod intentionat de persoane rãuvoitoare care încearcã sã obtinã anumite beneficii sau sã provoace pur si simplu rãu cuiva. În problemele de securitate avem de-a face, de regulã, cu adversari inteligenti si deseori bine dotati material. De aceea, lupta împotriva lor este foarte dificilã

si deseori este mentinutã la cote foarte înalte de spectaculozitate si interes.

Pentru a câstiga astfel de bãtãlii este nevoie sã-ti cunosti foarte bine adversarii, si înainte de toate, trebuie sã le întelegi motivele. Iatã, într-o prezentare succintã, câteva din principalele motive ale celor care în mod obisnuit sãvârsesc astfel de fapte.

Un elev sau un student oarecare poate sãvârsi o actiune de acest gen pentru a se distra, furând mesajele de postã electronicã a celorlalti. În schimb, un spãrgãtor o face ori pentru a testa securitatea sistemului cuiva, ori pentru a fura datele din calculatorul altuia.

Un om de afaceri poate fi interesat sã descopere planul strategic de marketing al unor competitori, în timp ce, un fost angajat al unei firme poate sãvârsi aceste fapte pentru a se rãzbuna cã a fost concediat.

Un finantist sau un contabil poate viza sustragerea unor sume de bani de la o companie si a le depozita într-un cont propriu. Tot asa si un sarlatan oarecare, care poate fura numere de cãrti de credit pentru a le vinde sau valorifica.

Motive cu totul distincte pot avea spionii sau teroristii: acestia vor urmãri în mod sigur aflarea unor secrete militare sau de alt interes din tabãra inamicului.

În general, securitatea unei retele de calculatoare poate viza urmãtoarele categorii de probleme:

1) *confidentialitatea*, adicã pãstrarea informatiei departe de utilizatorii neautorizati;

2) *autentificarea*, care constã în determinarea identitãtii unei persoane;

3) *nerepudierea*, care are în vedere semnãtura si confirmarea acesteia, si

4) *controlul integritãtii*, adicã siguranta cã mesajul apartine cu adevãrat celui de la care este asteptat.

În practicã, o retea de calculatoare este alcãtuitã din mai multe nivele. Fiecare nivel în parte poate contribui la securitatea acesteia. De exemplu, la nivelul legãturã de date pachetele transmise pe o linie punct-la-punct pot fi codificate când pãrãsesc una dintre masini si decodificate când intrã în cealaltã.

Dacã unele sesiuni trebuie sã fie în mod obligatoriu protejate, de exemplu acelea care implicã cumpãrãturile on-line prin cãrti de credit, altele nu necesitã neapãrat acest lucru. Nivelul cel mai important pentru asigurarea securitãtii unei retele este nivelul aplicatie. La acest nivel apare necesitatea utilizãrii unor protocoale suport care sã permitã functionarea aplicatiilor. Securitatea nu este asiguratã de un singur protocol, ci de un mare numãr de concepte si protocoale. Acestea sunt folosite pentru asigurarea securitãtii pentru aplicatiile care necesitã acest lucru.

19. Criptarea si decriptarea mesajelor

Arta de a concepe si construi cifruri se numeste criptografie iar cea de a sparge cifruri se numeste criptanalizã. Împreunã, acestea alcãtuiesc stiinta numitã criptologie.

Criptografia are o traditie veche. Ea a fost inventatã de cãtre cei care au vrut ca mesajele lor scrise sã fie secrete. Cele mai importante aplicatii au fost însã în domeniul militar. Întrucât a existat dintotdeauna pericolul

descifrării unui cod, singura solutie de protectie folosită la acea vreme se baza pe schimbarea rapidă a metodei de criptare.

Mesajul care trebuie criptat poartă numele de text clar, în timp ce mesajul criptat este cunoscut sub numele de text cifrat. Pentru a cripta si/sau decripta un mesaj este nevoie de o cheie. Asadar, în cazul în care inamicul reuseste să capteze mesajul, dacă nu cunoaste cheia, nu-l va putea descifra decât rareori si cu o mari dificultăti. O regulă fundamentală, utilizată în criptografie, presupune cunoasterea de către orice criptanalist a metodei generale de criptare. O cheie secretă are avantajul că poate fi schimbată ori de câte ori este nevoie; deci nu se schimbă metoda, ci doar cheia.

Cu cât cheia are o lungime mai mare, cu atât algoritmul de decriptare presupune un efort mai mare. O căutare exhaustivă în spatiul cheilor ar conduce la un efort exponential în raport cu lungimea acestora. Se apreciază uneori că secretul este acela de a avea un algoritm puternic, dar public, dimpreună cu o cheie suficient de lungă.

Este eronată aprecierea că, dacă un cifru poate rezista unui atac, atunci acesta este sigur. Desigur, există si cazuri în care criptanalistul poate ghici unele părti din textul clar.

În criptografia modernă se folosesc două tipuri de cifruri: cu substitutie si cu transpozitie. Primul se bazează pe faptul că fiecare literă sau grup de litere este înlocuit pentru deghizare cu altă literă sau alt grup de litere. Deci cifrurile cu substitutie păstrează ordinea simbolurilor din textul clar, dar le deghizează. În schimb, cele cu transpozitie reordonează literele, dar nu le deghizează.

Identificarea tipului de cifru este o problemă dificilă

pentru orice criptanalist. Acestia analizează frecventa de aparitie a unei litere si alte caracteristici specifice limbii respective (de exemplu, frecventa grupurilor de două sau mai multe litere). Incluzând si alte tehnici specifice acestei munci, criptanalistul poate ajunge mai întâi la rezolvarea dilemei privind tipul cifrării, apoi va trece la descifrarea cheii si a textului cifrat.

Construirea unui cifru imposibil de spart se face astăzi destul de simplu: ea se bazează pe alegerea unui sir aleator de biti pe post de cheie, după care se converseste textul clar într-un sir de biti. În final se aplică o operatie logică între cele două siruri, bit cu bit. Textul cifrat rezultat nu poate fi spart, deoarece orice text clar posibil este în mod egal un probabil candidat, fiecare literă apare la fel de des si deci textul cifrat nu furnizează absolut nici o informatie criptanalistului. Metoda cheilor acoperitoare, căci asa se numeste, are însă si unele dezavantaje: cheia nu poate fi memoratã, deci necesită o copie scrisă a acesteia, lungimea textului cifrat este limitată de dimensiunea cheii etc.

Metoda devine însă foarte utilă atunci când beneficiem de ajutorul calculatorului. Cheia, memoratã pe un CD special si "amestecată" cu ceva muzică, nu dă niciodată de bănuit.

Criptografia aplicată pe calculator se bazează pe două principii: 1) un mesaj criptat trebuie să conțină informatie redundantă, care nu ajută la întelegerea mesajului, dar împiedică intrusii să păcălească receptorul trimitând un mesaj fals. 2) sunt necesare unele măsuri pentru a împiedica intrusii să retransmită mesaje mai vechi. Se obisnuieste introducerea în fiecare mesaj a unei amprente de timp, validă doar pentru un termen scurt.

Desi are un caracter mai putin general, utilizarea algoritmilor cu cheie secretã este o metodã destul de puternicã. Criptografia modernã utilizeazã algoritmi de diverse tipuri, inclusiv metodele traditionale. Obiectivul este ca acestia sã fie complecsi si ireversibili, astfel încât un criptanalist sã nu poatã descifra mesajele. Uneori se adaugã un numãr suficient de mare de niveluri, astfel ca cifrul sã fie o functie extrem de complicatã.

Multi algoritmi foarte greu de spart sunt cu cheie publicã si se bazeazã pe calculul logaritmilor discreti sau pe curbe eliptice, pe dificultatea factorizãrii numerelor mari etc.

Existã asadar, numerosi algoritmi de criptare, dar existã si standarde în domeniul criptãrii, adoptate de unele tãri pentru anumite categorii de mesaje. De exemplu, Agentia americanã secretã NSA-National Security Agency, este o agentie spãrgãtoare de coduri, care utilizeazã cel mai mare numãr de specialisti matematicieni, informaticieni si criptologi din lume.

Si telefonia a gãsit solutii pentru a controla confidentialitatea mesajelor. Un recent pachet software, Ositron Tel 2.1, ce poate fi cumpãrat cu numai 200 DM, criptează în timp real cuvintele rostite, astfel încât un intrus nu poate auzi decât sunete nearticulate.

20. Semnãturile digitale

Dacã mesajele sãpate în piatrã au dãinuit vreme de milenii în aceleasi locuri, în schimb datele prelucrate de calculatoarele de astãzi pot fi transportate oriunde în

lume.

Tot din vremuri străvechi vine si credinta în păstrarea adevărului prin documente scrise. “Verba volant, scripta manent”, spune un vechi proverb latin. Odată cu aparitia tiparului lumea scrisului a fost zguduită puternic. Astăzi, calculatoare puternice, echipate cu scanere, imprimante laser si color si cu programe performante de grafică avansată, pot produce “minciuni autentice”. Mai mult, alături de documente falsificate, se pot atasa si fotografii false. Digitizarea fotografiilor cu ajutorul unui scanner si un editor grafic micsorează astăzi valoarea de dovadă a pozelor sau a negativelor. Depunerea rezultatului pe hârtie sau dischetă si transmiterea lui unui atelier pentru executarea unui diapozitiv sau a unui negativ color nu este deloc o treabă dificilă. Aparatele foto cu schitare digitală reprezintă un progres imens al sfârsitului de mileniu.

În conditiile în care fotocopiile nu sunt valabile, autenticitatea multor documente legale, financiare si de alt gen, este determinată de prezenta sau absenta unor semnături autorizate scrise de mână. Pe sistemele de calcul este necesară înlocuirea transportului fizic al documentelor scrise cu cernealã pe hârtie, cu altceva care să rezolve problema autentificării. Problema de a concepe un înlocuitor pentru semnăturile scrise de mână este destul de dificilă. De fapt, este necesar un sistem prin care una din părti poate trimite mesaje "semnate" celeilalte părti, astfel încât:

1) destinatarul să poată verifica identitatea pretinsă de expeditor - de exemplu, în sistemele financiare,

2) expeditorul să nu poată renega mai târziu

continutul mesajului - de exemplu, pentru protejarea destinatarului împotriva fraudei, si

3) destinatarul să nu poată să pregătească el însusi mesajul.

Ca si criptarea, semnăturile digitale pentru autentificare pot folosi chei secrete. Acestea sunt păstrate de către o autoritate centrală care stie totul si în care oricine are încredere. Fiecare utilizator alege o cheie secretă si o depune personal la autoritatea centrală. Atunci când clientul trimite un mesaj în clar semmnat, receptorul îl trimite la oficiul central, îl decriptează si îl reprimeste în clar cu o amprentă de timp. Dezavantajul acestei metode este acela că oricine trebuie să aibă încredere în autoritatea centrală, care poate citi toate mesajele semnate. Oficiul central apartine, de regulă, unui guvern, unei bănci sau oamenilor legii. Cu toate acestea, astfel de organizatii nu inspiră suficientă încredere cetătenilor. De aceea, sunt preferate de multe ori solutii care elimină existenta unei autorităti de încredere.

Tehnica semnăturilor digitale utilizează si chei publice. Dacă însă transmitătorul dezvăluie cheia secretă, atunci oricine poate transmite mesajul, inclusiv receptorul. Alt dezavantaj se poate manifesta atunci când transmitătorul decide să-si schimbe cheia periodic. Si în acest caz apare necesitatea ca o autoritate să înregistreze toate schimbările de chei si datele acestora. Cu toate aceste inconveniente, orice algoritm cu cheie publică poate fi folosit pentru semnături digitale. Standardul recunoscut în industrie este algoritmul RSA, dar există si alte variante, de exemplu, NIST-National Institute of Standard and Technology, propus în 1991 si devenit azi standardul DSS - Digital Signature Standard.

Acesta din urmă foloseste ca principiu de bază dificultatea calculului logaritmilor discreti în locul factorizării numerelor mari.

Tehnicile de semnătură digitală sunt criticate uneori pentru că înglobează în acelasi timp două functii distincte: autentificarea si confidentialitatea. Dacă autentificarea este necesară foarte des, confidentialitatea poate să nu fie necesară în multe din aplicatiile practice. Criptarea fiind un procedeu considerat lent, adeseori se doreste să existe posibilitatea de a se trimite documente ca text clar, însă semnate. În acest caz se aplică o tehnică bazată pe rezumate de mesaje, pentru rapiditatea criptării unui text cu un algoritm cu cheie publică.

O nouă tehnică, descoperită în 1979, este cunoscută sub numele de atacul zilei de nastere. Folosind idei împrumutate din teoria probabilităţii, ea are avantajul că reduce substantial numărul de operatii pentru criptare.

În general, implicatiile securităţii unei retele pentru securitatea individuală si a societăţii pot fi puternice. Unele consecinte pot atinge probleme sensibile, precum: algoritmii nu trebuie dezvăluiti; nici unui guvern nu-i convine ca cetătenii săi să aibă secrete fată de el; unele tări interzic cu desăvârsire criptografia neguvernamentală, doar guvernul detinând toate cheile utilizate. Deseori, intervin si oamenii legii care, sub motivatia de a prinde criminalii, doresc să impună diferite procedee de control.

Partea a II-a

VIRUSII CALCULATOARELOR

Scurtã istorie a virusilor

Istoria virusilor de calculatoare este lungã si interesantã. Dar ea a devenit cu adevãrat palpitantã abia din momentul în care a început sã se dezvolte industria PC-urilor. Pe mãsurã ce dezvoltarea acestor calculatoare noi progresa, a devenit posibilã si accesarea a mai mult de un program într-un singur computer. În acelasi timp, s-a manifestat si o reactie împotriva a tot ceea ce însemna computerul. Aceastã tendintã are rãdãcini mai vechi, dar impactul computerelor de tip PC a fost asa de mare, încât si reactiile împotriva acestora au început sã se facã mai evidente.

În anul 1986, niste programatori de la Basic&Amjad au descoperit cã un anumit sector dintr-un floppy disk contine un cod executabil care functiona de câte ori porneau computerul cu discheta montatã în unitate. Acestora le-a venit ideea înlocuirii acestui cod executabil cu un program propriu. Acest program putea beneficia de memorie si putea fi astfel copiat în orice dischetã si lansat de pe orice calculator de tip PC. Ei au numit acest program virus, ocupând doar 360 KB dintr-un floppy disc.

În acelasi an, programatorul Ralf Burger a descoperit cã un fisier poate fi fãcut sã se autocopieze, atasând o copie într-un alt director. El a fãcut si o demostratie despre acest efect pe care l-a numit VirDem (Virus Demonstration). Acesta a reprezentat un prim exemplu de virus, autentic dar destul de nevinovat, întrucât nu putea infecta decât fisierele cu extensia

.COM.

La scurt timp au început să aparã numerosi virusi, fabricati peste tot în lume. Ei au evoluat rapid, luând diverse forme si înglobând idei din ce în ce mai sofisticate.

Iatã o scurtã dar spectaculoasã evolutie a fabricării în serie în toate colturile lumii si lansării pe piatã a virusilor:

- în anul 1990 erau cunoscuti si catalogati 300 de virusi
- în anul 1991 existau peste 1000 de virusi
- în anul 1994 erau înregistrati peste 4000 de virusi
- în anul 1995 s-au înregistrat pseste 7000 de virusi

Anul 1995 este cunoscut ca fiind si anul în care a început să aparã conceptul de macrovirus, devenind în scurt timp o adevãratã amenintare, deoarece erau mult mai usor de fabricat decât pãrintii lor virusii. Acestia nu erau adresati numai anumitor platforme specifice, precum Microsoft Word pentru Windows 3.x/95/NT si Macintosh, astfel încât ei puteau fi folositi pentru orice program, usurându-se calea de aparitie a cunoscutilor microvirusi care au infestat fisierele la acea vreme produsul Lotus AmiPro.

Primul dintre macrovirusi a fost cel folosit în Word si Word Basic. În luna iulie 1996 a apărut si primul microvirus cunoscut sub numele ZM.Laroux care era destinat distrugerii produsului Microsoft Excel.

Ce este un virus de calculator

Nu ne-am propus în aceste capitole să lămurim complet problema si să discutăm toate particularitătile referitoare la virusii calculatoarelor. Ne-am propus doar să abordăm acest subiect din punct de vedere al realitătii obiective, pornind de la faptul că acesti virusii există, sunt o realitate de multă vreme si fac mult rău. Ne-am propus, totodată, să întelegem mai bine ce reprezintă acesti virusi ai calculatoarelor, cum se răspândesc ei, ce amenintă si cum ne putem apăra împotriva lor. În fine, vom prezenta câteva exemple, dintre cele mai concludente, si vom descrie pagubele produse. În fine, vom discuta si despre metodele practice de a combate acest flagel.

Mai precizăm că aceste capitole nu au deloc pretentia de a epuiza subiectul. Ele se adresează acelor utilizatori care folosesc calculatorul aproape zilnic dar nu-l cunosc suficient de bine. Ca urmare, nu vom oferi nici un lucru nou pentru programatorii, inginerii de sistem sau administratorii de sisteme, baze de date sau aplicatii. Cu alte cuvinte, nu-i vom putea ajuta în mod deosebit pe adevăratii specialisti ai calculatoarelor, interesati de această problemă în cele mai mici detalii.

A fost cu adevărat o mare surpriză pentru omenire atunci când a descoperit, acum câteva decenii, si a trebuit să accepte ideea existentei unor virusi de altă natură decât cea biologică.

Un virus de calculator, sau virus informatic asa cum i se mai spune, nu este altceva decât un program de dimensiuni mici, construit cu scopul de a face o glumă sau de a sabota pe cineva. Acest program are, de regulă,

proprietatea cã se autoreproduce, atasându-se altor programe si executând operatii nedorite si uneori de distrugere.

Dimensiunile mici ale programului-virus reprezintã o caracteristicã importantã, întrucât autorii tin foarte mult ca produsul lor cu intentii agresive sã nu fie observat cu usurintã.

Asa cum am mentionat deja, când un virus infectează un disc, de exemplu, el se autoreproduce, atasându-se la alte programe, inclusiv la programele vitale ale sistemului. Ca si în cazul unui virus real, efectele unui virus al calculatorului pot sã nu fie detectate o perioadã de mai multe zile sau sãptãmâni, timp în care, orice disc introdus în sistem poate fi infectat cu o copie ascunsã a virusului.

Atunci când apar, efectele sunt diferite, variind de la mesaje glumete la erori în functionarea programelor de sistem sau stergeri catastrofice a tuturor informatiilor de pe un hard disk. De aceea nu este indicat sã se plece de la ipoteza cã un virus nu înseamnã ceva mai mult decât o glumã.

În general, cei care construiesc virusi sunt programatori autentici, cu experientã bogatã si cu cunostinte avansate în limbajul de programare pe care îl folosesc. Elaborarea de virusi este uneori si o activitate de grup, în care sunt selectati, antrenati si plãtiti cu sume uriase specialistii de înaltã clasã.

Virusul informatic este, asadar, un program rãu intentionat, introdus în memoria calculatorului, care la un moment dat devine activ, atacând prin distrugere sau alterare fisiere sau autocopiindu-se în fisiere aflate pe diferite suporturi magnetice. Fiecare program infectat poate la rândul sãu sã infecteze alte programe.

Virusul este caracterizat de urmãtoarele proprietãti:

- poate modifica fisiere si programe ale utilizatorilor, prin inserarea în acestea a întregului cod sau numai a unei pãrti speciale din codul sãu

- modificãrile pot fi provocate nu numai programelor, ci si unor grupuri de programe

- are nevoie si poate sã recunoascã dacã un program a fost deja infectat pentru a putea interzice o nouã modificare a acestuia.

Fiecare virus se autoidentificã, în general pentru a evita sã infecteze de mai multe ori acelasi fisier. Identificatorul recunoscut de virus are sensul de "acest obiect este infectat, nu-l mai infectez".

Controversata problemã a virusilor de calculatoare a nãscut ideea cã orice virus poate fi combãtut, adicã depistat si anihilat. Cu toate acestea, existã programatori care sustin cã pot construi virusi ce nu pot fi detectati si distrusi. Este cazul unui grup de programatori polonezi care au anuntat pe Internet, în urmã cu câtiva ani, cã pot construi astfel de "arme" imbatabile. Programul lor, bine pus la punct, continea câteva idei interesante care, dacã ar fi fost duse la capãt, probabil cã ar fi dat multã bãtaie de cap utilizatorilor de servicii Internet. Supãrati de faptul cã lumea a exagerat atât de mult cu costurile pe care le-a provocat virusul cunoscut sub numele de "ILoveYou", acesti programatori intentionau sã demonstreze întregii lumi cã nu acest mult prea mediat virus este cel mai "tare". Dupã pãrerea lor, ar putea fi construiti virusi care pot distruge cu mult mai mult decât a fãcut-o "ILoveYou", adicã o pagubã la scarã planetarã estimatã atunci la circa 6 miliarde de dolari SUA. În plus, autorii au expus metode noi de reproducere a virusilort, fãrã posibilitãti prea mari de a putea fi depistati si anihilati.

Intentiile, fãcute publice de acesti indivizi, pãreau dintre cele mai diabolice. Din fericire, se pare cã acest plan diabolic nu a fost pânã la urmã dus la capãt, amenintãrile acestor indivizi oprindu-se doar la faza de proiect. Totusi, aceste amenintări au putut avea mãcar efectul unui adevãrat semnal de alarmã. A fost avertizatã întreaga omenire cã pot exista si din acest punct de vedere amenintări dintre cele mai serioase care, desigur, nu ar trebui deloc neglijate.

Clasificarea virusilor

Virusii informatici nu afectează numai buna functionare a calculatoarelor. Printr-o proiectare corespunzãtoare a pãrtii distructive, cu ei pot fi realizate si delicte de spionaj sau fapte ilegale de santaj si constângere.

Virusii pot fi clasificati dupã diferite criterii: modul de actiune, tipul de amenintare, grade de distrugere, tipul de instalare, modul de declansare etc. Existã unele clasificări mai vechi care, desigur, nu mai corespund astãzi. Totusi, o enumerare a acestora este benefică, deoarece ea reflectã diversitatea caracteristicilor si tipurilor de virusi. Iatã o astfel de clasificare, oferind pentru câteva variante mai interesante si unele detalii (în aceastã prezentare a fost preferatã ordinea alfabeticã, pentru a putea fi consultatã ca pe un dictionar):

. **Bacteria** - este programul care se înmulteste rapid si se localizează în sistemul gazdă, ocupând procesorul si memoria centrală a calculatorului, provocând paralizia completă a acestuia.

. **Bomba** (Bomb) - este un mecanism, nu neapărat de tip viral, care poate provoca în mod intentionat distrugerea datelor. Este de fapt ceea ce face faima virusilor. Pentru utilizator efectele pot varia de la unele amuzante, distractive, până la adevărate catastrofe, cum ar fi stergerea tuturor fisierelor de pe hard disk.

. **Bomba cu ceas** (Timer bomb) - este un virus de tip bombă, numit si bombă cu întârziere, programat special pentru a actiona la un anumit moment de timp. Este de fapt, o secventă de program introdusă în sistem, care intră în functiune numai conditionat de o anumită dată si oră. Această caracteristică foarte importantă face ca procesul de detectare să fie foarte dificil, sistemul putând să functioneze corect o bună perioadă de timp. Actiunea lui distructivă este deosebită, putând sterge fisiere, bloca sistemul, formata hard disk-ul si distruge toate fisierele sistem.

. **Bomba logică** (Logic bomb) - este un virus de tip bombă, care provoacă stricăciuni atunci când este îndeplinită o anumită conditie, precum prezenta ori absenta unui nume de fisier pe disc. De fapt, reprezintă un program care poate avea acces în zone de memorie în care utilizatorul nu are acces, caracterizându-se prin efect distructiv puternic si necontrolat. O astfel de secventă de program introdusă în sistem, intră în functiune numai conditionat de realizarea unor conditii prealabile.

. **Calul troian** (Trojan horse) - reprezintă

programul care, aparent este folositor, dar are scopul de distrugere. Este un program virus a cărui executie produce efecte secundare nedorite, în general neanticipate de către utilizator. Printre altele, acest tip de virus poate da pentru sistem o aparentă de functionare normală.

Calul troian este un program pe calculator care apare pentru a executa functii valide, dar contine ascunse în codul său instructiuni ce pot provoca daune sistemelor pe care se instalează si rulează, deseori foarte severe.

Un exemplu foarte cunoscut astăzi de un astfel de program este cel numit Aids Information Kit Trojan. Pe un model de tip "cal troian" s-a bazat marea păcălealã care a stârnit multă vâlvă la sfârsitul anului 1989. Peste 10.000 de copii ale unui disc de calculator, care păreau să conţină informatii despre SIDA, au fost expediate de la o adresă bine cunoscută din Londra, către corporatii, firme de asigurări si profesionisti din domeniul sănătătii, din Europa si America de Nord. Destinatarii care au încărcat discurile pe calculatoarele lor, au avut surpriza să descopere destul de repede că acolo se aflau programe de tip "cal troian", toate extrem de periculoase. Aceste programe au reusit să steargă complet datele de pe hard disk-urile pe care au fost copiate.

Programele de tip "cal-troian" mai contin o caracteristică importantă. Spre deosebire de virusii obisnuiti de calculator, acestia nu se pot înmulti în mod automat. Acest fapt nu constituie însă o consolare semnificativă pentru cineva care tocmai a pierdut zile si luni de muncă pe un calculator.

. **Viermele** (Worm) - este un program care, inserat într-o retea de calculatoare, devine activ într-o statie de lucru în care nu se rulează nici un program. El

nu infectează alte fisiere, asa cum fac adevăratii virusi. Se multiplică însă în mai multe copii pe sistem si, mai ales, într-un sistem distribuit de calcul. În acest fel "mănâncă" din resursele sistemului (RAM, disc, CPU etc.).

. **Virus** (Virus) - este un program care are functii de infectare, distructive si de incorporare a copiilor sale în interiorul altor programe. Efectele distructive nu pot fi sesizate imediat, ci după un anumit timp. Notiunea mai generală se referă adesea cu termenul de "virus informatic". Este de fapt un program care are proprietatea că se autocopiază, astfel încât poate infecta părti din sistemul de operare si/sau programe executabile. Probabil că principala caracteristică pentru identificarea unui virus este aceea că se duplică fără acordul utilizatorului. Asa cum sugerează si numele, analogia biologică este relativ bună pentru a descrie actiunea unui virus informatic în lumea reală.

. **Virus al sectorului de boot** (Boot sector virus) - este un tip de virus care distruge starea initială a procesului de încărcare. El suprascrie sectorul de boot al sistemului de operare. Un virus al sectorului de boot (încărcare) atacă fie sectorul de încărcare principal, fie sectorul de încărcare DOS de pe disc. Toti virusii sectorului de încărcare modifică într-un anume fel continutul sectorului de boot. Modificările sectorului de boot nu trebuie să fie prea extinse: unii virusi mai noi din această categorie sunt capabili să infecteze discul fix, modificând doar zece octeti din acest sector.

. **Virus atasat** (Appending virus) - este un virus care îsi atasează codul la codul existent al fisierului, nedistrugând codul original. Primul care se execută atunci când se lansează fisierul infectat este virusul. Apoi,

acesta se multiplicã, face sau nu ceva stricãciuni, dupã care redã controlul codului original si permite programului sã se execute normal în continuare. Acesta este modul de actiune al unui "virus clasic".

. **Virus companion** (Companion virus) - este un virus care infectează fisiere de tip .EXE prin crearea unui fisier COM având acelasi nume si continând codul viral. El speculează o anumitã caracteristicã a sistemului DOS prin care, dacã douã programe, unul de tip .EXE si celãlalt de tip .COM, au acelasi nume, atunci se executã mai întâi fisierul de tip .COM.

. **Virus criptografic** (Crypto virus)- un virus care se infiltrează în memoria sistemului si permite folosirea absolut normalã a intrãrilor si transmiterilor de date, având proprietatea cã, la o anumitã datã, se autodistruge, distrugând în acelasi timp toate datele din sistem si fãcându-l absolut inutilizabil. Un astfel de atac poate fi, pur si simplu, activat sau anihilat, chiar de către emitător aflat la distantã, prin transmiterea unei comenzi corespunzãtoare.

. **Virus critic** (Critical virus) - este un virus care pur si simplu se înscrie peste codul unui fisier executabil fãrã a încerca sã pãstreze codul original al fisierului infectat. În cele mai multe cazuri, fisierul infectat devine neutilizabil. Cei mai multi virusi de acest fel sunt virusi vechi, primitivi, existând însã si exceptii.

. **Virus cu infectie multiplã** (multi-partite virus) - este un virus care infectează atât sectorul de boot, cât si fisierele executabile, având caracteristicile specifice atât ale virusilor sectorului de încãrcare, cât si ale celor paraziti. Acest tip de virus se atasează la fisierele executabile, dar îsi plasează codul si în sistemul de operare, de obicei în MBR sau în sectoarele ascunse.

Astfel, un virus cu infectie multiplã devine activ dacã un fisier infectat este executat sau dacã PC-ul este încãrcat de pe un disc infectat.

. **Virus de atac binar** - este un virus care opereazã în sistemul de "cal troian", continând doar câtiva biti pentru a se putea lega de sistem, restul fiind de regulã mascat ca un “program neexecutabil”

. **Virus de legãturã** (Link virus) - este un virus care modificã intrãrile din tabela de directoare pentru a conduce la corpul virusului. Ca si virusii atasati, virusii de legãturã nu modificã continutul însusi al fisierelor executabile, însã alterează structura de directoare, legând primul pointer de cluster al intrării de directoare corespunzatoare fisierelor executabile la un singur cluster continând codul virusului. Odatã ce s-a executat codul virusului, el încarcã fisierul executabil, citind corect valoarea cluster-ului de start care este stocatã în altã parte.

. **Virus detasabil** (File jumper virus) - este un virus care se dezlipeste el însusi de fisierul infectat exact înaintea deschiderii sau executiei acestuia si i se reatasează atunci când programul este închis sau se terminã. Aceastã tehnicã este foarte eficientã împotriva multor programe de scanare si scheme de validare, deoarece programul de scanare va vedea un fisier "curat" si va considera cã totul este în regulã. Aceasta este o tehnicã de ascundere (stealth).

. **Virus invizibil** (Stealth virus) - este un virus care îsi ascunde prezenta sa, atât fatã de utilizatori, cât si fatã de programele antivirus, de obicei, prin interceptarea serviciilor de întreruperi.

. **Virus morfic** (Morphic virus) - un virus care îsi schimbã constant codul de programare si configurarea

în scopul evitării unei structuri stabile care ar putea fi usor identificatã si eliminatã.

. **Virus nerezident** (Runtime virus) - este opusul virusului rezident. Virusii nerezidenti în memorie nu rãmân activi dupã ce programul infectat a fost executat. El opereazã dupã un mecanism simplu si infecteazã doar executabilele atunci când un program infectat se executã. Comportarea tipicã a unui astfel de virus este de a cãuta un fisier gazdã potrivit atunci când fisierul infectat se executã, sã-l infecteze si apoi sã redea controlul programului gazdã.

. **Virus parazit** (Parasitic virus) - este un virus informatic, care se ataseazã de alt program si se activeazã atunci când programul este executat. El poate sã se ataseze fie la începutul programului, fie la sfârsitul sãu, ori poate chiar sã suprascrie o parte din codul programului. Infectia se rãspândeste, de obicei, atunci când fisierul infectat este executat. Clasa virusilor paraziti poate fi separatã în douã: virusii care devin rezidenti în memorie dupã executie si cei nerezidenti. Virusii rezidenti în memorie tind sã infecteze alte fisiere, pe mãsurã ce acestea sunt accesate, deschise sau executate.

. **Virus polimorf** (Polymorphic virus) - este un virus care se poate reconfigura în mod automat, pentru a ocoli sistemele de protectie acolo unde se instalează. El este criptat si automodificabil. Un virus polimorfic adaugã aleator octeti de tip "garbage" (gunoi) la codul de decriptare si/sau foloseste metode de criptare/decriptare pentru a preveni existenta unor secvente constante de octeti. Rezultatul net este un virus care poate avea o infãtisare diferitã în fiecare fisier infectat, fãcând astfel mult mai dificilã detectarea lui cu un scaner.

. **Virus rezident** (Rezident virus) - este un virus care se autoinstalează în memorie, astfel încât, chiar mult timp după ce un program infectat a fost executat, el poate încă să infecteze un fisier, să invoce o rutină "trigger" (de declansare a unei anumite actiuni) sau să monitorizeze activitatea sistemului. Aproape toti virusii care infectează MBR-ul sunt virusi rezidenti. În general, virusii rezidenti "agată" codul sistemului de operare.

Marea majoritate a virusilor actuali folosesc tehnici de ascundere. Există si un termen des folosit în acest domeniu; el se numeste stealth (ascundere) si desemnează tehnicile folosite de anumiti virusi care încearcă să scape de detectie. De exemplu, un lucru pe care-l pot face virusii rezidenti, este să intercepteze comenzile (functiile) DOS de tip DIR si să raporteze dimensiunile originale ale fisierelor, si nu cele modificate datorită atasării virusului. Tehnicile Spawning si File Jumper reprezintă metode de ascundere, fiind însă cu mult mai avansate.

Virusii spioni

Pe lângă numerosii virusi, cunoscuti la această oră în lumea calculatoarelor, există o categorie aparte de astfel de "intrusi", care au un rol special: acela de a inspecta, în calculatoarele sau retelele în care pătrund, tot ceea ce se petrece, si de a trimite înapoi la proprietar, la o anumită dată si în anumite conditii, un raport complet privind "corespondenta" pe Internet si alte "actiuni"

efectuate de către cel spionat prin intermediul calculatorului.

Practic, un astfel de virus nu infectează calculatorul si, mai ales, nu distruge nimic din ceea ce ar putea să distrugă. El se instalează, de regulă, prin intermediul unui mesaj de poştă electronică si asteaptă cuminte până apar conditiile unui răspuns la aceeasi adresă. Cât timp se află în retea, acesta culege informatiile care îl interesează, le codifică într-un anumit mod, depunându-le într-o listă a sa si apoi le transmite la proprietar.

Un virus de acest gen poate pătrunde si se poate ascunde, de exemplu, într-un fisier tip "doc" primit printr-un e-mail. El îsi începe activitatea odată cu închiderea unui document activ, atunci când verifică dacă acesta a fost infectat cu o anumită parte din codul său special.

Unii virusi din această categorie îsi i-au măsuri ca să nu fie depistati si distrusi de programele de dezinfectare.

Într-o secventă de cod, după o verificare si un control al liniilor, intrusul începe să înregistreze diferite mesaje si actiuni, le adaugă la lista sa secretă si asteaptă conditiile ca să le transmită la destinatar, nimeni altul decât cel care l-a expediat.

În unele variante ale sale de pe Internet acest tip de virus poate face singur o conexiune la o adresă pe care o identifică singur. După aceasta, totul devine foarte simplu. E ca si cum în casa noastră se află permanent cineva care asistă din umbră la toate convorbirile noastre secrete si nesecrete si, atunci când are prilejul, le transmite prin telefon unui "beneficiar" care asteaptă.

Din păcate, virusii spioni sunt de multe ori neglijati. Nici chiar programele de dezinfectare nu sunt prea preocupate să-i ia în seamă si să-i trateze, motivul principal fiind acela că ei nu au o actiune distructivă

directã.

Totusi, pagubele pot fi uneori însemnate, nemaipunând la socotealã si faptul cã nimeni pe lumea aceasta nu si-ar dori sã fie "controlat" în intimitatea sa. Un astfel de spion poate sta mult si bine într-un calculator, dacã nu este depistat la timp si înlãturat de un program serios de devirusare. Este, desigur, un adevãrat semnal de alarmã, pentru simplul motiv cã asemenea "intrusi" existã si pot pãtrunde în viata noastrã si pe aceastã cale.

Un astfel de virus spion a fost descoperit de un student în primãvara anului 1999, în reteaua de calculatoare a dezvoltatorilor de software ai Directiei Informaticã din CS Sidex SA. Desi la aceastã orã este cunoscut si numele celui care a promovat virusul cu pricina, o firmã de software din Bucuresti, din motive lesne de înteles nu-i vom dezvãlui numele aici. Scris în limbajul VBS, virusul nu a apucat sã-si facã "datoria", aceea de a colecta informatii confidentiale si diferite tipuri de documente active, deoarece a fost depistat la timp si înlãturat. Prezentãm, totusi, pe scurt, descrierea acestuia si modul sãu de actiune:

- virusul a apãrut în retea printr-un document de tip ".doc" atasat unui mesaj de postã electronicã
- el s-a declansat odatã cu închiderea documentului respectiv
- câteva linii speciale de cod ale virusului se autocopiau în anumite documente active si template-uri
- la închiderea documentului respectiv, verifica dacã a reusit infestarea, apoi actualiza un fisier propriu cu anumite informatii de genul: data si ora, numele taskului lansat, adresa etc.

- cu adresa captatã, prin intermediul FTP expedia la destinatie lista cu informatiile culese, împreunã cu documentul infestat

- transmiterea se fãcea în ziua de 1 a fiecãrei luni, în conditiile în care protectia de pe calculatorul gazdã era nulã.

Un program care actioneazã în acest mod este cunoscut în literatura de specialitate cu numele de spyware (spion).

O serie de virusi de e-mail, precum celebrul Melissa, încearcã sã trimitã documente confidentiale - personale sau ale companiei la care lucrati. Iar dacã celebrul cal troian numit "Back Orifice" si-a gãsit o cale cãtre sistemul dvs., el va oferi control deplin asupra întregului PC oricui va solicita acest lucru.

Chiar si în conditiile în care sistemul este bine protejat împotriva atacurilor din exterior, este posibil ca o trãdare sã se petreacã din interior. Cu alte cuvinte, atunci când vã conectati la Internet este posibil sã fie partajatã conexiunea cu un parazit, adicã un program spion care are propria sa activitate si care se conectează la momente prestabilite la site-ul sãu de Web.

Unele programe spyware sunt instalate în mod automat atunci când vizitati un anumit site de Web ce face apel la ele. Altele sunt instalate împreunã cu aplicatii de tip shareware sau freeware. Instalarea se produce uneori fãrã a fi constienti de ea sau chiar acceptabilã prin apãsarea butonului Yes fãrã citirea textului licentei de utilizare.

În presã au fost acuzate o serie de aplicatii spyware pentru inventarierea software-ului instalat pe sistemul utilizatorului, scanarea Registrului, cãutarea de informatii confidentiale, toate acestea fiind trimise apoi cãtre

anumite site-uri de Web. Adevărul este că nici o astfel de acuzatie nu s-a dovedit întemeiată. Programele spyware nu sunt denumite astfel pentru că ele "fură" informatii private ci pentru modul secret în care actionează, fără a fi cunoscute sau fără a cere vreo permisiune din partea utilizatorului.

Scopul lor declarat pare destul de inofensiv. Unele dintre ele, denumite adbots, programe de receptionat mesaje publicitare, afisează aceste informatii în programele asociate si încearcă să ajusteze mesajul publicitar preferintelor si obiceiurilor utilizatorilor. Altele colectează informatii statistice pentru clientii lor. Toate aceste programe pretind că vă protejează informatiile private si la o analiză atentă se dovedeste că au dreptate. Informatiile nepersonale ce sunt adunate de aceste programe ar putea fi totusi folosite într-un mod neadecvat, iar prezenta lor pe sistemul dvs. i-ar putea compromite securitatea.

Iată câteva exemple de acest gen. Unul dintre acestea se referă la programul Comet Cursors, care nu este altceva decât un control ActiveX realizat si oferit de firma Comet Systems (www.cometsystems.com). Acesta permite site-urilor de Web ce au licentiat acest control să ofere cursoare ciudate, animate si variat colorate. În functie de setările securitătii din browser-ul de Web, controlul ActiveX, semnat digital si certificat, se poate transfera si instala fără a vă cere permisiunea si fără cunostinta dvs. El contorizează numărul de vizitatori de pe site-urile de Web afiliate folosind tocmai aceste cursoare. Programul asociază fiecărui utilizator un număr de identificare unic, un ID, în asa fel încât să poată raporta numărul de vizitatori distincti. Nu se urmăreste o persoană reală, ci doar raportarea acestor vizitatori ca

numãr.

În acest mod, totusi, firma intrã în posesia adresei dvs. de IP. Prin aceasta se poate face legãturã cu persoana, prin linia închiriatã. Astfel, se poate afla prin ce furnizor de Internet vã conectati la retea. O dezinstalare a acestui program nu poate fi fãcutã cu multã usurintã. De aceea, uneori este nevoie de a apela chiar la firma în cauzã pentru a solicita un program de dezinstalare.

Un alt exemplu este produsul TSAdBot, de la firma Conducent Technologies, fostã TimeSink. El este distribuit prin intermediul mai multor programe shareware si freeware, printre care si versiunea de Windows a utilitarului popular de comprimare PKZip. Rolul sãu este acela de a transfera de la site-ul sãu reclame si a le afisa în timpul rulãrii programului respectiv. Programul raportează sistemul de operare, adresa de IP a furnizorului de servicii Internet, ID-ul programului pe care îl folosim si numãrul de reclame diferite ce au fost afisate. Poate, de asemenea, transmite când s-a fãcut clic pe un banner publicitar precum si rãspunsurile la un chestionar, dacã acesta a fost completat la instalarea produsului.

În timp ce rulati un program care înglobează si acest produs, acesta din urmã se foloseste de conexiunea Internet pentru a trimite informatii si a transfera mesajele publicitare. Doar un firewall personal, precum ZoneAlarm, vã poate avertiza de producerea acestui lucru.

Dezinstalarea unui astfel de program este si ea o operatie care poate da bãtãi de cap utilizatorilor. Uneori este necesar sã fie dezinstalate toate programele care îl folosesc pentru a fi siguri cã acest produs dispare definitiv din calculatorul dvs.

În acelasi mod actionează si produsul Aureate DLL de la Radiate.com, instalat de pe sute de programe

freewre si shareware si care, în timp ce afisează bannere publicitare atunci când programul rulează, transferă reclamele de la site-ul Radiate si raportează înapoi informatii despre ce reclame au fost vizionate si pe care s-a făcut clic si datele unui chestionar propriu care a fost completat la instalare sau care poate reapărea la un anumit timp de la instalarea initială. Dezinstalarea programului originar nu elimină si DLL-ul, care continuă să functioneze independent.

În plus fată de celelalte programe, Aureate DLL introduce si o bresă în securitatea sistemului gazdă, un lucru apreciat de specialisti ca fiind foarte periculos. Un hacker rău intentionat ar putea redirecta produsul să se conecteze la site-ul său. Astfel, acel server ar putea să preia controlul lui Aureate DLL si să-l determine să transfere fragmente periculoase de cod care apoi vor fi lansate în executie.

Linia de demarcatie dintre analizele demografice necesare marketingului si invadarea spatiului privat a fost stearsă cu mult înainte de inventarea spzware-ului. În momentul de fată, utilizatorul este bombardat de mesaje publicitare trimise prin postă electronică la anumite adrese. De fiecare dată când participati la un concurs, completati un chestionar sau dacă trimiteti un talon pentru vreo reducere, sunteti adăugati la baza de date a vânzătorului. Oamenii ce lucrează în marketing îsi doresc să afle cele mai mici aspecte ale vietii cumpărătorilor, în asa fel încât ei să fie "atinsi" de mesajele publicitare. Unii oameni par să nu fie deranjati de acest lucru, simtindu-se bine să primească scrisori si cataloage care se potrivesc propriilor interese si pasiuni. Dacă acest lucru nu vi se potriveste, atunci va trebui să stati în permanentă alertă.

Iatã si câteva sfaturi privind securitatea acestor chestiuni:

- verificati setãrile de securitate ale browser-ului Web pentru a fi sigur cã nici un control ActiveX nu poate fi instalat fãrã stirea dvs. În Internet Explorer 5, alegeti Options din meniul Tools si selectati tab-ul Security si setati optiunile complete pentru a elimina astfel de posibilitãti

- de fiecare datã când instalati un program sau un utilitar cititi cu atentie licenta însotitoare, chiar dacã vi se pare un lucru inutil. Dacã sunt mentionate sisteme integraste de livrare a reclamelor, folosirea în background a conexiunii Internet sau orice altceva ce duce la spyware, s-ar putea sã vã gânditi la abandonarea instalãrii. Si dacã, chiar dupã ce v-ati luat aceste precautii, noul joc sau utilitar afiseazã bannere dinamice, o idee bunã ar fi sã vã documentati în amînunt cu privire la functionarea lui.

- puteti afla destul de multe informatii de pe site-ul de Web al producãtorului programului spyware. Este bine sã consultati aceste informatii înainte de a instala un produs de tip shareware sau freeware.

- apelati la pagina de Web ShieldsUp! de pe site-ul de Web Gibson Research care testeazã securitatea sistemului în acelasi mod în care un hacker ar încerca sã vadã dacã existã vreo cale de atac.

În fine, apelati site-ul OptOut (www.grc.com/ optout.htm) de pe Internet, care oferã informatii si câteva instrumente pentru cei ce doresc sã nu mai fie o sursã de informatii de marketing prin intermediul programelor spyware. Existã informatii detaliate cu privire la toate programele spyware cunoscute, cu nume si adrese de Web ale furnizorilor, ce informatii sunt culese si ce

programe le integrează. Un astfel de utilitar costă mai putin de 25 $ USA, pret în care intră o perioadă nedefinită de actualizări gratuite ale bazei de date cu noi programe spyware. El localizează toate programele spyware din sistem si oferă posibilitatea eliminării lor. El caută în sistem aplicatii spyware cunoscute, raportează existenta lor si execută eliminarea fisierelor în cauză. În anumite variante, programul este oferit si gratuit.

Un cunoscut specialist în acest domeniu, Neil J. Rubenking, este de părere că până acum nu există nici o dovadă că programele declarate spyware adună informatii confidentiale sau că fac o legătură între aceste informatii si persoane individuale. S-ar putea să considerati că cedarea unor anumite informatii nonpersonale este micul pret ce trebuie plătit pentru programele gratuite. Dar posibilitatea de a se abuza de aceste informatii există, asa că este important să stiti cu cine vă partajati conexiunea la Internet.

Alte exemple de virusi

Prezentăm mai jos pe scurt câtiva dintre cei mai cunoscuti virusi, mai vechi si mai noi:

Brain - a apărut pentru prima dată la Universitatea din Maryland, fiind creat de doi frati din Lahore, Pakistan. După trei luni de la aparitie s-au numărat peste 100.000 de copii răspândită în întreaga lume. Într-una din variantele sale virusul înlocuieste numele volumului de dischetă cu numele său.

Cascade - produs în Germania.

Charlie - creat în anul 1987 de Frany Swoboda, virus care făcea ca un program să se autocopieze de opt ori.

Cyber-Tech-B - a fost programat să actioneze numai pe data de 13.12.1993.

Dark Avenger - fabricat în Bulgaria în anul 1990, care continea două noi idei: a) infestarea programelor foarte rapid, b) producerea pagubelor să se facă foarte subtil, pentru a nu putea fi detectat o perioadă de timp.

Data Crime - introduce o semnătură de 1168 octeti.

Form - se instalează în sectorul de boot al discului infectat si cauzează generarea unui sunet, de fiecare dată când se apasă o tastă. Virusul se declansează numai pe data de 18 a fiecărei luni. Odată cu sunetul se afisează pe ecran si un mesaj obscen la adresa unei persoane numite Corrinne, ca si când ar fi vorba de o răzbunare de natură eroticã a unui bun informatician.

Golden Gate - devine agresiv doar după ce a infectat nu mai putin de 500 de programe.

ILoveYou - a apărut pe Internet prin intermediul unui mesaj de e-mail, transmis prin Outlook sau MIRC, care continea un fisier atasat cu titlul tentant: "LOVE-LETTER-FOR-YOU.txt.vbs". Dând impresia că este un mesaj inofensiv (fisier cu extensia .TXT), la un dublu-clic sistemul îl execută, deoarece, în realitate, el este un fisier de tip VBScript. Virusul actionează prin distrugerea registrelor sistemului, rescrierea fisierelor cu extensia .DLL, .VBS, .VBE, .JS, .JSE, .CSS, .WSH, .SCT, .HTA, .JPG, .JPEG, .MP3, .MP2 si scripturile MIRC (cel mai popular program dedicat chat-urilor pe Internet).

Multi s-au lãsat pãcãliti, astfel cã mass-media a anuntat o pagubã la scarã mondialã de peste 6 miliarde dolari SUA. În Bucuresti, un grup de studenti a reusit în timp util sã capteze virusul si sã-i anihileze efectele.

Jerusalem - virusul are o origine care la vremea când a fost lansat a fost socotit ca fiind un atac terorist, datoritã actiunii distructive ce programa distrugerea de proportii a datelor la data împlinirii a 40 de ani de la desfiintarea statului palestinian si faptului cã a fost vãzut pentru prima datã la Universitatea Evreiascã din Ierusalem. Virusul se reproduce în interiorul executabilelor binare ale sistemului de operare DOS, fãrã a verifica noile infestãri. O altã variantã a acestui virus, denumitã "Jerusalem B", este mult mai îmbunãtãtitã si timp de câtiva ani a reprezentat cel mai mare pericol în retelele de tip Novell. O altã variantã a acestui virus se activeazã în fiecare zi de vineri pe 13 si sterge fisierul în loc sã îl infesteze.

KeyPress - afiseazã pe ecran sirul "AAAAA" atunci când se apasã o tastã.

Lehigh - infecteazã fisierul de comenzi MS-DOS numit COMMAND.COM si se multiplicã dintr-odatã în patru copii. A apãrut în toamna anului 1987, creat probabil de un student de la Universitatea Lehigh.

Maltese Amoebae - de asemenea, virus de tip polimorf.

Michelangelo - apãrut în 1992, a fãcut prãpãd în multe din calculatoare, cu toate cã presa a reusit sã informeze foarte repede despre aparitia acestui virus. Se declanseazã în fiecare zi de 6 martie.

Natas - citit invers înseamnã Satan. A apãrut în Statele Unite si în America Latinã. Virusul poate infecta sectorul de boot, tabela de partitii, precum si toate

fisierele care au extensiile .COM sau .EXE si care au fost executate cel putin odatã.

OneHalf - produs în Cehoslovacia.

Pathgen - produs în Anglia.

Stone - apãrut în Noua Zeelandã, fãcea sã aparã pe monitor mesajul "PC-ul tãu este de piatrã".

Suriv 01, 02, 03 - citit invers, înseamnã Virus.

Tequila - virus de tip polimorf, apãrut în Elvetia.

Tip.2475 - este o ruletã rusească foarte periculoasã. A apãrut în Rusia si s-a rãspândit imediat si în tara noastrã. Corupe memoria flash si suprascrie discul hard în Windows 9x.

VBS BubbleBoy - virus de tip "vierme", infecteazã corpul unui mesaj e-mail. Originar din Argentina, are o mãrime de 4992 octeti si este scris în VBScript. El functioneazã pe platforme Windows cu Internet Explorer 5.0 si Outlook 98/2000 sau Outlook Express.

Vendredi 13 - mãreste dimensiunea programelor infectate cu 512 octeti.

Vienna - introduce o semnãturã de 648 octeti.

Yale - creat în SUA.

Primul dintre macrovirusi este cunoscut ca fiind cel folosit în Word si Word Basic. În iulie 1996 a apãrut microvirusul **ZM.Laroux** care avea menirea de a da peste cap Microsoft Excel.

Cum ne apărăm împotriva virusilor

Pornind de la conceptul bine experimentat cã este mai putin costisitor sã previi decât sã tratezi, este necesar sã se acorde o atentie deosebitã problemei virusilor. Într-o formã simplistã, lupta împotriva virusilor s-ar putea rezuma la o singurã frazã: trebuie îmbunãtãtite programele si curãtate dischetele înaintea introducerii lor în unitatea centralã.

Existã astãzi mai multe organizatii internationale care se ocupã cu problemele virusilor pe calculator. Una dintre acestea se numeste CARO - Computer Anti-virus Researcher Organisation, si este o organizatie constituitã din cei mai reputati experti din lume care se ocupã cu standardizarea si clasificarea virusilor.

Încã din anul 1990 a fost înfiintatã o institutie specializatã în acest domeniu, numitã EICAR - Institutul European pentru Cercetarea Programelor Anti-Virus. Aceastã organizatie s-a bucurat de un real succes, mai ales în întâlnirile cu vânzãtorii de programe.

În decembrie 1990, firma Symantec a lansat produsul Norton Anti-Virus Software, astãzi foarte la modã. Tot în acelasi an, dar în luna aprilie, firma Central Point Anti-Virus a lansat produsul CPAV.

Existã mai multe publicatii internationale pe aceastã temã, iar Internet-ul abundã de materiale si informatii. Cea mai importantã revistã internationalã dedicatã raportãrii si analizei virusilor se numeste Virus Bulletin. De la lansarea sa în iulie 1989, revista a monitorizat noile dezvoltãri din domeniul programãrii virusilor si a evaluat cele mai actualizate instrumente si tehnici pentru combaterea amenintãrii reprezentate de virusi.

În lupta împotriva virusilor este necesar să se cunoască cele mai importante si eficiente mijloace, metode si tehnici care pot fi utilizate în acest scop. Pentru aceasta, este nevoie să ne familiarizăm cu câteva notiuni si concepte specifice.

Suma de control (Checksum) este o valoare numerică obtinută din octetii individuali ai unui fisier. Împreună cu data creării, mărimea si atributele DOS ale fisierului, suma de control este memoratã în fisiere de tip listă de control. De obicei, are lungimea de 32 sau 64 biti.

Un alt termen des utilizat este *CRC*. Acronimul lui "Cycled Redundancy Check", în traducere - "Control Redundant Ciclic", el reprezintă o metodă matematică folosită pentru verificarea integritătii datelor. Este o formă de sumă de control, care se bazează pe teoria polinoamelor de lungime maximă. Desi este mai sigură decât cea bazată pe o simplă sumă de control, metoda CRC nu oferă totusi o adevăratã securitate criptografică.

O secventă de octeti sau, mai general, o combinatie de secvente variabile, prin care programele antivirus încearcă să identifice virusii se numeste *semnătura* unui virus (virus signature).

Operatia prin care se elimină un virus dintr-un fisier sau dintr-un sistem se numeste *dezinfectie* (clean). Desigur, contaminarea unui calculator cu un virus informatic se numeste *infectie* (infection).

Tehnica prin care se adaugă unui program executabil o portiune de cod, pentru a se asigura autoverificarea sa, în asa fel încât suma sa de control să fie verificată înainte ca programul propriu-zis să se execute, se numeste *imunizare* (immunization). Orice modificare făcută programului poate fi deci verificată si executia refuzată. Această tehnică poate provoca multe

probleme deoarece ea interfera adesea cu programul pe care incearca sa-l protejeze.

Atunci când se generează o *amprentã* (o informatie de control) pentru un fisier spunem cã s-a efectuat o *inoculare* (inoculate). Este suficient apoi să se compare această amprentă cu alta calculatã ulterior pentru a detecta alterarea eventualã a fisierului de către un virus.

Un program antivirus care cautã fisiere infectate, analizând secvente identificabile ca apartinând unor virusi cunoscuti (asa numitele "semnãturi" de virus) se numeste *program de scanare* (scanner). Programele de scanare au diverse limitări, printre care, cea mai importantã este faptul cã ele nu pot cãuta decât virusi deja identificati sau cunoscuti.

Un *software antivirus* (anti-virus software) reprezintã un produs program utilizat pentru a identifica si deseori pentru a furniza mijloacele necesare eliminării virusilor de pe sistemele infectate. Acest proces este denumit frecvent "curãtare" sau "dezinfectare".

Un *software de dezinfectie* (desinfection software) nu este altceva decât un program care încearcã să îndepărteze virusii de pe discurile infectate, astfel încât să restaureze elementele infectate la starea lor anterioarã. Dat fiind faptul cã adesea virusii sunt polimorfi (schimbati de o manierã subtilã), software-ul de dezinfectare poate să facă greseli cu consecinte potential catastrofale pentru integritatea datelor. Detectia virusilor sectorului de încărcare este cu mult mai fezabilã decât cea a fisierelor executabile, iar utilizarea programelor de sistem (DEL, SYS, FDISK si FORMAT) reprezintã adesea o solutie preferabilã.

Vaccinul este un program pe calculator realizat pentru a oferi o protectie împotriva virusilor de calculator.

Adãugând un cod scurt la fisiere, de declansează o alarmã atunci când un virus încearcã sã modifice fisierul. Vaccinurile mai sunt numite si programe de imunizare.

Autorii rãuvoitori de virusi ai calculatoarelor stiu de existenta programelor de vaccinare si antivirus si unii dintre ei se ocupã cu crearea de noi virusi care sã le contracareze. Dacã folositi calculatorul pentru afaceri sau aplicatii profesionale vitale, protejati datele introducând în calculator numai copii noi, care nu au fost deschise, de programe obtinute direct de la producãtori.

Din activitatea programelor anti-virus pot rezulta si alarme false. O monitorizare a procesului de dezinfectare este deseori foarte utilã.

O metodã de detectare a fisierelor virusate constã în compararea periodicã a fisierului cu cel original, din datã, orã si dimensiune. Aceste teste nu prezintã totalã încredere deoarece atât data si ora, cât si dimensiunea fisierelor pot fi manipulate convenabil, fãrã a ne putea da seama dacã s-a umblat în fisierul original si dacã acesta a fost alterat.

Existã si alte elemente care pot fi verificate, cum ar fi sumele de control (check sum), mai de încredere, dar nu totalã, prin care datele dintr-un fisier sunt însumate si trecute printr-un algoritm specific, rezultând un fel de semnãturã pentru acel fisier. Sumele de control functioneazã pentru verificarea integritãtii unui fisier în cazul transferului dintr-un punct în altul. Pentru protectie, lista sumelor de control este necesar a fi pãstratã pe un server separat, chiar pe un mediu separat accesibil doar de root si de utilizatorii de încredere. Totusi aceastã tehnicã este insuficientã când sunt atacuri sofisticate împotriva integritãtii fisierelor, existând pericolul ca la destinatie sã ajungã un fisier necorespunzãtor.

Pe Internet se găsesc însă suficiente materiale referitoare la modul în care pot fi învinse sistemele care folosesc sume de control, multe dintre ele chiar prin actiunea virusilor. Multe dintre utilitarele antivirus folosesc o analizã a cifrei de control pentru a identifica activitãti de virusare.

Există tehnici satisfăcătoare bazate pe calcularea unei amprente digitale (digital fingerprint) sau semnãturã pentru fisiere. Algoritmii care realizează acest lucru fac parte din familia MD, cea mai cunoscutã implementare fiind MD5. Aceasta este o functie neinversabilã (one-way) care geherează semnătura digitală pentru un fisier prin intermediul unui algoritm de condensare a mesajului (message digest). Algoritmul preia la intrare un mesaj de o lungime arbitrară si produce un rezultat pe 128 biti denumit amprentã (fingerprint) sau rezumat (message digest). Algoritmul se bazează pe un concept conform căruia este imposibil prin prelucrare să se producă două mesaje cu acelasi rezumat sau să se reconstituie un mesaj pornind de la un anumit rezumat. Algoritmul MD5 este proiectat pentru aplicatii bazate pe semnãturi digitale, în care un fisier de dimensiuni mari trebuie comprimat într-un mod sigur înainte de a fi criptat cu o cheie privatã (secretã).

Un produs care utilizează algoritmul MD5 este S/Key dezvoltat de Bell Laboratories pentru implementarea unei scheme de parole unic valabile (one-time), care sunt aproape imposibil de spart, desi parolele sunt transmise în clar, dar datoritã faptului cã parola fiind de unicã valabilitate, nu mai este de nici un folos pentru un eventual intrus.

O tehnicã foarte interesantã aplicatã în combaterea virusilor se bazează pe utilizarea programelor

automodificabile (self-modifying program). Acestea sunt programe care îsi schimbã deliberat propriul lor cod, cu scopul de a se proteja împotriva virusilor sau copierilor ilegale. În acest mod devine foarte dificilã validarea prin mijloace conventionale.

Cine ne apãrã ?

În finalul acestui capitol prezentãm alte câteva sfaturi care ar putea fi foarte utile pentru a vã proteja sistemul împotriva virusilor calculatoarelor si o listã a principalelor programe antivirus care pot fi usor procurate.

Iatã, mai întâi, ce este foarte important sã se retinã:

- nu încercati programe executabile de pe sistemele de buletine informative dacã nu sunteti sigur cã ele sunt fãrã virusi (eventual ati vãzut pe altcineva folosind programul fãrã probleme).

- nu preluati programe executabile vândute prin postã si care tin de domeniul public sau în regim shareware, dacã nu se precizeazã cã se verificã fiecare program vândut.

- nu încãrcati niciodatã un program transmis de curând pe un sistem de buletine informative, pânã când el nu a fost verificat de operatorul de sistem. Când încãrcati programul, fãceti-o pe un sistem cu douã unitãti de dischetã, astfel încât el sã nu se apropie de hard disk.

- nu copiati dischete pirat ale programelor comercializate, deoarece ele pot contine virusi.

- cumpărati si folositi programe recunoscute de detectare a virusilor

- instalati un program de detectare a virusilor, rezident în memorie, care să examineze fisierele pe care le copiati în calculator.

LISTA PRINCIPALELOR UTILITARE ANTIVIRUS

Nr	Nume utilitar	Nume firmă	Platforma	Adresa
1.	AVX 2000 Desktop	Softwin	Win9x/NT	www.avx.ro
2.	BoDetect 3.5	Chris Benson	Win9x/NT	www.cbsoftsolutions.com
3.	Colectia	Simtel.Net	DOS, Win 3.x	
4.	Command AntiVirus	Command Software System, Inc.	Win3.x/9x/NT	www.commandcom.com
5.	CATCH MTE	VDS-Advanced Research Group	DOS, Win 3.x	
6.	F-PROT Professional Anti-Virus Toolkit	Data Fellows	DOS/Win3.x/9x	
7.	Integrity Master	Stiller Research	DOS/Win3.x/9x	
8.	InoculateIT Personal Edition 2.5.0	Computer Associates International, Inc.	Win9x/NT/2000	www.cai.com
9.	Iris Antivirus Plus	Iris Software	DOS/Win3.x/9x	
10.	LAN Desk Virus Protect 4.0	Intel Netware	WinNT	
11.	Norman Virus Control 4.8	Norman Data Defence System, Inc.	Win9x/NT/2000	www.norman.com
12.	Norton AntiVirus 2001	Symantec	Win9x/NT/2000	www.symantec.com
13.	Panda Antivirus Platinum 6.15.01	Panda Software	Win9x/NT	www.pandasoftware.com
14.	PC-Cillin 6.0	Trend Micro, Inc.	Win3.x/9x/NT	www.antivirus.com
15.	RAV AntiVirus Desktop 8	GeCAD SRL	Win9x/NT/2000	www.rav.ro
16.	Sweep	Sophos	Win95/NT	
17.	The Integrity Master	Stiller Research		
18.	Thunderbyte Anti-Virus	ThunderByte	Win3.x/9x/NT	
19.	Virus Alert	EVirus Corp.	Win9x/NT/2000	www.virusalert.com
20.	VirusSafe	Eliashim	Excel 2000	
21.	McAfee VirusScan	Network Associates, Inc	Win3.x,Win9x,NT	www.nai.com
22.	Virux for PC	Datawatch Corp.	DOS, Win 3.x	

Nu putem încheia acest capitol fără a spune câteva cuvinte despre legislatia împotriva atacurilor cu virusi de calculatoare. Asa cum spune un mare specialist în domeniu, Dr. Frederick B. Cohen, un mod de a lupta împotriva virusilor dăunători, din punct de vedere social, este acela bazat pe crearea si aplicarea în mod ferm a unor legi împotriva lor.

Deoarece la sfârsitul anilor '80 virusii de calculator deveniserã o amenintare substantialã, administratiile locale din SUA si multe dintre guvernele lumii au creat legi împotriva introducerii virusilor dãunători în sistemele de calcul fără consimtământul proprietarului. Desi existã anumite ambiguitãti în multe din ele, specialistii calculatoarelor apreciazã cã este mai bine ca aceste legi sã existe si sã fie aplicate decât sã lipseascã.

Legile împotriva propagării virusilor sunt absolut necesare, întrucât astãzi este un fapt bine cunoscut cã prin intermediul acestora se fac acte inimaginabile de sabotaj si sunt dovezi certe cã anumiti virusi sunt lansati de grupări teroriste (a se vedea istoria virusului "Jerusalem").

Tara noastrã nu beneficiazã la aceastã orã de o lege împotriva virusilor de calculator, în pofida faptului cã fenomenul s-a extins mult în ultimul timp si pe teritoriul României iar delictele de aceastã naturã nu mai pot fi tolerate.

Acelasi specialist mentionat mai sus sustine cã sunt necesare trei componente importante pentru ca lansarea unui virus într-un mediu de calcul sã constituie un delict. Acestea ar fi urmãtoarele:

- să fie lansat în mod intentionat
- să fie dãunãtor
- să nu fie autorizat.

Acestea ar constitui, în cazul în care ar fi prezente toate trei, baza cã a fost comis un delict. Chiar dacã aceste probleme nu sunt întotdeauna în mod necesar atât de clare si evidente, cei pusi ca să aplice legea pot totusi să hotărascã pe baza dovezilor.

Partea a III-a

INFRACTIUNEA INFORMATICĂ

Notiuni juridice

În dictionarul limbii române infractiunea este socotită ca fiind o faptă care prezintă pericol social, constând în încălcarea unei legi penale, în săvârsirea cu vinovătie a unei abateri de la legea penală, si care este sanctionată de lege. În articolul 17 din Codul Penal Român se defineste aproape asemănător infractiunea de drept comun, astfel: "*Infractiunea este fapta care prezintă pericol social, săvârsită cu vinovătie si prevăzută de legea penală*".

Conform aceluiasi dictionar al limbii române frauda reprezintă o înselăciune, hotie, sau un act de rea-credintă săvârsit de cineva, de obicei pentru a realiza un profit material de pe urma atingerii drepturilor altuia.

La prima vedere s-ar putea spune că, atunci când se comite o fraudă prin intermediul calculatorului în tara noastră, neexistând o lege care să sanctioneze fapta, aceasta n-ar trebui să fie catalogată drept infractiune. Desi pare un paradox, totusi lucrurile nu stau chiar asa. Chiar dacă în tara noastră nu există suficiente legi specifice care să combată infractiunea pe calculator, o bună parte din fapte pot totusi fi încadrate juridic. Pe de altă parte, nu putem neglija că majoritatea tărilor dezvoltate din lume au legi în acest domeniu, bine puse la punct, si mai devreme s-au mai târziu, le vom avea si noi. De aceea problema infractionalitătii pe calculator trebuie cunoscută, ea devenind, în ultimul timp, un adevărat flagel la scară mondială, cu tentacule suficient de periculoase si în tara noastră.

Primul lucru pe care ne propunem să-l tratăm este cel legat de întelegerea corectă a termenilor utilizati în acest domeniu, iar dintre acestia, vom începe cu cei juridici.

Asadar, frauda informatică, prin specificul ei este o infractiune cu un grad de periculozitate foarte ridicat. O eroare într-o bancă de date poate provoca pagube incalculabile.

Frauda informatică, asa cum este ea definită de lege, este caracterizată de fapte precum intrarea, alterarea, stergerea sau supraimprimarea de date sau de programe pentru calculator sau orice altă intruziune care ar putea să genereze o influentă a rezultatului, cauzând prin aceasta un prejudiciu material sau economic intentionat, făptuitorul urmărind să obtină un avantaj patrimonial pentru sine ori pentru altul.

Obiectul juridic al acestei infractiuni este dat de proprietatea aceluia sau acelora care detin informatii ce au fost fraudate, iar prin aceasta, implicit, este vorba de inviolabilitatea proprietătii, iar proprietatea a fost, este si va rămâne un drept sacru al oricărui cetătean, garantat de orice constitutie din lume.

Obiectul material îl constituie acel suport material, precum CD-ul, discheta, hard disk-ul etc., pe care pot fi înscrise datele si programele protejate.

Subiectul activ este reprezentat de orice persoană care răspunde penal, sau un subiect calificat precum unul dintre angajati care ar trebui să vegheze la bunul mers al sistemelor de gestiune informatizată, caz în care descoperirea lui este mai dificilă.

Intrarea este consideratã a fi intruziunea sau introducerea de date nereale sau care nu au ce căuta acolo, pătrunderea într-un loc interzis, ceea ce constituie

infractiunea.

Alterarea este definitã de modificãrile efective operate în acele date, partiale sau totale.

Stergerea înseamnã distrugerea datelor indiferent de suport.

Suprimarea este retinerea sau ascunderea de informatii, care se fac nedisponibile, ceea ce conduce la vinovãtie si intentie directã (premeditare).

Scurt istoric al infractionalitãtii pe calculator

Cu multi ani în urmã au existat voci care avertizau cã, într-o bunã zi computerul va preface toate formele de delincventã. Se pare cã a existat o mare dozã de adevãr în aceste previziuni si, mai mult, acestea au rãmas valabile si în ziua de azi.

Dacã luãm în considerare statisticile din ultimii cincisprezece ani, se poate sustine cu tãrie cã infractiunea asistatã de calculator nu poate fi socotitã deloc inofensivã si cã fenomenul este într-o continuã crestere.

Încã din momentul în care rãspândirea prelucrãrii automate a datelor a devenit o certitudine, s-a prevãzut cã delictul cel mai frecvent care va fi întâlnit în statisticile privind criminalitatea va deveni criminalitatea prin computer. Cu toate acestea, abia în penultimul deceniu al

secolului trecut s-au pus la punct primele legi importante pentru combaterea fenomenului.

În anul 1985 criminalitatea prin calculator a beneficiat si de o definitie destul de complexã: "Prin criminalitate prin computer se înteleg toate faptele în care prelucrarea automatã a datelor este un mijloc de actiune si care motivează bănuirea unei fapte penale". Această definitie include atât delictele criminalitătii prin calculator în sens restrâns cât si toate delictele în care prelucrarea automatã a datelor serveste drept instrument – ca de exemplu tăinuirea prin intermediul Mailbox-urilor.

Au existat si unele voci care considerau cã este o greselă să se folosească această notiune de criminalitate prin computer, deoarece discreditează informatica. De exemplu, profesorul Nagel de la IBM sustinea cã nici măcar inteligenta artificială nu poate produce "computere criminale" si cã, criminal poate fi doar omul, căci numai el are puterea de a converti orice lucru bun în arme.

Un calculator nu poate garanta o crimă perfectă, desi poate face ca unele ilegalităti să devină mai eficiente. El poate, de exemplu, să permită cifrarea informatiilor, împiedicând astfel accesul organelor de cercetare la ele, iar aceasta este o posibilitate intens exploatată de infractori, inclusiv teroristi.

Primele legi împotriva infractiunilor săvârsite cu ajutorul computerului contineau, în esentă, prevederi împotriva actelor de pătrundere în baze de date, de înselătorie si sabotaj, precum si de piraterie software care este reglementată, de regulă, prin legea copyright-ului. Dar aceste delicte ce caracterizează criminalitatea prin computer constituie doar o mică parte din cele posibile. La scurt timp s-a dovedit cã si traficul de stupefiante,

comertul ilegal cu arme, pornografia infantilã, diverse forme de delicte economice si chiar unele infractiuni privind protectia mediului înconjurãtor pot fi fãcute prin intermediul calculatorului.

Din acest motiv, pe la sfârsitului anului 1986, spectrul acestor delicte a fost extins pentru toate delictele care folosesc prelucrarea automatã a datelor ca instrument de actiune. Atunci a fost abordat termenul “Computer Aided Crime” care a fost cunoscut sub denumirea de “criminalitate prin computer în sens redus si lãrgit”.

Notiunile utilizate, insuficient clarificate la acea vreme, au fost de naturã sã provoace si anumite confuzii. De exemplu, politia tinea douã statistici paralele privind criminalitatea: cea a criminalistilor de tip clasic si cea a informaticienilor care se ocupau cu "Computer Aided Crime", adicã cu un domeniu particular de utilizare a calculatoarelor.

În spiritul acelorasi confuzii au actionat si infractorii care întelegeau criminalitatea prin computer drept o “alternativã”, cel mult ilegalã, de folosire a prelucrãrii automate a datelor.

Diversitatea lumii informatice în permanentã schimbare si evolutie a condus în scurt timp si la o diversitate enormã a abuzurilor prin prelucrarea automatã a datelor. Specialistii calculatoarelor descopereau în permanentã ceva nou, iar fantezia nu le-a lipsit deloc.

Asa cum era de asteptat, aceastã evolutie a afectat si structura organelor de cercetare penalã. Fenomenul a cuprins în scurt timp întreaga economie si chiar statul. Azi nici o organizatie criminalã serioasã nu poate fi imaginatã fãrã suport informatic, iar politia este nevoitã sã tinã seamã de acest fapt în toate cercetãrile sale. Acest fapt

impune si o pregãtire a functionarilor criminalisti în domeniul informaticii, dar si competente politienesti în acest domeniu. Asa cum sustin unii, informatica ar trebui sã devinã materie de examen la facultãtile care pregãtesc cadre pentru politie.

Pe de altã parte, de oricâtã protectie prin instrumente de securitate ar beneficia prelucrarea automatã a datelor, criminalii pot anula accesul politiei la datele care dovedesc efractia lor. Iar acestia din urmã dovedesc chiar un interes mai mare pentru securitatea datelor decât firmele pãgubite.

Ultimii ani ai secolului douãzeci au zguduit lumea prin descoperirea unei noi tehnici tipografice. Noile echipamente, precum scannerele, imprimantele laser si color si software-ul grafic, CD-ROM-ul si altele au fãcut posibil nu numai ca un computer sã poatã poatã fi utilizat în tipografie iar cartea sã poatã deveni "electronicã", dar si sã producã "minciuni patentate" de genul reproducerii monedelor, falsificãrii înscrisurilor de tot felul, documentelor si fotografiilor etc. În acest mod prelucrarea numericã poate micsora valoarea de dovadã chiar si a pozelor sau a negativelor.

Astãzi este o certitudine - calculatorul a devenit cel mai popular instrument de falsificare.

Clasificarea delictelor informatice

Înainte de a prezenta în detaliu caracteristicile anumitor categorii de fraude informatice, începem prin a prezenta, foarte succint, o enumerare a acestora, fãrã

pretentia de exhaustivitate, ci doar în intentia de a se putea observa mai usor cã tipurile de infractiuni din acest domeniu sunt multe si diverse. Acesta ar putea fi primul motiv pentru care ar trebui sã ne îngrijorãm iar autoritãtile ar trebui sã se autosesizeze si sã ia serios subiectul, mãcar acordându-i o atentie cuvenitã.

. falsificarea de dovezi, voalarea înselãtoriile prin computer si cifrarea spargerilor mafiote

. teletransmisia de date pentru tãinuire

. pornografia de toate genurile, inclusiv cea infantilã

. comandã de organe pentru transplant

. sabotarea prin virusi

. distribuirea materialelor ilegale (pornografice, propagandist-teroriste) sau software nelicentiat

. spionajul economic si militar

. spargerea de jocuri

. fapte ilegale de santaj si constângere

. falsificãri de monede, înscrisuri, acte

. digitizarea fotografiilor false si falsificãri pe baza aparatelor foto cu schitare digitalã

. traficul de stupefiante

. comertul ilegal cu arme

. diverse forme de delicte economice

. infractiuni privind protectia mediului înconjurãtor

. furtul de carduri

. omorul sãvârsit prin intermediul calculatorului (modificarea premeditatã de diagnostice etc.)

. comertul cu carne vie

. atacuri de tip terorist

. manipularea sistemelor de pazã si protectie

. utilizarea frauduloasã a Internetului:

- frauda datoratã falsei identitãti si a spionilor în retea (snipers)
- furtul timpului de navigare pe Internet
- blocarea retelelor prin supraîncãrcare
- fraude datorate actiunilor protestatare, elitiste sau de afirmare ale hackerilor
- atacurile împotriva serverelor DNS (Domain Name Server)
- fraude datorate intrusilor (furtul de parole
- password sniffers), compromiterea securitãtii la nivelul întregii retele.
- Conectarea anonimã prin serviciile telnet si socks ale proxy-urilor Wingate, prost configurate.

. fraude asupra informatiilor sau calculatoarelor

- atacul în centrale PABX private si publice (prin servicii DISA sau voicemail)
- fraude asupra retelelor virtuale private (VNP)
- intrarea în bãnci de date si retele.

. abuz de informatii - obtinerea de informatii "folositoare" sau coduri de acces si vânzarea acestora (de obicei cu colaborarea din interior)

. Mesaje electronice nesolicitate (spams).

În recomandarea Consiliului Europei R(89)9 sunt icluse într-o listã infractiunile realizate cu ajutorul calculatorului, întâlnite pânã acum în practicã si care au

perturbat destul de grav anumite relatii sociale. Lista principalã se referã la:

- frauda informaticã
- falsul informatic
- prejudiciile aduse bazelor de date, datelor si programelor de calculator
- sabotajul informatic
- accesul neautorizat
- interceptarea neautorizatã
- reproducerea neautorizatã de programe protejate

Lista secundarã cuprinde:

- alterarea datelor sau programelor de calculator
- spionajul informatic
- utilizarea neautorizatã a unui calculator
- utilizarea neautorizatã a unui program de calculator.

Pirateria software

Pirateria software înseamnã folosirea nepermisã si utilizarea fãrã drept de autor a unui program de calculator. Acest subiect a mai fost analizat. Fenomenul de piraterie software este unul dintre cele mai rãspândite din lume, iar în tara noastrã a ajuns la cote îngrijorãtoare. Sondajele aratã cã rata pirateriei soft din România este una dintre cele mai ridicate din lume.

Gunter von Gravenreuth, inginer dar si avocat si un foarte bun specialist în procese de piraterie soft, sustine

cã, desi politia a început sã se specializeze si sã se obisnuiascã cu astfel de infractiuni, existã totusi si astãzi mari diferente, în special de naturã regionalã, în ceea ce priveste clarificarea informaticã a organelor de cercetare, referindu-se, desigur, la modul diferit cum este privit fenomenul în diferite state sau localitãti importante. Practic, existã o divergentã de pãreri referitoare la pirateria software. Unii considerã si astãzi cã orice program de calculator ar trebui sã fie un bun public, pentru care ar trebui plãtitã doar o taxã generalã, asa cum se face pentru utilizarea în comun a unei autostrãzi sau al unui pod. Altii, dimpotrivã, sustin cã un program de calculator este un act de creatie, care necesitã niste costuri de productie si cã ar trebui sã se vândã ca orice alt produs fabricat.

Disputa va continua, desigur, însã legile copyright-ului sunt destul de aspre în unele tãri si acesta este un adevãr incontestabil.

Business Software Alliance estima, în urmã cu câtiva ani, existenta a peste 840.000 de site-uri care vând software pe Internet. Multe afaceri obscure de tip on-line posedã site-uri foarte atractive si profesionale, astfel încât pânã si cei mai securizati consumatori on-line pot cãdea victima acestora. Afacerile Internet ce ascund astfel de fraude folosesc adesea adrese de e-mail multiple si site-uri de Web, fãcând astfel mult mai grea misiunea oficialitãtilor în ceea ce priveste localizarea si pedepsirea lor.

Răspândirea virusilor

Si acest subiect a fost dezbãtut pe larg într-un capitol anterior. Fenomenul de răspândire a virusilor reprezintã un pericol important, asupra cãruia ar trebui sã se îndrepte atentia noastrã.

Virusii calculatoarelor sunt cu mult mai dãunãtori decât s-ar putea întelege dupã o primã analizã. Ei nu sabotează numai functionalitatea computerelor. Printr-o proiectare corespunzãtoare a pãrtii distructive prin intermediul virusilor pot fi realizate si acte de spionaj sau alte delicte majore, precum santajul si constângerea.

În topul international al tipurilor de amenintări pe calculator autorii de virusi ocupã locul trei.

Furturi de bani si informatii

Unele grupuri criminale, plasate pe locul patru în ierarhia mondialã a tipurilor de amenintări asupra sistemelor informatice au ca obiectiv principal obtinerea de bani si alte avantaje prin vânzarea informatiilor furate sau prin realizarea de tranzactii bancare ilegale.

Un rol important în acest domeniu este detinut de către diferitele structuri de servicii secrete care au început sã foloseascã canalele de comunicatii si Internetul ca mijloace de obtinere a informatiei.

Oricum, se pare cã furtul de informatii este cel mai putin interesant pentru "spãrgãtorii" de coduri. Cu toate acestea, o politicã de genul "nu am secrete în calculatorul meu, deci nu am motive sã mã tem de hackeri" nu este deloc potrivitã.

Furturi prin Mailbox

Comertul cu programe furate prin cãsute postale reprezintã una dintre cele mai vechi infractiuni informatice. Numai în primii ani programele de calculator au fost comercializate, în cea mai mare parte a lor, prin anunturi în ziare. Când acest procedeu a devenit prea periculos, infractorii au început sã foloseascã formulare pentru post-restant. În zilele noastre piratii transferã softul prin Mailbox. Noua metodã se poate aplica si pentru alte bunuri furate, precum casete video cu pornografie infantilã sau casete video care glorificã violenta, sau cu materiale propagandist-teroriste.

Transmisia de date la distantã prin Mailbox sau Btx reprezintã nu numai calea de comercializare a mãrfurilor, ci si cea de comunicatie între infractori pe care politia nu o mai poate controla.

Se apreciazã cã prima indicatie cu privire la falsificarea Eurochesue-rilor s-a rãspândit printr-un Mailbox, imediat dupã instalarea primelor automate de bani. Astãzi, fenomenul a luat o amploare îngrijorãtoare.

Falsificarea de valori

Aceastã categorie de infractiuni se referã la falsificarea de monedã sau de alte valori, prin intermediul unor scannere performante, imprimante laser etc. În aceeasi clasã de infractiuni sunt incluse totodatã si fabricarea intrumentelor proprii de falsificare.

Atacuri asupra ATM, debit-card, PC passwords, PIN

Atacurile asupra ATM-urilor, debit-cards, PC passwords, PIN-urilor (Personal Identification Number) sunt utilizate pentru activarea ATM-urilor, a numerelor de cont ale credit si debit-card-urilor, a codurilor de acces la distantã si a microprocesoarelor telefoanelor mobile rãspunzãtoare de facturare. Computerele sunt folosite intens în fraudarea financiarã, nu numai ca instrument al "crimei", dar si pentru a pãtrunde (hacking) în bazele de date si a sustrage informatii confidentiale asupra conturilor financiare. Existã trei tipuri de fraude financiar-electronicã:

- sustragerea informatiilor de cont
- clonarea microcipurilor telefoanelor mobile în scopul fraudãrii tranzactiilor on-line
- scanarea instrumentelor negociabile de platã, care sunt apoi contrafãcute prin metode de desktop publishing.

Furturi de carduri

O nouã categorie de ilegalisti este cea a carderilor iar operatiunile de acest gen sunt cunoscute sub numele de carding. Rolul acestora în lumea infractiunilor informatice este acela de a câstiga bani sau obiecte prin spargerea unor site-uri ce contin în bazele de date numere de cãrti de credit.

Carderii nu fac altceva decât sã valorifice numerele unor cãrti de credite, de la distanta si sub

adăpostul oferite de un fotoliu comod în care stau ceasuri întregi în fata unui computer conectat la Internet. Informatiile pe care le obtin, dupã o muncã deseori istovitoare, sunt folosite pentru a cumpăra de la magazinele on-line diferite produse, pe care le vând apoi la preturi mai mici.

Pierderile anuale cauzate prin fraudarea credit-card-urilor sunt estimate de către institutiile financiare numai din SUA, la miliarde de dolari.

Spionajul computerizat

Despre acest tip de delict nu există informatii suficiente, deoarece foarte rar sunt făcute publice declaratiile exacte despre aria de cuprindere a spionajului computerizat. Cu toate acestea, statistica mentionează si cifre despre trădarea secretelor de firmă si ale celor de afaceri. Însă indicatorii sintetici furnizati nu permit exprimări detaliate.

Atacuri teroriste

Nu trebuie să ne mire faptul că si teroristii au trecut în ultimul timp la utilizarea noilor tehnologii de transmitere a informatiei prin Internet, pentru a pune la punct planuri, pentru a obtine fonduri si pentru a comunica în siguranță. În ierarhia tipurilor de amenintări asupra sistemelor informatice acestia ocupă pozitia a cincea. Cu toate acestea, simplul fapt că organizatiile teroriste încep să se bazeze din ce în ce mai mult pe tehnologia informatiei constituie un real avertisment.

Înselãtoria prin computer

Înselãtoria prin intermediul computerului reprezintã delictul de bazã apãrut în statistici si a fost recunoscut la început prin douã categorii importante: abuzul asupra automatelor de bani si asupra celor de jocuri. Toate celelalte forme de înselãtorie prin computer, despre care circulã zvonuri spectaculoase, sunt la aceastã orã, conform datelor statistice, neimportante.

Sabotajul prin computer

Statisticile despre sabotajele prin computer furnizeazã cifre foarte ridicate, în continuã crestere. Cu toate acestea, realitatea este disproportionatã iar principala cauzã este lipsa de entuziasm a firmelor pãgubite în a face publice informatiile. O oglindã partialã a realitãtii poate fi redatã si de comparatia dintre numãrul mare de virusi rãspânditi în întrega lume cu delictele de sabotaj prin computer.

Atacuri împotriva protectiei mediului înconjurãtor

În timp ce calculatoarele sunt utilizate tot mai des în supravegherea unor procese, ele devin pe zi ce trece instrumente indispensabile. S-a ajuns astfel la o stare de dependentã ce nu mai are cale de întoarcere. Odatã cu certitudinea cã numai calculatorul mai poate garanta controlul prescris al reglementãrilor legale de

supraveghere a aerului si apei, s-a deschis si calea unor posibilitãti de atac si de fraudã si în acest domeniu.

În acest domeniu lucrează interdisciplinar biologi, fizicieni, medici si informaticieni. Rãmâne de netãgãduit faptul cã nu existã securitate sutã la sutã a prelucrării automate a datelor.

Exemple de fraude informatice

În legãturã cu delictele comise prin intermediul calculatorului existã la aceastã orã un adevãr incontestabil: doar o micã parte a acestora sunt descoperite de politie iar organele de anchetã dispun de un volum mic de informatii. În acelasi timp, acestia nici nu sunt pregãtiti suficient de bine pentru un domeniu aproape nou.

În acest context, analizând cifrele relativ scãzute din statisticile acestor infractiuni, s-ar putea trage concluzia falsã cã pericolul este supraestimat. Societãtile, în general, nu sunt pregãtite suficient de bine la aceastã orã pentru a preîntâmpina aceste infractiuni.

Prezentãm în continuare câteva exemple concrete de infractiuni sãvârsite prin intermediul calculatorului, atât pe plan mondial, cât si pe plan autohton.

. Primele cazuri importante de acces neautorizat au fost depistate în 1985 când a fost penetratã cunoscuta retea ArpaNet. În acelasi an revista on-line "Phrack" a publicat o listã destul de bogatã de numere de apel dial-up. În continuare aceastã activitate s-a desfãsurat din plin. Pentru tinerii americani inteligenti care dispuneau de serviciile unui calculator electronic începea sã se deschidã o lume nouã, în general lipsitã atunci de legi.

. Unul din cazurile celebre de fraudã informaticã este cel al unui grup de crackeri care a preluat controlul centralei telefonice de la Casa Albã, utilizând-o pentru convorbiri telefonice transatlantice.

. Pe data de 6 ianuarie 1993, câtiva hackeri din Marea Britanie au pătruns în banca de date a unei companii comerciale din Londra, operând un transfer de 10 milioane de lire sterline. Este un exemplu de infractiune concretă, fâcând parte din categoria "campaniilor active", adică a acelora care lasă prejudicii ce pot fi imediat cuantificate.

. Tot în aceeasi perioadă câteva site-uri oficiale americane au fost "ocupate" de o actiune spectaculoasă, de tip protestatar, a unor chinezi. Acestia au introdus în locul mesajelor standard existente, propriile lor texte de protest, provocând un fel de mini-războiu psihologic. Este un exemplu de "campanie pasivă", cu implicatii de natură psihologică în primul rând, dar si de natură politică, fiind mai degrabă o dovadă că războiul informational a devenit o realitate care nu mai poate fi neglijată.

. În anul 1993 un chinez a fost condamnat la moarte prin împuscare pentru o fraudă de 193 milioane USD. Abia după înregistrarea acestui caz unic, statul chinez a elaborat si prima lege în acest domeniu.

. Un cunoscut hacker american, a cărui poveste a stat si la baza realizării unui film de susces, a fost prins si pedepsit de justitie; la scurt timp a fost eliberat cu o interdictie de câtiva ani să se apropie de un telefon public.

. Iată un exemplu de infractiune de omor: un individ, dorind să-si elimine rivalul aflat la tratament într-un spital din Florida, a pătruns în baza de date a spitalului modificând diagnosticul pacientului. Fiind tratat pentru altceva decât boala de care suferea, pacientul a decedat în scurt timp.

. Jim Jarrard din Simi Valley, California, a avut surpriza să constate că în timp ce si-a lăsat calculatorul

într-o noapte să functionze pentru a finaliza un download de mari dimensiuni, un hacker i-a accesat PC-ul prin conexiunea DSL si a instalat un program care i-a permis să controleze calculatorul, să fure fisiere importante si să steargă informatiile de pe hard disk-uri. Jarrard a scăpat de catastrofă datoritã unei blocări neasteptate a sistemului.

. Allan Soifer, administrator de postă electronicã în Ottawa, nu si-a dat seama cã un hacker îi scana PC-ul de acasă de câteva ore. Hackerul gãsise o poartã de intrare si avea nevoie numai de o parolã pentru a accesa fisierele. Acesta bombarda respectivul calculator cu parole generate aleator, sperând cã va nimeri combinatia corectã. Victima a fost norocoasă deoarece avea instalat ZoneAlarm, un program de protectie de tip firewall personal preluat de la firma ZoneLabs. Programul l-a alertat despre multitudinea de parole cu care era bombardat PC-ul. În plus, el a putut identifica chiar ISP-ul hackerului pe care l-a localizat în Anchorage, Alaska.

. Câteva exemple de virusi reali, altele decât cele arhicunoscute, dar care au provocat pagube însemnate în diferite companii si organizatii americane:

- "Typo", virus orientat pe distrugerea datelor care creează erori de dactilografiere atunci când utilizatorul depăseste 60 de cuvinte pe minut.

- Un virus de distrugere a productiei a fost lansat într-o intreprindere metalurgică, si avea rolul de a micsora cu câteva grade temperatura în cea de-a treia fază a procesului de răcire a otelului, conducând la o calitate inferioară a produsului.

- Cel mai mic virus a fost scris prin rescrierea algoritmului comenzii Unix "sh". Acesta avea dimensiunea de 8 caractere si în afarã de reproducere nu mai avea altã functie.

- La începutul anilor '90 dintr-un institut de cercetări din Bulgaria a fost lansat în circulatie un set de 24 virusi care au fost cu greu detectati atât în Europa, cât si în SUA.

Fraude informatice autohtone

. Un hacker din România, supărat pe preturile mereu în crestere practicate de RomTelecom, a pătruns în reteaua societătii si a modificat tarifele din site, făcându-le 1 leu pentru 5 ore de convorbire.

. Niste hackeri români au pătruns în urmă cu câtiva ani într-un server extern al Pentagonului. Desi nu sau ales cu nimic, site-ul fiind de micã importantă, ei au fost descoperiti la timp înainte de a provoca anumite stricăciuni.

. Ministerele de Interne, Justitie si Finante din tara noastră au fost atacate de mai multe ori de virusi ce au adus modificări majore ale informatiilor din site-urile respective.

. În urmă cu un an, pe când guvernul a anuntat mărirea accizelor la băuturile alcoolice, pe pagina de Web a Ministerului de Finante a pătruns un hacker care a introdus în site mesajul de protest: "Acest site a fost spart de Regele Berii".

. Câtiva hackeri români si-au bătut o vreme joc de pagina de Web a guvernului, amestecând pozele acesteia.

. Un alt hacker din România a reusit să intre pe site-ul FBI, "prinzând" pe acesta poza lui Ion Iliescu.

. În ceea ce priveste comertul electronic, românii s-au specializat în realizarea de cumpărături de pe magazinele virtuale aflate în afara tării (marea majoritate fiind în SUA), folosind cărti de credit furate sau false. În acest scop au fost folosite site-uri specializate în comert electronic si baze de date cu numere de cărti de credit. Atacurile de acest gen sunt favorizate si de faptul că timpul dintre momentul plătii nelegitime si momentul în care proprietarul cărtii de credit sesizează evenimentul si refuză plata este suficient de mare.

. Un hacker român a descoperit niste bug-uri (erori) în reteaua de calculatoarele a unui cetătean american care tocmai deschisese un Internet-Cafe în Bucuresti. L-a avertizat pe acesta în câteva rânduri cu privire la faptul că administratorul acelei retele nu-si face corect datoria sau nu se pricepe să-si protejeze sistemul. Americanul l-a invitat pe hacker să vină să lucreze la firma sa. Si de atunci, acesta este angajat acolo, are un salariu decent, taxiul decontat, telefonul plătit de firmă etc.

. Alt hacker român a blocat calculatorul unui individ pe care nu-l simpatiza deloc, în asa fel încât atunci când îl deschidea intra pe Word, scria un text si se reseta. Desigur, calculatorul a devenit practic inutilizabil. Revenind la sentimente mai bune, hackerul a îndreptat el însusi situatia doar după câteva zile.

. Un foarte bun hacker român, de data aceasta în sensul initial al termenului de hacker, a găsit niste bug-

uri în reteaua firmei Ericsson si a trimis acesteia constatările lui si felul în care se poate rezolva problema. A primit în schimb de la patronii firmei un telefon de ultimul tip, placat cu aur.

. La începutul lunii octombrie, 1999 Judecătoria Ploiesti a pronuntat prima sentintă de condamnare a administratorului firmei ANDANTINO la sase luni de închisoare cu suspendare conditionată a executării pedepsei. Pe data de 18 septembrie 1998 inculpatul a fost surprins de politisti si inspectori ai Oficiului Român pentru Drepturi de Autor în timp ce vindea CD-uri cu programe de calculator la punctul de lucru al societătii sale. "Aceasta este prima sentintă penală în materie de piraterie software de la adoptarea în anul 1996 a Legii nr. 8 a Drepturilor de Autor si Drepturilor Conexe si reprezintă o primă dovadă concludentă că proprietatea intelectuală începe să fie respectată si în România" a declarat un avocat reprezentant pentru România al Business Software Alliance.

. În primăvara anului 1999, pe unul din calculatoarele din reteaua dezvoltatorilor de software din Sidex a fost descoperit un virus spion. Intrusul nu a apucat însă să-si atingă scopul, fiind detectat si anihilat la timp. Tot atunci a fost descoperit si autorul, o firmă de soft din Bucuresti care urmărea anumite interese comerciale cu Sidex. La vremea respectivă primul autor acestui manual a publicat un articol într-un cotidian local despre acest eveniment, fără însă a oferi detalii suficiente, ci doar cu intentia de avertizare asupra acestei categorii de pericole.

. În toamna anului 2000, un hacker a pătruns în sistemul informatic al CS SIDEX SA. Sistemul, bazat pe o retea de câteva calculatoare Hewlett-Packard 9000, a

fost "deranjat" de un intrus care a început prin a lansa câteva mesaje injurioase, apoi si-a vărsat amarul pe directorul IT. Neluându-se măsurile cuvenite, intrusul a apărut si a doua zi, reusind să lanseze în executie două comenzi Unix de stergere a fisierelor care începeau cu o anumită literă. Intruziunea a fost posibilă din cauză că hackerul a cunoscut datele de identificare (UserName si Password) ale unui programator. Din fericire, lucrurile s-au oprit aici, găsindu-se imediat metode de a repara stricăciunile provocate si de a se înlătura pe viitor pericolul unor astfel de atacuri.

. Si alte institutii si societăti din Galati au trecut prin astfel de evenimente, multe din ele nefăcându-se publice, în ideea de a-l tenta pe infractor să revină si altădată când, se presupunea că, vor fi pregătiti să-l prindă în flagrant. Unii infractori au fost prinsi, dar au scăpat cu o simplă admonestare, fără vâlvă prea mare, altii însă nu au fost prinsi si identificati nici în ziua de azi.

Arta si psihologia hackerilor

. Hackeri sunt considerati uneori drept vrăjitori ai calculatoarelor, mai ales atunci când acestia trimit e-mail-uri sau diverse mesaje administratorilor de sistem pentru a-i anunta că au un "bug" în sistemul de securitate. Nu odată acestia au oferit chiar si solutiile de acoperire a slăbiciunilor de protectie a sistemelor.

. Multi hackeri se distrează pur si simplu atunci când pătrund în calculatoarele altora, făcând diferite glume cum ar fi schimbarea background-ului de pe desktop, închiderea si deschiderea CD-Rom-ului etc.

. Hackerii verifică si "competenta" administratorilor de sistem, supunându-i pe acestia la diferite încercări pentru a vedea dacă se pricep sau nu să tină sistemele sub protectie. Multi administratori sunt uneori terorizati, pur si simplu.

. Ce caută hackerii prin calculatoarele altora? De obicei, acestia urmăresc un cont, un card, o parolă de acces, anumite crack-uri, programe sau licente.

. Hackerii "operează" de multe ori pe conexiunile adversarilor, "transferând" astfel o bună parte din cheltuielile de comunicatie la acestia din urmă.

. Cunoscutul virus de tip worm numit "I love You", care a produs una dintre cele mai mari pagube din lume (estimată la circa 6 miliarde USD), a fost raportat de unii hackeri cu câteva luni înainte. Avertismentul lor nu a fost luat în seamă, astfel că s-a întâmplat ceea ce stim cu totii.

. Hackerii mărturisesc că există anumite site-uri cu niste programe pe care, dacă le folosesti "cu cap", nu te depistează nimeni. Dar există si reversul, adică programe pe care le poti folosi ca să depistezi orice intruziune.

. Un hacker român a blocat calculatorul unui individ pe care nu-l simpatiza deloc, în asa fel încât atunci când îl deschidea intra direct pe Word, scria un text si se reseta. Desigur, calculatorul a devenit practic inutilizabil. Revenind la sentimente mai bune, hackerul a îndreptat el însusi situatia doar după câteva zile.

. Hackerii si-au constituit organizatii care revendicã diverse drepturi, derivate, în mare mãsurã, chiar din "Declaratia universalã a drepturilor omului". "Etica hackerului" este cartea de cãpãtâi a acestora. Printre altele, aceasta prevede urmãtoarele:

- accesul la calculatoare trebuie sã fie total si nelimitat
- toate informatiile trebuie sã fie gratuite
- hackerii trebuie sã fie judecati dupã faptele lor, nu dupã alte criterii, cum ar fi vârsta, diplomele, rasa sau pozitia socialã
- poti crea artã si poti aduce frumusete cu ajutorul calculatorului.
- calculatoarele îti pot schimba viata în bine.

Se pare cã efectul a fost benefic deoarece, dupã aparitia acestui cod deontologic, hackerii au rãrit mult atacurile referitoare la câstigurile bãnesti si le-au intensificat pe cele care se referã la drepturi cetãtenesti.

. Hackerii au si un festival anual care a ajuns la a patra editie, ultima dintre ele desfãsurându-se la Las Vegas.

Instrumente folosite de hackeri

Aceste instrumente au fost special create pentru a identifica atât calculatoarele existente într-o retea, cât si slãbiciunile acestora. O bunã parte a acestora existã fabricatã si poate beneficia oricine de ea de pe Internet sau din alte surse. Sunt însã si instrumente pe care le

preparã însusi hackerul, ori de câte ori are nevoie de ele, în functie de necesitãtile care apar. Pentru cã trebuie sã fim convinsi cã un hacker adevãrat este un foarte bun specialist în domeniul calculatoarelor si se pricepe foarte bine sã-si construiascã instrumentele de lucru sau sã le perfectioneze pe cele de care dispune. În plus, el este si foarte inventiv.

Instrumentele de care vorbim nu se limiteazã doar la aplicabilitatea lor numai pe sistemele direct conectate la Internet, ci pot fi extinse la majoritatea retelelor care nu au un sistem de securitate bine implementat.

Unii cititori ar putea considera cã nu este deloc indicat sã fie publicate metodele si practicile infractorilor, care pot ajunge pe mâna unor alti potentiali rãufãcãtori. Nu am prezenta aici o parte din instrumentele si tehnicile folosite de hackeri în activitatea lor adesea de naturã infractionalã, dacã nu am fi convinsi cã:

a) o bunã parte a acestora a fost publicatã în diferite reviste de specialitate (vezi bibliografia), existând totodatã un bogat material documentar, prezentat în detaliu pe diferite site-uri din Internet
b) cunoasterea practicilor acestora ne învatã mai bine cum sã combatem acest fenomen infractional.

Începem prin a prezenta cîteva dintre cele mai cunoscute metode de atac.

1. Host Scans - este o metodã de descoperire a calculatoarelor din retea. Se bazeazã pe scanarea unui numãr de adrese de Internet si, dacã se primeste un rãspuns, înseamnã cã existã sisteme ce au adresele respective configurate, deci pot fi atacate.
2. Port Scan - metoda are la bazã scanarea

pentru identificarea porturilor deschise ale aplicatiilor (application access points), acestea urmând a fi exploatate pentru obtinerea accesului la sistem.

3. Denial-of-Service (DoS) - are scopul de a împiedica accesul la computerul respectiv al persoanelor autorizate; metoda poate consta atât în schimbarea parametrilor sau configuratiei sistemului cât si în instalarea unui program ce va fi utilizat pentru a genera un trafic foarte mare (atac) către un sistem prestabilit. Iatã câteva exemple de atacuri de tip DoS:

- *Fragmentation Attack* - protocolul TCP/IP gestioneazã mesajele foarte mari prin fragmentarea lor pentru a putea fi trimise prin retea, fiind apoi reasamblate la destinatie. Au fost dezvoltate mai multe tehnici care exploateazã slãbiciunile sistemelor de calcul ducând la blocarea acestora. Atacurile folosesc ICMP sau UDP, utilizând multe fragmente foarte mici sau fragmente ce simuleazã un pachet foarte mare imposibil de asamblat. Un astfel de atac este renumitul "Ping of Death"

- *Smurf Attack* - reprezintã atacul în care se generează un pachet ICMP echo request (acelasi cu cel utilizat de Ping) cu adresa sursã a victimei dintr-o retea si adresa destinatie reprezentând adresa de broadcast în altã retea. În cea de-a doua retea se generează un trafic foarte mare trimis la toate computerele active, care, la rândul lor, rãspund adresei victimei, blocându-l.

- *SYN Flooding* - este destinat blocării serverelor ce oferã servicii, cum ar fi cele de Web. Atacatorul simuleazã deschiderea unei sesiuni TCP prin trimiterea unui numãr foarte mare de pachete SYN (Start) fãrã a mai rãspunde la informatiile de confirmare

(handshake), blocând masina destinatie, aceasta neputând deschide alte conexiuni legitime.

Atacurile de tip DoS sunt foarte usor de replicat si aproape imposibil de prevenit. Vina principalã o poartã însãsi structura Internetului si a protocoalelor sale care au fost proiectate pentru a asigura livrarea mesajelor si având la origine încrederea reciprocã, indiferent de problemele de comunicatie si nefiind gândit împotriva unor persoane ce nu au aceleasi idealuri mãrete precum creatorii sãi.

Pentru a lansa un atac de tip DoS este nevoie sã exite un script ce poate fi gãsit pe o serie de site-uri ale hackerilor sau poate fi creat de hacker, script care sã fie capabil sã scaneze milioane de servere din întreaga lume pentru gãsirea celor vulnerabile si care care sã-si inoculeze codul sãu în serverele vizate.

Falsificarea pachetelor, tranzitarea pachetelor mãsluite, rãmâne mecanismul cheie al marii majoritãti a atacurilor si a spamming-ului. Falsificarea pachetelor este posibilã datoritã posibilitãtilor oferite de unele sisteme de operare si de producãtorii de routere. Ea este un mod gresit de a implementa confidentialitatea.

Printr-o combinatie de mecanisme de criptare si de servere specializate se poate merge oriunde sub protectia totalã a anonimatului si se pot face cumpãrãturi electronice în deplinã sigurantã.

. Un hacker cautã o adresã IP, dupã care scaneazã intervalul pe care poate exista un canal. Odatã stabilit canalul e ca si cum cei doi ar fi legati prin placa de retea. Se scaneazã apoi porturile, care sunt standard, iar dacã reuseste sã intre poate sã facã orice se poate face de la acel port.

. Intrarea propriu-zisã se poate face prin suprascrierea unui cod de boot pe care sã-l facã sã accepte ceea ce se doreste. Acesta reprezintã un bug de program. Altfel, se poate cãuta o portitã, adicã o eroare de programare.

. Pãtrunderea în calculatorul altuia se face, de obicei, prin lansarea un virus de tip "cal troian" care poate prelua în anumite conditii controlul sistemului.

. Cum ajunge virusul la destinatie? Prin pãcãlealã. Iatã un exemplu povestit de un hacker autohton: intri pe IRC, te dai drept fatã si-i propui partenerului de discutie sã-i trimiti o pozã si ... la pozã atasezi virusul. Pânã se lãmureste celãlalt despre ce e vorba, ai pãtruns în calculatorul lui.

. Evident, virusul de tip "cal troian" trimis trebuie sã fie unul dintre cei care nu poate fi detectat de programele anti-virus cele mai utilizate. Însã, de multe ori se poate merge aproape la sigur si pe ideea cã multi nu au nici cea mai micã protectie împotriva virusilor.

Despre parola de BIOS

Cea mai uzualã metodã de protectie este parola folositã la deschiderea calculatorului, adicã asa numita parolã de BIOS. Existã douã metode de a depãsi situatia în care ai nevoie sã cunosti parola si în acelasi timp sã intri în BIOS:

a) Cea mai popularã si comodã este aceea de a trece de parolã scriind câteva parole comune care, în principiu, ar trebui sã functioneze pe orice BIOS. Acestea sunt: Lkwpeter, j262, AWARD_SW, Biostar. Dacã nici una dintre acestea nu functioneazã, sigur se gãseste una

care să meargă la adresa de Web www.altavista.box.sk.

b) Cea de-a doua metodă, ceva mai complicată, necesită "deschiderea" calculatorului si extragerea bateriei care asigură energie CMOS-ului. Pentru această operatie trebuie să identificati placa de bază si să găsiti acea baterie de litiu rotundă care seamănă cu o monedă de argint. Va trebui apoi s-o scoateti, iar după 30 de secunde s-o puneti la loc. Când veti deschide calculatorul, după această operatie, va uita cu desăvârsire de parolă.

Din experienta unor hackeri

Furtul unui cont pe Internet este foarte posibil. Accesul la Internet se poate face, în general, prin două metode: se plătesc aproximativ 20 USD în contul oricărui provider si taxa lunară sau se fură contul unui oarecare user conectat deja. Userul nu trebuie să fie întotdeauna o persoană fizică, ci poate fi si o organizatie.

Mai întâi se scanează o zonă de adrese IP. Aceasta se poate afla de pe un calculator deja conectat la Internet, de exemplu, dintr-un Internet-cafe. Dacă, de exemplu, IP-ul este 212.0.203.42, atunci se scanează de la 212.0.203.0 la 212.0.203.255. În momentul scanării este de preferat să nu vă legati printr-un server, ci direct, iar viteza folosită ar trebui să fie cea reală, apăsând "scan". În scurt timp, în partea stângă a ferestrei vor apărea adrsele IP ale computerelor care sunt disponibile în retea si denumirile acestora (ex.: 212.0.203.24 cu C:/ si D:/). Cu alte cuvinte, cineva extrem de neglijent v-a pus la dispozitie hard-ul si CD-ul.

Operatiile se pot face prin intermediul unui soft de tip "IP scanner", numit Legion 2.1, care este cât se poate de simplu de utilizat, nefiind necesare nici mãcar instructiuni preliminare. Se poate crea astfel acces direct pe hardul unui computer strãin.

Pe hardurile strãine pot exista accese de tip "read-only", în care se poate doar vizualiza informatia, sau "full-mode", prin care se poate accesa total informatia.

În caz cã unele dintre calculatoare au parole, nu este nici o problemã, deoarece Legion 2.1 are un algoritm de tip 'brute-force" cu care se poate intra. Odatã intrat pe hard disk-ul computerului strãin trebuie cãutat directorul Windows si copiate de acolo toate fisierele cu extensia .pwl (de exemplu, name.pwl). În aceste fisiere se aflã parola si identificarea de care este nevoie pentru conectarea la provider. Însã fisierele .pwl sunt cifrate. Acest impediment poate fi evitat cu ajutorul unui program care "sparge" acest tip de fisier. Un soft dedicat acestui gen de operatiune este RePwl.

De aici mai departe nu mai trebuie decât sã faceti rost de telefonul providerului de la care tocmai aveti un cont. Aceste informatii le puteti afla direct de pe site-urile providerilor în cauzã.

Vestitul hacker Kevin Mitnik avea o metodã proprie de a-si pregãti spargerea unui server. El proceda astfel: suna mai întâi providerul si încerca sã afle parola, dându-se drept un user care a uitat parola si ar dori sã obtinã una nou?. Metoda mergea în aproximativ 5% din cazuri, depinzând de multe ori de cine ridica receptorul.

Alte stiri despre infractiuni informatice

. O crestere a rolului Internetului ca mediu de desfãsurare a unor fraude ce aduc mari neajunsuri este datã si de urmãtorul exemplu. Dupã o studiu efectuat de Jupiter Communications, populatia on-line din SUA a atins în 1998 cifra de 60 milioane, reprezentând 22,4% din populatia totalã. Dupã unele statistici guvernamentale, cel putin 46 milioane de americani au cumpãrat on-line pânã în anul 2000, cheltuind în jur de 350 USD/persoanã/ an.

. Multe grupãri de hackeri se dovedesc tot mai bine organizate si mai profesioniste. Ele sunt cu cel putin un pas înaintea capacitãtii politiei si a expertilor în securitatea informaticã de a prevedea infractiunea.

. Companiile care gestioneazã cãrtile de credit înregistreazã anual pagube de ordinul miliardelor de USD. România este una dintre cele mai importante surse de plãti frauduloase, asa încât, majoritatea firmelor americane refuzã sã accepte plãti cu cãrti de credit emise cetãtenilor români. Politia românã este în posesia unui mare numãr de reclamatii cu privire la aceste fraude.

. Un apãrãtor al legii apreciazã: "Hotul modern nu mai este un bun trãgãtor, ci are cunostinte de programare si de gestiune informatizatã a sistemului bancar. El stã undeva într-o parte a lumii si sparge o bancã aflatã la sute sau mii de kilometri, iar acest lucru îl face în voie, acoperit de anonimatul pe care îl oferã retelele de comunicatii. Nu se pune problema de atac armat, riscul e minim, performanta maximã, nici nu existã vãrsare de sânge - lucruri care în conditii clasice pot constitui ori circumstante agravante ori concurs de infractiuni".

. Calculatorul a devenit deja principalul corp delict al majoritãtii infractiunilor moderne.

. În SUA s-a înfiintat la 8 mai 2000 Centrul de reclamatii pentru fraude pe Internet (IFCC - The Internet Fraud Compliant Center), o asociere între NW3C (The National White Collar Crime Center) si FBI (The Federal Bureau of Investigation). FBI manifestã un interes deosebit pentru depistarea fraudelor, anihilarea infractorilor, protejarea pãgubitilor.

. Cele mai frecvente infractiuni sunt cele bazate pe comertul electronic, incluzând folosirea cãrtilor de credit. Pe locul doi se aflã infractiunile care au în vedere retelele de calculatoare si sistemele de comunicatii.

. Într-un studiu recent despre securitatea sistemelor informatice ale unor corporatii si agentii guvernamentale americane, realizat de Computer Securites Institute cu ajutorul FBI, au apãrut urmãtoarele cifre:

- 90% dintre organizatii au detectat probleme de securitate în ultimile 12 luni
- 70% au raportat probleme importante, altele decât virusi, furturi de laptop-uri sau abuzuri în folosirea legãturii la Internet
- 74% au sustinut cã au avut pierderi financiare
- trei ani la rând s-a constatat cresterea numãrului de accesãri neautorizate prin Internet (59%), fat? de 38% din reteaua internã
- 273 de institutii au raportat pierderi de aproape 266 milioane USD (media anualã fiind 120 milioane USD).

Reclamatiile înregistrate în numai sase luni sunt: 2/3 din totalul plângerilor sunt fraude în domeniul licitatiilor.

Mãrfurile nelivrate si plãtile neefectuate acoperã alte 22% din reclamatii, frauda comisã prin spargerea codurilor cãrtilor de credit si a celor de debit nu depãseste 5%. Altele: cãrti de credit-debit = 4,8%, fraude de confidentã 4,6%, fraude de investitii = 1,2%, altele = 3%. Paguba totalã reclamatã a atins cifra de 4,6 milioane USD, cu o medie de 894 USD per persoanã reclamantã.

Cine sunt infractorii?

- Bãrbatii sunt "mult mai hoti" decât femeile,
- Cei mai experti hackeri sunt americanii,
- Românii se situeazã pe locul patru.

Pãgubitii sunt bãrbati, cu vârsta 30-50 ani, cei mai multi din afara business-ului si rezidenti în unul din cele mai mari state americane. Vârsta medie a infractorilor: 26 ani.

. Topul primelor 10 tãri de provenientã a infractorilor:

1. 92,2%-Statele Unite	2. 1,8 % - Canada
3. 1,3 % -Ucraina	4. 1,1 % - România
5. 0,5 % -Anglia	6. 0,3 %- Hong Kong
7. 0,3 % -Australia	8. 0,2 % - Indonezia
9. 0,2 % -Germania	10. 0,2 % - Olanda.

. Peste 1,3 milioane de români au folosit reteaua Internet în anul 2000, statisticile asezându-ne din acest punct de vedere pe locul 4 în Europa de Est.

. Cu 1000 USD se pot cumpãra echipamente pentru a produce cãrti de credit.

. Pe Internet existã liste a tipurilor de infractiuni în mediul virtual precum si descrierea lor (inclusiv un FAQ) cu tipurile de fraude on-line.

. Produsul Microsoft Outlook, unul dintre cele mai populare programe de e-mail aflate în uz, a fost lansat pe piatã cu unele bug-uri care permiteau unui programator rãu intentionat sã lanseze un atac prin e-mail. Aceastã "scãpare" permitea totodatã si pãtrunderea unor noi tipuri de virusi e-mail, din categoria "cailor troieni".

. De curând a fost înfiintat si un "Muzeu al fraudei pe Web", de cãtre compania Ad Cops, care contine în prezent o colectie doar cu 13 exponate, pentru ajutor împotriva fraudei prin e-commerce.

. Frauda pe calculator, în ciuda restrictiilor legislative severe, reprezintã un pericol major. Astfel, într-o statisticã americanã, acest delict se ordoneazã astfel:

- furt de bani: 45%
- furt de date si/sau programe: 16%
- distrugerea programelor: 15%
- alterãri de date: 12%
- furt de servicii: 10%
- diverse delicte: 2%.

Clasamentul alcãtuit dupã valoarea medie în dolari a pagubelor produse aratã astfel:

1. 93.000 pentru distrugeri de date si/sau sisteme
2. 55.166 pentru furturi de programe si date
3. 10517 pentru furturi de bani.

. De curând Microsoft a lansat ceea ce reprezintã prima sa aplicatie dedicatã securitãtii - un sistem firewall si pentru Web cache. Internet Sucurity and

Acceleration (ISA) Server este produsul pentru securitate si performante din familia serverelor .NET. Acesta protejeazã reteaua fatã de un acces neautorizat, fatã de atacurile externe, realizând inspectii privind securitatea asupra traficului de retea în ambele directii si alertând administratorii în cazul unei activitãti suspecte. Editia standard a produsului ISA Swerver costa circa 1.500 USD per procesor, iar editia scalabil? pentru organizatii costã circa 6000 USD per procesor.

. În SUA existã nu mai putin de 6 agentii guvernamentale care se ocupã cu fraudele pe Internet si au rolul sã investigheze si sã instrumenteze cazurile semnalate.

. Statisticile americane apreciazã cã fraudele financiare au atins cifra de 45 % din totalul infractiunilor informatice.

. O fabricã de microprocesoare costã circa 6 miliarde USD, constructia si exploatarea ei durează în jur de 3 ani, dupã care nu se poate reutiliza aproape nimic.

. Criptarea este singura metodã care asigurã o confidentialitate perfectã.

. În afarã de unul sau douã servicii de provider de Internet din tara noastrã, toate celelalte nu sunt certificate.

. Existã virusi ce pot provoca si stricãciuni ale pãrtii de hard? Iatã o întrebare pe care si-o pun multi. Rãspunsul este da. Iatã si douã exemple: unii scriu si rescriu portiuni de hard pânã îl stricã, altii deschid si închid placa de bazã pânã o ard.

. În ultimii doi ani au fost furate din Internet mai mult de 300.000 de carduri. Multi dintre pãgubiti nici nu si-au dat seama iar hackerii nu au nici un interes sã atragã atentia asupra lor.

. În ultimii ani au cãzut pe mâna hackerilor unele dintre cele mai renumite site-uri si centre de comert electronic, precum: Amazon, eBay, Yahoo, NBD s.a.

. Hackerii, constituiti în diferite organizatii, pot declansa chiar si actiuni comune de rãzbunare sau protest. O arestare a unui hacker, cunoscut sub numele de "Stormbringer", a condus la scoaterea din functiune în mai multe rânduri a site-ului FBI, precum si la numeroasele atacuri de gen "Denial-Of-Services" asupra site-urilor comerciale. De mai multe ori asupra porturilor din serverele care sustin aceste pagini s-a abãtut o ploaie de date care a fãcut ca paginile sã nu mai poatã fi accesate. Desi existã mai multe tipuri de protectie împotriva acestui gen de atacuri, o protectie importantã a fost pusã la dispozitie de curând si poate fi întâlnitã la adresa:
http://solid.ncsa.uiuc.edu/~liquid/patch/don_lewis_tcp.diff.

. "Într-o tarã în care legile sunt într-o miscare permanentã, în care se manifestã o imobilitate excesivã a legislatiei, nu mai este suficientã forma gutenbergianã a documentelor", sublinia cu ocazia unei conferinte de presã domnul Gabriel Liiceanu, directorul Editurii Humanitas.

. Cu ajutorul programului Ositron Tel 2.1 poate fi controlatã confidentialitatea mesajelor telefonice. Acest soft criptează în timp real cuvântul rostit, astfel încât ascultãtorul nu poate auzi decât sunete nearticulate. Se utilizează procedeul OTPS de criptare cu o cheie lungã si una scurtã. Alte informatii pot fi gãsite la adresa: http://www.ositron.com.

Partea a IV-a

SECURITATEA INFORMATIEI

Necesitatea securizării informatiei

Securitatea informatiei reprezintă un lucru extrem de important pentru fiecare computer conectat la Internet, sau aflat într-o retea de tip intranet, extranet si chiar o retea locală. Mai mult, chiar si pentru un PC stand-alone securitatea informatiei poate fi o problemă serioasă, atunci când acesta contine informatii personale, secrete, cu anumite grade de confidentialitate.

Securitatea informatiei protejează informatia de o paletă largă de pericole legate de asigurarea continuă a activitătilor, de minimizarea pagubelor si de maximizarea recuperării investitiilor si a oportunitătilor de afaceri.

Indiferent dacă calculatorul se află într-un birou la serviciu sau pe un pupitru de acasă, asigurarea securitătii informatiei se poate pune cu aceeasi acuitate.

Evident, în cazul în care avem de-a face cu o retea de calculatoare asigurarea securitătii reprezintă o problemă deosebit de serioasă si, totodată, cu mult mai dificilă.

Multe din atacurile recente de tip denial-of-service care au reusit să pună într-un real pericol câteva site-uri de Web foarte populare, unele chiar guvernamentale, au reusit să pună pe jar autoritătile din mai multe tări puternic dezvoltate. Unele voci au sustinut chiar că

pericolul este mult mai mare decât se presupunea până atunci.

Au existat suficiente dovezi care sustineau pozitia acelora ce credeau cã atacurile hackerilor au fost posibile din cauzã cã s-a reusit obtinerea accesului doar la computerele slab protejate. Cu alte cuvinte, spãrgãtorii de coduri au succes doar acolo unde nu se asigurã o adevãratã securitate.

Asa cum am avut ocazia sã mentionãm în capitolul despre virusii spioni ai calculatoarelor, existã o serie de virusi de e-mail, cum ar fi celebrul virus Melissa, care încearcã sã "fure" - din calculatorul de acasã sau de la birou - si sã trimitã la o destinatie prestabilitã documente confidentiale.

Pericolul sabotajului prin calculator bazat pe virusi, care pot face distrugeri extraordinare, este astãzi bine cunoscut si de necontestat. Ca sã nu mai vorbim de virusi care pot prelua controlul complet asupra unui calculator dintr-o retea, precum periculosul cal troian "Back Orifice".

În pofida unor sisteme legislative destul de bine puse la punct, furtul de informatii prin intermediul calculatorului s-a extins foarte mult, mai ales în unele tãri care detin tehnologii avansate. El reprezintã un domeniu extrem de delicat, iar pentru protectia si securitatea datelor se fac eforturi uriase. Anual se cheltuiesc sume imense pentru preîntâmpinarea fraudelor pe calculator. Numai pentru SUA unele statistici indicã sume, cheltuite anual în acest scop, situate între 4 si 6 miliarde de dolari.

Cele enumerate mai sus ar putea însemna doar o micã parte din numeroasele motive pentru care este necesar sã se acorde o atentie deosebitã securitãtii informatiei din calculatoare.

S-ar putea spune cã majoritatea utilizatorilor din cele mai mari si mai importante institutii din lume se aflã sub acoperirea unor firewall-uri de companie sau personale si cã, în cazul lor, securitatea este complet asiguratã. În realitate însã, lucrurile nu stau chiar asa. Si dovezi în acest sens existã, desigur. Aproape zilnic apar pe Internet stiri despre spargerea unor site-uri de Web importante, despre furturi de informatii din diverse retele dintre cele mai bine puse la punct. Iar dacã mai punem la socotealã si faptul cã, multi dintre cei pãgubiti refuzã sã-si facã publice accidentele de aceastã naturã, chiar si din simplul motiv de a nu risca pierderea credibilitãtii sau a prestantei, atunci, desigur, putem considera cã statisticile nu ne oferã dimensiunea realã a fenomenului, iar acesta este cu mult mai îngrijorãtor.

În contextul afacerilor informatia si procesele pe care se sprijinã sistemele si retelele informatice sunt subiecte deosebit de importante. Cele trei caracteristici de bazã ale informatiei, anume confidentialitatea, integritatea si disponibilitatea, sunt esentiale pentru mentinerea competitivitãtii, profitabilitãtii, legalitãtii si imaginii comerciale ale unei organizatii.

Din ce în ce mai mult, organizatiile, sistemele si retelele lor informatice sunt confruntate cu amenintarea securitãtii informatiilor provocate de un larg spectru de surse, incluzând frauda, spionajul, sabotajul, vandalismul, incendiile si inundatiile. O sursã comunã de pericol este reprezentatã de atacurile virusilor electronici care pot provoca daune si distrugeri considerabile. Aceste mijloace devin din ce în ce mai agresive si mai sofisticate.

Unii oameni de afaceri si profesionisti au ajuns la concluzia cã un hacker suficient de competent poate pãtrunde în aproape orice sistem de calcul, inclusiv în

cele care au fost protejate prin metode bazate pe parole si criptarea datelor.

Altii, mai sceptici, sustin cã, chiar si atunci când un sistem este bine protejat împotriva atacurilor din exterior, rãmâne întotdeauna alternativa trãdãrii din interior. Multe date secrete, cum ar fi listele de clienti, salariile angajatilor, investitii si bugete, referate confidentiale s.a., pot fi copiate pur si simplu pe o dischetã, iar aceasta poate fi scoasã de la locul de muncã deseori chiar fãrã sã se sesizeze ceva.

Calculatoarele de tip mainframe rezolvã problema furtului prin aceastã sursã pãstrând calculatorul si suporturile mari de stocare a datelor încuiate. În cazul mainframe-urilor, singura cale de a putea folosi datele este cea oferitã de terminalele aflate la distantã, si care sunt dotate cu un ecran, o tastaturã, dar nu si cu unitãti de disc.

Din cauza acestei sigurante suplimentare oferite de sistemele de tip mainframe, unii experti sustin cã retelele locale de calculatoare personale ar trebui configurate la fel, uitând cã centralizarea excesivã a mainframe-urilor a fost unul din principalele motive pentru care s-au dezvoltat calculatoarele personale.

Orice conectare obisnuitã la Internet nu este întotdeauna lipsitã de riscuri. Conexiunea propriu zisã, absolut inocentã la prima vedere, ar putea fi însotitã prin partaj fraudulos de cãtre un parazit sau un program spion, care are un rol foarte bine definit: de a fura o parte din informatiile manipulate, desigur, parte din ele cu caracter strict confidential pentru proprietar.

Sunt atât de mari pericolele care ne pasc? Cu sigurantã cã existã si o mare dozã de neîncredere în

aprecierile de naturã pesimistã a unora, si de multe ori, cu sau fãrã voie, se exagereazã.

În lumea specialistilor IT se obisnuieste sã se spunã cã un PC este complet protejat de un produs firewall si de un program antivirus. Existã produse informatice care pot asigura o protectie foarte bunã pentru grupurile mici sau pentru PC-urile individuale. De exemplu, firewall-uri precum ZoneAlarm (www.zonelabs.com) sau BlackICE Defender (www.netice.com), sunt foarte la modã astãzi. Iar produsele antivirus sunt, asa cum am avut ocazia sã mai spunem, foarte multe si foarte eficace.

Tranzitia cãtre o societate informationalã implicã nevoia de informatii credibile, iar progresul tehnologic are implicatii de ordin exponential asupra evolutiei. Din acest punct de vedere necesitatea securizãrii informatiei pãstrate si procesate prin intermediul calculatoarelor decurge pur si simplu din necesitatea de conectare si de comunicare, iar globalizarea si Internetul au schimbat complet fata lumii la confluenta dintre mileniului.

Securitatea informatiei

Informatia este un produs care, ca si alte importante produse rezultate din activitatea umanã, are valoare pentru o organizatie si în consecintã, este necesar sã fie protejatã corespunzãtor.

Informatia poate exista în mai multe forme: poate fi scrisã sau tipãritã pe hârtie, memoratã electronic, transmisã prin postã sau utilizând mijloace electronice, ilustratã pe filme sau vorbitã într-o conversatie. Indiferent de formele sub care existã, indiferent de mijloacele prin

care este stocatã sau partajatã, informatia trebuie totdeauna strict protejatã.

În ceea ce ne priveste vom preciza cã, desi conceptul de securitate a informatiei este cu mult mai larg, referintele din acest manual cuprind doar aspecte legate strict de informatia pãstratã si procesatã prin intermediul caculatorului.

Din punct de vedere al pãstrãrii si securitãtii informatia este caracterizatã de:

- *confidentialitate*: caracteristicã a informatiei care asigurã accesibilitatea numai pentru cei autorizati sã aibã acces la ea,
- *integritatea*: reprezintã garantia acuratetii si completitudinii informatiei si a metodelor de prelucrare a acesteia,
- *disponibilitatea*: reprezintã asigurarea cã numai utilizatorii autorizati au acces la informatii si la produsele aferente oricând existã o solicitare în acest sens.

Fiecare organizatie în parte îsi poate implementa propriul sãu sistem de asigurare a securitãtii informatiei. Un management al securitãtii informatiei se realizeazã prin implementarea unui set corespunzãtor de actiuni care cuprinde politici, practici, instrumente si proceduri, structuri organizationale, precum si functii software. Toate actiunile trebuie prevãzute, definite si aplicate pentru a asigura cã sunt întrunite obiectivele specifice de securitate ale organizatiei.

Din punct de vedere al gradului de confidentialitate pe care îl asigurã informatia comportã mai multe nivele de secret:

- informatii nesecrete
- informatii secrete:
- secret de serviciu,
- secret
- strict secret,
- strict secret de importantã deosebitã.

Un sistem integrat de securitate a informatiilor cuprinde nu mai putin de sapte sisteme de securitate:

1. Securitatea fizicã
2. Securitatea personalului - need to know
3. Securitatea administrativã
4. Securitatea IT (INFOSEC)
5. Securitatea comunicatiilor (COMSEC)
6. Securitatea criptograficã
7. Securitatea emisiilor EM (TEMPEST)

Pentru a întelege mai bine care sunt mecanismele de asigurare a unei bune securitãti a informatiei este necesar sã clarificãm care sunt tipurile de amenintări asupra celor trei caracteristici esentiale ale informatiei.

Iatã principalele tipuri de amenintări, întâlnite în mod uzual în retele Internet si Intranet:

1. *Tipuri de atacuri*:
    a) intruziune (utilizator legitim, identificare falsã)
    b) blocarea serviciilor (denial-of-service)
    c) furtul de informatii.
2. *Scopul atacului*:
    a) amuzament
    b) palmares

c) vandalism
d) spionaj
e) stupiditate si accidente

3. *Se asigurã protectie pentru*:
   a) date si informatii
      - confidentialitatea,
      - integritatea,
      - disponibilitatea.
   b) resurse calculator
   c) reputatie.

LISTA PRINCIPALELOR SERVICII INTERNET / INTRANET / EXTRANET

1. Mesagerie electronicã
2. Transfer de fisiere
3. Terminal cu acces la distantã si executie comenzi
4. Stiri (buletine informative)
5. World Wide Web
6. Alte servicii de informare:
   . Gopher
   . WAIS (Wide Area Information Service)
   . Informatii despre persoane
7. Servicii de conferintã în timp real (Talk, IRC)
8. Servicii de nume (DNS)
9. Servicii de coordonare retea (Network management services)
10. Serviciul de timp (time service)
11. Sistemul fisierelor de retea (Network file systems)

Măsuri si contramăsuri de protectie:

Modele de securitate:

1.1. Fără protectie specială (securitate minimă asigurată de furnizorul de echipamente sau programe)

1.2. Securitate prin obscuritate

1.3. Securitate la nivel de host pentru retele mici - se asigură prin autentificare si limitare a accesului

1.4. Securitate la nivel de retea pentru retele mari - se asigură prin sisteme Firewall

Servicii de autentificare si limitare a accesului:

2.1. Tipuri de acces la servicii:

- "anonim" (fără autentificare)
- "nonanonim" (cu autentificare)

2.2. Mecanisme de autentificare:

- printr-o caracteristică fizică personală
  - . scanare digitatie
  - . scanare retină
  - . scanare vocală
- prin cunostinte individuale
  - . parolă
  - . chestionar
- printr-un obiect personal
  - . smart card

2.3. Servere de autentificare - asigurare comunicatie securizată între client si server.

Firewall - o componentă sau un set de componenete care restrictionează accesul între o retea protejată si Internet sau alte seturi de retele.

Tehnici folosite:

a) Filtrare de pachete - dirijează pachetele între host-urile interne si externe în mod selectiv. Filtrarea permite sau blochează diferitele tipuri de pachete în functie de "politica" de securitate stabilită (screening router), astfel:

- blocarea tuturor conexiunilor de la sisteme din afara retelei interne, cu exceptia conexiunilor de intrare SMTP (se asigură numai receptia e-mail)
- blocarea tuturor conexiunilor de la sisteme precizate
- permiterea serviciilor e-mail si FTP si blocarea serviciilor considerate periculoase (acces terminal, si altele)

b) Serviciul "proxy" - este un program care dialoghează cu servere externe din partea clientilor din reteaua internă. "Proxy client" discută cu serverul proxy, care translatează (releu) solicitările acceptate către serverele reale si apoi translatează către clienti. Sunt cunoscute si sub numele de "gateway la nivel aplicatie". Serverul proxy gestionează comunicatia între utilizatori si serviciile Internet conform unei scheme de securitate.

Mesagerie securizată:

a) Confidentialitatea mesageriei electronice

b) Sisteme de e-mail sigur (pe bază de criptografie)

. PGP - Pretty Good Privacy - este un pachet complet de securitate a e-mail-ului care furnizează o confidentialitate destul de bună, autentificare, semnătură digitală si compresie. Este distribuit gratis prin

Internet, sisteme de informare în retea si retele comerciale. Este disponibil pentru platformele MS-DOS, Windows, UNIX, MacIntosh. Utilizează algoritmi de criptare existenti (RSA, IDEA, MD5)

. PEM - Privacy Enhanced Mail - este un pachet de postă cu confidentialitate sporită, standard oficial Internet (RFC 1421 - RFC 1424). Administrarea cheilor este mult mai structurată decât în PGP. Cheile sunt certificate de o "autoritate de certificare" (numele utilizatorului, cheia publică si data de expirare).

Securitate Web (browsere, servere si comunicatii Web)

a) Browsere

. atacuri facilitate de erorile în implementarea browserelor

. utilizarea răuvoitoare a facilităților oferite de browsere

b) Securitatea serverelor Web

. atacuri comune

. securizarea codurilor active

c) Pericolul scripurilor CGI

. oferă utilizatorilor posibilitatea de a determina serverul să execute operatii

. securizarea scripturilor CGI:

. testarea cuprinzătoare a fiecărui script nou

. tratarea complexă a datelor introduse

. interzicere metacaractere tip shell Unix, care pot forta sistemul să execute actiuni neintentionate si potential devastatoare

. testare script cu o diversitate de

browsere

. interzicere asamblări nume de fisiere pe baza celor introduse de utilizator

d) Transmiterea de mesaje si fisiere în sigurantă

. SSL - Secure Cocket Layer - un produs dezvoltat de Netscape Communications care furnizează criptare cu cheie publică pentru TCP/IP (HTTP, telnet, ftp) între două calculatoare host

. S-HTTP - Secure HTTP - un protocol dezvoltat de asociatia CommerceNet care operează la nivelul protocolului HTTP, solicitând expeditorului si destinatarului să negocieze si să folosească o cheie sigură.

Aspecte privind protectia informatiei

Calculatoarele personale prezintã vulnerabilitãti pentru cã în general nu existã protectie hardware a memoriei interne si externe: un program executabil poate avea acces oriunde în memoria internã sau pe hard-disk.

În orice sistem de calcul, protectia presupune asigurarea programelor si datelor împotriva urmãtoarelor actiuni:

1. pierderi accidentale, cauzate de cãderile de tensiune, defectarea unitãtilor de hard disk-uri
2. accesare neautorizatã a datelor si programelor, prin actiuni de parolare si criptare a informatiilor, oprind si copierea neautorizatã
3. fraudã pe calculator (sustragerea sau alterarea de date, furturi de servicii)
4. virusarea software-ului.

Pentru o protectie eficientã este necesar sã fie cunoscute si sã se asigure urmãtoarele elemente:

1. identificarea accesului prin reguli si relatii între utilizatori si resurse
2. evidenta accesului, pentru urmãrirea utilizãrii resurselor sistemului, precum si pentru posibilitatea refacerii unor date în caz de distrugere
3. integritatea si confidentialitatea datelor
4. functionalitatea programelor.

Mijloacele prin care se poate asigura protectia sunt:

1. mãsuri organizatorice, contra distrugerii datorate catastrofelor naturale referitoare la selectia

profesionalã a personalului, organizarea unui sistem de control a accesului, organizarea pãstrãrii si utilizãrii suporturilor de informatii

2. mãsuri juridice, care cuprind documente normative care controleazã si reglementeazã procesul prelucrãrii si folosirii informatiei

3. mijloace informatice, constituite din programe de protectie si tehnici de criptare a informatiei.

Cele mai cunoscute si utilizate modele de asigurare a protectiei (autorizare a accesului) sunt:

a) Modelul Hoffman

Modelul constã dintr-un set de reguli care considerã 4 tipuri de obiecte protejate: utilizatori, programe, terminale si fisiere, fiecare cu 4 caracteristici de securitate:

- autoritatea (nesecret, confidential, secret, strict secret)
- categoria (compartimente specifice de grupare a datelor (acces limitat, acces cu aprobare)
- dreptul (grupã de utilizatori care au acces la un obiect dat)
- regimul (multimea modurilor de acces la un obiect dat: citire, actualizare, executie program)

b) Modelul Kent

Modelul are 5 dimensiuni: împuterniciri, utilizatori, operatii, resurse, stări. El contine un proces de organizare a accesului bine definit, printr-un algoritm. Accesul la date este considerat ca o serie de cereri ale utilizatorilor pentru operatiile la resurse, într-un moment în care sistemul se aflã într-o stare anumitã.

Terminologie

Identificarea reprezintă recunoasterea unui nume, număr sau cod afectat unei persoane, proces sau echipament.

Autentificarea reprezintă verificarea dacă persoana, procesul sau echipamentul reprezintă ceea ce pretinde a fi, având un anumit drept de acces la o resursă protejată. Aceasta se execută verificând informatiile furnizate de utilizator prin compararea cu informatiile de identificare si autentificare continute de sistem. Aceste informatii, din cauza cerintelor de siguranță, trebuie reverificate periodic prin autentificarea persoanelor implicate. Pentru procedura de autentificare se folosesc parole sau alte tipuri de informatii (cont, nume, cuvinte). Dacă utilizatorul furnizează corect aceste informatii, sistemul de calcul acceptă în continuare dialogul.

Autentificările se pot face:

1. prin parolă, un sir de caractere tastate de utilizator care va fi validat de calculator.
2. prin chestionar, o serie de întrebări standard si răspunsurile aferente.
3. prin proceduri, se execută o anumită procedură de calcul, implementată pe calculator pe baza unui anumit algoritm. Metodă mai sigură, dar mai costisitoare ca timp si resurse de calcul consumate.
4. prin metode criptografice, schimbarea unei valori unice bazată pe o cheie prestabilită.

Autorizarea accesului reprezintă permisiunea de executie a unor anumite operatiuni asupra unor resurse ale calculatorului (fisiere, baze de date, înregistrări, programe etc.).

Vulnerabilitatea reprezintă caracteristica hardware-ului sau software-ului de a permite utilizatorilor

neautorizati să obtină accesul sau să-si mărească nivelul de acces.

Scara vulnerabilitătilor, functie de gradul descrescător de periculozitate pentru sistemul victimă, este datã de:

1. *gradul A*: un potential pericol pentru întregul sistem, permitând utilizatorilor de la distantă rău intentionati acces neconditionat. Cele mai periculoase provenind din administrarea sau configurarea eronată a sistemului. Una din surse este generată de fisierele de configurare livrate o datã cu software-ul Web. Aceste fisiere contin avertismente referitoare la scripturile model livrate, care pot oferi unui intrus din afara retelei posibilitatea de a citi anumite fisiere sau chiar accesul la nivel de cont.

2. *gradul B*: permit utilizatorilor locali să-si mărească nivelul de privilegii, putând obtine controlul asupra sistemului. Permit accesul neautorizat, fiind cauzate de o disfunctionalitate a programului de trimitere postă electronică send-mail, care permite evitarea testării identitătii utilizatorului local si astfel acesta poate obtine o formă de acces ca root.

3. *gradul C*: permit oricărui utilizator, din interior sau exterior, să întrerupă, să degradeze sau să obstructioneze functionarea sistemului. Acestea sunt numai la nivelul functiilor de retea ale sistemului si pot fi corectate de autorii software-ului sau prin programe de corectie (patch-uri) de la producătorul de soft. Aceste vulnerabilitãti conduc la refuzul serviciului (DoS-Denial of Service), prin atacuri care sunt constituite din trimiteri de volume mari de cereri de conexiune către un server care se va supraaglomera, va fi în situatia de a răspunde lent,

în imposibilitatea de a răspunde la cereri.

Atacuri

Spãrgãtoarele de parole sunt programe care pot decripta parole sau care pot dezactiva protectia prin parole. Se folosesc programe de simulare care încearcã sã gãseascã o corespondentã (potrivire) între variantele de parole cifrate si textul cifrat original. Aceste programe folosesc calculatorul pentru încercarea cuvânt cu cuvânt la viteze de calcul mari, pentru ca în final sã se ajungã la cuvântul sau cuvintele corespunzãtoare.

Interceptoarele (sniffers) sunt dispozitive software sau hardware care capturează informatiile transportate printr-o retea indiferent de protocolul de comunicatie. Vor sã configureze interfata de retea (placa de retea) în modul neselectiv si prin aceasta sã poatã sã captureze traficul de retea.

Scanerele sunt un program care detectează punctele slabe în securitatea unui sistem local sau la distantã. Detectarea vulnerabilitãtilor de securitate pe orice server. Atacã porturile TCP/IP si înregistrează rãspunsul de la tintã, putând obtine informatii despre aceasta. Atribute: gãseste un server sau o retea, aflã serviciile care rulează pe server si testează aceste servicii pentru a gãsi vulnerabilitãtile.

Legislatia privind securitatea informatiei

Dacã în SUA reglementãrile internationale privind securitatea informatiei au fost cuprinse în proiectul mai larg cunoscut sub numele Orange Book - 1985, echivalentul acestora în Europa este asigurat de Criteriile Comune de evaluare a securitãtii pentru IT - 1999 -V2.1.

În 1986 în SUA a fost adoptatã legea privind fraudele si abuzul prin utilizarea calculatorului electronic (Computer Fraud and Abuse Act).

Ca reper de aplicare a legii în SUA este reprezentativ celebrul proces US versus Morris, generat de lansarea unui virus informatic de tip vierme (Morris worm). Procesul s-a bazat pe acuzatia accesării intentionate si neautorizate a unor computere de interes federal, cauzând pagube si pierderi mai mari de 1000 $ (conform legislatiei).

La scurt timp dupã aceasta au apãrut noi amendamente legislative, cu pedepse diferentiate functie de gravitatea cazurilor de infractionalitate. Au fost create organizatii pentru a stopa sau limita infractionalitatea.

California este socotitã se pare capitala mondialã a fraudelor si delictelor efectuate cu calculatorul electronic. În acest stat existã acte legislative specifice referitoare la cracking (Codul Penal din California, Sectiunea 502) cu lista de actiuni care intrã sub autoritatea legii: activitãtile neautorizate, penetrarea sistemelor, stergerea, modificarea, furtul, copierea, afisarea, distrugerea, precum si refuzul serviciilor. Legea prevede pedepse penale aspre, care în cazul minorilor sunt suportate de pãrinti sau tutori.

În alte state americane legile locale sunt diferentiate ca duritate a pedepselor. În Texas situatia este mai putin strictã, acsiunile de acces ilegal la un calculator fiind diferentiat clasate drept contraventii sau infractiuni de

diferite nivele de periculozitate. Statul Georgia, de exemplu, are pedepse de până la 15 ani închisoare si 50.000 USD amendă.

Alte detalii cu privire la statutul delictelor pe calculator pot fi găsite la adresa site-ului de Web al EFF - Electronic Frontier Foudation: http://www.eff.org care cuprinde si lista legilor în domeniul infractionalitătii cu calculatorul.

China are o legislatie foarte dură. Associated Press anunta că un cetătean chinez care a fraudat electronic o bancă cu 192.000 USD a fost condamnat si executat în 1993. Actul legislativ din China este Regulamentul privind conexiunile globale prin retele.

În Rusia există Decretul nr.334/1995 semnat de presedintele de atunci Eltîn, care cuprinde atributiile Agentiei Federale pentru Comunicatii si Informatii Guvernamentale. Există putină informatie referitoare la legislatia cu privire la Internet. Cazul unui cracker care a reusit să penetreze sistemul bancar CityBank, prin care si-a însusit sume de bani, partial recuperati, arestat la Londra si pentru care a fost făcută cerere de extradare în SUA.

În Comunitatea Europeană, tratamentul acordat activitătilor de cracking este oarecum diferit de cel din SUA. Într-un raport al Consiliului Europei au fost făcute următoarea propunere: "în vederea convergentei tehnologiei informatiei si a telecomunicatiilor, legea referitoare la supravegherea tehnică în scopul investigatiei delictelor, cum ar fi interceptarea telecomunicatiilor, trebuie revăzută si amendată, acolo unde este necesar, pentru a asigura aplicabilitatea sa. Legea trebuie să permită autoritătilor de investigare să

profite de toate măsurile tehnice necesare si să permită colectarea traficului pentru investigarea delictelor".

Toate tările Uniunii Europene au devenit sensibile la problema delictelor cu calculatorul. Marea Britanie a adoptat în 1990 legea privind folosirea necorespunzatoare a calculatoarelor (Computer Misuse Act). Se citează un caz de condamnare a unui autor de virusi electronici. Se subliniază că politia engleză a raportat un număr redus de cazuri din cauză că firmele prejudiciate nu prea doresc să-si facă publice pagubele datorate de compromiterea retelelor proprii.

Legislatiile privind calculatoarele sunt confruntate cu situatii de acces neautorizat de pe tot globul. În toate statele si jurisdictiile, tendinta actuală este protejarea datelor, existând initiative legislative în Elvetia, Marea Britanie si SUA. Aproape toate legile noi care apar contin clauze referitoare la protectia datelor.

Alte aspecte privind legislatia se referă la decenta în comunicatii, existând o initiativă legislativă în statul Pennsylvania (Communications Decency Act) care nu a fost adoptată. Se aplică însă alte prevederi legale care reglementează modurile de exprimare (Fighting Word Doctrine - Doctrina cuvintelor injurioase). De exemplu, în 1995 un fost student a fost acuzat de instigare la ură în cyberspatiu pentru că a trimis un mesaj electronic de amenintare către 60 de studenti.

Legislatia în domeniul utilizării Internetului pentru stoparea actiunilor care aduc prejudicii persoanelor si institutiilor. Se asociază această retea de interes public cu o autostradă (informationalã), în care participantii la trafic trebuie să respecte anumite norme, în caz contrar riscă o amendă sau închisoare functie de gravitatea abaterii de la norma si de pagubele produse.

Există si un standard international, adoptat de mai multe tări, care cuprinde o parte explicativă si o parte cu prevederi si recomandări pentru asigurarea securitătii informatiei. Acesta a apărut în anul 1999 si se numeste BS 7799.

România nu beneficiază la această oră decât de o singură lege, si anume, Legea nr.8/1996 cu privire la protectia drepturilor de autor si conexe, cunoscută si sub numele de legea copyrightului. Aceasta vizează aspecte privind pirateria software, dar până la această oră nu se cunosc mai mult decât câteva cazuri în care legea a fost aplicată, desi tara noastră detine un loc de frunte la nivel mondial în acest domeniu al infractionalitătii.

De curând autoritătile guvernamentale din România au elaborat două proiecte de lege privind semnătura digitală si comertul electronic. Inspirate din directivele Uniunii Europene, aceste legi ar putea să la o "economie mai competitivă si mai eficientă", asa cum declară o persoană autorizată din guvern. Se prea poate să fie asa si aceste legi sunt asteptate de multă vreme dar... unde sunt legile împotriva infractionalitătii pe calculator? Cele câteva care există sau sunt pe cale să apară sunt "originale", continând chiar si unele ambiguităti si neputând fi aplicate cu eficientă, iar "inspiratia" lor de natură europeană aproape că nu se vede.

Sfaturi privind securitatea informatiei

Sfaturi pentru alegerea parolei

Cei care comit fraude informatice stiu bine cã, cei mai multi îsi aleg parolele pe baza unor date strict legate de persoana lor, precum: data de nastere, poreclele, numele celor apropiati sau cuvinte usor de memorat ca parolã. De multe ori acest mecanism de protectie prin parolã nici nu este folosit.

Nu insistãm aici asupra necesitãtii utilizãrii parolei. Considerãm cã aceastã necesitate a fost deja bine întelesã. Însã câteva sfaturi pentru alegerea unei parole considerãm cã n-ar strica. Asadar, iatã-le:

- Alegeti o parolã la întâmplare, astfel încât nimeni sã nu poatã sã facã vreo legãturã între persoana dvs. si cuvântul ales.

- Deschideti la întâmplare o carte opriti-vã asupra unui cuvânt care vi se pare cel mai potrivit ca fiind nelegat de persoana dvs. Este indicat ca acestui cuvânt sã-i adãugati, acolo unde credeti cã-i mai usor de retinut, un caracter special

- Este de preferat sã retineti parola, sã nu o notati nicãieri unde ar putea avea acces si altcineva.

- Dacã totusi considerati cã parola este un cuvânt greu de retinut si existã posibilitatea de a-l uita,

este indicat să îl notati undeva, într-un loc în care să nu ajungă cineva cu usurintă.

- Dacă scrieti parola pe ceva, o idee bună ar fi aceea să o scrieti într-un mod ciudat, care să nu sugere că este vorba de o parolă

- Un sfat mult mai bun ar fi să inventati un sistem propriu pe care să-l puteti folosi cu usurintă pentru a schimba des parola, fără să existe riscul de a o uita. De exemplu, din "LeonardoDaVinci" folositi la fiecare trei zile câte cinci litere consecutive, într-o ordine pe care o stiti numai dvs., eventual adăugându-i si un alt caracter special (cifră, semn de punctuatie etc.).

Nu uitati: Criptarea este singura care asigură confidentialitatea.

Sfaturi pentru verificarea securitătii

1. La adresa www.microsoft.com puteti găsi în mod regulat pentru cele mai noi update-uri de securitate
2. Nu folositi componenta de "File and Print Sharing" de la Microsoft Networks. Cel mai bine ar fi să o stergeti.
3. Este indicat să utilizati cele mai bune si actualizate programe de antivirusi pentru a bloca programele de tip "cal troian".
4. Considerati fisierele atasate la mesajele de e-mail ca fiind nesigure si tratati-le ca atare.
5. Instalati programe firewall personale. Cele mai indicate în acest moment sunt:
   a) BlackICE Defender pentru utilizatori care nu doresc să devină experti în securitate
   b) ZoneAlarm pentru cei care vor să stie toate detaliile despre conexiunea lor de Internet.

6. O sigurantã maximã, pentru cazul în care aveti o conexiune permanentã la Internet, este oferitã pur si simplu prin oprirea calculatorului atunci când nu mai aveti treabã cu el.

Cãi de apãrare împotriva atacurilor

Asa cum era de asteptat, marea diversitate a cãilor posibile de atac a impus dezvoltarea unei diversitãti de cãi de apãrare. Cele mai importante si cunoscute cãi de apãrare împotriva atacurilor sunt:

1. CLI-Calling Line Identification - permite deschiderea conexiunii prin ISDN pe baza numãrului apelantului.
2. ISDN Call-back - la sosirea unui apel pe ISDN se respinge conexiunea, fãrã deschiderea canalului de comunicatie (rezultând reducerea costurilor) si sunarea la numãrul ISDN al apelantului.
3. PPP Call-back - la sosirea unui apel pe ISDN sau dial-up, se deschide conexiunea, se autentificã prin PPP utilizatorul, dupã care se închide canalul de comunicatie si se sunã înapoi apelantul.
4. PAP - Password Authentication Protocol - este un protocol de identificare prin combinatia utilizator/parolã.
5. CHAP - Challenge Handshake Authentication Protocol - este similar cu protocolul PAP, însã trimiterea informatiilor de autentificare se face criptat.
6. RADIUS - permite validarea utilizatorilor sau sesiunilor de comunicatie, utilizând o bazã de date cu reguli bine stabilite (standardizat).

7. Firewall - este o solutie de protectie împotriva accesului neautorizat în retele conectate permanent la Internet.

8. Secure Shell Remote Management - permite obtinerea unei sesiuni criptate pentru administrarea sistemelor de la distantã.

9. VPN criptate - se utilizeazã Internetul ca suport de transport pentru transferul de date, sesiunile de comunicatie fiind autentificate, criptate. Se asigurã integritatea informatiilor transferate (DES, 3DES, Ipsec, ISAKMP/IKE).

Utilizarea Firewall

Asa cum am mai precizat, un firewall este o componentã sau un set de componente care restrictioneazã accesul între o retea protejatã si Internet sau alte seturi de retele.

Trebuie sã stim cã un firewall nu este o solutie pentru toate problemele de securitate. Totusi, el reprezintã o "primã linie" de apãrare împotriva atacurilor iar utilizarea ei trebuie tratatã cu seriozitate. O aplicare superficialã a unui firewall poate fi mai degrabã dãunãtoare decât folositoare. De aceea, cunoasterea pânã la cele mai mici detalii chiar a acestui instrument este foarte importantã.

Un sistem firewall reprezintã o combinatie de solutii hardware si software destinatã conectãrii în sigurantã la retele partajate de date, precum Internetul. El permite sau blocheazã, dupã caz, accesul, pe baza politicilor si regulilor, urmãrind tot timpul evenimentele care apar la interfata cu reteaua publicã.

Există la această oră trei tehnologii cunoscute, conform clasificării National Computer Security Association, care nu se exclud reciproc. Le prezentăm pe scurt în continuare:

1. Packet Filtering Firewall - functionează pe baza informatiilor continute în header-ele unitătilor de date de nivel 3 sau 4 (Network and Transport Layer) ce înseamnă să traverseze o interfată a routerului, constând în aplicarea de filtre pe baza unor reguli (filtre statice):

a) adresa sursă si/sau destinatie,
b) tipul protocolului (TCP, ICMP, UDP),
c) numărul portului sursă si/sau destinatie.

Avantaje: este simplu si usor de realizat, nu este mare consumator de resurse.

Dezavantaje: se bazează numai pe informatii de nivel 3 si 4 (nivel retea si transport), porturile TCP si UDP rămânând deschise accesului neautorizat.

3. Application Gateway Firewall (proxy servers) - conexiunile între două retele sunt realizate prin intermediul unor programe specifice (proxy servers). Acestea sunt specifice pentru fiecare aplicatie sau protocol, orice alt tip de trafic fiind refuzat.

Avantaje: oferă sigurantă.

Dezavantaje: necesită servere relativ puternice, iar programele necesare sunt destul de scumpe.

4. Stateful Inspection Firewall (dynamic packet Filtering Firewalls) - contine un modul care inspectează informatiile continute în pachet până la nivelul aplicatie pentru a se convinge că aplicatia se comportă cum este normal, datele sunt "verificate" nu "procesate" ca în cazul application gateways. Pachetele care sosesc sunt verificate pentru a se stabili legătura cu pachetele

precedente prin intermediul stării sesiunii. Când se detectează o deviere de la starea sesiunii, firewall-ul blochează restul sesiunii. Porturile de comunicatie sunt deschise si închise pe baza unor politici.

Avantaje: se monitorizează continuu starea fluxurilor de date, reactionând imediat la orice încercare de interceptare/modificare a acestora, filtrările dinamice se bazează pe politici si reguli definite, este transparent utilizatorului, fiind usor de adaptat la noile aplicatii Internet, fără resurse excesive.

Dezavantaje: solutia nu este aplicată decât la putini producători de routere.

Lista de programe Firewall

Nume	Adresa Web	Pret USD
Aladdin Knowledge Systems Esafe Desktop 2.2	www.eAladdin.com/esafe	gratuit
McAfee.com Personal Firewall	www.mcafee.com	40
Network ICE BlackICE Defender !.9	www.networkice.com	40
Sybergen Networks SecureDesktop2.1	www.sybergen.com/products	30
Symantec Norton PersonalFirewall2000	www.symantec.com	50
Zone Labs ZoneAlarm 2.1	www.zonelabs.com	gratuit
Digital Robotics Internet Firewall 2000		40
Delta Design NetCommando 2000		30
Plasmatek Software ProtectX 3 Standard Edition		25
Tiny Software Tiny Personal Firewall		29

Protectie împotriva atacurilor DoS

Dintre formele de atac cunoscute, cea mai "spectaculoasă" prin efect este Denial of Service (DoS). Efectul acesteia constă în blocarea serviciilor existente pe computerul respectiv. Mai precis, este o încercare de a bloca accesul la calculator a acelora care aveau acest drept, adică a persoanelor autorizate. Realizarea acestui

scop se face, de regulã, prin schimbarea parametrilor sau configuratiei sistemului sau, uneori, prin instalarea unui program strãin care are ca scop generarea unui trafic foarte mare în sistemul atacat.

Atacurile de tip DoS sunt de multe tipuri. Ele sunt usor de replicat si aproape imposibil de prevenit. Motivul principal este structura Internetului si a protocoalelor sale care au fost proiectate pentru asigurarea livrării mesajelor bazatã pe încrederea reciprocã, fãrã a tine seamã de unele probleme de comunicatie si de faptul cã pot exista persoane care manifestã alte interese, care nu au nimic în comun cu cele ale creatorilor acestor sisteme.

Iatã câtiva pasi care trebuie fãcuti pentru protectia împotriva acestor tipuri de atacuri:

1. Protejarea serverelor, asigurarea cã serverele sunt impenetrabile, odatã cu o curãtenie "la sânge" printre fisierele necunoscute.
2. Ridicarea exigentelor fatã de furnizorii de servicii. Acestora li se va cere sã se conformeze unor standarde larg acceptate de eticã si performantã tehnicã.
3. Scoaterea în afara legii a pachetelor mãsluite. Nu existã absolut nici un motiv pentru a emite pachete care sã continã în header decât propria adresã de IP. Pachetele mãsluite nu ar trebui sã pãrãseascã niciodatã routerele furnizorilor de Internet. Este vorba practic de o mânã de sisteme de operare si de câtiva mari producãtori de routere, desi implementarea unor sisteme de filtrare a traficului ar fi o muncã uriasã si lipsitã de eficientã. Printr-o combinatie de mecanisme de criptare si de servere specializate se poate merge oriunde sub protectia totalã a anonimatului si se pot face cumpãrãturi electronice în deplinã sigurantã.

4. Autentificarea generalã.. Internetul este un ocean urias de mesaje, care pot fi citite de oricine înainte de a ajunge la destinatie. Fiecare mesaj ar trebui sã aibã o autentificare. Prin aceasta se asigurã ca site-urile tintã sã dispunã de un mecanism simplu si eficient de protectie împotriva atacurilor. Astfel, se va putea mãri si gradul de confidentialitate a informatiei, deoarece, un astfel de furnizor va putea sã verifice usor cã un pachet anume provine într-adevãr de la un client al sãu, chiar dacã nu va putea spune cu precizie care este acel client.

5. Interzicerea scanner-elor. Pe log-urile serverelor pot fi vãzute numeroase ping-uri si încercãri înregistrate în ele. Nici unul dintre acestea nu face parte din traficul normal al retelei. Toate acestea pot fi stopate de furnizori prin identificarea unor comportamente tipice ale programelor de scanare, a adreselor si a porturilor.

Sfaturi pentru protejarea retelei

Diversi analisti si experti în probleme de securitate, precum si directori de corporatii sau agenti ai Serviciului Secret SUA, sugereazã urmãtoarele sfaturi pentru protectia retelelor:

1. Asigurati-vã cã nici o persoanã nu controleazã sistemul de la un capãt la celãlalt.
2. Cereti fiecãrui persoane sã se conecteze în retea folosind parola proprie.
3. Atribuiti drepturile de supervizare unui grup mai mare de persoane.
4. Executati salvãri de sigurantã (backup) în fiecare sãptãmânã.

5. Realizati un sistem strict pentru accesul la benzile magnetice.

6. Păstrati întotdeauna în altă parte o copie a salvărilor se sigurantă de pe benzile magnetice.

7. Efectuati salvări de sigurantă atât pentru desktop-uri si laptop-uri, cât si pentru servere.

8. Rotiti benzile magnetice pentru salvările de sigurantă, nu folositi una si aceeasi bandă de mai multe ori la rând.

9. Păstrati serverele în locuri sigure.

10. Fiti la zi cu versiunile de software.

11. Utilizati un software de detectie a intruziunilor nedorite, care să vă alerteze în cazul unei lovituri.

12. Asigurati-vă că nu au existat două perechi de ochi care să vadă codul înainte să fie introdus în sistem.

13. Trebuie să aveti un departament pentru garantarea securitătii informatiei (cel putin o persoană si apoi câte una în plus pentru fiecare o mie de angajati), separat de departamentul de IT si care să raporteze direct către responsabilul pentru transmiterea informatiei.

14. Cheltuiti cel putin 3-5% din bugetul de IS pe asigurarea securitătii informatiei. Instruiti personalul care asigură securitatea informatiei pentru a fi în măsură să detecteze angajatul care a fost perturbat sau nemultumit de ceva, mai ales dacă acest angajat detine si o functie critică privind regimul informatiilor confidentiale de firmă.

15. Întăriti securitatea pe parcursul unor evenimente mai deosebite, cum sunt fuziunile sau reducerile de personal, care i-ar putea deranja pe unii angajati si i-ar determina să aibă un comportament neloial fată de companie.

16. Monitorizati reteaua - setati un program software care să vă alerteze atunci când o persoană lucrează în altă parte decât în biroul său sau în afara programului general.

17. Scanati mesajele electronice pentru a vedea ceea ce iese din companie, verificati de două ori benzile de backup si desemnati pe altcineva să facă salvările curente dacă persoana luată în vizor este chiar cea care se ocupa anterior, în mod curent.

18. Prevedeti în contractul individual cu fiecare angajat reguli si sanctiuni.

19. Fiti siguri că persoanele cu sarcini critice de IS sunt asigurate.

Concedierea unui angajat important precum administratorul de sistem trebuie să vă îngrijoreze si să vă determine să luati anumite măsuri speciale. Iată cam care ar fi acestea:

1. Modificati parola fiecărui angajat, astfel încât fostul administrator să nu mai poată pătrunde în sistem.

2. Verificati că benzile cu salvările de siguranță sunt chiar acolo unde le este locul, asigurati-vă că informatiile au fost salvate corect si că benzile functionează corect. Faceti o nouă salvare de siguranță.

3. Încuiati toate locurile în care cel concediat avea acces toată ziua.

4. Căutati un alt administrator care să fie gata să preia responsabilitătile predecesorului său.

5. Intrati în sistem si verificati numele de utilizatori si parolele pentru a observa orice neregulă sau lucru neobisnuit.

6. Fiti sigur că orice acces în retea se asociază cu o parolă.

7. Protejati accesul fizic la oricare din serverele de fisiere, de aplicatii sau de e-mail.

8. Verificati "usile din spate" ale sistemului, cum este cazul cu Back Orifice din Windows NT.

9. Asigurati-vã cã nu exista nici un element vulnerabil care sã nu fi fost îndreptat - administratorul ar fi putut lãsa unele nise în sistem, astfel încât sã poatã intra fraudulos.

10. Îmbunãtãtiti-vã sistemul de detectie a intruziunilor.

11. Setati software-ul pentru a vã avertiza noul administrator în cazul unor anomalii în sistem, cum ar fi modificarea fisierelor.

Partea a V-a

VIITORUL INFORMATIC

Războiul cibernetic

Războiul cibernetic, cunoscut în literatura de specialitate sub numele de *cyberwar*, are ca scop penetrarea, distrugerea sau degradarea sistemelor informationale si a băncilor de date ale unui inamic. Aceasta înseamnă slăbirea puterii de luptă a unui dusman, prin toate mijloacele informatice posibile care pot conduce la “balansarea cântarului puterii de partea ta...", asa cum afirmă analistii de la RAND.

În realizarea acestor obiective se folosesc tehnologii dintre cele mai diverse pentru intreprinderea unor actiuni precum:

- colectarea de date,
- comunicatii tactice,
- identificare de tipul "prieten sau dusman",
- directionarea armelor "inteligente",
- bruierea comunicatiilor inamicului,
- "orbirea" sistemelor sale de ghidaj,
- supraaglomerarea băncilor sale de date si a sistemelor de receptie electronică etc.

Cyberwar poate avea implicatii directe sau indirecte, în dimensiunea strict militară a conducerii operatiunilor, pentru integrarea unor domenii speciale precum cel psihologic si cel politic.

De asemenea, cyberwar poate fi aplicat în diverse situatii, cum ar fi:

- conflicte de intensitate mare sau micã,
- mediile conventionale sau non-conventionale,
- scopuri ofensive sau defensive.

Tintele unui Cyberwar sunt, asa cum le preciza Michael Wilson, membru al grupului de studii NEMESIS în lucrarea sa “The Precipice Problem: A Guide to the Destabilization of Western Civilization”, sunt:

. **comunicatiile** – pot fi utilizate pentru a induce panicã si teroare prin întreruperea functionalitãtii mijloacelor conventionale de comunicare, a televiziunilor si radiourilor, întrucât aceste sisteme au devenit complet dependente de conexiunile la sateliti, iar securitatea acestora este foarte slabã. Comunicatiile telefonice sunt tinte relativ usor de atins, alãturi de ele fiind transcodoarele cu microunde sau chiar satelitii, care pot fi distrusi doar prin reprogramarea motoarelor de pozitionare ce sunt controlate de la sol. Pot fi întrerupte obiective critice cum ar fi centralele telefonice de urgentã, serviciile medicale, ambulantele, pompierii, serviciile politiei, alarmele de orice fel conectate la sisteme de supraveghere centralizate etc. Comunicatiile guvernamentale sunt tinte preferate, mai ales la nivelul infiltrãrilor în bazele de date si al unor eventuale campanii de comenzi contradictorii care sã provoace autoblocarea sistemelor informationale. Acest lucru se poate obtine fie prin introducerea unor comenzi de operare precise, fie prin plasarea unui virus care sã actioneze în trepte, spre exemplu, dupã integrarea unui mesaj parvenit prin e-mail în baza operationalã de date. Existã laboratoare militare care au primit sarcina sã elaboreze astfel de virusi care nu actioneazã decât în conditii speciale prestabilite.

Câtorva laboratoare superspecializate din Sillicon Valley au si primit comanda de a realiza unele programe care să permită, selectiv, distrugerea unor arme care folosesc software american, prevenind astfel, în extremis, folosirea intentionată a unei "găuri negre" de către specialistii părtii adverse.

. **centralele energetice** – sistemele de distributie a energiei electrice si cele de supraveghere constituie obiective strategice si sunt tinte relativ usor de atins.

. **transport-logisticã** – majoritatea sistemelor moderne de transport sunt dirijate prin sisteme esentiale de control al traficului, iar acestea sunt complet dependente de computere. Din acest motiv sunt foarte usor de paralizat. De exemplu, sistemele de transport aerian, ca si transporturile fluviale, terestre sau feroviare. Unele din ele pot fi anihilate prin intermediul bazelor lor de date de coordonare si programare.

. **sistemele financiare** – pot fi tintele cele mai evidente prin retelele de transfer financiar, inclusiv băncile locale si toate noile metode de acces la fonduri. De asemenea, sistemele de credit, inclusiv cărtile sau oficiile de credit, pot constitui tinte ale unui cyberwar. Se apreciază că, cu putin ajutor din partea sistemelor financiare aflate în functiune, este posibil să poat? fi distruse concomitent piata de valori si cea financiară a lumii doar într-un interval de câteva minute.

. **serviciile sociale** – cu doar putine instrumente speciale se poate introduce haosul în serviciile sociale, prin simpla distrugere sau virusare a bazei de date pentru plata salariilor, a pensiilor si alocatiilor etc.

În doctrina US Air Force, în care există foarte multe definitii si analize, întâlnim si o definitie a războiului informational: “Războiul informational reprezintă orice actiune pentru a împiedica, exploata, corupe sau distruge informatia inamicului si functiile sale, protejând pe cele proprii împotriva unor asemenea actiuni si exploatând propria informatie asupra operatiunilor militare".

Deoarece spărgătorii de coduri cunosc suficient de bine subtilitătile pătrunderii prin efractie, adică pur si simplu prin “ocolirea” codurilor de protectie ale sistemelor de calculatoare sau bazelor de date ale adversarului, ei pot juca un rol esential în pregătirea unor operatiuni de cyberwar. Numeroase exemple, o parte din ele fiind deja prezentate în acest manual, demonstrează aceste "calităti" incontestabile ale hackerilor.

Distrugerile provocate pe scară largă de spărgătorii de coduri chinezi asupra site-urilor Departamentului afacerilor interne si al energiei din SUA, dar si “preluarea” site-ului ambasadei SUA din Beijing demonstrează, nu pentru prima oară, că războiul informational există si se poartă deja în zonele care comportă un risc înalt pentru securitatea mondială.

În cazurile prezentate nu este vorba, asa cum uneori se încearcă a se acredita ideea, că avem de-a face cu actele vreunor adolescenti geniali si rebeli, că sunt doar actiuni izolate care nu trebuie luate în serios. Majoritatea exemplelor cunoscute din acest domeniu dovedesc faptul că războiul informational este o realitate cu care ar trebui să încercăm să ne obisnuim. Avem de-a face, desigur, cu actiuni care pot produce o îngrijorare, atât în plan militar, cât si în rândul responsabililor cu securitatea sistemelor informationale. Astfel de exemple arată gradul ridicat de risc pe care îl presupune în acest moment dependenta

extremã a sistemelor de control si comandã fatã de structurile unor super-calculatoare.

Unii însã mai considerã cã "povestile si miturile despre rãzboiul informational si despre securitatea computerelor – echivalentul modern al povestilor cu stafii – contamineazã acum totul, de la relatãrile din ziare pânã la rapoartele oficiale. Cu toate cã mijloacele de informare în masã sunt pline de povesti înspãimântãtoare despre site-uri web penetrate de hackeri si spargerea codurilor de securitate a retelelor companiilor publice sau private, scenariile amenintãtoare au rãmas pânã acum doar simple scenarii". Aceasta este pãrerea lui George Smith publicatã într-un articol la sfârsitul anului trecut în prestigioasa publicatie americanã “Issues in science and technology”. Argumentatia sa se bazeazã pe realitatea unor provocãri lansate, în joacã, de unii indivizi sau unele companii ca pe niste glume.

Existã însã multe alte argumente care sustin exact contrariul. Unul din ele este un raport publicat chiar de Departamentul Apãrãrii din SUA si redactat de “Defence Science Board Summer Study Task Force on Information Arhitecture for the Battelfield”. Acesta sustine: “SUA se aflã acum sub un atac ce tine de rãzboiul informational, declansat de adversari diversi, începând de la hackerul adolescent pânã la autorul unor penetrãri pe scarã mare, foarte sofisticate, în sistemele de telecomunicatii si de computere”.

Unele fapte extrem de grave au fost reunite într-un nou concept OOTW (Operations Other Than War), adicã operatiuni care nu apartin rãzboiului. Acestea au fost grupate în operatiuni care pot comporta douã dimensiuni: una de naturã militarã iar cealaltã non-militarã.

Dimensiunea militarã cuprinde trei tipuri de noi misiuni:

a) contracararea informationalã
b) atacurile asupra zonei de comandã si control

c) informatiile în domeniul culegerii de informatii.

Operatiunile de contracarare informationalã sunt destinate controlului informatiei, mentinerii accesului la informatie si securizarea integritãtii propriilor sisteme de informatii, în acelasi timp interzicând sau deteriorând accesul inamicului la informatii. Ele pot comporta atât aspecte defensive cât si aspecte ofensive.

Contracararea informationalã împiedicã intrarea adversarului pe domeniul informational prin mijloace specifice precum: atacul fizic, lansarea de tinte false, operatiuni psihologice, atacul informational si rãzboiul electronic.

Dezvoltarea de noi pârghii informationale pentru cresterea eficientei totale a fortelor armate este un alt tip de operatiune din rãzboiul informational. Aceasta se concretizeazã prin intermediul unor operatiuni specifice, care includ supravegherea, recunoasterea, identificarea de luptã, datele despre vreme, navigatie, spionaj, controlul comunicatiilor si centrelor de comandã.

Dimensiunea non-militarã cuprinde operatiuni care nu apartin rãzboiului. Acest tip de operatiuni reprezintã, de fapt, noutãtile care survin cu adevãrat pentru schimbarea rãzboiului traditional. Aici sunt incluse posibilitãtile de a cenzura si difuza propaganda purã pe

canalele de informatii mondiale, precum CNN sau BBC, sau servicii de tip CompuServe sau Prodigy.

Una din dimensiunile nontraditionale este definitã de unii analisti de la RAND cu numele de netwar, termen care se referã la posibilitatea unui conflict extins bazat pe folosirea informatiilor între natiuni sau între societãti diferite. Scopul unui netwar este acela de a încerca deteriorarea, întreruperea sau modificarea a ceea ce populatia-tintã stie sau crede cã stie despre sine si despre lumea înconjurãtoare. El poate fi focalizat asupra elitelor sau asupra opiniei publice, sau chiar asupra amândurora si poate implica o serie de campanii de propagandã sau psihologice, subversiuni culturale sau psihologice, transmiteri de informatii false sau infiltrarea de persoane în structurile presei locale, infiltrarea unor retele de computere si a bazelor de date, precum si eforturile de promovare a miscãrilor disidente sau de opozitie, folosind resursele specifice ale retelelor de computere.

La aceastã orã existã si sunt deja operationale manualele de infiltrare în sistemele informationale precum si tehnicile de propagandã si de rãzboi psihologic în care prima linie este mass-media din tara-tintã. Asadar, nu avem de-a face cu o simplã teorie seducãtoare, ci cu sisteme viabile de actiune concretã.

Realitatea virtualã

Realitatea virtualã (VR - Virtual Reality) reprezintã un sistem de calcul care poate da utilizatorului iluzia unei lumi generate pe calculator si a posibilitãtii de a cãlãtori în voie prin aceastã lume.

În realitatea virtualã utilizatorul poartã o pereche de ochelari speciali are afiseazã o imagine stereoscopicã si o mãnusã cu senzori, care îi permite anipularea "obiectelor" în mediul virtual.

Sistemele de realitate virtuala au fost inspirate de mai multã vreme de simulatoarele de zbor. Ele merg mult mai departe, prin introducerea utilizatorului într-o lume generatã pe calculator. Gama de aplicatii potentiale include, de exemplu, arhitectura, unde sistemele VR permit arhitectilor sã prezinte clientilor parcurgerea tridimensionalã VR a structurilor propuse. Si medicii pot sã încerce noi tehnici chirurgicale pe pacienti simulati, în trei dimensiuni.

Un sistem secund de realitate virtualã (second-person virtual reality) este un sistem de realitate virtualã care nu încearcã sã atragã utilizatorul într-o lume generatã pe un calculator cu ajutorul ochelarilor speciali si al mãnusilor; în schimb, acesta oferã utilizatorului un ecran video cu o foarte bunã descriere si o cabinã de pilot cu comenzi de navigatie, cum sunt cele din programele simulatoare.

Bucla de reactie prin electrocutare (electrocutaneous feedback) este o metodã primitivã de a furniza o buclã de reactie tactilã în sistemele de realitate virtualã prin administrarea unui soc de micã tensiune în

pielea utilizatorului. Acesta simte o usoarã furnicãturã. Prin variatia tensiunii electrice si a frecventei curentului se produc variatii în aceastã senzatie pe care utilizatorul o poate distinge.

Stereoscopia este o tehnolgie care prezintã douã imagini luate din perspective usor diferite, care, atunci când sunt vizualizate împreunã cu ajutorul unui stereoscop, creazã o iluzie profundã de spatiu tridimensional. Aparatele de vizualizare stereoscopicã erau foarte cunoscute în secolul trecut si tehnologia existã si astãzi, fiind unul dintre fundamentele realitãtii virtuale.

HMD (Head-Mounted Display) este un set stereoscopic de ochelari speciali ce dau senzatia de spatiu tridimensional. Afisajele montate pe ochelari sunt parte integrantã a sistemelor VR, care permit utilizatorilor sã se simtã ca si când ar explora o lume realã, care de fapt a fost creatã cu un sistem de calcul.

Mãnusa senzorialã (sensor glove) în sistemele VR, este o interfatã de forma unei mãnusi care permite utilizatorului sã manipuleze si sã deplaseze obiecte virtuale într-un mediu VR.

Realitatea virtualã a captat rapid imaginatia publicului, sprijinit de imaginile teribilului cercetãtor Jaron Lanier în domeniul VR, de la VPL Research, Inc.; de descrierea realitãtii virtuale ca fiind "LSD electronic" datã de chitaristul Jerry Garcia de la formatia Grateful Dead; si de legãtura dintre lumile generate de sistemele VR si genul cyberspace de fictiune stiintificã.

Descrierile senzationale ale relatiilor sexuale bazate pe realitatea virtualã ti teledidonics (sex cu o persoanã aflatã la distantã mediat prin dispozitive VR conectate prin modem) au dus la incitarea interesului public.

Cele mai promitãtoare aplicatii VR se gãsesc totusi în domenii ca stingerea incendiilor si terapia prin radiatii.

Cel mai mare potential comercial al sistemelor VR se aflã fãrã îndoialã în domeniul distractiilor. Un exemplu: NEC Corporation experimenteaz? "un laborator virtual de schi", în care schiorii virtuali îsi pun ochelari de protectie, bete si schiuri virtuale. Programele laboratorului simulează pârtiile din toatã lumea. Un salon de schi virtual va fi inaugurat la Tokyo si în alte orase. Un avantaj major: vã puteti distruge doar limita de credit a contului din bancã.

Teledildonics este o aplicatie posibilã pentru viitor, de realitate virtualã si tehnologie a telecomunicatiilor, care ar putea permite ca douã persoane sã facã sex, chiar dacã sunt separate de distante mari. Tehnologia necesarã pentru teledildonics nu existã încã, dar laboratoarele de tehnicã înaltã lucrează la ea. Teledildonics ar avea nevoie de canale de comunicatie cu o lãtime de bandã incredibilã. Liniile de telefon de astãzi pot transmite pân? la 14.400 de biti de informatie pe secundã, dar teledildonics ar avea nevoie de aproape 3 miliarde. Totusi, expertii realitãtii virtuale considerã cã este posibil.

Teleprezenta (telepresence) este senzatia psihicã de a fi cufundat într-o realitate virtualã, care este suficient de persuasivã si de convingãtoare pentru a fi luatã drept realitate. Cei care vizitează punctul de atractie numit Star Tours din Disneyland trãiesc o experientã de tipul telepresence. În Star Tours, vã îmbarcati pe o navã - de fapt un vehicul care se deplasează pe un traseu, cu viteze mici, simulând curbe, rotiri, accelerări si frânări - si puteti vedea un film de mare rezolutie cu o cãlãtorie interstelarã, care este coordonatã perfect cu miscările

vehiculului. Rezultã o teleprezentã care va convinge cã vã deplasati cu viteze fantastice.

Comunitatea virtualã reprezintã un grup de oameni, care este posibil sã nu se fi întâlnit niciodatã, cu interese si preocupãri comune si care comunicã unii cu altii prin postã electronicã si prin grupurile de discutie. Cei care doresc sã fie membri ai unor astfel de comunitãti, simt nevoia sã-si gãseascã un loc si sã stabileascã legãturi emotionale profunde cu alti participanti, chiar dacã relatiile care apar sunt mediate de calculator si poate niciodatã nu vor implica o întrevedere fatã în fatã.

Un *echipament virtual* înseamnã simularea unui echipament de calculator sau a unui periferic, cum ar fi o unitate de hard-disk sau o imprimantã, care nu existã. Într-o retea localã, un calculator poate sã parã a avea un hard-disk enorm, care în realitate este pus la dispozitia statiei de lucru prin legãturile din retea la calculatorul server.

O *masinã virtualã* este, un spatiu de memorie protejat, creat de cãtre capacitãtile hardware ale procesorului. Fiecare masinã virtualã poate rula propriile programe, izolate complet de alte masini. Masinile virtuale pot avea acces fãrã conflicte si la tastaturã, imprimante si la alte dispozitive.

Masinile virtuale pot fi create de cãtre un calculator care are circuitele necesare si multã memorie cu acces aleatoriu (RAM).

Termenul de cyberspace (ciberspatiu) a fost introdus de William Gibson, în cartea sa Neuromancer din 1982, odatã cu crearea genului de literaturã stiintifico-fantasticã cyberpunk.

Ciberspatiul este un spatiu virtual creat de sistemele de calcul. O definitie a spatiului este "o întindere

tridimensionalã fãrã margini, în care apar obiecte si evenimente care au pozitii si directii relative". În secolul 20, sistemele de calcul creeazã un nou tip de spatiu cãruia i se potriveste aceastã definitie: ciberspatiu (termenul ciber se referã la calculatoare).

În realitatea virtualã ciberspatiul poate fi experimentat direct prin punerea unei cãsti care afiseazã o lume ce nu existã în realitate. Hoinãrind prin aceastã lume, puteti "apuca" obiecte, puteti trece dintr-o "camerã" în alta si puteti intreprinde alte actiuni ce par destul de reale persoanei ce poartã casca.

Ciberspatiul poate fi creat de sisteme de calcul mai putin sofisticate decât cele ce experimenteazã realitatea virtualã. Sustinãtorii postei electronice vor mãrturisi imediat cã posibilitatea de a comunica si cu alti utilizatori, aflati peste tot în lume, rupe barierele sociale si de distantã într-un mod plin de însufletire.

Cybersexul este o formã de erotism de la distantã, posibil printr-un forum de discutii pe un calculator, în timp real. Termenul este sinonim cu *compusex*. Pentru a simula un partener virtual, se transmite o fantezie sexualã favoritã sau se descrie în termeni însufletiti ceea ce ati face dacã persoana ar fi de fatã în realitate. Cybersexul are loc pe liniile de conversatie de pe sistemele de buletine informative pentru adulti, în care se schimbã mesaje cu o altã persoanã care este conectatã la acelasi sistem. Aceste linii de conversatie oferã sex formal - unul din motivele pentru care oamenii le apeleazã.

Ce ne mai oferă viitorul ?

Calculatoarele vor deveni mai umane iar programele mai inteligente

Puterea de calcul a crescut în ultimii ani cu o ratã uluitoare, iar noile tehnologii vor continua sã contribuie la pãstrarea aceluiasi ritm. Prin anul 1965, Gordon Moore, cofondator al companiei Intel, a prezis cã densitatea de tranzitoare dintr-un circuit integrat se va dubla anual. Legea lui Moore, asa cum este ea cunoscutã astãzi, a fost valabilã trei decenii la rând. Bucurându-se si în prezent de o deosebitã popularitate, pe baza ei se apreciazã cã va exista un miliard de tranzistoare într-un cip din anul 2011 sau poate chiar un curând, iar calculatoarele vor deveni mai puternice decât ne-am putea imagina. Dezvoltarea microprocesoarelor se va extinde pânã la limita barierelor fizice.

În viitorul apropiat conexiunile rapide în retea si Internetul se vor standardiza si vor influenta activitatea si calitatea vietii. Retelele vor fi mai rapide, vor fi pretutindeni fãrã sã fie vizibile, si ne vom putea conecta la ele de oriunde. Se vor îmbunãtãti protocoalele de comunicatie, se vor dezvolta retele WAN care vor lega eforturile industriale, guvernamentale si academice, va exploda piata portabilelor fãrã fir, a celularelor bazate pe tehnologii digitale etc.

Calculatoarele vor avea atribute umane precum posibilitatea de reactie la vorbire sau la instructiunile scrise si de a rãspunde la întrebãri cât mai natural. Se

apreciază că noile tehnologii vor permite interactionarea cu calculatoarele aproape ca si cum s-ar face cu o altă persoană. Practic, lucrul cu calculatorul va deveni cât mai natural. Interfata cu utilizatorul va suferi transformări care vor părea mult mai umane.

Procesarea în limbaj natural sau abilitatea de a răspunde la o întrebare formulată cu claritate va putea deveni tehnica fundamentală care va sta la baza calculatoarelor inteligente.

Există si în prezent unele site-uri care folosesc o interfată în limbaj natural (vezi Ask Jeeves, psihiatrul simulat Eliza, Red de la Neuromedia pentru service virtual, Klone Server Andrette, Social Inteligence Server de la NetSage etc.). Recunoasterea vocii este iarăsi un domeniu în plină dezvoltare (Jupiter-MIT pentru întelegerea vorbirii, unele aplicatii cartografice, un sistem care oferă informatii aviatice s.a.).

Si întelegerea emotiei este în atentia laboratoarelor de cercetare, pentru care se concep senzori psihologici atasati corpului si camere video de dimensiuni mici care înregistrează expresiile faciale si permit calculatoarelor să monitorizeze reactiile umane. Sunt în plină efervescentă de creatie masini care pot exprima emotie si proiecte precum Bruzard de la MIT, un personaj tridimensional interactiv cu fata de copil care foloseste expresii faciale pentru a răspunde la întrebări, sau Flow de la Microsoft Research care va permite să stati la calculator si să participati la o întâlnire virtuală.

În paralel cu realizarea unor calculatoare mai umane se dezvoltă si software-ul inteligent. Programul care pare că se gândeste pe sine va deveni în curând o realitate. Interfetele cu limbaj natural pot constitui un semn că softul e mai destept dar există multe alte zone în care el

devine mai uman. Un program de calculator va putea interpreta, de exemplu, un număr suficient de mare de tipuri de comenzi în limbaj natural. Este cazul să reamintim aici cazul celebrului program de sah Deep Blue care în 1997 l-a învins pe campionul mondial Garry Kasparov.

Software-ul va prelua si noua tehnologie a retelelor neuronale care constituie la această oră o tendintă majoră cu aplicatii în recunoasterea formelor, ce se bazează pe învătarea din experientă. Recunoasterea optică a caracterelor, recunosterea vorbirii si chiar recunosterea chipului uman poate fi atribuită în mare măsură retelelor neuronale.

Calculatorul va ajuta si doctorii în analiza stării pacientilor si îi va asista la crearea de noi retete si medicamente. De asemenea, retelele Bayesian vor continua să fie dezvoltate de Microsoft Research si se vor construi programe care gîndesc si reactionează asa cum o face si omul.

Internetul va deveni o imensă magazie de informatii iar Web-ul va fi curând capabil să anticipeze si să livreze informatia precisă de care avem nevoie. În viitor site-urile vor sti mai multe despre noi. Ele vor sti multe si despre propriul continut ca si despre cel al altor site-uri. Web-ul, care se bazează acum pe HTML, va fi refăcut cu XML, un metalimbaj proiectat pentru a lăsa mai usor grupurile să descrie cu tag-uri standard continutul oricărui tip de fisier.

Site-urile vor putea fi personalizate după gustul si preferintele noastre de informare. Ele vor arăta asa cum ne dorim, ba mai mult, ele ne pot sugera sau recomanda multe lucruri. Căutarea va fi îmbunătătită substantial, motoarele vor fi mai puternice si vor putea căuta nu

numai text ca acum ci si graficã, continut video, culori, forme si texturi de date-imagini etc.

În paralel se va dezvolta puternic fabricarea unor dispozitive care vor gândi. Procesoarele înglobate în diverse dispozitive se multiplicã uluitor de repede fãcând ca procesoarele PC-urilor sã fie simple pete în ecosistemul digital. În prezent vânzãrile cipurilor pentru PC-uri se exprimã în milioane de unitãti, pe când cele ale procesoarelor încorporate în diferite dispozitive în miliarde. Si în prezent proportia aceasta se va pãstra sau va fi adâncitã. Aparatele casnice pot deveni mai "inteligente". Sã dai drumul la masina de spãlat de la celular sau sã ordoni frigiderului cum sã-ti fie laptele poate fi un vis, dar nu pentru mult timp. Noile dispozitive pentru Internet pot fi dotate cu ecran sensibil la atingere, calendar, carte de adrese, e-mail, conexiune Internet, recunoasterea scrisului, apel vocal si rãspunsuri vocale.

Calculatorul va arãta, desigur, altfel. Cercetãtorii au creat deja un ecran color din opt plãci LCD bazate pe polimeri. Acesta se pliazã cât sã încapã în buzunar si, desfãcut o datã devine o tablã de scris, de douã ori o carte sau un browser Web, iar desfãcut complet devine destul de mare ca sã afiseze hãrti sau sã lucreze ca un ecran de PC.

Greoiul ecran CRT va fi înlocuit cu unul mic, luminos si de înaltã rezolutie, care poate fi luat oriunde. Se lucreazã la ecrane ultra-subtiri, constituite din milioane de bule de plastic închise într-un buzunar de ulei cu o folie de cauciuc (firma XEROX), la o tehnologie pentru masinile de tipãrit care citesc datele de pe documentele existente pe hârtie (DataGlyphs-XEROS), precum si la o cernealã (E Ink) care poate fi utilizatã la tipãrit având

proprietatea de a-si schimba culoarea sub influenta unui câmp electric.

Economia va fi pe Internet iar distractia va fi virtualã

Nici o afacere în afara Internet-ului, suna un slogan în urmã cu doar câtiva ani. Producãtorii de dispozitive mobile de acces la Internet prevãd o ascensiune puternicã a acestora în anii urmãtori. Clientii pot alege între un telefon mobil sau un notebook cu telefon incorporat. Lãrgirea portofoliului de servicii se bazeazã deocamdata pe protocolul WAP - Wirelees Automation Protocol.

Infrastructura de transmisie se îndreaptã cãtre marea performantã. Mãrirea considerabilã a lãtimii de bandã trimite cãtre legãturile prin satelit si cablurile din fibrã de sticlã care împânzesc tot mai mult globul. Legãturile radio oferã o alternativã mai ieftinã în cazul în care folosirea cablurilor subterane pentru utilizatorii finali este prea costisitoare sau este tehnic imposibilã. În viitor, utilizatorii vor putea sã aleagã între diferiti furnizori de servicii ca si între diferitele tipuri de infrastructuri de comunicare.

Internetul are potentialul de a revolutia relatiile de afaceri. În prezent, aproape toate informatiile necesare pentru realizarea unei tranzactii sunt disponibile pe Internet. Furnizorii si clienti angajati în comertul electronic depind de modul în care sunt realizate tranzactiile si de instrumentele de securitate. În plus, aplicatiile de comert electronic trebuie sã fie usor de utilizat. Industria de software se strãduieste sã ofere cele mai bune solutii. Un site Web nu mai este doar o simplã "fereastrã a unui magazin virtual" în care o companie îsiafiseazã produsele

si serviciile. Programe specializate permit clientului să-si configureze produsul dorit (un automobil, de exemplu). Verificări de asigurare a plauzibilitătii asigură selectarea doar a optiunilor compatibile. După configurarea automobilului, clientul are posibilitatea să vadă produsul finit din diverse unghiuri pe ecranul monitorului. Când este multumit, printr-un singur clic, utilizatorul poate intra în dialog cu furnizorul pentru a-i comunica doleantele sale.

Deaorece succesul în afaceri este în strânsă legătură cu gradul de satisfacere a cerintelor clientilor, centrelor de informare li se acordă din ce în ce mai multă importantă. Aproximativ 3 miliarde de telefoane si o jumătate de miliard de faxuri sunt instalate în întreaga lume. Centrele de informare trebuie să fie capabil să manipuleze o variatate de tipuri de mesaje (faxuri, apeluri telefonice, postă electronică). Răspunsul la această problemă este mesageria unificată. Practic, acest lucru înseamnă că toate mesajele primite sunt descifrate si prelucrate de un sistem integrat de calculatoare.

Din ce în ce mai multe servicii sunt directionate prin asa numitele retele inteligente. Lista aplicatiilor include gestiunea apelurilor, servicii de informare pentru clienti, servicii de fax, conferinte telefonice si video-conferinte.

Internetul functionează ca o retea universală care leagă furnizorii de componente, producătorii, distribuitorii si clientii. Prin definitie, Internetul trebuie să transporte diferite tipuri de date dintr-o gamă foarte variată de surse. Industria de software a dezvoltat instrumente sofisticate de translatare si integrare pentru a asigura că recipientii pot descifra si procesa aceste date pe sistemele proprii. De exemplu, mesajele Internet primite de un telefon WAP

mobil sunt prelucrate automat de un program de translatare incorporat.

Toate marile târguri internationale de tehnologie informaticã sunt supraaglomerate de furnizori de software de bazã si de aplicatie. Din ce în ce mai multe aplicatii sunt dezvoltate si destinate tehnologiilor bancare, proiectarea si productia asistate de calculator, solutii de management de intreprindere, de mobilitate în afaceri etc. Noi sisteme de operare, noi versiuni ale acestora din ce în ce mai performante sunt aruncate zilnic pe piatã.

Economia viitorului va fi mai globalã, electronicã si se va baza pe Internet. Internetul se dovedeste a fi atât de plin de succes copiind si îmbunãtãtind modul de a face cumpãrãturi si cãile de a face afaceri, încât în curând, mai repede decât orice previziune a oricãrui expert, economia pe Internet va constitui cea mai mare parte a infrastructurii economiei globale.

Exemple de economie pe Internet: priceline.com unde se specificã pretul pentru biletele de avion, licitatiile eBay, cu liste de aproape 2 milioane de pozitii, amazon.com, unde 8 milioane de oameni au cumpãrat cãrti si muzicã la pret redus, jocul la bursã online care gestioneazã în mod curent 400 de miliarde de dolari si operatiile bancare aferente, este livrarea de legume la usã via FedEX si livrarea prin postã a medicamentelor. Cei 180 de milioane de americani conectati la Web care vor cheltui online 41 de miliarde de dolari în 2002 (de la 7 miliarde cu numai un an în urmã) o vor face din ce în ce mai mult.

Distractia va deveni din ce în ce mai atractivã în mediile virtuale. Personajele digitale devin cu mult mai pline de viatã si atrag cu mult mai mult spre jocuri, filme si locuri de discutie decât atunci când erau doar

bidimensionale.

De când personajele au devenit mult mai umane, reprezentarea digitalã a actorilor joacã un rol de seamã în filmele hollywoodiene. Perifericele vor fi din ce în ce mai sofisticate: ochelarii stereoscopici 3-D si joystick-urile "force feedback", care stimuleazã diferite actiuni, casca stereoscopicã, mãnusa VR etc.

Selectia de filme creste exponential, jocurile devin mai vii, discutiile în direct devin mai realiste si mai fantastice pe PC.

Identitatea noastrã va fi digitalã

Chiar si identitatea noastrã va deveni una digitalã asa cum lumea va fi din ce în ce mai digitalã. Identitatea nu este altceva decât un amalgam de informatii personale, care creste constant si sunt stocate în bazele de date ale statului si ale municipalitãtii, spitalelor si centrelor medicale, companiilor de asigurãri, magazinelor, bãncilor si mai multor agentii guvernamentale decât ne putem închipui. În aceastã situatie numai o identitate digitalã, unicã, este salvarea. Ea va putea fi purtatã în permanentã la noi, încorporatã într-un cip, pentru a apela la toate serviciile si convenientele moderne.

Autentificarea personalã, desi simplã, este o problemã la care încã se mai lucreazã si se mai cautã solutii. Produsele de autentificare personalã pot fi perechi ID-parolã, jetoane cerere/rãspuns, cartele inteligente, dispozitive biometrice sau altele care asigurã un profil unic. Functiile biometrice se vor regãsi curând în

tastaturile si dispozitivele de indicare ale calculatoarelor, pe măsură ce se va începe productia de cipuri dedicate scanării amprentelor.

Viata privată înseamnă în era digitală abilitatea de a controla informatiile despre noi însine prin mijloace tehnice si legale. Biometrica poate măsura caracteristicile noastre unice precum amprentele. Atributele individuale ale fetei noastre sunt măsurate si în relatie una cu alta dau un model matematic complex digitizat. Fiecare iris sau retină au motive unice ce pot fi citite ca un cod de bare. Un cuvânt spus poate fi verificat prin telefon cu o înregistrare digitală pentru accesul la o bază de date. Geometria mâinii, schema vaselor de sânge ale bratului si harta porilor nostri pot fi folosite ca identificare unic?. Chiar gemenii identici au amprente diferite, dar si forma pumnului este unică.

Copii vor deveni mai inteligenti

Un studiu făcut de Digital Research în rândul a 615 familii americane si publicat în toamna anului 1999, a avut la baza chestionarului următoarele întrebări: 1) Contribuie calculatoarele la cresterea gradului de inteligentă al copiilor? 2) Ce abilităti dezvoltă folosirea calculatorului? 3) Devin copiii mai creativi folosind calculatorul? 4) Vă asistati sau supravegheati copiii în timp ce se află la calculator?

Răspunsurile par să fie încurajatoare. Calculatorul contribuie nu numai la cresterea abilităților în solutionarea problemelor, dar chiar si a celor de comunicare, îmbogătire a vocabularului sau ortografiei, îmbunătătirea creativitătii. Sondajul sustine că, prin utilizarea calculatoarelor, copiii devin mai inteligenti. Astfel, 68%

dintre cei chestionati apreciazã cã, copiii care folosesc un PC, devin mai inteligenti si numai 13% nu cred acest lucru. De asemenea, se apreciazã cã, dintre copiii care folosesc calculatoarele, 61% sunt mai creativi, 2% mai putin creativi, 25% nu devin deloc mai creativi iar 12% nu se pot pronunta. Majoritatea celor chestionati cred cã este foarte util sã poti asigura copiilor accesul la tehnologia modernã, pentru familiarizarea cu utilizarea calculatorului, lucru indispensabil în procesul educational precum si în desfãsurarea oricãrei activitãti. Altii sustin cã PC-ul prosteste mai mult decât ajutã la cresterea inteligentei.

Alte abilitãti pe care sondajul le apreciazã cã pot fi dezvoltate la copii prin utilizarea calculatorului sunt:

. 70% - rezolvarea problemelor
. 69% - citit
. 69% - matematicã
. 63% - limbaj/comunicare
. 63% - abilitãti tehnice
. 61% - corecturã
. 60% - cercetare
. 60% - vocabular.

Strategii românesti

. Nevoia de securitate a organizatiilor a crescut odatã cu trecerea la interconectarea calculatoarelor în retele locale, dar adevãrata explozie a avut loc dupã introducerea retelelor de intreprindere, Intranet-uri si Extranet-uri, conectarea acestora la Internet si trecerea la

informatizarea totalã a activitãtii, actiune care este cunoscutã sub numele de *e-business*.

. Insecuritatea în domeniul IT poate conduce într-o bunã mãsurã la pierderea intimitãtii persoanei, la frica de posibilele furturi ale datelor aflate în tranzit.

. Politica de securitate informaticã a unei institutii trebuie sã se subordoneze politicii de securitate generalã a acesteia. Nu se poate vorbi de securitatea informaticã înainte de a se examina nevoile si normele generale de securitate. Realizarea unei politici de securitate nu este o problemã simplã, dar nici una foarte complicatã. Un mic ghid de implementare în cinci pasi a unei astfel de politici este prezentat în continuare de cãtre un specialist al firmei Compaq:

1. Determinati ce anume doriti sã protejati (documente, disponibilitatea echipamentelor, imaginea firmei) .
2. Determinati împotriva cãror riscuri doriti sã vã apãrati.
3. Evaluati probabilitãtile si costurile asociate diferitelor riscuri si determinati un buget corespunz?tor pentru evitarea lor.
4. Alegeti si implementati mijloacele de protectie, folosindu-vã de bugetul stabilit la pasul anterior.
5. Reveniti la primul pas pentru a revizui periodic normele de securitate informaticã.

. Un intrus care reuseste sã "fure" identitatea electronicã a unui utilizator legitim poate produce multe daune înainte de a fi descoperit si eliminat din sistem Din acest motiv, autentificarea utilizatorilor reprezintã, de

multe ori, cel mai important element în asigurarea securitãtii sistemelor informatice.

. *E-economia* sau economia electronicã cunoaste trei atribute esentiale: viteza de rãspuns, disponibilitatea neîntreruptã si asigurarea securitãtii datelor.

. *Societatea Informationalã* reprezintã un obiectiv strategic al Guvernului României pe termen mediu si una din conditiile de preaderare la Uniunea Europeanã. Ea presupune o economie si o societate în care accesul, achizitia, stocarea, prelucrarea, transmisia, rãspândirea si utilizarea cunostintelor si a informatiei joacã un rol decisiv. Un asemenea obiectiv nu se poate atinge fãrã anumite schimbãri în administratie (e-government), în afaceri (comertul electronic), în educatie (educatia la distantã), în culturã (centre multimedia si biblioteci virtuale) si în maniera de a lucra (lucrul la distantã). Desigur, baza acestor transformãri se numeste o reprezintã utilizarea pe scarã largã a Internet-ului iar factorii implicati sunt infrastructura de comunicatii si aplicatii informatice.

. *E-government* înseamnã o guvernare electronicã, on-line, adicã accesul electronic la serviciile publice. Ea implicã definirea unor registre-nomenclatoare nationale, redefinirea fluxurilor administrative si interministeriale, implementarea infrastructurii de comunicatii voce-date, precum si dezvoltarea si implementarea aplicatiilor specifice administratiilor de stat.

. Normele de reglementare a domeniului tehnologiei informatiei vizeazã, din punctul de vedere al guvernului, urmãtoarele: semnãtura electronicã, protectia datelor personale, domeniile de tip .ro, servicii ISP si de transmisii de date, comertul electronic (e-comerce), standardele si listele de profesii si/sau domenii de

activitate si High Tech, registrele nationale (în special registrul populatiei), criptografie, plãti electronice s.a.

. Guvernul s-a gândit si la unele initiative antifraudã, practic fiind prevãzute actiuni care vor fi derulate în scopul asigurării securitãtii sistemelor, protectiei datelor personale si a prelucrării acestora, reducerii pirateriei software si prevenirii fraudelor prin intermediul calculatorului.

. Legea privind semnãtura electronicã, elaboratã de Ministerul Comunicatiilor si Tehnologiei Informatiei, este instrumentul prin care tranzactiile si transmisiile de date efectuate prin intermediul Internetului pot fi autentificate de cãtre pãrtile implicate. Semnãtura electronicã a unei persoane fizice sau juridice este direct legatã de identitatea acelei persoane, prin intermediul unui certificat eliberat de un furnizor de servicii de certificare. Furnizorii de certificate trebuie acreditati de cãtre o autoritate din domeniu, subordonatã MCTI. Acestia pot fi persoane fizice sau juridice române sau strãine si sunt supusi sanctiunilor pentru încãlcarea prevederilor legii, în cazul în care eliberează certificate false sau incomplete, dacã nu asigurã confidentialitatea datelor personale ale posesorului de certificat sau dacã nu operează modificări ale datelor dintr-un certificat, la cererea posesorului. Legea este primul pas spre dezvoltarea e-comerce si e-economie, conducând practic cãtre o economie mai competitivã si mai eficientã. Este o lege care asigurã securitatea transmiterii informatiei în Intranet si, mai ales, în Internet. Documentul trimis în acest mod, nu numai cã va purta amprenta unicã a expeditorului dar, lucru si mai important, va putea fi modificat numai lãsând urma celui ce a fãcut modificarea.

. Proiectul de lege privind comertul electronic, elaborat tot de MCTI, reprezintã un alt mare pas cãtre înaltele tehnologii ale Occidentului. El a apãrut, în mod logic, dupã cel privind semnãtura electronicã si a fost inspirat de modelul european, deschizând calea recunoasterii serviciilor ce pornesc din România cãtre Europa. Altfel spus, legea defineste mijloacele electronice, serviciile informationale si furnizorii acestor servicii, comunicarea comercialã si autoritãtile sau organele cu atributii de supraveghere si control pentru a oferi posibilitatea încheierii contractelor pe cale electronicã.

. *Cyber-Center*, un proiect propus de MCTI, reprezintã o retea de facultãti, studenti, persoane fizice, antreprenori, avocati si arhitecti de sisteme informatice, care lucreazã împreunã pentru a identifica si experimenta schimbãrile si oportunitãtile spatiului virtual - cyberspace. Altfel spus, dezvoltarea unor parcuri tehnologice pentru identificarea si experimentarea schimbãrilor si oportunitãtilor spatiului virtual si construirea, utilizarea si punerea la dispozitia publicului - în mod gratuit - a unui site Web pentru lecturi de specialitate si forumuri tehnice de discutii, precum si inovatia si dezvoltarea afacerilor si crearea si administrarea unei burse virtuale de proiecte în domeniul Comunicatiilor si Tehnologiei Informatiilor.

. Alte proiecte de viitor ale MCTI în domeniul tehnologiei informatiei:

- Accelerarea introducerii calculatoarelor si a accesului la Internet în unitãtile de învãtãmânt scolar si liceal,

- Infrastructura de comunicatii voce-date a Guvernului României,

- Servicii de informare electronicã pentru cetãteni - sistem national distribuit de informare electronicã,

- Centre multimedia pentru cetãteni în toate colectivitãtile locale cu peste 5000 locuitori,

- Biblioteca virtualã.

ANEXA

DICTIONAR

Administrator de retea (network administrator) - persoanã care rãspunde de întretinerea unei retele locale si care acordã asistentã utilizatorilor.

Aplicatie (aplication) - utilizarea unui calculator cu un anumit scop, cum ar fi scrierea unui roman, tipărirea unor note de platã sau amplasarea textului si a graficii pe un buletin informativ. Se foloseste deseori ca sinonim pentru termenele: software de aplicatie sau program de aplicatie.

Arhitecturã (architecture) - structura fizicã sau proiectul unui calculator si al componentelor sale, de la structura sa internã de functionare si circuitele specifice, pânã la programele ce îl fac sã functioneze. Termenul este folosit deseori pentru a descrie capacitatea internã a unui calculator de a trata datele.

Arhitecturã client/server (client/server architecture) - un tip de proiect pentru aplicatiile ce rulează într-o retea în care volumul de prelucrări de tip back-end, cum ar fi executarea unei căutări într-o bază de date, are loc pe un server. Prelucrările de tip front-end, care implică o comunicare cu utilizatorul, sunt tratate de aplicatii mai mici distribuite statiilor de lucru client.

Arhitectura retelei (network architecture) - set

complet de standarde de echipamente, programe si cablări pentru proiectul unei retele locale.

Arhivã (archive) - un fisier comprimat cu scopul de a avea o stocare eficientã din punct de vedere al spatiului ocupat si care contine unul sau mai multe fisiere.

Atac activ (active atack) - atac asupra unui sistem prin care se introduc informatii false sau se corup informatiile deja existente în sistem.

Atac pasiv (passive atack) - atac asupra unui sistem prin care se extrag informatii, dar nu se introduc si nici nu se stricã vreo informatie existentã.

Backup - salvare de sigurantã, o copie a programelor de aplicatie instalate sau a fisierelor de date create. Actiunea de copiere a fisierelor pe un alt disc.

Bazã de date (database) - o colectie de informatii corelate despre un subiect, organizate într-o modalitate utilã care oferã o bazã sau un fundament pentru procedurile de regãsire a informatiei, de apreciere si de luare de decizii.

Bibliotecã (library) - colectie de programe sau rutine, scrise într-un anumit limbaj de programare, pãstrate cu sistemul de operare si disponibile pentru scopuri de prelucrare.

Buffer - o unitate de memorie cu sarcina de a pãstra temporar informatii, destinate mai ales componentelor mai lente.

Bug - eroare de program, care determinã programul sau sistemul de calcul sã functioneze eronat, sã producã rezultate incorecte sau sã se blocheze. În traducere directã - parazit - a fost nãscocit când o insectã adevãratã a fost descoperitã blocând unul dintre circuitele electronice digitale dintr-un calculator ENIAC.

Bus - magistralã, un traseu electronic intern prin care sunt transmise semnalele dintr-o parte a calculatorului în alta.

Cablu coaxial (coaxial cable) - în retelele locale, un cablu de conectare de bandã largã prin mijlocul cãruia trece un fir izolat. În jurul firului izolat se aflã un al doilea fir fãcut din metal solid sau stil plasã.

CD-ROM - acronim pentru "Compact Disk - Read Only Memory", o tehnologie de memorare opticã, care foloseste compact discuri. Poate stoca pânã la 650 MB de date. Pe un singur CD-ROM pot fi pãstrate compactat pânã la 250.000 de pagini de text.

Ciberfobia (cyberphobia) este teama exageratã si irationalã de calculatoare. Remarcatã de psihoterapeutul Craig Brod si altii, ciberfobia provine din stressul de care indivizii se lovesc când încearcã sã facã fatã unei societãti dirijate din ce în ce mai mult prin calculator.

Ciberspatiu (cyberspace) - spatiu virtual creat de sistemele de calcul. Termen din realitatea virtualã ce poate fi experimentat prin punerea unei cãsti care afiseazã o lume ce nu existã în realitate, dar care oferã o senzatie de realitate.

Clear - a sterge, a înlătura date dintr-un document - fisier.

Client - într-o retea, o statie de lucru cu capacitãti de prelucrare, cum ar fi un calculator personal, care poate cere informatii sau aplicatii de la un server de retea.

Cluster - unitate de alocare. Pe o dischetã sau un hard-disk, unitatea de bazã în stocarea datelor. O unitate de alocare include douã sau mai multe sectoare.

Cod (code) - cod pentru a exprima un algoritm de rezolvare a unei probleme într-un limbaj de programare.

Compatibilitate (compatibility) - capacitate a unui dispozitiv, program sau adaptor de a functiona cu sau în locul unui anumit tip sau model de calculator, dispozitiv sau program. De asemenea, capacitatea unui calculator de a rula programele scrise pentru a fi rulate pe un alt calculator.

Comunicatii de date (data communication) - transferul de informatii de la un calculator la altul, ce se face direct prin conexiunile de cablu, precum în retelele locale, sau prin linii telefonice, folosind modemuri.

Conectivitate (connectivity) - capacitatea de a fi conectat. Gradul în care un anumit calculator sau program poate functiona într-o retea.

Confidentialitatea datelor (data privacy) - în retelele locale, limitarea accesului la un fisier astfel încât alti

utilizatori din retea să nu poată afisa continutul acelui fisier.

Criptare (encryption) - procedură de încifrare sau de codificare a datelor astfel încât utilizatorii care nu cunosc parola corespunzătoare să nu poată citi aceste date.

Decriptare (decryption) - proces de descifrare a datelor dintr-o formă criptată astfel încât să poată fi citite datele.

DES (Data Encrypted Standard) - standard de criptare a datelor, care foloseste un algoritm pentru criptare/decriptare de date, de 64 biti, utilizând o cheie de 56 biti. Este foarte des folosită în domeniul financiar.

Desktop - suprafata de lucru pe un calculator. Într-o interfată grafică cu calculatorul, o reprezentare a lucrului de zi cu zi, ca si când v-ati uita la un birou adevărat cu dosare pline cu lucrări de făcut.

Desktop computer - calculator de birou.

Director (directory) - un index pe care îl puteti afisa si care contine fisierele păstrate pe un disc sau pe o portiune de disc.

Dispozitiv (device) - orice componentă hardware sau periferic, cum ar fi o imprimantă, modem, monitor sau mouse, care poate receptiona si/sau transmite date.

Document - un fisier ce contine o lucrare creată precum un raport de afaceri, o notă sau o foaie de calcul.

Driver - un fisier sau program de pe disc ce contine informatiile necesare unui program să opereze un periferic precum un monitor sau o imprimantă.

E-mail (Electronic mail) - postă electronică, utilizarea unei retele pentru a transmite si a receptiona mesaje.

Etica pasionatilor (hacker ethic) - un set de principii morale ce erau cunoscute comunitătii din prima generatie a pasionatilor (1965-1982), descrise de Steven Levy în Hackers (1984). Conform eticii pasionatilor, toate informatiile tehnice ar trebui în principiu să fie la îndemâna tuturor, astfel încât nu este niciodată lipsit de etică să obtii accesul la un sistem pentru a examina si afla diverse informatii. Totusi, este întotdeauna lipsit de etică să distrugi, să modifici sau să muti datele în asa fel încât să provoci daune sau pagube altora. Din nefericire, în tot mai multe state, această activitate este scoasă în afara legii.

Firmware - programele de sistem care sunt stocate în memoria permanentă (ROM) a unui calculator sau în alte circuite ale lui, cum ar fi circuitele BIOS din calculatoarele compatibile IBM PC. Aceste programe nu pot fi modificate.

Fisier (file) - un document sau o altă colectie de informatii stocate pe un disc si identificat printr-un nume unic.

Fisier binar (binary file) - un fisier ce contine date sau instructiuni de program într-un format ce poate fi citit

de calculator. Nu poate fi afisat continutul real al fisierului binar cu mijloace obisnuite de vizualizare.

Fisier comprimat (compressed file) - un fisier transformat de către un utilitar într-un format special care minimizează spatiul necesar stocării pe disc.

Fisier corupt (corrupted file) - fisier defect, care contine date amestecate si de nerecuperat.

Fisier infectat (infected file) - fisier contaminat cu un virus informatic.

Format - aranjarea informatiilor pentru a fi stocate, tipărite sau afisate.

Groupware - programe de aplicatii care sporesc productivitatea cooperării si asocierii grupurilor mici de colaboratori.

Hacker - spărgător de coduri. Un entuziast al calculatoarelor căruia îi place să învete totul despre sistemele de calcul si care, printr-o programare inteligentă, împinge sistemul spre cel mai înalt nivel de performantă. Prin anii '80 presa a redefinit termenul pentru a include pe pasionatii care pătrund prin sistemele de securitate ale sistemelor de calcul. Desi unii sunt cu adevărat spărgători de coduri atrasi de pătrunderea în sistemele de calcul ale corporatiilor si organizatiilor, redefinirea dată de presă termenului a aruncat o pată peste activitătile multor utilizatori creativi ai calculatoarelor.

Hardware - componentele electronice, plăcile, perifericele si echipamentele care alcătuiesc un sistem de calcul; se distinge de programele (software) care spun acestor componente ce să facă.

Infectie (infection) - prezenta unui virus în cadrul unui sistem de calcul sau pe o dischetă. Infectarea poate să nu fie evidentă utilizatorului; de exemplu, multi virusi rămân ascunsi până la o anumită dată si oră, când afisează mesaje nebunesti sau sterg datele.

Integritatea datelor (data integrity) - proprietatea informatiilor păstrate într-o bază de date de a avea acuratete, de a fi complete si consistente.

Interfata (interface) - legătură între două dispozitive hardware, două aplicatii sau între un utilizator si programele de aplicatie, cu ajutorul căreia se obtine un schimb corect de date.

Internet - un sistem de retele de calculatoare interconectate, cu scopul de a se extinde în toată lumea, care înlesneste serviciile de comunicare a datelor cum ar fi deschiderea unei sesiuni de lucru de la distantă, transferul de fisiere, posta electronică si grupurile de discutii. Este o cale de a conecta retelele existente de calculatoare, care extinde mult posibilitătile fiecărui sistem participant. Originile lui sunt într-un sistem de calcul numit ARPAnet, al departamentului de apărare din Statele Unite, o retea experimentală realizată în 1969 pentru a înlesni colaborarea stiintifică în cercetarea militară. ARPAnet reprezintă o filozofie unică de

comunicatii de tip peer-to-peer în care fiecare calculator din sistem este pe deplin capabil să adreseze orice alt calculator.

O retea de calculatoare bazată pe modelul ARPAnet este cel mai bine descrisă ca fiind o colectie de centre de calcul autonome, locale si cu autocoordonare, care sunt legate sub forma unei anarhii ordonate. Motivatia realizării retelei ARPAnet a fost strict de ordin militar: reteaua trebuia să fie capabilă să facă fată unui atac ce putea distruge portiuni mari din ea. Conceptul functionează bine, după cum s-au convins Statele Unite si aliatii săi în timpul războiului din Golf. Reteaua de comandă si control a Irakului, modelată după tehnologia ARPAnet, a rezistat cu succes eforturilor aliatilor de a o distruge. De aceea tehnologia derivată din ARPAnet este acum pe lista de export "No-No".

Internet a fost initial realizată pentru a fi folosită în institutiile de învătământ, dar tehnologia sa permite practic oricărui sistem să se conecteze la ea printr-o poartă electronică. Astfel, mii de sisteme de calcul ale marilor firme, precum si sistemele de postă electronică cu platã ca MCI sau CompuServe, au devenit părti componente în Internet. Cu peste două milioane de calculatoare gazdă ce deservesc 20 de milioane de utilizatori, Internet se extinde cu un milion de noi utilizatori în fiecare lună. Aproape oricine poate obtine acces la Internet.

Laptop (laptop computer) - un calculator mic, portabil, care are greutate mică si dimensiuni destul de mici pentru a putea fi tinut în poală (lap). Cele care cântăresc mai putin de trei kilograme si pot intra în servietă se numesc notebook.

Licentã de program (software license) - întelegere legalã inclusã în programele comerciale. Licenta de program indicã drepturile si obligatiile persoanei care a cumpãrat programul si limiteazã penalitãtile pentru producãtorul programului.

Mailbox - cãsutã postalã; în posta electronicã, o locatie de stocare ce pãstreazã mesajele adresate unui individ în lipsa acestuia. Un anumit mesaj pe ecran informeazã utilizatortul cã îl asteaptã o corespondentã.

Migrare (migrare) - o trecere de la platforma unui echipament de calcul, un sistem de operare sau o versiune de program mai vechi la una nouã. De exemplu, observatorii industriei se asteaptã ca marile corporatii sã migreze de la MS-DOS la Microsoft Windows.

Modem - dispozitiv care converteste semnalele digitale generate de portul serial al calculatorului în semnale analogice, modulate, necesare transmisiei prin linii telefonice si, în mod analog, transformã semnalele analogice de intrare în echivalentul lor digital.

Multimedia - metodã ce are la bazã calculatorul, de prezentare a informatiilor folosind mai multe mijloace de comunicare (cum e textul, grafica si sunetul) si care pune accentul pe interactivitate.

Parola (password) - un instrument de sigurantã folosit pentru a identifica utilizatorii autorizati ai unui program de calculator sau retea de calculatoare si pentru

a defini drepturile lor, cum sunt permiterea numai a citirii, a citirii si a scrierii sau a copierii fisierelor.

Piraterie software (software piracy) - copierea neautorizatã si ilegalã a programelor cu marcã înregistratã.

Politica de securitate (security policy) - set de reguli, principii si practici care determinã modul în care acestea sunt implementate într-o organizatie. Ea trebuie sã mentinã principiile politicii generale de securitate ale organizatiei respective.

Program - o secventã de instructiuni specificând actiunea pe care calculatorul ar trebui sã o realizeze. Adesea, termenul de "software" este folosit pentru a descrie un program de calculator.

Program antivirus (antivirus program) - un utilitar proiectat pentru a detecta si a înlãtura virusi de calculator din memorie si din discurile de stocare a datelor. Poate fi utilizat si pentru a crea suma de control pentru fisierele vulnerabile de pe un disc, sã salveze sumele de control într-un fisier special si sã le utilizeze apoi pentru a determina dacã fisierele au fost modificate de un virus nou. Programele speciale rezidente în memorie pot sã detecteze tentativele neobisnuite de acces la zone vitale ale discului si la fisierele sistem si sã verifice fisierele copiate în memorie pentru a avea certitudinea cã nu sunt infectate.

Protectia datelor (data protection) - un grup de

tehnici utilizat pentru a mentine trei aspecte necesare datelor confidentiale, integritate si disponibilitate.

Protectie la scriere (read-only) - cu capacitatea de a fi afisat, dar nu sters. Dacã, dupã afisarea unor date ce pot fi doar citite, acestea pot fi editate, formatate sau modificate într-un alt fel, ele nu pot fi salvate în acelasi fisier.

Protectie prin parolã (password protection) - o metodã de a limita accesul la un program, fisier, calculator sau o retea solicitând introducerea unei parole.

Protocol de comunicatie (communication protocol) - standard care coordoneazã transferul de informatii între calculatoarele de pe o retea sau folosind telecomunicatiile. Calculatoarele implicate trebuie sã aibã aceleasi configurãri si sã foloseascã aceleasi standarde pentru a evita erorile.

Retea (network) - un sistem de comunicatii si de schimb de date bazat pe calculatoare, creat prin conectarea fizicã a douã sau mai multe calculatoare.

Retea client/server (client/sever network) - retea de tip client/server. O metodã de alocare a resurselor într-o retea astfel încât puterea de calcul sã fie distribuitã între calculatoarele din retea, dar unele resurse comune sã fie centralizate pe un server.

RoWildList - listã a tuturor virusilor în circulatie de pe teritoriul României. Lista este actualizatã permanent de cei mai buni specialisti români în domeniu si poate fi

consultatã oricând pe acest site. Sistemul de organizare folosit este dupã modelul de functionare a "WildList", care contine lista tuturor virusilor în circulatie pe plan mondial.

Scanner - dispozitiv periferic ce digitizează lucrările artistice sau fotografiile si stochează imaginea sub forma unui fisier ce poate fi combinat cu text în multe programe de prelucrare a textelor si de machetare.

Screen saver - program de protectie a ecranului. Un program utilitar care prelungeste viata monitorului schimbând afisarea de pe ecran când plecati de la calculator.

Scut (shield) - program antivirus care încearcã sã prindã virusii prin modul în care acestia îsi desfãsoarã activitatea (de exemplu, identificarea încercãrilor de alterare a unor fisiere .EXE sau scrierea peste sectorul de încãrcare a discului).

Securitate (security) - sigurantã, protejarea datelor, astfel încât persoanele neautorizate sã nu le poatã examina sau copia.

Semnãturã (signature) - în posta electronicã si în grupurile de discutie pe calculator, un mic fisier (de aproximativ trei-patru linii) care contine numele, organizatia, adresa, adresa de postã electronicã si, optional, numerele de telefon ale celui care transmite mesajul. Majoritatea sistemelor pot fi configurate ca sã anexeze automat acest fisier la sfârsitul fiecãrui mesaj pe care îl transmiteti.

Semnãturã de virus (virus signature) - cod de program care ajutã la identificarea unui virus ce afectează un sistem de calcul.

Server (file server) - într-o retea localã, un calculator personal care stochează pe hard disk-ul lui programele de aplicatii si fisierele de date pentru toate statiile de lucru din retea.

Shareware - programe de calculator cu marcã înregistratã care sunt puse la dispozitia utilizatorilor pentru a fi testate; dacã programul este agreat si luati hotãrârea sã-l folositi, trebuie plãtitã o taxã celui care l-a creat.

Sistem de operare (operating system) - program de control principal pentru un calculator, care coordonează functiile interne ale calculatorului si oferã mijloace de control asupra operatiilor calculatorului. De exemplu, MS-DOS, OS/2, Windows etc.

Software - programe de sistem, utilitare sau de aplicatii exprimate într-un limbaj ce poate fi citit de calculator.

Sumã de control (checksum) - acronim pentru SUMmation CHECK. În comunicatiile de date, o tehnicã de detectare a erorilor în care bitii dintr-o unitate de date sunt însumati si rezultatul transmis alãturi de date. Calculatorul care receptionează verificã apoi suma. Dacã ea diferã, probabil a intervenit o eroare în transmisie. Se foloseste si în programele de detectare a virusilor, sumele

de contriol sunt calculate pentru fiecare fisier dintr-un director si rezultatele sunt salvate într-un fisier păstrat în director. Când programul executã cãutarea, comparã informatiile sumei de control păstrate în director cu suma de control curentã pentru fiecare fisier parcurs. O diferentã apãrutã între cele douã sume poate indica faptul cã fisierul a fost infectat de un virus care nu are o semnãturã cunoscutã.

TCP/IP (Transfer Control Protocol/Internet Protocol) - set de standarde (protocoale) pentru transmisia de date si corectarea erorilor, care permite transferul de date de pe un calculator conectat la Internet pe altul.

Telecomunicatie (telecommunication) - transmiterea informatiilor, fie exprimate prin voce, fie prin semnale de calculator, prin sistem telefonic.

Terminal - un dispozitiv de intrare/iesire, format dintr-o tastaturã si un display video, folosit de obicei în sistemele cu mai multi utilizatori.

Text - date compuse numai din caractere ASCII standard, fãrã nici un cod special de formatare.

Virus - un program de calculator, cu scopul de a face o glumã sau un sabotaj, care se autoreproduce, atasându-se altor programe si executând operatii nedorite si uneori de distrugere.

Virtual - care nu este real; o reprezentare pe calculator a ceva real.