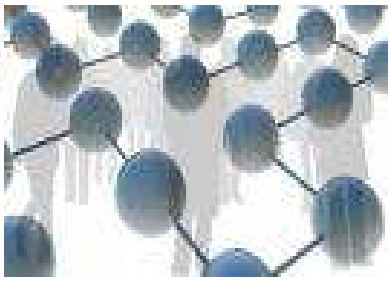
Reţeaua de calculatoare

Reţeaua de calculatoare (engl.: *computer network*) leagă între ele o mulţime mai mică sau mai mare de calculatoare, astfel încât un calculator poate accesa datele, programele şi facilităţile unui alt calculator din aceeaşi reţea. De obicei e nevoie desigur şi de măsuri de restricţie/siguranţă a accesului.

Metodele de conectare sunt în continuă dezvoltare şi deja foarte diverse, începând cu tot felul de cabluri metalice şi de fibră de sticlă, cabluri submarine, şi terminând cu legături prin radio cum ar fi WLAN, Wi-Fi sau Bluetooth, prin raze infraroşii ca de ex. IrDA sau chiar prin intermediul sateliţilor. Foarte răspândită este metoda Ethernet, termen care se referă la natura fizică a cablului folosit şi la tensiunile electrice ale semnalului. Cel mai răspândit protocol de comunicare în reţelele Ethernet se numeşte CSMA/CD ("*Carrier Sense Multiple Access / Collision Detection*"). Dacă drept mediu fizic sunt utilizate undele radio, atunci reţeaua se numeşte reţea fără fir (*wireless*).

Reţelele de calculatoare se împart după extinderea lor în următoarele tipuri: LAN, MAN, WAN şi, ceva mai nou, PAN. Reţelele relativ mici, de exemplu cu cel mult câteva sute de calculatoare în aceeaşi clădire legate între ele direct, se numesc *Local Area Network* (LAN). O reţea de tip LAN dar fără fir (prin unde radio) se numeşte WLAN (Wireless LAN). Reţele de mare întindere geografică, de exemplu între 2 oraşe, pe o ţară, un continent sau chiar pe întreaga lume, se numesc(WAN). Reţelele particulare de tip WAN au fost iniţial foarte costisitoare. La ora actuală însă, cele mai multe conexiuni de tip WAN folosesc ca mijloc de comunicaţie Internetul - acesta este universal şi public, deci nu foarte controlabil de către un utilizator, dar foarte convenabil ca preţ. În sfârşit, PAN înseamnă Personal Area Network - o reţea de foarte mică întindere, de cel mult câţiva metri, constând din aparatele interconectabile pe care o persoană le poartă cu sine, ca de exemplu telefon mobil, player MP3 sau aparat de navigaäie portabil



Cablu retea

RETEAUA DE CABLURI PENTRU... INTERNAUTI

-De problema cablurilor, beneficiaza cateva persoane care folosesc o suprafata mai mica sau mai mare din terasa, a carei suprafata este COMUNA TUTUROR locatarilor, aceasta fiind prin contract si proprietatea TOTUROR .
-Existenta acesteia, presupune intretinere si reparatie periodica din partea asociatiei, ... pe banii locatarilor.
-Daca va angajati in scris, catre Asociatie, ca suportati o parte, sau integral intretinerea si reparatia terasei, atunci sigur AFACEREA dvs. va prospera daca-mi permiteti..... si pe ingaduinta locatarilor, reprezentati de Presedintele asociatiei.

Cu bine!

Fibra optica

Conexiunea prin fibra optica

Comunicatiile au atins un punct in care, oricat de mare ar fi nevoia dumneavoastra de comunicatii, ea poate fi acoperita. Facem lucrul acesta, in principal, cu ajutorul tehnologiior broadband. Cea mai puternica dintre ele - fibra optica.

Tehnic vorbind, transmisia datelor prin fibra optica se bazeaza pe conversia impulsurilor electrice in lumina. Aceasta este apoi transmisa prin manunchiuri de fibre optice pana la destinatie, unde este reconvertita in impulsuri electrice.

Pentru dumneavoastra, asta inseamna:

- rata de transfer foarte mare in raport cu celelalte tipuri de conexiune (practic nelimitata, si inca imposibil de folosit la maximum de catre aplicatiile existente);
- mai multa siguranta - fibra optica este insensibila la perturbatii electromagnetice si este inaccesibila scanarilor ilegale (interceptari ale transmisiunilor);
- posibilitatea de instalare rapida si simpla, in orice conditii, datorita greutatii reduse a cablului optic si existentei mai multor tipuri de cabluri.

Dezvoltam, impreuna cu RCS, propria nostra retea nationala de fibra optica, integral functionala in acest moment, in lungime de peste 2500 Km, cu o capacitate totala de transport de 2,5Gbps.

De asemenea, am pus la punct retele metropolitane de fibra optica (MAN - Metropolitan Area Network), care faciliteaza schimbul local de informatii si care, in combinatie cu retelele de cablu TV, ne permit sa oferim clientilor nostri servicii de acces de mare viteza in toate judetele tarii. (detalii despre infrastructura RDS)

Hekari

Hackerii sunt pasionati ai informaticii, care, de obicei au ca scop "spargerea" anumitor coduri, baze de date, pagini web etc. Ei sunt considerati infractori, în majoritatea statelor lumii. Hackerii adevarati nu "distrug", de obicei, pagini inofensive, cum ar fi paginile personale. Tintele obisnuite ale atacurilor hackerilor sunt sistemele importante, care au protectii avansate si contin informatii strict secrete, cum ar fi bazele de date ale Pentagonului sau cele de la NASA. Odata obtinute, aceste fisiere (informatii) sunt publicate pe tot Internet-ul, pentru a fi vizionate sau folosite de cât mai multe persoane.

Orice hacker advarat trebuie sa respecte un "Cod de legi al hackerilor", care este bine stabilit, cunoscut si respectat.

Hackeri amatori

Exista "hackeri" care ataca tinte aleatoare, oriunde si oricând au ocazia. De exemplu, atacurile tot mai frecvente asupra Yahoo si Hotmail au blocat motoarele de cautare si conturile de mail respective pentru câteva zile, aducând prejudicii de milioane de dolari.

Aceste atacuri (care reprezinta o încalcare destul de grava a "Codul de legi al hackerilor") au de obicei în spate persoane care "au fost curiosi numai sa vada ce se întâmpla" sau "au dorit sa se distreze". Acesti atacatori virtuali nu sunt hackeri adevarati, pentru ca nu-si scriu singuri nuke -

urile (programele pentru bombardare - nucleare) pe care le folosesc, procurându-si-le de pe Internet sau din alte surse.

Acesti hackeri amatori sunt singurii care ajung în fata justitiei. Motivul este simplu. Acei hackeri adevarati care îsi pot scrie singuri nuke - urile, sunt, de obicei destul de inteligenti pentru a face anumite sisteme care sa induca în eroare pe toti aceea care ar încerca sa determine sursa atacului.

Crackeri

Crackerii reprezinta un stil anumit de hacker, care sunt specializati în "spargerea" programelor shareware, sau care necesita un anumit cod serial. Singurii care sunt prejudiciati de aceasta categorie de hackeri sunt cei care scriu si proiecteaza programele "sparte".

Sistemele de protectie ale aplicatiilor respective pot fi "înfrânte" prin doua metode:

Introducerea codului, care poate fi gasit fie pe Internet, fie cu ajutorul unui program asemanator cu OSCAR 2000, care este o biblioteca de coduri.

A doua metoda este folosita pentru sistemele de protectie mai avansate, care necesita chei hardware (care se instaleaza pe porturile paralele ale computerului si trimit un semnal codat de câte ori le este cerut de catre programul software), sunt patch-urile. Ele sunt programele care sunt facut special pentru anumite aplicatii software, care odata lansate modifica codul executabil, inhibând instructiunile care cer cheia hardware.

Patch-urile si bibliotecile de coduri seriale se gasesc cel mai des pe Internet. Ele sunt facute de anumite persoane (care sunt câteodata fosti angajati ai firmelor care au scris software-ul respectiv) care vor doar sa aduca pagube firmei proiectante.

Desi pare ciudat, cracking - ul este considerata "piraterie computerizata", reprezentând o infractiune serioasa. Totusi, foarte rar sunt depistati cei care plaseaza patch-uri si coduri seriale pe Internet.

Setul de unelte al unui hacker

Precum am mai precizat, hackerii adevarati îsi scriu singuri software-ul ce le e necesar. Multe dintre aceste programe, dupa ce sunt testate, sunt publicate pe Internet. Bineînteles, programele folosite pentru "spargerea" serverelor de la Pentagon sau pentru decodarea fisierelor codate pe 64 biti nu se vor gasi asa de usor pe Net, ele fiind tinute secrete de realizatorii lor.

Prezentam în continuare câteva dintre programele pentru hackerii amatori:

BoGUI BackOrifice. Un produs al The Dead Cow Cult, Bogui reprezinta un program de control al computerelor din reteaua dumneavoastra locala. Comenzi ca System Lockup (sau Restart) nu-l vor prea bine dispune pe utilizatorul computerului tinta. Singura problema a acestui program este ca toate comenzile sunt pachete transmise unui virus troian, astfel încât, daca computer-ul destinatie nu este infectat, bombardamentul cu Back Orifice nu va avea nici un efect.

Net Nuke. Acest program are o multime de versiuni, desi toate au acelasi efect si mod de operare: trimit un pachet nedefragmentabil prin retea, astfel încât când computer-ul tinta va încerca sa-l defragmenteze, nu va reusi decât sa blocheze portul de retea.

Mail Nukers. Sunt programe care bombardeaza o casuta de posta electronica cu un numar mare de

mesaje (care de obicei depaseste 10000). Acest bombardament duce la blocarea sau chiar pierderea unei casute de e-mail. Majoritatea acestor programe au optiuni care permit trimiterea de mail-uri anonime.

Aceste programe pot fi procurate de catre oricine foarte usor de pe Internet. Din pacate, unele dintre ele sunt folosite si ca un mediu de raspândire a virusilor, care pot avea efecte secundare foarte grave. Oricum, nu este recomandata abuzarea de aceste programe sau folosirea lor în scopuri (prea) distrugatoare.

Mass E - Mail-eri

Mass E - Mail-eri sau spameri sunt acei hackeri care transmit cantitati enorme de e-mail (sau alt fel de informatii), continând oferte nesolicitate, sau informatii aleatoare, transmise în scopul de a bloca anumite servere. Majoritatea site-urilor importante cum ar fi Yahoo, Amazon.com sau Hotmail au anumite sisteme de filtrare care ar trebui sa protejeze serverele respective de atacurile cu cantitati enorme de informatii. Aceste capcane sunt însa usor de evitat chiar si de începatorii în domeniul hackingului.

În ultimul timp serverele precizate mai sus precum si multe altele au fost supuse la puternice "atacuri cu informatii", la care nu puteau face fata. S-au trimis mesaje la o capacitate de aproape un MB/secunda, desi serverele respective suportau un trafic obisnuit de pâna la 1 - 1,5 GB saptamânal.

Spamerii, prin atacurile lor prejudiciaza cu sute de milione de dolari serverelor tinta. Tot odata sunt afectati si utilizatorii serverelor respective, traficul fiind complet blocat, trimiterea sau primirea mesajele sau utilizarea altor servicii asemanatoare fiind imposibila.

Va întrebatia cum se pot trimite cantitati atât de mari de informatii, la o viteza uimitoare, fara ca hackerii respectivi sa fie localizati fizic. Este relativ simplu pentru ei: transmit mesajele de pe aproximativ 50 de adrese de mail, dupa care deviaza informatia transmisa prin mai multe puncte din lume (diferite servere). Astfel, este foarte de greu sa fie detectati, echipele de specialisti de la FBI lucrând saptamâni (chiar luni) întregi pentru a prinde infractorul virtual, de multe uri neajungând la rezultate concrete.

Singura problema (a hackerilor) care apare în cazul acestor devieri succesive ale informatiei este aceea ca unul din serverele prin care "trece" informatia în drumul ei catre "tinta" finala se poate bloca. Informatia nu va ajunge în întregime la destinatie, puterea atacului scazând substantial. Astfel de cazuri se pot considera atacurile din ultimul timp, serverele afectate nefiind cele vizate de hackeri.

Protectii

Daca într-o zi chiar dumneavoastra veti fi una dintre nefericitele victime ale atacului unui hacker rautacios? Cum va puteti apara reteaua, baza de date sau pagina de pe web ?

Acestea probleme sunt importante pentru foarte multi utilizatori de computere, care utilizeaza în mod regulat Internet-ul. Exista protectii împotriva atacurile hackerilor. Singura problema este aceea ca regulile si protectiile sunt facute pentru a fi încalcate.

Deci, oricât de complexe si de sigure ar parea sistemele dumneavoasra de securitate, ele pot fi ocolite si "sparte".

Exista totusi anumite metode care, deocamdata, ar putea îngreuna putin viata hackerilor, mai ales a spammeri-lor (acesta fiind cel mai folosit în ultimul timp). Aceste ar trebui în primul rând aplicate de providerii de Internet (ISP):

Va trebui eliminate toate fisierele necunoscute de pe servere (care ar usura atacurile hackerilor), astfel încât se va tine o stricta evidenta a lor.

Eliminarea pachetelor care au alt header decât propria adresa de IP (pachete masluite). Ele pot fi folosite de unii utilizatori sub pretextul necesitarii anonimatului. Exista însa alte modalitatii de ati pastra anonimatul, folosind sisteme de criptare si a unor servere specializate.

Interzicerea comportamentelor specifice scanarii porturilor. Astfel se pot dezactiva programele care scaneaza zeci de mii de porturi din întreaga lume, pentru a face o lista cu cele vulnerabile.

Scanarea atenta a serverelor de "sniffere", programele care retin informatiile importante care intra si ies dintr-un server (username-uri, parole, numere de carti de credit etc).

Pe lânga metodele de protectie prezentate mai sus exista si multe multe altele, mai mult sau mai putin vulnerabile.

În orice caz, pâna la aducerea securitatii la un nivel acceptabil mai este mult de lucru...

Concluzii

Ce sunt hackerii cu adevarat ? Ce vor ei de fapt ? Acestea sunt întrebari la care numai un hacker adevarat poate raspunde (ceea ce nu se întâmpla prea des).

Vom încerca totusi sa explicam câteva din scopurile lor:

Adevar. Multi dintre hackeri "sparg" cele mai ciudate si complexe coduri de la Pentagon si NASA în speranta ca vor reusi sa demonstreze existenta "omuletilor verzi" sau a altor "teorii ale conspiratiei"

Superioritate.Demonstrarea superioritatii lor fata de "marii" programatori, sistemele informatice si serverele care le apartin este scopul multor hackeri.

Distractie. Unii hackerii fac "distrugeri" masive doar pentru a se distra pe seama celor care îsi vad munca distrusa în câteva secunde.

Protest. "Distrug" anumite site-uri de web sau baze de date fiindca nu sunt de acord cu informatia transmisa de ele.

Bani. Uneori se "sparg" bazele de date de la banci, pentru a transfera câteva milioane de dolari în contul propriu. Aceste operatiuni sunt foarte riscante, necesita experienta în domeniu, nefiind încercate de prea multi hackeri.

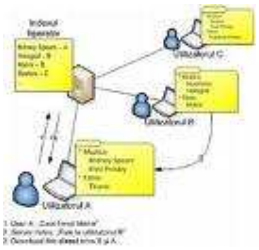
Anumiti hackeri, care au demonstrat de ce sunt în stare, fara a aduce pagube semnificative, devin consultanti în probleme de securitate computerizata. Ei poarta numele de "hackeri în alb". În câteva luni se va descoperi o noua metoda de hacking care sa depaseasca cu mult cunostiintele hackerului respectiv. Concluzia ca hackerii

sunt "o specie ce nu poate evolua în captivitate".

Într-adevar, "viata de hacker" este foarte incitanta, tentanta, nostima si interesanta, dar în acelasi timp foarte riscanta si periculoasa. Majoritatea statelor lumii considera hackingul o infractiune foarte grava, pentru care pedeapsa meritata este considerata de obicei interzicerea folosirii computerului, în unele cazuri, chiar ... PENTRU TOT RESTUL VIETII!!!

RETELE

Retelele de calculatoare au aparut din necesitatea partajarii datelor, si a resurselor hardware, existente intr-o societate intre mai multi utilizatori. În fiecare societate existau un numar oarecare de calculatoare, fiecare lucrând independent. Cu timpul acestea, pentru a putea fi utilizate intr-un mod mai eficient, au fost conectate impreuna prin intermediul unor dispozitive, dând astfel nastere la o retea. O retea reprezinta un ansamblu de calculatoare interconectate prin intermediul unor medii de comunicatie, asigurându-se in acest fel utilizarea in comun de catre un numar mare de utilizatori a tuturor resurselor fizice (hardware), logice (software si aplicatii de baza) si informationale (baze de date) de care dispune ansamblul de calculatoare conectate. De asemenea mai putem spune ca printr-o retea intelegem o colectie de calculatoare autonome interconectate intre ele.



Virusi

Virusii informatici sunt cele mai periculoase arme in razboiul datelor. In multe tari, astfel de programe au fost declarate ilegale iar autorii lor au primit diverse sanctiuni. Numarul actual al virusilor este foarte mare (o cifra exacta este greu de dat) mai ales ca zilnic apar virusi noi. Noi va punem la dispozitie cateva date generale, pentru a intelege mai bine felul in care virusii actioneaza si cum

Definitia virusilor :
Un virus este un program capabil de a se inmulti, strecurandu-se printre programele de pe un calculator sau dintr-o retea si provocand diverse efecte, de la unele inofensive, pana la unele

distructive.
In domeniul informatic se utilizeaza termenul virus din cauza asemanarilor functionale dintre aceste bucati de cod (programe) si vietuitoarele microbiologice.
O definitie ceva mai academica, spune ca virusul este de fapt un acronim, provenit de la Vital Information Resources Under Siege.

2. Efectele pe care le produc virusi :
Virusul ajunge in calculatorul tau printr-un transfer de fisiere - de pe o discheta sau cd, din retea, sau ca atasament la un e-mail. Un virus bine scris nu-si va trada prezenta pentru un timp, pentru ca ar putea fi detectat, de aceea va incerca sa profite de timp pentru a se inmulti. Copiile sale pot fi identice cu el sau pot fi diferite (virusi polimorfi).
Dupa ce indeplineste anumite conditii de inmultire, virusul incepe sa scoata capul in lume. Efectele sale pot fi unele nedistructive: canta o melodie (Doodle) sau afiseaza mesaje pe ecran: "Apa depistata in microprocesor. Functionarea poate fi compromisa. Se recomanda oprirea calculatorului cateva ore pentru uscare" – Alexander; "Critical error 08/15: Too many fingers on keyboard [Prea multe degete pe tastatura]" – Fingers, sau poate avea efecte rauvoitoare si distructive: trimite e-mailuri cu documente confidentiale (SirCam), distruge informatiile de pe hard-disk, formateaza hard-disk-ul, suprascrie Flash-BIOS-ul etc.

3. Tipuri de virusi :
Istoric virusi

1949
Sunt puse pentru prima oara bazele teoriilor legate de programele care se autoreproduc.

1981
Virusii Apple 1, 2, si 3 sunt printre primii virusi "in the wild". Descoperiti in sistemul de operare Apple II, virusii se raspandesc in Texas A&M prin intermediul jocurilor piratate.

1983
In teza sa de doctorat, Fred Cohen defineste pentru prima oara formal un virus de calculator ca fiind "un program ce poate afecta alte programe de calculator, modificandu-le intr-un mod care presupune abordarea unor copii evoluate ale lor."

1986
Doi programatori, Basit si Amjad, inlocuiesc codul executabil din sectorul boot al unui floppy-disk cu propriul lor cod, care infecta fiecare floppy de 360 Kb accesat pe orice drive. Floppy-urile infectate aveau "Š Brain" ca eticheta de disc (volume label).

1988
Scapa din lesa unul dintre cei mai cunoscuti virusi: Jerusalem. Activat in fiecare vineri 13, virusul afecteaza fisierele .exe si .com si sterge toate programele rulate in cursul acelei zile.

1990
Symantec lanseaza pe piata Norton AntiVirus, unul dintre primele programe antivirus dezvoltate de catre una dintre marile companii.

1991
Tequila este primul virus polimorf cu raspandire pe scara larga gasit "in the wild". Virusii polimorfi fac ca detectarea lor de catre scanerele de virusi sa fie dificila, prin schimbarea modul de actiune cu fiecare noua infectie.

1992
Exista 1300 de virusi, cu aproape 420% mai multi decat in decembrie 1990. Previziunile sumbre ale virusului Michelangelo ameninta colapsul a circa 5 milioane de calculatoare pe data de 6 martie. Insa doar 5,000-10,000 de calculatoare se intampla sa "dea coltul".

1994
Farsa de proportii din partea email-ului hoax (alarma falsa) Good Times. Farsa se bazeaza pe amenintarea unui virus sofisticat care e capabil sa stearga un intreg hard prin simpla deschidere a emailului al carui subiect este "Good Times". Desi se stie despre ce e vorba, hoaxul revine la un interval de 6-12 luni.

1995
Word Concept, virus de Microsoft Word, devine unul dintre cei mai raspanditi virusi din anii '90.

1998
StrangeBrew, actualmente inofensiv si totusi raportat, este primul virus care infecteaza fisierele Java. Virusul modifica fisierele CLASS adaugand la mijlocul acestora o copie a sa si incepand executarea programului din interiorul sectiunii virusate.
Virusul Cernobal se raspandeste rapid prin intermediul fisierelor ".exe". Dupa cum o sugereaza si notorietatea numelui sau, virusul este nemilos, atacand nu numai fisierele dar si un anumit cip din interiorul computerelor infectate.

1999
Virusul Melissa, W97M/Melissa, executa un macro dintr-un document atasat emailului, care transmite mai departe documentul la 50 de adrese existente in Outlook address book. Virusul infecteaza si documente Word pe care le trimite ca atasamente. Melissa se imprastie mult mai rapid decat alti virusi anteriori infectand cam 1 milion de calculatoare.
Bubble Boy este primul virus care nu mai depinde de deschiderea atasamentului pentru a se executa. De indata ce userul deschide email-ul, Bubble Boy se si pune pe treaba.

2000
Love Bug, cunoscut si sub numele de ILOVEYOU se raspandeste via Outlook, asemanator modului de raspandire al Melissei. Acest virus e primit ca un atasament .VBS, sterge fisiere, inclusiv MP3, MP2 si JPG si trimite username-uri si parole gasite in sistem autorului virusului.
W97M.Resume.A, o noua varianta a Melissei, este "in the wild". Virusul se comporta cam ca Melissa, folosindu-se de un macro Word pentru a infecta Outlook-ul si pentru a se raspandi.
Virusul Stages deghizat intr-un email gluma despre etapele vietii, se raspandeste prin Internet. Deloc specific celorlalti virusi anteriori, Stages este ascuns intr-un atasament cu extensie falsa .txt, momind utilizatorii sa-l deschida. Pana la aparitia sa, fisierele text erau considerate fisiere sigur .