Criminalitatea informatică poate cauza multe probleme în societatea modernă. Prin urmare, România a adoptat legislaţia privind criminalitatea informatică care corespunde pe deplin convenţiilor şi standardelor internaţionale. Totuşi, această legislaţie poate fi complexă din punctul de vedere al aplicării sale pentru autorităţile care o implementează, în special pentru aceia care sunt mai puţin familiarizaţi cu computerele şi serviciile electronice ca parte a vieţii de fiecare zi.

Portalul eFrauda a fost realizat de către Ministerul Comunicaţiilor şi Tehnologiei Informaţiei şi este gestionat împreună cu Serviciul de Combatere a Criminalităţii Informatice din cadrul Ministerului Administraţiei şi Internelor şi secţia specializată din Parchetul de pe lânga Înalta Curte de Casaţie şi Justiţie. Portalul dă oricui posibilitatea de a sesiza autorităţile cu privire la o posibilă fraudă sau alte activităţi ilegale pe Internet.
www.efrauda.ro

Acest *Ghid introductiv pentru aplicarea dispoziţiilor legale referitoare la criminalitatea informatică* a fost elaborat de către proiectul RITI dot-Gov, în cooperare cu Ministerul Comunicaţiilor şi Tehnologiei Informaţiei. *Ghidul* asigură asistenţă pentru autorităţile care aplică legea şi pentru toţi cei care sunt implicaţi în prevenirea criminalităţii informatice.

Proiectul RITI dot-Gov face parte din Iniţiativa pentru Tehnologia Informaţiei în România, RITI, a cărei implementare a fost începută în 2002 de către Misiunea din România a Agenţiei Statelor Unite pentru Dezvoltare Internaţională (USAID), în cooperare cu Ministerul Comunicaţiilor şi Tehnologiei Informaţiei. Proiectul RITI dot-Gov este implementat în România de Internews Network Inc, o organizaţie non-profit cu sediul în Statele Unite.

Pentru informaţii suplimentare:
www.usaid.gov/info_technology/dotcom
www.riti-internews.ro
www.internews.org
www.mcti.ro

GHID
INTRODUCTIV PENTRU APLICAREA DISPOZIŢIILOR LEGALE REFERITOARE LA CRIMINALITATEA INFORMATICĂ

INTERNEWS
RITI dot-Gov

MCTI

Bucureşti,
Mai 2004

Elaborarea acestui ghid a fost posibilă prin asistența asigurată de către Centrul de Servicii Regional Budapesta al Agenției Statelor Unite pentru Dezvoltare Internațională, USAID, în cadrul Acordului nr. CA # 186-A-00-02-00101-00; LA#GDG-A-00-01-00009-00; Internews Network/RITI dot-Gov Project.

Opiniile exprimate în cadrul acestui document aparțin autorilor şi nu reprezintă în mod necesar vederile Agenției Statelor Unite pentru Dezvoltare Internațională.

Capitolul I - Sisteme informatice şi medii de stocare

Dispozitive de calcul

Calculatorul electronic propriu-zis este principala sursă de informaţii pentru investigator. Pe calculator, informaţiile sunt stocate pe unităţile de hard-disc. O unitate de hard-disc este un dispozitiv ce permite înregistrarea magnetică a datelor, alcătuit din unul sau mai multe discuri rigide, capete de citire/scriere şi mecanisme mecanice protejate de o carcasă metalică, închisă etanş. Capacitatea de stocare a unui hard-disc normal este în zilele noastre de câteva zeci sau sute de *gigabytes*. Un calculator poate avea unul sau mai multe hard-discuri, de tipuri şi capacităţi diferite.

Calculator Personal – PC

Calculatoarele portabile sunt calculatoare concepute pentru a putea fi mutate cu uşurinţă. Datorită performanţelor la care au ajuns, unele dintre acestea pot fi folosite de utilizatori ca staţie de lucru permanentă.

Laptop

Tipurile de calculatoare portabile sunt:

- transportabile
- laptop
- ultra-uşoare
- de mână (se mai numesc Poket PC-uri, *Palm*-uri sau PDA-uri - *personal digital assistant*)

Smartphone

Chiar şi în cazul în care nu sunt folosite în mod permanent, calculatoarele portabile sunt o sursă importantă de informaţii, deoarece pot fi folosite pentru stocarea unor date, posibil confidenţiale, ce trebuie transportate în afara locaţiilor unde securitatea este asigurată.

În ultima vreme, datorită posibilităţilor tehnice de a miniaturiza dispozitivele de calcul, acestea au fost integrate în echipamente portabile de mici dimensiuni. Cel mai bun exemplu în acest sens este telefonul mobil, care a căpătat caracteristici de mini-calculator. Pe lângă jurnalele ultimelor

convorbiri, un telefon modern poate conţine liste de adrese, calendarele întâlnirilor, documente şi notiţe etc. având capacităţi superioare chiar PC-urilor de acum câţiva ani.

Dischete - Floppy Disks

Echipamentele periferice:

- *tastatura* nu are funcţia de stocare de informaţii, fiind doar un dispozitiv de introducere a datelor. Totuşi există anumite dispozitive care se pot ataşa tastaturilor şi care pot să înregistreze secvenţele de taste apăsate de utilizatori. Deşi sunt răspândite foarte puţin, aceste dispozitive sunt foarte uşor de procurat.
- *monitoarele* nu sunt capabile să stocheze informaţii. În trecut, datorită limitărilor tehnice se puteau determina imagini sau text ce au rămas un timp mai îndelungat pe ecran, prin impresiunile produse pe fosforul tubului catodic. Monitoarele moderne nu mai prezintă acest efect.
- *imprimantele* pot constitui surse de informaţii importante. De exemplu: imprimantele de tip laser permit relevarea imaginii ultimelor pagini imprimate. Această tehnică trebuie utilizată înainte de decuplarea imprimantei de la reţeaua de alimentare cu energie electrică, fapt ce necesită prezenţa unui expert la locul percheziţiei. Unele imprimante laser dispun de un hard-disc de *buffer* pe care sunt stocate informaţiile ce urmează a fi imprimate. Capacitatea unui astfel de disc este între 2 şi 10 Mb. Datele stocate pe aceste discuri pot fi obiectivate potrivit unor proceduri relativ simple. Pentru modelele mai vechi de imprimante, ce utilizează cartuşe cu bandă (*ribbon*), se poate reconstitui textul imprimat prin examinarea panglicii. Metoda este similară analizei panglicii de la maşina de scris.

Imprimantă

Mediile externe de stocare a informaţiilor sunt:

- *unităţile de CD-ROM* (acronim de la *Compact Disc-Read Only Memory* - memorie numai pentru citire de pe compact-disc) sunt dispozitive de stocare a datelor pe discuri optice, folosind tehnologia compact-discului. Datele sunt citite cu un sistem bazat pe raze laser, iar nu pe mijloacele magnetice folosite în cazul celorlalte metode de stocare a datelor informatice. Unele unităţi de tip CD-ROM (*CD-recorder*) pot fi folosite şi pentru înregistrarea datelor pe suport optic.

- *dischetele*. Cel mai comun tip de dischete folosite astăzi sunt dischetele de 3,5 ţoli. În trecut au fost utilizate şi dischetele de 5,25 ţoli. Dischetele constituie un mediu de stocare selectivă a datelor de către utilizatori. Salvarea datelor pe dischetă este realizată de utilizatori din diferite motive, cum ar fi: crearea de copii de siguranţă a unor fişiere importante, înregistrarea de date pe care utilizatorul nu doreşte să le stocheze pe calculatorul întreprinderii, copierea unor fişiere în vederea transferării lor pe alt calculator etc.

CD – Disc Compact

- *discurile de salvare de siguranţă*. Informaţiile din copiile de siguranţă create pentru evitarea pierderii informaţiilor în cazul unei pene a sistemului sunt o sursă importantă pentru investigatori. O dată cu ridicarea discurilor de salvare de siguranţă trebuie să fie consemnate cât mai multe informaţii asupra modului de realizare a copiilor de siguranţă, în special tipurile de echipamente, programele şi procedurile folosite. Informaţia de siguranţă este salvată de obicei pe discuri optice de capacitate mare, cu această destinaţie, cum ar fi discurile de tip *Zip* sau *Jazz*, produse de Iomega dar poate exista pe orice tip de mediu de stocare. În ultima perioadă au devenit foarte populare memoriile flash, foarte mici ca dimensiuni, cu capacităţi destul de mari (cuprinse între 32 de *megabytes* şi câţiva *gigabytes*). *discurile optice* (cele mai populare fiind *CD*) sunt suporturi de stocare de mare capacitate a datelor digitale. Capacitatea unor astfel de discuri este de la 650 Mb (CD-urile) la 4 Gb (DVD-urile). Discurile optice pot fi de tip normal (numai pentru citire, fără a exista posibilitatea înregistrării de date), înregistrabile (este posibilă citirea şi scrierea de date pe disc, fără a fi posibilă ştergerea datelor), sau cu posibilitate de rescriere (este posibilă citirea, scrierea şi ştergerea datelor pe disc).

Unitate de stocare USB (Flash)

Hard disc detaşabil

- *hard-discurile detaşabile* sunt de asemenea un mediu de stocare a informaţiei. Ele au capacităţi similare cu cele fixe, si sunt folosite în general pentru transferul fişierelor de mari dimensiuni.

Tipologia datelor aflate pe suporturile specifice

Sisteme de fişiere

Funcţia primară a sistemelor informatice este să stocheze şi să proceseze date. Datele procesate şi stocate de sistemele informatice pot fi clasificate în patru mari categorii: date active, date arhivate, date salvate de siguranţă şi date reziduale.

Datele active informaţii disponibile şi accesibile utilizatorilor. Ele se prezintă sub forme foarte variate, cum ar fi: documente realizate de procesoarele de text, calendare electronice, liste de adrese, fişiere grafice, fişiere audio, etc.

O particularitate o reprezintă faptul că în cazul datelor de natură informatică copia şi originalul sunt absolut identice (prin copiere nu se schimbă nimic). Evidenţa datelor active poate fi făcută cu ajutorul unor programe speciale denumite gestionare de fişiere, sau prin executarea unor comenzi specifice sistemelor de operare.

Datele arhivate sunt informaţii care nu mai sunt utilizate în mod curent, fiind stocate în mod separat, pentru a elibera spaţiul de pe disc. Datele arhivate cuprind şi fişierele duplicat. Fişierele duplicat sunt fişierele create automat de calculator în cazul apariţiei unor probleme tehnice (cum ar fi blocarea sistemului, întreruperea alimentării cu energie electrică etc.), având rol de recuperare a datelor. Ele au terminaţii de fişier specifice, şi sunt stocate de obicei în locaţii diferite de fişierele originale. Importanţa lor constă în crearea unor copii multiple ale documentelor, copii pe care utilizatorul nu le poate şterge şi de a căror existenţă, de cele mai multe ori, nici nu are cunoştinţă. Prin compararea copiilor duplicate cu originalul pot fi făcute observaţii asupra modificărilor intervenite între diferitele variante ale documentului.

Datele salvate de siguranţă (sau datele de *backup*) sunt informaţii copiate pe medii de stocare portabile, cu scopul punerii la dispoziţia utilizatorilor a datelor lor în cazul intervenţiei unei pene a sistemului. Frecvenţa de realizare a copiilor de siguranţă depinde atât de tipul sistemelor informatice (calculator neconectat în reţea, sau reţea de calculatoare) cât şi de procedurile utilizatorilor.

În cazul reţelelor, o practică tipică este realizarea unei copii de siguranţă complete o dată pe săptămână, de obicei vinerea, şi realizarea zilnică a unei copii suplimentare, vizând salvarea datelor modificate în ziua respectivă; în aceste cazuri, se copiază de obicei numai informaţia aflată pe serverul reţelei, nu şi cea aflată pe calculatoarele (terminalele) utilizatorilor individuali. La sfârşitul lunii este realizată copia de siguranţă lunară, care este stocată separat, şi este păstrată o perioadă de timp variind de la câteva săptămâni la câteva luni. În practică mediile pe care se realizează copiile lunare se reutilizează după o anumită perioadă de timp.

Pentru calculatoarele ce nu sunt conectate în reţea, în lipsa unui sistem de copiere de siguranţă propriu, posesorii lor copiază de regulă fişierele cărora le atribuie mai mare importanţă, fie pe dischete, fie pe alte medii de stocare, cum ar fi hard-discuri detaşabile, CD-uri inscriptibile, discuri flash, etc.

Folosirea informaţiilor de pe mediile de stocare pentru copiile de siguranţă este utilă datorită păstrării informaţiei un timp mai îndelungat. Cu toate acestea, lipsa unei

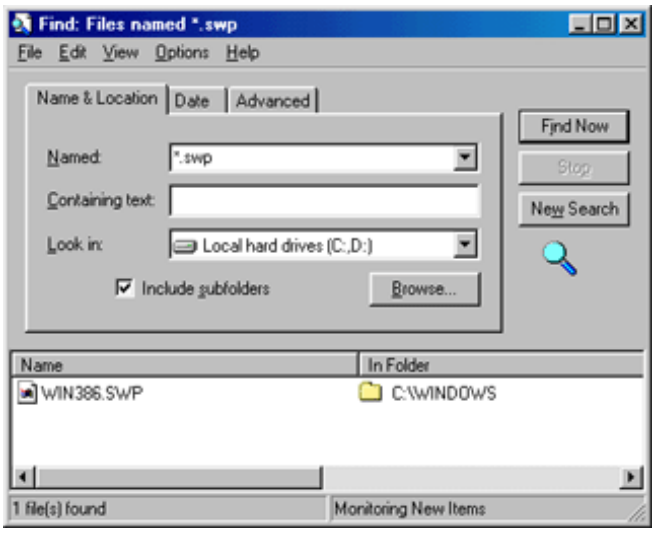
organizări a datelor aflate pe aceste medii, precum şi faptul că de obicei fişierele salvate de siguranţă sunt compresate din economie de spaţiu, fac mai dificilă investigaţia.

Datele reziduale sunt informaţii ce aparent au fost eliminate din sistem dar care mai persistă în forme specifice, putând fi recuperate. Astfel de date reziduale sunt: fişierele şterse care se mai află pe disc, fişierele temporare, fişierele de schimb, datele aflate în spaţiul inactiv, datele din *buffer* şi *clipboard*.

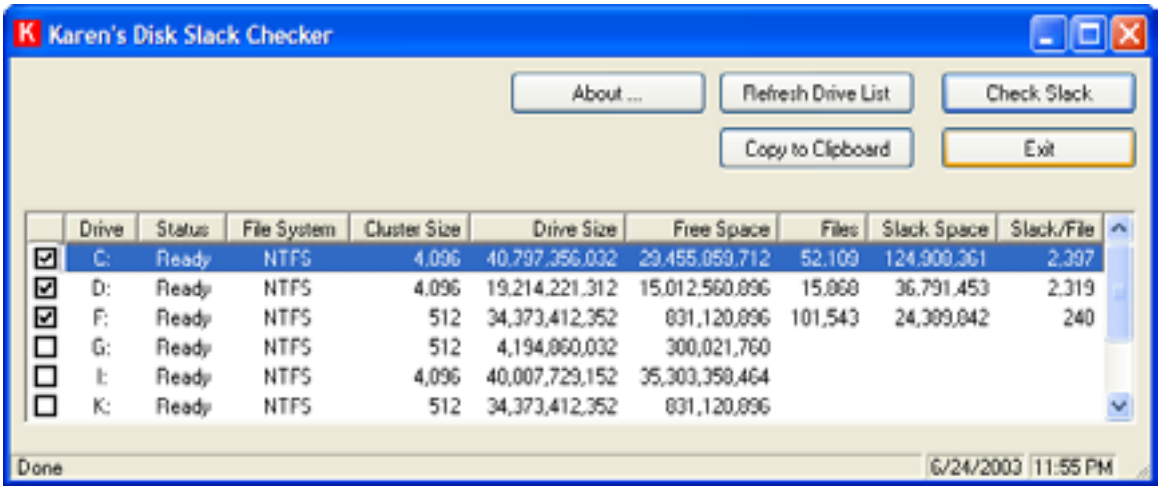
În cazul ***ştergerii*** normale a unui fişier, datele nu sunt eliminate de pe disc, ci calculatorul marchează porţiunile pe care s-a aflat fişierul respectiv ca libere, putând fi deci rescrise. În cazul în care suprascrierea nu are loc (în cazurile în care ştergerea a fost recentă, sau dacă există suficient spaţiu liber pe disc, şi nu au avut loc operaţiuni de rutină privind întreţinerea sistemului, cum ar fi defragmentări sau optimizări), fişierul, sau porţiuni ale acestuia se află încă pe disc, putând fi recuperate. Pentru recuperare se utilizează programe speciale. De fapt, datele devin nerecuperabile abia după ce spaţiul de pe disc pe care se aflau au fost suprascrise de 7 ori. Există programe speciale care pot face această operaţiune (suprascrierea de 7 ori), pentru a şterge definitiv anumite date.

Fişierele temporare sunt fişierele create de sistemul de operare sau de un alt program pentru a fi utilizate în timpul sesiunii de lucru. În multe cazuri fişierele temporare nu sunt şterse de pe disc, putând fi astfel recuperate informaţiile conţinute în ele.

Fişierele de schimb (sau fişierele *swap*) sunt fişiere ascunse, create de sistemul de operare pentru a fi folosite la păstrarea de porţiuni ale fişierelor de program şi de date care nu încap în memorie. Fişierele de schimb sunt o formă de memorie virtuală. Informaţia din fişierele de schimb poate fi analizată cu ajutorul unor programe speciale.



Spaţiul "inactiv" (*slack space*) reprezintă spaţiul, aflat în cadrul unei unităţi fizice de stocare a datelor pe disc (*cluster*), ce nu este acoperit de porţiunea de fişier ce ocupă unitatea respectivă. Cum sistemul de operare DOS nu permite stocarea a mai mult de un fişier în cadrul unei unităţi de stocare, diferenţa între mărimea fişierului curent şi mărimea unităţii de stocare este considerată spaţiu "inactiv", neutilizat. Acest spaţiu poate conţine informaţii ce pot fi recuperate folosind programe specifice. De asemenea, acest spaţiu, ca şi unităţile de stocare considerate avariate, pot fi folosite de utilizatori avansaţi ai sistemelor informatice în scopul ascunderii de informaţii.



Program care permite lucrul cu spaţiu „inactiv”

Buffer-ul este o zonă de memorie rezervată utilizării ca depozit intermediar, în care sunt păstrate temporar datele ce aşteaptă să fie transferate dintr-o locaţie în alta. Datele aflate în *buffer* pot fi recuperate cu ajutorul unor programe speciale.

Clipboard-ul este o porţiune de memorie, cu caracter special, întreţinută de sistemele de operare bazate pe modul de lucru cu ferestre (cum ar fi Windows). În *clipboard* sunt stocate datele ce sunt transferate dintr-un program în altul. Datele copiate prin *clipboard* au un caracter static, ele nereflectând modificările ulterioare, şi pot fi obiectivate prin metode obişnuite de lucru.

Date despre mediul sistemului informatic

Fişierele de date nu constituie sigurele posibilităţi de relevare a informaţiilor aflate în sistemele informatice. În categoria datelor despre sistemul informatic intră evidenţele de auditare, jurnalul activităţilor calculatorului, lista de control a accesului, precum şi alte informaţii ce nu pot fi imprimate.

Evidenţele de auditare sunt un mijloc de urmărire a tuturor activităţilor ce afectează anumite date, începând din momentul creării lor până la eliminarea din sistem. Ele sunt folosite de majoritatea programelor de gestiune a reţelelor de calculatoare. Aceste evidenţe, precum şi jurnalul computerului (*computer log*) pot oferi informaţii despre cine şi când a accesat sistemul, de unde şi pentru cât timp, precum şi operaţiunile făcute de acesta (modificări, copieri, ştergeri, etc.).

Pe lângă evidenţele de auditare, un număr mare de întreprinderi au instalate programe speciale de monitorizare a utilizării de către un angajat a sistemelor informatice proprii. Aceste programe pot furniza informaţii despre programele accesate, fişierele utilizate, mesajele de poştă electronică trimise si primite, siturile de Internet vizitate, etc.

Lista de control a accesului (*ACL*) este lista asociată unui fişier, ce conţine numele utilizatorilor şi grupurilor ce au permisiunea să acceseze şi să modifice acel fişier. Nivelul de acces a utilizatorilor la fişierele respective depinde de atribuţiile sau poziţia angajatului în cadrul întreprinderii.

Informaţiile ce nu pot fi imprimate sunt de asemenea surse importante pentru investigatori. Astfel de informaţii sunt: data şi timpul, ataşate fiecărui fişier, informaţiile despre crearea, accesarea şi modificarea unor fişiere (furnizate, de exemplu, de editoarele de text), comentariile şi notele ce nu sunt destinate imprimării, etc.