Domeniul de aplicatie al raspunderii juridice civile pentru prejudiciile cauzate prin atacul cu virusi informatici

Conf.dr. Mircea TOMA, conf.dr. Emil STAN
Academia de Politie ,,Alexandru Ioan Cuza", Bucuresti

Lucrarea îsi propune sa evidentieze si sa evalueze pagubele atacurilor cu virusi informatici pe baza concluziilor desprinse din utilizarea unor modele matematice (Tippett 91). În baza acestor ipoteze de lucru sunt evidentiate, în cadrul masurilor de securitate aplicate sistemelor informatice, masuri juridice, cu deosebire în situatia raspunderii penale, administrative si civile.
***Cuvinte cheie**: virus informatic, MS – DOS, WINDOWS, Internet, securitatea sistemului de calcul, software antivirus, raspundere civila.*

1. Virusi informatici

În unele tari cum ar fi: Franta, Elvetia, Germania, utilizarea virusilor informatici pentru a periclita datele se pedepseste conform legii. De asemenea este ilegal de a produce, a oferi, a importa, a distribui, a promova sau a pune la dispozitia beneficiarilor potentiale programe care vor afecta calitatea datelor si de a da algoritmi de producere a unor astfel de programe.

Aceste activitati sunt pedepsite datorita impactului serios pe care îl au asupra calitatii datelor (Ivan, 1998). Lucrarea îsi propune ca, evidentiind prejudiciile cauzate de virusii informatici, sa justifice necesitatea unor legi specifice, atât în domeniul penal, cât si în cel civil.

Adevarate bijuterii ale tehnicii programarii, virusii au fost creati de autorii lor si raspânditi din curiozitate, din joaca, din vanitate sau rautate, pentru a stimula crearea de noi sisteme de protectie sau programe (inclusiv antivirus) sau de-a dreptul pentru a crea dezastre.

În unele tari, cum este Bulgaria, scrierea virusilor pare a fi o preocupare nationala (Bontchev, 1994). Totusi în general, autorii de virusi sunt persoane tinere, care sunt înca la scoala sau la facultate.

Au fost raportate cazuri si de adulti care au raspândit virusi informatici. Astfel este cazul lui Joseph Pop din UK care a distribuit un disc ,,Aids Information". Acest program oferea o serie de informatii despre virusul HIV, dar în acelasi timp criptografia hard-discul utilizatorului.

Dupa ce a fost arestat în S.U.A si judecat în U.K, a fost recent pus în libertate pe baza marturiei unui psihiatru.

Mark Washburn (Anglia) este autorul unei serii lungi de virusi. El motiva actiunea sa prin faptul ca dorea sa creeze un virus care nu poate fi descoperit de antivirusuri.

Odata patrunsi în calculator sau retele, virusii informatici au deseori o comportare asemanatoare celor biologici: se multiplica, se localizeaza într-o zona a programului sau sistemului si apoi ataca. Unii pot sa produca un bruiaj sonor sau vizual, sa opreasca aplicatiile, sa blocheze sistemul de operare, sa distruga bazele de date ori structurile fizice ale calculatorului, sa supraîncarce functionarea sistemelor si retelelor si sa determine prabusirea lor ori dimpotriva încetinirea dramatica a functionarii sistemului sau retelei.

Sunt cunoscute numeroase atacuri cu virusi care au creat pagube importante si care nu au ocolit, ba dimpotriva, sistemele unor institutii de importanta deosebita precum C.I.A., N.A.S.A, PENTAGON etc.

Gradul de portabilitate apropiat de 100% a software-ului pe PC - uri a facut ca problema virusilor pe PC-uri sa aiba cel mai mare impact pe calculatoarele IBM – PC si compatibile. Exista o mare varietate

de efecte pe care le genereaza virusii pe calculator. Chiar cei mai putin distructivi au o serie de efecte colaterale.
Sistemul de operare MS – DOS sau sistemul Windows sunt sisteme complet deschise. Nici o portiune a acestora nu este protejata în memorie sau pe disc. Multe proceduri, cum sunt cele prezente permanent în memorie (TSR–uri), nu sunt bine definite si controlate. De asemenea, constatam ca multi virusi încearca sa lucreze în multi-tasking, ceea ce MS – DOS nu suporta. Prin urmare, apar multe conflicte între virusi si alte programe, inclusiv sistemul de operare. Cei mai noi virusi „stealth" se furiseaza ca noile tipuri de avioane cu acelasi nume si ridica probleme mari. Rezultatele sunt dificil de estimat. Acestea pot duce fie la programe care nu mai merg, fie la compromiterea întregului hard-disc.
Virusii se manifesta si produc daune diferentiat. Cu titlu de exemplu prezentam caracteristicile modului de actiune ale unor virusi:
a) **Virusul Israeli** (Vineri – 13) actioneaza în ziua specificata de nume, stergând toate programele existente pe hard-disc. Pâna atunci, virusul se poate observa prin faptul ca sistemul este mai lent si apare din când în când un dreptunghi cu un text care se deplaseaza.
b) **Virusul Oropax** are ca efect lansarea unei melodii din 5 în 5 minute. În timp ce PC-ul cânta, nu mai executa alte programe. S-au semnalat si cazuri când studentii deliberat au infectat reteaua de calculatoare a universitatii, creând astfel rumoare în timpul orelor.
c) **Virusul Vaksim** este mai putin distructiv. El provoaca un beep sonor, de câte ori se lanseaza un program nou. Pentru a scapa de acest virus este nevoie de o formatare la nivelul de jos al hard discului.
d) **W95.CIH (Chernobyl)**.
CIH este un virus care infecteaza fisierele executabile Windows 95/98/NT 32-biti. Când se executa un program infectat pe o masina Windows 95/98, virusul va infecta memoria RAM. Desi fisierele sistem NT pot fi infectate, virusul nu se poate activa pe sistem în timp ce executa Windows NT si memoria nu va fi infectata. CIH apoi infecteaza fisierele noi atunci când acestea vor fi deschise. Unele variante actioneaza pe 26 aprilie sau 26 iunie, în timp ce alte variante actioneaza pe 26 ale fiecarei luni. Virusul va scrie pe primul MB al harddiscului date random, apoi va încerca sa modifice anumite parti din BIOS (software-ul care initializeaza si conduce relatiile si fluxul de date dintre anumite terminale (hard-disc, porturile seriale si paralele, tastatura). Prin rescrierea unei parti din BIOS, virusul va face ca sistemul sa nu porneasca când acesta se conecteaza la reteaua electrica. Virusul cauta mai întâi spatiile goale, neutilizate din fisier, apoi se rupe însusi în mai multe bucati si se ascunde în acele spatii neutilizate.
e) Virusi pe e-mail
1) Uneori apar pe Internet mesaje ca: "Daca primesti un e-mail intitulat «It takes get's to say Jesus» nu trebuie deschis. Acest virus va sterge tot ce exista pe harddisc". Aceasta informatie a fost lansata pe 21 aprilie de la IBM.
2) De asemenea mesajul e-mail „RETURNED OR UNABLE TO DELIVER" este în fapt un virus.
3) Virusul Hitler pune stapânire pe calculator si nu sunt remedii împotriva lui.
4) Virusul Good Times nu exista. Multe persoane si centre de cercetari AV primesc mesaje despre acest virus, mai ales în perioada vacantelor, când posta electronica este mai aglomerata.
În ultima perioada s-a constatat ca unele mesaje lansate pe Internet sunt pacaleli (hoax).
f). **Back Orifice** este un instrument alcatuit din doua piese principale: o aplicatie client si una server.
Punând stapânire pe masina, virusul:
- executa orice aplicatie de pe masina în cauza

- restarteaza aceste masini
- închide masina
- vizualizeaza continutul oricarui fisier de pe masina virusata
- transfera fisiere la si de la aceasta masina
- citeste parolele utilizatorului curent

Un alt virus, care are aceleasi simptome este Net Bus.

Autorii acestor virusi, grupul de hackeri „Cult of the Dead Cow" a vrut sa arate întregii comunitati informatice slaba preocupare pentru securitate a firmei Microsoft (Internet Magazin, noiembrie '98).

Aparitia si dezvoltarea exponentiala a virusilor si amenintarile pe care acestia le exercita au determinat aparitia unei noi dimensiuni a sistemelor de calcul: asigurarea securitatii calculatoarelor si protectiei la virusi. Protectia de soft antivirus a devenit o adevarata industrie, dar din pacate, se afla într-un cerc vicios: actualizarea listelor se face trimestrial în timp ce aparitia si multiplicarea virusilor se face zilnic.

Trebuie recunoscut însa ca o serie de infectii se produc prin nerespectarea unor norme elementare de securitate precum utilizarea unor dischete neverificate, nelansarea periodica sau dezactivarea scanerelor antivirus, etc.

2. Atacul virusului, atac la securitatea sistemului de calcul

Sistemele de calcul si retelele actuale nu sunt imune fata de amenintarea virusilor.

Practic constatam cresterea anomaliilor software, iar amenintarea hackerilor este mai actuala ca oricând.

Termeni ca „sistem sigur" sau „sistem de operare sigur", des întâlniti, sunt derutanti deoarece nu sunt transpusi în realitate.

Securitatea calculatoarelor acopera:

- confidentialitatea (protectia fata de accesul neautorizat la date)
- integritatea (garanteaza ca datele sunt disponibile în forma lor fizica si logica - semantica)
- accesibilitate si disponibilitate

În prezent masurile de securitate se iau pentru asigurarea confidentialitatii datelor, neglijând aspectele legate de integritate si accesibilitate. Pentru asigurarea confidentialitatii sunt folosite mecanisme de control a legalitatii utilizarii sistemului si mecanisme de identificare si autentificare, pentru verificare si control acces. Pentru asigurarea integritatii datelor se folosesc aceleasi proceduri.

Modelele de integritate de asemenea fac apel la mecanisme de control al accesului, la modul de formare a interogarilor bazei de date sau la separarea zonelor de interes. Sistemele cu o securitate deosebita se bazeaza pe modele formale si metode de verificare complexa. Modelele de securitate formala definesc „securitatea" ca îndeplinirea unor anumite proprietati de siguranta si garanteaza ca, prin începerea sesiunii de lucru dintr-o stare sigura si prin aplicarea regulilor modelului, aceste proprietati de siguranta se vor mentine în continuare, adica, sistemul va ramâne în acea stare.

Dar, a garanta securitatea în întelesul prezentat anterior duce la o utilizare improprie a sistemului. Definitiile modelului de securitate reduc conceptul de securitate la câteva proprietati. Drept consecinta, chiar si sistemul cu gradul de securitate cel mai înalt, conform acestor criterii, nu poate fi privit ca sigur în sensul general. De altfel, s-a demonstrat ca aceste sisteme pot fi infectate cu virusi.

Metodele existente pentru detectarea infectarii cu virusi care se bazeaza pe observarea utilizarii sistemului în conditii anormale, care nu tin seama de vulnerabilitatea sistemului, nu garanteaza securitatea.

Reguli ale sistemelor expert ridica probabilitatea detectiei atât a virusilor cunoscuti (vechi) cât si a celor necunoscuti (noi) sistemului expert. lipsa consideratiilor de integritate constituie unul din motivele incapacitatii programelor antivirus de a preveni infectarea de produse soft antivirus.

De cele mai multe ori, aspectele de integritate si mecanismele de control ale integritatii lipsesc.
Listele privind controlul accesului, care stocheaza si programele accesate, pot preveni o modificare ilegala a programului. Astfel de mecanisme sunt rar implementate. Prin urmare, desi a fost recunoscuta ca fiind o amenintare de prim rang, infectarea cu virusi nu poate fi prevenita de sistemele ,,sigure".

3. Software antivirus

Deseori, utilizatorul se confrunta cu problema virusilor informatici, care au putut fi introdusi în calculator fie de pe o discheta, de pe un CD sau din Internet.
Pâna când virusul nu se manifesta prin scrierea unui mesaj, prin compromiterea unui fisier, prin încetinirea activitatii calculatorului sau pur si simplu, calculatorul nu mai merge, este greu de detectat prezenta unui virus.
Totusi, unii virusi furnizeaza câteva elemente pe baza carora pot fi descoperiti precum:
- schimbarea dimensiunii fisierului sau a datei de creare a acestuia;
- cresterea duratei de încarcare a programului;
- un program nu mai începe sa ruleze;
- o activitate neobisnuit de mare a harddiscului sau a dischetei;

Utilizarea instrumentelor antivirus usureaza activitatea de detectare si eliminare a virusilor.
Exista mai multe software-uri antivirus care folosesc tehnologii diferite. Cel mai obisnuit tip este scanner-ul. Acesta examineaza fisierele de pe discul specificat, încercând sa identifice ,,semnaturile" virusilor cunoscuti. Fiecare virus are o unica semnatura, care este un sir de instructiuni. Din pacate, virusii noi, ale caror semnaturi n-au fost incluse în baza de semnaturi a antivirusului, nu pot fi descoperiti.
Alte tipuri de instrumente antivirus sunt cele care includ programele prezente continuu în memoria RAM sau cele care se executa de fiecare data când se deschide calculatorul.

4. Dimensiunea pagubelor

Au existat preocupari de a cuantifica pagubele produse de virusi. Nu au fost însa efectuate încercari de a cuantifica libertatea utilizatorului, neîncrederea si alte neajunsuri mai putin tangibile.
Au fost elaborate modele matematice (Tippett '91) pentru raspândirea virusilor în comunitatea informatica. Acesta porneste de la trei ipoteze:
1). virusii nu au defecte, sunt perfecti;
2). majoritatea calculatoarelor nu au ,,anticorpi" pentru virusi;
3). copierea virusilor este un proces binar.
Pe baza acestor ipoteze, a fost creata formula dezvoltarii populatiei de virusi, care prezinta o crestere exponentiala. Astfel s-au estimat aceste pagube la 1,25 miliarde de dolari pe 4–5 ani, daca numai 10% din PC-uri sunt infectati cu virusi.
Acest model nu a fost înca acceptat de majoritatea informaticienilor.
Astfel Skulason (1992) a aratat ca prin raspândirea larga a antivirusului inventat de el în Islanda, pentru o perioada de timp nu au mai fost înregistrati virusi.
Se poate considera ca desi ipotezele lui Tippett sunt corecte, concluziile sunt false. Astfel, populatia de virusi creste exponential numai la început, urmând apoi o saturatie sau cel putin o perioada cu o crestere liniara, când este mai dificil pentru virus sa gaseasca un PC neinfectat.
Scanarea si alte metode antivirus vor coborî nivelul de saturare, prin urmare existând sansa coborârii numarul de PC-uri infectate.
Astfel, ipoteza ca procesul de copiere al virusilor este binar pare incorecta, neexistând o intercomunicativitate omogena între calculatoare. În general, virusii se localizeaza la un anumit grup de calculatoare si prin urmare procesul de infectare este limitat.

Desi amenintarea virusilor nu este asa de puternica ca cea descrisa de Tippett, aceasta amenintare trebuie luata în serios. Miile de virusi care exista si sunt creati zilnic, din care 20% sunt deosebiti de rai, scaderea eficientei antivirusilor (astfel se înmultesc programele antivirus precum un singur virus) fac ca activitatea cercetatorilor din centrele antivirus (AV) sa fie foarte intensa.

5. Raspunderea juridica pentru prejudiciile cauzate de virusi

În ansamblul masurilor de securitate aplicate sistemelor de calcul nu trebuie neglijate masurile juridice, cu deosebire institutia raspunderii (penale, administrative, civile).

Cu referire la raspunderea civila pentru prejudiciile cauzate de virusii informatici, aceasta poate fi angajata pentru repararea pagubelor cauzate utilizatorilor în sarcina persoanelor responsabile.

Mentionam ca normele civile nu cuprind dispozitii exprese cu privire la prejudiciile cauzate de virusi, dar sunt perfect aplicabile regulile dreptului comun. Astfel, potrivit art. 998 Cod Civil, ,,orice fapta a omului care cauzeaza altuia prejudicii, obliga pe cel din a carui greseala s-a ocazionat, a-l repara". Este limpede ca sub incidenta acestui articol intra si toate categoriile de fapte cauzatoare de prejudicii prin virusi (elaborarea de virusi, propagarea, atacul etc.).

O problema de interes teoretic si practic în materie priveste domeniul persoanelor a caror responsabilitate civila ar putea fi angajata.

O prima categorie de acest fel o constituie autorul virusului (în masura în care aceasta calitate poate fi dovedita) daca se probeaza ca acesta a facut sa se propage în mediu informatic acel virus.

Responsabilitatea sa va fi solidara cu a celor care au raspândit din culpa virusul ori care au încalcat sau împiedicat sa functioneze masurile si sistemele de protectie.

Raspunderea juridica civila poate îmbraca nu numai forma raspunderii pentru fapta proprie, ci si forma raspunderii pentru fapta altei persoane ori a raspunderii pentru fapta lucrului în general sau a raspunderii contractuale.

Astfel, vor putea fi chemate sa raspunda pentru altul:

a. parintele pentru fapta prejudiciabila a copilului minor;

b. profesorul pentru fapta prejudiciabila a elevului aflat sub supravegherea sa (spre exemplu atunci când la cursurile de informatica elevii infecteaza si scot din functiune calculatoarele sau reteaua liceului ori a altor institutii prin atacuri cu virusi);

c. societatea comerciala sau institutia pentru faptele angajatilor (ca raspundere a comitetului, precum în ipoteza vânzarii de calculatoare cu soft preinstalat infectat);

d. proprietarul calculatorului sau retelei utilizate de un client, cu scop distructiv (precum cafenelele cu acces la Internet), ca raspundere pentru fapta lucrului.

e. Persoana fizica sau juridica, care în temeiul unui contract îsi asuma sarcina asigurarii securitatii sistemului informatic sau al retelei si nu îndeplineste aceasta obligatie.

Toate aceste categorii de persoane responsabile vor putea invoca existenta unei cauze de exonerare de raspundere, în conditiile legii.

Cu tot acest larg domeniu de aplicatie al raspunderii pentru prejudiciul cauzat de virusi ea este rareori utilizata în practica.

6. Concluzii

Desi multe tari occidentale au legi care protejeaza proprietatea de toate formele, pare dificila aplicarea acestor legi la calculatoare. În unele tari, informatia nu este considerata proprietate si prin urmare nu este protejata de lege.

În alte cazuri, tribunalele vad atacul la persoana sau la o institutie pe Internet ca nepedepsibila, deoarece conceptul este

prea abstract. Înca nu exista legi în care se face distinctia între program si date.
În Germania, numai virusii care distrug date sau modifica programul infectat constituie un act ilegal, nespecificând daca autorul virusului raspunde pentru actiunea virusului când iese de sub control. De altfel nu exista înca nici un fel de caz pedepsit în tribunal (Biba, 1997).
Încercarea de introducere în S.U.A a legii federale ,,Computer Virus Eradication Act" a fost respinsa (1995), motivându-se ca virusul este o forma de manifestare a personalitatii si , deci nu poate fi limitata.
Prin urmare, legislatia speciala împotriva autorilor de virusi informatici si a raspunderii constiente a acestora, înca se lasa asteptata. Pâna atunci este pe deplin dreptul comun, cu deosebire raspunderea civila delictuala.

Bibliografie

Anderson R.E., Denning P. ,,ACM code of etichs and profesional conduct", Computer security, oct. 1997.
1. Bell D.E., ,,Secure Computer Systems", Mitre Corporation, Bedford, Mass, 1993.
2. Biba K.J., ,,Integrity Considerations for Secure Computer System", USAF, Bedford, Mass, 1987.
3. Bontchev , ,,The Bulgarian and soviet virus factories", Proceedings of the First International Virus Conference, Jersey, UK, 1997.
4. Skulason T., ,,Antivirus in Island", Proceeding of ACM Society, 1992.
5. Tippett A., ,,Matemathical Model for Virus Population", Willey, 1991.
6. Toma M., Stan E., ,,Consideratii juridice privind virusii informatici", "Comsec", AThM, 1994.
7. Ivan I., Nosca Ghe., Tcaciuc S., Pârlog O., Caciula R., ,,Calitatea datelor", Inforec, 1999.