Informatica în lume

ARMELE JURIDICE CONTRA VIRUȘILOR

Raportul privind securitatea informatică, redactat de "Copmisia informatică" a Cigref (Club Informatique des Grandes Entreprises Françaises) a constatat că "sabotajul în domeniul software devine un risc care trebuie să preocupe, fiind în continuă creștere și avînd consecințe din ce în ce mai grave."

De asemenea, raportul recomandă "integrarea securității informatice și protecția împotriva contaminărilor în strategia globală de securitate, luînd în considerare în schema directoare a microinformaticii, utilizarea de produse antivirus ca mijloace preventive pentru diagnosticarea/tratarea contaminărilor și crearea unei structuri care să permită întreprinderilor de a fi informate cu privire la amenințările de tip contaminări și instrumentele asociate."

Cigref recomandă întreprinderilor și direcțiilor lor generale (a căror implicare este esențială) punerea în aplicare a tuturor mijloacelor de organizare, juridice și tehnice, stabilind raportul optim între eficacitatea mijloacelor utilizate și constrîngerile impuse utilizatorului (pierderi de performanțe, costuri).

Din punct de vedere juridic, întreprinderea victimă poate urmări în justiție pe autorul unui program-virus, atît în plan civil, cît și în plan penal. Conform Codului civil, o acțiune civilă are în vedere "orice faptă a unui individ care îi cauzează altuia un prejudiciu, îl obligă pe păgubitor la repararea stricăciunilor (cf. art. 1382 din Codul civil). Este și în cazul virusului informatic, deoarece acesta este creația intelectuală a omului, avînd tocmai destinația de a provoca un prejudiciu. Mai este necesar ca victima să identifice pe autorul virusului și să dovedească actul vinovat, prejudiciul adus și legătura de cauzalitate dintre cele două elemente. În toate cazurile în care autorul nu va putea fi identificat sau virusul va putea fi detectat chiar înainte ca acesta să producă pagube, punerea în aplicare a responsabilității civile va fi imposibilă.

Începînd din 1988, Codul penal permite victimei să acționeze pe teren penal, sancționînd orice atingeri, directe sau indirecte, aduse sistemului de prelucrare automată de date (Legea 88-19 din 05.01.1988).

Calea penală prezintă mai multe avantaje: pe de o parte, faza de instrucție procură facilități în dovedirea fraudei, victima profitînd de mijloacele represive de care dispun judecătorii pentru a clarifica o afacere (mijloace reunite de dovedire, percheziții, sechestrări....); pe de altă parte, responsabilitatea penală va putea fi angajată, chiar dacă nu s-a produs nici o pagubă, tentativa fiind sancționată cu aceleași pedepse ca și fapta, în vreme ce responsabilitatea civilă nu intră în vigoare decît dacă prejudiciul este dovedit. Astfel, oricare ar fi prejudiciul cauzat, chiar dacă victima nu a luat nici o măsură de securitate, sancțiunile cele mai grele au drept scop reprimarea simplei tentative de "injectare" a virusului, ca și simpla participare la o contaminare.

Pe de altă parte, prin acțiunea penală există pentru victimă riscurile de a se vedea reclamînd o reparație în caz de neurmărire și de a nu putea fi audiată ca martoră la instrucție ca și la dezbateri, fapt ce ar putea fi jenant, mai ales dacă victima este singurul martor.

Textul represiv al legii vizează orice atingeri aduse sistemelor de prelucrare automată a datelor. Articolul 462-4 al Codului penal definește pe larg sistemele informatice, protejînd, de asemenea, software-urile, datele, rețelele și tot ceea ce poate fi alterat sau distrus de un virus. În acest sens, sînt penalizate accesul și întreținerea frauduloasă, atît a sistemului în întregime, cît și numai a unei părți din acesta (Art. 462-2 din Codul penal), împiedicarea în mod voluntar a funcționării unui sistem (Art. 462-3 din Codul penal), prejudicierea datelor ca și a rețelelor (Art. 462-7 din Codul penal), textul legii avînd în vedere orice modificare intervenită, atît în modul de prelucrare, cît și în modul de transmisie.

Virusul, care se caracterizează prin modul său de reproducere și prin efectul său distrugător, este vizat în mod direct, fie că se mulțumește să înregistreze cheile de acces, că împiedică utilizarea programelor de aplicație sau sistemul de afișare a datelor sau, mai grav, că merge pînă la distrugerea a întregi blocuri de date, de programe sau de module de sistem, fie că se afectează chiar sectorul de inițializare de date sau că se poate ajunge pînă la cumul de atacuri diferite.

Nu se poate invoca aici scuza de legitimă apărare pentru a scăpa de urmărirea penală, programul-virus neputînd fi considerat ca o măsură de apărare proporțională unui atac injust. Obiectivul, pe de o parte, nu este defensiv, deoarece virusul, care nu se limitează să asigure protecția unui program contra unei eventuale agresiuni, va perturba funcționarea aplicațiilor, fără a fi fost declanșat de comportamentul dezordonat al utilizatorului. Pe de altă parte, agresiunea se vădește disproporționată, fiind imposibil de stăpînit. Prejudiciul nu se limitează la un program, el afectînd mai multe aplicații, reproducîndu-se în lanț în alte programe, va atinge sistemul de exploatare, putînd declanșa procese de distrugere a discului fix.

Legea din 1988 are în vedere trei niveluri de sancțiuni, în funcție de gravitatea prejudiciului cauzat și de caracterul voluntar sau involuntar al actului. Accesul sau întreținerea frauduloasă a sistemului, căruia i s-au adus în mod voluntar prejudicii justifică acordarea celor mai grele pedepse.

Această fraudă "supra-agravată" va fi, astfel, sancționată cu pedepse cu închisoarea (de la 3 luni la 3 ani) și cu amendă între 10000 și 100000 FF. (Art. 462-3 din Codul penal) sau de la 2000 la 500000 FF. (Art. 462-4 din Codul penal), în cazul modificării modului de transmisie sau de prelucrare și de prejudiciere a datelor, fie că este vorba de suprimare (ștergere), introducere sau modificare.

Se are în vedere, de asemenea, repararea prejudiciului suportat de victimă, pagubă ce poate avea o valoare considerabilă.
Pentru creşterea eficienţei, legea adaugă şi cîteva protecţii. Pedepsele se aplică, indiferent dacă delictul a fost complet sau nu dus la îndeplinire sau a rămas la stadiul de tentativă (Art. 462-7 din Codul penal), prevedere care permite urmărirea penală, atît numai a tentativei de contaminare a sistemului cu virus, chiar dacă nu a fost dusă la îndeplinire, cît şi de "injectare" a virusului care nu şi-a făcut încă efectul fiind detectat la timp, chiar dacă nici un prejudiciu nu a fost cauzat încă.
Preventiv şi pentru a asigura securitatea, sancţiunile se aplică, atît celor care au comis delictul, cît şi celor care s-au înţeles să participe la realizarea acestuia (Art. 462-8 din Codul penal). Înţelegerea va fi sancţionată cu aceeaşi pedeapsă ca delictul principal, şi în caz de concurs de împrejurări de infracţiuni, cu pedeapsa pentru delictul cel mai grav. Aceasta permite urmărirea în justiţie şi a celui care s-a lăsat convins să sprijine introducerea virusului în sistemul victimei.
Legea vizează protecţia tuturor sistemelor care sînt sau nu dotate cu un dispozitiv de securitate. Actele de sabotaj, prin "injectarea" de virus sau prin alte mijloace, contra sistemelor neprotejate sînt, de asemenea, reprimate pe cale penală.
Legea nu impune, din păcate, în mod expres instalarea de mijloace tehnice preventive , numai dreptul penal venind să compenseze slaba protejare a întreprinderilor, motiv pentru care responsabilii acestora nu se grăbesc să investească într-o politică de securitate.
Anumite precauţii elementare, un plan de securitate se dovedesc utile în practică, în lupta contra virusilor: salvarea regulată a datelor pe discuri fixe, conservarea a cel puţin două seturi de salvare, controlarea software-urilor care provin din afara întreprinderii şi testarea acestora pe un post izolat, formatarea dischetelor de utilizare, verificarea taliei fişierelor, controlarea accesului altor persoane, sînt consemne recomandate de Cigref pe care toate întreprinderile ar trebui să le respecte, chiar dacă nu există o metodă imparabilă de depistare a virusilor.
Aceste măsuri sînt cu atît mai necesare, cu cît existenţa sau absenţa dispozitivelor de securitate nu vor fi indiferente judecătorilor în caz de litigiu, spiritul legii legînd realizarea delictului informatic de existenţa unei protecţii suficiente a sistemului.
Dezbaterile parlamentare din Franţa de elaborare a textului legii din 1988 o dovedesc, chiar dacă textul definitiv nu a reluat în mod expres această condiţie numai cu scopul de a sancţiona toate acţiunile frauduloase, inclusiv cele comise împotriva serviciilor destinate publicului.
Van Dorsselaere, B. - Les armes juridiques contre les virus; în: Distributique, nr.96, februarie 1992, pp.86-88.

Traducere:
Victoria Haiduc