ANALELE ŞTIINȚIFICE ALE UNIVERSITĂȚII „AL.I.CUZA" IAŞI
Tomul LII, Ştiințe Juridice, 2006

UNELE ASPECTE DE ORDIN CRIMINOLOGIC PRIVIND INFRACTORUL INFORMATIC

DANIEL ATASIEI

În studiile de specialitate se apreciază că fenomenul criminalității informatice poate fi explicat prin conjunctura a trei factori: *motivație, oportunitatea comiterii crimei* şi *lipsa „pazei" din partea victimei*[1].

Motivațiile criminalului informatic vor face obiectul unei analize în prezentul studiu, în vreme ce *oportunitatea* şi *lipsa „pazei"* pot face obiectul unei alte discuții referitoare la tema mai largă a prevenirii criminalității informatice, a mijloacelor de realizare a acestei prevenții.

Motivațiile atacului informatic sunt dintre cele mai diverse, sunt diferite în raport cu natura infracțiunii informatice comise şi pot consta în: lăcomie, dorința de putere, răzbunarea, încercarea limitelor sau spiritul de aventură, dorința de a gusta din fructul "oprit"[2].

Posibilitatea pentru un singur individ de a controla, prin intermediul unui sistem informatic, o mare instituție sau organizație reprezintă un act de forță, de putere şi poate reprezenta, prin el însuşi, o satisfacție personală a infractorului.

Dorința de a provoca pagube altuia, de a distruge poate izvorî din dorința de răzbunare, din invidie, ură ş.a. Alteori publicitatea în jurul actelor criminale săvârşite în spațiul cibernetic, condamnarea lor publică, doza de mirare şi admirație cu care unele articole de presă prezintă atacuri „îndrăznețe" constituie – pentru alții – un alt motiv pentru continuarea activităților infracționale.

Aceste mobiluri nu sunt nici noi şi nici asociate doar unui anumit tip de comportament criminal. Noutatea rezidă doar în capacitatea impresionantă a noilor tehnologii de a facilita comiterea unor acte infracționale.

Atacurile de natură informatică asupra sistemelor computerizate sunt clasificate, în raport cu poziția atacatorului, în atacuri *interne* şi atacuri *din exterior*.

---

[1] Peter Grabosky, *Computer Crime: A Criminological Overview*, studiu pregătit în vederea prezentării în cadrul workshopului asupra Infracțiunilor comise cu ajutorul calculatorului în cadrul celui de-al X-lea Congres O.N.U. asupra prevenirii infracțiunilor şi tratamentului infractorilor, Viena, 15.04.2000, disponibil pe www.aic.gov.au/conferences/ other/grabosky peter/2000-04-vienna.html accesat la 01.03.2005.

[2] *Ibidem*.

Pentru o bună perioadă de timp s-a apreciat – pe baza rapoartelor şi supravegherilor efectuate de instituţii specializate în prevenirea atacurilor informatice sau de companiile de securitate informatică – că majoritatea atacurilor vizând sistemele informatice provin de la persoane din interiorul companiilor sau care au lucrat în interiorul acestora având acces la sistemele informatice şi la sistemele de securitate.

Rapoartele întocmite pentru anul 2004 arată însă o uşoară modificare, o scădere a atacurilor din interior şi o echilibrare – ca număr – cu cele provenind din exterior (hackeri).

Pentru prezenta lucrare am avut în vedere trei rapoarte publicate în anul 2005 întocmite de instituţii şi companii recunoscute pentru profesionalism, rapoarte care acoperă însă regiuni diferite ale globului: **IC3 2004 - Internet Crime Fraud Report (1 ianuarie 2004 - 31 decembrie 2004)**[3]**, Information Security Breaches Survey 2004 (PriceWaterhouse Coopers)**[4] **şi Global Information Security Survey 2004** [5]**.**

În studiul realizat de Ernst & Young în anul 2004, fiind întrebaţi cu privire Ia sursa vulnerabilităţii lor informatice, majoritatea repondenţilor au pus pe prima poziţie agresiunile venite din exteriorul companiei (hackeri), aceste atacuri ocupând un loc central în preocupările de securitate ale marilor companii timp de ani buni.

Tendinţa ultimilor ani arată însă că numărul atacurilor interne este mult mai mare decât cel înregistrat de statistici şi, pe departe, mult mai păguboase pentru companii decât atacurile venite din exterior. E vorba de utilizatorii legitimi ai sistemelor informatice, de cele mai multe ori fiind vorba de chiar angajaţi ai companiilor sau instituţiilor vizate. Pe măsură ce organizaţiile permit un mai mare acces la informaţiile deţinute, riscurile de securitate informatică cresc exponenţial cu numărul de persoane ce capătă acest acces.

În plus, atacatorii din interior acţionează în condiţiile unui risc minim de detecţie a faptelor lor, prezenţa lor în sistem fiind una plauzibilă, fără a crea suspiciuni. Există de asemenea posibilitatea ca infractorul informatic din interior să săvârşească faptele neintenţionat, să producă pagube din ignoranţă sau neglijenţă[6].

---

[3] Raport anual întocmit de Centrul Naţional privind Criminalitatea „gulerelor albe" şi F.B.I. (S.U.A.) disponibil la adresa www.ifccfbi.gov/strategy/2004_IC3Report.pdf accesată la 0l.03.2005.

[4] Raport anual întocmit de compania PriceWaterhouseCoopers pentru Marea Britanie, disponibil la adresa de internet: www.security-survey.gov.uk accesat la 01.03.2005.

[5] Raport anual întocmit de compania Ernts & Young disponibil la adresa www.ev.com/globalsecuritysurvev accesată la data de 01.03.2005.

[6] Global Information Security Survey E&Y, *op.cit.*, f. 13.

Periculozitatea crescută a atacurilor generate de proprii angajați este datorată împrejurării că aceşti angajați au, de regulă, cunoştințe aprofundate despre arhitectura sistemului de securitate informatică şi pot desfăşura cu mult mai multă uşurință decât hackerii operațiuni interzise (fraude, furt de informații, ştergere sau degradare de date informatice, sabotaj). Mai mult, experiența Poliției italiene arată că mult mai periculoase sunt şi atacurile din exterior atunci când există complicitatea unui angajat din interiorul companiei[7].

Atacurile din interior reprezintă au problematică deosebită, dificilă, urmare a trăsăturilor pe care le presupune un asemenea atac. Un studiu de specialitate[8] arată că principalele caracteristici ale atacului din interior sunt:

1. o foarte mare incidență în rândul infracțiunilor informatice (70-80% din numărul total al atacurilor informatice);
2. dificultatea obiectivă de identificare a autorului;
3. consecințe importante pentru organizația atacată, dar şi pentru autor;
4. determinare insuficientă pentru luarea de contramăsuri;
5. factorul uman constituie principalul factor de risc.

Principalul factor de risc intern îl constituie persoanele a căror sarcină în interiorul organizației este tocmai acela de a se ocupa de designul, întreținerea şi operarea sistemelor informatice.

Studiile efectuate pe tema criminalității informatice, în special cele care s-au centrat pe problema criminalității din interiorul organizațiilor au concluzionat că problema atacurilor interne există, constituie o problemă reală ale cărei dimensiuni sunt încă puțin descoperite şi analizate. Se vorbeşte chiar despre cunoaşterea doar unei părți infirme din amploarea fenomenului, doar a vârfului icebergului. Acest lucru de datorează mai multor împrejurări, una dintre cele mai importante piedici în descoperirea tuturor acestor acte o constituie atitudinea managerilor sau a celorlalți conducători ai instituțiilor care preferă să rezolve asemenea probleme în mod rapid, fără a crea vâlvă, "în linişte", pentru a evita impactul publicității negative asupra organizației.

În aceste condiții, cei descoperiți ca şi comițând asemenea acte pleacă "în linişte" în altă parte fără a fi implicată poliția sau vreo altă instituție specializată, fără a exista un cazier sau alte referințe negative odată cu angajarea la noul loc de muncă. Se mai adaugă şi o oarecare superficialitate a angajatorului de a verifica trecutul profesional al unui nou angajat.

---

[7] Marco Strano, *Inside Attack: what prevention?*, articol publicat în Telematic Journal of Clinical Criminology, 2004 – www.criminologia.org accesat la 01.03.2005.

[8] Fabio Batelli, Roberta Bruzzone, *Prinicpali caratteristiche dell'attacco "inside"* în Telematic Journal of Clinical Criminoogy, iunie 2004, www.criminologia.org accesat la 01.03.2005.

La fel ca şi în situaţia atacurilor externe, şi la cele interne motivaţiile criminale sunt cele mai diverse. Astfel, unele acte de sabotaj sau de şantaj au fost comise de foşti angajaţi nemulţumiţi de concedierea lor, de transferul acestora sau de diminuări salariale. În alte cazuri, motivaţiile angajaţilor ţin de lăcomie, de urmărirea unor câştiguri financiare în mod ilegal profitând de poziţia pe care o ocupă în sânul organizaţiei şi de accesul pe care această poziţie îl conferă la sistemele informatice. Alţi făptuitori comit faptele în scop de spionaj, de furt de informaţii - fiind denumiţi "cârtiţe".

Un raport al Institutului de Securitate Informatică al S.U.A.[9] realizat în anul 1998 arăta că în urma unui atac extern costurile se ridică în medie la 56.000 $, în vreme ce atacul intern costă companiile în medie 2.700.000 $[10].

În mod paradoxal deşi atacurile interne sunt numeroase şi creează prejudicii însemnate, studiile de specialitate referitoare la aceste atacuri sunt puţine la număr iar conducerile companiilor s-au orientat în efectuarea de investiţii privind sisteme de securitate informatică care să protejeze faţă de atacurile din exterior.

Dintre cei din interior, care în mod obişnuit au acces la sistemele informatice ale unei organizaţii, prezintă interes criminologie în special acei specialişti care au drept sarcină să proiecteze, să menţină sau să opereze sistemele de securitate informatică. Acest interes criminologie – ca potenţial grup de comitere a infracţiunilor informatice din interior – este justificat de împrejurarea că aceste persoane au cunoştinţele necesare pentru a putea conduce un asemenea atac şi, de asemenea, prin natura poziţiei lor, au acces (legitim) la date informatice importante.

Nu doar angajaţii sunt incluşi în categoria de mai sus (angajaţii pe baza unui contract de muncă), dar şi alte categorii de persoane care pe o perioadă mai scurtă sau mai mare de timp au acces la sistemele informatice ale organizaţiei din interiorul acestora: subcontracori, consultanţi, angajaţi temporari, foşti angajaţi.

Angajaţii companiei (cu normă întreagă sau cu jumătate de normă) prezintă de regulă cel mai mare risc din punct de vedere al atacurilor din interior. Ca parte stabilă a personalului unei organizaţii, angajatul se bucură de încrederea celor din jur, se consideră că are interesul ca firma la care este angajat să prospere, să aibă o bună productivitate. De aceea, în situaţia proastei funcţionări a sistemelor informatice proprii angajaţi ai organizaţiei sunt puşi în afara vreunei suspiciuni.

---

[9] The Computer Security Institute – http://www.gocsi.com/.

[10] Studiul a fost citat în articolul *The Insider Threat to Information Systems – The Psychology of Dangerous Insider*, Eric Saw, Keven Ruby, Jerrold Post – www.pol-psych.com/sab.pdf – publicat iniţial în Security Awareness Bulletin 2/1998.

Cercetarea cazurilor în care proprii angajați au produs pagube companiei prin utilizarea din interior a sistemelor informatice a dus la concluzia că motivațiile ce au stat la baza actelor lor au fost diverse incluzând lăcomia, dorința de răzbunare pentru pretinse nedreptăți, dorința de rezolvare a unor probleme personale, dorința de a ieşi in evidență, de a-şi proteja poziția sau de a avansa, dorința de a-şi testa priceperea, de a-şi manifesta mânia, de a-i impresiona pe alții[11].

Subcontractorii partenerii, consultanții şi angajații temporar deşi au acces la sistemele interne de securitate ale organizației, nu sunt supuşi aceluiaşi sistem de filtrare, de verificare ca în cazul angajaților permanenți. De regulă, anterior angajării unei persoane într-o companie marile firme realizează o verificare a situației anterioare a candidatului, a referințelor de la locurile de muncă anterioare, a situației cazierului judiciar. În cazul subcontractorilor, a partenerilor, consultanților sau a angajaților temporari asemenea verificări nu se realizează sau sunt superficiale. În cazul subcontractorilor, a companiilor partenere, verificarea personalului propriu cade în sarcina acestora, nefiind la îndemâna companiei beneficiare.

În plus, în raport de caracterul temporar al activității acestor categorii de specialişti nu se poate vorbi, spre deosebire de situația angajaților, nici măcar de acel minim sentiment de loialitate față de companie.

Practica unor companii de securitate americane (dar nu numai) de a angaja foşti hackeri prin prisma capacităților lor intelectuale nu face uneori decât să crească pericolul atacurilor interne[12] câtă vreme o persoană condamnată anterior pentru săvârşirea de infracțiuni informatice poate oricând recidiva.

Din categoria *foştilor angajați* fac parte persoane care au fost anterior angajate ale unei organizații şi care mai încă un acces la sistemele informatice ale acesteia, la informațiile deținute - fie direct, prin intermediul unor „portițe" create din timp în sistemul de securitate[13], fie indirect, prin intermediu! altor

[11] *The Insider Threat to Information Systems – The Psychology of Dangerous Insider*, Eric Saw, Keven Ruby, Jerrold Post – www.pol-psych.com/sab.pdf, publicat inițial în Security Awareness Bulletin 2/1998.

[12] E o modalitate de a "pune lupul paznic la oi" încredințând securitatea informatică unei persoane care anterior a fost condamnată/anchetată tocmai pentru penetrarea barierelor de securitate.

[13] Mici programe informatice denumite "backdoors" – "portițe din spate" care, odată implantate în sistemul informatic respectiv permit celui care deține "cheia" acestor portițe să acceseze din exterior sistemul informatic sau chiar să preia controlul total al acestuia. De regulă aceste "backdoor" sunt plantate de fostul angajat din timp, din perioada în care lucra la respectiva companie, ca măsură de siguranță personală.

persoane care în continuare lucrează în cadrul acelei companii (prietenei, foşti colegi de muncă ş.a.)[14].

Studiile de specialitate au arătat că există o serie de trăsături comune specialiştilor în informatică, persoane care sunt de regulă foarte vulnerabile tulburărilor emoționale, dezamăgirii, nemulțumirilor personale, toate acestea afectând capacitatea de rațiune şi control a individului, sporind riscul comiterii de infracțiuni informatice[15]. Aceste cercetări efectuate pe plan internațional au mai arătat că introducerea pe scară largă a tehnologiilor informației a influențat sistemul cognitiv al individului care a suferit adevărate alterări ale percepției, alterări ce pot interfera, în diferite modalități şi la diferite nivele cu nivelul de cunoaştere şi cu sistemul cognitiv complex care dirijează conduita persoanei[16].

Caracteristicile comune care sporesc riscul activităților infracționale din interior includ *dependența de computer, o antecedență de frustrări personale şi sociale, o "flexibilitate" etică*, un amalgam de lipsă loialitate, sentiment de îndreptățire şi lipsă de compasiune. *Dependența de calculator* include două categorii distincte de persoane: dependența manifestată prin ataşamentul de sistemul informatic în sine şi dependența manifestată de activitatea on-line permisă de rețelele de calculatoare (de exemplu, internetul).

Cei din prima categorie – dependenți de calculator - manifestă un interese deosebit în explorarea sistemelor informatice şi a rețelelor şi percep spargerea parolelor sau codurilor ca o modalitate onorabilă de stimulare intelectuală punându-i la încercare pe specialiştii în securitate informatică care au creat acele sisteme de securitate.

Cei din a doua categorie – dependenții de activitatea on-line – sunt descrişi de studiile de specialitate ca persoane care petrec multe ore în fața calculatoarelor, de multe ori pierzând noțiune timpului, aceste activități on-line interferând semnificativ cu viețile lor personale. E vorba de cei implicați în

[14] Donald Burleson, un programator la compania USPA& IRA Co., o companie de securitate informatică, după ce a fost concediat pe motiv că folosea calculatoarele companiei în interes personal, a creat un virus care avea drept efect ştergerea unei părți semnificative din platforma companiei, urmând ca operațiunea să se repete de la sine, cu altă parte a platformei informatice dacă o anumită valoare predeterminată nu ar fi fost introdusă în sistem până la o dată limită. Folosind un duplicat al cheilor de acces, făptuitorul a intrat în clădirea companiei şi, cu ajutorul unui program de tip "backdoor" a depăşit sistemele de securitate informatică, a accesat calculatoarele şi a instalat şi rulat virusul în cauză.

[15] *The Insider Threat to Information Systems - The Psychology of Dangerous Insider*, Eric Saw, Keven Ruby, Jerrold Post – www.pol-psych.com/sab.pdf, publicat inițial în Security Awareness Bulletin 2/1998.

[16] Fabio Batelli, Roberta Bruzzone, *op. cit.*

relații mediate de prezența calculatorului în special prin intermediul grupurilor de chat (discuții) sau a jocurilor on-line.

Majoritatea persoanelor în cauză sunt introvertite, cu puține aptitudini de interacțiune socială, care găsesc în calculator o modalitate de a interacționa cu alte persoane îmbrățișând aceleași interese, totul petrecându-se nu în mod direct, ci indirect, la adăpostul anonimatului și siguranței oferite de sistemul informatic. Asemenea persoane ajung să trăiască o viață virtuală, să împărtășească emoții și sentimente în mediul virtual într-o manieră pe care nu ar reuși-o în lumea reală, materială.

Antecedența frustrărilor sociale și personale este o altă trăsătură des întâlnită în rândul infractorilor informatici ce acționează din interior. E vorba de frustrări determinate de conflicte în familie, în grupul de prieteni sau chiar la locul de muncă. De regulă aceste persoane preferă o viață bine organizată, predictibilă, preferă mai mult compania calculatorului decât acea a semenilor, au mai dificultăți în a interacționa social, tind să fie izolați. Aceste trăsături accentuează vulnerabilitatea lor emoțională, sentimentul de însingurare, nemulțumirea și dezamăgirea în legătură cu activitatea desfășurată la locul de muncă. Aceste persoane sunt mai puțin predispuse a discuta nemulțumirile sau orice altă problemă cu superiorii, manifestând și dezvoltând o neîncredere față de aceștia și în general, față de autoritate. în egală măsură aceleași trăsături accentuează și vulnerabilitate față de recrutarea sau manipularea din partea unor atacatori externi. Tehnologia informațiilor a adus cu sine și un impact asupra limitelor *etice* ale persoanei. Deși reprobabile și condamnabile din punct de vedere moral atunci când se petrec în lumea reală, unele activități (sustragere de bunuri, date și informații, violarea corespondenței, spargerea și pătrunderea într-un sistem ș.a.) devin mai "acceptabile" când se petrec în spațiul virtual.

La această "flexibilitate" etică contribuie, potrivit studiilor realizate de specialiști, lipsa unei pregătiri speciale privind lucrul cu calculatorul, a unor reguli clare privind limitele acestei utilizări, lipsa unei educații corespunzătoare din familie sau din școală.

De asemenea lipsa unor limite vizibile, stabilite a spațiului virtual, lipsa unui contact față în față cu potențiala victimă influențează atitudinea infractorului informatic și diminuează percepția rezultatelor dăunătoare pe care acesta le generează.

Aceiași autori[17] apreciază că la erodarea standardelor etice a contribuit chiar industria calculatoarelor fie prin introducerea unor bariere ultraprotective în materia achiziționării de programe software, fie chiar prin angajarea hackerilor și încercarea de transformare a acestora din agresori ai sistemelor informatice în specialiști în securitate informatică.

[17] *Ibidem.*

Loialitatea redusă poate favoriza comiterea de infracțiuni informatice din interiorul companiilor. În privința specialiștilor IT s-au conturat două grupuri: cei care se identifică cu organizația care i-a angajat (existând o loialitate față de interesele acesteia) şi cei care se identifică cu însăşi profesia de programatori informatici, loialitatea față de organizație fiind mult redusă. Această ultimă categorie de persoane este cea mai expusă comiterii de infracțiuni informatice, trecerea la comiterea actelor ilicite putând avea loc şi pe fundalul ambiguităților legate de drepturile de proprietate intelectuală asupra codurilor-sursă sau a programelor informatice dezvoltate.

Lipsa de loialitate este adesea însoțită şi de manifestarea unei atitudini de persoană *îndreptățită la un tratament special, preferențial* în raport cu alte categorii de angajați. Această atitudine derivă din credința specialistului IT, asociată deseori unei personalități narcisiste, că ea este o persoană specială şi că i se datorează recunoaşterea acestei calități, recunoaşterea unor privilegii şi a unui tratament privilegiat. Uneori chiar staff-ul companiilor acceptă un tratament diferit al unor specialişti IT, acceptă că sunt puțin diferiți față de angajatul obişnuit şi fac excepții de la regulile ce sunt impuse şi ar trebui respectate de toți angajații.

Nerecunoaşterea unui asemenea statut "special" din partea conducerii companiei poate genera o atitudine de furie față de conducere şi față de ideea de autoritate, crearea unui sentiment de nedreptate şi încurajarea ideii de "răzbunare" tradusă în comiterea de acte infracționale.

Lipsa de compasiune şi înțelegere este o alta trăsătură ce caracterizează atacatorul intern. Studiile de specialitate au arătat că această lipsă de înțelegere şi compasiune este mult mai mare în cazul infracțiunilor comise în ciberspațiu față de cele comise în lumea reală, infractorul informatic fiind incapabil a percepe impactul negativ al faptei sale, este incapabil a se pune în locul victimei sale. Această atitudine este susținută şi de caracterul impersonal al lumii virtuale, de anonimitatea oferită de rețelele informatice. Această "anonimitate" naşte sentimentul invincibilității: dacă pătrunderea într-o bancă în scopul jefuirii de bani presupune o asiduă pregătire a planurilor, procurarea de arme, de coduri de acces, riscul de a fi împuşcat, timp material pentru comiterea faptei, spargerea bazei de date şi transferarea aceloraşi sume de bani poate dura minute sau secunde şi absența tuturor riscurilor fizice pentru persoana atacatorului[18].

[18] *Studying the psychology of virus writers and hackers. An interview with researcher Sarah Gordon* interviu realizat în cadrul emisiunii "Frontline" ("Linia întâi") la televiziunea americană PBS, disponibil pe internet la adresa http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/psycho.html accesată la 01.03.2005.

- Abstract -

Cybercrime is the result of the conjunction of tree factors: motivation, opportunity and lack of guardianship. This article analyzes the motivation of computer criminals.

There are two types of attacks against computers – from the point of view of the position of the cybercriminal – the outsiders and the insiders. For a long period, it was considered that, the inside attacks were the majority of crimes, but recent studies have shown a relatively balanced position between inside and outside attacks.

The inside attack is more likely to be left unreported by the companies, who prefer to solve any "problem" inside, without the implication of police and justice authorities. This policy strongly relates with the image that a company has in the eyes of partners and clients, any major breach of security affecting this image. However, it looks like the companies prefer to adopt more drastic measures against exterior attacks, than to recognize and to take measures to prevent the inside attacks.

The inside attacker is more dangerous by the power he has, by the possibility of remaining undetected. His motivation is diverse: vengeance, sabotage, blackmail, greed, espionage, theft of information ("moles").

The inside attacker is not always an employee of that company. There are cases where disgruntled ex-employees commit cybercrimes. The subcontractors are also on the list of the potential computer criminals.

There are some characteristics of the insider that make him an potential cybercriminal against his company: computer dependency, prior personal and/or social frustrations, an ethical "flexibility", reduced loyalty, lack of compassion and understanding, all that in the context of the anonymity of internet activities.