ADRIAN MUNTEANU

ABOUT COMPUTER PRIVACY AND COMPUTER FRAUD IN ROMANIA

1. Introduction

In January 2001, a Romanian hacker has launched a major distributed denial of service (DDoS) forcing one of the largest IRC (*Internet Relay Chat*) networks, Undernet, to shut down much of its service. At that moment, Romania lacks the legal infrastructure to deal with those attacks and was placed on a black list because some e-commerce sites have made the decision to reject all buying orders, which originate from Romania.

In the last years, Romania was identified like a country where computers intrusion and computer related crime grows up.

In the IFCC 2001 Internet Fraud Report (January 1, 2001—December 31, 2001)[1] Romania was ranked fourth among the top 10 countries for Internet fraud. In the IFCC 2002 Internet Fraud Report[2] Romania was ranked the fifth but the percentage was 1.7 (See Table 1).

The Romanian Police official report for 2000-2002 state that was identified 465 related computer crime actions[3]. Until the end of 2002 Romania, unfortunately, does not have sufficient laws to fight Internet crime. In 2003, the situation is changed. There are few laws that require investigation and prosecution of computer crime.

Table no.1

Top Ten Country in 2001

Perpetrators	% of total perpetrators
United States	87.6
Nigeria	2.7
Canada	2.5
ROMANIA	**0.9**
United Kingdom	0.9
South Africa	0.5

An. Inst. cerc. cc. „Gh. Zane", t. 12, Iaşi, 2003, p. 97–102

Table no. 1 (continuare)

Australia	0.4
Indonesia	0.3
Togo	0.3
Russia	0.2

Source: IFCC 2001 Annual Report [1]

2. Computer privacy and personal information

The Law

At the end of 2001 a BBC news announce that European Parliament takes the necessary steps regard the use of cookies without the user consent. The European measures starts from the reality: Internet facilities and on-line services do not assure the privacy of the users.

Regulation like Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[4], UNCITRAL (*United Nations Commission on International Trade Law*)[5] recommendation on electronic commerce, Computer Fraud and Abuse Act[6] or Privacy Protection Act[7] (in USA) represent some of the international efforts made in this domain.

Starting from this, Romania is trying to adapt his legislation by taking measures at the national level regarding computer related crimes.

The Romanian Constitution state under Title II (*Fundamental Rights, Freedoms, and Duties*), Article 26 that "*(1) Public authorities shall respect and protect privacy, family and private life.*"

After 10 years, in November 2001, the Romanian Parliament enacted Law 676/2001 on the *Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector[8]*. This law ensures the specific conditions of guaranteeing the right to protection of privacy with regard to the processing of personal data in the telecommunications sector and applies to the operators of public telecommunications networks and the providers of publicly available telecommunications services.

Article 9 of this law state:

"(1) Traffic data related to subscribers and users, processed in order to establish the calls made and stored by the provider of a publicly available telecommunications service or by the operator of a public telecommunications

network must be erased or made anonymous upon the termination of the call, without prejudice to the provisions of paragraphs (2) to (4).

(2) Processing of data containing: the number or identification of subscriber's station, the address of the subscriber and the type of the station, the total number of units that have to be billed for the countering period, the number of the called subscriber, the type, the starting time and the duration of the calls effected or the volume of data transmitted, the date of call or service, other information relating to payments, such as the advance payments, payments for installing, disconnections and reminders, carried out for the purpose of subscriber billing or interconnection payments is permitted only within 3 years from the due date of the payment obligation corresponding to the invoice, respectively, from the due date of the payment obligation corresponding to the interconnection.

(3) The provider of a publicly available telecommunications service may process only the significant data referred to in paragraph (2) for the purpose of marketing or selling its own services, only with the notification of the subscriber and his express consent

Even if Ministry of Communication and Information Technology[9] was the originally regulatory and responsibility authority, in 2002 it was changed for *the National Regulatory Authority for Communication* (NRAC)[10] who is a public legal person subordinated to the Government, fully financed from extra-budgetary incomes.

Related to this first law is Law 677/2001 for the *Protection of Persons concerning the Processing of Personal Data and the Free Circulation of Such Data[11]* which applies to the processing of personal data, made, totally or partially, through automatic data processing systems (or computerized systems), as well as to the processing through means other than automatic, which are part of, or destined to, an evidence system.

Article 1 of this law *guarantee and protect the right to personal, family and private life, concerning the processing of personal data. Personal data are any information referring to a person, identified or identifiable; an identifiable person is that person who can be identified, directly or indirectly, particularly with reference to an identification number or to one or more specific details of his physical, physiological, psychical, economical, cultural or social identity.*

Any operation or set of operations that is performed upon the personal data, by automatic processing systems or non-automatic, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure to a third party by transmission, dissemination

or by any other way, combination or alignment, blocking, erasure or destruction represent processing of personal data.

For a better understanding of the law, I specify that the term *processing* may include, for example:

– Creating a customer evidence system;
– Editing a file with personal data;
– Collecting data about readers from web forms;
– Collecting data about web pages visitors;
– Personal data base archiving;
– Disclosure of personal data.

The supervisory authority for this law is the People's Advocate (Ombudsman) who adopted in 2002 several regulations in order to proper apply Law 677/2001.

Finally, in 2001, Law 682/2001 was enacted to ratify the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108). In fact, the two laws mentioned earlier follow the European Union Telecommunications Privacy and Data Protection Directives[12].

3. Electronic commerce and computer fraud

The Law

Under the pressure of European Community, Romania signed the Council of Europe Cyber-Crime Convention[13] on November 23, 2001 at Budapest.

Based on this Convention, in 2002 Romania adopted Law 365/2002 on Electronic Commerce. The purpose of this law is *to establish the conditions of supplying information society services as well as to establish the infringements certain deeds regarding the safety of the domains used for electronic commerce, the issuing and use of electronic payment instruments as well as the use of identification data to carry out financial operations, in order to provide a favorable framework for the free movement of these services and the development of safety conditions for them.*

Article 16 of the law defines the service provider obligations:

(1) The service providers are bound to notify the competent public authorities right away, about activities that seem illegal carried out by the recipients of their services or about information supplied by these ones that seem illegal.

(2) The service providers are bound to communicate the authorities mentioned at paragraph (1) right away, at their request, information that may allow the identification of the recipients of their services with whom these providers have concluded contracts regarding the permanent information storage.

(3) The service providers are bound to interrupt, temporarily or permanently, the transmission into a communication network or the storage information supplied by a recipient of the respective service, especially by eliminating the information or by blocking the access to it, the access to a communication network or the supply of any other information society service, if these measures were required by a public authority, ex-officio or at the receipt of a claim or complaint from any person.

Regarding the unauthorized operations in an information system this law state:

- The authorized access to an information system or a domain is punish by imprisonment from 3 months to 3 years or by fine.
- The unauthorized data transfer into an information system or domain for the personal use or to third parties is punished by imprisonment from 1 to 12 years.
- The unauthorized modification, partial or total destruction of the stored information into an information system or domain is punished by imprisonment from 3 to 15 years.

However, many provisions of the Cyber Crime Convention, especially the definitions of the crimes, were incorporate into Title III (on *Preventing and Fighting Cyber-Crime*) of the Anti-Corruption Law 161/2003[14].

Based on this law, the authorities, and public institutions with competence in the domain, in collaboration with the service providers, the non-governmental organizations and other representatives of the civil society promote policies, practices, measures, procedures and minimum standards for the security of the computer systems.

This law punishes offences against the confidentiality and integrity of data and computer systems, computer-related offences, and child pornography through computer systems.

4. Conclusion

The Romanian legal authorities cooperate directly, under the conditions of the law and by observing the obligations, resulting from the

international legal instruments Romania is part of, with the institutions with similar attributions in other states, as well as with the international organizations specialized in the domain.

At the request of the Romanian competent authorities or of those of other states, on the territory of Romania common investigations can be performed for the prevention and fighting the cyber-crime.

In order to ensure an immediate and permanent international cooperation in the cyber-crime domain, within the Organized Crime Fighting and Anti-drug Section of the prosecutor's Office belonging to the Supreme Court, a cyber-crime fighting service is create as a contact point available permanently.

In addition, the Ministry of Communications and Information Technology is studying the opportunity to setting up Expertise and Security Incident Response Center (CERIS in original, an organism similar to american CERT). CERIS will offer security information and advices for organizations as result of security incidents.

Most of computer crimes involve fraud and money. For Romanian authorities, the next step is to recognize the role of information systems auditor.

References

The following reference list contains hyperlinks to World Wide Web pages. Readers are warned however that:

1. these links existed as of the date of publication but are not guaranteed to be working thereafter.

2. the contents of Web pages may change over time. Where version information provided in References, different version may not contain the information or the conclusions referenced.

1. http://www1.ifccfbi.gov/strategy/IFCC_2001_AnnualReport.pdf
2. http://www1.ifccfbi.gov/strategy/2002_IFCCReport.pdf
3. http://www.politiaromana.ro/date_statistice.xls
4. http:// www.dataprivacy.ie/6aii-1c.htm
5. http://www.uncitral.org/en-index.htm (*Model Law on Electronic Signatures* adopted in 2001, *Model Law on Electronic Commerce with Guide to Enactment* adopted in 1996 with additional article 5 *bis* as adopted in 1998, *Recommendation on the Value of Computer Records (1985)*)
6. http://www4.law.cornell.edu/uscode/18/1030.html
7. http://www4.law.cornell.edu/uscode/42/2000aa.html
8. http://www.anrc.ro/legislatie_interna_eng/L676-2001.pdf
9. http:// www.mcti.ro
10. http://www.anrc.ro/en
11. http://www.avp.ro/leg677en.html
12. http://www.avp.ro/indexen.html
13. http://europa.eu.int/comm/internal_market/privacy/index_en.htm
14. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm