VULNERABILITY AND E-CRIMINALITY OF IT

Mareş Valerica

Economic Studies Academy of Bucharest Faculty of Accounting and Management Information Systems Piaţa Română nr.6, sector 1, Bucharest, Romania maresvalerica@yahoo.com 0721906108

Mareş Marius Daniel

SPIRU HARET University Faculty of Management, Finance and Accounting str. Ion Ghica, nr 13, sector 3, Bucharest, Romania maresmariusdaniel@yahoo.com 0722704696

The development of an informational society requires consolidating trust in information and communication technology (ICT), the protection of personal data and of the right to a private life, but also promoting a world and national unification of the informatic safety in the context of a growing dependence on ICT of societies throughout the world, which become vulnerable to e-criminality. The development, difusion and the consequences of computers are a part of a larger context – the one of informational society and of the era of knowledge.

Keywords: informational society, information and communication technology, informatic safety, vulnerable to e-criminality, knowledge

Jel classification: L86, D80, K20

Introduction:

Communication is natural to human beings and differenciates us from the rest of animals and so everywhere in companies, organizations, agencies and at home, communication increases in breath, intensity and frequency of utilization, under a number of forms.

Together with the intesifying of communication, unsolicited communication also intensifies, bringing a harming content or phishing attacks, transforming communication froma challange into an impossible mission. Internet, which is is the informational „network of networks" that unites a couple of thousand networks of different ranks which come from tens of countries of the world, is strongly affected. Despite the fact that Internet is a virtual network, which combines a growing number of interconnected *Local Area Networks or LANs* – public and private, *Wide Area Networks* or WANs, regional and national networks. Internet is the largest quarter of *Cyberspace* and provides the users with several major services: *World Wide Web*, *Electronic Mail*, *Messenger*, *Usernet*, *Internet Relay Chat* etc, and this diversity of communication makes it vulnerable.

By definition vulnerability represents that state of exposing a valuable thing to a particulat threat, for example a PC disconnected from Internet is not vulnerable to an Internet Worm. The threats represent a sum of unpleasant events that can cause losses to a firm's values. We can include here a list of natural threats as fires, floods, earthquakes, but also human intentional threats as hackers and the inevitable human errors.

Nowadays threats change continuously in form and the mechanisms and security solutions that have to protext the users againsts spam of many kinds, phishing, makware, viruses and even against concertated attacks against the e-mail servers. Few technologies are capable of providing protection against all these phenomena, that continue to grow. Thus, in december 2007, a study was showing that 80% of all e-mails were spam, while 84% of respondends were recognizinf that they had viruses sent by email.

It is well known that, through the services it provides, Internet has brought and brings many advantages to scientific research, education, administration, business, inter-human communication, but in the same time it was and is exposed to dangers that reside in the fact that the network, miraculous through the benefits it provides to man, also represents a media that is extremely favorable to those who commit indesirable social acts, acts that can spread from terorist acts to sexual harrasment or spreading pornographic images. By connecting to this network with a computer (on which was installed an adequate software program) and a modem, through a simple telephone line or cable, any individual can be one *click* distance from a crime. Those who are interested in it, acting relatively anonimously, haven't hesitated to make this small step. More precisely, many criminals from the most diverse types and ranks have immediatel „moved" their business on the virgin territory of Internet, succeeding to become, in a very short time, more efficient than ever in comitting socially dangerous acts. Many companies don't have the capacity to adapt to these attacks by using solutions that are hard to update or by rigid procedures.

1. Exchanges of information. Opportunity and risk

Any organization is confronted with the necesity of achieving a good mnagement of resources: material, human and infromational. In more and more activity sectors, informatization and the existence of computer networks which manage great part of their activity, allow executing economic and financial operation (for example electronic payment systems) that have seen a spectacular development.

The importance of data processed with the aid of the personal computer can transform security in a key element. Security is the junction of four poles of divergent interests: the *decident responsibles*, the *techniciens* that serve the system, the *users* that use it and the audit which controls. We can note that the lack of security is the fruit of lack of interaction and common reflexion between parts. In our country, at least theoretically, many companies wish for a strong and easy to control security of the „accounting and financial area".

The exchange of accounting and financial information, by using new technologies, can be done relatively easily, but there will have to be a proof of quality and of the degree of protection ensured. The lack of concern for information security will lead to major risks and disfunctionalities. Companies with a reduced financial strength can be taken out of the market by a security event. The lack of an informatics system can lead to a temporary halt of the business which implies stopping sales and thus it leads to losses. Here we can raise a couple of questions: "By improving the informatics accounting, is there also an increase in its insecurity?" "What risks are due to new technologies and what are due to financial and accounting information itself?" "What is the connection between the quality of the informatics security and that of the financial and accounting information and the accounting segment in general?"

Any modern entity incorporates *Informatics and Communication Resources* that include all devices of printing, display, storage and all the activities associated to the computer that imply using any device capable of receiving email, navigating on Web, in other words, capable of transmitting, storing, administering electronic data, including but not limited to: mainframes, servers, personal computers, notebooks, pocket books, *Personal Digital Assistant* – PDA, pagers, distributed processing units, laboratory and medical equipment connected to the network, telephones, facsimile, printers and other accessories that have to be managed and securitized. To these can be added the procedures, the facilities of the programs, the data that are designed, constructed, made operational and maintained in order to create, collect, register, process, store, receive, display and transmit information necessary to the internal and external media entities.

The risk represents the intersection between threat and vulnerability and can originate from the internal and external media. The external risks of the organization impend the activity and are related to:

-political risks (conflicts, alliances etc);
-financial and economic risks (prices, inflation, stock market);
-informatics and techno logics risks;
-risk products (medicines, automobiles);
-new frauds;
-blocking of communication ways;
-epidemics and epizootics;
-natural hazards (floods, storms, heavy snows, earthquakes) etc.

The attempt to quantify the risk is a challenging and interesting task. In the majority of the cases, the risk is associated with the effective costs of acquisition, maintenance and development of the protection mechanisms. Most representations of risk use:

-*Annual rate of occurrence* – this represents the number of times in a year a treat can occur. It is achieved by reporting estimates over a past period, taking into account the improvements to the system.

-*The probability of a loss* – represents the sum that an organization looses when a disaster occurs.

Movement of criminal „businesses" to the Internet ground did not occur randomly, but from reasons as pragmatic as possible, which take into account that this world network has at least three important advantages:

-Distance removal.
-Minimal costs.
-An "anonymous".

Unfortunately, all the domains of the Internet, so beneficial for the majority of honest users of this informational network, are at the same time some of the most profitable infractional fields for those interested to use them for other purposes. Nowadays, when the minimal technical means and financial expenses are extremely low, any user can connect to Internet in order to access a series of databases from around the world, we can expect at any time that a person with evil intentions of a psychically ill person, from anywhere on the globe, to cause immense damage to individuals, communities or even states situated at tens of thousands of kilometers away. Specialists estimate that "the terrorist of tomorrow will be able to cause more damage with a keyboard than with a bomb". It is more and more evident that, nowadays terrorist groups use informational technology to achieve their subversive purposes.

Electronic attacks through viruses and "informatics bombs" created by informatics pirates reconverted to the economic warfare or to manipulating the stock exchanges and destructive sabotage represent major dangers for informatics systems.

In the current conditions, when there is a large number of databases which grace to the Internet can be consulted from any part of the world, informatics spying widens and diversifies. Information threat is a concern for many companies from various fields. Commercial information, as are the lists of products, prices, clients, providers, product promoting methods. Fabrication methodologies, personnel training methodologies, know-how, inventions that are on the way to be patented or marketing studies, are among the most exposed to criminals.

2. Security of information systems and e-criminality

The impressive development of technology led to an increse in profts, on the one side, and to an increase in dangers and fearfulness on the other side. As the electronic media become more accesible to the general public, the informatic criminality is developed and diversified, becoming more than traditional fraud or falsification. On Internet, information became the cheapest weapon in the world, but the problem of its security gives headaches to the world's powers, as on Internet every computer is like a leaf of a tree and the network components are like branches. It is enough to cut a branch and its result is equivalent to cutting the leaf.

The sofisticated world of the informatic systems is extremely alluring being a digital world where are possible electronic businesses, efficient documentation over Internet, distance learning, instanteneous communications, but apart from that the information technology is not lacking in risks – one of the most important being the **e-criminality**.

The notion of informatics criminality is now more than the traditional definition referring to criminality against informatics systems, and also includes most crimes that can be done over the Internet using information systems. Informatics criminality has a very high price in economic terms as well as from a human security perspective.

Before the age of developing informational technologies, the main concern in regard to informatics data was keeping their confidentiality, something that could not be achieved by simply protecting them physically (for example, by locking them with a key in the rooms were information was being stored).

Nowadays, along with the confidentiality there are the important aspects of security of the IT that have become a complex and concerning problem for all organization types, being in the same time a legal requirement. In order to ensure the security of the IT and of the personal data, the authorities and public institutions with competences in the field, the service providers, nongovernmental organizations and other representatives of the civil society have common activities and programs in order to prevent e-criminality.

Criminals can launch massive attacks with informatics viruses against telecommunication networks for defense, electric power, gas and water or against the systems for traffic control for aeronautic, naval and terrestrial industries, against informatics systems of banks, stock exchanges, insurance societies, that can disturb the activities in these fields.

The security requests of the informatics systems are based on a number of operational and integration, legal, social, moral and human aspects with other informatics systems. Informatics criminality can have severe consequences that can extend to heavy financial and reputation losses that also come together with the security events, and in these conditions the security management of the informatics systems becomes extremely important.

In respect to criminality in the field of data networks, especially Internet, one can distinguish the infractionality that aims at paralyzing the entire system or a part of it or a structure that works with it, through virus programs or attack of the type *Denial of Service*(DoS).

The age in which hackers wanted to prove their programming abilities has passed. Meanwhile they discovered opportunities to make profit over Internet, as through Phishing. There are numerous traps through which criminals can get rich in the virtual space, as by cloning the sites of banks, when the client receives an e-mail in which it is required to enter on the site of the so called bank, the account data, the username, the password and the secret access codes, and all the thief have to do is to empty the account. According to the estimates of the Organization for Security and Cooperation in Europe (OSCE), the informatics criminality produces an annual loss of 100 billion dollars. The German association of the commercial society claims that in Germany, in 2007, the total value of the damage amounted to 13 billion euro. Other studies say that e-criminality has become even more profitable than drug traffic. The international authorities for legal pursuits have identified three regions in the world from which come the majority of the trap e-mails: Russia, China in Brazil, areas in which the illegal businesses flourish. The interest of the hackers is mainly focused on the passwords of top-managers, in order to obtain extremely valuable information.

In the current crisis conditions it is to be noted that e-criminality is done more frequently through:

-a larger number of viruses, worms and trojans that attack computer networks;

-sending by email of false deduction coupons in the name of well known companies;

-an intensification of attacks caused by spyware, scanning ports, informatics sabotages, pornography, computer thrift (desktop and mobile), abuses of employees;

-an increased incidence of attacks from within organizations;

-attacks executed from outside that are aimed at countries like: USA, China, Russia, Nigeria, South Korea, Germany and India.

More and more attacks are done through zombie computers grouped in networks called botnet through which criminals' pirate computers, without the knowledge of the owners of the computers and use them for sending spam or for destroying other computers. Programs can be distributed in different ways, one of them being as attachment to e-mail or downloads from certain sites.

Few technologies can provide protection against all these phenomena that continue to increase (e.g. in December 2007 approximately 65% of all e-mails were spam) and a solution is being searched which would solve the current challenges. The concept of Unified Threat Management (UTM) offers a global approach to the problem of the security of IT, by protecting the clients against attacks of versions types as:

-scanning IP Reputation;
-antispam based on patterns of messages;
-white lists and blacklists;
-antivirus based on signatures of families of viruses;
-protection against “zero-hour outbreaks”;
-intrusions prevention systems at the e-mail level.

The informatics criminality does not comprise only spam and viruses, it can also strike other aspects of the economic and social life. There have been cases when the adepts of different terrorist organizations, on certain occasions, as the success of some of their actions, build site of sympathy for such groups, presenting details for preparing them and congratulating the courage and the mastership of terrorists as if it was a game. Other sites provide updated information for creating bombs or instructions for manipulating explosive substances.

Another category of terrorist activities over Internet is the dissemination of messages of hate and incitation to violence through the Web pages and unfortunately things don’t stop at such activities, which in most cases are a precursor of real terrorist actions and can get to incitation to attack and finally to organize grave criminal acts. Criminal organizations have converted with an amazing speed to the most sophisticated technologies and they use encrypted software for communicating over Internet with a high degree of security. Network is a formidable means also for organized bands that deal with drugs and arms traffic, as well as medicines, with washing black money etc, because these bands understood that Internet is an ideal communication means, cheap, fast and pretty secure when using encryption software.

In many countries of the world, displaying and distributing obscene materials in public is against the law. There is no doubt that Internet, through its open nature, has become such a place. Thus, performing such activities through a mega-network, is most of the times prone to breaking the law. Nevertheless locations that contain materials for adults are very numerous and the growing number of these sites and the negative impact of disseminating obscene materials, of popularizing child pornography on Internet have led to an increasing concern of the public opinion regarding the multiplication of such an activity over the network. The fact that deviant behavior has moved their place of action does not change their criminal nature.

Apart from the older forms of e-criminality related to Internet, there are also some new ones like: “offers for adoption” that cover selling of children or organs for transplant.

Despite the sustained efforts of a company to protect its clients, a growing number of users of the Internet have lost their faith in the efficiency of the security methods and that’s why a new culture of security is required in the contemporary society.

Pirating computer software represents another form of criminality related to Internet. It is achieved by downloading programs spread over the Internet, on a computer, when this operation is not authorized by the titular of the author rights.

3. Investigating e-criminality

The investigation of e-criminality has a series of particularities that differentiates it fundamentally from other types of investigation due to its nature that supposes using scientific and certified instruments for insurance, collection, validation, identification, analysis, interpretation, documentation and presentation of digital probes, obtained from informatics sources, used in order to facilitate discovering the truth.

The investigation of e-criminality has to have a series of specific characteristics necessary for ensuring a high degree of correctness:

-authentication (proof of the source of the probes);
-credibility (lack of doubts concerning credibility and solidity of the probes);
-completeness (acquiring all existing probes and keeping their integrity);
-certitude;
-lack of interferences and of contamination of probes as a result of the investigation or of the probe management.

In the process of e-criminality investigations, the following steps will be followed:

1. Identification of the incident supposes recognition of the incident and determining its type.
2. Preparing the investigation which supposes preparing of the instruments, verification of procedures, obtaining documents that allow the inquisition.
3. Formulating a strategy of approach function of the involved technology and of the possible consequences for the people and institutions involved. The aim of formulating this strategy is to maximize the potential of obtaining relevant probes, while minimizing the negative impact on the victim.
4. Insuring the probes – isolating, insuring and storing digital or physical probes.
5. Collecting probes – recording the physical ambiance and copying of the digital probes, by using specific practices and procedures.

6. Examination of probes that suppose a deep visualization of the probes in order to search for elements that are connected to the respective offence. This supposes localizing and identification of probes as well as the documentation of each step in order to facilitate the analysis.
7. The analysis of probes by determining the significance of probes and drawing the conclusions related to the incriminated offence.
8. Inquiring the victims and the offenders.
9. Presenting the probes – drawing the conclusions and presenting them in an intelligible way for no specialists. This synthesis has to be accompanied by a detailed technical documentation.
10. Returning the probes – returning the objects retained during the investigations to their owners or in some cases confiscating those objects.
11. Advertising the crime in order to intimidate future offenders.

Informatics crime investigations can be helped by certain institutions, national and international organizations, associations and private persons.

There is the concern that hackers will go further and will modify price lists, juridical texts or even scientific research results, which would have grave consequences. Nevertheless as there is no security system entirely secure, it is recommended to be aware of the risks that exist when running a business that uses informatics systems

Conclusions:

1. Internet was and is subject to dangers that originate in this network which apart from advantages also represents an external media favorable for those who commit social and economic offences.
2. In order to increase informatics safety, to reduce to a minimum the use of services for illegal purposes and to consolidate trust in informational technology, it is essential that the Internet service providers and the authorities that supervise the application of law to cooperate efficiently, taking into account the role of each party, the cost of the cooperation and the rights of the citizens, until an Internet traffic laws system of legal system is created. Thus, people will be concerned not only with the correct use and the continuous development in the domain of informational technology and Internet, but also to establish the legal framework in which the interactions will take place.
3. Informatics criminality is a phenomenon that negatively affects the international image of a country.

BIBLIOGRAPHY

1.Ioana Vasiu - *Criminalitatea informatică*, Ed. Nemira, Bucharest, 1998
2.Tudor Amza, Cosmin Amza – *Criminalitate informatică*, Ed. Lumina Lex, Bucharest, 2003.
3.Victor-Valeriu Patriciu et al. - *Internet-ul şi dreptul*, Ed. ALL BECK, Bucharest, 1999.
4. ***„Ghidul introductiv pentru aplicarea dispoziţiilor referitoare la criminalitatea informatică”, Bucharest, 2004.
5.http://www.coe.int/cybercrime
6.http://www.riti-internews.ro/ro/cybercrime.htm
7.http://www.legi-internet.ro/conventie_crim_info.htm
8.http://und.ro