ANNALS of the ORADEA UNIVERSITY.

Fascicle of Management and Technological Engineering, Volume VI (XVI), 2007

DATA PROTECTION – A NECESSITY TO MAINTAIN THE CUSTOMERS TRUST IN AN E-BUSINESS

Naiana ȚARCĂ, Ioan ȚARCĂ
University of Oradea, ntarca@uoradea.ro, nelut@uoradea.ro

Keywords: e-business, company's private network, data security, firewall

Abstract. E-business is designed corresponding to a model in which the client is posted on a central place. The company turnover is conditioned by the data degree of confidentiality. This is why a large part of the funds invested in e-business are allocated to security issues, both to protect data and to maintain the clients' confidence. Each company need to develop its' own data security policy, adequate to their activities, to permit the detection of the methods that can create damages and to establish real protection methods.

1. INTRODUCTION

Nowadays more and more information is stored and transmitted by electronic means, which determine changes in the way the companies approaches the business. The Internet and other communications media brings lots of benefits and allows competition advantages achievements. Businesses can be developed through means which couldn't be possible in the past. A new business world develops, full of possibilities, where companies can benefit from the advantages of the quick communications and advanced data acquisition, data computing and transmission. The companies' efficiency increases and also their financial results rise. But in the mean time problems concerning data security occurs.

Internet communications are open and uncontrolled. This fact conflicts with e-business needs, which needs confidentiality and integrity for transmitted data. The exponential rise of the e-business imposes a secure business environment.

E-business is designed corresponding to a model in which the client is posted on a central place. All the steps in which the client is involved such as the product evaluation, command placement, data completion for financial transaction, delivery following, are recorded. Thus the company turnover is conditioned by the data degree of confidentiality. This is why a large part of the funds invested in e-business are allocated to security issues, both to protect data and to maintain the clients' confidence.

For Romania, a country with emerging economy the digital infrastructure security is a compulsory condition to stay inside the new global economy. The information protection and data transmission channels security represents the main inquiry of a modern business environment, attractive to the investors all around the world.

The Internet technologies create equal business opportunities for all kind of economies. Search engines do not make differences between sites from a geographical point of view, which means that the producers from emergent economy countries like Romania have the same appreciation as those from countries with full blown economies.

Distances annihilation offers the consumers a real choose freedom, but also implies expenses regarding data security.

2. DATA SECURITY ASSURANCE – AN IMPERATIVE CONDITION IN E-BUSINESS SUCCESS

Data security can no longer be treated from a technical point of view; it needs to be included in the company's management. This is because that for every company information is a very important good, which has to be adequately protected, to assure activity continuity, possible damage decrease, welfare and business opportunities maximize. Data security is decisive in the company advantage in regard to the concurrence, in profit earning capacity assurance and for a favorable public image.

To earn and maintain the clients' faith each company has to be sure that its' marketing and public relations departments can effectively communicate the measures taken to protect their money and intimacy.

Although informatics intrusions may have huge costs, a lot of Romanian companies do not allocate enough resources to protect them. The situation tends to change anyhow. Information security technologies are considered to be an important factor on which the company success depends. They are suitable not only to reduce the risks but also to obtain profit and new affair opportunities. They are also means for business goals. Therefore they need to be included in the companies' strategic thought process.

Each company need to develop its' own data security policy, adequate to their activities, to permit the detection of the methods that can create damages and to establish real protection methods. The following consequences should appear in the case of proper data security measure lack:

- partially or totally data destruction;
- data theft;
- data integrity loss
- access loss at their own information

The following specific issues occur in virtual reality regarding data security:

- the burglar doesn't have to be present at the crime zone, thus annulling geographical distances. Considering the fact that the threat can appear from anywhere the way data security is regarded and specific delinquent profiles are identified must be changed.
- security violation methods in virtual reality assume a quick attack and it is almost impossible to detect the aggression in real time.
- the responsibility for a certain degree of data security is divided between more participants. Even though a company assures a good security degree for its own network, connecting with other networks, such as Internet implies risks, therefore imposing complementary data security means.

Because of this the old methods of data security assurance remain important but as long as the companies get virtual identities, these are no more sufficient.

Data security threats may have lots of causes: disasters or natural calamities, equipments failure, human operating errors, manipulation or frauds. The first three types of treat occurs accidentally, meanwhile the last is intentional. Certain studies in data security domain estimates that 50% of the incident costs are caused by voluntary destructive actions, 25% due to natural disasters and equipment failure and 25% caused by human errors (fig.1).

Accidental threats can be avoided using the old data security methods, such as regular data savings, mirroring, access rights limitation.

The use of the Internet in business assumes new methods and techniques to avoid voluntary threats. This is due to the fact that the Internet creates a large field of action to the evil-minded threats:

- data interception. No data are being modified or erased but the confidentiality rules are infringed.
- transit data interception; they arrives to another person that the person for which they are delivered

- deletion, modification, re-transmission or delay of the messages, old or fake messages insertion, message order change. These attacks modify the computers, communication systems and data state.
- messages having false identities
- destructive type software creation, which sometimes essentially affects data security. These attacks unauthorized read information, destroying them partly or even totally.

Defending methods were developed, facing possible ways of attack, such as: Calling Line Identification, ISDN Call-back, Password Authentication Protocol, Challenge Handshake Authentication Protocol, Secure Shell Remote Management, Crypt Virtual Private Network and Firewall.

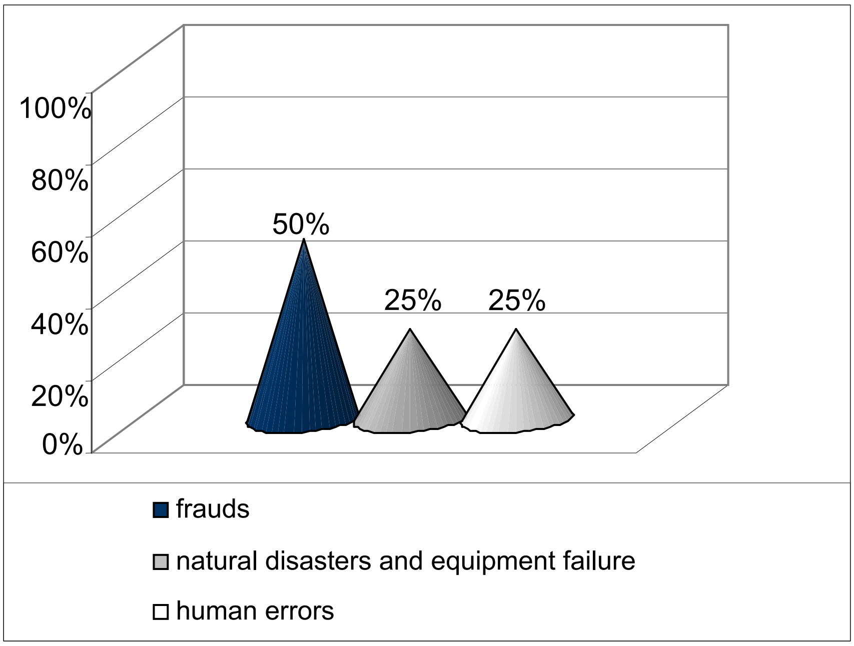

Fig. 1 Costs generated by the companies' data security threats

To protect e-business network security issues deals with:

- access to the information only for the authorized users, and totally access denied to unauthorized users
- protection against message tampering
- identification of the person that currently communicates and the type of access granted
- messages authenticity assurance.

To assure the network security, the following issues are implemented:

- block access procedures at the network level (firewall, intrusions detection system)
- security policies at the resource access level (servers, workstations, e-mail, web) through operating systems applications
- data codification techniques to insure data transportation through the network without the possibility of being intercepted and read by unauthorized receptors
- specific mechanisms at the physical level (physical protection of the transmission lines) which generally is very expensive and difficult to achieve.

3. FIREWALL – A SOLUTION FOR E-BUSINESS PROTECTION

Similar to a firewall inside a building which denies the fire to cross from one part of a building to another, the Internet firewall denies the danger the arrives from the Internet to pass inside the company's intranet.

Firewall is a filter that stops certain network traffic and allows another. It is interposed between the company's network and Internet (fig.2), having the following roles:

- the information that needs to enter or exit the company network is forced to pass through a single access point where is subjected to a rigorous control.
- prevents the intention of an attack and searches for appropriate means of counteraction.

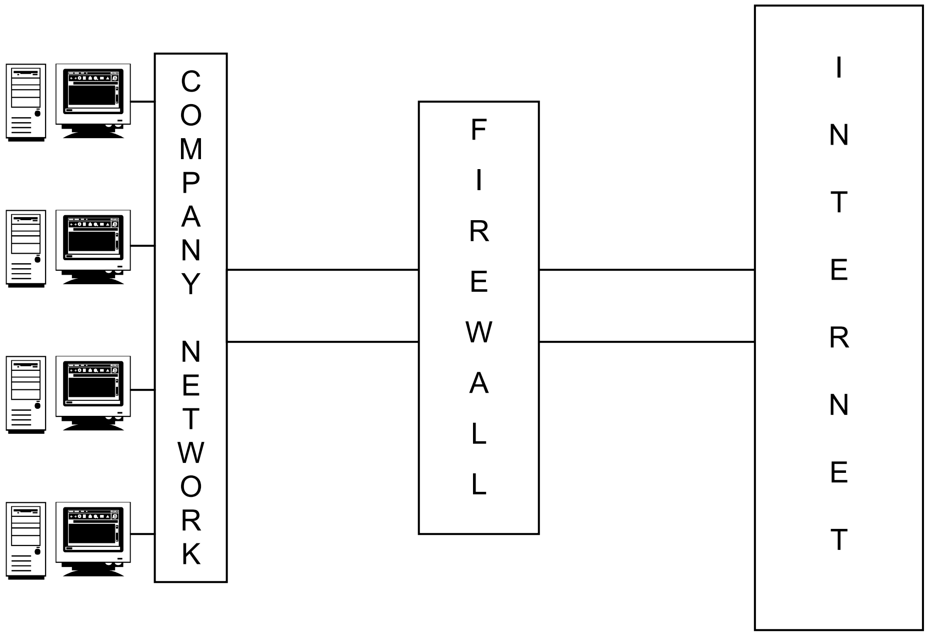

Fig. 2 A firewall which insulates a company network from the Internet

This way all the traffic arriving from and exiting to the Internet passes the Firewall.

Significant benefits are offered by the Firewall, such as:

- firewall is intended as a control point. All the traffic regardless of its direction must pass through this point. This way the attention ca be concentrated upon the company's own security issues in one single point; this is the point where company's network is connected to the Internet.
- firewall filters the traffic allowing data passing based only on a specific set of rules
- because all the traffic passes through firewall this is a good place to collect information about the network utilization, abuses, etc.
- using an internal firewall, a network section of the company can be separated from other sections. An internal firewall is useful when in a section of the network high importance data is manipulated, information forbidden to be seen in other sections.

Firewall offers a good protection against a network threats but does not constitutes a complete security solution. It cannot solve any kind of security issue. Thus:

- firewall cannot protect the company network against evil-minded users inside the network. These users can tear out destroy or modify data, can erase or modify software, without being detected by the firewall
- firewall can detect the traffic that passes it but can do nothing to the one that passes through other points.
- The company should not consider that once firewall installed it will always protect the network. The firewall installed at a certain moment will protect the network against attacks known at the moment of the installation. But it cannot protect the network against the new type of attacks, appeared afterwards.
- firewall cannot protect against viruses. Virus detection represents an extremely difficult operation.

A firewall solution should be expenses enough but is less expensive and more efficient than other security means and certainly less expensive than an inadequate security solution.

In the last period of time more firewall dealers appeared on the market, their products integrating more and more functions.

When a company decides to acquire a firewall is necessary to understand the way it was conceived and how does it work. Some companies consider that the firewall evaluation necessitates a great effort and decides to build their own firewall. The decision of buying or constructing a firewall depends on the technicians inside the company, the allocated budget, the platform used, services, and the needed level of security.

4. CONCLUSIONS

Two aspects regarding data security issues need to be prevalently considered in an e-business:

- the integrity of the company's network resources, which means their availability, regardless the functioning defects, hardware and/or software, or the illegal tries of data steal and/or modification.
- The private character, which means the individual right to control or influence what type of information regarding a person should be memorized in files or databases and who can access them.

In Romania data security assurance is closely tied to the following aspects:

- the awareness of the data security at the managing levels. Some managers of the small and medium size companies consider the data security as a sort of black-hole where money enters and no benefit is achieved.
- not always the employees have the necessary competence to use the computers. Big sized companies afford hiring high qualified employees, whilst small sized companies cannot afford this. Big sized companies make efforts to qualify their employees whilst small size companies make small or none efforts of this type.
- big and medium sized companies' applicative programs are created considering data security issues. Small companies rather use pirated software or applications created by non-specialists, which not only that do not incorporate security issues but in some case they don't function correctly, thus altering data.
- financial possibilities of the company. Big sized companies, having great profits, invest in data security. Small sized companies rarely make this kind of investment and often insufficiently to assure a minimum of security.

BIBLIOGRAPHY

[Bru01] Bruhn, M. Orientarea spre clienți. Temelia afacerii de succes, Editura Economică, Bucureşti, 2001

[Hel00] Held, G., Hundley, K. CISCO – Arhitecturi de securitate, Editura Teora, Bucureşti, 2000

[McC01] McClure, S., Scambray, J., Kurtz, G. Securitatea rețelelor, Editura Teora, Bucureşti, 2001

[Nor05] Northrup, T. Windows Vista Security and Data Protection Improvements, Microsoft TechNet, June 1, 2005

[Ogl02] Ogletree, T.W. Firewals. Protecția rețelelor conectate la Internet, Editura Teora, Bucureşti, 2002

[Tar07] Țarcă, N. Rolul prezenței on line în adaptarea ofertei unei firme la cerințele clienților, Proceedings of the 3rd Internațional Scientific Conference ECO-TREND 2006 „Economics and Globalization", Universitaria Publishing House, Craiova, 2007

[Tar07] Țarcă, N. Rolul prezenței on line în adaptarea ofertei unei firme la cerințele clienților, Proceedings of the 3rd Internațional Scientific Conference ECO-TREND 2006 „Economics and Globalization", Universitaria Publishing House, Craiova, 2007

[WEB06] http://www.enisa.eu.int/ European Network and Information Security Agency