Risks and stakes of the e-trading

Constantin Yamkoudougou, Security Consultant
email: security at itconstantin.com

23 novembre 2005

what kind of practices can mitigate e-trading risks ?

The electronic trade still called E-trade must deal with two major obstacles. First, the perception of a product on an Internet portal is not the same one as the glance in a window of the real world where the product can be carried with hand. The customer does not have for example the possibility of touching nor measuring the products as in a traditional trade. It is thus legitimate that this one fears to be seen delivering products which are not in physical or technical conformity compared to the leaflets of sales on the web site of trade. The second difficulty which explains the greatest reserve of the customers for the conclusion of the act of purchase remains security. Indeed, the electronic trade requires the use of bank on line and of course transfers of funds, which makes run to the customer the risks of usurpation of identity, fraud and diversion of its means of payment. Many technologies and protocols of security were developed but generally, the vulnerability of these systems depends on their implementation. For example a storage of bank card numbers on a database and a nonrigorous management of the access to these data can be a source of large embezzlement if an unauthorized individual gained access to the information of such a base. Online businesses have the obligation to put in place technicals means and management to ensure the security of the transactions, however observing few rules can help customers to reduce advent of the risks mentioned above. Some of these rules can be stated as below for each one of us :
- make your purchases on sites of great notoriety,
- purchase goods if possible on sites of companies having a local or national physical presence. Indeed, the diversity of the rights of trade according to countries' is so important that in the event of financial embezzlement, it is better to deal with company of proximity
- update regularly your operating system with hot fixes or patches published by the editors
- lock your computer each time it is not used.
- deactivate the automatic seizure in the forms of Web pages
- check that your browser passes well in safe (SSL mode) mode before transmitting confidential data.

- pay attention to the indiscreet eyes which can be on the top of your shoulders and may take note of personal information before it is transmitted.
- regularly change the password of your computer. Avoid downloading and installing free programs of Internet which could compromise or transmit discreetly your personal data to unauthorized third parties.

Believe or not, some famous businesses have been hacked

Every business or information system connected to Internet is exposed to all cyber vandalism a priori. This risk is still increased when the companies has important digital activities, i.e. that it quasi totality of commercial activity takes place on Internet.

In 2000, Yahoo or CNN Internet portals were victims of attacks by distibuted deny of service. This type of attack has a direct incidence on the sales turnover of the companies concerned but more especially on the credibility of the customers of the aforesaid Internet Portals. In the United Kingdom, an Internet Service Provider Could Nine went bankrupt at the end of a series of attacks which compromised its network and its customers' database in January 2002.

figures of vandalism on Internet in 2001

Do you know that when you are connected to Internet you are the target of more than one thousand of potential attacks every hour ?. According to laboratory ICSA Labs, more than 3500 threats on computers is recorded every hour. The same laboratory estimated that in the first quarter of 2001 more than 7 665 000 attacks occurred in the world. This figure has probably multiplied by ten since this time.

The techniques and the tools of hacking used are numerous. Among the most current techniques one can quote the techniques of usurpation of name, addresses, disguise of data, identity theft and acts of sabotage by deny of services. These statistics do not take into account viruses, logic bombs or trojans which are fast propagation agents.

This last type of agents (virus, worm) can be combined to classical methods of hacking which make them increasingly harmful : for example deny of service and corruption of system ; corruption and propagation by anonymity of email. The Red Code, Nimda and Klez are eloquent examples to illustrate the complexity of this type of attack.

Red Code and Nimda exploits a vulnerability of the Web server of Microsoft in order to compromise a greater number of other weakened servers. Nimda integrates a research program of email addresses in the address' books of the compromised stations and then transmits in an autonomous way an infected email by disguising the source address. To ensure its propagation on each remote host, the same worm exploits a break-in of the standard of structuring and coding the messages of electronic mail which enables him to be carried out when an infected message is opened.

The cybercriminality is not today any more a myth exploited by cinematographic industries of the Eighties but a daily reality that each company should integrate in its information system.

Is there a return on investment of computer security ?

A traditional reproach which is made to the entities of security management of information in businesses is the great difficulty to define precisely its return on investment. To evaluate the profitability of the function of computer security in an analytical groundwork of compatibility is certainly not easy. The common mean to do this is an evaluation compared to the risks incurred by the company. Beyond the border of the company, the question of the profitability of the computer security can also arise with as much acuity on a macro economic level. It is for example important to know at the local, national and even world level the impact of attacks and viruses on a given economy.

An analysis of the American newspaper The Computer Economics showed that the year 2000 was certainly most criminal in data processing. As an example ' I Love You' would have cost with him all alone approximately 8.75 billion dollars. The most expensive virus of 2001 was the Red Code whose damage rise to 2.62 billion dollars, followed-up of ' SirCam ' (1.15 billion dollars) and finally ' Nimda ' (0.635 billion dollars).

According to the same source the total cost of computer hacking would have passed from 17.1 billion dollars in 2000 to 13.2 billion dollars in 2001 and this mainly because of systematic integration of tools like anti-virus and firewalls in the information processing systems.

The computer security that one quantifies and evaluates its profitability with so much difficulty can be compared with peace for any economy. Without it, no digitial economy would be viable.

Ref : The Computer Economics