E-BUSINESS SECURITY ASPECTS

COSTINELA-LUMINITA DEFTA
UNIVERSITY OF PITESTI, STR. LIVIU REBREANU, NR. 46-58, BUCURESTI,
lumi.defta@yahoo.com

Abstract:
An effective business relationship is based on the trust between the business partners, the security insurance being a key element. This fits for all type of activities and also for those like e-business. E-business consists mostly in the implementation of the business processes by using the information technology and internet services. Since all business processes must be connected to the internet and available for users, the choice of the information solutions on which e-business is built is crucial for the security. In this paper we will highlight the potential threats and the common tools used to ensure the information security in an e-business environment.

Key words: *e-business, security, internet, information technology, transactions.*

JEL classification: *L21, L86, M15*

Introduction

E-business represents the term used to describe the information systems and applications that drive business processes using web technologies. It is a more generic term than e-commerce because it refers to not only buying and selling but also servicing customers and collaborating with business partners. E-business allows companies to link their internal and external processes more efficiently and effectively, and work more closely with suppliers and partners to better satisfy the needs and expectations of their customers, leading to improvements in overall business performance.
E-business is much more than a web presence, because there are a lot of tools designed to help business work better: collaboration tools, mobile and wireless technology, social media, etc.
E-business is normally divided into the following groups:

- business to business (B2B) includes all applications intended to enable or improve relationships within firms and between two or more companies. In practical terms in this category belongs any company that uses the Internet to order from suppliers, to receive invoices and make payments.
- business to consumer (B2C) refers to the relations between the trader and the final consumer. It is the process of selling products and / or services for personal consumption. Buyers are individuals, families or other groups that buy products / services to meet individual needs.
- business to administration (B2A) covers transactions between companies and governmental organizations, such as city, local, regional, national governments and governmental agencies such as the European Commission.
- consumer to consumer (C2C) group is represented by the web-based auctions. Through this system, it can be negotiated the prices for broad categories of goods (from electronic to art objects or books). The most famous electronic auction portal is probably eBay (http://www.ebay.com).

- business to employee (B2E) uses its own intranet system which allows companies to provide products and/or services to their employees. Typically, companies use B2E networks to automate employee-related corporate processes.

The usage of public networks like Internet causes new requirements for e-business security. Because e-business information exchange contains valuable assets, including order information, money transfers, product information a lack of privacy, integrity or confidentiality can cause a huge damage to an organization and its business. Neglecting adequate security measures in B2B applications, which exposes a company's network to customers and partners may land a company in hot water. In a B2B environment, even simple mistakes could lead to leakage of data that no trading partner would ever tolerate.

Basic security aspects

Basically, the following security aspects should be met in e-business environments: confidentiality, integrity, availability, key management, non-repudiation, authentication.

Confidentiality allows only authorized parties to read protected information. It must be ensured through the access control to resources and by securing the transmission and the storage of the data. For an online business, we must verify the identity of the person we are doing business with.

Integrity of the data and programs is a very important subject even though it is often neglected in daily life. Integrity means that only authorized subjects (i.e. users or computer programs) are permitted to modify data (or executable programs).

Integrity ensures data remains as is from the sender to the receiver. If someone added an extra bill to the envelope, which contained your credit card bill, he has violated the integrity of the mail.

Availability ensures you have access and are authorized to resources. For an online business it is important to obtain the evidence of the date, time and place at which a contract was made.

The *key management* provides secure distribution and management of keys needed to provide secure communications.

Non repudiation provides undeniable, end-to-end proof of each message's origin and recipient.

The *authentication* securely identifies clients and servers with digital signatures and certificates.

E-business security threats

Believing that they are not at risks, some business owners don't protect enough their network infrastructure from spyware, viruses, worms, hackers, customer data theft and other threats. They must be more aware of the most common e-business security threats, which we tried to summarize below.

Although there are plenty of security threats which may break an e-business platform, we will list only some of them: denial of service, malicious code, network sniffing, spoofing, social engineering, eavesdropping, secrecy threat, backdoors, integrity threat, insider employee threat, copyright infringement, Active X Controls, viruses, worms, etc.

Some of the easiest and most profitable attacks are based on tricking the shopper, also known as *social engineering* techniques. These attacks involve surveillance of the shopper's behavior, gathering information to use against the shopper. For example, a mother's maiden name is a common challenge question used by numerous sites. If one of these sites is tricked into giving away a password once the

challenge question is provided, then not only has this site been compromised, but it is also likely that the shopper used the same logon ID and password on other sites.
A common scenario is that the attacker calls the shopper, pretending to be a representative from a site visited, and extracts information. The attacker then calls a customer service representative at the site, posing as the shopper and providing personal information. The attacker then asks for the password to be reset to a specific value.
Another common form of social engineering attacks are phishing schemes. Typo pirates play on the names of famous sites to collect authentication and registration information.

The *viruses, worms* are another common security threats encountered daily especially in e-mail attachments, Word and Excel macros, etc. Risks can also come from popular social networking sites.
A virus can attach itself to other software, such a patch to an application that is really designed to implement itself to other application for which it was not intended. In this way it can infect all application to which it can gain access. A worm is a type of virus that replicates itself on the computers that it infects. A macro virus is a type of virus that is coded as a small program (macro) which is embedded in a file. The effects of viruses can cause significant harm to the operations of the e-business, and can very easily go undetected before the harm is already done. A Trojan horse is a program that appears to be legitimate but actually contains another program or block of undesired malicious, destructive code, disguised and hidden in a block of desirable code. Trojans can be used to infect a computer with a virus. Be aware of messages containing links to current events, entertainment, or other high traffic content. It has been reported that these links take the user to phishing websites where personal user details can be stolen or worms, Trojans or viruses can strike.

Two *spoofing* threats can affect an e-business process: IP and email spoofing. Through an *e-mail spoofing*, a hacker is able to hide his identity by changing the information in an e-mail header. An imposter posing as a computer support technician could convince an employee to divulge passwords and other confidential information, and then impersonate the employee and gain access to the system. E-mail spoofing can also be related to virus transfers and spam mail. Spam is any unwanted e-mail message, often advertising a product and sent in bulk. Spammers commonly operate under falsified e-mail addresses. Viruses are also generally distributed under false e-mail addresses.
IP spoofing is most frequently used in *denial-of-service attacks*. In such attacks, the goal is to flood the victim with overwhelming amounts of traffic, and the attacker does not care about receiving responses to the attack packets. Packets with spoofed addresses are thus suitable for such attacks. They have additional advantages for this purpose—they are more difficult to filter since each spoofed packet appears to come from a different address, and they hide the true source of the attack. By changing his IP address, an unauthorized individual may be able to gain access to an e-business system. A spoofed IP address could lead to legitimate e-mail being sent to an imposter rather than to the legitimate party.
The spoofing types are forms of a common security violation known as a man in the middle (MITM) attack. In these attacks, a malicious party intercepts a legitimate communication between two friendly parties. The malicious host then controls the flow of communication and can eliminate or alter the information sent by one of the original participants without the knowledge of either the original sender or the recipient. In this way, an attacker can fool a victim into disclosing confidential information by spoofing the identity of the original sender, who is presumably trusted by the recipient.

Secrecy is the prevention of unauthorized information disclosure while privacy is the protection of individual rights to nondisclosure. Secrecy is a technical issue requiring sophisticated physical and logical mechanisms whereas privacy protection is a

legal matter. One significant threat to e-business is theft of sensitive or personal information, including credit card number, names, address and personal preferences. This kind of theft can occur anytime anyone submits information over the Internet because it is easy for an attacker to record information packets for later examination.
The same problem can occur in e-mail transmission. Software applications called sniffer programs provide the means to record information that passes through a computer or router that is handling Internet traffic. Sniffer programs can read messages e-mail messages and unencrypted Web client-server message traffic such as user login, passwords and credit card numbers.
The *backdoors* represents electronic holes in e-business software that are left open accidentally (or intentionally) by a software developer. Either way, the content is exposed to secrecy threats. A backdoor allows anyone with knowledge of the existing of the backdoor to cause damage by observing transactions, deleting or stealing data.

An *integrity threat*, also known as active wiretapping exists when an unauthorized party can alter a message stream of information. Unprotected banking transactions, such as deposit amounts transmitted over the Internet, are subject to integrity violations. An integrity violation implies a secrecy violation because an intruder who alerts information can read and interpret that information. Unlike secrecy threads, where a viewer simply sees restricted information, integrity threads can cause a change in the actions a person or corporation takes because mission-critical transmission has been altered.

Insider employee threat refers to an employee who can steal a company cash, equipment, furniture, supplies and vital business information. Most security systems are designed to prevent outsiders from breaking in to steal or vandalize property. Unfortunately, these security systems do little to prevent a trusted employee from robbing a company.

E-business defense

Despite the existence of the security threats presented above (and also many others), e-business can be a safe and secure activity. Fortunately, there are plenty of ways to protect an e-business from internet security threats. A practical approach to e-business security starts by reconciling the disparate business and security agendas within an organization. Managers must agree on the balance between speed, cost, effort, and security. This will include consideration of the size of the specific e-business opportunity and the specific assets at risk, as well as an assessment of potential threats based on whether the initiative is intended for an intranet, extranet, or the public Internet. Although there are many solutions and advices that can improve the e-business security, we will try to list some of them especially for the threats presented in this paper.

A recommended way to fight against *viruses and worms* is to install and use anti-virus programs, anti-spyware programs, and firewalls on all computers in the e-business. Firewalls can be separate appliances, built into wireless systems, or a software firewall that comes with many commercial security suites. Also we must ensure that all computer software is up-to-date and contains the most recent patches for the operating system and anti-virus program.

The firewalls can help us also to fight against *IP spoofing* if it is configured to disallow access to incoming requests from specific IP addresses. Implementing encryption and authentication will also reduce spoofing threats. Both of these features are included in Ipv6, which will eliminate current spoofing threats. Additionally, we should eliminate all host-based authentication measures, which are sometimes common for machines on the same subnet. Ensure that the proper authentication measures are in

place and carried out over a secure (encrypted) channel. Also I good idea is to use the replication system for the data storage. The replication process increases the security of the system and also improves the speed of data operations.

An e-business system is only as secure as the people who use it. If an employee for example chooses a weak password, or does not keep their password confidential, then an attacker can pose as that user. This is significant if the compromised password belongs to an administrator of the system. In this case, there is likely physical security involved because the administrator client may not be exposed outside the firewall. Users need to use good judgment when giving out information, and be educated about possible phishing schemes and other *social engineering* attacks. They must not provide information about the organization, including its structure or networks, unless they are certain of a person's authority to have the information.

One solution for the *integrity threat* represents the usage of an end-to-end encrypted data channel. Ensure privacy by protecting data in transport and use encryption from browser to host, to ensure that critical or confidential data is not exposed as it travels over internal or external networks. This can be accomplished by using the SSL (Secure Socket Layer) protocol that encrypts data between the client's computer and the site's server. When an SSL-protected page is requested, the browser identifies the server as a trusted entity and initiates a handshake to pass encryption key information back and forth. Now, on subsequent requests to the server, the information flowing back and forth is encrypted so that a hacker sniffing the network cannot read the contents. The SSL certificate is issued to the server by a certificate authority authorized by the government.

There are a number of ways a company can protect itself from *insider employee threats*. One of them is to divide critical functions and responsibilities among employees within the organization, limiting the possibility that one individual could commit sabotage or fraud without the help of other employees within the organization.
Also a good idea is to implement strict password and authentication policies. Make sure every employee uses passwords containing letters and numbers, and do not use names or word. Moreover, be sure to change passwords every 90 days, and most importantly, delete an employee's account or change the passwords to critical systems, after an employee leaves the company. This makes it harder for disgruntled employees to damage the systems after they have left.

To prevent the *intrusion detection* a good practice is to log any attempted unauthorized access to the system. If a user logs on, and attempts to access resources that he is not entitled to see, or performs actions that he is not entitled to perform, then this indicates the account has been co-opted and should be locked out. Analysis of the security logs can detect patterns of suspicious behavior, allowing the administrator to take action. In addition to security logs, we can use business auditing to monitor activities such as payment processing. We can monitor and review these logs to detect patterns of inappropriate interaction at the business process level.

Digital signatures and certificates are important control procedures that establish the *identity* of a party to an e-business transaction. In the same way that a signature on a paper document verifies or authorizes important information, a digital signature provides assurance that, for example, an order is legitimate. Data encryption is also an important component of ensuring the authenticity of digital signatures and certificates.
One area of security technology that is contributing to the reduction of falsified identity within e-business firms is biometrics, the use of unique physical characteristics to prevent unauthorized individuals from accessing a company's computer system. Under a biometric approach, distinctive physical characteristics (such as voice patterns, fingerprints, facial structure, or signature dynamics) are identified for each authorized user of a computer system. When an individual wants to access the system, a biometric

device compares the physical input against that stored within the computer system. They must match in order for the individual to be given access.

Conclusions

E-business systems inherently possess a higher degree of risk than mainstream applications, and thus require a greater degree of security. Because of this risk, security should be considered as a fundamental aspect of an e-business system design.

E-business depends on providing customers, partners, and employees with access to information, in a way that is controlled and secure. Managing e-business security is a multifaceted challenge and requires the coordination of business policy and practice with appropriate technology. A practical approach to e-business security starts by reconciling the disparate business and security agendas within an organization. Managers must agree on the balance between speed, cost, effort, and security. Managers must then review their e-business efforts in light of the security pitfalls described above.

REFERENCES

1. Defta L., "Information Security in E-learning Platforms" - 3rd World Conference on Educational Sciences, 2011;
2. Emil B., "Securitatea datelor in sistemele informatice economice" – PhD Thesis, 2004;
3. Graeme P., Matthew J.W., "Benchmarking E-business Security: A Model and Framework" - International Journal of Information and Computer Security, 2007;
4. Iacob N., "Data replication in distributed environments" - Journal "Constantin Brancusi" University of Targu Jiu Annals - Economics Series, 2010;
5. Lord P., "Managing E-Business Security Challenges" – An Oracle White Paper, 2002;
6. McDowell M., "How To Prevent Social Engineering and Phishing" – US-CERT Cyber Security Tips, 2004;
7. Stephen A., "E-business security and controls" – CPA Journal, 2001;
8. Zota R., "Elemente de securitate pentru Internet Banking" – Revista Informatica Economica, 2000;
9. http://www.businessknowhow.com/security/insider.htm
10. http://en.wikipedia.org/wiki/IP_address_spoofing
11. http://www.networkworld.com/news/2004/0924ebussites.html