

Report on the current and future security factors

Internet security: what does it mean?

What should be understood about Internet security tools is that they are like any other security system in a company. They help minimize the risk of serious damage in the eventuality of an attack. Physical stores are equipped with locks on the doors, alarm systems, bars on the windows, security cameras and in some cases guards are posted at the doors. Even with all these elements in place, companies still feel the need to purchase theft insurance to protect their investments. The companies understand the limits of all physical security and therefore plan accordingly.

This should be the same for Internet security, which, essentially, should be engaged as an extension of physical security. Simply put, some things are important to secure regardless of whether you are dealing in a physical or electronic environment (i.e. credit card numbers, employee information, business records, etc.) and these areas must be individually identified and addressed. Understanding and treating Internet security is essential. The rationale for security in the physical marketplace is the same as in the electronic only the means are different. In short, Internet security is an exercise in risk management. Done correctly, transacting over an Internet site can be much safer than providing your credit card number over the phone or giving your credit card to a waiter in a restaurant! When examining the issue of Internet security, or when considering the purchase of any Internet security system, there are a several basic questions that the company has to ask itself:

- What information, records and communications need to be protected;
- What are the threats to these assets and, what are the risks that the threats will occur?
- Given these needs, what are the potential strengths and limitations of available Internet security options;
- How does the security system react with other applications you are currently using;
- What other equipment (hardware or software) will be needed to make it as secure as possible, and;
- What type of training will employees need to ensure that the system functions properly?

The answers to the above questions will help the company to recognise its needs with respect to an Internet security system. A better understanding of the security issues and their impact on the company business, allows the company to reduce the clients concerns

Available solutions

There are several solutions to improve the SME Internet security. These solutions could be used alone or combined each other.

It is possible to classify these solution in three categories:

- Solutions addressed to preserve the data privacy
- Solutions addressed to preserve the Local Area Network (LAN) form external intrusions
- Solution addressed to protect Intranet connections.

The first ones are addressed to preserve the data privacy (i.e. customers credit card numbers) and are cryptography based. The second ones are addressed to preserve the LAN integrity from external attacks. In this category it possible insert: Firewalls, and Anti-virus. The last ones are addressed to render safe the connection between the LAN and the external world. These connections could be used for remote work or e-commerce. In this category it is possible to insert: IP based Virtual Private Network (VPN), Digital Signature, Digital Certificates, SSL and Secure HTTP.

A brief description of the solutions mentioned is provided below.

Encryption

Encryption is part of a larger process called cryptography: the science of keeping data secure and protected by transforming the data through the application of a mathematical formula. Cryptography has four key elements:

1. Encryption: the process of encoding the data.
2. Decryption: the process of decoding the data.
3. Algorithm: the mathematical formula applied to the message that both encrypts and decrypts the data.
4. Key: a particular code that when applied to an algorithm encrypts and decrypts the data in a way that allows the data to be traced to a particular person or company.

This process is commonly referred to simply as encryption, most likely because it is this element of the process that secures the data and keeps it private. Primarily, this tool is a software-based solution and should not include significant hardware costs in most cases. It is a key tool for privacy, as it allows only authorised parties to view the data. Encryption is also a key tool to ensure data integrity, as it protects information/data from being modified or corrupted.

Firewall

A firewall will control and filter Internet services to block any unauthorised traffic. It can be used to manage the orderly and secure transfer of information between the Internet and a secure business network.

Firewalls may also enforce restrictions on internal users, such as the public Internet services that users are allowed to access, the times of day allowed for browsing, and whether FTP or mail attachments can be downloaded.

Anti-Virus Software

Anti-virus software is a utility that searches incoming messages and data and your personal computer's hard disk for viruses and removes any viruses that are found.

Most anti-virus programs include an auto-update feature that enables the program to download profiles of new viruses from the Internet or a designated server so that it can continue to protect against new viruses.

This tool is key to ensuring the integrity of information and data that you receive from others and the data you keep on your personal computer. Viruses can cause serious damage to both your electronic (data/documents) and physical (computer hard drive) capital. When regularly updated, anti-virus software is an inexpensive security tool that is extremely effective.

Internet Protocol based Virtual Private Networks (IP VPNs)

IP VPNs provides the secure transport of private communications over the public networks. IP VPN combines encryption tools and Internet protocol tunnelling to ensure user authentication. It is used primarily when an enterprise wishes to provide mobile or remote workers with secure access to company data that is only accessible over internal company networks (i.e. a LAN). Thus, if you are travelling, opening a new location/office or are just working from home, you can access your internal company securely by using an IP VPN.

Digital Signatures

Digital signatures are the electronic functional equivalent of a personal physical signature. In fact, digital signatures are considered even more secure than physical signatures because they cannot be forged. Digital signature technology is a key security tool that functions to ensure user authentication and non-repudiation i.e. digital signatures prove that the transaction took place between identifiable parties. A sender attaches a digital signature to a message. The receiver is the only one that can read the message and at the same time he is assured that the message was indeed sent by the sender.

Digital Certificates

Digital certificates validate that the person/organization using a particular cryptographic key is who they claim to be. Digital certificates provide key information (similar to a drivers licence, for instance) on the user of that key. Digital certificates, therefore, represent an important Internet security tool that works to authenticate parties to a transaction and provide non-repudiation

SSL and Secure HTTP

Short for Secure Sockets Layer, a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:.

Another protocol for transmitting data securely over the World Wide Web is Secure HTTP (S-HTTP). Whereas SSL creates a secure connection between a client and a server, over which any amount of data can be sent securely, S-HTTP is designed to transmit individual messages securely. SSL and S-HTTP, therefore, can be seen as complementary rather than competing technologies. The Internet Engineering Task Force (IETF) as a standard has approved both protocols.

The right solution

There is no “ideal solution” but several good solutions that can be applied in the company. A good solution is a combination of two or more solutions above-mentioned.

In the following some examples are provided, addressed to cover different company needs.

Secure e-mail

Make safe the e-mail flow mean, on one hand preserve the data from malicious viruses on the other preserve the e-mail content. It is possible to have the first one using an anti-virus application; the second one could be obtained using an encryption solution.

Preserve the data privacy

Preserving documents from a fraudulent reading can be obtained using a encryption policy. All sensible documents must be stored only in encrypted status.

Preserve the LAN integrity

In this case the objective is to stop external attack to the company LAN. External attack could be virus-attack or hacking attack. The former could be stopped using an anti-virus application (the best anti-virus applications could be installed either as single PC protection or as a net protection). A firewall is necessary to stop hacking attack. This case is similar to the above-illustrate case. The firewall must be installed between the LAN and the external world. It will be necessary to install a personal firewall if each single PCs have a dial-up connection, it will be necessary to install a net firewall if the net is permanently connected with the Internet.

Remote Access

Some companies need to allow to their employees to access to the company LAN from a remote station. In this case it is necessary to certify the user that asks to be connected. Several solutions could be applied in this case. Digital certified, SSL, Secure HTTP, Internet Protocol based Virtual Private Networks (IP VPNs)

On-line payments

In this case it is necessary to preserve the information exchanged between the customers and the company and authenticate the transaction.

To meet the first need it is possible to apply the same solutions used for remote access, to solve the second one it is necessary to use a digital signature solution.