The Information Security in companies

Information systems are frequently exposed to various types of threats which can cause different types of damages that might lead to significant financial losses. Information security damages can range from small losses to entire information system destruction. They are:

The effects of various threats vary considerably: some affect the confidentiality or integrity of data while others affect the availability of a system. Currently, organizations are struggling to understand what the threats to their information assets are and how to obtain the necessary means to combat them which continues to pose a challenge.

Talking about the defining of security threats, there are security threat classification model which allows to avoid threat impact quickly as a threat varies over time. Threats may be cause by: Natural disasters, Power outages, Hardware breakdowns, Human errors, Software failures, Security breaches, Acts of war, Viruses, Technical issues and others.

The Information Security Triad: Confidentiality, Integrity, Availability (CIA).

The most popular self-data technologies are:

Access Control

Once a user has been authenticated, the next step is to ensure that they can only access the information resources that are appropriate.

Encryption

Many times, an organization needs to transmit information over the Internet or transfer it on external media such as a CD or flash drive. In these cases, even with proper authentication and access control, it is possible for an unauthorized person to get access to the data. Encryption is a process of encoding data upon its transmission or storage so that only authorized individuals can read it.

Backups

Another essential tool for information security is a comprehensive backup plan for the entire organization. Not only should the data on the corporate servers be backed up, but individual computers used throughout the organization should also be backed up.

The frequency of backups should be based on how important the data is to the company, combined with the ability of the company to replace any data that is lost. Critical data should be backed up daily, while less critical data could be backed up weekly.

Firewalls

Another method that an organization should use to increase security on its network is a firewall. A firewall can exist as hardware or software (or both). A hardware firewall is a device that is connected to the network and filters the packets based on a set of rules. A software firewall runs on the operating system and intercepts packets as they arrive to a computer. A firewall protects all company servers and computers by stopping packets from outside the organization's network that do not meet a strict set of criteria. A firewall may also be configured to restrict the flow of packets leaving the organization. This may be done to eliminate the possibility of employees watching YouTube videos or using Facebook from a company computer.

Intrusion Detection Systems

Another device that can be placed on the network for security purposes is an intrusion detection system, or IDS. An IDS does not add any additional security; instead, it provides the functionality to identify if the network is being attacked. An IDS can be configured to watch for specific types of activities and then alert security personnel if that activity occurs.