It management

Business, Management

Information security: policy, procedure and standard

Policies can be described as instructions or a set of statements that is used to provide guidance to employees of some organization. Appropriate courses of action can be defined within policies, as well as generalized requirements for people inside and outside of the organization. Sometimes policies can equivalent to a set of business rules. Usually, information security policies are unique to the business that deploys them, but they typically define goals, beliefs, worker responsibilities and ethics within the organization. It should be noted that policies are mandatory and can be viewed as a set of laws in full force within the company. For example, taking a different course of action might require an approval of a high-ranking executive. The language used while writing policies rules have no ambiguity and results in a dry set of explicit rules (Curtin, 1997).

Meanwhile, standards are recommendations and requirements for the implementation of policies. While both are mandatory, policies are high-level and standards are low-level. This implies that policies provide general statements, while standards provide specific requirements. Standards are used primarily to ensure security consistency across the organization (What are Policies, Standards, Guidelines and Procedures? 2009). Usually, standards define algorithms, design concepts, etc. The so-called " information security architecture" is essentially a set of integrated information security standards.

In turn, procedures are essentially just step by step instructions that help employees to implement different policies and standards. They are explicit and comprehensible low-level specifics.

Let us point out a few more differences between them. First of all, policies are long-term, while standards are relatively short-term as they need to be changed more often due to their nature (What is the difference between security policies, standards and procedures? 2011). Usually, standards like business processes or particular piece of software change every few years. Second of all, policies target a wider audience, while standards usually provide requirements to certain people.

For example, suppose that company policy states that all employees must ensure privacy of correspondence. In that case, company standard could require them to use strong passwords and prohibit the use of unencrypted e-mail. If company policy clearly states the need to back up important folders, company standard should define the proper software, while company procedure should give a step-by-step guidance to software installation process and further maintenance.

What if company policy requires employees to wear ties? In that case, company standard would list appropriate ties, whereas company procedure would be a useful step-by-step guide to tying and wearing a tie.

Finally, how to define policies, standards, and procedures if we need to build the Information Security System? Let us do it this way:

ISF – policy: all of the company data must be protected at all costs; ISF – standard: encrypt all the sensitive information, log transfers and password protect your accounts; ISF – procedure: here is the step by step instructions for encrypting data, keeping logs and choosing strong passwords. Describe and explain the difference between firewalls, IDS, IPS, Proxy Servers, and Honeypots

A firewall's primary goal is to ensure the security of the network. It does that by means of controlling network traffic, analyzing incoming and outgoing data packets. The verdict on each packet is made based on the special set of rules. There are two types of firewalls: software-based and hardware-based. Usually, firewall acts as a gateway between internal and external networks.

Intrusion detection systems (IDS) allow the worker to monitor traffic and system activities, keep logs and obtain audit data from the system. When an intrusion is detected, IDS alert the user about it.

Intrusion prevention systems (IPS) are designed to monitor network and system for malicious activity, notify user about it, respond to malicious activity by blocking or stopping it, log relevant information and so on. Like IDS, IPS monitors traffic and activities, but, at the same time, they are able to respond to detected intrusions.

A proxy server is a server that acts like an intermediary between computers on the local network and the Internet. It means that every request from the client's computer, as well as every response from the Internet, is evaluated by the proxy server. There are lots of reasons why one would want to use a proxy server. Among them are anonymity, child control, and hacking. Sometimes, proxy servers can act as simple firewalls.

Honeypot is a modern-day cyber trap for modern-day cyber mice. Usually, it is a computer with some data of some value to the potential attackers. The trick is to disguise it as a vulnerable target, while monitoring traffic and system activities in order to detect an intrusion. There are two types of honeypots: production honeypots and research honeypots. Production honeypots are often used within bigger security systems in order to improve overall protection. Research honeypots resemble spies: they capture a lot of information and are used mainly by military organizations. Moreover, the biggest risk in using a honeypot lies in losing it to attackers as it may be used to harm other systems.

How firewalls differ from proxy servers? Firewalls work on the packet level, while proxy servers work on an application protocol level. Therefore, from these two only firewalls can decide whether or not to block particular packets. However, if you try to disable proxy server, computers will not be able to connect from the LAN to the Internet; the situation is different with firewalls, as they are, in fact, just different sets of rules, and it is possible to create an exception that will allow computers to connect to the Internet (“ The difference between the firewall and the application level proxy server”, n. d.).

How IDS differ from IPS? The main difference between them lies in how they ensure network safety. As was mentioned earlier, IDS alerts the user when they discover malicious activity. When they detect an attack, they can reset

TCP connections or even re-write firewall rules in real time. Meanwhile, IPS filters network traffic and tries to preempt malicious activity. Although, IPS offer better protection, it is advisable to use IPS and IDS concurrently.