

## Computer Security - Policies

In this chapter we will explain security policies which are the basis of security for the technology infrastructure of your company.

In a way they are the regulatory of the behaviors of your employees towards the use of technology in the workplace, that can minimize the risk of being hacked, information leak, internet bad usage and it also ensures safeguarding of company resources.

In real life you will notice the employees of your organization will always tend to click on bad or virus infected URL's or email attachments with viruses.

### Role of the Security Policy in Setting up Protocols

Following are some pointers which help in setting u protocols for the security policy of an organization.

- Who should have access to the system?
- How it should be configured?
- How to communicate with third parties or systems?

Policies are divided in two categories –

- User policies
- IT policies.

User policies generally define the limit of the users towards the computer resources in a workplace. For example, what are they allowed to install in their computer, if they can use removable storages.

Whereas, IT policies are designed for IT department, to secure the procedures and functions of IT fields.

- **General Policies** – This is the policy which defines the rights of the staff and access level to the systems. Generally, it is included even in the communication protocol as a preventive measure in case there are any disasters.
- **Server Policies** – This defines who should have access to the specific server and with what rights. Which software's should be installed, level of access to internet, how they should be updated.
- **Firewall Access and Configuration Policies** – It defines who should have access to the firewall and what type of access, like monitoring, rules change. Which ports and services should be allowed and if it should be inbound or outbound.
- **Backup Policies** – It defines who is the responsible person for backup, what should be the backup, where it should be backed up, how long it should be kept and the frequency of the backup.
- **VPN Policies** – These policies generally go with the firewall policy, it defines those users who should have a VPN access and with what rights. For site-to-site connections with partners, it defines the access level of the partner to your network, type of encryption to be set.

## Structure of a Security Policy

When you compile a security policy you should have in mind a basic structure in order to make something practical. Some of the main points which have to be taken into consideration are –

- Description of the Policy and what is the usage for?
- Where this policy should be applied?
- Functions and responsibilities of the employees that are affected by this policy.
- Procedures that are involved in this policy.
- Consequences if the policy is not compatible with company standards.

## Types of Policies

In this section we will see the most important types of policies.

- **Permissive Policy** – It is a medium restriction policy where we as an administrator block just some well-known ports of malware regarding internet access and just some exploits are taken in consideration.
- **Prudent Policy** – This is a high restriction policy where everything is blocked regarding the internet access, just a small list of websites are allowed, and now extra services are allowed in computers to be installed and logs are maintained for every user.
- **Acceptance User Policy** – This policy regulates the behavior of the users towards a system or network or even a webpage, so it is explicitly said what a user can do and cannot in a system. Like are they allowed to share access codes, can they share resources, etc.
- **User Account Policy** – This policy defines what a user should do in order to have or maintain another user in a specific system. For example, accessing an e-commerce webpage. To create this policy, you should answer some questions such as –
  - Should the password be complex or not?
  - What age should the users have?
  - Maximum allowed tries or fails to log in?
  - When the user should be deleted, activated, blocked?
- **Information Protection Policy** – This policy is to regulate access to information, how to process information, how to store and how it should be transferred.
- **Remote Access Policy** – This policy is mainly for big companies where the user and their branches are outside their headquarters. It tells what should the users access, when they can work and on which software like SSH, VPN, RDP.

- **Firewall Management Policy** – This policy has explicitly to do with its management, which ports should be blocked, what updates should be taken, how to make changes in the firewall, how long should be the logs be kept.
- **Special Access Policy** – This policy is intended to keep people under control and monitor the special privileges in their systems and the purpose as to why they have it. These employees can be team leaders, managers, senior managers, system administrators, and such high designation based people.
- **Network Policy** – This policy is to restrict the access of anyone towards the network resource and make clear who all will access the network. It will also ensure whether that person should be authenticated or not. This policy also includes other aspects like, who will authorize the new devices that will be connected with network? The documentation of network changes. Web filters and the levels of access. Who should have wireless connection and the type of authentication, validity of connection session?
- **Email Usage Policy** – This is one of the most important policies that should be done because many users use the work email for personal purposes as well. As a result information can leak outside. Some of the key points of this policy are the employees should know the importance of this system that they have the privilege to use. They should not open any attachments that look suspicious. Private and confidential data should not be sent via any encrypted email.
- **Software Security Policy** – This policy has to do with the software's installed in the user computer and what they should have. Some of the key points of this policy are Software of the company should not be given to third parties. Only the white list of software's should be allowed, no other software's should be installed in the computer. Warez and pirated software's should not be allowed.