SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

Unit IV- Network Threats

Topic :Computer Security policies

Computer Security policies

- It define the goals and elements of the organization's computer system,
- Policies are divided in different categories
- **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.

- **IT policies**

It 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.**

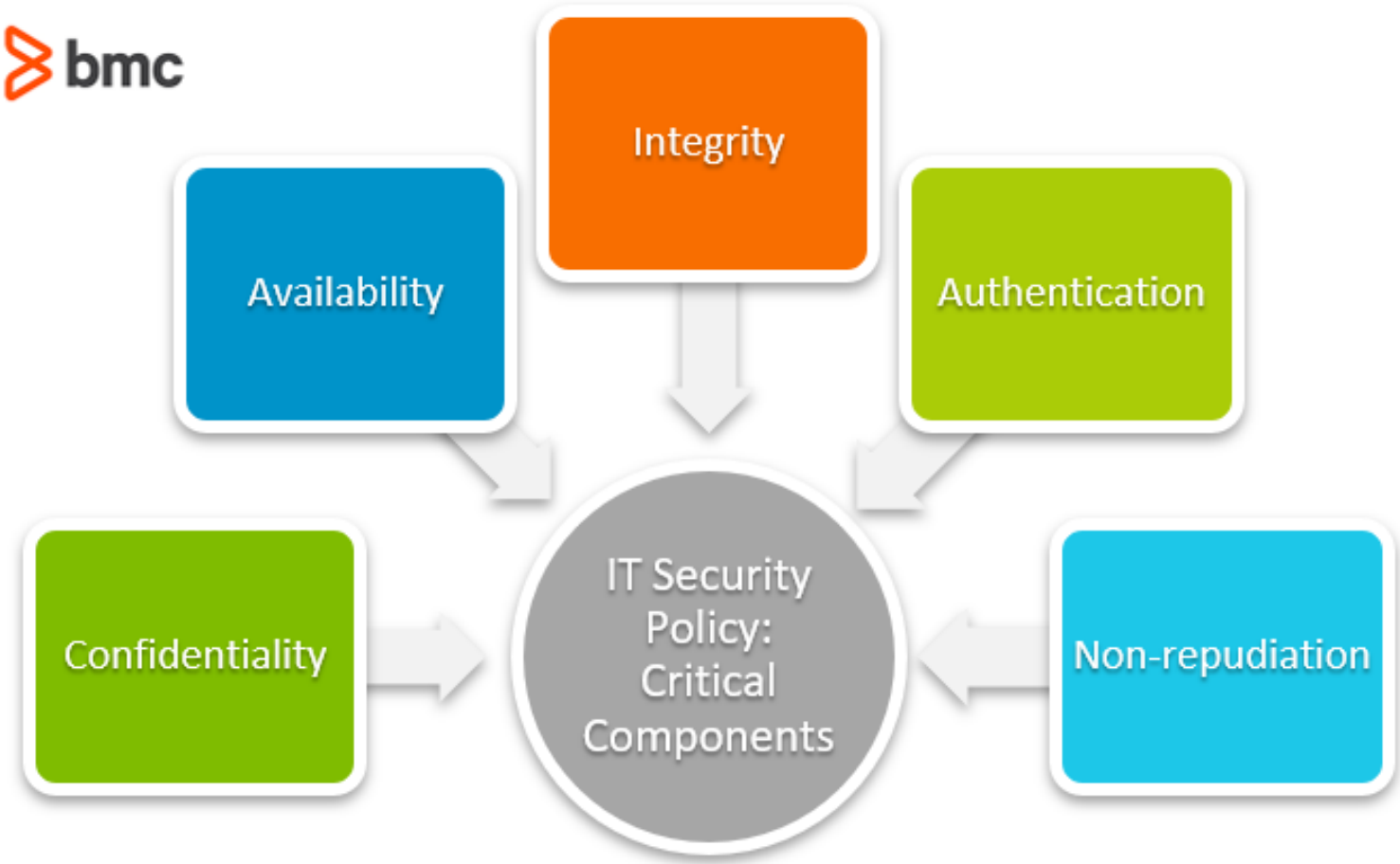
- **Backup Policies** − It defines who is the **responsible person for backup**, what should be the backup, where it should be backed up, how long it should be kept and the frequency of the backup.
- **VPN Policies** − These policies generally go with **the firewall policy**, it defines those users who 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.

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.

- **Information Protection Policy** − This policy is to **regulate access to information**, hot 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.
- **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.
- **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.


bmc
Integrity
Availability
Authentication
Confidentiality
IT Security Policy: Critical Components
Non-repudiation

Any Query????

Thank you……