COMPUTING SECURITY CONCEPTS AND PROBLEMS

LAB 1

18. 01

Acceptable Use Policy

Policies

1. Ownership :

- The assets and computers are not for personnel use and are prohibited.
- The users should not save their private passwords or try to save their private files into the company system.
- By default, external drives or thumbdrives are prohibited, and users are not advised to do so.
- Always update the system software and keep your system up-to-date.
- The company has rights to access the system 24/7.

2. Network Access :

- Firewalls are always active in a company's network, so reaching out to some sites may be prohibited.
- Employees should never try to use VPN or proxy servers; if they do, they may face serious problems.
- Sharing personnel files on the cloud is strictly prohibited.
- Don't try to access Tor or other onion servers; if so, an employee may get into trouble.
- Don't try to use WiFi adapters or other network devices on our servers.

3. Privacy :

- The whole system and network are not private; they are continuously monitored by zscalar, which will save the user's logs into the system.
- The company has full rights to access the files and systems of the employee.
- The IT team has full control over read and write access to the system.
- The company has the right to terminate the system from the network if it finds any malicious activity.
- If any malicious activity is found, the company has the right to totally terminate the user's access.

4. Exploitation :

- Employees should not exploit the resources of the organization and try to engage in suspicious activities.
- If an employee is found suspicious and it is proven, the organization has the right to file a case.
- Any suspicious activity found by the organization will result in the immediate termination of the employee and its access without any prior information.
- Employees should follow the company's guidelines with access to resources and use the system responsibly.

18.03

a. Disaster recovery is important as it determines the momentum of the company after an adverse attack, so it is crucial to involve the best employees to recover the situation well.

Employees who can be included in this process are:

- Disaster Recovery and Business Continuity :
- Senior Information Analyst
- Human Resource Manager
- IT Specialist
- Legal Advisors
- External Managers
- Crucial contracters

b. Backups are very important, and backing up the client's data and information about the supply chain is mandatory. Storing critical information, like insider management, and safeguarding the company's legal policies are important backups. Ongoing projects and tax records are important too.

Temporary logs and cache, user preferences and settings, and their temporary files are non-essential data, which is not necessarily important for backup in my opinion.

c. Top 3 disaster recovery companies:

- Zerto
- AOMEI Cyber Backups
- Carbonite

The above services have automated technologies and facilities to handle the system, as well as the ability to transfer between public, private, and hybrid clouds. We can also customize the policies and system configurations for better management.

Top 3 services for business continuity:

- Ncontracts.
- Oracle ERP Cloud.
- FICO Decision Central

Ncontracts is a SaaS-based risk management and compliance solution, whereas Oracle uses automated processes and has AI embedded systems for better management of the processes. FICO Decision Central manages all decision assets and analytic models across the entire lifecycle.

Lab Analysis :

1. The supervisor was dictating about the workplace policy, which describes the activities that are not encouraged during business hours as they fall under payroll timing. The HR manager manages and maintains these policies to ensure the proper functioning and efficiency of the company.

2. We can be safe when we are able to differentiate between good and bad, but some attacks like social engineering confuse people about what is real and what is fake. Social engineering attacks are popular because they clone the original websites, links, and themes to attack the clients to gain their credentials, access, passwords, etc. Social engineering includes backdoors, keyloggers, reverse communications, etc. Therefore, one of the most dangerous attacks on cyber security should be taught to employees of the company to avoid those traps.

3. Disaster recovery and business continuity are both confusing in some cases, but in my opinion, in order to recover from a disaster, the business should be alive and continue running so that it can properly recover. Therefore, business must be continued first by enabling risk management, etc., and then recovering from the adverse effects of disaster is critical to rebuilding the business or organization.

Key Term Quiz :

1. Disaster Recovery
2. Business Continuity
3. User education
4. Acceptable Use Policy

19. 02 :

Password Policy:

Having a strong password is important for safeguarding the accounts and system. The security policies for passwords are as follows:

- Having a password with more than eight characters is mandatory.
- Using a combination of characters with symbols and numbers will make the password so secure.
- Not repeating the same characters simultaneously will create a strong password.
- Change the passwords regularly and update them to keep the system secure.
- Keeping non-relative text and numbers in passwords helps improve the password.
- Don't use the same password for different applications to ensure the safety of the system.