Chapter-#03

Cyber Security Principles

Cyber Security Principles

- **What are Cyber Security Principles?**
- Cyber security principles act as a set of instructions that help to safeguard networks and systems against cyber threats. There are several cyber security or IT security principles to ensure the safety of networks and the devices connected to them.
- The UK internet industry and Government recognized the need to develop a series of Guiding Principles for improving the online security of the ISPs' customers and limit the rise in cyber-attacks. Cyber security for these purposes encompasses the protection of essential information, processes, and systems, connected or stored online, with a broad view across the people, technical, and physical domains.
- These Principles recognize that the ISPs (and other service providers), internet users, and UK Government all have a role in minimizing and mitigating the cyber threats inherent in using the internet.
- These Guiding Principles have been developed to respond to this challenge by providing a consistent approach to help, inform, educate, and protect ISPs' (Internet Service Provider's) customers from online crimes. These Guiding Principles are aspirational, developed and delivered as a partnership between Government and ISPs. They recognize that ISPs have different sets of customers, offer different levels of support and services to protect those customers from cyber threats.

Cyber Security Principles

- **Need for Defining Cyber Security Principles**
- Most organizations working in this digital era rely on the internet, wireless networks, and computer systems to operate properly. To make sure that the data they share across networks and different systems are safe from unauthorized access and manipulation, they need to put a cyber security framework in place.
- The principles of cyber security assists organizations in creating robust frameworks to enforce strict security of networks and data.
- **Framing a Risk Management Regime**
- One of the first principles of cyber security is to define and create a risk management strategy for the organization to handle all the potential cyber threats. While developing the strategy or regime, it becomes essential to take input from the executives of the organization along with the professional guidance of experts who have taken proper Cyber Security training. While strategizing, all the threats and their sources need to be identified and defined clearly. This helps to make rules and regulations that aim to minimize the vulnerabilities in the organization's IT infrastructure.
- **Example**: A team of cyber security monitors a system and identifies all the vulnerabilities. The people at the management level review all the vulnerabilities and discuss which vulnerabilities need to be eliminated by the cyber security team.

Cyber Security Principles

1. Economy of mechanism

This principle states that Security mechanisms should be as simple and small as possible. The Economy of mechanism principle simplifies the design and implementation of security mechanisms. If the design and implementation are simple and small, fewer possibilities exist for errors. The checking and testing process is less complicated so that fewer components need to be tested.

Cyber Security Principles

- Interfaces between security modules are the suspect area which should be as simple as possible. Because Interface modules often make implicit assumptions about input or output parameters or the current system state. If the any of these assumptions are wrong, the module's actions may produce unexpected results. Simple security framework facilitates its understanding by developers and users and enables the efficient development and verification of enforcement methods for it.
- To create a simple and efficient cyber security framework, it is essential to identify what types of threats it needs to tackle and how. An organization may create multiple modules for enforcing cyber security, with each module having its specific assumptions and input data requirements. Therefore, it is important to create only those modules that fulfil the cyber security needs of the organization.
- Creating too many modules or setting incorrect assumptions may lead the whole system to produce unexpected results.
- **Example:** A file encryption mechanism that allows the admin to encrypt any type of file and prevent access for unauthorized users. Instead of creating a security mechanism for each file type, it is better to use an encryption mechanism that protects all types of files.

Cyber Security Principles

- **2. Fail-safe defaults**
- The Fail-safe defaults principle states that the default configuration of a system should have a conservative protection scheme. This principle also restricts how privileges are initialized when a subject or object is created. Whenever access, privileges/rights, or some security-related attribute is not explicitly granted, it should not be grant access to that object.
- **Example:** If we will add a new user to an operating system, the default group of the user should have fewer access rights to files and services.
- **3. Least Privilege**
- This principle states that a user should only have those privileges that need to complete his task. Its primary function is to control the assignment of rights granted to the user, not the identity of the user. This means that if the boss demands root access to a UNIX system that you administer, he/she should not be given that right unless he/she has a task that requires such level of access. If possible, the elevated rights of a user identity should be removed as soon as those rights are no longer needed.

Cyber Security Principles

- **4. Open Design**
- This principle states that the security of a mechanism should not depend on the secrecy of its design or implementation. It suggests that complexity does not add security. This principle is the opposite of the approach known as "security through obscurity." This principle not only applies to information such as passwords or cryptographic systems but also to other computer security related operations.
- **Example:** DVD player & Content Scrambling System (CSS) protection. The CSS is a cryptographic algorithm that protects the DVD movie disks from unauthorized copying.
- **5. Complete mediation**
- The principle of complete mediation restricts the caching of information, which often leads to simpler implementations of mechanisms. The idea of this principle is that access to every object must be checked for compliance with a protection scheme to ensure that they are allowed. As a consequence, there should be wary of performance improvement techniques which save the details of previous authorization checks, since the permissions can change over time.

Cyber Security Principles

- Whenever someone tries to access an object, the system should authenticate the access rights associated with that subject. The subject's access rights are verified once at the initial access, and for subsequent accesses, the system assumes that the same access rights should be accepted for that subject and object. The operating system should mediate all and every access to an object.
- **Example:** An online banking website should require users to sign-in again after a certain period like we can say, twenty minutes has elapsed.
- **6. Separation of Privilege**
- This principle states that a system should grant access permission based on more than one condition being satisfied. This principle may also be restrictive because it limits access to system entities. Thus before privilege is granted more than two verification should be performed.
- **Example:** To su (change) to root, two conditions must be met-
- The user must know the root password.
- The user must be in the right group (wheel).

Cyber Security Principles

- **7. Least Common Mechanism**
- This principle states that in systems with multiple users, the mechanisms allowing resources shared by more than one user should be minimized as much as possible. This principle may also be restrictive because it limits the sharing of resources.
- **Example:** If there is a need to be accessed a file or application by more than one user, then these users should use separate channels to access these resources, which helps to prevent from unforeseen consequences that could cause security problems.
- **8. Psychological acceptability**
- This principle states that a security mechanism should not make the resource more complicated to access if the security mechanisms were not present. The psychological acceptability principle recognizes the human element in computer security. If security-related software or computer systems are too complicated to configure, maintain, or operate, the user will not employ the necessary security mechanisms. For example, if a password is matched during a password change process, the password changing program should state why it was denied rather than giving a cryptic error message. At the same time, applications should not impart unnecessary information that may lead to a compromise in security.
- Example: When we enter a wrong password, the system should only tell us that the user id or password was incorrect. It should not tell us that only the password was wrong as this gives the attacker information.

Cyber Security Principles

- **9. Work Factor**
- This principle states that the cost of circumventing a security mechanism should be compared with the resources of a potential attacker when designing a security scheme. In some cases, the cost of circumventing ("known as work factor") can be easily calculated. In other words, the work factor is a common cryptographic measure which is used to determine the strength of a given cipher. It does not map directly to cyber security, but the overall concept does apply.
- **Example:** Suppose the number of experiments needed to try all possible four character passwords is 24^4 = 331776. If the potential attacker must try each experimental password at a terminal, one might consider a four-character password to be satisfactory. On the other hand, if the potential attacker could use an astronomical computer capable of trying a million passwords per second, a four-letter password would be a minor barrier for a potential intruder.
- **10. Compromise Recording**
- The Compromise Recording principle states that sometimes it is more desirable to record the details of intrusion that to adopt a more sophisticated measure to prevent it. **Example:** The servers in an office network may keep logs for all accesses to files, all emails sent and received, and all browsing sessions on the web. Another example is that Internet-connected surveillance cameras are a typical example of a compromise recording system that can be placed to protect a building.

Purpose of Cyber Security Principles

- Cyber security design principles guide organizations to implement cyber security and protect their information systems and data against cyber-attacks and illicit activities. Any organization can make use of them to facilitate the following processes:
- **1. Governance:** This process focuses on monitoring networks for any suspicious activity. It can be simply understood as identifying and managing security risks, both online and offline.
- **2. Detection:** It aims to detect and identify the events related to security and data breaches. This simply means be on the lookout to identify and understand cyber security events and cyber security incidents.
- **3. Protection:** This is a simple one to understand. Protection involves the implementation of various mechanisms to protect networks and systems against cyber attacks.
- **4. Respond:** This process aims to recover the system or network after the occurrence of a security breach. This means the techniques and tools to mitigate cyber security incidents and recover from them.