Cyber Security

Introduction to Cyber Security

Cyber security Introduction - Cyber Security Basics:

Cyber security is the most concerned matter as cyber threats and attacks are overgrowing. Attackers are now using more sophisticated techniques to target the systems. Individuals, small-scale businesses or large organization, are all being impacted. So, all these firms whether IT or non-IT firms have understood the importance of Cyber Security and focusing on adopting all possible measures to deal with cyber threats.

What is cyber security?

"Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement etc"

OR

Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

- The term cyber security refers to techniques and practices designed to protect digital data

- The data that is stored, transmited or used on an information system.

OR

Cyber security is the protection of Internet - connected systems, including hardware, software, and data from cyber attacks.

It is made up two words one is cyber and other is security.

- Cyber is related to the technology which contains systems, network and programs or data.

- Whereas security related to the protection which includes systems security, network security and application and information security.

Why is cyber security important?

Listed below are the reasons why cyber security is so important in what's become a predominant digital world:

- Cyber attacks can be extremely expensive for businesses to endure.

- In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage
- Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber attacks.
- Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold.

Because of the above reasons, cyber security has become an important part of the business and the focus now is on developing appropriate response plans that minimize the damage in the event of a cyber attack.

But, an organization or an individual can develop a proper response plan only when he has a good grip on cyber security fundamentals.

Cyber security Fundamentals - Confidentiality:

Confidentiality is about preventing the disclosure of data to unauthorized parties.

It also means trying to keep the identity of authorized parties involved in sharing and holding data private and anonymous.

Often confidentiality is compromised by cracking poorly encrypted data. Man-in-the-middle (MITM) attacks, disclosing sensitive data.

Standard measures to establish confidentiality include:

- Data encryption
- Two-factor authentication
- Biometric verification
- Security tokens

Integrity

Integrity refers to protecting information from being modified by unauthorized parties.

Standard measures to guarantee integrity include:

- Cryptographic checksums
- Using file permissions
- Uninterrupted power supplies
- Data backups

Availability

Availability is making sure that authorized parties are able to access the information when needed.

Standard measures to guarantee availability include:

- Backing up data to external drives
- Implementing firewalls
- Having backup power supplies
- Data redundancy

Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

Cyber-attacks can be classified into the following categories :

1. Web-based attacks
2. System-based attacks

Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows -

1. Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example - SQL Injection , code Injection, log Injection , XML Injection etc.

2. DNS Spoofing

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attackers computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

3. Session Hijacking

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

4. Phishing

Phishing is a type of attack which attempts to steal Sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

5. Brute force

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test on organization's network security.

6. Denial of Service

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single Internet connection to attack a server. It can be classified into the following -

Volume-based attacks - Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

Protocol attacks - It consumes actual server resources, and is measured in a packet.

Application layer attacks - Its goal is to crash the web server and is measured in request per second.

7. Dictionary attacks

This type of attack stored the list of a commonly used password and validated them to get original password.

8. URL Interpretation

It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

9. File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

10. Man in the middle attacks

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

System - based attacks

These are the attacks which are intended to compromise a computer or a computer network. Some of the important System - based attacks are as follows -

1 Virus

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self - replicating malicious computer program that replicates by inserting copies of itself into other computer programs when ~~executed.~~ It can also execute instructions that cause harm to the system.

2. Worm

It is a type of Malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

3. Trojan horse

It is a malicious program that occurs unexpected changes to computer selting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened / executed some malicious code will run in the background.

4. Backdoors

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

5. Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

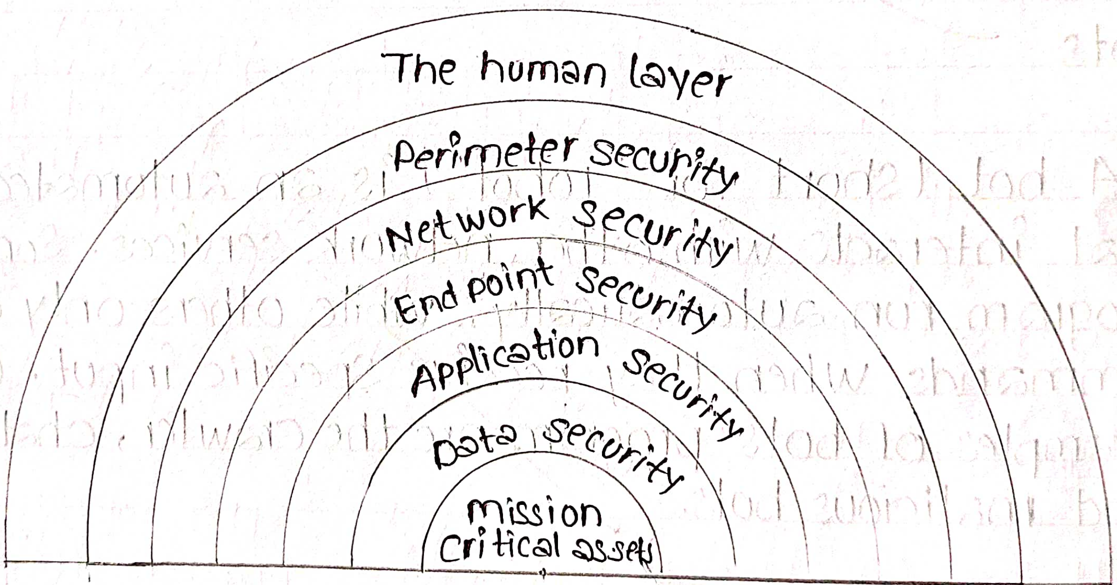
The 7 layers of cyber security should center on the mission critical assets you are seeking to protect.

1. Mission Critical Assets – This is the data you need to protect

2. Data Security – Data security controls protect the storage and transfer of data

3. Application Security – Applications security controls protect access to an application, an application's

The 7 layers of Cybersecurity



access to your mission critical assets, and the internal security of the application.

4. Endpoint Security - Endpoint security controls protect the connection between devices and the network.

5. Network Security - Network security controls protect an organization's network and prevent unauthorized access of the network.

6. Perimeter Security - Perimeter security controls include both the physical and digital security methodologies that protect the business overall.

7. The Human Layer - Humans are the weakest link in any cyber security posture. Human security controls include phising simulations and access management controls that protect mission critical assets from a wide variety of human threats, including cyber criminals, malicious insiders, and negligent users.

Vulnerability, threat, Harmful acts

As the recent epidemic of data breaches illustrates, no system is immune to attacks. Any company that manages, transmits, stores, or otherwise handles data has to institute and enforce mechanisms to monitor their cyber environment, identify vulnerabilities, and close up security holes as quickly as possible.

Before identifying specific dangers to modern data systems, it is crucial to understand the distinction between cyber threats and vulnerabilities.

Cyber threats are security incidents or circumstances with the potential to have a c negative outcome for your network or other data management systems.

Examples of common types of security threats include phising attacks that result in the installation of malware that infects your data, failure of a staff member to follow data protection protocols that cause a data breach, or even a tornado that takes down your company's data headquarters, disrupting access.

Vulnerabilities are the gaps or weaknesses in a system that make threats possible and tempt threat actors to exploit them.

Types of vulnerabilities in network security include but are not limited to SQL injections, server misconfigurations, cross-site scripting, and transmitting sensitive data in a non-encrypted plain text format.

When threat probability is multiplied by the potential loss that may result, cyber security experts, refer to this as a risk.

SECURITY VULNERABILITIES, THREATS AND ATTACKS -

Categories of vulnerabilities

- Corrupted (Loss of integrity)
- leaky (Loss of confidentiality)
- Unavailable of very slow (Loss of availability)

— Threats represent potential security harm to an asset when vulnerabilities are exploited

— Attacks are threats that have been carried out

- Passive - Make use of information from the system without affecting system resources
- Active - Alter system resources or effect operation
- Insider - Initiated by an entity inside the organization
- Outsider - Initiated from outside the perimeter

Computer criminals

Computer criminals have access to enormous amounts of hardware, software, and data ; they have the potential to cripple much of effective business and government throughout the world. In a sense, the purpose of computer security is to prevent these criminals from doing damage.

We say computer crime is any crime involving a computer or aided by the use of one. Although this definition is admittedly broad, it allows us to consider ways to protect ourselves, our businesses, and our communities against those who use computers maliciouly.

One approach to prevention or moderation is to understand who commits these crimes and why. Many studies have attempted to determine the characteristics of computer criminals. By studying those who have already used computers to commit crimes, we may be able in the future to spot likely criminals and prevent the crimes from occuring.

CIA Triad

The CIA Triad is actually a security model that has been developed to help people think about various parts of IT security.

CIA triad broken down:

Confidentiality

It's crucial in today's world for people to protect their sensitive, private information from unauthorized access.

Protecting confidentiality is dependent on being able to define and enforce certain access levels for information.

In some cases, doing this involves separating information into various collections that are organized by who needs access to the information and how sensitive that information actually is - i.e. the amount of damage suffered if the confidentiality was breached.

Some of the most common means used to manage confidentiality include access control lists, volume and file encryption, and Unix file permissions.

Integrity

Data integrity is what the "I" in CIA Triad stands for.

This is an essential component of the CIA Triad and designed to protect data from deletion or modification from any unauthorized party, and it ensures that when an authorized person makes a change that should not have been made the damage can be reversed.

Availability

This is the final component of the CIA Triad and refers to the actual availability of your data. Authentication mechanisms, access channels and systems all have to work properly for the information they protect and ensure it's available when it is needed.

Understanding the CIA triad

The CIA Triad is all about information. While this is considered the core factor of a majority of IT security, it promotes a limited view of the security that ignores other important factors.

For example, even though availability may serve to make sure you don't lose access the resources needed to provide information when it is needed, thinking about information security in itself doesn't guarantee that someone else hasn't used your hardware resources without authorization.

It's important to understand what the CIA Triad is, how it is used to plan and also to implement a quality security policy while understanding the various principles behind it. It's also important to understand the limitations it presents. When you are informed, you can utilize the CIA Triad for what it has to offer and avoid the consequences that may come along by not understanding it.

Assets and Threat

What is an Asset :-

An asset is any data, device or other component of an organization's systems that is valuable - often because it contains sensitive data or can be used to access such information.

For example : An employee's desktop computer, laptop or company phone would be considered an asset, as would applications on those devices. Likewise, critical infrastructure, such as servers and support systems, are assets. An organization's most common assets are information assets. These are things such as databases and physical files - i.e. the sensitive data that you store.

What is a threat :

A threat is any incident that could negatively affect an asset - for example, if it's lost, knocked offline or assessed by an unauthorized party.

Threats can be categorized as circumstances that compromise the confidentiality, integrity or availability of an asset, and can either be intentional or accidental.

Intentional threats include things such as criminal hacking or a malicious insider stealing information, whereas accidental threats generally involve employee error, a technical malfunction or an event that causes physical damage, such as a fire or natural disaster.

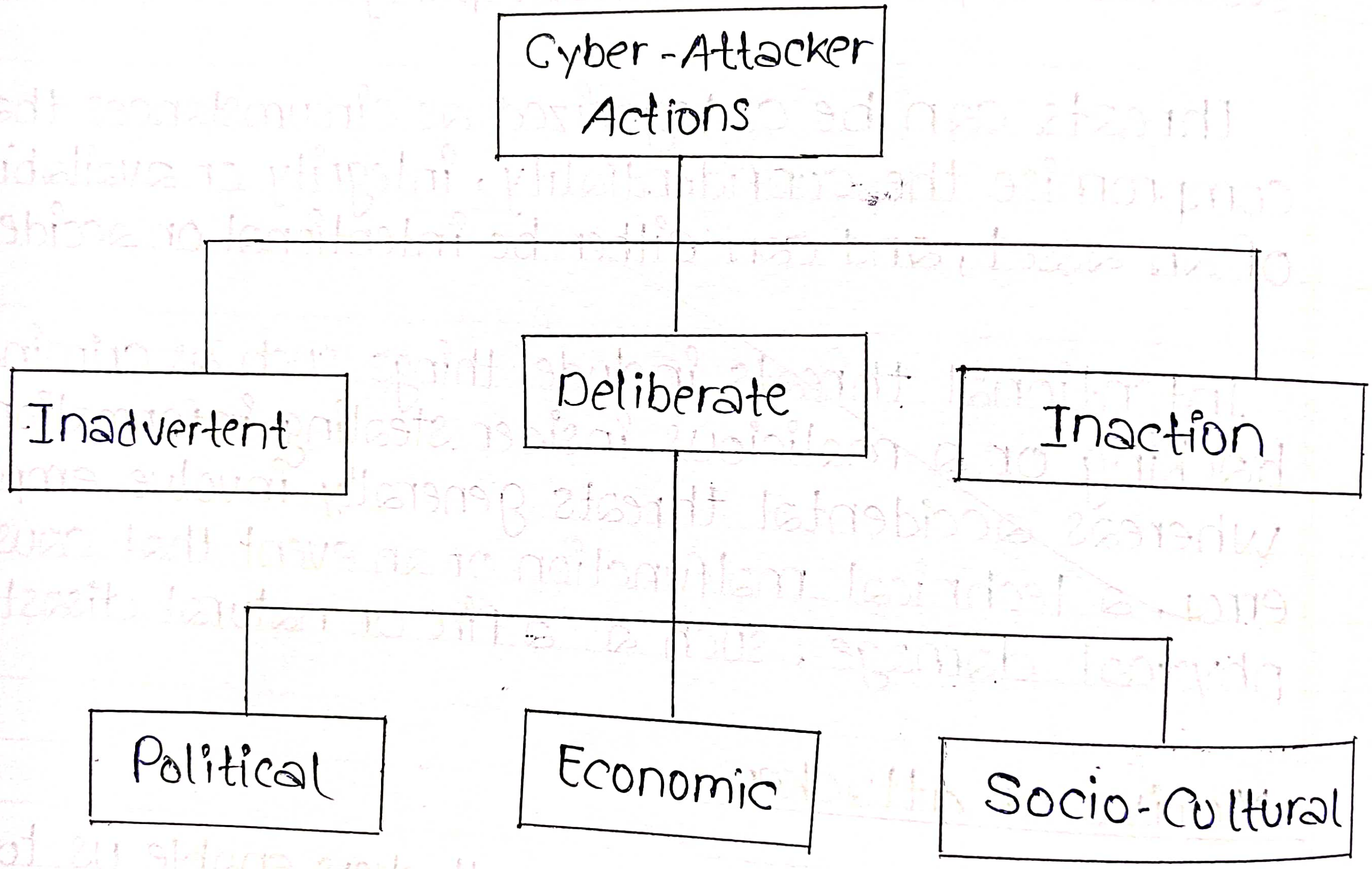
Motive of Attackers

The categories of cyber - attackers enable us to better understand the attackers' motivations and the actions they take. As shown in Figure, operational cyber security risks arise from three types of action: i)

(i) Inadvertent actions (generally by insiders) that are taken without malicious or harmful intent;

(ii) Deliberate actions (by insiders or outsiders) that are taken intentionally and are meant to do harm;

(iii) Inaction (generally by insiders), such as a failure to act in a given situation, either because of a lack of appropriate skills, knowledge, guidance, or availability of the correct person to take action of primary concern


Cyber-Attacker Actions
Inadvertent
Deliberate
Inaction
Political
Economic
Socio-Cultural

here are deliberate actions, of this which there are three categories of motivation.

1. Political motivations :- emamplex include destroying, disrupting, or taking control of targets; espionage; and making political statements, protests, or retaliatory actions.

2. Economic motivations :- examples include destroying, disrupting theft of intellectual property or other economically valuable assets (e.g., funds, credit card information); fraud; industrial espionage and sabotage; and blackmail.

3. Socio-cultural motivations :- examples include attacks with philosophical, theological, political, and even humanitarian goals. Socio-cultural motivations also include fun, curiosity, and a desire for publicity or ego gratification.

Types of cyber-attacker actions and their motivations when deliberate

Active attacks:

An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data enroute to the target.

Types of Active attacks:

Masquerade:- In this attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for. A masquerabe may be attempted through the use of stolen login IDs and passwords, through finding security gaps in programs or through bypassing the authentication mechanism.

Sessio replay: In this type of attack, a hacker steals an authorized user's log in information by stealing the session ID. The intruder gain access and the ability to do anything the authorized user can do on the website.

Message modification: In this attack, an intruder alters packet header addresses to direct a message to a diffent distination or modify the data on a target machine.

In a denial of service (DOS) attack, users are deprived of access to a network or web b resource. This is generally accomplished by overwhelming the target with more traffic than it can handle.