UNIT 6 INTRODUCTION TO CYBER SECURITY

> Introduction to Cyber Security

Cyber Security - the process/practice of protecting computer systems, networks and data from digital attacks, unauthorized access, and breaches

- Also called as Information Technology security / Electronic information security

Importance ? i) Protects sensitive data ii) Prevents Financial loss iii) Maintains Privacy iv) Protects Businesses and Reputation v) Support Growth and Innovations

Principles of Cyber Security ? Confidentiality, Integrity & Availability (CIA)

Layers of Security

Layer 1 - Mission critical assets (most imp parts of company like customer data)
This is data that is essential for core functioning & survival of an organization. This is the information you must safeguard.

Layer 2 - Data security (data is what hackers really want)
This protect the movement and storage of data, which is target of cybercrime. The most care must be taken with this layer because it is the foundation of your company.
Strategy - Encrypt files and disks, Backup imp data regularly, use 2 factor authentication and properly wipe old devices.

Layer 3 - Application Security (apps/software also needs protection from hackers)
This protects applications from unauthorized access and ensures secure communication with mission-critical assets
Strategy - Regularly update applications, Use secure coding & app firewalls.

Layer 4 - Endpoint Security (protects devices like laptop, mobiles)
This protects the connection between user device & the organizational network
Strategy - Encrypt devices, Make sure all devices are safe & updated

Layer 5 - Network Security (not everyone should have access to everything)
This focuses on safeguarding internal systems & ensuring that users & devices have limited access inside the network.
Strategy - Give access to only those parts of network that employees really need, Use network segmentation to limit any damage if attack happens.

Layer 6 - Perimeter Security (protecting company's boundary both physically & digitally)
Makes sure that both the physical & digital security methods protect overall business
Strategy - Use firewalls, antivirus software.

Layer 7 - The Human Layer

Humans are considered the weakest link in cybersecurity, responsible for almost 90 % of data breaches. Mission-critical assets must be protected from cybercriminals, malicious insiders, phishing simulations, etc.

Strategy - Teach ppl about cyber threats like phishing, Train them to use strong passwords & follow safe habbits, Use access control to limit what users can do.

Vulnerability

The weakness or flaw in system that attackers can use to break in or cause damage.

Examples - App that is not updated and has a bug.
A weak password like '12345'.
A server without firewall.
Employees clicking on phishing emails.

Vulnerabilities mostly happens due to —

i) Hardware Vulnerability
Problems in physical devices like chips, computers, routers.
Eg. manufacturing defects, unprotected ports.
Soln: Use trusted hardware vendor, Secure device settings.

ii) Software Vulnerability
Weakness in programs or applications.
Eg: Bugs, outdated software, wrong coding practices.
Soln: Regular updates, secure coding

iii) Network vulnerability
Issues in how data travels betn systems.
Eg. Unsecured Wifi, open ports, no firewall.
Soln: Use encryption, firewalls

iv) Procedural Vulnerability
Weakness due in organizaion operational methods.
Eg. Password procedure, training procedure
Soln: Teach them about threats.

Threats

A Threat is any potential danger that can exploit a vulnerability in a system to cause harm, steal data or damage systems

Types:

- Malware - malicious software designed to damage / steal data
- Phishing - fraudulent attempts to steal sensitive info often through fake emails or websites.
- MITM - When attacker intercepts & alter communication betn 2 parties
- DOS - Attackers flood system with requests causing it to crash
- SQL Injection - Attackers insert malicious code into SQL query to steal data.
- Password Attacks - Attempts to crack passwords using various methods.

Harmful acts -

Malware = malicious software.
software that is created to damage, steal or compromize systems & data.
The unwanted tasks are performed in host computer for the benefit of third party. displays unwanted advertisements & collect user data
Eg. Virus, Worm (self-replicating program), Spyware (secret spy), Adware

MITM (Man In The Middle)
Attacker secretly listens in / changes the conversation betn 2 parties.

SQL Injection
The attacker inserts malicious SQL code into the input field on a website in order to access the database.

DOS Attack
Attacker makes the network unavailable for user to communicate, by overloading it with unwanted messages.

Internet Governance
Internet Governance refers to the rules, policies, and processes that guide how the internet operates and how it is used. It involves decisions about how the infrastructure of the internet is built, managed and regulated.

Who is Involved in Internet Governance?
1) Government - create laws & policies related to the internet use & digital infra
2) Private sector - companies like Google, Microsoft and ISP help build & manage internet infrastructure.
3) International Organizations - work on global agreements & policies to manage the internet. Eg. ICANN.
4) Civil society - Non-profit organizations, activities & communities that advocate for users rights, privacy and freedom of expression. Eg. EFF

Issues in Internet Governance?
1) Some ppl dont have internet access (ppl in remote / poor areas)
2) Controlling what ppl see online
3) Copying & Stealing content
4) AI & Technology moving fast
5) Data is constantly been collected
6) Different countries want diff things (Tiktok is banned in India)
7) Cyber attacks and Online Safety.

Key aspects
1) Infrastructure & Standardization Line - It covers hardware & standard rules
2) Logical dimension - refers to rules, protocols and systems that allow data to be transfered processed & structured on the internet. Its about how data is organized & communicated logically.
3) Content dimension - actual data & info that is shared on the internet.

4) Social Dimension - focus on impact of internet on society.
5) Development Dimension - how internet contibutes to social & economical development.

Computer Criminals

The individuals or groups who use computers and the internet to commit illegal activities. They can target people, organizations, or even governments for personal gain, harm or simply out of malice.

Hackes - gain unauthorised access to computer/networks.
Phishers - trick people into giving up personal info.
Cyberstalkers - use internet to stalk others., etc.

Types of cybercrime? Hacking, Child pornography and abuse, Theft, Malicious software, fraud mails/calls, Dark web (Online illegal selling) etc

Assets and Threats

An asset is any data, device or other component that is valuable.
Asset is valuable because it contains sensitive information or can be used to access such information.
Asset contains hardware, software and confidential information.
Eg. Personal data (your name, password, bank details), company's confidential documents, Servers, laptops and mobile phones, Intellectual property (like product design, software codes), etc.

Motive of attackers

Types of cyber-attacker action:
1) Inadvertent actions (By Mistake) - These are generated by insiders. These actions are taken without malicious/harmful intention.
Eg. Accidently sends a secret file to wrong person by email

2) Deliberate actions (On purpose) - Generated by insiders or outsiders. These actions are taken intentionally and are intended to do harm.
   - ↳ Political motivation - destroying, disrupting, spying & making political statements, etc
   - ↳ Economical motivation - stealing of intellectual property like funds, credit card details, blackmailing, etc.
   - ↳ Socio-cultural motivation - fun, curiosity, desire for publicity or ego satisfaction

3) Inaction (Doing Nothing) - Generated by insiders. Fails to act or ignores known security issue. Lack of skills, knowledge. Eg weak password.

Types of Attacks - Active & Passive

Software Attacks

It happens when an attacker uses a program / malicious code to damage, steal or control computer or network. ((Malware??))

Types of malware/software attacks

1) Virus - self replicating program code. It needs your action to activate like opening a file. It corrupts or deletes files.
2) Worm - Replicating code that comes via emails. It slows down networks, eats up bandwidth.
3) Trojan Horse - Looks like useful program but is actually harmful inside. It steals your data or gives control to hackers.
4) Adware - Used for forced advertising. Slows down device and tracks browsing.
5) Spyware - spy on what you do & steals data without knowing.
6) Scareware - scares you with fake warnings to trick you into buying fake software. (eg. Your PC is infected)

Hardware Attacks

It happens when physical parts of a computer are damaged, modified or hacked. (chips, usb, servers)

Examples include

1) Damaging devices - like physically breaking servers
2) Inserting malicious hardware.
3) Hardware Trojans - Tiny bad circuits added secretly during manufacturing that later allows hackers to control the device.
4) Eavesdropping Hardware - Spl. hardware tool that capture your keyboard typing (called "keyloggers")
5) Side channel attacks - Hacker use info like electricity usage, sound or timing to guess secret data from the device.

Cyber Threats

Cyber Warfare – When countries attack each other using computers & internet instead of weapons. Goal is to damage important systems (like power plants, defense systems) of enemy country.

Types of cyber warfare

1) Espionage (spying) - spying other countries to steal secret.
2) Sabotage (Destruction) - Attacking critical systems to damage, destroy or stop important services. Eg. shutting down water supply.
3) DOS attack
4) Propoganda - Spreading fake news to change public opinion or create confusion
5) Surprise Attack - sudden, without warning attack.

Cyber Crime – Crimes done using computers or internet. Goal is to steal money, data or harm people.
Example: Online frauds, hacking, identity theft.

Cyber Stalking – following, threatning or harrasing someone online repeatedly. It is an act of constant & unwanted contact from someone online. Goal is to scare or control the victim
Eg. Sending creepy msg again & again, watching someone's activities online without permission.
Who? Coworkers, Former spouses, Friends, Boyfriends, Girlfriends, Ex partners, Online associates, etc

Cyber Terrorism – Using computers or internet to create fear, damage systems or harm people for political or religious reasons. Goal is to spread fear like real terrorism but through technology.
Eg. Hacking airports, hospitals, government websites.

Cyber Espionage – Spying on companies or countries through hacking to steal secrets. Goal is to get confidential information.
Eg. Stealing military secrets, company trade secrets, etc.