DAR ES SALAAM INSTITUTE OF TECHNOLOGY

(DIT)

CLASS: OD21IT

COURSE: ORDINARY DIPLOMA IN INFORMATION TECHNOLOGY

MODULE NAME: CYBER SECURITY AND PRIVACY

MODULE CODE: ITT 06218

LECTURER NAME: SAKINA MSONDE

TASK: GROUP ASSIGNMENT

STUDENT NAME	REGISTRATION
VALENCE MWIGANI	210210920638
FAUDHIA KAYAGE	2102209110461
ALLY IDRIS	2102209210212
SULEIMAN ABDALAH	210210920620
EMMANUEL SWAY	2102209212994

IDENTIFY CYBER SECURITY PREVENTIVE MECHANISMS FROM COMMON CYBERSECURITY THREATS AND ATTACKS.

Preventive mechanism in cyber security is a shield against cyber-attacks or a proactive measures designed to stop threats in their tracks before they can wreak havoc on your systems and data.

PREVENTIVE MECHANISMS FROM COMMON CYBERSECURITY THREATS AND ATTACKS.

Phishing

In phishing, an attacker masquerades as a reputable organization or individual to trick an unsuspecting victim into handing over valuable information, such as passwords, credit card details and intellectual property. . Emails are most commonly used to distribute malicious links or attachments.

Phishing Emails preventive mechanism *(User Awareness Training and Multi-Factor Authentication (MFA))* Educate users to identify phishing attempts (sender address, urgency, generic greetings).Implement MFA to add an extra layer of login security beyond passwords.

Malware, short for malicious software, is an umbrella term used to refer to a hostile or intrusive program or file that's designed to exploit devices at the expense of the user and to the benefit of the attacker.

Malware preventive mechanism is use *of Up-to-date Anti-Malware Software and Secure Downloads.* Use reputable anti-malware software that actively scans for and removes threats. Practice safe download habits (trusted sources, verify file extensions).

Password Attacks

This consist of Brute-Force and Dictionary Attacks. Brute-force attack occurs when an attacker can try well-known passwords, such as password123, or ones based on information gathered from a target's social media posts, like the name of a pet, to guess user login credentials through trial and error. Dictionary attack. Similar to a brute-force attack, a dictionary attack uses a preselected library of commonly used words and phrases, depending on the location or nationality of the victim.

Its preventive mechanisms are use of *Strong Passwords and Password Managers*. Use complex passwords with a combination of uppercase and lowercase letters, numbers, and symbols. *Password managers* generate and store strong, unique passwords for different accounts. Account lockouts automatically disable access after a certain number of failed login attempts, hindering brute-force and dictionary attacks.

Denial-of-Service (DoS) Attacks attack involves the use of numerous compromised computer systems or mobile devices to target a server, website or other network resource.

Its preventive mechanism are Traffic Filtering & Redundancy

Traffic Filtering: Implement traffic filtering mechanisms to identify and block malicious traffic patterns during DoS attacks. This could involve analyzing traffic volume, source IP addresses, and packet content.

Redundancy: Utilize redundant servers or cloud-based solutions to ensure service continuity even if one server is overwhelmed by a DoS attack. This distributes traffic across multiple servers, minimizing the impact of the attack.

SQL Injection Attacks. A SQL query is a request for some action to be performed on a database, and a well-constructed malicious request can create, modify or delete the data stored in the database. It can also read and extract data such as intellectual property, personal information of customers or employees, administrative credentials and private business details.

Its preventive mechanism include Input Validation & Database Security

Input Validation: Enforce strict input validation on web applications to sanitize user input before processing it. This prevents attackers from injecting malicious code (e.g., SQL queries) that could exploit vulnerabilities in the database.

Database Security: Implement strong database security measures like: User authentication with strong passwords and access controls. Encryption of sensitive data at rest and in transit. Regular security audits and vulnerability assessments of the database infrastructure.

Man-in-the-Middle (MitM) Attacks the attacker secretly intercepts messages between two parties. A successful MitM attack enables attackers to capture or manipulate sensitive personal information, such as login credentials, transaction details, account records and credit card numbers.

Man-in-the-Middle (MitM) preventive mechanisms are *Encryption and Secure Connections*. Enforce HTTPS (Hypertext Transfer Protocol Secure) for all web traffic. HTTPS encrypts communication between your browser and the server, making it impossible for attackers to intercept data in transit during a MitM attack.

Secure Connections: Use secure connections Virtual Private Networks (VPNs)

URL interpretation/URL poisoning

A URL Interpretation attack, also sometimes referred to as URL poisoning, is used to gather confidential information, such as usernames and database records, or to access admin pages that are used to manage a website. If an attacker does manage to access privileged resources by manipulating a URL, it's commonly due to an insecure direct object reference vulnerability in which the site doesn't properly apply access control checks to verify user identities.

Preventive Mechanisms for Malicious URL Interpretation:

User Awareness Training: Educate users on identifying red flags in URLs, such as:

Misspelled domain names (e.g., “eample” instead of “example”).

Unusual subdomains or paths (e.g., a bank website URL shouldn’t lead to an “.exe” file download).

Hovering over the link to see the actual destination address (often different from the displayed text).

Security Software: Some security software solutions can scan URLs for suspicious content or known phishing attempts and warn users before they click.

HTTPS Everywhere: This browser extension automatically enforces HTTPS encryption for websites whenever possible, making it harder for attackers to intercept data.

Ransomware

Ransomware is usually installed when a user visits a malicious website or opens a doctored email attachment. Traditionally, it exploits vulnerabilities on an infected device to encrypt important files, such as Word documents, Excel spreadsheets, PDFs, databases and system files, making them unusable. The attacker then demands a ransom in exchange for the decryption key needed to restore the locked files

Some preventive mechanisms to safeguard yourself from ransomware attacks:

Backups:

Regular Backups: Implement a regular backup schedule for your critical data. Backups should be stored offline on a separate device or cloud storage with strong access controls. This ensures you have a clean copy of your data to restore in case of an attack.

Test Backups: Regularly test your backups to ensure they are complete and usable. A successful backup test verifies that you can restore your data in case of a ransomware attack.

User Education:

Phishing Awareness: Train users to identify phishing emails that could lead to ransomware infection. Educate them on red flags like suspicious attachments, generic greetings, and urgency tactics.

Safe Download Practices: Educate users on safe download practices. This includes downloading files only from trusted sources and verifying file extensions before opening them.

SUMMARY ON PREVENTIVE MECHANISM FROM COMMON CYBER SECURITY THREATS AND ATTACKS

THREATS AND ATTACKS	TYPES	PREVENTIVE MECHANISM
Phishing	phishing emails	1. User Awareness Training 2.Multi-Factor Authentication (MFA)
Malware	Viruses, Trojan	1.Up-to-date Anti-Malware Software 2. Secure Downloads
Password Attacks	Brute-Force attacks Dictionary Attacks	1. Strong Passwords 2. Password Managers.
Denial-of-Service (DoS) Attacks	flooding services crashing services	1. Traffic filtering 2. Redundancy
SQL Injection Attacks	In-Band SQLi Error- based SQLi	1. Input validation 2. Database security
Man-in-the-Middle (MitM)	Email hijacking Wi-Fi eavesdropping	1. Encryption 2. Secure Connections
URL interpretation/URL poisoning	Malware infection Data manipulation	1. User awareness training 2. Security software 3. HTTPs everywhere
Ransomware	Locker ransomware Wiper ransomware	1. Backups a) Regular backups b) Test backups 2. User education a) phishing awareness b) Safe download practices

REFERENCE

https://www.techtarget.com/searchsecurity/tip/6-common-types-of-cyber-attacks-and-how-to-prevent-them

https://www.bluevoyant.com/knowledge-center/7-types-of-cyber-threats-how-to-prevent-them-2022-guide

https://www.bluevoyant.com/knowledge-center/7-types-of-cyber-threats-how-to-prevent-them-2022-guide#cyber-threat-prevention-strategies