Assignment-1

SUBMITTED BY:
AYUSH KUMAR JHA
500086400
B.C.A-IOT (2020-2023)

Cyber-security

Cybersecurity is the protection of internet-connected systems such as hardware, software, and data from cyber threats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

With an increasing number of users, devices, and programs in the modern enterprise, combined with the increasing deluge of data -- much of which is sensitive or confidential -- the importance of cybersecurity continues to grow. The growing volume and sophistication of cyber attackers and attack techniques compound the problem even further.

The cybersecurity field can be broken down into several different sections, the coordination of which within the organization is crucial to the success of a cybersecurity program.

These sections include the following:

Maintaining cybersecurity in a constantly evolving threat landscape is a challenge for all organizations. Traditional reactive approaches, in which resources were put toward protecting systems against the biggest known threats, while lesser-known threats were undefended, are no longer a sufficient tactic. To keep up with changing security risks, a more proactive and adaptive approach is necessary. Several key cybersecurity advisory organizations offer guidance. For example, the National Institute of Standards and Technology (NIST) recommends adopting continuous monitoring and real-time assessments as part of a risk assessment framework to defend against known and unknown threats.

The benefits of implementing and maintaining cybersecurity practices include:

- Business protection against cyberattacks and data breaches.
- Protection for data and networks.
- Prevention of unauthorized user access.
- Improved recovery time after a breach.

- Protection for end-users and endpoint devices.
- Regulatory compliance.
- Business continuity.
- Improved confidence in the company's reputation and trust for developers, partners, customers, stakeholders, and employees.

The process of keeping up with new technologies, security trends and threat intelligence is a challenging task. It is necessary in order to protect information and other assets from cyber threats, which take many forms. Types of cyber threats include:

- Malware is a form of malicious software in which any file or program can be used to harm a computer user. This includes worms, viruses, Trojans and spyware.
- Ransomware is another type of malware. It involves an attacker locking the victim's computer system files -- typically through encryption -- and demanding a payment to decrypt and unlock them.
- Social engineering is an attack that relies on human interaction to trick users into breaking security procedures to gain sensitive information that is typically protected.
- Phishing is a form of social engineering where fraudulent email or text messages that resemble those from reputable or known sources are sent. Often random attacks, the intent of these messages is to steal sensitive data, such as credit card or login information.
- Spear phishing is a type of phishing attack that has an intended target user, organization, or business.
- Insider threats are security breaches or losses caused by humans -- for example, employees, contractors, or customers. Insider threats can be malicious or negligent in nature.
- Distributed denial-of-service (DDoS) attacks are those in which multiple systems disrupt the traffic of a targeted system, such as a server, website, or other network resources. By flooding the target with messages, connection requests, or packets, the attackers can slow the system or crash it, preventing legitimate traffic from using it.
- Advanced persistent threats (APTs) are prolonged targeted attacks in which an attacker infiltrates a network and remains undetected for long periods of time with the aim to steal data.

- Man-in-the-middle (MitM) attacks are eavesdropping attacks that involve an attacker intercepting and relaying messages between two parties who believe they are communicating with each other.

Other common attacks include botnets, drive-by-download attacks, exploit kits, malvertising, vishing, credential stuffing attacks, cross-site scripting (XSS) attacks, SQL injection attacks, business email compromise (BEC), and zero-day exploits.