Cyber Security

Information System

Dr. Ibrahim El Awadi

Mostafa ashraf ali
Mostafa Mahmoud
Mahmoud wael

Definition of Cyber Security

Cyber security is the body of technologies and process which practices protection of network, computers, data and programs from unauthorized access, cyber threats, attacks or damages.

It deals with controlling physical access to hardware alongside protecting harm coming via network access and code injection.

The sole purpose of cyber security is to defend the integrity of computing assets belonging to or connecting to an organization's network.

Evolution of Cyber Security

Cyber security practices continue to evolve as the internet and digitally dependent operations develop and change. According to Secureworks, people who study cyber security are turning more of their attention to the two areas in the following sections.

The Internet of Things

Individual devices that connect to the internet or other networks offer an access point for hackers. Cytelligence reports that in 2019, hackers increasingly targeted smart home and internet of things (IoT) devices, such as smart TVs, voice assistants, connected baby monitors and cellphones. Hackers who successfully compromise a connected home not only gain access to users' Wi-Fi credentials, but may also gain access to their data, such as medical records, bank statements and website login information.

The Explosion of Data

Data storage on devices such as laptops and cellphones makes it easier for cyber attackers to find an entry point into a network through a personal device. For example, in the May 2019 book Exploding Data: Reclaiming Our Cyber Security in the Digital Age, former U.S. Secretary of Homeland Security Michael Chertoff warns of a pervasive exposure of individuals' personal information, which has become increasingly vulnerable to cyber attacks.

Consequently, companies and government agencies need maximum cyber security to protect their data and operations. Understanding how to address the latest evolving cyber threats is essential for cyber security professionals.

Types of Cyber Security Threats

Cyber security professionals should have an in-depth understanding of the following types of cyber security threats:

1. Malware

- Block access to key network components (ransomware)
- Install additional harmful software
- Covertly obtain information by transmitting data from the hard drive (spyware)
- Disrupt individual parts, making the system inoperable

2. Emotet

3. Denial of Service

4. Man in the Middle

5. Phishing

6. SQL Injection

7. Password Attacks

Advantages of studying cyber security

- The ability to get any information you want to know
- The salaries are rewarding and high
- The specialization is required in the future as it is one of the technological specialties
- Job opportunities are available due to the lack of graduates
- Gain a lot of logical thinking skills
- Developing competencies and level of professionalism in the field of computer science
- Protect data and information from leakage, theft, practical plagiarism, and infringement of copyright and preservation rights
- Keeping pace with technological development
- Provide an advanced level of protection
- Provide an advanced level of protection

Disadvantages of studying cyber security

- Cybersecurity guarantee requires many stages of application security and data security
- Difficulty dealing with firewalls, known as firewalls
- The need to always update new software in order to maintain security systems
- Consume a lot of time
- The labor market needs a high level of experience to work in this field

What is meant by the security triangle (confidentiality, integrity and availability of information) CIA :

Confidentiality:

What is meant by confidentiality of information is to ensure that information is only accessed by the persons authorized to access this information, in addition to setting the foundations and standards for the access process and the necessary powers to do so in a manner that categorically guarantees that only persons authorized to access this information can obtain it and no one else can that.

Integrity:

Integrity means maintaining consistency and accuracy of data throughout its entire life cycle and ensuring that it is not altered or replaced during the information life cycle. Data must not be altered during transmission, and steps must be taken to ensure that data cannot be altered by unauthorized persons.

Availability:

Availability of information means that information is available when requested or needed at any time. Availability is best ensured by keeping all devices in a healthy and efficient condition, making repairs immediately when needed, and making sure that the operating system gets the necessary updates and upgrades.