Cyber Security

Introduction

The 1970s was the genuine start of cyber security. This all started with the Advanced Research Projects Agency Network project (ARPANET). This was the connectivity network that existed before the internet. A man named Bob Thomas discovered that a computer program could be moved across a network. As it moved, the software would leave a trail behind it. He designed the application to be able to navigate between Tenex terminals over ARPANET. The software was called the 'Creeper'.

Ray Tomlinson, the creator of email, created the Reaper, which was a tracking program that tracked down and eliminated the Creeper. Thus, the Reaper was the first computer worm and the first example of antivirus software. It was also the first self-replicating program.

Definition

Cyber security is the use of technology, processes, and controls to defend against cyber-attacks on systems, networks, programs, devices, and data.

When to Use it

It is best for individuals and businesses who wants to protect and manage their risks as they make use of the web.

Details

Cyber security is a procedure that safeguards networks and devices against external attacks. Businesses generally hire Cyber Security professionals to safeguard sensitive information, maintain staff productivity, and boost customer trust in products and services. It is a collection of strategies used to safeguard the integrity of networks, programs, and data against assault, damage, or unwanted access.

Governments realized that unauthorized access to this vast infrastructure may cause a slew of issues. In the second half of the decade, a number of scholarly publications were published that looked into techniques to ensure this security. They also went over the potential dangers.

Types of Cyber dangers include the following:

1. **Malware** - Malware refers to malicious software, which is the most prevalent method of cyber-attack. The cybercriminal or hacker uses it to disrupt or harm the system of a legitimate user. Botnet software, RATs (remote access Trojans), rootkits and bootkits, spyware, Trojans, viruses, and worms are all examples of malware.
2. **Phishing** - Phishing is a sort of cybercrime in which the sender appears to be a legitimate entity such as PayPal, eBay, financial institutions, or friends and coworkers. Usually it is in a form of a link which will take users to a fake website where they will be asked to enter sensitive information such personal information, banking and credit card information, social security numbers, usernames, and passwords. By clicking the link, malware will be installed on the target machines, allowing hackers to remotely control them.
3. **SQL Injection (SQLI)** - SQL injection is a typical attack in which fraudsters manipulate backend databases with malicious SQL scripts to get access to critical information. The hostile actor can see, edit, or remove sensitive company data, user lists, or private customer details stored in the SQL database after the attack is successful.
4. **Domain Name System (DNS) attack** - DNS poisoning attacks, which corrupt the DNS in order to reroute traffic to malicious websites. The cyber thieves utilize weaknesses in the Domain Name System to redirect users to malicious websites and steal data from targeted machines.
5. **Distributed denial of service (DDoS)** - It is a form of cyber threat or malicious effort in which fraudsters use Internet traffic to fulfill legitimate requests to the target or its surrounding infrastructure, causing the target's regular traffic to be disrupted.

Examples

Critical infrastructure cyber security

Because SCADA (supervisory control and data acquisition) systems generally rely on older software, critical infrastructure organizations are more vulnerable to attack than others. The Regulations, among other things, require businesses to take suitable technical and organizational steps to control their security risks.

Network Security

Addressing vulnerabilities in your operating systems and network architecture, including servers and hosts, firewalls and wireless access points, and network protocols, is part of network security.

Cloud Security

Cloud security is a set of procedures and technology aimed at addressing external and internal security concerns. As they implement their digital transformation strategy and include cloud-based tools and services into their infrastructure, businesses require cloud security.

IoT (Internet of Things) security

IoT security is the act of protecting Internet devices and the networks to which they're connected from threats and breaches by identifying, protecting, and monitoring risks, as well as assisting in the repair of vulnerabilities from a variety of devices that can pose security risks to your business.

Application security

Application security is the process of creating, integrating, and testing security measures into applications to protect them from dangers like illegal access and alteration. Addressing vulnerabilities originating from unsafe development processes in the design, coding, and publication of software or a website is what application security is all about.

References:

https://www.ibm.com/ph-en/topics/cloud-security#:~:text=Cloud%20security%20is%20a%20collection,as%20part%20of%20their%20infrastructure.

https://cybermagazine.com/cyber-security/history-cybersecurity

https://www.simplilearn.com/introduction-to-cyber-security-article#cyber_security_education

https://www.itgovernance.co.uk/what-is-cybersecurity

https://www.fortinet.com/resources/cyberglossary/iot-security#:~:text=Security%20in%20IoT%20is%20the,security%20risks%20to%20your%20business.