Tyrone Joshua C. Jaco
CS301

Common Threats to Devices

1.) **Attacks with Denial-of-Service (DoS)**

Through Denial-of-Service attacks, attackers can overload devices with traffic, making them unavailable and interfering with regular operations.

2.) **Zero-Day Exploits**

Before developers can release patches or updates, devices are susceptible to attacks that take advantage of undiscovered software vulnerabilities (zero-day exploits).

3.) **Physical Loss or Theft**

Devices are vulnerable to physical theft or loss, which could reveal private data to uninvited parties and call for strong physical security measures.

4.) **Spyware and malware**

Malicious software, such as spyware and malware, can compromise device security and privacy and is frequently installed without the user's knowledge or consent.

5.) **Bot networks**

Devices have the potential to join botnets—a network of compromised systems—that are managed by hackers and used to carry out malicious tasks like orchestrating coordinated attacks.

Common Threats to Local Access Networks

1.) **Unprotected Wireless Networks**

It is imperative to utilize secure connections to protect data, as connecting to unprotected Wi-Fi networks leaves devices vulnerable to possible eavesdropping and illegal access.

2.) **Interception of Data**

Threat actors can intercept and steal data while it is in transit, jeopardizing the privacy of sensitive data as it moves between networks and devices.

3.) **Misconfigured Networks**

Vulnerabilities brought about by improperly configured network settings may result in security breaches.

4.) **Eavesdropping**

unapproved network communication interception that compromises private data.

5.) **Unauthorized Entry**

Threat actors entering local networks without authorization, which could result in data breaches or system manipulation.

Common Threats to Cloud Domains

1.) **Lack of Compliance**

noncompliance with industry or regulatory compliance standards, putting data security and legal ramifications at danger.

2.) **Insecure APIs**

Cloud application programming interface (API) vulnerabilities could be used to gain unauthorized access or manipulate data.

3.) **Insufficient Identity and Access Management**

Unauthorized people may obtain unauthorized permissions as a result of poorly maintained user access controls.

4.) **Outages in Cloud Services**

Access to vital apps and data, as well as business operations, may be impacted by disruptions in cloud services.

5.) **Shared Technology Vulnerabilities**

When numerous users share the same underlying cloud infrastructure, there is a risk because vulnerabilities could impact numerous entities.

Common Threats to Physical Facilities

1.) **Natural Disasters**

Catastrophes such as earthquakes, fires, or floods can harm buildings, interfering with business operations and possibly resulting in data loss.

2.) **Social Engineering Attacks**

manipulation of people to enter buildings without authorization, frequently by taking advantage of weaknesses in people.

3.) **Theft or Loss of Devices**

Information security is directly threatened when devices holding sensitive data are physically stolen or lost.

4.) **Unauthorized Access to Facilities**

Sensitive data and equipment can be compromised by intruders who physically enter buildings.

5.) **Supply Chain Risks**

Inadequate security in the supply chain may result in vulnerabilities being introduced into physical facilities.

Laws that prohibit cybercrime in the Philippines

1.) **Republic Act No. 10175 (Cybercrime Prevention Act of 2012)**

This law, which was passed on September 12, 2012, defines and addresses cybercrime and offers procedures for its investigation, prevention, and repression.

2.) **Anti-Child Pornography Act of 2009 (Republic Act No. 9775)**

This law, which focuses on crimes committed online, makes it illegal to create, possess, or distribute child pornography and imposes fines on offenders.

3.) **Data Privacy Act of 2012 (Republic Act No. 10173)**

This act, which prioritizes data protection, ensures the security and privacy of people's data by instituting measures to prevent unauthorized access to personal information.

4.) **Electronic Commerce Act of 2000 (Republic Act No. 8792)**

This law addresses offenses related to computers, such as hacking and unauthorized access to computer systems, while also promoting e-commerce.

5.) **Cybersecurity Act of 2012 (Republic Act No. 10844)**

In order to provide a secure cyber environment and protect the country's vital information infrastructure from cyber threats, this law establishes the National Cybersecurity Plan.

Cyber Laws & Liabilities in the US (Civil, Criminal, & Regulatory)

1.) **Gramm-Leach-Bliley Act (GLBA) - Regulatory**

A regulatory law known as GLBA requires financial institutions to put security measures in place and protect the privacy of their consumers.

2.) **Health Insurance Portability and Accountability Act (HIPAA) - Regulatory**

HIPAA is a set of regulations that governs how electronic health information is protected, protecting patient privacy and security in the healthcare industry.

3.) **Federal Trade Commission (FTC) Act - Regulatory**

The FTC Act gives the Federal Trade Commission the authority to impose rules and regulations against unfair or deceptive cybersecurity practices.

4.) **Electronic Communications Privacy Act (ECPA) - Civil**

By controlling electronic communication interception and safeguarding electronic communication privacy, ECPA addresses civil concerns.

5.) **Computer Fraud and Abuse Act (CFAA) - Criminal**

The CyberFinancial Access Act (CFAA) makes hacking and data theft illegal and penalizes unauthorized access to computer systems.