Introduction

Madiba Hudson-Quansah

Contents

Chapter 1

Introduction

Definition 1.0.1: Security

A state of being secure and free from danger or harm, i.e. the actions taken to make someone or something secure. Protection from adversaries (those who would do harm), intentionally or otherwise, is the goal of security.

1.1 Key Objectives of Security

Definition 1.1.1: Repudiation

The ability to deny the authenticity of one's signature on a document or a message that one originated.

Confidentiality - Covers data confidentiality and privacy.

- **Data Confidentiality** - Information is not made available or disclosed to unauthorized individuals, entities, or processes.

- **Privacy** - Assures that individuals control or influence what information related to them may be collected and stored, and by whom and whom that information may be disclosed.

Integrity - Data Integrity and System Integrity.

- **Data Integrity** - The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.

- **System Integrity** - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability - Assures that systems work promptly and service is not denied to authorized users.

Authenticity - The property of being genuine and being able to be verified and trusted. Ensures users are who they say they are and that each input arriving at the system came from a trusted source.

Accountability - Assures that the actions of an entity can be traced uniquely to that entity. Supports non-repudiation, deterrence, fault isolation, intrusion detection, and after-the-fact forensic analysis.

The CIA triad (Confidentiality, Integrity, and Availability) is a widely used model for understanding and implementing security measures. Additionally Accountability and Authenticity are also important objectives in security, making the complete set often referred to as the CIAAA triad.

Chapter 2

Terminology

2.1 Asset

Definition 2.1.1: Asset / System Resource

Anything that needs to be protected because it has value to an organization, both tangible and intangible.

There are general asset categories:

Hardware - Physical devices that support computing and networking

Software - Programs and system components that run on hardware

Data - Information that organizations store, process and transmit. Generally the most important asset.

Communication facilities and Networks - Infrastructure that enables data transfer and connectivity.

People - Human actors who interact with or affect information systems.

2.2 Vulnerability and Threats

Definition 2.2.1: Vulnerability

A weakness in an asset that could be exploited or triggered by a threat source.

Examples of vulnerabilities include:

- Unpatched applications or operating systems
- An unrestricted wireless access point.
- An open port on a firewall.

Definition 2.2.2: Threat

Any circumstance or event with the potential to adversely impact organizational operations, assets, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information , and/or denial of service.

Definition 2.2.3: Threat Agent

An entity that can cause harm to an asset. Represents the source of a threat. Can be forces of nature, as well as human or non-human actors.

Definition 2.2.4: Adversary

An individual, group, organization or government that conducts or has the intent to conduct detrimental activates. Considered a human threat agent or attacker.

Definition 2.2.5: Attack

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade or destroy information system resources or the information itself.

2.3 Security Controls and Countermeasures

Definition 2.3.1: Security Control / Safeguard

Any measure or mechanism put in place to protect the confidentiality, integrity, and availability of an information system. For example, policies, procedures, technical measures, and physical protections.

Definition 2.3.2: Countermeasure

A device or technique with the objective of the impairment of the operation effectiveness of adversarial activities. All countermeasures are security controls, but not all security controls are countermeasures. For example deploying an antivirus in response to a data breach.

Some security control categories are:

Physical Controls

- Locks
- Walls / Fences
- Guards

Prodedural / Administrative Controls

- Laws
- Regulations
- Policies

Techinical

- Passwords
- Access Controls
- Firewalls

2.4 Risk and Risk Management

Definition 2.4.1: Risk

A measure of the extent to which an entity it threatened by a potential event. A function of

- The adverse impacts that would arise if the circumstance or event occurs
- The likelihood of occurrence.